EVALUASI MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) PADA KANTOR WILAYAH DITJEN PERBENDAHARAAN NEGARA JAWA TIMUR

Lembar Pengesahan
TUGAS AKHIR

Disusun Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada

Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

MUSTAQIM SIGA
5211 105 703

Surabaya, Juli 2014

KETUA JURUSAN SISTEM INFORMASI

Dr.Eng Febriliyan Samopa, S.Kom, M.Kom
NIP 19730219 199802 1 001

EVALUASI MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) PADA KANTOR WILAYAH DITJEN PERBENDAHARAAN JAWA TIMUR

Disusun Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

Mustaqim Siga
5211 105 703

Disetujui Tim Penguji: Tanggal Ujian: Juli 2014
Periode Wisuda : September 2014

1. **Tony Dwi Susanto, S.T, M.T,Ph.D** ..... **(Pembimbing 1)**
2. **Bekti Cahyo H. S.Si, M.Kom** ..... **(Pembimbing 2)**
3. **Dr.Apol Pribadi Subriadi S.T, M.T** ..... **(Penguji 1)**
4. **Anisah Herdiyanti, S.Kom, M.Sc** ..... **(Penguji 2)**

SURABAYA
JULI, 2014

EVALUASI MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) PADA KANTOR WILAYAH DITJEN PERBENDAHARAAN NEGARA JAWA TIMUR

Nama Mahasiswa	**:**	**Mustaqim Siga**
NRP	**:**	**5211 105 703**
Jurusan	**:**	**Sistem Informasi FTIF-DJPBN**
Dosen Pembimbing	:	**Tony Dwi Susanto, S.T, M.T, Ph.D** **Bekti Cahyo Hidayanto, S.Si, M. Kom**

ABSTRAK

Dukungan teknologi informasi (TI) sangat diperlukan untuk menjamin terselenggaranya pelayanan prima Ditjen Perbendaharaan, khususnya Kantor Wilayah Ditjen Perbendaharaan (Kanwil DJPBN) sebagai instansi vertikal Ditjen Perbendaharaan di Daerah Tingkat I / Propinsi di seluruh Indonesia. Seiring dengan bertambahnya dukungan TI tersebut, risiko keamanan yang melekat pada teknologi informasi juga akan semakin bertambah. Faktor keamanan informasi adalah faktor penting dalam menjamin penerapan TI dapat berjalan dengan baik. Berdasarkan KMK No. 479/KMK.01/2010 maka kebijakan dan standar sistem manajemen keamanan informasi di lingkungan Kementerian Keuangan mengacu kepada ISO/IEC 27001:2005. ISO/IEC 27001:2005 merupakan dokumen standar internasional tentang sistem manajemen keamanan informasi atau

Information Security Management Sistem (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan dalam upaya untuk mengevaluasi, mengimplementasikan dan memelihara keamanan informasi di perusahaan berdasarkan "best practice" dalam pengamanan informasi

Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2005.

Dalam pelaksanaannya ada sejumlah aspek yang biasanya tidak dapat terpenuhi oleh instansi dalam rangka penerapan keamanan informasi berdasakan indeks KAMI tersebut. Faktor penyebab inilah yang kemudian menjadi aspek penentu penilaian lainnya secara krusial tentang penerapan indeks KAMI dalam institusi pemerintahan. Selain faktor penyebab, beberapa faktor kesuksesan juga diukur sebagai masukan bagi pihak manajerial dan organisasi secara keseluruhan demi meningkatkan tingkat kematangan organisasi dalam rangka pengelolaan keamanan informasi pada institusinya.

Berdasarkan uraian di atas, pada tugas akhir ini akan dibahas mengenai evaluasi manajemen keamanan informasi menggunakan indeks keamanan informasi (KAMI) dengan studi kasus pada Kanwil DJPBN Jawa Timur. Metode penelitian dalam penyusunan tugas akhir ini dimulai dari pemahaman kondisi existing pengelolaan keamanan informasi, studi literatur dan studi lapangan, kemudian pelaksanaan uji kesiapan menggunakan indeks KAMI,

analisis dan pembahasan serta penyusunan dokumen tugas akhir

Kata kunci : ***evaluasi, keamanan informasi, indeks KAMI, ISO IEC 27001:2005.***

Halaman ini sengaja dikosongkan

INFORMATION SECURITY MANAGEMENT EVALUATION USING INDEKS KEAMANAN INFORMASI (KAMI) IN KANTOR WILAYAH DITJEN PERBENDAHARAAN NEGARA JAWA TIMUR

Name	**:**	**Mustaqim Siga**
NRP	**:**	**5211 105 703**
Department	**:**	**Sistem Informasi FTIF-DJPBN**
Supervisor	:	**Tony Dwi Susanto, S.T, M.T, Ph.D** **Bekti Cahyo Hidayanto, S.Si, M. Kom**

ABSTRACT

Information technology support is needed to ensure the implementation of Director General of Treasury excellent service by Kantor Wilayah Ditjen Perbendaharaan as a vertical unit at 1st Degree State / Province entire Indonesia. However, the increase of IT in addition to support the processes also carries increasing risks. Security information factor is the important factor to ensure IT implementation becomes well. According to KMK No.479/KMK.01/2010 policy and standard information security management system (ISMS) in Ministry of Finance refer to ISO/IEC 27001:2005. ISO/IEC 27001:2005 is international standard documents of information security management system (ISMS) that provide general framework to evaluate, implementate and preserve information security according to the information security best practices.

Indeks KAMI is evaluation instruments to analyze information security level at government institution.

Evaluation conducted to areas that being scope of research that comply for every aspect defined by ISO/IEC 27001 : 2005.

In implementation, there are many aspect that can't be completed by institution using security information based on Indeks KAMI. This causalistic factors became the important aspect crutially to implement Indeks KAMI on government institution. Besides that, there are succesfull factors that must be counted as a presentation to manajerial and organization to increase maturity level at the institutional information security implementation.

Based on those reason, this research will focus on information security management system using Indeks KAMI with case study at Kanwil DJPBN Jawa Timur. The stage of this research starts with understanding of existing information security condition, literature study and observation study, next to evaluation of the readiness using standart, analysis, and compiling research documents.

Keyword : ***evaluation, information security, indeks KAMI, ISO/IEC 27001:2005***

BAB II
TINJAUAN PUSTAKA

Pada bagian ini akan dibahas mengenai tinjauan pustaka dan teori-teori yang mendukung dalam pengerjaan tugas akhir. Teori-teori tersebut antara lain; teori teknologi informasi, keamanan informasi, serta penjelasan Indeks KAMI.

2.1 Direktorat Jenderal Perbendaharaan

Berdasarkan PMK 184/PMK.01/2010 tentang Organisasi dan Tata Kerja Kementerian Keuangan, maka Direktorat Jenderal Perbendaharaan adalah unit eselon I yang bertugas merumuskan serta melaksanakan kebijakan dan standardisasi teknis di bidang perbendaharaan negara.

2.1.1 Kantor Pusat Direktorat Jenderal Perbendaharaan

Direktorat Jenderal Perbendaharaan atau selanjutnya disebut DJPBN adalah salah satu unit eselon I Kementerian Keuangan Republik Indonesia. Direktorat Jenderal Perbendaharaan memiliki tugas merumuskan serta melaksanakan kebijakan dan standardisasi teknis di bidang perbendaharaan negara sesuai dengan kebijakan yang ditetapkan oleh Menteri Keuangan, dan berdasarkan peraturan perundang-undangan yang berlaku. Dan dalam melaksanakan tugas dimaksud, Direktorat Jenderal Perbendaharaan menyelenggarakan fungsi:

a. Penyiapan perumusan kebijakan Kementerian Keuangan di bidang perbendaharaan negara;
b. Pelaksanaan kebijakan di bidang perbendaharaan negara sesuai dengan peraturan perundang-undangan yang berlaku;
c. Penyusunan standar, norma, pedoman, kriteria, dan prosedur di bidang perbendaharaan negara;

d. Pemberian bimbingan teknis dan evaluasi di bidang perbendaharaan negara;
e. Pelaksanaan administrasi Direktorat Jenderal

Hal tersebut sesuai dengan Peraturan Menteri Keuangan Nomor: 184/PMK.01/2010 Tentang Organisasi dan Tata Kerja Kementerian Keuangan

2.1.2 Kantor Wilayah Ditjen Perbendaharaan Negara Jawa Timur

Kantor Wilayah Direktorat Jenderal Perbendaharaan (Kanwil Ditjen Perbendaharaan) adalah unit eselon II secara vertikal di bawah Direktorat Jenderal Perbendaharaan dalam struktur organisasi pada Kementerian Keuangan. Unit eselon II ini bukanlah unit organisasi baru karena nomenklatur sebelumnya adalah Kantor Wilayah Direktorat Jenderal Anggaran. Nomenklatur Kantor Wilayah Direktorat Jenderal Perbendaharaan resmi digunakan pada tahun anggaran 2004 sesuai dengan Keputusan Menteri Keuangan Nomor: 302/KMK.01/2004 Tentang Susunan Organisasi Departemen Keuangan. Hal ini tidak terlepas dari pelaksanaan reformasi organisasi dan menajamen keuangan negara dan sebagai upaya menyelaraskan perangkat organisasi melalui penegasan fungsi Kementerian Keuangan atas amanat dari UU Nomor 17 Tahun 2003 tentang Keuangan Negara dan UU Nomor 1 Tahun 2004 tentang Perbendaharaan Negara

Tugas Kanwil Ditjen Perbendaharaan Provinsi Jawa Timur :

Melaksanakan koordinasi, pembinaan, penyuluhan, bimbingan teknis, penelaahan, monitoring, evaluasi, penyusunan laporan, verifikasi dan pertanggungjawaban

di bidang perbendaharaan dalam wilayah kerja Provinsi Jawa Timur berdasarkan peraturan perundang-undangan yang berlaku

Fungsi Kanwil Ditjen Perbendaharaan Provinsi Jawa Timur :

a. penelaahan, pengesahan, dan revisi dokumen pelaksanaan anggaran, serta penyampaian pelaksanaannya kepada instansi yang telah ditentukan;
b. penelaahan dan penilaian keserasian antara dokumen pelaksanaan anggaran dengan pelaksanaan di daerah;
c. pemberian bimbingan teknis pelaksanaan dan penatausahaan anggaran;
d. pemantauan realisasi pelaksanaan anggaran;
e. pembinaan teknissistem akuntansi;
f. pelaksanaan akuntansi dan penyusunan laporan keuangan pemerintah;
g. pemantauan dan evaluasi pelaksanaan penyaluran dana perimbangan;
h. pembinaan pengelolaan keuangan Badan Layanan Umum (BLU);
i. pembinaan pengelolaan penerimaan negara bukan pajak (PNBP);
j. pelaksanaan pengelolaan dana investasi dan pemberian pinjaman kepada daerah;
k. pengawasan kewenangan dan pelaksanaan teknis perbendaharaan dan bendahara umum;
l. pelaksanaan verifikasi atas pertanggungjawaban belanja program pension;
m. verifikasi dan penatausahaan pertanggungjawaban dana Perhitungan Fihak Ketiga (PFK);
n. pelaksanaan kehumasan;
o. pelaksanaan administrasi Kantor Wilayah Direktorat Jenderal Perbendaharaan

2.1.3 Nilai-nilai Kementerian Keuangan

Kementerian Keuangan mengembangkan nilai-nilai Kementerian Keuangan dari hasil peleburan dan kontemplasi nilai-nilai yang sebelumnya telah diterapkan secara berbeda pada masing-masing eselon satu. Peleburan ini penting untuk membangun kembali kesinergian seluruh jajaran kementerian keuangan serta untuk menunjukkan kepada masyarakat secara lebih jelas perubahan yang diwujudkan oleh Kementerian Keuangan secara keseluruhan. Penerapan nilai-nilai keutamaan Kementerian Keuangan ini menunjukkan bahwa Kementerian Keuangan memberikan warna spesifik bagi PNS di lingkungan Kementerian Keuangan tidak sama dengan PNS lainnya terutama dalam hal karakter dan budaya kerja. Penerapan nilai-nilai ini juga merupakan bagian dari langkah Kementerian Keuangan sebagai penggerak reformasi birokrasi di Indonesia agar nantinya penerapan nilai-nilai organisasi juga diterapkan dalam level birokrasi lainnya. Nilai-nilai Kementerian Keuangan Meliputi 5 Nilai dan 10 Perilaku Utama yang diinternalisasikan dalam setiap pegawainya. Nilai-nilai tersebut meliputi :

a. Integritas
b. Profesionalisme
c. Sinergi
d. Pelayanan
e. Kesempurnaan

Nilai-nilai Kementerian Keuangan ini diwujudkan dalam 10 perilaku utama yang meliputi :

a. Bersikap tulus, jujur, dan dapat dipercaya.
b. Menjaga martabat dan tidak melakukan hal-hal tercela.

c. Mempunyai keahlian dan pengetahuan yang luas.
d. Bekerja dengan hati.
e. Memiliki sangka baik, saling percaya dan menghormati.
f. Menemukan dan melaksanakan solusi terbaik.
g. Melayani dengan berorientasi pada kepuasan pemangku kepentingan.
h. Bersikap proaktif dan cepat tanggap.
i. Melakukan perbaikan terus menerus.
j. Mengembangkan inovasi dan kreativitas.

2.1.4 Satuan Kerja

Satuan Kerja atau selanjutnya disebut satker adalah instansi pemerintah baik pusat maupun daerah. Menurut Peraturan Menteri Keuangan Nomor 171/PMK.05/2007 tentang Sistem Akuntansi dan Pelaporan Keuangan Pemerintah Pusat, satker adalah Kuasa Pengguna Anggaran/Pengguna Barang yang merupakan bagian dari unit suatu organisasi pada Kementerian Negara/Lembaga yang melaksanakan satu atau beberapa kegiatan dari suatu program.

Satker yang menjadi objek penelitian tugas akhir ini adalah satker yang berada pada wilayah Kanwil DJPBN Jawa Timur.

2.2 Tata Kelola dan Tata Kelola Teknologi Informasi

Pengertian tata kelola menurut ISACA dalam buku IT Government Based on COBIT 4.1 (DJPBNM, 2007) adalah kumpulan proses yang saling terkait dan terstrukturisasi untuk mengarahkan dan mengontrol organisasi dalam mencapai tujuan. Sedangkan Rahmania mendefinisikan tata kelola sebagai struktur dan proses yang dibuat berdasarkan keputusan lembaga dan menyangkut praktek pengambilan keputusan.

Weill dan Ross yang dikutip oleh Jogiyanto dan Abdillah (2011) mendefinisikan tata kelola sistem dan teknologi informasi sebagai penspesifikasian hak keputusan dan rangka akuntabilitas untuk mengarahkan perilaku yang dInginkan dalam penggunaan IT.

2.3 Teknologi Informasi

Secara umum teknologi informasi adalah segala bentuk teknologi yang diterapkan untuk memproses dan mengirimkan informasi dalam bentuk eletronik (Lucas, 2000). Sedangkan menurut Alter (2002), teknologi informasi mencakup perangkat keras dan perangkat lunak untuk melaksanakan 1 (satu) atau sejumlah tugas pemrosesan data seperti menangkap, mentransmisikan, menyimpan, mengambil, memanipulasi atau menampilkan data. Pendapat berbeda dikemukakan oleh Turban, et al (1999), yang menggunakan istilah teknologi informasi untuk menjabarkan sekumpulan sekumpulan sistem informasi, pemakai dan manajemen. Dari beberapa pendapat diatas, dapat ditarik satu kesimpulan mengenai definisi teknologi informasi, yaitu segala bentuk teknologi yang terdiri atas perangkat lunak, perangkat keras, manusia, jaringan dan manajemen yang digunakan untuk menyimpan, memproses, dan mendistribusikan informasi kepada penggunaSatker yang menjadi objek penelitian tugas akhir ini adalah satker yang berada pada wilayah Kanwil DJPBN Jawa Timur.

2.4 Sistem Informasi

Menurut Hall (2001), sistem informasi adalah sebuah rangkaian prosedur formal dimana data dikelompokkan, diproses menjadi beberapa informasi dan didistribusikan kepada pemakai. Sedangkan menurut (Turban, et al, 1999), sebuah sistem informasi mengumpulkan, memproses, menyimpan, meng-analisis, menyebarkan informasi untuk tujuan yang spesifik. Dari beberapa pendapat diatas, dapat ditarik satu kesimpulan mengenai definisi sistem informasi,

yaitu suatu sistem yang secara umum terdiri atas sekumpulan komponen, prosedur pengumpulan, pemrosesan, penyimpanan, analisis dan penyebaran data/informasi kepada pengguna dimana komponen komponen maupun prosedur tersebut memiliki tujuan yang sama, dikerjakan bersama dengan menerima masukan dan menghasilkan luaran dalam sebuah proses transformasi yang teroganisir.

2.5 Keamanan Informasi

Keamanan informasi merupakan aspek penting dalam usaha melindungi aset informasi dalam suatu organisasi. Keamanan dapat berupa

- *Physical Security* yang memfokuskan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
- *Personal Security* yang overlap dengan '*physical security'* dalam melindungi orang-orang dalam organisasi
- *Operation Security* yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.
- *Communications Security* yang bertujuan mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi.
- *Network Security* yang memfokuskan pada pengamanan peralatan jaringan data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Keamanan informasi secara umum mempunyai 3 karakteristik penting antara lain :

- *Confidentiality* (kerahasiaan)
  Merupakan landasan utama dalam setiap kebijakan keamanan sistem informasi. Kerahasiaan ini merupakan seperangkat aturan yang, diberikan subyek diidentifikasidan objek, menentukan apakah suatu subjek tertentu dapat mendapatkan akses ke objek tertentu. Selain itu merupakan aspek yang memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
- *Integrity*
  Taraf kepercayaan terhadap sebuah informasi.Dalam konsep ini tercakup data integrity dan source integrity.Keutuhan data terwujud jika data/informasi belum diubah (masih asli), baik perubahan yang terjadi karena kesalahan atau dilakukan sengaja oleh seseorang.
- *Availability*
  Ketersediaan sumber informasi.Jika sebuah sumber informasi tidak tersedia ketika dibutuhkan, bahkan bisa lebih buruk lagi.Ketersediaan ini bisa terpengaruh oleh faktor teknis, faktor alam maupun karena faktor manusia. Meskipun ada tiga faktor yang berpengaruh, tetapi umumnya manusia adalah link paling lemahnya. Karenanya, wajar jika Anda perlu memperhatikan perlunya menggunakan tools untuk data security, misalnya sistem backup atau anti virus.

  Ketiga karakteristik ini dapat dihubungkan sebagai gambar berikut :

Gambar 2.1 Diagram CIA

2.6 ISO IEC 27001 : 2005

ISO/IEC 27001:2005 merupakan standard keamanan informasi yang dikembangkan oleh International Organization for Standarization (ISO) dan International Electrotecnical Comission (IEC). Diterbitkan pada bulan Oktober 2005, dengan tujuan untuk menciptakan sebuah panduan pembuatan, penerapan, pelaksanaan, pengawasan, analisis, pemeliharaan dan pendokumentasian Sistem Manajemen Keamanan Informasi (SMKI) yang dapat diacu oleh berbagai jenis organisasi diantaranya adalah lemabaga pemerintahan. ISO/IEC 27001:2005 didesain untuk memastikan bahwa kendali keamanan yang dibuat untuk melindungi aset-aset informasi dan menciptakan kepercayaan dengan pihak-pihak yang terkait sudah memadai dan sesuai (iso.org, 2006). Pemanfaatan ISO/IEC 27001:2005 digunakan untuk berbagai keperluan, antara lain sebagai berikut :

a. Sebagai panduan untuk merumuskan tujuan dan kebutuhan keamanan disebuah organisasi
b. Sebagai alat untuk memastikan bahwa risiko-risiko keamanan yang ada telah tertangani dengan efektif
c. Sebagai alat untuk memastikan bahwa standard keamanan yang digunakan oleh perusahaan telah mematuhi hokum dan perundang-undangan
d. Sebagai alat untuk menentukan status manajemen keamanan informasi pada sebuah organisasi

e. Sebagai panduan bagi auditor, baik internal maupun eksternal untuk menentukan kesesuaian antara SMKI yang ada dengan kebijakan, arahan dan standard yang diacu oleh organisasi
f. Sebagai panduan implementasi keamanan informasi dalam berbisnis

Struktur organisasi ISO/IEC 27001 dibagi dalam dua bagian besar yaitu :

1. Klausul : *Mandatory process*

Klausul (pasal) adalah persyaratan yang harus dipenuhi jika organisasi menerapkan SMKI dengan menggunakan standard ISO/IEC 27001

2. Annex A : *Security Control*

Annex A adalah dokumen referensi yang disediakan dan dapat dijadikan rujukan untuk menentukan kontrol keamanan apa (security control) yang perlu diimplementasikan dalam SMKI, yang terdiri dari 11 klausul kontrol keamanan, 39 kontrol objectif dan 133 kontrol. Untuk memahami persyaratan apa saja yang harus dipenuhi saat membangun SMKI sesuai standar ISO/IEC 27001 maka diperlukan pemahaman terhadap struktur isi dokumen ISO/IEC 27001

2.7 Indeks Keamanan Informasi (KAMI)

Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi. Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang

untuk dapat digunakan oleh instansi pemerintah dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya Tugas Pokok dan Fungsi yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan potret indeks kesiapan – dari aspek kelengkapan maupun kematangan – kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001:2009. Hasil evaluasi indeks KAMI menggambarkan tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001:2009 dan peta area tata kelola keamanan sistem informasi di instansi pemerintah. Sebagai gambaran, hasil evaluasi indeks KAMI

Alat evaluasi ini kemudian bisa digunakan secara berkala untuk mendapatkan gambaran perubahan kondisi keamanan informasi sebagai hasil dari program kerja yang dijalankan, sekaligus sebagai sarana untuk menyampaikan peningkatan kesiapan kepada pihak yang terkait (stakeholders). Penggunaan dan publikasi hasil evaluasi Indeks KAMI merupakan bentuk tanggungjawab penggunaan dana publik sekaligus menjadi sarana untuk meningkatkan kesadaran mengenai kebutuhan keamanan informasi di instansi pemerintah. Pertukaran informasi dan diskusi dengan instansi pemerintah lainnya sebagai bagian dari penggunaan alat evaluasi Indeks KAMI ini juga menciptakan alur komunikasi antar pengelola keamanan informasi di sector pemerintah sehingga semua pihak dapat mengambil manfaat dari lessonlearned yang sudah dilalui. Alat evaluasi Indeks KAMI ini secara umum ditujukan untuk digunakan oleh instansi pemerintah di tingkat pusat.Akan tetapi satuan kerja yang ada di tingkatan Direktorat Jenderal, Badan, Pusat atau Direktorat

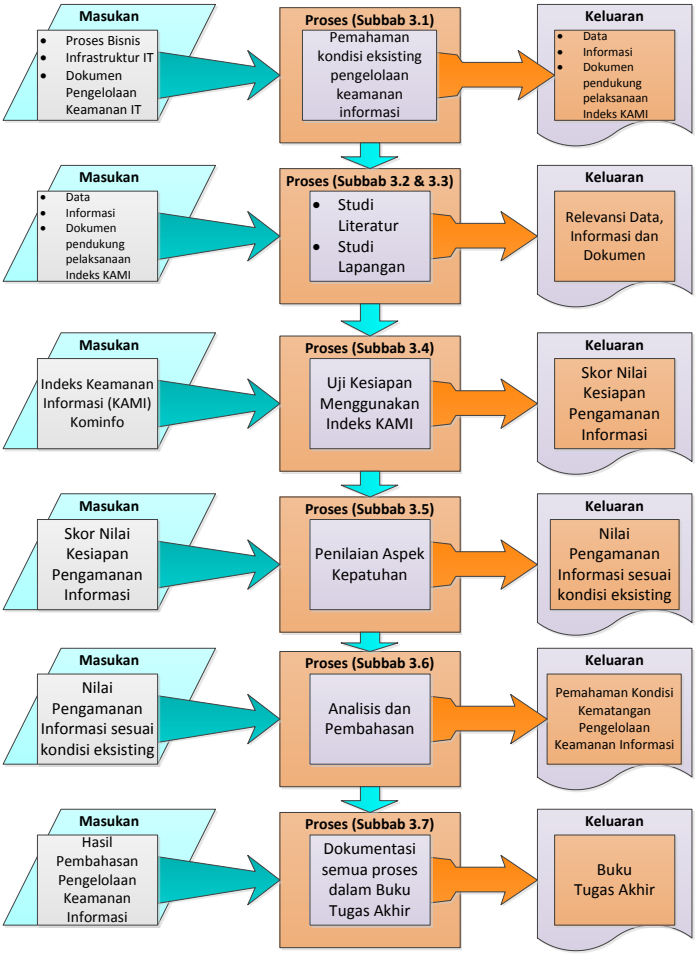
juga dapat menggunakan alat evaluasi ini untuk mendapatkan gambaran mengenai kematangan program kerja keamanan informasi yang dijalankannya.Evaluasi ini dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggung jawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya. (Panduan Penerapan Tata Kelola KIPPP, 2014)

Untuk implementasinya, indeks KAMI bagi Penyelenggara Pelayanan Publik meliputi 5 (lima) komponen, sebagai berikut :

1. Kebijakan dan manajemen organisasi;
2. Manajemen risiko (risk management);
3. Kerangka kerja;
4. Manajemen aset informasi;
5. dan teknologi

Pemaparan di atas sesuai dengan Surat Edaran Menteri Komunikasi dan Informatika.

BAB III
METODOLOGI PENGERJAAN TUGAS AKHIR



Gambar 3.1 Metode Pengerjaan Tugas Akhir

3.1 Pemahaman Kondisi *Eksisting* Pengelolaan Keamanan Informasi

Studi awal ini dilakukan dengan pengkajian mengenai kondisi kekinian Kanwil DJPBN Jawa Timur meliputi kelengkapan dokumentasi keamanan informasi, infrastruktur, proses bisnis organisasi, serta hal-hal lain yang diperlukan guna memperoleh gambaran umum tugas akhir. Tahapan ini didukung melalui observasi langsung dan pengumpulan data dan informasi dari berbagai pihak. Tahapan ini juga bertujuan untuk mengidentifikasi masalah mengenai kondisi dan gambaran umum permasalahan keamanan informasi yang ada di Kanwil DJPBN Jawa Timur. Dalam penelitian ini fokus permasalahan yang diungkapkan adalah kurang lengkap dan detailnya dokumen dan aspek pengelolaan dalam lingkungan keamanan informasi yang terdapat di lokasi penelitian.

3.2 Studi Literatur

Studi literatur merupakan tahapan dimana dilakukan pengumpulan literatur-literatur terkait dengan permasalahan baik berupa jurnal, text book, tugas akhir, tesis maupun sumber bacaan lain yang bisa didapatkan dari internet. Pada tahap ini data yang dicari adalah data penelitian sebelumnya, peraturan serta pemikiran beberapa pakar mengenai keamanan informasi dan hal lainnya menyangkut keamanan sistem informasi dengan indeks KAMI. Hasil akhir studi literatur ini adalah didapatkannya data, informasi, dokumen pendukung yang memiliki relevansi secara keilmuan dengan pelaksanaan pengelolaan keamanan informasi. Dengan adanya studi literatur pula, data dan pemahaman terhadap topik ini menjadi lebih jelas dan lengkap

3.3 Studi Lapangan

Dalam studi lapangan terbagi menjadi 2 metode, yaitu melalui metode observasi dan wawancara

3.3.1 Observasi

Observasi merupakan tahapan dimana dilakukan pengumpulan data dengan mengamati secara langsung keadaan yang sebenarnya terjadi di lapangan. Dalam tugas akhir ini, observasi dilakukan pada Kanwil DJPBN Jawa Timur untuk mengetahui kondisi nyata di Kanwil DJPBN Jawa Timur. Data yang dicari selama observasi adalah struktur organisasi, rencana strategis organisasi, kebijakan, proses-proses aliran informasi serta proses pengelolaan keamanan di dan/atau dari Kanwil DJPBN Jawa Timur. Dengan mengetahui proses tersebut dapat diperoleh data mengenai tindakan serta proses pengelolaan keamanan TI pada Kanwil DJPBN Jawa Timur

3.3.2 Wawancara

Wawancara merupakan salah satu upaya untuk mengidentifikasi permasalahan dengan cara memberikan pertanyaan secara langsung kepada pihak-pihak yang terlibat dalam permasalahan yang diangkat. Wawancara dilakukan untuk mendapatkan informasi mengenai kesadaran pegawai mengenai keamanan TI, latar belakang pegawai di bidang TI, pendidikan dan pelatihan bidang TI yang pernah diikuti oleh pegawai, peran dan tanggung jawab pegawai terhadap keamanan TI serta kebijakan penunjukan dan penempatan karyawan mengenai keamanan TI.

Wawancara dilakukan terhadap beberapa pihak yang terlibat langsung dalam kegiatan operasional Kanwil

DJPBN Jawa Timur dan bertanggung jawab terhadap keamanan informasi di Kanwil DJPBN Jawa Timur. Di antaranya Kepala Kantor cq. Kepala Bagian Umum serta Kepala Bidang Supervisi KPPN dan Kepatuhan Internal. Dengan data-data tersebut dapat diperoleh informasi mengenai kondisi pengelolaan TI pada Kanwil DJPBN Jawa Timur

3.4 Uji Kesiapan Menggunakan Indeks KAMI

Pada tahap ini dilakukan penilaian terdapat kebutuhan klasifikasi terhadap peran TIK dalam instansi atau cakupan evaluasinya. Selain itu penggambaran infrastruktur serta satuan kerjanya secara singkat dilakukan secara kuantitatif kepada responden.Tahapan penilaian keamanan jaringan hanya dilakukan secara menyeluruh pada semua area indeks KAMI. Penilaian dalam indeks KAMI dilakukan berdasarkan standar ISO/IEC 27001:2009. Seluruh pertanyaan yang ada dalam area tersebut akan dikelompokkan menjadi tiga kategori pengamanan, sesuai dalam penerapan standar ISO/IEC 27001. Pertanyaan yang terkait dengan kerangka kerja dasar keamanan informasi masuk dalam kategori "1", untuk efektivitas dan konsistensi penerapan termasuk dalam kategori "2", sedangkan hal-hal yang merujuk pada kemampuan untuk selalu meningkatkan kinerja keamanan informasi adalah kategori "3".

Pada ketiga kategori pertanyaan tersebut, responden kemudian diminta untuk menjawab setiap pertanyaan dengan pilihan status penerapan

a. Tidak Dilakukan
b. Dalam Perencanaan;
c. Dalam Penerapan atau Diterapkan Sebagian;
d. Diterapkan Secara Menyeluruh

Setiap jawaban akan diberi skor yang nilainya disesuaikan dengan tahapan penerapan (kategori) bentuk pengamanan. Tabel pemetaan skor dapat dilihat di bawah ini

	Kategori Pengamanan		
Status Pengamanan	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

Gambar 3.2 Kategori Pengamanan

Nilai untuk kategori pengamanan yang tahapannya lebih awal lebih rendah dibandingkan dengan nilai untuk tahapan selanjutnya. Hal ini sesuai dengan tingkat kompleksitas yang terlibat dalam proses penerapannya. Untuk pertanyaan kategori “3” hanya dapat diisi jika terkait dengan kategori “1” dan “2” sudah diisi dengan status minimal “Diterapkan sebagian”. Berikut contoh pertanyaan pada area Tata Kelola Keamanan Informasi

Bagian II: Tata Kelola Keamanan Informasi

Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				Status
#			Fungsi/Instansi Keamanan Informasi	
2.1	II	1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi, termasuk penetapan kebijakan terkait?	Tidak Dilakukan
2.2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Tidak Dilakukan
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Tidak Dilakukan
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Tidak Dilakukan
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Tidak Dilakukan
2.6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan
2.7	II	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Tidak Dilakukan
2.8	II	1	Apakah organisasi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Tidak Dilakukan
2.9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan
2.10	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal maupun eksternal untuk mengidentifikasikan persyaratan/kebutuhan pengamanan dan menyelesaikan permasalahan yang ada?	Tidak Dilakukan

Gambar 3.3 Contoh Pertanyaan Area Tata Kelola

Penilaian kemudian dilakukan dengan menganalisis jumlah di masing-masing area dan menganalisis apakah jumlah tersebut sudah mencapai atau melewati ambang batas pencapaian tingkat kematangan (TK) tertentu. Penghitungan dilakukan dengan dengan menerapkan prinsip:

1. Pencapaian Tingkat Kematangan dilakukan sesuai dengan kelengkapan dan (konsistensi + efektivitas) penerapannya.

2. Tingkat Kematangan yang lebih tinggi mensyaratkan kelengkapan, konsistensi dan efektivitas pengamanan di level bawahnya.
   a. Pencapaian suatu Tingkat Kematangan II dan III hanya dapat dilakukan apabila sebagian besar di Tingkat Kematangan sebelumnya [x-1] sudah "Diterapkan Secara Menyeluruh".
   b. Khusus untuk pencapaian TKIV dan TKV mengharuskan seluruh bentuk pengamanan di tingkat-tingkat sebelumnya sudah "Diterapkan Secara Menyeluruh." Hal ini memberikan efek

kesulitan yang lebih tinggi untuk mencapai 2 (dua) tingkatan terakhir tingkat kematangan.

c. Detail perhitungan ambang batas pencapaian Tingkat Kematangan I-V diuraikan di bagian lain dalam dokumen ini.

3. Untuk membantu memberikan uraian yang lebih detail, tingkatan ini ditambah dengan tingkatan antara - I+, II+, III+, dan IV+, sehingga total terdapat 9 tingkatan kematangan. Sebagai awal, semua responden akan diberikan kategori kematangan Tingkat I. Sebagai padanan terhadap standar ISO/IEC 2700:2005, tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah Tingkat III+.

3.5 Penilaian Aspek Kepatuhan

Untuk memproses data ke tahap selanjutnya yaitu penilaian terhadap semua data yang telah dikumpulkan, maka perlu dilakukan adanya validasi sesuai dengan kondisi nyata pengamanan informasi yang ditangani Kanwil DJPBN Jawa Timur. Validasi data dilakukan dengan menggunakan sejumlah data dan informasi pendukung diantaranya:

- Hasil observasi langsung
- Dokumen pendukung seperti Kebijakan, Pedoman, Prosedur, Standar, Instruksi Kerja
- Dokumentasi seperti foto dan video
- dll

3.6 Analisis dan Pembahasan

Pada tahapan ini, kelengkapan dan kematangan sesuai hasil penilaian yang telah dilakukan sebelumnya dianalisis. Analisis secara umum dibahas pada semua area keamanan indeks KAMI yang didapat dari tahap sebelumnya. Hasil

analisis yang diperoleh menjadi bahan pembahasan akan evaluasi keamanan informasi yang terdapat di Kanwil DJPBN Jawa Timur.

Untuk analisis kelengkapan dilakukan dengan validasi berdasarkan indeks keamanan informasi (KAMI) terhadap nilai pengisian yang dilakukan oleh responden dengan mengacu kepada skor penilaian kelengkapan sebagaimana termuat dalam Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik section A.9 Mekanisme Penilaian Kelengkapan (Gambar 3.4). Sedangkan untuk analisis kematangan pengelolaan keamanan informasi dilakukan dengan menganalisis jumlah di masing-masing area dan menganalisis apakah jumlah tersebut sudah mencapai atau melewati ambang batas pencapaian tingkat kematangan (TK) tertentu. Hasil dari masing-masing area akan menjadi acuan pemetaan dan pemeringkatan dan menjadi dasar bagi pemberian OPINI tentang kondisi tata kelola keamanan informasi di Kanwil DJPBN Propinsi Jawa Timur berdasarkan kategori :

a. Pasif
b. Reaktif
c. Aktif
d. Proaktif
e. Terkendali, dan
f. Optimal.

	Tata Kelola	Manajemen Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi	
Jumlah pertanyaan Tahap 1	8	9	11	21	13	
Jumlah pertanyaan Tahap 2	6	4	8	9	10	
Jumlah pertanyaan Tahap 3	6	2	7	4	1	
Total jumlah pertanyaan	20	15	26	34	24	(119)
Jumlah skor maksimal	**114**	**69**	**144**	**153**	**108**	**(588)**
Batas Skor Min untuk Skor Tahap Penerapan 3*	40	34	54	78	66	
Jumlah Pertanyaan Tk Kematangan II	**11**	**9**	**10**	**26**	**13**	
Jumlah pertanyaan Tahap 1	*8*	*9*	*8*	*21*	*13*	
Jumlah pertanyaan Tahap 2	*3*	*0*	*2*	*5*	*0*	
Jumlah Pertanyaan Tk Kematangan III	**3**	**2**	**11**	**8**	**10**	
Jumlah pertanyaan Tahap 1	*0*	*0*	*3*	*0*	*0*	
Jumlah pertanyaan Tahap 2	*3*	*2*	*6*	*4*	*10*	
Jumlah pertanyaan Tahap 3	*0*	*0*	*2*	*4*	*0*	
Jumlah Pertanyaan Tk Kematangan IV	**6**	**2**	**3**	**0**	**1**	
Jumlah pertanyaan Tahap 2	*0*	*0*	*0*	*0*	*0*	
Jumlah pertanyaan Tahap 3	*6*	*2*	*3*	*0*	*1*	
Jumlah Pertanyaan Tk Kematangan V	**0**	**2**	**2**	**0**	**0**	
Jumlah pertanyaan Tahap 3	*0*	*2*	*2*	*0*	*0*	

Gambar 3.4 Penilaian Skor

Dalam tahapan analisis dan pembahasan ini pula dilaksanakan pengumpulan bukti dan temuan dalam pelaksanaan pengamanan informasi dan identifikasi faktor penyebab beserta faktor pendukung dalam pengimplementasian pengamanan berdasarkan indeks KAMI untuk status pengelolaan keamanan informasi lingkup Kanwil DJPBN Jawa Timur. Selanjutnya dilakukan penyajian atas identifikasi faktor-faktor penyebab, usulan tindakan perbaikan, beserta tindak lanjut dan verifikasi dengan mengadaptasi evaluasi sistem manajemen keamanan informasi yang menggunakan form CPAR (Gambar 3.6). Untuk pengisian CPAR itu sendiri dilakukan berdasarkan kaidah PLOR yaitu :

1. P (*Problem*) : Apa permasalahannya / ketidaksesuaiannya, yang dalam hal ini adalah menyangkut aspek pada penilaian indeks KAMI.
2. L (*Location*) : Dimana lokasi terjadinya permasalahan / ketidaksesuaiannya, yang dalam hal ini adalah Kanwil DJPBN Jawa Timur

3. O (*Objective*) : Obyektif / bukti ketidaksesuaian, yang juga mencakup temuan dalam pelaksanaan keamanan informasi berdasarkan penilaian indeks KAMI.
4. R (*Reference*) : Referensi yang dipakai untuk menetapkan suatu hal dinyatakan tidak sesuai (prosedur, standar, instruksi kerja, dan lain-lain), yang dalam hal ini ditujukan pada kebijakan, pedoman, panduan, prosedur, tata kelola, perundang-undangan, SOP, nota dinas dan surat tugas terkait pengelolaan keamanan informasi lingkup Kanwil DJPBN Jawa Timur.

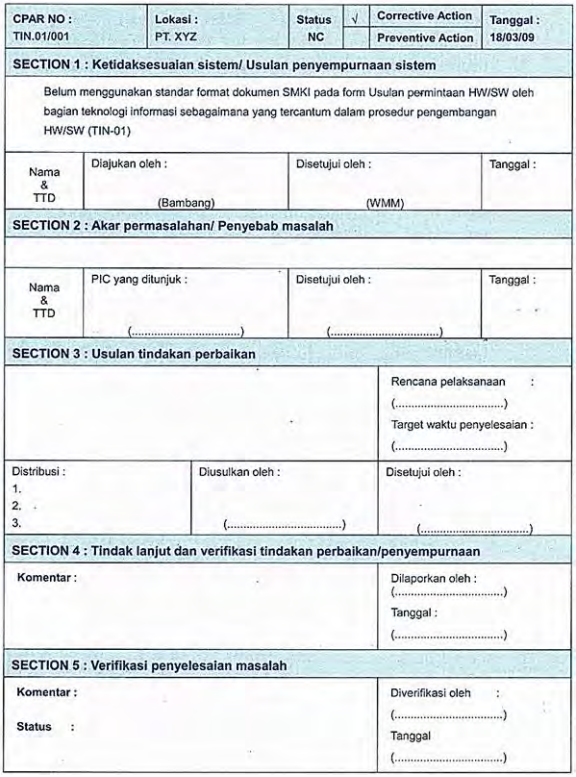
Secara terpadu seluruh jawaban pada pertanyaan indeks KAMI akan memunculkan temuan berdasarkan pembuktian pada Lampiran B – G. Temuan ini menjadi dasar dalam penentuan faktor penyebab dan pendukung. Berdasarkan analisis faktor penyebab dan pendukung inilah kemudian diwujudkan usulan tindakan perbaikan pada form CPAR pada Lampiran H – L. Dan berdasarkan seluruh usulan tindakan perbaikan maka dibuatkanlah sebuah rangkuman generalisasi dalam rekomendasi umum pada tiap area pengelolaan keamanan informasi sebagaimana tertuang pada Bab VI.

Gambar 3.5 Alur pembuatan usulan dan rekomendasi

3.7 Penyusunan Dokumen Tugas Akhir

Setelah hasil analisis dan pembahasan didapatkan, maka langkah selanjutnya adalah pendokumentasian keseluruhan pelaksanaan proses diatas. Dokumentasi ini meliputi proses pelaksanaan uji kesiapan menggunakan indeks

KAMI, analisis dan pembahasan serta pembuatan laporan berdasarkan adaptasi form CPAR. Setiap tahap dalam pelaksanaan proses SMKI ini didokumentasikan ke dalam buku tugas akhir. Pembuatan buku tugas akhir juga dilakukan guna mengetahui apakah hasil tugas akhir sesuai dengan tujuan-tujuan yang telah ditetapkan serta memberikan saran berupa pengembangan atau perbaikan penelitian selanjutnya



CPAR NO : TIN.01/001	Lokasi : PT. XYZ	Status NC	√	Corrective Action / Preventive Action	Tanggal : 18/03/09
SECTION 1 : Ketidaksesuaian sistem/ Usulan penyempurnaan sistem					
Belum menggunakan standar format dokumen SMKI pada form Usulan permintaan HW/SW oleh bagian teknologi informasi sebagaimana yang tercantum dalam prosedur pengembangan HW/SW (TIN-01)					
Nama & TTD	Diajukan oleh : (Bambang)	Disetujui oleh : (WMM)			Tanggal :
SECTION 2 : Akar permasalahan/ Penyebab masalah					
Nama & TTD	PIC yang ditunjuk : (.....)	Disetujui oleh : (.....)			Tanggal :
SECTION 3 : Usulan tindakan perbaikan					
				Rencana pelaksanaan : (.....) Target waktu penyelesaian : (.....)	
Distribusi : 1. 2. 3.	Diusulkan oleh : (.....)	Disetujui oleh : (.....)			
SECTION 4 : Tindak lanjut dan verifikasi tindakan perbaikan/penyempurnaan					
Komentar :				Dilaporkan oleh : (.....) Tanggal : (.....)	
SECTION 5 : Verifikasi penyelesaian masalah					
Komentar : **Status :**				Diverifikasi oleh : (.....) Tanggal (.....)	

Gambar 3.6 Form CPAR

Halaman ini sengaja diskosongkan

BAB IV
ANALISIS DATA

4.1 Pemahaman Kondisi *Existing* Pengelolaan Keamanan Informasi

Observasi ini dilakukan dengan mengamati kondisi eksisting baik dari profil Kanwil Dirjen Perbendaharaan Jawa Timur, proses bisnis, dan infrastruktur. Hasil observasi digunakan sebagai langkah awal untuk melakukan penilaian keamanan informasi di Kanwil DJPBN Provinsi Jawa Timur.

a. Profil Kanwil DJPBN Jawa Timur

   Kantor Wilayah DJPBN Jawa Timur merupakan instansi vertikal di lingkungan Direktorat Jenderal Perbendaharaan Departemen Keuangan Republik Indonesia. Kanwil DJPBN Jawa Timur beralamat di Gedung Keuangan Negara I Lantai 1-4 Jalan Indrapura No. 5 Surabaya.

   Sebagai instansi vertikal di bawah Direktorat Jenderal Perbendaharaan, Kanwil DJPBN Jawa Timur menjalankan tugas melaksanakan koordinasi, pembinaan, supervisi, bimbingan teknis, dukungan teknis, monitoring, evaluasi, penyusunan laporan, verifikasi dan pertanggungjawaban di bidang perbendaharaan berdasarkan peraturan perundang-undangan.

   Kantor Wilayah DJPBN Jawa Timur dalam menjalankan tugasnya didukung oleh 1 (satu) bagian umum dan 4 (empat) bidang, yaitu:

   1. Bagian Umum
   2. Bidang Pembinaan Pelaksanaan Anggaran I
   3. Bidang Pembinaan Pelaksanaan Anggaran II
   4. Bidang Pembinaan Akuntansi dan Pelaporan Keuangan, dan

5. Bidang Supervisi KPPN dan Kepatuhan Internal

Masing - masing bidang dipimpin oleh Kepala Bidang dan didukung oleh beberapa Kepala Seksi dan Pelaksana.

b. Visi dan Misi Kanwil DJPBN Jawa Timur

1. Visi

   Menjadi Pengelola Perbendaharaan Negara yang Profesional, Transparan dan Akuntabel dalam Proses Mewujudkan Bangsa yang Mandiri dan Sejahtera.

2. Misi

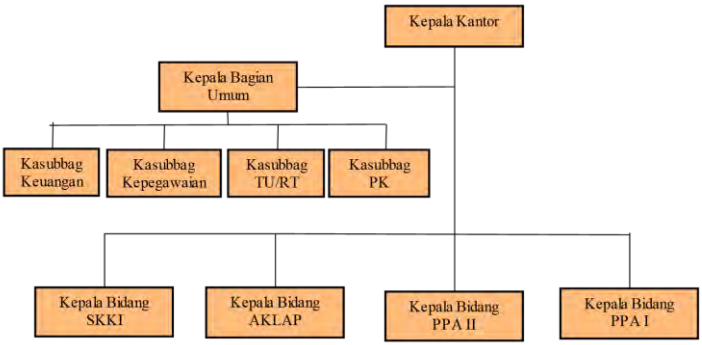
   - Mewujudkan pelaksanaan anggaran yang berbasis kinerja secara tertib, taat pada peraturan perundang-undangan, efisien, efektif, transparan dan bertanggung jawab serta memperhatikan rasa keadilan dan kepatuhan.
   - Mewujudkan pengelolaan kas negara yang efisien, efektif, transparan dan akuntabel.
   - Menghasilkan pelayanan di bidang perbendaharaan dan informasi keuangan yang cepat, tepat dan akurat.
   - Mewujudkan pengelolaan piutang pemerintah yang dananya bersumber dari dalam dan luar negeri dan kredit program secara profesional, berkelanjutan dan akuntabel.

3. Fungsi Kanwil DJPBN Jawa Timur

   - Penelaahan, pengesahan, dan revisi dokumen pelaksanaan anggaran serta penyampaian pelaksanaannya kepada instansi yang telah ditentukan;
   - Penelaahan dan penilaian keserasian antara dokumen pelaksanaan anggaran dengan pelaksanaan di daerah;

- Pemberian bimbingan teknis pelaksanaan dan penatausahaan anggaran;
- Pemantauan realisasi pelaksanaan anggaran;
- Pembinaan teknis sistem akuntansi;
- Pelaksanaan akuntansi dan penyusunan laporan keuangan pemerintah;
- Pemantauan dan evaluasi pelaksanaan penyaluran dana perimbangan;
- Pembinaan pengelolaan keuangan badan layanan umum (BLU);
- Pembinaan pengelolaan penerimaan negara bukan pajak;
- Pelaksanaan pengelolaan dana investasi dan pinjaman kepada daerah;
- Pengawasan kewenangan dan pelaksanaan teknis perbendaharaan dan bendahara umum negara;
- Pelaksanaan verifikasi atas pertanggungjawaban belanja program pensiun;
- Verifikasi dan penatausahaan atas pertanggungjawaban dana Perhitungan Fihak Ketiga (PFK);
- Pelaksanaan kehumasan; dan
- Pelaksanaan administrasi Kantor Wilayah SDM yang profesional.

c. Struktur Organisasi



Gambar 4.1 Struktur Organisasi Kanwil DJPBN Jawa Timur

Daftar susunan Pejabat Kanwil DJPBN Jawa Timur :

- Kepala Kantor : Pardiharto
- Kepala Bagian Umum : Hari Utomo
- Kasubbag Keuangan : Gatot Witjaksono
- Kasubbag Kepegawaian : Djoko D Kardianur
- Kasubbag TU/RT : Abdul Wakhid
- Kasubbag PK : Hari Purwono
- Kepala Bidang PPA I : Joko Pramono
- Kepala Bidang PPA II : Halistiani Trisarita
- Kepala Bidang AKLAP : Rabindhra Aldy
- Kepala Bidang SKKI : Siswoto

d. Struktur Bidang SKKI (Supervisi KPPN dan Kepatuhan Internal)

Secara umum fungsi terkait dengan teknologi informasi adalah tanggung jawab dari seluruh pegawai pada Kanwil DJPBN Jawa Timur namun untuk proses bisnis dan teknis

aplikasi lebih banyak menjadikan Bidang SKKI sebagai sumber informasi dan dukungan aplikasi. Berikut Kepala Bidang dan daftar Kepala Seksi pada Bidang SKKI beserta tanggung jawab

1. Siswoto (Kepala Bidang SKKI), bertanggung jawab melaksanakan pembinaan proses bisnis, supervisi, implementasi, dan bimbingan teknis operasional aplikasi pada KPPN, penilaian kinerja dan pemenuhan standar tata kelola KPPN, pemantauan pengendalian intern, pengelolaan risiko, kepatuhan terhadap kode etik dan disiplin, dan tindak lanjut hasil pengawasan, serta perumusan rekomendasi perbaikan proses bisnis.
2. Kemas Yusman (Kasi Kepatuhan Internal), bertanggung jawab melakukan penyiapan bahan koordinasi dan pemantauan pengendalian intern, pengelolaan pengaduan, pengelolaan risiko, kepatuhan terhadap kode etik dan disiplin pegawai, dan tindak lanjut hasil pengawasan, serta penyiapan bahan rekomendasi perbaikan proses bisnis dan laporan hasil penindakan kepatuhan internal.
3. Hadi Susanto Resbowo (Kasi Supervisi Proses Bisnis), bertanggung jawab melakukan pembinaan proses bisnis pelaksanaan tugas Kuasa BUN pada KPPN, pelayanan perbendaharaan, dan penilaian kinerja KPPN serta monitoring dan evaluasi pemenuhan standar tata kelola.
4. Sonny Kurniawan (Kasi Supervisi Teknis Aplikasi), bertanggung jawab melakukan pemantauan, supervisi, implementasi, bimbingan teknis operasionalisasi, dan monitoring standardisasi infrastruktur aplikasi.

e. Gedung Keuangan Negara I

Secara fisik, gedung Kanwil DJPBN Jawa Timur merupakan bagian dari Gedung Keuangan Negara

Surabaya I. Gedung Keuangan Negara (GKN) merupakan milik Kementerian Keuangan. GKN ini berfungsi sebagai kantor pelayanan bagi layanan publik Kementerian keuangan secara umum, yang meliputi pelayanan pajak, bea cukai, perbendaharaan, kekayaan negara dll.

Kementerian Keuangan memiliki 20 GKN yang tersebar di 16 ibukota propinsi dan 4 kabupaten/ kota di seluruh Indonesia. Gedung Keuangan Negara secara administratif berada di bawah koordinasi unit Sekretariat Jenderal Kementerian Keuangan. Pembinaan terhadap GKN dilaksanakan oleh Biro Perlengkapan. Sesuai Keputusan Menteri Keuangan Nomor 124/KMK.01/1983 tanggal 7 Februari 1983, pengelolaan aset Gedung Keuangan Negara dilakukan oleh Kepala Rumah Tangga GKN. Adapun tugas/kewajiban dan tanggung jawab Kepala Perwakilan Kementerian Keuangan dan Kepala Rumah Tangga GKN antara lain adalah sebagai berikut:

a. Kepala Rumah Tangga GKN ditetapkan oleh Menteri Keuangan dari Pejabat dalam lingkuangan Kementerian Keuangan yang berkantor di GKN, atas usul Kepala Perwakilan Kementerian Keuangan;
b. Kepala Rumah Tangga GKN bukan merupakan jabatan/organisasi struktural;
c. Kepala Rumah Tangga GKN diberi wewenang pengelolaan anggaran perawatan GKN, dan dalam melaksanakan tugasnya bertanggung jawab kepada Menteri Keuangan secara hierarkis melalui Kepala Perwakilan dan Sekretariat Jenderal Kementerian Keuangan;
d. Kepala Rumah Tangga GKN bertanggung jawab atas perawatan dan pemeliharaan umum kebersihan, saniter, keamanan dan ketertiban lingkungan GKN;

e. Kepala Rumah Tangga GKN diwajibkan bekerja sama dengan Kepala Perwakilan dan para Kepala Kantor dalam menentukan kebijaksanaan pokok dan pengawasan pengelolaan dan pemeliharaan GKN.

Gedung Keuangan Negara Surabaya I terletak di jalan Indrapura Nomer 5 Surabaya. GKN Surabaya I memiliki luas area 16.898 m2, dan dengan tahun perolehan 1963.
Gedung Keuangan Negara Surabaya I yang ditunjang dengan kapasitas listrik 2.250 KVA merupakan kantor bagi beberapa satuan kerja instansi vertikal Kementerian Keuangan di Surabaya. Satuan kerja yang beralamat di GKN Surabaya I yaitu:

a. Kanwil DJPBN Propinsi Jatim, yang berada pada lantai 1, 2 dan 3 dengan luas lahan 3127,48 m2.
b. KPTIK BMN Surabaya, yang berada pada lantai 2 dengan luas lahan 421,36 m2.
c. KPPN Surabaya I, yang berada pada lantai 3 dan 4 dengan luas lahan 1.589,12 m2.
d. KPKNL Surabaya, yang berada pada lantai 1, 5, 6 dengan luas lahan 1.632,72 m2.
e. Pengadilan Pajak Surabaya, yang berada pada lantai 6 dengan luas lahan 751,68 m2.
f. KPP Pratama Surabaya Krembangan, yang berada pada lantai 1, 2, 3 dengan luas lahan 2.707,22 m2.
g. KPP Pratama Surabaya Pabean CTK, yang berada pada lantai 1, 2, 3 dengan luas lahan 2.398,44 m2.

f. Sistem Perbendaharaan dan Anggaran Negara

Dari hasil pengamatan, terdapat satu sistem utama yang menyokong seluruh proses bisnis Dirjen Perbendaharaan baik Kantor Pusat maupun Kanwil DJPBN Jawa Timur

yaitu Sistem Perbendaharaan dan Anggaran Negara (SPAN). SPAN sendiri adalah Sistem Informasi yang menggabungkan beberapa fungsi seperti Perencanaan Anggaran, Pelaksanaan Anggaran, Manajemen Kas, serta Akuntansi dan Pelaporan dalam satu sistem aplikasi. SPAN juga merupakan sistem informasi Keuanagan Negara yang terintegrasi dalam mendokumentasikan setiap transaksi keuangan dan mendukung penyajian laporan keuangan dan manajerial, didesain dengan relasi yang baik antara pemilihan software, hardware, SDM, prosedur, kontrol, dan data serta operasi terotomasi secara penuh bermuara pada database yang terpusat. Keseluruhan keunggulan ini menjadikan proses bisnis utama Dirjen Perbendaharaan terkait dengan teknologi informasi menjadi tanggungjawab Pusat dengan porsi yang lebih maksimal. Hal ini pula yang telah menjadikan kontrol keamanan informasi menjadi sangat efisien karena proteksi utama sistem telah terintegrasi dan fungsi proteksi pada eselonisasi II dan III lebih kepada kontrol akses dan 10 aspek keamanan informasi lainnya dalam porsi yang lebih minim.

g. Kebijakan dan peraturan terkait pengelolaan keamanan informasi

Sebagai dasar hukum utama dalam seluruh pelaksanaan pengelolaan keamanan informasi, sejumlah kebijakan dan peraturan pengelolaan keamanan yang menjadi dasar penerapan diantaranya :

- KMK. No.40/KMK.01/2010 tentang Rencana Strategis Kementerian Keuangan tahun 2010 – 2014.
- KMK No.479/KMK.01/2010 tentang Kebijakan dan Standar Manajemen Keamanan Informasi di Lingkungan Kementerian Keuangan
- KMK No. 512/KMK.01/2009 tentang Kebijakan dan Standar Penggunaan Akun dan Kata Sandi, Surat

Elektronik, dan Internet di lingkungan Departemen Keuangan
- KMK. No. 350/KMK.01/2010 tentang Kebijakan dan Standar Pengelolaan Data Elektronik di lingkungan Kementerian Keuangan
- KMK No. 274/KMK.01/2010 tentang Kebijakan dan Standar Pertukaran Data Elektronik di lingkungan Kementerian Keuangan
- KMK No. 351/KMK.01/2011 tentang Kebijakan dan Standar Siklus Pengembangan Sistem Informasi di lingkungan Kementerian Keuangan
- dll

4.2 Studi Literatur

Hasil pada tahap ini telah dicantumkan pada Bab III.

4.3 Studi Lapangan

Studi lapangan dilakukan untuk keseluruhan aspek pada Kanwil DJPBN Jawa Timur. Aktivitas ini dikerjakan setelah mendapatkan pemahaman terkait keamanan informasi yang jelas dari hasil observasi awal.

Langkah selanjutnya adalah pengumpulan data dari kondisi kekinian Kanwil DJPBN Jawa Timur, juga dilakukan pengumpulan Temuan sebagai validasi hasil evaluasi keamanan informasi nantinya. Pengumpulan data ini meliputi dokumen pendukung terkait dengan area pada indeks KAMI meliputi tata kelola, risiko, kerangka kerja, aset dan teknologi.

4.4 Uji Kesiapan Menggunakan Indeks KAMI

Pelaksanaan uji kesiapan penilaian keamanan informasi menggunakan indeks KAMI dilaksanakan pada rentang 10 Maret 2014 – 24 Maret 2014 dengan menggunakan penilaian berdaarkan Indeks KAMI Kementerian Kominfo versi 2.3 19 April 2012. Responden adalah Bapak Hari Utomo sebagai kepala Bagian

Umum dan Bapak Heru Susanto selaku Pelaksana Supervisi Teknis Aplikasi Bidang (SKKI) Supervisi KPPN dan Kepatuhan Internal

4.4.1 Menetapkan peran atau tingkat kepentingan TIK secara umum di instansi

Tahap ini menjelaskan parameter penilaian untuk mengukur peran dan tingkat kepentingan TIK pada Kanwil DJPBN Jawa Timur. Peran dan tingkat kepentingan pada aplikasi KAMI dibagi menjadi 4 level. 4 level itu antara lain: rendah, sedang, tinggi dan kritis. Berikut pembagian level dalam menetapkan peran TIK :

Peran TIK				
Rendah		Indeks (Skor Akhir)		Status Kesiapan
0	12	1	124	Tidak Layak
		125	272	Perlu Perbaikan
		273	585	Baik/Cukup
Sedang		Skor Akhir		Status Kesiapan
13	24	0	174	Tidak Layak
		175	312	Perlu Perbaikan
		313	588	Baik/Cukup
Tinggi		Skor Akhir		Status Kesiapan
25	36	0	272	Tidak Layak
		273	392	Perlu Perbaikan
		393	588	Baik/Cukup
Kritis		Skor Akhir		Status Kesiapan
37	48	0	333	Tidak Layak
		334	453	Perlu Perbaikan
		454	588	Baik/Cukup

Gambar 4.2 Pembagian Level Pada Indeks KAMI

Berikut hasil penilaian Peran TIK di Kanwil DJPBN Jawa Timur :

Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi			
Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi anda.			
[Tingkat Kepentingan] Minim; Rendah; Sedang; Tinggi; Kritis		**Status**	Skor
#	**Karakteristik Instansi**		
1.1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis	Minim	0
1.2	Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis	Rendah	1
1.3	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas Pokok	Tinggi	3
1.4	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Kritis	4
1.5	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda	Kritis	4
1.6	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda	Kritis	4
1.7	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi	Kritis	4
1.8	Tingkat sensitifitas pengguna sistem TIK di Instansi anda	Kritis	4
1.9	Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya	Kritis	4
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda	Kritis	4
1.11	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK	Kritis	4
1.12	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	Kritis	4
	Skor Peran dan Tingkat Kepentingan TIK di Instansi	**40**	

Gambar 4.3 Contoh Hasil Penilaian

Menurut hasil di atas yaitu **40** (*catatan* : *akan divalidasi dalam penilaian aspek kepatuhan*) menunjukkan tingkat ketergantungan Kanwil DJPBN Jawa Timur yang kritis dalam proses bisnis yang dijalankannya. Hasil kuisioner untuk peran TIK ini juga digunakan sebagai acuan dalam menganalisis capaian serta tingkat kepentingan dan kematangan Kanwil DJPBN Jawa Timur dalam hal implementasi TIK.

4.4.2 Menilai kesiapan keamanan dengan indeks KAMI

Pada tahapan penilaian terdapat kebutuhan klasifikasi terhadap peran TIK dalam instansi atau cakupan evaluasinya. Selain itu penggambaran infrastruktur serta satuan kerjanya secara singkat dilakukan secara kuantitatif kepada responden. Tahapan penilaian

keamanan informasi akan dilakukan secara menyeluruh pada semua area indeks KAMI. Penilaian dalam indeks KAMI dilakukan berdasarkan standar ISO/IEC 27001:2009. Seluruh pertanyaan yang ada dalam area tersebut akan dikelompokkan menjadi tiga kategori pengamanan, sesuai dalam penerapan standar ISO/IEC 27001. Pertanyaan yang terkait dengan kerangka kerja dasar keamanan informasi masuk dalam kategori "1", untuk efektivitas dan konsistensi penerapan termasuk dalam kategori "2", sedangkan hal-hal yang merujuk pada kemampuan untuk selalu meningkatkan kinerja keamanan informasi adalah kategori "3".

Pada ketiga pertanyaan tersebut, responden kemudian diminta untuk menjawab setiap pertanyaan dengan pilihan status penerapan

- Tidak Dilakukan
- Dalam Perencanaan;
- Dalam Penerapan atau Diterapkan Sebagian;
- Diterapkan Secara Menyeluruh

Setiap jawaban akan diberi skor yang nilainya disesuaikan dengan tahapan penerapan (kategori) bentuk pengamanan. Tabel pemetaan skor dapat dilihat di bawah ini

	Kategori Pengamanan		
Status Pengamanan	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

Gambar 4.4 Pemetaan Skor

Terdapat beberapa kategori kelompok pertanyaan berdasarkan tingkat kelengkapan pengamanannya

a. Kategori I berdasarkan Area yang terkait dengan bentuk kerangka kerja dasar keamanan informasi

b. Kategori II berdasarkan Penilaian tingkat efektifitas dan konsistensi penerapannya
c. Kategori III berdasarkan Kemampuan untuk selalu meningkatkan kinerja keamanan informasi

Terdapat beberapa kondisi tingkat kematangan :

a. Tingkat I - Kondisi Awal
b. Tingkat II - Penerapan Kerangka Dasar
c. Tingkat III - Terdefinisi dan Konsisten
d. Tingkat IV - Optimal

Tingkat kematangan menunjukkan kepedulian mengenai pengamanan baik secara manajerial atau secara teknis. Tingkat keamtangan juga menunjukkan rutinitas kegiatan pengamanan yang telah dilaksanakan. Berikut keterangan warna tabel berdasarkan tingkat, kategori, dan status pengamanan

Keterangan warna tabel :

Tingkat Keamanan		Tingkat Kematangan Keamanan II
		Tingkat Kematangan Keamanan III
		Tingkat Kematangan Keamanan IV
		Tingkat Kematangan Keamanan V
Kategori Pengamanan		Kategori Kelengkapan Pengamanan I
		Kategori Kelengkapan Pengamanan II
		Kategori Kelengkapan Pengamanan III
Status Pengamanan		Tidak Dilakukan
		Dalam Perencanaan
		Dalam Penerapan / Diterapkan Sebagian
		Diterapkan Secara Menyeluruh

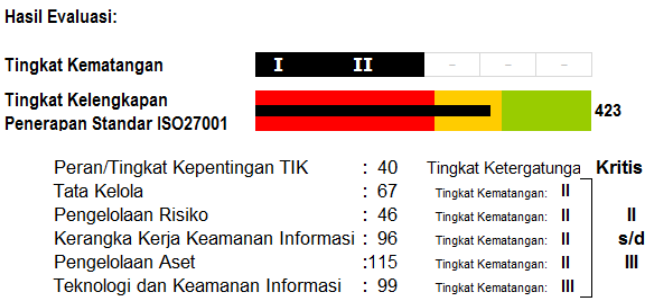
Gambar 4.5 Definisi Tingkat Kematangan Indeks KAMI

Nilai untuk kategori pengamanan yang tahapannya lebih awal lebih rendah dibandingkan dengan nilai untuk tahapan selanjutnya. Hal ini sesuai dengan tingkat kompleksitas yang terlibat dalam proses penerapannya. Untuk pertanyaan kategori "3" hanya dapat diisi jika terkait dengan kategori "1" dan "2" sudah diisi dengan status minimal "Diterapkan sebagian". Berikut contoh pertanyaan pada area Tata Kelola Keamanan Informasi

a. Data Responden

Indeks Keamanan Informasi (Indeks KAMI)	
Identitas Instansi Pemerintah	*Kanwil DJPBN Prop. Jawa Timur* *Direktorat Jenderal Perbendaharaan* *Kementerian Keuangan RI*
Alamat	*Jl. Indrapura No.5 Surabaya* *Gedung Keuangan Negara I* *Surabaya 60175*
Nomor Telpon	*031-3539902*
Email	*heru.susanto74@depkeu.go.id*
Pengisi Lembar Evalluasi	*Heru Susanto*
NIP	*19740410 1994021 001*
Jabatan	*Pelaksana*

Gambar 4.6 Data Responden



Gambar 4.7 Hasil *Self Assestment* Indeks KAMI

Tata Kelola Keamanan Informasi

Bagian II: Tata Kelola Keamanan Informasi					
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan info					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Fungsi/Instansi Keamanan Informasi**		
2.1	II	1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	alam Penerapan / Diterapkan Sebagia	2
2.2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	alam Penerapan / Diterapkan Sebagia	2
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	alam Penerapan / Diterapkan Sebagia	2
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	alam Penerapan / Diterapkan Sebagia	2
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	alam Penerapan / Diterapkan Sebagia	2
2.6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	alam Penerapan / Diterapkan Sebagia	2
2.7	II	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	alam Penerapan / Diterapkan Sebagia	2
2.8	II	1	Apakah organsiasi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	alam Penerapan / Diterapkan Sebagia	2
2.9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	alam Penerapan / Diterapkan Sebagia	4
2.10	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal maupun eksternal untuk mengidentifikasikan persyaratan/kebutuhan pengamanan dan menyelesaikan permasalahan yang ada?	alam Penerapan / Diterapkan Sebagia	4

Gambar 4.8 Tata Kelola Informasi

Risiko

Bagian III: Pengelolaan Risiko Keamanan Informasi					
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Kajian Risiko Keamanan Informasi**		
3.1	II	1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	alam Penerapan / Diterapkan Sebagia	2
3.2	II	1	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	alam Penerapan / Diterapkan Sebagia	2
3.3	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?	alam Penerapan / Diterapkan Sebagia	2
3.4	II	1	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	alam Penerapan / Diterapkan Sebagia	2
3.5	II	1	Apakah Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	alam Penerapan / Diterapkan Sebagia	2
3.6	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	alam Penerapan / Diterapkan Sebagia	2
3.7	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	alam Penerapan / Diterapkan Sebagia	2
3.8	II	1	Apakah Instansi anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	alam Penerapan / Diterapkan Sebagia	2
3.9	II	1	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	alam Penerapan / Diterapkan Sebagia	2
3.10	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas biaya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	alam Penerapan / Diterapkan Sebagia	4

Gambar 4.9 Pengelolaan Risiko

Kerangka Kerja

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapanny					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#	**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**				
4.1	II	1	Apakah kebijakan dan prosedur keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	alam Penerapan / Diterapkan Sebagia	2
4.2	II	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	alam Penerapan / Diterapkan Sebagia	2
4.3	II	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	alam Penerapan / Diterapkan Sebagia	2
4.4	II	1	Apakah tersedia mekanisme untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	alam Penerapan / Diterapkan Sebagia	2
4.5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi?	alam Penerapan / Diterapkan Sebagia	2
4.6	II	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset tercantum dalam kontrak dengan pihak ketiga?	alam Penerapan / Diterapkan Sebagia	2
4.7	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	alam Penerapan / Diterapkan Sebagia	4
4.8	II	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi?	alam Penerapan / Diterapkan Sebagia	4
4.9	III	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch,* alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	alam Penerapan / Diterapkan Sebagia	4
4.10	III	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	alam Penerapan / Diterapkan Sebagia	4

Gambar 4.10 Kerangka Kerja

Pengelolaan Aset Informasi

Bagian V: Pengelolaan Aset Informasi					
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Pengelolaan Aset Informasi**		
3.1	II	1	Apakah tersedia daftar inventaris aset informasi yang lengkap dan akurat?	alam Penerapan / Diterapkan Sebagia	2
3.2	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?	alam Penerapan / Diterapkan Sebagia	2
3.3	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dan matrix yang merekam alokasi akses ters	alam Penerapan / Diterapkan Sebagia	2
3.4	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	alam Penerapan / Diterapkan Sebagia	2
3.5	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	alam Penerapan / Diterapkan Sebagia	2
3.6	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	alam Penerapan / Diterapkan Sebagia	2
			Apakah Instansi anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?		
3.7	II	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda	alam Penerapan / Diterapkan Sebagia	2
3.8	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	alam Penerapan / Diterapkan Sebagia	2
3.9	II	1	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI	alam Penerapan / Diterapkan Sebagia	2
3.10	II	1	Peraturan pengamanan data pribadi	alam Penerapan / Diterapkan Sebagia	2
3.11	II	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	alam Penerapan / Diterapkan Sebagia	2
3.12	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	alam Penerapan / Diterapkan Sebagia	2
3.13	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	alam Penerapan / Diterapkan Sebagia	2
3.14	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	alam Penerapan / Diterapkan Sebagia	2

Gambar 4.11 Pengelolaan Aset Informasi

Teknologi

Bagian VI: Teknologi dan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Pengamanan Teknologi**		
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	alam Penerapan / Diterapkan Sebagia	2
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?	Diterapkan Secara Menyeluruh	3
6.3	II	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset komputer dan perangkat jaringan, yang dimutakhirkan sesuai perkembangan dan kebutuhan?	Diterapkan Secara Menyeluruh	3
6.4	II	1	Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Diterapkan Secara Menyeluruh	3
6.5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Diterapkan Secara Menyeluruh	3
6.6	II	1	Apakah keseluruhan infrastruktur dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Diterapkan Secara Menyeluruh	3
6.7	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh	3
6.8	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh	3
6.9	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Diterapkan Secara Menyeluruh	3
6.10	II	1	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Diterapkan Secara Menyeluruh	3
6.11	III	2	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	Diterapkan Secara Menyeluruh	6
6.12	III	2	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Diterapkan Secara Menyeluruh	6
6.13	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	Diterapkan Secara Menyeluruh	6

Gambar 4.12 Teknologi dan Keamanan Informasi

Untuk memproses data ke tahap selanjutnya yaitu penilaian aspek kepatuhan, dilakukan pembandingan skor indeks KAMI Kanwil DJPBN Jawa Timur dengan semua bukti nyata berdasarkan kondisi keamanan informasi yang ditangani Kanwil DJPBN Jawa Timur saat ini. Berikut data pendukung aspek kepatuhan yang dilakukan pada tugas akhir ini antara lain :

- Hasil observasi langsung
- Dokumentasi seperti foto dan video
- Daftar perundang-undangan dan dokumen tertulis lainnya terkait pengelolaan keamanan informasi.

4.5 Penilaian Aspek Kepatuhan

Tahap ini merupakan tahap penilaian aspek kepatuhan untuk memastikan skor pada uji kesiapan indeks KAMI dan implementasi sesungguhnya sesuai dengan bukti yang ada.

Penilaian Aspek Kepatuhan dilakukan terinci dengan menganalisis isian item pertanyaan, item temuan, bukti kesesuaian serta catatan (jika ada). Penghitungan komparasi sederhana antara *self assestment* dan *objective assetment* penilaian aspek kepatuhan dapat terlihat sebagai berikut :

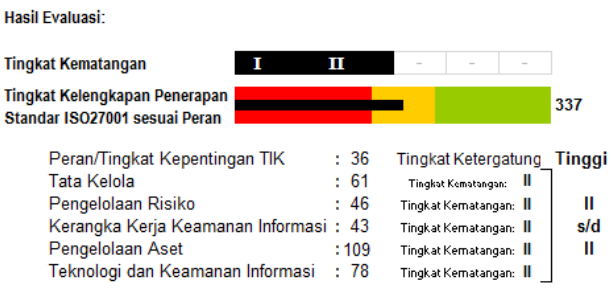
Tabel 4.1 Perbandingan Aspek Kepatuhan

Area	***Self Assestment***	***Objective Assestment***
Peran TIK	40	36
Nilai 5 Area	423	337

Berikut ini perbandingan porsentase nilai kepatuhan :

Tabel 4.2 Porsentase Perbandingan Kepatuhan

Perhitungan	Self Assestment	Objective Assestment
Nilai	$\frac{423\ x\ 100\%}{588}$= 72%	$\frac{337\ x\ 100\%}{588}$ =57.31%



Gambar 4.13 Nilai Indeks KAMI setelah Penilaian Kepatuhan

- Perhitungan didapat dengan membandingkan antara nilai sekarang dengan nilai maksimal status kesiapan dengan peran TIK tertinggi yaitu 588.
- Perbandingan ini menjelaskan kepatuhan perangkat pengamanan informasi yang terdapat di Kanwil DJPBN Jawa Timur sesuai dengan checklist Indeks KAMI.
- Nilai perbandingan kondisi *self assestment* cenderung lebih tinggi karena belum dilakukan penilaian aspek kepatuhan terhadap semua bukti pendukung evaluasi keamanan informasi. Sedangkan untuk kondisi setelahnya sudah dilakukan penilaian aspek kepatuhan untuk mengetahui apakah isian responden sesuai dengan ketersediaan bukti atau tidak.
- Hasil perbandingan tersebut menjelaskan mengenai kondisi ketersediaan perangkat keamanan informasi baik secara SDM, dokumentasi, hingga tindakan teknikal yang yang sudah dilakukan namun perlu diperbaiki dalam hal kelengkapan serta ketersediaan.

Halaman ini sengaja dikosongkan

BAB V
ANALISIS HASIL DAN PEMBAHASAN

5.1 Analisis Skor Per Bagian

Nilai analisis skor yang menajdi dasar dalam pembahasan pada bab ini adalah penilaian berdasarkan aspek penilaian obyektif (*objective assestment*).

5.1.1 Bagian Peran TIK

Sebelum proses penilaian terhadap 5 (lima) area dilakukan secara kuantitatif, proses klasifikasi dilakukan terlebih dahulu terhadap peran TIK dalam instansi atau cakupan evaluasinya. Responden juga diminta untuk mendeskripsikan infrastruktur TIK yang ada dalam satuan kerjanya secara singkat. Tujuan dari proses ini adalah untuk mengelompokkan instansi ke "ukuran" tertentu: Rendah, Sedang, Tinggi dan Kritis. Dengan pengelompokan ini nantinya bisa dilakukan pemetaan terhadap instansi yang mempunyai karakteristik kepentingan TIK yang spesifik.

Berikut ini menjelaskan skor yang didapatkan mengenai peran TIK dalam hal tingkat ketergantungan dan tingkat ketersediaan TIK bagi layanan Kantor Wilayah Direktorat Jenderal Perbendaharaan Jawa Timur.

Tabel 5.1 Penilaian Peran TIK

No	Karakteristik pertanyaan	Bobot	Skor
1.1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis	Minim	0
1.2	Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis	Rendah	1
1.3	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas Pokok dan Fungsi Instansi anda	Tinggi	3
1.4	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Tinggi	3
1.5	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda	Kritis	4

No	Karakteristik pertanyaan	Bobot	Skor
1.6	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda	Kritis	4
1.7	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi pemerintah lainnya atau terhadap ketersediaan sistem pemerintah berskala nasional	Tinggi	3
1.8	Tingkat sensitifitas pengguna sistem TIK di Instansi anda	Tinggi	3
1.9	Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya	Kritis	4
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda	Kritis	4
1.11	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK	Tinggi	3
1.12	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	Kritis	4
	Skor Peran dan Tingkat Kepentingan TIK di Instansi	**36**	Tinggi

Tabel 5.2 Total Anggaran Tahunan TIK

Kode	Detil	Volume	Satuan	Harga	Jumlah
523121	**Belanja Biaya Pemeliharaan Peralatan dan Mesin**				
	Personal Komputer / Laptop	149	UNIT	Rp 630,000	Rp 93,870,000
	UPS	15	UNIT	Rp 120,000	Rp 1,800,000
	Printer	66	UNIT	Rp 600,000	Rp 39,600,000
	Mesin Fotokopi	1	UNIT	Rp 1,000,000	Rp 1,000,000
	Faksimili	10	UNIT	Rp 800,000	Rp 8,000,000
					Rp 144,270,000
521119	**Belanja Barang Operasional Lainnya**				
	Pengelolaan Website	1	TH	Rp 2,000,000	Rp 2,000,000
	Sewa Internet	1	TH	Rp 12,000,000	Rp 12,000,000
					Rp 14,000,000
532111	**Belanja Modal Peralatan dan Mesin**				
	Scanner	2	UNIT	Rp 20,000,000	Rp 40,000,000
	Camera Digital	1	UNIT	Rp 15,000,000	Rp 15,000,000
	Infocus / LCD Proyektor	4	UNIT	Rp 9,000,000	Rp 36,000,000
	Pengadaan CCTV	10	UNIT	Rp 5,000,000	Rp 50,000,000
					Rp 141,000,000
					Rp 299,270,000

Dari hasil di atas terlihat nilai alokasi anggaran tahunan terkait dengan teknologi informasi dibawah 1 Milyar (Angka RKA-KL menunjukkan dua ratus sembilan puluh sembilan juta dua ratus tujuh puluh ribu rupiah) dan pengguna yang dalam hal ini dimaksudkan adalah karyawan Kanwil DJPBN juga menunjukkan angka yang rendah berkisar pada 115 Pegawai. Namun disisi bawahnya menunjukkan bahwa tingkat ketergantungan Kanwil DJPBN Jawa Timur akan kebutuhan TIK bernilai **tinggi** yang secara detail dapat dilihat di tabel bawah ini :

Tabel 5.3 Status Ketergantungan Peran TIK

Status Ketergantungan		
Terendah	**Tertinggi**	**Klasifikasi**
0	12	Rendah
13	24	Sedang
25	36	Tinggi
37	48	Kritis

Hal ini berarti menunjukkan bahwa SPAN (Sistem Perbendaharaan dan Anggaran Negara) yang telah dijelaskan sebelumnya mampu memenuhi tingkat kebutuhan TIK sebagai layanan perbendaharaan dan keuangan negara yang sangat diperhitungkan dengan alokasi sumberdaya (SDM dan pendanaan) yang lebih minim. Jika secara menyeluruh dilihat dari status ketergantungan yang bersifat **tinggi,** maka dampak kerugian jika keamanan informasi khususnya gangguan pada teknologi informasi akan dapat menghambat proses perbendaharaan maupun penganggaran baik secara data ataupun informasi.

5.1.2 Bagian Tata Kelola

Tabel 5.4 Penilaian Bagian Tata Kelola

2.1	II	1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Dalam Penerapan / Diterapkan Sebagian	2
2.2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Dalam Penerapan / Diterapkan Sebagian	2
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	2

2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	2
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Dalam Penerapan / Diterapkan Sebagian	2
2.6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	2

2.7	II	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Dalam Penerapan / Diterapkan Sebagian	2
2.8	II	1	Apakah organsiasi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Dalam Penerapan / Diterapkan Sebagian	2
2.9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	4

2.10	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal maupun eksternal untuk mengidentifikasikan persyaratan/kebutuhan pengamanan dan menyelesaikan permasalahan yang ada?	Dalam Penerapan / Diterapkan Sebagian	4
2.11	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	4

2.12	III	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	Dalam Penerapan / Diterapkan Sebagian	4
2.13	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	Dalam Penerapan / Diterapkan Sebagian	4
2.14	III	2	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	Dalam Penerapan / Diterapkan Sebagian	4

2.15	IV	3	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Dalam Perencanaan	3
2.16	IV	3	Apakah Instansi anda sudah mendefinisikan paramater, metrik dan mekanisme pengukuran kinerja pengelolaan keamanan informasi?	Dalam Perencanaan	3
2.17	IV	3	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Dalam Perencanaan	3
2.18	IV	3	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan dan	Dalam Perencanaan	3

			mengevaluasi pencapaiannya secara rutin, termasuk pelaporannya kepada pimpinan Instansi?		
2.19	IV	3	Apakah Instansi anda sudah mengidentifikasi legislasi dan perangkat hukum lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisis tingkat kepatuhannya?	Dalam Perencanaan	3
2.20	IV	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Dalam Penerapan / Diterapkan Sebagian	6
			Total Nilai Evaluasi Tata Kelola	**61**	**II**

Berikut ini adalah penjelasan tabel kategorisasi kontrol beserta nilainya.

Pada tabel di bawah ini dijelaskan bahwa kategori kontrol dengan pertanyaan 1 yang berjumlah 8 bernilai 16. Sedangkan untuk pertanyaan tahap 2 dengan jumlah 6 bernilai 24. Dari hasil yang didapat maka jumlah pertanyaan untuk Tahap Penerapan 1 dan 2 berjumlah 40. Untuk mengetahui status kelengkapan pada bagian ini adalah dengan membandingkan jumlah tahap penerapan 1 dan 2 dengan skor minimal Tahap Penerapan 3 yang sudah ditentukan pada aplikasi indeks KAMI untuk bagian Tata Kelola yaitu 40. Didapat bahwa jumlah skor pada tahap penerapan 1 dan 2 adalah 40 sehingga dapat disimpulkan skor sudah melebihi Tahapan Penerapan 3. Untuk bagian Tata Kelola disimpulkan sudah mencapati Tingkat Kematangan II.

Berikut tingkat kelengkapan beserta nilainya seperti tabel di bawah ini :

Tabel 5.5 Tingkat Kelengkapan Tata Kelola

	Tata Kelola Keamanan	Nilai
Kategori Kontrol (Tahap)		
1	8	16
2	6	24
3	6	21
Total Pertanyaan	**20**	**61**

Nilai tingkat kelengkapan pada masing-masing kategori pengamanan terkait dengan tata kelola keamanan akan menentukan tingkat kematangan pada bagian ini. Semakin tinggi nilai tingkat kelengkapan maka semakin tinggi pula tingkat kematangan keseluruhan pada tiap bagian. Berikut hasil tingkat kematangan pada bagian Tata Kelola

Tabel 5.6 Tingkat Kematangan Tata Kelola

	Pertanyaan Tata Kelola	Nilai	
Kategori Tingkat Kematangan			**Tingkat validitas kematangan**
II	11	28	Y
III	3	12	N
IV	6	21	N
Total Pertanyaan	**20**	**61**	

Catatan :

- Pada Tingkat Kematangan II, status sudah menunjukkan valid karena sudah melebihi tingkat pencapaian yaitu dengan skor 28. Untuk memperoleh tingkat valid kematangan > II, jumlah skor pertanyaan Kategori Kematangan II harus mencapai 80% (33,6) begitu pula untuk Tingkat Kematangan diatasnya (TKIII - TKV).
- Tingkat validitas bukan menunjukkan valid atau tidaknya data namun valid atau tidaknya skor untuk menuju tahap tingkat kematangan selanjutnya.

Hasil penilaian bidang Tata Kelola Kanwil DJPBN Jawa Timur secara umum menunjukkan bahwa skor untuk bagian ini 61 dengan tingkat kematangan pada Level II. Pada tingkat kematangan tersebut dapat dianalisis bahwa :

- Pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.
- Proses pengamanan berjalan tanpa dokumentasi atau rekaman resmi.
- Langkah pengamanan operasional yang diterapkan bergantung kepada pengetahuan dan motivasi individu pelaksana.

- Bentuk pengamanan secara keseluruhan belum dinilai .efektifitasnya.
- Kelemahan dalam manajemen pengamanan masih banyak ditemukan dan tidak dapat diselesaikan dengan tuntas oleh pelaksana maupun pimpinan sehingga menyebabkan dampak yang sangat signifikan.
- Manajemen pengamanan belum mendapatkan prioritas dan tidak berjalan secara konsisten.
- Pihak yang terlibat kemungkinan besar masih belum memahami tanggung jawab mereka.

5.1.3 Bagian Risiko

Tabel 5.7 Penilaian Bagian Risiko

3.1	II	1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Dalam Penerapan / Diterapkan Sebagian	2
3.2	II	1	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Dalam Penerapan / Diterapkan Sebagian	2

3.3	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?	Dalam Penerapan / Diterapkan Sebagian	2
3.4	II	1	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Dalam Penerapan/ Diterapkan Sebagian	2
3.5	II	1	Apakah Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	Dalam Penerapan / Diterapkan Sebagian	2
3.6	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Dalam Penerapan / Diterapkan Sebagian	2

3.7	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Dalam Penerapan / Diterpakan Sebagian	2
3.8	II	1	Apakah Instansi anda sudah menjalankan inisiatif analisis/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	Dalam Penerapan / Diterapkan Sebagian	2
3.9	II	1	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Dalam Penerapan / Diterapkan Sebagian	2

3.10	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas biaya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	Dalam Penerapan / Diterapkan Sebagian	4
3.11	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Dalam Penerapan / Diterapkan Sebagian	4
3.12	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi untuk memastikan konsistensi dan efektifitasnya?	Dalam Penerapan / Diterapkan Sebagian	4

3.13	IV	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	Dalam Penerapan / Diterapkan Sebagian	4
3.14	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan / meningkatkan efektifitasnya?	Dalam Penerapan / Diterapkan Sebagian	6
3.15	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Dalam Penerapan / Diterapkan Sebagian	6
			Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi	**46**	**II**

Pada tabel di bawah ini dijelaskan bahwa kategori kontrol dengan pertanyaan Tahap Penerapan 1 yang berjumlah 9 bernilai 18. Sedangkan untuk pertanyaan Tahap Penerapan 2 dengan jumlah 4 bernilai 16. Dan dua pertanyaan Tahap Penerapan 3 bernilai 12. Dari hasil yang didapat maka jumlah pertanyaan untuk Tahap Penerapan 1 dan 2 berjumlah 34. Cara mengetahui status

kelengkapan pada bagian ini adalah dengan membandingkan jumlah Tahap Penerapan 1 dan 2 dengan skor minimal Tahap Penerapan 3 yang sudah ditentukan pada aplikasi indeks KAMI yaitu 34. Didapat bahwa jumlah skor Tahap penerapan 1 dan 2 adalah 34 sehingga dapat disimpulkan skor sama dengan skor minimal Tahapan Penerapan 3.

Berikut akan dijelaskan tingkat kelengkapan beserta nilainya seperti tabel berikut :

Tabel 5.8 Tingkat Kelengkapan Pengelolaan Risiko

	Pengelolaan Risiko	Nilai
Kategori Kontrol (Tahap)		
1	9	18
2	4	16
3	2	12
Total Pertanyaan	**15**	**46**

Sedangkan untuk tingkat kematangan dapat dijelaskan pada tabel di bawah ini

Tabel 5.9 Tingkat Kematangan Pengelolaan Risiko

	Pengelolaan Risiko	Nilai	
Kategori Tingkat Kematangan			**Tingkat validitas kematangan**
II	9	18	Y
III	2	8	N
IV	2	8	N
V	2	12	N
Total Pertanyaan	**15**	**46**	

Catatan :

- Untuk memperoleh tingkat kematangan II, jumlah skor pertanyaan Kategori Kematangan II harus mencapai skor pencapaian pada tingkat ini yaitu 18. Sedangkann untuk memperoleh tingkat valid kematangan > II, jumlah skor pertanyaan Kategori Kematangan II harus mencapai valid yaitu 80% (nilai 21.6) begitu pula Tingkat Kematangan diatasnya (TKIII - TKV). Jadi hasil di atas secara otomatis menunjukkan bahwa status Tingkat Kematangan lanjut untuk TKIII, TKIV, dan TKIV sudah tidak valid karena hasil skor yang kurang memenuhi tingkat pencapaian.
- Tingkat validitas bukan menunjukkan valid atau tidaknya data namun valid atau tidaknya skor untuk menuju tahap tingkat kematangan selanjutnya.

Hasil penilaian bidang pengelolaan risiko keamanan informasi Kanwil DJPBN Jawa Timur secara umum menunjukkan bahwa skor untuk bagian ini 46 dengan tingkat kematangan pada Level II. Pada tingkat kematangan tersebut dapat dianalisis bahwa :

- Pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.
- Proses pengamanan berjalan tanpa dokumentasi atau rekaman resmi.
- Langkah pengamanan operasional yang diterapkan bergantung kepada pengetahuan dan motivasi individu pelaksana.
- Bentuk pengamanan secara keseluruhan belum dinilai .efektifitasnya.
- Manajemen pengamanan belum mendapatkan prioritas dan tidak berjalan secara konsisten

5.1.4 Bagian Kerangka Kerja

Tabel 5.10 Penilaian Bagian Kerangka Kerja

4.1	II	1	Apakah kebijakan dan prosedur keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	Dalam Penerapan / Diterapkan Sebagian	2
4.2	II	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	Dalam Penerapan / Diterapkan Sebagian	2
4.3	II	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	Dalam Penerapan / Diterapkan Sebagian	2

4.4	II	1	Apakah tersedia mekanisme untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	2
4.5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	2
4.6	II	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset tercantum dalam kontrak dengan pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	2
4.7	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	Dalam Penerapan / Diterapkan Sebagian	4

4.8	II	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	4
4.9	III	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasitanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	Dalam Perencanaan	2
4. 10	III	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Dalam Perencanaan	2

4. 11	III	2	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?	Dalam Perencanaan	2
4. 12	III	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?	Dalam Penerapan / Diterapkan Sebagian	4

4.13	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Dalam Penerapan / Diterapkan Sebagian	0
4.14	III	3	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	Dalam Perencanaan	0
4.15	IV	3	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	Dalam Perencanaan	0

4.16	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Dalam Penerapan / Diterapkan Sebagian	0
Pengelolaan Strategi dan Program Keamanan Informasi					
4.17	II	1	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisis risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	Dalam Penerapan / Diterapkan Sebagian	2
4.18	II	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	Dalam Penerapan / Diterapkan Sebagian	2
4.19	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program	Dalam Penerapan / Diterapkan Sebagian	2

			kerja organisasi anda?		
4.20	III	1	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	Dalam Penerapan / Diterapkan Sebagian	2
4.21	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?	Dalam Perencanaan	1
4.22	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Dalam Perencanaan	2

4.23	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Dalam Perencanaan	2
4.24	IV	3	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisis untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Dalam Perencanaan	0
4.25	V	3	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada untuk memastikan bahwa keseluruhan inisiatif tersebut telah	Dalam Perencanaan	0

			diterapkan secara efektif?		
4.26	V	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Dalam Perencanaan	0
			Total Nilai Evaluasi Kerangka Kerja	**43**	**II**

Terdapat 2 (dua) aspek besar pada bagian evaluasi kerangka kerja ini yakni Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi dan Pengelolaan Strategi dan Program Keamanan Informasi

Berikut ini adalah penjelasan tabel kategorisasi kontrol untuk hasil evaluasi kerangka kerja beserta nilainya. Pada tabel di bawah ini dijelaskan bahwa kategori kontrol dengan pertanyaan 1 yang berjumlah 11 bernilai 21. Sedangkan untuk pertanyaan tahap 2 dengan jumlah 8 bernilai 22. Dari hasil yang didapat maka jumlah pertanyaan untuk Tahap Penerapan 1 dan 2 berjumlah 43. Untuk mengetahui status kelengkapan pada bagian ini adalah dengan membandingkan jumlah tahap penerapan 1 dan 2 dengan skor minimal Tahap Penerapan 3 yang sudah ditentukan pada aplikasi indeks KAMI untuk bagian Kerangka Kerja yaitu 54. Didapat bahwa jumlah skor Tahap penerapan 1 dan 2 adalah 43 sehingga dapat disimpulkan skor tidak mencukupi Tahapan Penerapan 3. Untuk Tingkat Kematangan, skor pencapaian Tingkat kematangan II telah terpenuhi. Untuk bagian Kerangka

Kerja disimpulkan telah mencapai Tingkat Kematangan II namun tidak mencapat Tingkat Kematangan III, karenanya memenuhi skor untuk kategori Tingkat Kematangan II. Berikut tingkat kelengkapan beserta nilainya seperti tabel di bawah ini :

Tabel 5.11 Tingkat Kelengkapan Kerangka Kerja

	Pengelolaan Kerangka Kerja	Nilai
Kategori Kontrol (Tahap)		
1	11	21
2	8	22
3	7	0
Total Pertanyaan	**26**	**43**

Nilai tingkat kelengkapan pada masing-masing kategori pengamanan akan menentukan tingkat kematangan pada bagian ini. Berikut ini hasil tingkat kematangan pada bagian Kerangka Kerja

Tabel 5.12 Tingkat Kematangan Kerangka Kerja

	Pengelolaan Kerangka Kerja	Nilai	
Kategori Tingkat Kematangan			**Tingkat validitas kematangan**
II	10	24	Y
III	11	19	N
IV	3	0	N
V	2	0	N
Total Pertanyaan	**26**	**43**	

Catatan :

- Skor Tingkat Kematangan II (TKII) bagian ini adalah 24 sehingga status telah menunjukkan valid karena skor

pertanyaan pada TKII telah melebihi atau sama dengan nilai pada batas skor minimum tingkat pencapaian TKII yaitu dengan skor 24. Namun belum memenuhi skor minimum TKIII dimana 11 pertanyaan di TK III harus bernilai 53 sehingga disimpulkan bahwa bagian Kerangka Kerja baru mempunyai TK II secara keseluruhan.

- Untuk memperoleh validitas TK > II, maka jumlah skor pertanyaan Kategori TK II harus mencapai 80% (28.8) begitu pula Kematangan diatasnya (TKIII - TKV).
- Tingkat validitas bukan menunjukkan valid atau tidaknya data namun valid atau tidaknya skor untuk menuju tahap tingkat kematangan selanjutnya.

Hasil penilaian bidang kerangka kerja pengelolaan keamanan informasi secara umum menunjukkan bahwa skor untuk bagian ini 43 dengan tingkat kematangan pada Level II. Pada tingkat kematangan tersebut dapat didefinisikan bahwa :

- Pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.
- Bentuk pengamanan secara keseluruhan belum dapat dibuktikan efektivitasnya
- Langkah pengamanan operasional yang diterapkan bergantung kepada pengetahuan dan motivasi individu pelaksana.
- Kelemahan dalam manajemen pengamanan masih banyak ditemukan dan tidak dapat diselesaikan dengan tuntas oleh pelaksana maupun pimpinan sehingga menyebabkan dampak yang sangat signifikan.
- Manajemen pengamanan belum mendapatkan prioritas dan tidak berjalan secara konsisten.

5.1.5 Bagian Pengelolaan Aset

5.1	II	1	Apakah tersedia daftar inventaris aset informasi yang lengkap dan akurat?	Dalam Penerapan/ Diterapkan Sebagian	2
5.2	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?	Dalam Penerapan/ Diterapkan Sebagian	2
5.3	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dan matrix yang merekam alokasi akses tersebut	Dalam Penerapan/ Diterapkan Sebagian	2
5.4	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	Dalam Penerapan/ Diterapkan Sebagian	2
5.5	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Dalam Penerapan/ Diterapkan Sebagian	2
5.6	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Dalam Penerapan/ Diterapkan Sebagian	2
			Apakah Instansi anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?		

5.7	II	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda	Dalam Penerapan/ Diterapkan Sebagian	2
5.8	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	Dalam Penerapan/ Diterapkan Sebagian	2
5.9	II	1	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI	Dalam Penerapan/ Diterapkan Sebagian	2
5. 10	II	1	Peraturan pengamanan data pribadi	Dalam Penerapan/ Diterapkan Sebagian	2
5. 11	II	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	Dalam Penerapan/ Diterapkan Sebagian	2
5. 12	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Dalam Penerapan/ Diterapkan Sebagian	2
5. 13	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Dalam Penerapan/ Diterapkan Sebagian	2
5. 14	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Dalam Penerapan/ Diterapkan Sebagian	2
5. 15	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden	Dalam Penerapan/	2

			terkait kegagalan keamanan informasi	Diterapkan Sebagian	
5.16	II	1	Prosedur *back-up* ujicoba pengembalian data (*restore*)	Dalam Penerapan/ Diterapkan Sebagian	2
5.17	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Dalam Penerapan/ Diterapkan Sebagian	4
5.18	III	2	Proses pengecekan latar belakang SDM	Dalam Penerapan/ Diterapkan Sebagian	4
5.19	III	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Dalam Penerapan/ Diterapkan Sebagian	4
5.20	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Dalam Penerapan/ Diterapkan Sebagian	4
5.21	III	2	Prosedur kajian penggunaan akses (*user access review*) dan langkah pembenahan apabila terjadi ketidak sesuaian (*non-conformity*) terhadap kebijakan yang berlaku.	Dalam Penerapan/ Diterapkan Sebagian	4
5.22	III	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisis kepatuhan terhadap prosedur *backup*-nya?	Dalam Perencanaan	3
5.23	III	3	Apakah tersedia daftar rekaman pelaksanaan	Dalam Penerapan/	6

			keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Diterapkan Sebagian	
5.24	III	3	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?	Dalam Penerapan/ Diterapkan Sebagaian	6
#			**Pengamanan Fisik**		
5.25	II	1	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?	Diterapkan Secara Menyeluruh	3
5.26	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Diterapkan Secara Menyeluruh	3
5.27	II	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	Diterapkan Secara Menyeluruh	3
5.28	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan	Diterapkan Secara Menyeluruh	3

			pasokan listrik atau dampak dari petir?		
5.29	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Dalam Penerapan/ Diterapkan Sebagian	2
5.30	II	2	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	Diterapkan Secara Menyeluruh	6
5.31	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Diterapkan Secara Menyeluruh	6
5.32	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Diterapkan Secara Menyeluruh	6
5.33	II	2	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang	Dalam Penerapan/ Diterapkan Sebagian	4

			dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)		
5.34	II	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?	Dalam Penerapan/ Diterapkan Sebagian	6
			Total Nilai Evaluasi Pengelolaan Aset	**109**	**II**

Berikut ini adalah tabel kategorisasi kontrol keranka pengelolaan asset beserta nilainya. Pada tabel di bawah ini dijelaskan bahwa kategori kontrol dengan pertanyaan 1 yang berjumlah 21 bernilai 46. Sedangkan untuk pertanyaan tahap 2 dengan jumlah 9 bernilai 42. Dari hasil yang didapat maka jumlah pertanyaan untuk Tahap Penerapan 1 dan 2 berjumlah 88. Untuk mengetahui status kelengkapan pada bagian ini adalah dengan membandingkan jumlah tahap penerapan 1 dan 2 dengan skor minimal Tahap Penerapan 3 yang sudah ditentukan pada aplikasi indeks KAMI untuk bagian Pengelolaan Aset yaitu 74,4. Sehingga dapat disimpulkan skor sudah memenuhi Tahapan Penerapan 3.

Berikut tingkat kelengkapan beserta nilainya seperti tabel di bawah ini

Tabel 5.13 Tingkat Kelengkapan Pengelolaan Aset

	Pengelolaan Aset	Nilai
Kategori Kontrol (Tahap)		
1	21	46
2	9	42
3	4	21
Total Pertanyaan	**34**	**109**

Nilai tingkat kelengkapan pada masing-masing kategori pengamanan akan menentukan tingkat kematangan pada bagian ini. Semakin tinggi nilai tingkat kelengkapan maka semakin tinggi pula tingkat kematangan keseluruhan pada tiap bagian.

Berikut hasil tingkat kematangan pada bagian Pengelolaan Aset.

Tabel 5.14 Tingkat Kematangan Pengelolaan Aset

	Pengelolaan Aset	Nilai	
Kategori Tingkat Kematangan			**Tingkat validitas kematangan**
II	26	72	Y
III	8	37	N
Total Pertanyaan	**34**	**109**	

Catatan :

- Skor Tingkat Kematangan II (TK II) bagian ini adalah 72 sehingga status sudah menunjukkan valid karena skor pertanyaan pada TKII sudah memenuhi nilai pada batas skor tingkat pencapaian TKII yaitu dengan skor 62.

- Untuk memperoleh validitas Tingkat Kematangan > II, maka jumlah skor pertanyaan Kategori Tingkat Kematangan III harus mencapai 80% (74.4), namun dengan angka 72 tidak memenuhi TK III.
- Tingkat validitas bukan menunjukkan valid atau tidaknya data namun menunjukkan valid atau tidaknya skor untuk menuju tahap tingkat kematangan selanjutnya.

Hasil penilaian bidang Pengelolaan Aset Kanwil DJPBN Jawa Timur secara umum menunjukkan bahwa skor untuk bagian ini 109 dengan tingkat kematangan pada Level II. Pada tingkat kematangan tersebut dapat didefinisikan bahwa :

- Pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.
- Proses pengamanan berjalan tanpa dokumentasi atau rekaman resmi.
- Langkah pengamanan operasional yang diterapkan bergantung kepada pengetahuan dan motivasi individu pelaksana.
- Bentuk pengamanan secara keseluruhan belum dinilai efektifitasnya.
- Kelemahan dalam manajemen pengamanan masih banyak ditemukan dan tidak dapat diselesaikan dengan tuntas oleh pelaksana maupun pimpinan sehingga menyebabkan dampak yang sangat signifikan.
- Manajemen pengamanan belum mendapatkan prioritas dan tidak berjalan secara konsisten. Pengelolaan asset belum mendapat perhatian karena ketiadaan laporan BMN secara detil
- Pihak yang terlibat kemungkinan besar masih belum memahami tanggung jawab mereka.

5.1.6 Bagian Teknologi

6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Dalam Penerapan / Diterapkan Sebagian	2
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?	Diterapkan Secara Menyeluruh	3
6.3	II	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset komputer dan perangkat jaringan, yang dimutakhirkan sesuai perkembangan dan kebutuhan?	Diterapkan Secara Menyeluruh	3
6.4	II	1	Apakah Instansi anda secara rutin menganalisis kepatuhan penerapan konfigurasi standar yang ada?	Dalam Penerapan /Diterapkan Sebagian	2
6.5	II	1	Apakah jaringan, sistem dan aplikasi	Dalam Penerapan /Diterapkan	2

			yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Sebagian	
6.6	II	1	Apakah keseluruhan infrastruktur dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Dalam Penerapan /Diterapkan Sebagian	2
6.7	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Dalam Penerapan/ Diterapkan Sebagian	2
6.8	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Dalam Penerapan/ Diterapkan Sebagian	2
6.9	II	1	Apakah semua log dianalisis secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Dalam Penerapan/ Diterapkan Sebagian	2
6. 10	II	1	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting	Dalam Perencanaan	1

			sesuai kebijakan pengelolaan yang ada?		
6.11	III	2	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	Dalam Perencanaan	2
6.12	III	2	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Dalam Perencanaan	2
6.13	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	Dalam Penerapan/ Diterapkan Sebagian	4
6.14	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Diterapkan Secara Menyeluruh	6

6.15	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*, dan penarikan akses?	Diterapkan Secara Menyeluruh	4
6.16	III	2	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Diterapkan Secara Menyeluruh	6
6.17	II	1	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	Dalam Penerapan/ Diterapkan Sebagian	2
6.18	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Dalam Penerapan / Diterapkan Sebagian	2
6.19	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Diterapkan Secara Menyeluruh	3

6.20	III	2	Apakah ada rekaman dan hasil analisis (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus telah dimutakhirkan secara rutin dan sistematis?	Dalam Penerapan / Diterapkan Sebagian	4
6.21	III	2	Apakah adanya laporan penyerangan virus yang gagal/sukses ditindaklanjuti dan diselesaikan?	Dalam Penerapan / Diterapkan Sebagian	6
6.22	III	2	Apakah keseluruhan sistem (aplikasi, perangkat komputer dan jaringan) sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Dalam Penerapan / Diterapkan Sebagian	4
6.23	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi keamanan yang diverifikasi/validasi pada saat pengembangan dan uji-coba?	Diterapkan Secara Menyeluruh	4
6.24	IV	3	Apakah Instansi anda melibatkan pihak independen untuk	Dalam Penerapan / Diterapkan Sebagian	6

			mengkaji kehandalan keamanan informasi secara rutin?		
			Total Nilai Evaluasi Teknologi dan Keamanan Informasi	**78**	**II**

Berikut ini adalah tabel kategorisasi kontrol beserta nilainya. Pada tabel di bawah ini dijelaskan bahwa kategori kontrol dengan pertanyaan Tahap Penerapan 1 yang berjumlah 13 bernilai 28. Sedangkan untuk pertanyaan Tahap Penerapan 2 dengan jumlah 10 bernilai 44. Dari hasil yang didapat maka jumlah pertanyaan untuk Tahap Penerapan 1 dan 2 berjumlah 72. Untuk mengetahui status kelengkapan pada bagian ini adalah dengan membandingkan jumlah Tahap Penerapan 1 dan 2 dengan skor minimal Tahap Penerapan 3 yang sudah ditentukan pada aplikasi indeks KAMI untuk area Teknologi yaitu 66. Didapat bahwa jumlah skor Tahap penerapan 1 dan 2 adalah 72 sehingga dapat disimpulkan skor telah melebihi Tahapan Penerapan 3 dan dinilai tahapan ini telah valid. Berikut tingkat kelengkapan pada tiap pertanyaan Tahap Penerapan beserta nilainya seperti tabel di bawah ini

Tabel 5.15 Tingkat Kelengkapan Teknologi

	Pengelolaan Teknologi	**Nilai**
Kategori Kontrol (Tahap)		
1	13	28
2	10	44
3	1	6
Total Pertanyaan	**24**	**78**

Nilai tingkat kelengkapan pada masing-masing kategori pertanyaan Tahap penerapan akan menentukan tingkat kematangan pada bagian ini. Berikut hasil tingkat kematangan pada area Teknologi

Tabel 5.16 Tingkat KematanganTeknologi

	Pengelolaan Teknologi	Nilai	
Kategori Tingkat Kematangan			**Tingkat validitas kematangan**
II	13	28	Y
III	10	44	N
IV	1	6	N
Total Pertanyaan	**24**	**78**	

Catatan :

- Skor Tingkat Kematangan II (TKII) bagian ini adalah 28 sehingga status telah menunjukkan valid karena skor pertanyaan pada TK II telah melebihi atau sama dengan nilai pada batas skor tingkat pencapaian TK II yaitu dengan skor 26. Dengan melampaui skor valid minimum TK II yaitu 17 sehingga disimpulkan bahwa area Teknologi mempunyai TK II untuk secara keseluruhan.
- Untuk memperoleh validitas TK > II, maka jumlah skor pertanyaan Kategori TK II harus mencapai 80% (31.2) begitu pula untuk Tingkat Kematangan (TK III - TK V). Kondisi saat ini, skor untuk pertanyaan TK II area ini adalah 28 yang berada dibawah skor valid tingkat pencapaian TK >II yaitu 31,2.
- Untuk validitas TK IV, maka jumlah skor pertanyaan Kategori TK III harus mencapai 80% (58). Dan skor menunjukkan Kanwil DJPBN berakhir pada TK II.

- Tingkat validitas bukan menunjukkan valid atau tidaknya data namun menunjukkan valid atau tidaknya skor untuk menuju tahap tingkat kematangan selanjutnya.

Hasil penilaian Kanwil Direktorat Jenderal Perbendaharaan Jawa Timur secara umum menunjukkan bahwa skor untuk bagian ini 78 dengan tingkat kematangan pada Level II. Pada tingkat kematangan tersebut dapat didefinisikan bahwa

- Pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.
- Proses pengamanan berjalan tanpa dokumentasi atau rekaman resmi.
- Langkah pengamanan operasional yang diterapkan bergantung kepada pengetahuan dan motivasi individu pelaksana.
- Bentuk pengamanan secara keseluruhan belum dinilai efektifitasnya.
- Kelemahan dalam manajemen pengamanan masih banyak ditemukan dan tidak dapat diselesaikan dengan tuntas oleh pelaksana maupun pimpinan sehingga menyebabkan dampak yang sangat signifikan.

5.2 Analisis Skor Akhir Indeks KAMI

Pada bagian ini akan dibahas mengenai hasil skor akhir secara keseluruhan lima area keamanan informasi pada layanaan Direktorat Jenderal Perbendahraan yang dikelola oleh Kantor Wilayah Direktorat Jenderal Perbendaharaan Jawa Timur. Berikut hasil Tingkat Kematangan untuk seluruh area berdasarkan tingkat validitas skor.

Tabel 5.17 Status Kematangan Lima Area

Validitas	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi
Tingkat Kematangan I					
Validitas	Yes	Yes	Yes	Yes	Yes
Status	I	I	I	I	I
Tingkat Kematangan II					
Validitas	Yes	Yes	Yes	Yes	Yes
Status	II	II	II	II	II
Tingkat Kematangan III					
Validitas	No	No	No	No	No
Status	No	No	No	No	II
Tingkat Kematangan IV					
Validitas	No	No	No	No	No
Status	No	No	No	No	No
Status Akhir	II	II	II	II	II

Tabel 5.17 di atas menunjukkan status Tingkat Kematangan akhir tiap area yaitu

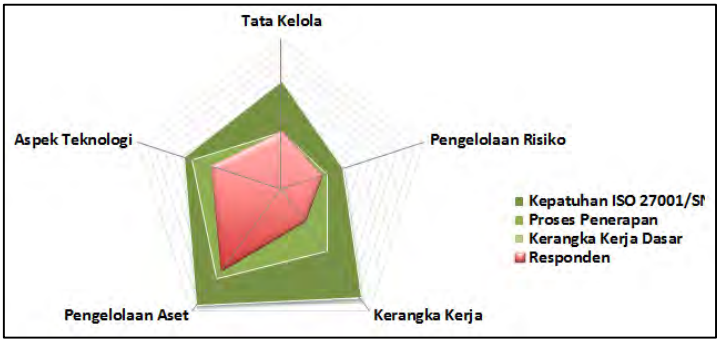
- Penilaian area Tata Kelola dalam tahap tingkat kematangan II
- Penilaian area Pengelolaan Risiko dalam tahap tingkat kematangan II
- Penilaian area Kerangka Kerja dalam tahap tingkat kematangan II
- Penilaian area Pengelolaan Aset dalam tahap tingkat kematangan II
- Penilaian area Teknologi dalam tahap tingkat kematangan II

Dari hasil di atas dapat dilihat bahwa perolehan nilai Tingkat Kematangan merata pada perolehan skor secara keseluruhan yang terdapat di semua area pengamanan informasi (TK) yaitu pada level II. Level II dalam indeks KAMI mendefinisikan kondisi aktif Kanwil DJPBN Jawa Timur di antaranya :

- Pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.
- Proses pengamanan berjalan tanpa dokumentasi atau rekaman resmi. Beberapa tindakan pengamanan telah memiliki kebijakan setingkat Peraturan Menteri Keuangan ataupun Keputusan Menteri Keuangan namun belum di*cascade* ke dalam prosedur atau panduan yang implementatif pada pelaksanaan pengamanan informasi di tingkat operasional / pelaksana.
- Bentuk pengamanan secara keseluruhan belum dapat dibuktikan efektivitasnya. Hal ini terlihat dari belum adanya laporan / *report* dari seluruh langkah pengamanan yang dilakukan. *Feedback* dari suatu langkah pengamanan yang tersaji dalam laporan merupakan tolok ukur pertama penilaian efektivitas
- Kelemahan dalam manajemen pengamanan masih banyak ditemukan dan tidak dapat diselesaikan dengan tuntas oleh pelaksana maupun pimpinan sehingga menyebabkan dampak yang sangat signifikan.
- Manajemen pengamanan belum mendapatkan prioritas dan tidak berjalan secara konsisten. Hal ini terlihat dari serangkaian kegiatan pengamanan yang pelaksanannya belum menjadi bagian dari SFO (*strategy focused organization*) dan ketiadaan dokumentasi pengelolan keamanan yang runtut dari proses identifikasi, analisis, implementasi, evaluasi dan report dari pelaksanaan pengamanan informasi

- Pihak yang terlibat kemungkinan besar masih belum memahami tanggung jawab mereka

Hasil keseluruhan terhadap lima area indeks KAMI ditampilkan pada diagram jaring laba-laba skor Indeks KAMI di bawah ini :



Gambar 5.1 Diagram Jaring Indeks KAMI

Gambar di atas menunjukkan bahwa :

- Warna merah responden menjelaskan mengenai persebaran jawaban dari lima area
- Level kepatuhan paling signifikan didapat Pengelolaan Aset karena telah melampaui atau memenuhi bagian Kerangka Kerja Dasar atau Tingkat Kematangan II menuju Tingkat Keamanan II+ (selisih valid 3 poin).
- Sedangkan area lainnya yakni Tata Kelola, Pengelolaan Risiko, Kerangka Kerja dan Teknologi dinyatakan butuh peningkatan karena jawaban responden terhadap Kerangka Kerja hanya pada Tingkat Kematangan II.
- Untuk menuju pada jaring Kepatuhan ISO 27001/SNI yang lebih baik maka Kanwil DJPBN Jawa Timur harus memperhatikan semua area baik aspek :

- Kerangka kerja dasar, contohnya adanya rencana strategi, kebijakan, prosedur, instruksi kerja mengenai keamanan informasi
- Konsistensi penerapan, contohnya formulir, *checklist monitoring*, laporan, dll
- Tindakan peningkatan kinerja keamanan, contohnya sosialisasi, tes online, evaluasi untuk efektivitas pelaksanaan pengamanan

- Hasil skor terakhir seluruh area adalah 337 dengan kondisi peran penggunaan TIK termasuk dalam kondisi **Tinggi.** Hasil skor tersebut menunjukkan status kesiapan yaitu **perlu perbaikan,** yang secara detail dapat dilihat pada tabel di bawah ini
- Dari aspek peran TIK, Kanwil DJPBN Jawa Timur menunjukkan skor sangat tinggi / kritis yaitu 36 dari 48 yang artinya kebutuhan TIK bagi instansi tergolong vital bagi layanan perbendaharaan negara. Angka peran yang tinggi secara otomatis menginginkan suatu penerapan pengelolaan keamanan informasi yang tinggi pula yang terlihat dari aspek kesiapan dan kematangan penerapan keamanan. Sedangkan status kesiapan pada skor 337 dari nilai maksimal 588 yang artinya masih perlu perbaikan untuk kelengkapan perangkat keamanan seluruh area antara lain Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, dan Teknologi.
- Tingkat kematangan keseluruhan area berada pada level II dari level V (kesiapan sertifikasi ISO/IEC 27001:2005) yang artinya sudah terdapat penerapan keamanan informasi di Kanwil DJPBN Jawa Timur secara aktif.

Tabel 5.18 Status Kesiapan Keamanan Keseluruhan

Skor	Range		Status
25-36	0	272	Tidak Layak
	273	392	Perlu Perbaikan
	393	588	Baik/Cukup

Langkah-langkah untuk perbaikan pengelolaan keamanan informasi Kanwil DJPBN Jawa Timur diantaranya :

- Melaksanakan dan menerapkan semua kebijakan dan prosedur keamanan informasi pada semua area pengamanan.
- Memonitoring segala aktivitas teknologi informasi meliputi kinerja pegawai, kinerja hardware, kinerja software, dan pengimplemenatasian sistem penerapan regulasi (sanksi/ hukuman) yang terkait pengelolaan keamanan informasi.
- Mengevaluasi setiap penerapan kebijakan dan prosedur terkait keamanan informasi untuk menilai efektifitas dan efisiensi kinerja terhadap segala aktivitas teknologi informasi
- Untuk memaksimalkan pencapaian tingkat kematangan keamanan informasi, maka sebaiknya Kanwil DJPBN mendefinisikan perangkat keamanan informasi misal SDM, rencana strategi, kebijakan, prosedur hingga instruksi kerja untuk semua bagian disertai dengan pengamanannya.

  Penggunaan Indeks KAMI sendiri memiliki sejumlah aspek yang harus disempurnakan terkat dengan penilaian kesiapan, ambang batas 80 % dan penyajian pada dashboard di tiap area termasuk pendefinisian tingkat pengendalian yang diharapkan (*desired level of control*). Dan kedepannya diharapkan penyempurnaan tersebut terlaksana demi mencapai standarisasi pengelolaan keamanan informasi berdasarkan ISO/IEC 27001:2005.

5.3 Corrective Preventive Action Report (CPAR)

Corrective Action / tindakan pencegahan adalah tindakan menghilangkan penyebab masalah (ketidaksesuaian) yang ditemukan atau situasi yang tidak dikehendaki untuk mencegahnya terulang kembali (*prevent recurrence*)

Preventive Action / tindakan pencegahan adalah tindakan untuk menghilangkan penyebab potensi masalah (ketidaksesuaian) agar tidak terjadi (*prevent occurrence*)

Mengadaptasi konteks tata naskah dinas berdasarkan PMK.151/PMK.01/2010 tentang Pedoman Tata Naskah Dinas Kementerian Keuangan, maka bentuk paling tepat dalam penyajian *Corrective Preventive Action Report* (CPAR) adalah disposisi yang memiliki unsur-unsur lokasi, obyek dan tindak lanjut pelaksanaan atau penyelesaian.

Berdasarkan Sarno (2009), CPAR Form adalah form yang digunakan untuk mendokumentasikan sejumlah aspek terkait dengan ketidaksesuaian sistem atau usulan penyempurnaan sistem. Semua analisis ini didapatkan dari tindakan pembuktian ketidaksamaan operasional dengan dokumen yang ditemukan saat observasi. Pengisian CPAR seharusnya ringkas, jelas dan padat serta tidak memungkinkan penafsiran ganda. Pengisian dilakukan dengan mengacu pada kaidah PLOR (*problem, location, object and reference*).

- *Problem* : Apa permasalahannya / ketidaksesuaiannya
- *Location* : Dimana lokasi terjadinya
- *Objective* : Bukti ketidaksesuaian
- *Reference* : Referensi yang dipakai untuk menetepakan suatu hal dinyatakan tidak sesuai

Pada bagian CPAR ini akan dibahas mengenai penyebab masalah dan usulan tindakan untuk semua bagian. Analisis penyebab dan usulan tindakan didasarkan pada hasil observasi dan kelengkapan bukti pendukung yang ada.

Secara umum terdapat keterkaitan komprehensif antara pertanyaan pada indeks keamanan informasi (indeks KAMI), temuan yang muncul berdasarkan jawaban yang diberikan atas tiap-tiap pertanyaan, usulan tindakan perbaikan pada form CPAR

dari analisis obyek pertanyaan dan temuan serta penyajian rekomendasi umum sebagai bentuk generalisasi dari keseluruhan usulan tindakan perbaikan yang pada form CPAR untuk tiap-tiap area pengelolaan keamanan informasi.

Lebih lanjut tentang CPAR akan dijelaskan sebagai berikut :

Section 1 : Obyek berisi penjelasan tentang bahasan utama yang diambil dari 119 pertanyaan dalam penilaian dengan indeks keamanan informasi (indeks KAMI)

Contoh (pada Kerangka Kerja 4.1) :

Kebijakan dan prosedur keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya (Indeks KAMI Area Kerangka Kerja Pertanyaan 4.1)

Section 2 : Penyebab / pendukung berisi faktor – faktor penyebab maupun faktor pendukung yang ditemukan dari hasil temuan atas penetapan status jawaban yang diberikan pada pertanyaan untuk obyek tersebut. Keseluruhan temuan dapat dilihat pada Penilaian Aspek Kepatuhan Lampiran B – G.

Contoh (pada Kerangka Kerja 4.1) :

DJPBN sudah memiliki sejumlah kebijakan terkait pengelolaan keamanan informasi dan telah melaksanakan sejumlah tindakan pengamanan berdasarkan kepada KMK.479/KMK.01/2010 tentang kebijakan dan prosedur keamanan informasi namun sejumlah kebijakan (berdasar 11 area) belum semuanya memiliki petunjuk teknis dan prosedur pelaksanaan pengamanan pada tingkat Eselon II Kanwil DJPBN Jawa Timur

Section 3 : Usulan tindakan perbaikan berisi sejumlah langkah-langkah yang dibutuhkan sebagai perbaikan untuk permasalahan

yang muncul terkait dengan ketidaksesuaian / ketidaklengkapan pranata yang seharusnya ada pada obyek yang dibahas.

Contoh (pada Kerangka Kerja 4.1) :

1. Mendefinisikan tujuan serta ruang lingkup keamanan informasi yang ada di KANWIL DJPBN terutama untuk cakupan yang lebih spesifik terkait dengan pelaksanaan teknis pengelolaan keamanan informasi.
2. Menentukan kesesuaian kebijakan dan prosedur keamanan infomasi dengan kebijakan dan keamanan infomasi DJPBN secara umum berdasarkan undang-undang
3. Mendefinisikan peran dan tanggung jawab keamanan infomasi di dalamnya berdasarkan KMK No.479/KMK.01/ 2010 tentang peran dan tanggungjawab pengelola keamanan informasi termasuk peran dan tanggungjawab Information Security (IS) Manager dan Information Security (IS) Officer.
4. Merujuk referensi dari peraturan instansi, serta peraturan kepatuhan keamanan informasi lain yang terkait.
5. Membuat kontrol pengendalian pengelolaan keamanan informasi sesuai dengan proses bisnis KANWIL DJPBN dalam bentuk prosedur, instruksi kerja, petunjuk pelaksanaan (juklak), petunjuk teknis (juknis) berdasarkan Pengendalian Umum KMK No.479/KMK.01/2010.
6. Untuk dapat menuju pada tingkat keamanan yang lebih tinggi, kepatuhan pada kebijakan dan prosedur sebaiknya dievaluasi berkala tiap bulan atau semester. Setiap laporan evaluasi hendaknya didokumentasikan secara resmi dan dikomunikasikan serta disosialisasikan kepada semua pihak pelaksana DJPBN.

Section 4 : Tindak lanjut dan verifikasi adalah rangkaian tindakan yang dilaksanakan sebagai petunjuk dari pimpinan terkait dengan obyek pada section 1 sekaligus sebagai verifikasi atas usulan tindakan perbaikan terhadap obyek permasalahan secara institusional.

Contoh (pada Kerangka Kerja 4.1) :

Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera.

Form 5.1 CPAR Kerangka Kerja 4.1

<table>
<tr><td colspan="4"> 
KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN KANTOR WILAYAH PROVINSI JAWA TIMUR
GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640</td></tr>
<tr><td colspan="4">Section 1 : Obyek</td></tr>
<tr><td colspan="4">Kebijakan dan prosedur keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya</td></tr>
<tr><td>Nama & TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
<tr><td colspan="4">Section 2 : Penyebab / Pendukung</td></tr>
<tr><td colspan="4">DJPBN sudah memiliki sejumlah kebijakan terkait pengelolaan keamanan informasi dan telah melaksanakan sejumlah tindakan pengamanan berdasarkan kepada KMK.479/KMK.01/2010 tentang kebijakan dan prosedur keamanan informasi namun sejumlah kebijakan (berdasar 11 area) belum semuanya memiliki petunjuk teknis dan prosedur pelaksanaan pengamanan pada tingkat Eselon II Kanwil DJPBN Jawa Timur.</td></tr>
<tr><td>Nama & TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
<tr><td colspan="4">Section 3 : Usulan tindakan perbaikan</td></tr>
<tr><td colspan="4">Mendefinisikan tujuan serta ruang lingkup keamanan informasi yang ada di KANWIL DJPBN terutama untuk cakupan yang lebih spesifik terkait dengan pelaksanaan teknis pengelolaan keamanan informasi
Menentukan kesesuaian kebijakan dan prosedur keamanan infomasi dengan kebijakan dan keamanan infomasi DJPBN secara umum berdasarkan undang-undang.
Mendefinisikan peran dan tanggung jawab keamanan infomasi di dalamnya berdasarkan KMK No.479/KMK.01/2010 tentang peran dan tanggungjawab pengelola keamanan informasi termasuk peran dan tanggungjawab Information</td></tr>
</table>

Security (IS) Manager dan Information Security (IS) Officer Merujuk referensi dari peraturan instansi, serta peraturan kepatuhan keamanan informasi lain yang terkait. Membuat kontrol pengendalian pengelolaan keamanan informasi sesuai dengan proses bisnis KANWIL DJPBN dalam bentuk prosedur, instruksi kerja, petunjuk pelaksanaan (juklak), petunjuk teknis (juknis) berdasarkan Pengendalian Umum KMK No.479/KMK.01/2010 Untuk dapat menuju pada tingkat keamanan yang lebih tinggi, kepatuhan pada kebijakan dan prosedur sebaiknya dievaluasi berkala tiap bulan atau semester. Setiap laporan evaluasi hendaknya didokumentasikan secara resmi dan dikomunikasikan serta disosialisasikan kepada semua pihak pelaksana DJPBN			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Dari usulan tindakan perbaikan pada CPAR Kerangka Kerja 4.1 dan sejumlah tindakan perbaikan pada pertanyaan-pertanyaan selanjutnya untuk area Kerangka Kerja maka terbentuk sejumlah rekomendasi umum untuk perbaikan pada area Kerangka Kerja. Dalam hal ini rekomendasi perbaikan untuk Area Kerangka Kerja Keamanan Informasi adalah :

- Merencanakan dan menerapkan kebijakan dan prosedur keamanan informasi terhadap semua aktifitas teknologi informasi yang sudah didefinisikan komposisi, peran, wewenang dan tanggungjawabnya.
- Merencanakan evaluasi pengelolaan kebijakan keamanan informasi yang telah digunakan dengan mencantumkan peran, wewenang dan tanggungjawabnya.

- Melaksanakan dokumentasi dan pelaporan terhadap penerapan kerangka kerja pengelolaan keamanan informasi secara berkala.

(diolah dari sejumlah usulan tindakan perbaikan area Kerangka Kerja dan didasarkan pada KMK No.479/KMK.01/2010 dan KMK No.260/KMK.01/2009).

Bagian CPAR untuk kelima area pengelolaan ini selengkapnya tercantum pada lampiran H hingga L.

Halaman ini sengaja dikosongkan

BAB VI
KESIMPULAN DAN REKOMENDASI

Pada bab ini menjelaskan kesimpulan dan saran untuk keamanan informasi pada Kantor Wilayah Dirjen Perbendaharaan Jawa Timur. Perbaikan ini nantinya bisa digunakan untuk meningkatkan tingkat kelengkapan serta kematangan keamanan informasi berdasarkan 5 area yang sudah ditentukan.

6.1 Kesimpulan

Kesimpulan yang dapat diambil secara menyeluruh dalam pengerjaan tugas akhir dengan studi kasus evaluasi pengelolaan keamanan perbendaharaan negara oleh Kanwil DJPBN Jawa Timur antara lain :

- Berdasarkan kondisi sebelum penilaian aspek kepatuhan didapat skor keseluruhan area antara lain area Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, dan Teknologi berjumlah **423** (dari nilai maksimal **588**). Nilai yang sangat tinggi untuk status kesiapan TIK di lingkup Kanwil DJPBN.
- Dari aspek penilaian Peran TIK khususnya peran teknologi informasi bagi Kanwil DJPBN, menunjukkan bahwa peran TIK bagi institusi ini relatif tinggi yang menandakan peranan vital TIK bagi pelaksananaan perbendaharaan lingkup Kanwil DJPBN Jawa Timur (skor **36** dari **48**).
- Status kesiapan pengelolaan keamanan informasi yang meliputi kelengkapan perangkat keamanan pada 5 area yakni Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, dan Teknologi dinilai masih perlu adanya perbaikan (skor **337** dari nilai maksimal **588**).
- Hasil penilaian berdasarkan aspek kepatuhan menunjukkan pengelolaan keamanan informasi pada Kanwil DJPBN Jawa Timur guna menunjang pelayanan perbendaharaan sudah

dalam penerapan, namun dinilai masih perlu diperbaiki dalam hal kelengkapan perangkat pengamanannya (prosentase 57,31% temuan sesuai dan 14.69 % temuan yang tidak sesuai).

- Tingkat kematangan per-area untuk Tata Kelola terdapat pada level II, area Pengelolaan Risiko pada level II, area Kerangka Kerja berada pada level II, area Pengelolaan Aset berada pada level II, serta area Teknologi pada level II.
- Tingkat kematangan keseluruhan area berada pada level II dari level V (kesiapan sertifikasi ISO/IEC 27001:2005) yang artinya sudah terdapat pemahaman keamanan informasi di Kanwil DJPBN Jawa Timur namun masih tergolong aktif bukan proaktif.
- Berdasarkan status kesiapan yang terlihat dari skor akhir pengelolaan keamanan informasi, maka pengelolaan keamanan informasi dinyatakan masih perlu adanya perbaikan dalam memenuhi standarisasi ISO/IEC 27001:2005 terlebih pada efektifitas pelaksanaan kerangka kerja keamanan informasi berdasarkan penilaian indeks KAMI dimana aspek kepatuhan kerangka kerja memiliki nilai prosentase terkecil dibandingkan area evaluasi lainnya (prosentase 38% dari nilai capaian obyektif terhadap maksimum nilai area kerangka kerja).
- Perbaikan pengelolaan keamanan informasi di Kanwil DJPBN berdasarkan status kesiapan di atas lebih dispesifikkan pada area kerangka kerja dengan didukung oleh dokumen-dokumen prosedural sebagi implementasi kebijakan. Perbaikan dan peningkatan keamanan informasi dari seluruh pertanyaan pada lima area evaluasi keamanan yang tersebut di atas baik dari segi teknis dan non-teknis secara spesifik terlampir pada lampiran H-L.

6.2 Rekomendasi Perbaikan 5 Area Pengamanan

Rekomendasi yang dapat diambil sebagai perbaikan secara menyeluruh untuk peningkatan kelima area pengelolaan keamanan informasi :

6.2.1 Rekomendasi Perbaikan Area Tata Kelola Keamanan Informasi

- Efektivitas pengamanan dievaluasi berkala melalui proses yang terstruktur
- Memperbaiki beberapa kelemahan dalam sistem manajemen tata kelola sehingga dapat menghasilkan dampak signifikan terhadap pengelolaan keamanan informasi
- Meningkatkan poin-poin tata kelola keamanan yang sudah mematuhi ambang batas minimum pada area tata kelola
- Meningkatkan kesadaran semua pihak baik pimpinan, pelaksana dan pihak ketiga untuk menyadari tanggungjawab pengelolaan keamanan informasi
- Menerapkan seluruh persyaratan dan standar kompetensi dan keahlian pelaksana dalam pengelolaan keamanan informasi
  (berdasarkan KMK No.479/KMK.01/2010 Poin I, II, IV)

6.2.2 Rekomendasi Perbaikan Area Pengelolaan Risiko

- Merencanakan dan menerapkan seluruh pengelolaan risiko menjadi bagian dari kriteria penilaian efektifitas pengamanan terhadap semua layanan perbendaharaan Kanwil DJPBN
- Merencanakan dan mengevaluasi secara menyeluruh terhadap program pengelolaan risiko keamanan yang akan dilaksanakan

- Melaksanakan dokumentasi peningkatan langkah mitigasi yang diterapkan untuk mengetahui kondisi perkembangan penanganan dan pengendalian risiko
  (Berdasarkan PMK No.191/PMK.09/2008 dan KMK No.479/KMK.01/2010 Poin III, V dan XI)

6.2.3 Rekomendasi Perbaikan Area Kerangka Kerja Keamanan Informasi

- Merencanakan dan menerapkan kebijakan dan prosedur keamanan informasi terhadap semua aktifitas teknologi informasi
- Merencanakan dan menerapkan proses pengembangan rencana pemulihan bencana terhadap layanan TIK (teknologi informasi komunikasi) yang sudah didefinisikan komposisi, peran, wewenang dan tanggungjawabnya
- Merencanakan evaluasi pengelolaan kebijakan keamanan informasi yang telah digunakan dengan mencantumkan peran, wewenang dan tanggungjawabnya
- Melaksanakan dokumentasi dan pelaporan terhadap penerapan kerangka kerja pengelolaan keamanan informasi secara berkala
  (Berdasarkan KMK No.479/KMK.01/2010 dan KMK No.260/KMK.01/2009)

6.2.4 Rekomendasi Perbaikan Area Pengelolaan Aset Keamanan Informasi

- Merencanakan dan menerapkan secara menyeluruh proses penerapan definisi tingkatan akses dan matrix yang merekam alokasi akses
- Merencanakan dan menerapkan secara menyeluruh prosedur pengelolaan aset informasi
- Menerapkan sanksi atau hukuman yang telah dibuat kepada semua pihak yang lalai dalam melaksanaan pengelolaan keamanan aset informasi

- Merencanakan dan melaksanakan secara menyeluruh tata tertib pengamanan komputer, email, intranet dan internet serta pertukaran data dan informasi
- Melaksanakan pengendalian dan evaluasi secara menyeluruh terhadap aset informasi dan dokumentasi terhadap semua aktifitas pengelolaan keamanan aset informasi

  (Berdasarkan KMK No.479/KMK.01/2010 Poin III dan VIII, KMK No.512/KMK.01/2009 dan KMK No.21/KMK.01/2012)

6.2.5 Rekomendasi Perbaikan Area Teknologi dan Keamanan Informasi

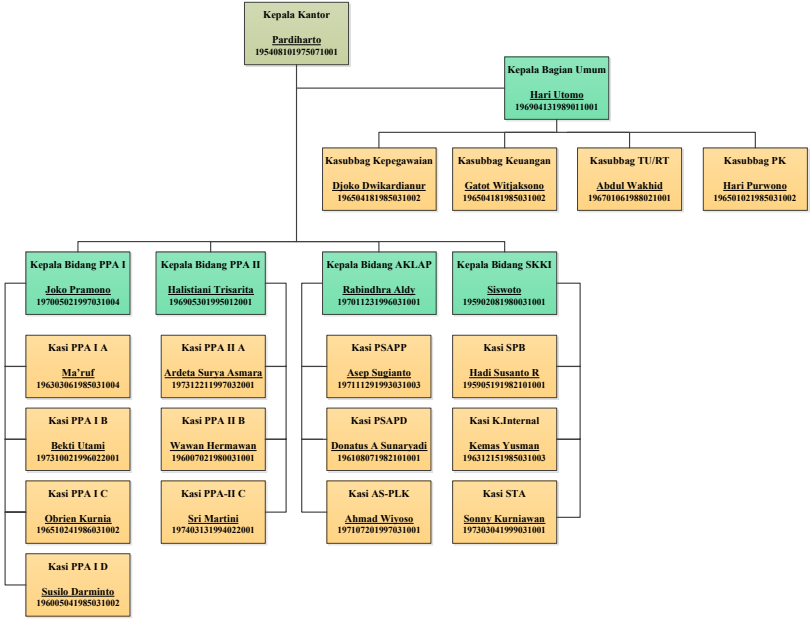
- Merencanakan penerapan secara menyeluruh pada proses konfigurasi standar untuk keamanan sistem bagi keseluruhan asset informasi dan perangkat jaringan yang dimutakhirkan
- Merencanakan dan menerapkan secara menyeluruh proses pengamanan untuk mendeteksi dan mencegah akses jaringan yang tidak resmi
- Melaksanakan secara menyeluruh prosedur keamanan informasi
- Menerapkan sanksi kepada seluruh pihak yang lalai dalam melaksanakan pengelolaan teknologi dan keamanan informasi
- Melaksanakan secara menyeluruh dokumentasi dan pelaporan terhadap segala aktifitas pengelolaan TIK (teknologi informasi komunikasi)

  (Berdasarkan KMK No.479/KMK.01/2010, KMK No. 512/KMK.01/2009, KMK No. 274/KMK.01/2010 dll)

Halaman ini sengaja dikosongkan

Lampiran A

A.1 Struktur Organisasi Kanwil DJPBN Jawa Timur



Gambar A.9.1 Struktur Organisasi Kanwil

Lampiran B

B.1 Penilaian Aspek Kepatuhan Peran TIK

Tabel B.10.1 Penilaian Aspek Kepatuhan Peran TIK

1.1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis	Minim
	Temuan	Total anggaran teknologi informasi Kanwil DJPBN kurang dari 1 Milyard (RKA-KL menunjukkan angka Rp. 299.270.000,00)
	Bukti	Dokumen RKA KL, DIPA Kanwil (Foto **M-3** dan **M-4**)
	Kesesuain (Ada/Tidak)	Ada
	Tanggal penyesuaian	3 Mei 2014

1.2	Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis	Rendah
	Temuan	Jumlah staff/ pegawai DJPBN Jawa Timur pada setiap Bidang dan Seksi yang menggunakan infrastruktur sekitar 115 (seratus lima belas) pegawai
	Bukti	List pegawai pada struktur organisasi Kanwil DJPBN Jawa Timur (Gambar A.1)
	Kesesuaian (Ada/Tidak)	Ada
	Tanggal penyesuaian	29 April 2014
1.3	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas Pokok dan Fungsi Instansi anda	Tinggi

	Keterangan pilihan	1. Kritis - Digunakan sebagai sarana utama penyelenggaraan layanan publik dan tugas utama instansi yang bersifat nasional dan strategis 2. Tinggi - Digunakan sebagai sarana utama penyelenggaraan layanan publik dan tugas utama instansi 3. Sedang - Digunakan untuk membantu penyelenggaraan layanan publik atau tugas utama instansi 4. Digunakan untuk menunjang kegiatan rutin 5. Hanya digunakan untuk mempermudah sejumlah kecil pekerjaan rutin, pencatatan, penyimpanan salinan dokumen, dll
	Temuan	Tingkat ketergantungan sangat tinggi terhadap layanan teknologi untuk menjalankan layanan publik dan/atau fungsi perbendaharaan baik untuk Revisi DIPA, Akuntansi Pelaporan, dll
	Bukti	SOP Kanwil DJPBN, aplikasi SPAN untuk Revisi DIPA pada Kanwil DJPBN (Foto **M-2 dan M-34**)
	Kesesuaian (Ada/Tidak)	Ada

	Tanggal penyesuaian	28 April 2014
	Catatan	Tugas dan layanan seluruh pelaksanaan fungsi perbendaharaan yang dilakukan oleh Kanwil DJPBN Jawa Timur berdasarkan teknologi dan bentuknya adalah Sistem Perbendaharaan dan Anggaran Negara yang memiliki fungsi penting terkait keuangan negara
1.4	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Kritis
	Keterangan pilihan	▶ Kritis - Proses kerja sistem/aplikasi yang merupakan rahasia negara dan data/informasi penting yang bersifat strategis ▶ Tinggi - Proses kerja sistem/aplikasi merupakan aset nasional dan data/ informasi penting berskala nasional ▶ Sedang - Ada sejumlah proses kerja sistem/aplikasi yang sangat spesifik dan data/informasi yang sulit didapatkan dari tempat yang lain ▶ Rendah - Ada sejumlah proses kerja sistem/aplikasi yang spesifik sesuai tugas instansi dan data/informasi yang bisa

		didapatkan dari tempat lain ▶ Minim - Tidak ada atau sedikit sekali - proses kerja sistem/aplikasi yang bersifat umum dan penyimpanan data publik
	STATUS : DUGAAN	
	Pengubahan Status Kepatuhan	
	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Tinggi
	Temuan	Nilai kekayaan intelektual SPAN (sistem perbendaharaan dan anggaran Negara) merupakan data internal yang spesifik dan sangat penting serta berskala nasional dan merupakan aset nasional.
	Bukti	Screenshot Fungsionalitas SPAN (Sistem Perbendaharaan dan Anggaran Negara), Foto DIPA (Daftar Isian Pelaksanaan Anggaran) (Foto **M-4 dan M-35)**
	Kesesuaian (Ada/Tidak)	Ada
	Tanggal penyesuaian	28 April 2014

	Catatan	Outcome yang dihasilkan oleh Kanwil Ditjen Perbendaharaan bersifat sangat spesifik beberapa diantaranya adalah DIPA, Laporan Keuangan Pemerintah Pusat (LKPP) yang menjadi acuan dalam evaluasi penganggaran yang dikenal dengan APBN, Laporan Akuntabilitas Kinerja Instansi Pemerintah (LAKIP) dan sejumlah output terkait dengan Daftar Isian Pelaksanaan Anggaran yang pelaksanaanya sangat spesifik terkait dengan penjabaran APBN bagi seluruh Kementerian lembaga bagi seluruh Satuan kerja dan tidak bisa ditemukan pada institusi pemerintahan lain di Indonesia. Namun sifatnya adalah informasi public berdasar UU No.14 thn 2008
1.5	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda	Kritis
	Keterangan pilihan	▶ Kritis - Tidak tersedianya layanan masyarakat karena digunakan sebagai sarana utama penyelenggaraan layanan publik dan tugas utama instansi yang bersifat nasional dan strategis ▶ Tinggi - Mengganggu tersedianya

		layanan masyarakat karena digunakan sebagai komponen utama penyelenggaraan layanan publik dan tugas utama instansi, sulit untuk digantikan proses manual ▶ Sedang - Berdampak pada tingkat layanan masyarakat karena digunakan untuk membantu penyelenggaraan layanan publik atau tugas utama instansi ▶ Rendah - Tidak mengganggu kinerja karena digunakan untuk menunjang kegiatan rutin ▶ Minim - Tidak ada dampak terhadap kinerja karena hanya digunakan untuk mempermudah sejumlah kecil pekerjaan rutin, pencatatan, penyimpanan salinan dokumen, dll
	Temuan	Dampak dari kegagalan sistem bagi Kanwil DJPBN Jatim mengganggu tersedianya layanan publik dalam bidang perbendaharaan (DIPA) yang proses administratifnya sangat mustahil jika dilakukan secara manual

	Bukti	Screenshot Alur Revisi DIPA dan lingkup Satker secara Nasional dalam SPAN (Foto **M-15 dan M-36)**
	Kesesuaian (Ada/Tidak)	Ada
	Tanggal penyesuaian	28 April 2014
	Catatan	Layanan teknologi informasi merupakan basis dalam pelaksanaan aplikasi DIPA yang melayani seluruh satker. Selain itu juga web SPAN melayani dalam pemrosesan serta akses aplikasi internal di Kanwil. Hal ini menyebabkan teknologi informasi menjadi hal penting bagi pendukung otomatisasi proses bisnis di dalamnya, tidak hanya fungsi pokok namun juga dalam bidang administratif.
1.6	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda	Kritis
	Keterangan pilihan	▶ Minim – Sistem beroperasi secara individu, tidak terkait dengan sistem lainnya ▶ Rendah: Sistem beroperais secara terintegrasi dengan sistem lainnya, tetapi ketersediaannya tidak mengganggu

		sistem lain tersebut ▶ Sedang: Sistem beroperasi secara terintegrasi dengan sistem lainnya, gangguan ketersediaan akan mengganggu sistem lain tersebut ▶ Tinggi: Sistem harus beroperasi dengan sistem lainnya dan gangguan ketersediaan akan sangat mengganggu sistem lain tersebut ▶ Kritis: Sistem merupakan bagian / komponen penting dari sistem lainnya, dan gangguan ketersedian mengganggu layanan yang berskala nasional
	Temuan	Menurut temuan pada jawaban di atas bahwa tingkat ketergantungan ketersediaan sistem layanan menghubungkan antar seksi dan bidang di Kanwil DJPBN dengan fungsi terpadu secara nasional. Ketergantungan tersebut mengakibatkan terganggunya layanan public berisfat nasional dan dalam jumlah data yang sangat besar terutama dalam hal penganggaran dan pencairan dana

	Bukti	Screenshot visual Kompleksitas SPAN dalam Keuangan Negara dan Skala Transformasi (Foto **M-36 dan M-37**)
	Kesesuaian(Ada/Tidak)	Ada
	Tanggal penyesuaian	28 April 2014
1.7	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi pemerintah lainnya atau terhadap ketersediaan sistem pemerintah berskala nasional	Kritis
	Pilihan Jawaban	▶ Minim: tidak ada dampak apapun ▶ Rendah: dampaknya tidak berarti, hanya mengakibatkan terganggunya ketersediaan sejumlah kecil data/proses umum ▶ Sedang: gangguan yang dapat menghambat pekerjaan atau layanan publik, hilangnya data/informasi publik dengan jumlah yang cukup besar ▶ Tinggi: gangguan terhadap layanan publik yang bersifat nasional, hilangnya data publik dalam jumlah sangat besar ▶ Kritis: gangguan terhadap layanan publik yang bersifat strategis, terkait data /

		informasi rahasia milik negara
	STATUS : DUGAAN	
	Pengubahan Status Kepatuhan	
	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi pemerintah lainnya atau terhadap ketersediaan sistem pemerintah berskala nasional	Tinggi
	Temuan	Dampak kegagalan sistem dapat mengganggu proses pekerjaan atau layanan perbendaharaan serta rusaknya data dalam jumlah yang cukup besar secara nasional terkait keuangan Negara
	Bukti	Screenshot tupoksi dan layanan KANWIL DJPBN pada website, RKA-KL Nasional dan jumlah KPPN se-Jawa Timur yang menjelaskan mengenai unit-unit kerja dan satker yang dihubungkan oleh sistem perbendaharaan DJPBN. **(Foto M-1, M-38)**
	Kesesuaian (Ada/Tidak)	Ada
	Catatan	Layanan teknologi informasi merupakan basis dalam pelaksanaan aplikasi DIPA yang melayani seluruh satker. Selain itu juga web SPAN melayani dalam pemrosesan serta akses

		aplikasi internal di Kanwil. Jumlah KPPN yang ditangani dalam Provinsi Jawa Timur juga menunjukkan kepentingan yang tinggi terhadap TIK. Hal ini menyebabkan teknologi informasi menjadi hal penting untuk mendukung otomatisasi proses bisnis di dalamnya, tidak hanya fungsi pokok namun juga dalam bidang administratif. Namun DIPA sebagai produk Kanwil sifatnya adalah informasi public berdasar UU No.14 thn 2008
1.8	Tingkat sensitifitas pengguna sistem TIK di Instansi anda	Kritis
	Keterangan pilihan	▶ Minim: tidak peduli - jarang menggunakan ▶ Rendah: membutuhkan layanan TIK, tetapi mudah mencari alternatif lain ▶ Sedang: membutuhkan layanan TIK untuk menunjang pekerjaan rutin ▶ Tinggi: sangat membutuhkan layanan TIK untuk tugas utama ▶ Kritis: sangat membutuhkan layanan TIK untuk menjalankan tugas instansi
	STATUS : DUGAAN	

	Pengubahan Status Kepatuhan	
	Tingkat sensitifitas pengguna sistem TIK di Instansi anda	Tinggi
	Temuan	Stakeholder Kanwil DJPBN seperti satker, dan karyawan sangat membutuhkan layanan teknologi informasi guna menjalankan proses pelayanan perbendaharaan.
	Bukti	Screenshoot SPAN, screenshot penggunaan aplikasi, screenshot tupoksi dan layanan KANWIL DJPBN yang terkait SPAN (**Foto M-1, M-16, dan M-34**)
	Kesesuian (Ada/Tidak)	Ada
	Tanggal Validasi	25 April 2014
	Catatan	Hampir keseluruhan fungsionalitas di Kanwil DJPBN menggunakan TIK sebagai instrument utama dalam menjalankan tugas pokok. Namun terdapat pula sejumlah fungsi administratif yang sifatnya klerikal .

1.9	Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya	Kritis
	Keterangan pilihan	▶ Minim: tidak ada kaitannya dengan kepatuhan terhadap Kebijakan, Peraturan/UU ▶ Rendah: ada sejumlah Kebijakan yang harus diikuti dalam penyelenggaraan layanan menggunakan sistem ini ▶ Sedang: proses kerja sistem/aplikasi harus mematuhi sejumlah Kebijakan dan Peraturan internal atau eksternal ▶ Tinggi: proses kerja sistem/aplikasi harus mengikuti Peraturan dan UU ▶ Kritis: proses kerja sistem/aplikasi harus mematuhi sejumlah UU dan perangkat hukum terkait
	Temuan	Proses kerja sistem/aplikasi mengenai perbendaharaan negara harus mematuhi Kebijakan dan Peraturan dan pelaksanaannya mengacu pada peraturan dan keputusan negara. Namun kondisinya untuk secara teknis penggunaan layanan aplikasi masih membutuhkan cascading

		peraturan kedalam juknis-juknis yang mengaturnya.
	Bukti	Screenshot sejumlah peraturan perundang-undangan untuk pelaksanaan Sistem Perbendaharaan dan Anggaran Negara dan sejumlah KMK/PMK yang mengatur implementasi aplikasi lainnya **(Foto M-39 dan M-40)**
	Kesesuaian (Ada/Tidak)	Ada
	Tanggal penyesuaian	25 April 2014
	Catatan	Pada dokumen perundang-undangan dijelaskan mengenai beberapa proses kerja sistem/aplikasi mulai dari - Proses Revisi DIPA yang patuh pada PMK No.7/PMK.02/2014 - PMK Penggunaan Username dan Password Aplikasi SPAN - PMK tentang Aplikasi Sistem Perbendaharaan Anggran Negara Diikuti pula sejumlah peraturan untuk aplikasi yang berkaitan dengan administratif (tata usaha dan kepegawaian) yang

		sepenuhnya didokumentasikan dalam peraturan atau petunjuk penggunaan secara formal.

1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda	Kritis
	Keterangan pilihan	▶ Minim - tidak ada dampak apapun ▶ Rendah - dampaknya tidak signifikan, hanya mengakibatkan terganggunya atau terungkapnya sejumlah kecil data atau kegiatan/program kerja umum ▶ Sedang - terungkapnya informasi yang sangat mengganggu program kerja, hilangnya data/informasi publik dengan jumlah yang cukup besar ▶ Tinggi - terungkapnya informasi sensitif atau terbatas yang dapat berakibat pada gagalnya program kerja atau mengganggu kinerja / kredibilitas pemerintah

		▶ Kritis - hilangnya aset informasi penting berskala nasional atau terungkapnya informasi rahasia terkait keamanan negara
	Temuan	Potensi kerugian bagi keuangan negara akan terjadinya kegagalan keamanan informasi berdampak kritis karena pasti akan menggagalkan dan akan mengganggu program kerja pencairan dana dan pengelolaan anggaran nasional, khususnya pada lingkup DJPBN dan satuan kerja dalam wilayah bayar 33 provinsi seluruh Indonesia
	Bukti	Screenshot tupoksi dan layanan DJPBN, RKA-KL Nasional dan skala fungsionalitas SPAN dengan lingkup pada seluruh Satker secara Nasional yang keseluruhan DIPAnya dihubungkan oleh sistem perbendaharaan dan anggaran negara DJPBN. **(Foto M-1, M-36 dan M-38)**
	Kesesuaian (Ada/Tidak)	Ada
	Tanggal penyesuaian	26 April 2014

	Catatan	Potensi kerugian hilangnya data atau kegagalan keamanan informasi dapat menyebabkan terhambatnya proses penganggaran dan perbendaharaan karena KANWIL DJPBN sendiri juga mengelola input data serta proses akses sambungan secara nasional. Dampak negatif tidak secara langsung menggagalkan program kerja satuan kerja (SATKER), namun berdampak pada kesulitan pencairan dana satker lingkup wilayah dan penganggaran secara Nasional.

1.11	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK	Kritis
	Keterangan pilihan	▶ Minim: sistem dapat dioperasikan sendiri dengan teknologi yang mudah ditemui di pasaran ▶ Rendah: sistem dapat dioperasikan sendiri dengan dukungan teknisi eksternal, teknologi dengan spesifikasi yang tidak umum

		▶ Sedang: sistem harus dioperasikan dengan dukungan teknis dari pihak eksternal, teknologi dengan spesifikasi yang cukup spesifik ▶ Tinggi: sistem tidak dapat dioperasikan tanpa dukungan teknis dari pihak eksternal, teknologi dengan spesifikasi yang sangat spesifik ▶ Kritis: sistem hanya dapat dioperasikan dengan dukungan teknis dari pihak eksternal tertentu, teknologi dengan spesifikasi tinggi dan ketersediaan perangkat yang sangat terbatas
	STATUS : DUGAAN	
	Pengubahan Status Kepatuhan	
	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK	Tinggi
	Temuan	Tingkat ketergantungan Kanwil DJPBN dalam menjalankan/mengoperasikan sistem layanan jaringan harus dibantu oleh pihak ketiga dengan teknologi yang cukup spesifik dengan penggunaan perangkat yang umumnya digunakan dalam dukungan TIK

	Bukti	Screenshot proses aplikasi, suasana pelayanan dan ruang lingkup SPAN (**M-41, M-42 dan M-43**)
	Kesesuian (Ada/Tidak)	Ada
	Tanggal penyesuaian	25 April 2014
	Catatan	Dari hasil observasi menunjukkan bahwa kegiatan operasional baik sistem atau fisik pada Kanwil serta yang terkait aplikasi SPAN (Sistem Perbendaharaan dan Anggaran Negara) merupakan sistem informasi yang sangat spesifik dan khusus, bernilai strategis dan menggunakan sejumlah panduan / *standart operating procedure* dalam rangka pengelolaan keuangan Negara. Permasalahan terhadap sistem ini ditangani langsung oleh SPAN sebagai satker dan Direktorat Transformasi Perbendaharaan pada Kantor Pusat.
1.12	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan inssformasi	Krirtis

	Keterangan pilihan	▶ Minim: hanya digunakan sebagai penunjang pekerjaan rutin (pencatatan, penyimpanan salinan dokumen umum, dll) - sistem relatif bersifat terbuka ▶ Rendah: digunakan untuk menunjang sejumlah kegiatan tugas pokok, sistem hanya digunakan secara internal organisasi ▶ Sedang: digunakan untuk membantu penyelenggaraan layanan publik atau tugas utama instansi, sistem digunakan secara internal dan terbatas ▶ Tinggi: digunakan sebagai sarana utama penyelenggaraan layanan publik dan tugas utama instansi, akses ke fungsi administrasi sistem atau basis data dibatasi untuk yang mempunyai wewenang ▶ Kritis: digunakan sebagai sarana utama penyelenggaraan layanan publik dan tugas utama instansi yang bersifat nasional dan strategis, akses ke fungsi administrasi sistem atau basis data

		dibatasi secara ketat, dengan wewenang dan pemantauan khusus
	Temuan	Tingkat kekritisan layanan perbendaharaan negara dianggap **kritis** karena memang berfungsi sebagai layanan publik dalam bidang teknis perbendaharaan serta proses administrative yang diatur khusus bagi kepentingan yang berwenang baik tingkat manajerial maupun pegawai Kanwil DJPBN.
	Bukti	Screenshot akun pengguna SPAN, screenshot akses kewenangan SPAN, penguncian ipconfig dalam akses SPAN **(Foto M-20, M-29 dan M-44)**
	Kesesuaian (Ada/Tidak)	Ada
	Tanggal penyesuaian	25 April 2014

	Catatan	Tingkat klasifikasi pengguna perbendaharaan negara terdiri dari front dan middle serta manajerial. Pengguna tersebut diidentifikasi dengan adanya email domain @depkeu.go.id, atau akses khusus user SPAN. Hal tersebut menunjukkan bahwa untuk masuk ke dalam aplikasi SPAN membutuhkan autentifikasi username dan password. Pengaturan penggunaan akses untuk SPAN juga diatur secara tersendiri sehingga tidak seluruh pegawai memiliki Akses kepada Aplikasi SPAN.

Lampiran C

C.1 Penilaian Aspek Kepatuhan Area I – Tata Kelola

Tabel C.11.1 Penilaian Aspek Kepatuhan Area I – Tata Kelola

2.1	II	1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pimpinan (Kanwil, Kabu, Kabid dan Kasie) secara resmi dan prinsip bertanggung jawab pada pelaksanaan program keamanan termasuk dalam kebijakan terkait
			Bukti	▶ KMK 479/KMK.01/2010 yang mensyaratkan terbentuknya CISO ▶ Tanggung jawab pimpinan pada *Strategy Focused Organization* **(Foto M-9 dan M-12)**
			Kesesuian (Kesesuian (Ada/ Tidak))	Ada
			Tanggal penyesuaian	22 April 2014

2.2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Kanwil DJPBN memiliki fungsi dan bagian secara spesifik mempunyai tugas dan tanggung jawab mengelola keamanan informasi secara informal pada Bidang SKKI khususnya Supervisi Teknis Aplikasi dan Seksi Kepatuhan Internal. Pada kondisi yang seharusnya, DJPBN mensyaratkan adanya *Information Security Officer* dalam organisasi (KMK.479/KMK.01/2010), namun pengimplementasian penugasan tim keamanan informasi belum dilakukan secara tertulis.
			Bukti	▶ *Printscreen* KMK 479 / KMK.01 / 2009 ▶ *Strategy Focused Organization* pada Supervisi Teknis Aplikasi **(Foto M-9 dan M-12)**

			Kesesuian (Kesesuian (Ada/ Tidak))	Ada
			Tanggal penyesuaian	20 April 2014
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak pejabat / petugas pelaksana DJPBN khususnya dalam penerapan KMK 479/KMK.01/2010 CISO (Kakanwil DJPBN) mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi namun pembentukannya belum dilaksanakan di tingkat Kanwil DJPBN Jatim masih dilaksanakan dalam pengendalian internal SKKI
			Bukti	Screenshot tanggung jawab CISO dan IKU Supervisi Teknis Aplikasi **(Foto M-7 dan M-24)**
			Kesesuian (Kesesuian (Ada/ Tidak))	Ada
			Tanggal penyesuaian	20 April 2014

2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Penanggung jawab keamanan informasi dalam hal ini Supervisi KPPN dan Kepatuhan Internal diberikan alokasi sumber daya manusia yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi. Berdasarkan pengamatan pada struktur organisasi untuk tenaga manajerial karyawan sudah memadai begitupun untuk teknis jumlah karyawan namun terkendala dengan tidak adanya penetapan khusus SKKI untuk fungsi tim keamanan informasi.
			Bukti	▶ Output SKKI pada SFO Kanwil DJPBN ▶ Kriteria serta tanggung jawab pada IKU SKKI

				▶ Slide Tim Keamanan Informasi Kominfo ▶ Jumlah alokasi pada kebijakan teknis yang belum ada (Foto **M-7, M-9 dan M-33**)
			Kesesuian (Kesesuian (Ada/ Tidak))	Ada, namun untuk alokasi dan kebijakan teknis memang belum ada
			Tanggal penyesuaian	25 April 2014
			Catatan	Pada dokumen pengendalian internal, pengawasan terkait pengendalian aplikasi, pelaksana dan dokumen ada tapi belum diatur alokasi sumber daya berdasarkan tingkat sekuritas masing-masing aspek TRP. Kebijakan terkait CISO tingkat eselon II belum secara eksplisit (masih dalam lingkup pengendalian internal).
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Dalam Penerapan / Diterapkan Sebagian

			Temuan	Pihak pelaksana Supervisi KPPN dan Kepatuhan Internal dalam proses dan fungsinya telah menerapkan kebutuhan audit internal termasuk persyaratan seregasi kewenangan dalam rangka melaksanakan fungsi berdasarkan SFO Kanwil DJPBN namun untuk keamanan informasi secara eksplisit belum tertuang lebih detil kedalam teknis pelaksanaan pengendalian
			Bukti	Daftar Uji Pengendalian Utama Tabel Rancangan Pengendalian Laporan Pengendalian Utama Tw.3 SFO (strategy focused organization) (Foto **M-9, M-45, M-46 dan M-47**)
			Kesesuian (Ada/ Tidak)	Ada
			Tanggal penyesuaian	3 Mei 2014
			Catatan	Tugas dan wewenang didefinisikan berdasarkan kinerja pembuatan pengendalian utama organisasi misal pengendalian prosedur sebagai acuan pelaksana dalam

				menjalankan tanggung jawabnya. Untuk lebih pada tugas spesifik keamanan informasi biasanya dipetakan pada *cascading master plan* (dalam hal ini SFO) dan dokumen pengelolaan risiko
2.6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	DJPBN umumnya dan Kanwil DJPBN khususnya sudah mendefiniskkan persyaratan / standar kompetensi dan keahlian pelaksana SKKI dalam hal pengendalian internal namun spesifik pengelolaan keamanan informasi secara khusus belum didefinisikan. Namun telah dimulai program-program seleksi kompetensi terkait keamanan informasi
			Bukti	Screenshot IKU SKKI Brief Tes Keamanan Informasi

				Pelaksanaan Tes Online Keamanan **(Foto M-7, M-21 dan M-22)**
			Kesesuian (Kesesuian (Ada/ Tidak))	Ada
			Tanggal penyesuaian	3 Mei 2014
2.7	II	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pelaksana pengendalian internal di DJPBN khususnya yang dilakukan oleh Kanwil DJPBN sudah memiliki kompetensi dan keahlian yang memadai sesuai persyaratan / standar yang berlaku dan diterapkan secara menyeluruh namun untuk keamanan informasi secara khusus masih menunggu evaluasi tes online keamanan informasi DJPBN
			Bukti	IKU pegawai yang mensyaratkan Dokumen daftar kompetensi (*hard competency*) yang bersifat wajib pada Seksi Kepatuhan Internal dan

				Tes Online Keamanan Informasi (Foto **M-7 dan M-21**)
			Kesesuian (Ada/ Tidak)	Ada, namun ada beberapa yang tidak sesuai misal kriteria dan kompetensi yang diharapkan dalam *hard competency* tidak tertulis / terdokumentasikan.
			Tanggal penyesuaian	3 Mei 2014
2.8	II	1	Apakah organsiasi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak Kanwil DJPBN telah menerapkan secara menyeluruh mengenai program sosialisasi dan peningkatan pemahaman untuk keamanan informasi dengan semua pihak terkait. Semua program dilaksanakan secara online dan offline melalui serangkaian test ataupun sosialisasi dan gugus kendali mutu.

			Bukti	Contoh sertifikat pelatihan atau sosialisasi, Gugus Kendali Mutu dan tes online terkait pengelolaan keamanan informasi **(Foto M-14, M-21 dan M-32)**
			Kesesuian (Ada/ Tidak)	Ada
			Tanggal penyesuaian	3 Mei 2014
2.9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Kanwil DJPBN dalam proses menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengamanan
			Bukti	Bukti pelatihan atau sertifikasi pejabat atau petugas, uji kompetensi yang tertera di website SPAN dan brief tes online keamanan informasi **(Foto M-21, M-26, dan M-32)**
			Kesesuian (Ada/ Tidak)	Ada

			Tanggal penyesuaian	28 Mei 2014
2.10	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal maupun eksternal untuk mengidentifikasikan persyaratan/kebutuhan pengamanan dan menyelesaikan permasalahan yang ada?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	DJPBN untuk masa sekarang dalam proses menerapkan tanggung jawab pengelolaan keamanan informasi dengan pihak pengelola / pengguna aset informasi secara internal maupun eksternal berdasarkan KMK..479 /KMK 01/ 2010 termasuk kontrak kerjasama dengan pihak ketiga dan kontrak kerjasama dengan satuan pengamanan Kanwil DJPBN
			Bukti	▶ Penetapan 11 Area Pengendalian berdasar ISO 27001:2005 lingkup Departemen Keuangan dengan cakupan internal dan eksternal (KMK No.479 / KMK.01/2010) ▶ SPer Satuan Pengamanan

				▶ Pedoman Akses Pihak Ke-3 **(Foto M-12 dan M-69)**
			Kesesuian (Kesesuian (Ada/ Tidak))	Ada, beberapa hanya pihak internal, pihak eksternal belum didefinisikan lebih terperinci
			Tanggal penyesuaian	27 April 2014
2.11	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak DJPBN khususnya Kanwil DJPBN secara menyeluruh menerapkan koordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan) dan pihak eksternal terkait yang berkepentingan (aparat keamanan) untuk menerapkan dan menjamin seluruh kepatuhan pengamanan informasi.
			Bukti	Dokumentasi satuan pengamanan, 11 Area Keamanan informasi KMK

				479/KMK.01/2010 (**Foto M-25 dan M-69**)
			Kesesuian (Ada/ Tidak)	Ada, beberapa (pengamanan aset informasi pada Kanwil / GKN dilakukan dengan perangkat teknologi dan Satuan Pengamanan
			Tanggal penyesuaian	3 Mei 2014
			Catatan	Satuan kerja yang terkait dengan sistem dan aplikasi khususnya pada SPAN-DJPBN antara lain - DJA - Sekjen - Pusintek - DJPBN Namun secara spesifik untuk keamanan informasi khusunya perbendaharaan negara belum terlalu didefinisikan dalam fungsi tiap bagian ataupun pihak eksternal seperti adanya SKB, dll

2.12	III	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	DJPBN telah menerapkan tanggung jawab mengenai pengelolaan 11 domain area keamanan informasi berdasar KMK 479/KMK.01/2010 dan BCM berdasar KMK. 260/KMK. 01/2009 serta Analisis Resiko
			Bukti	▶ KMK 260/ KMK.01/2009 terkait DRP dan BCM DJPBN ▶ DRC SPAN pada website span ▶ Dokumen Pengelolaan Risiko ▶ Dokumen Mitigasi Risiko ▶ (Foto **M-8, M-75, M-76 & M-77**)
			Kesesuian (Ada/ Tidak)	Ada
			Catatan	▶ DRP (disaster recovery plan) merupakan dokumen pengelolaan bencana termasuk tindakan mitigasi, sedangkan BCP (Business Continuity Plan) adalah

				dokumen keberlangsungan penyediaan produk dan layanan pada tingkat yang diterima pasca gangguan
2.13	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Kanwil DJPBN secara menyeluruh melaporkan kondisi kinerja/ efektivitas dan kepatuhan program melalui laporan pengendalian internal kepada pimpinan instansi secara rutin
			Bukti	*Strategy Focused Organization* LPPPI Kanwil DJPBN Triwulan 3 LPPPI KPPN April 2014 (Foto **M-9, M-78 dan M-79**)
			Kesesuaian (Ada/Tidak)	Ada, namun hanya beberapa.
			Tanggal penyesuaian	3 April 2014

			Catatan	Belum secara spesifik menyebut laporan pengamanan informasi, namun ada pengendalian yang berkala serta laporan rutin terkait pengendalian informasi dan checklist maintenance perangkat secara keseluruhan; dan resmi dilaporkan kepada pimpinan instansi
2.14	III	2	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	Dalam Penerapan/ Diterapkan Sebagian
			Temuan	DJPBN berdasar KMK 479/ KMK.01/2010 melaksanakan evaluasi atas seluruh rekomendasi terkait TIK dan wujud nyatanya adalah SPAN sebagai program khusus untuk sasaran strategis TIK termasuk pengamanan informasi berdasar Renstra KMK.40/KMK.01/2010 hal. 66 dst. Khusus pada Kanwil DJPBN

				hal-hal yang mencakup pengelolaan informasi menjadi konsideran khusus bagi Seksi STA (Supervisi Teknis Aplikasi) SKKI
			Bukti	▶ KMK No.40/KMK.01/2010 ▶ KMK No.479/KMK.01/2010 ▶ SFO Kanwil DJPBN **(Foto M-9, M-12 dan M-80)**
			Kesesuian (Ada/ Tidak)	Ada
			Tanggal penyesuaian	25 April 2014
2.15	IV	3	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Dalam Perencanaan
			Temuan	Pimpinan satuan kerja di Kanwil DJPBN diharuskan melakukan penetapan program khusus untuk pengamanan informasi namun saat ini belum ada penerapan di tingkat Kanwil karena kurangnya

				penjelasan rinci dari KMK.479 /KMK.01.2010 dan KMK.350/ KMK.01/2010 yang sebelumnya telah mensyaratkan kepatuhan pengamanan informasi yang juga menjadi tanggungjawab secara menyeluruh institusi.
			Bukti	▶ KMK No.40/KMK.01/2010 ▶ KMK No.479/KMK.01/2010 ▶ KMK No.350/KMK.01/2010 **(Foto M-12,M-18 dan M-80)**
			Kesesuian (Ada/ Tidak)	Ada
			Tanggal penyesuaian	3 April 2014
			Catatan	Pada ke-3 KMK ini diatur mengenai kebutuhan infrastruktur serta pengembangan informasi termasuk didalamnya pengamanan informasi. Kurangnya juknis mengenai program khusus untuk tindakan pengamanan informasi lingkup Kanwil menjadikannya tidak terprogram secara khusus.

2.16	IV	3	Apakah Instansi anda sudah mendefinisikan paramater, metrik dan mekanisme pengukuran kinerja pengelolaan keamanan informasi?	Dalam Perencanaan
			Temuan	Pimpinan satuan kerja di Kanwil DJPBN diharuskan mendefinisikan parameter, metric dan mekanisme untuk pengamanan informasi, namun saat ini belum ada penerapan di tingkat Kanwil karena kurangnya penjelasan rinci dari KMK.479 /KMK.01.2010 dan KMK.350/ KMK.01/2010 yang sebelumnya telah mensyaratkan kepatuhan pengamanan informasi yang juga menjadi tanggungjawab secara menyeluruh institusi.
			Bukti	▶ KMK No.40/KMK.01/2010 ▶ KMK No.479/KMK.01/2010 ▶ KMK No.350/KMK.01/2010 **(Foto M-12,M-18 dan M-80)**
			Kesesuian (Ada/ Tidak)	Ada
			Tanggal penyesuaian	3 April 2014

2.17	IV	3	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Dalam Perencanaan
			Temuan	Pimpinan satuan kerja di Kanwil DJPBN diharuskan mendefinisikan program penilaian kinerja untuk pengamanan informasi dalam penilaian hard competency, namun saat ini belum ada penerapan di tingkat Kanwil karena kurangnya penjelasan rinci dari KMK.479 /KMK.01.2010 dan KMK.350/ KMK.01/2010 yang sebelumnya telah mensyaratkan kepatuhan pengamanan informasi yang juga menjadi tanggungjawab secara menyeluruh dalam institusi.
			Bukti	▶ KMK No.40/KMK.01/2010 ▶ KMK No.479/KMK.01/2010 ▶ KMK No.350/KMK.01/2010 **(Foto M-12,M-18 dan M-80)**
			Kesesuaian (Ada/Tidak)	Ada

			Tanggal penyesuaian	3 April 2014
			Catatan	Pada ke-3 KMK ini diatur mengenai kebutuhan infrastruktur serta pengembangan informasi termasuk didalamnya pengamanan informasi. Kurangnya juknis mengenai program khusus untuk tindakan pengamanan informasi lingkup Kanwil menjadikannya tidak terprogram secara khusus dan masih menjadi bagian penilaian dari pengendalian internal Kanwil DJPBN. Penilaian kinerja berdasar IKU-pun belum secara spesifik mensyaratkan tentang kemampuan pengelolaan keamanan informasi
2.18	IV	3	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan dan mengevaluasi pencapaiannya secara rutin, termasuk pelaporannya kepada pimpinan Instansi?	Dalam Penerapan / Diterapkan Sebagian
			STATUS : DUGAAN	

			Pengubahan Status Kepatuhan	
			Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan dan mengevaluasi pencapaiannya secara rutin, termasuk pelaporannya kepada pimpinan Instansi?	Dalam Perencanaan
			Temuan	Pimpinan satuan kerja di Kanwil DJPBN diharuskan mendefinisikan target dan sasaran untuk pengelolaan pengamanan informasi termasuk evaluasinya secara rutin, namun saat ini belum ada penerapan di tingkat Kanwil karena kurangnya penjelasan rinci dari KMK.479 /KMK.01.2010 dan KMK.350/KMK.01/2010 yang sebelumnya telah mensyaratkan kepatuhan pengamanan informasi dan juga penetapan target dan sasaran pengeloaaan keamanan informasi dalam institusi.
			Bukti	▶ KMK No.40/KMK.01/2010

				▶ KMK No.479/KMK.01/2010 ▶ KMK No.350/KMK.01/2010 **(Foto M-12,M-18 dan M-80)**
			Kesesuaian (Ada/Tidak)	Ada
			Tanggal penyesuaian	25 April 2014
			Catatan	Pada ke-3 KMK ini diatur mengenai kebutuhan infrastruktur serta pengembangan informasi termasuk didalamnya evaluasi pengamanan informasi. Kurangnya juknis mengenai program khusus untuk tindakan pengamanan informasi lingkup Kanwil menjadikannya tidak terprogram secara khusus dan masih menjadi bagian dari evaluasi pengendalian internal Kanwil DJPBN. Penilaian pengendalian berdasar SFO-pun belum secara spesifik mensyaratkan tentang evaluasi pengelolaan keamanan informasi

2.19	IV	3	Apakah Instansi anda sudah mengidentifikasi legislasi dan perangkat hukum lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisis tingkat kepatuhannya?	Dalam Penerapan / Diterapkan Sebagian
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah Instansi anda sudah mengidentifikasi legislasi dan perangkat hukum lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisis tingkat kepatuhannya?	Dalam Perencanaan
			Temuan	Pimpinan satuan kerja di Kanwil DJPBN diharuskan mendefinisikan analisis tingkat kepatuhan untuk pengelolaan pengamanan informasi termasuk legislasi dan perangkat hukumnya, namun saat ini belum ada analisis tingkat kepatuhan di tingkat Kanwil karena kurangnya penjelasan rinci dari KMK.479 /KMK.01.2010 dan KMK.350/ KMK.01/2010 yang sebelumnya telah mensyaratkan

				kepatuhan pengamanan informasi dan juga penetapan analisis tingkat kepatuhan pengeloaaan keamanan informasi dalam institusi.
			Bukti	▶ KMK No.40/KMK.01/2010 ▶ KMK No.479/KMK.01/2010 ▶ KMK No.350/KMK.01/2010 **(Foto M-12,M-18 dan M-80)**
			Kesesuian (Kesesuian (Ada/ Tidak))	Ada
			Tanggal penyesuaian	3 April 2014
			Catatan	Pada ke-3 KMK ini diatur mengenai pengendalian dan aspek kepatuhan pengamanan informasi termasuk didalamnya kewajiban evaluasi pengamanan informasi. Kurangnya juknis mengenai compliance / kepatuhan untuk tindakan pengamanan informasi lingkup Kanwil menjadikannya tidak terprogram secara khusus dan masih menjadi bagian dari evaluasi pengendalian internal Kanwil DJPBN. Penilaian pengendalian

				berdasar SFO-pun belum secara spesifik mensyaratkan tentang evaluasi kepatuhan pengelolaan keamanan informasi
2.20	IV	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Dalam Penerapan / Diterapkan Sebagian
			Bukti	Disamping ketiga produk hukum diatas, dalam KMK No. 512/KMK.01/2010 terdapat sanksi pelanggaran baik administratif dan sanksi teknis (Foto **M-12,M-13, M-18 M-80**)
			Kesuaian (Ada/Tidak)	Ada
			Tanggal penyesuaian	6 April 2014
			Catatan	Kebijakan terkait keamanan informasi dan langkah penanggulanagan insiden telah didefinisikan namun pelanggaran hukum hanya ditemukan pada KMK.512/ KMK.01/2010 yang mengatur Sanksi Administratif dan

				Sanksi Teknis sesuai PP No.53 tahun 2010 tentang Disiplin Pegawai Negeri Sipil

Lampiran D

D.1 Penilaian Aspek Kepatuhan Area II Risiko

Tabel D.12.0.1 Penilaian Aspek Kepatuhan Area II Risiko

3.1	II	1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN telah memiliki SFO yang mempunyai program kerja pengelolaan risiko dan mitigasi risiko yang terdokumentasi dan secara resmi digunakan (acuan pada PMK.191/PMK.09/2008)
			Bukti	SFO (*strategy focused organization*) mengenai fungsi pembuatan laporan evaluasi pelaksanaan pengelolaan risiko (termasuk di dalamnya dokumen daftar profil risiko) -Identifikasi Risiko Kanwil DJPBN -Analisis Risiko Kanwil DJPBN -Evaluasi Risiko Kanwil DJPBN -Penangana Risiko Kanwil DJPBN **(M-9,M-75, M-76, M-81 dan M-82)**

			Kesesuaian (Ada/Tidak)	Ada
			Tanggal penyesuaian	6 April 2014
3.2	II	1	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN dalam proses penyesuaian berdasarkan PMK.191 / PMK.08/2008 diharuskan membuat kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi digunakan
			Bukti	PMK.191/PMK.08/2008 dan SFO mengenai pelaksanaan pengelolaan risiko (termasuk di dalamnya dokumen pengelolaan risiko) **(M-9, M-75, M-76, M-81, M-82, M-83 dan M-84)**
			Kesesuaian (Ada/Tidak)	Ada
			Tanggal penyesuaian	6 April 2014

3.3	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN dalam proses penyesuaian berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi digunakan mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap performa DJPBN
			Bukti	PMK.191/PMK.08/2008 dan SFO mengenai pelaksanaan pengelolaan risiko (termasuk di dalamnya dokumen pengelolaan risiko) **(M-9, M-75, M-76, M-81, M-82, M-83 dan M-84)**
			Kesesuaian(Ada/Tidak)	Ada

			Tanggal penyesuaian	6 April 2014
3.4	II	1	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN dalam proses penyesuaian berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi digunakan termasuk penetapan ambang batas risiko terhadap performa DJPBN berdasarkan level risiko, level konsekuensi, kategori risiko, level frekuensi dan personal judgement (LR, LK, C, LF) untuk menentukan apakah Fraud, Srategis, Operasional, Compliance&Finansial)
			Bukti	SFO (*strategy focused organization*) mengenai fungsi pembuatan laporan evaluasi pelaksanaan pengelolaan risiko (termasuk di dalamnya dokumen daftar profil risiko) -Identifikasi Risiko Kanwil DJPBN

				-Analisis Risiko Kanwil DJPBN -Evaluasi Risiko Kanwil DJPBN -Penangana Risiko Kanwil DJPBN **(M-9,M-75, M-76, M-81 dan M-82)**
			Kesesuaian (Ada/Tidak)	Ada
			Tanggal penyesuaian	6 April 2014
3.5	II	1	Apakah Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN dalam proses penyesuaian berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang dokumen didalamnya termasuk Tabel Rancangan Pengendalian yang terdokumentasi dan secara resmi digunakan termasuk aset informasi pengendalian yang didalamnya berisi aplikasi pendukung dan dokumen pendukung sebagai aset informasi, pelaksana pengendalian sebagai pengelola dan unsur pengendalian

				lainnya terhadap performa DJPBN berdasarkan jenis kegiatan, keluaran, tujuan dan identifikasinya.
			Bukti	SFO (*strategy focused organization*) mengenai fungsi pembuatan laporan evaluasi pelaksanaan pengelolaan risiko (termasuk di dalamnya dokumen daftar profil risiko) -Identifikasi Risiko Kanwil DJPBN -Analisis Risiko Kanwil DJPBN -Evaluasi Risiko Kanwil DJPBN -Penangana Risiko Kanwil DJPBN -Tabel Rancangan Pengendalian **(M-9,M-46,M-75,M-76,M-81,M-82)**
			Kesesuaian (Ada/Tidak)	Ada
			Catatan	Diterapkan sebagian karena belum dinyatakan pengelolaan keamanan informasi termasuk aset informasi masih dipaparkan secara umum pada prosedur serta penanggung jawabnya belum secara spesifik mengenai pengamanan perangkat keamanan informasi.

	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN dalam proses penyesuaian berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang dokumen didalamnya termasuk Tabel Rancangan Pengendalian yang terdokumentasi dan secara resmi digunakan termasuk aset informasi pengendalian yang didalamnya berisi aplikasi pendukung dan dokumen pendukung sebagai aset informasi, pelaksana pengendalian sebagai pengelola dan unsur pengendalian lainnya terhadap performa DJPBN berdasarkan jenis kegiatan, keluaran, tujuan dan identifikasinya. Namun belum dilakukan pembedaan secara detil tentang aset utama karena seluruh komponen pengendalian masuk dalam kategori aset utama

			Bukti	SFO (*strategy focused organization*) mengenai fungsi pembuatan laporan evaluasi pelaksanaan pengelolaan risiko (termasuk di dalamnya dokumen daftar profil risiko) -Identifikasi Risiko Kanwil DJPBN -Analisis Risiko Kanwil DJPBN -Evaluasi Risiko Kanwil DJPBN -Penangana Risiko Kanwil DJPBN -Tabel Rancangan Pengendalian **(M-9,M-46,M-75,M76,M-81,M-82)**
			Kesesuian (Ada/Tidak)	Ada
			Tanggal penyesuaian	6 April 2014
3.7	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN dalam sebagai unit pelaksana vertical DJPBN telah mengimplementasikan PMK.191/ PMK .08/2008 yang melaksanakan suatu kerangka kerja pengelolaan risiko dimana dokumen didalamnya termasuk analisis risiko aset

				informasi yang dideskripsikan pada Analisis Risiko. Hal ini juga dilakukan dalam rangka menunjang pengimmplementasian KMK.479/ KMK.01/2010 Poin IX terkait Pengendalian Pengelolaan Gangguan Keamanan Informasi
			Bukti	KMK.No.479/KMK.01/2010 SFO (*strategy focused organization*) mengenai fungsi pembuatan laporan evaluasi pelaksanaan pengelolaan risiko (termasuk di dalamnya dokumen daftar profil risiko) -Identifikasi Risiko Kanwil DJPBN -Analisis Risiko Kanwil DJPBN -Evaluasi Risiko Kanwil DJPBN -Penangana Risiko Kanwil DJPBN -Tabel Rancangan Pengendalian **(M-9, M-12, M-46, M-75, M-76, M-81dan M-82)**
			Kesesuian (Ada/ Tidak)	Ada
			Tanggal penyesuaian	6 Mei 2014

3.8	II	1	Apakah Instansi anda sudah menjalankan inisiatif analisis/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	Dalam Penerapan/ Diterapkan Sebagian
			Temuan	KANWIL DJPBN dalam proses penyesuaian berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi digunakan mencakup definisi dan hubungan tingkat klasifikasi risiko, sistem pengendalian, pilihan opsi penanganan dan opsi penanganan terpilih terkait dengan performa DJPBN
			Bukti	KMK.No.479/KMK.01/2010 SFO (*strategy focused organization*) mengenai fungsi pembuatan laporan evaluasi pelaksanaan pengelolaan risiko (termasuk di dalamnya dokumen daftar profil risiko)

				-Identifikasi Risiko Kanwil DJPBN -Analisis Risiko Kanwil DJPBN -Evaluasi Risiko Kanwil DJPBN -Penangana Risiko Kanwil DJPBN -Tabel Rancangan Pengendalian **(M-9, M-12, M-46, M-75, M-76, M-81dan M-82)**
			Kesesuaian (Ada/Tidak)	Ada
			Tanggal penyesuaian	6 April 2014
3.9	II	1	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN dalam proses penyesuaian berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi digunakan mencakup definisi dan hubungan tingkat klasifikasi risiko, sistem pengendalian, pilihan opsi penanganan dan opsi

				penanganan terpilih terkait dengan performa DJPBN
			Bukti	KMK.No.479/KMK.01/2010 SFO (*strategy focused organization*) mengenai fungsi pembuatan laporan evaluasi pelaksanaan pengelolaan risiko (termasuk di dalamnya dokumen daftar profil risiko) -Identifikasi Risiko Kanwil DJPBN -Analisis Risiko Kanwil DJPBN -Evaluasi Risiko Kanwil DJPBN -Penangana Risiko Kanwil DJPBN -Tabel Rancangan Pengendalian **(M-9, M-12, M-46, M-75, M-76, M-81dan M-82)**
			Kesesuaian (Ada/Tidak)	Ada
			Tanggal penyesuaian	6 April 2014

3.10	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas biaya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN dalam proses pelaksanaan berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi digunakan termasuk penetapan ambang batas risiko terhadap performa DJPBN berdasarkan level risiko, level konsekuensi, kategori risiko, level frekuensi dan personal judgement (LR, LK, C, LF) untuk menentukan apakah Fraud, Srategis, Operasional, Compliance&Finansial)
			Bukti	SFO (*strategy focused organization*) mengenai fungsi pembuatan laporan evaluasi pelaksanaan pengelolaan

				risiko (termasuk di dalamnya dokumen daftar profil risiko) -Identifikasi Risiko Kanwil DJPBN -Analisis Risiko Kanwil DJPBN -Evaluasi Risiko Kanwil DJPBN -Penanganan Risiko Kanwil DJPBN **(M-9,M-75, M-76, M-81 dan M-82)**
			Kesesuaian (Ada/Tidak)	Ada
			Tanggal penyesuaian	6 April 20012
			Catatan	Dalam pelaporan terkait risiko dilakukan pula deskripsi konsekuensi risiko, level risiko, dasar pemilihan penanganan dan trend risiko demi menjamin efektifitas pelaksanaan risiko dan mendorong tingkat risiko menuju ke trend yg lebih kecil/lebih rendah
3.11	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Dalam Penerapan / Diterapkan Sebagian

			Temuan	KANWIL DJPBN dalam proses pelaksanaan berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi dilaporkan berkala kepada pimpinan terkait performa DJPBN berdasarkan level risiko, level konsekuensi, kategori risiko, level frekuensi dan personal judgement (LR, LK, C, LF) untuk menentukan apakah Fraud, Srategis, Operasional, Compliance&Finansial)
			Bukti	SFO (*strategy focused organization*) mengenai fungsi pembuatan laporan evaluasi pelaksanaan pengelolaan risiko (termasuk di dalamnya dokumen daftar profil risiko) -Identifikasi Risiko Kanwil DJPBN -Analisis Risiko Kanwil DJPBN -Evaluasi Risiko Kanwil DJPBN -Penanganan Risiko Kanwil DJPBN -LHPPI KPPN Bulan April 2014

				-LPPI Kanwil Triwulan III-2013 **(M-9, M-75, M-76, M-78, M-79, M-81 dan M-82)**
			Kesesuaian (Ada/Tidak)	Ada
			Tanggal penyesuaian	6 April 2014
			Catatan	Seluruh dokumentasi langkah mitigasi risiko dievaluasi secara semesteran pada Eselon II (Kanwil) dan secara Bulanan pada Eselon III demi menjamin efektifitas pengendalian risiko dan mendorong tingkat risiko menuju ke trend yg lebih kecil/lebih rendah
3.12	III	1	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi untuk memastikan konsistensi dan efektifitasnya?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN dalam proses pelaksanaan berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi dilaporkan berkala kepada pimpinan terkait performa DJPBN

				berdasarkan level risiko, level konsekuensi, kategori risiko, level frekuensi dan personal judgement (LR, LK, C, LF) untuk menentukan apakah Fraud, Srategis, Operasional, Compliance & Finansial). Tindakan pembinaan menjadi tanggungjawab pimpinan demi menjamin efektifitas pelaksanaan risiko dan mendorong tingkat risiko menuju ke trend yg lebih kecil/lebih rendah
			Bukti	SFO (*strategy focused organization*) mengenai fungsi pembuatan laporan evaluasi pelaksanaan pengelolaan risiko (termasuk di dalamnya dokumen daftar profil risiko) -Identifikasi Risiko Kanwil DJPBN -Analisis Risiko Kanwil DJPBN -Evaluasi Risiko Kanwil DJPBN -Penanganan Risiko Kanwil DJPBN -LHPPI KPPN Bulan April 2014 -LPPI Kanwil Triwulan III-2013 **(M-9, M-75, M-76, M-78, M-79, M-**

				81 dan M-82)
			Kesesuian (Ada / Tidak)	Ada
			Tanggal penyesuaian	6 April 2014
3.13	IV	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN dalam proses pelaksanaan berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi dilaporkan berkala kepada pimpinan terkait performa DJPBN berdasarkan level risiko, level konsekuensi, kategori risiko, level frekuensi dan personal judgement (LR, LK, C, LF) untuk menentukan apakah Fraud, Srategis, Operasional, Compliance & Finansial). Tindakan

				pembinaan menjadi tanggungjawab pimpinan demi menjamin efektifitas pelaksanaan risiko dan mendorong tingkat risiko menuju ke trend yg lebih kecil/lebih rendah
			Bukti	SFO (*strategy focused organization*) mengenai fungsi pembuatan laporan evaluasi pelaksanaan pengelolaan risiko (termasuk di dalamnya dokumen daftar profil risiko) -Identifikasi Risiko Kanwil DJPBN -Analisis Risiko Kanwil DJPBN -Evaluasi Risiko Kanwil DJPBN -Penanganan Risiko Kanwil DJPBN -LHPPI KPPN Bulan April 2014 -LPPI Kanwil Triwulan III-2013 **(M-9, M-75, M-76, M-78, M-79, M-81 dan M-82)**
			Kesesuaian (Ada/Tidak)	Ada
			Tanggal penyesuaian	6 April 2014
			Catatan	Revisi profil risiko dilakukan secara konsisten dalam semua unit berdasarkan pantauan bulanan

				dalam rangka penyusunan analisis risiko bulan/semester selanjutnya
3.14	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN dalam proses pelaksanaan berdasarkan PMK.191 /PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi dilaporkan berkala kepada pimpinan terkait performa DJPBN berdasarkan level risiko, level konsekuensi, kategori risiko, level frekuensi dan personal judgement (LR, LK, C, LF) untuk menentukan apakah Fraud, Srategis, Operasional, Compliance & Finansial). Tindakan penilaian untuk meningkatkan efektifitas pengendalian risiko dan mendorong tingkat risiko menuju ke trend yg lebih kecil/lebih rendah

				umunya dilakukan dengan memperhatikan dasar pemilihan opsi penanganan dan dilaporkan secara berkala untuk mendapatkan masukan dari kebijakan yang lebih tinggi
			Bukti	SFO (*strategy focused organization*) mengenai fungsi pembuatan laporan evaluasi pelaksanaan pengelolaan risiko (termasuk di dalamnya dokumen daftar profil risiko) -Identifikasi Risiko Kanwil DJPBN -Analisis Risiko Kanwil DJPBN -Evaluasi Risiko Kanwil DJPBN -Penanganan Risiko Kanwil DJPBN -LHPPI KPPN Bulan April 2014 -LPPI Kanwil Triwulan III-2013 **(M-9, M-75, M-76, M-78, M-79, M-81 dan M-82)**
			Kesesuaian (Ada/Tidak)	Ada

			Tanggal penyesuaian	6 April 2014
3.15	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN dalam proses pelaksanaan berdasarkan PMK.191 /PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi dilaporkan berkala kepada pimpinan terkait performa DJPBN berdasarkan level risiko, level konsekuensi, kategori risiko, level frekuensi dan personal judgement (LR, LK, C, LF) untuk menentukan apakah Fraud, Srategis, Operasional, Compliance & Finansial). Tindakan penilaian untuk meningkatkan efektifitas pengendalian risiko dan mendorong tingkat risiko menuju ke trend yg lebih kecil/lebih rendah

				umunya dilakukan dengan memperhatikan dasar pemilihan opsi penanganan dan dilaporkan secara berkala untuk mendapatkan masukan dari kebijakan yang lebih tinggi. Masuknya unsur penilaian persentase laporan mitigasi risiko dan laporan pengendalian internal dalam IKU SKKI memastikan unsur ini dalam indicator kinerja untuk proses bisnis Kanwil DJPBN
			Bukti	SFO (*strategy focused organization*) mengenai fungsi pembuatan laporan evaluasi pelaksanaan pengelolaan risiko (termasuk di dalamnya dokumen daftar profil risiko) -Identifikasi Risiko Kanwil DJPBN -Analisis Risiko Kanwil DJPBN -Evaluasi Risiko Kanwil DJPBN -Penanganan Risiko Kanwil DJPBN

				-LHPPI KPPN Bulan April 2014 -LPPI Kanwil Triwulan III-2013 -IKU SKKI Kanwil DJPBN -Deskripsi IKU Pengendalian Internal **(M-7, M-9, M-75, M-76, M-78, M-79, M-81, M-82 dan M-85)**
			Kesesuaian (Ada/Tidak)	Ada
			Tanggal penyesuaian	6 April 2014
			Catatan	Masuknya laporan pengelolaan risiko dalam penilaian obyektif Indikator Kinerja Utama diharapkan mengefektifkan langkah evalusi dan perbaikan ke depan.

Halaman ini sengaja dikosongkan

Lampiran E

E.1 Penilaian Aspek Kepatuhan Area III - Kerangka Kerja

Tabel E.13.1 Penilaian Aspek Kepatuhan Area III - Kerangka Kerja

4.1	II	1	Apakah kebijakan dan prosedur keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	DJPBN sudah memiliki sejumlah kebijakan terkait pengelolaan keamanan informasi dan telah melaksanakan sejumlah tindakan pengamaanan berdasar kepada KMK.479/KMK.01/2010 tentang kebijakan dan prosedur keamanan informasi namun sejumlah kebijakan (berdasar 11 area) belum semuanya memiliki petunjuk teknis dan prosedur pelaksanaan pengamanan pada tingkat eselon II

			Bukti	KMK. No.479/KMK.01/2010, KMK.No.260/KMK.01/2009 dan Dokumen Kebijakan dan Prosedur keamanan lainnya **(Foto M-12, M-13, M-18, M-23, M-85, M-86, M-87 dan M-88)**
			Tanggal Penyesuaian	28 April 2014
			Catatan	Ruang lingkup Kebijakan serta prosedur masih secara umum belum secara spesifik pada keamanan informasi khususnya implementasi prosedur/ juknis 11 area pengamanan Kanwil DJPBN dari KMK No.479/KMK.01/2010
4.2	II	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	Dalam Penerapan / Diterapkan Sebagian

			Temuan	Kebijakan keamanan informasi telah sebagian ditetapkan secara formal, dipublikasikan kepada pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya
			Bukti	-Gugus Kendali Mutu (GKM) Kanwil sebagai ajang sosialisasi. -Kumpulan Peraturan dan Dokumen Output Kanwil DJPBN di Ruang Kepala Bagian Umum -Link Daftar Peraturan pada Website Sekretariat Jenderal -Link Pustaka pada Website SPAN -Kumpulan peraturan pada web semua unit Kement..Keuangan **(Foto M-14,M-91,M-92 & M-94)**
			Ada / Tidak	Ada
			Tanggal penyesuaian	28 April 2014

			Catatan	Kebijakan pada prosedur organisasi umumnya berbentuk PMK dan KMK yang kesemuanya diakses lewat ftp perbendaharaan yang terbuka pada intranet seluruh kantor. Partisipasi aktif dari pegawai menjadi keharusan dalam mengakses seluruh peraturan. Dalam periode observasi Ruang Arsip sedang diperbaiki
4.3	II	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak KANWIL DJPBN sudah menerapkan serta mengelola dokumen kebijakan dan prosedur dalam proses bisnisnya baik secara online maupun offline. Pengelolaan dokumen sendiri menjadi rencana kerja TU/RT Kanwil DJPBN

			Bukti	-KMK.21/KMK.01/2012 BMN -KMK.479/KMK.01/2010 Poin Kebijakan Pengendalian Dok. -Rencana Kerja Th.2014 TU/RT. -Kumpulan Peraturan dan Dokumen Output Kanwil DJPBN di Ruang Kepala Bagian Umum -Link Daftar Peraturan pada Website Sekretariat Jenderal -Link Pustaka pada Website SPAN -Kumpulan peraturan pada web semua unit Kement..Keuangan **(Foto M-12, M-14, M-91, M-92, M-93, M-94 & M-98)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	28 April 2014
4.4	II	1	Apakah tersedia mekanisme untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian

			Temuan	Pihak bagian KANWIL DJPBN sudah mempunyai mekanisme namun belum secara spesifik mengarah pada keamanan informasi kepada pihak terkait serta pihak ketiga serta masih diatur secara insidentil (maintenance, sosialisasi, rapat dll), belum terdokumentasikan kedalam prosedur tertulis
			Bukti	Pedoman Akses Pihak Ketiga Surat Tugas Maintenace Formulir Permintaan User Akses **(Foto M-74, M-95 dan M-96)**
			Kesesuaian(Ada/Tidak)	Ada, beberapa
			Tanggal Penyesuaian	6 April 2014
4.5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian

			Temuan	DJPBN dalam proses menerapkan prosedur keamanan informasi wajib merefleksikan kebutuhan mitigasi dari kerangka kerja pengelolaan risiko (mis : KMK. 479/KMK.01/2010 Poin VI Pengelolaan Komunikasi dan Operasional merefleksikan pengendalian *scanning* sebelum meng*upload* ADK Bank/Pos Persepsi dalam TRP dan instalasi *antivirus* terupdate pada LHPPI.
			Bukti	-KMK.479/KMK.01/2010 -Tabel Rancangan Pengendalian -Laporan LHPPI Kanwil DJPBN (Foto **M-12, M-46 dan M-79**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	6 April 2014
4.6	II	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset tercantum dalam kontrak dengan pihak ketiga?	Dalam Penerapan/ Diterapkan Sebagian

			Temuan	Pihak DJPBN telah menerapkan sejumlah aspek keamanan informasi seperti pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset sebagaiaman tercantum dalam KMK.479 Poin XI, KMK.512, KMK.351 dan sejumlah peraturan lainnya namun pengimplementasian dalam kontrak pihak ketiga yang dikelola Kanwil masih dilakukan secara informal & belum tertulis.
			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2009 KMK.351/KMK.01/2011 BA (Berita Acara) **(Foto M-12,M-13, M-99, M-100)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	6 April 2014

4.7	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	DJPBN dalam proses menerapkan sebagian sanksi atau konsekuesi pelanggaran kebijakan keamanan informasi berdasarkan perundang-undangan. Belum ditemukan hingga saat ini pelanggaran terkait keamanan informasi namun jika ditemukan dilakukan penerapan Sanksi berdasar KMK 512/KMK.01/2010 poin 5 yakni Sanksi Teknis berupa penonaktifan akses dan Sanksi Administratif sesuai PP 30 th 1980 sebagaimana telah diubah dengan PP 53 Tahun 2010 tentang Peraturan Disiplin Pegawai Negeri Sipil
			Bukti	KMK.512/KMK.01/2010 Poin 5 (Foto **M-13**)

			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	6 April 2014
4.8	II	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi?	Dalam Penerapan/ Diterapkan Sebagian
			Temuan	Tidak disebutkan secara eksplisit prosedur secara resmi dalam pengelolaan pengecualian terhadap penerapan keamanan informasi namun PP.53 tahun 2010 menyebutkan bahwa kebijakannya dilakukan oleh : -Presiden; -Pejabat Pembina Kepegawaian -Gubernur -Kepala Perwakilan Republik Indonesia; dan -Pejabat yang berwenang
			Bukti	KMK.512/KMK.01/2010 PP 53 tahun 2010 **(Foto M-13 dan M-101)**
			Kesesuaian(Ada/Tidak)	Ada

			Tanggal Penyesuaian	6 April 2014
4.9	III	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasitanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	Dalam Penerapan/ Diterapkan Sebagian
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
4.9	III	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	Dalam Perencanaan
			Temuan	Pihak KANWIL DJPBN masih dalam proses menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi security patch, alokasi tanggung jawab, serta rilis security patch baru dan memastikan pemasangan serta pelaporan berdasarkan KMK 479/KMK.01/2010 Poin VIII &X

			Bukti	KMK.479/KMK.01/2010 (Foto **M-12**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	6 April 2014
4.10	III	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Dalam Penerapan / Diterapkan Sebagian
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Dalam Perencanaan

			Temuan	Sistem terbaru yang diimplementasikan dalam lingkup DJPBN adalah SPAN. Namun sebagai sistem dengan tingkat pemenuhan kebutuhan lintas Direktorat maka evaluasi resiko dilakukan oleh Satker SPAN pada Kantor Pusat dengan mitigasi risiko yang tertuang dalam web SPAN yang menjelaskan tentang adanya DRC (Disaster Recovery Centre) SPAN sementara pada lingkup vertical identifikasi risiko terkait SPAN telah dilakukan namun belum ada mitigasi risko secara detil (implementasi SPAN berada pada masa transisi untuk 7 Kanwil & KPPN-KPPN yang diliputinya)
			Bukti	KMK479/KMK01/2010 Poin VIII -Web SPAN tentang DRC -Identifikasi Risiko -Analisis Risiko

				-Evaluasi Risiko (Foto **M-12, M-75, M-76, M-77 dan M-78**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	6 April 2014
4.11	III	2	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?	Dalam Penerapan / Diterapkan Sebagian
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*)	Dalam Perencanaan

			dan jadwal penyelesaiannya?	
			Temuan	KMK479/KMK01/2010 Poin VIII bagian 6 menyatakan kerentanan teknis dengan sejumlah pengamanan dan langkah-langkah jika *patch* tidak tersedia, namun tidak dijabarkan secara terperinci langkah–langkah tersebut dan jadwal penyelesaiannya dan di tingkat vertical belum dibuatkan juknis lebih lanjut. Fakta terkini tentang sistem terbaru yang diimplementasikan dalam lingkup DJPBN adalah SPAN. Untuk sementara pada lingkup vertical identifikasi risiko terkait SPAN telah dilakukan namun belum ada mitigasi risko secara detil berikut waktu penyelesaiannya (implementasi SPAN berada pada masa transisi untuk 7 Kanwil & KPPN-KPPN yang diliputinya)

			Bukti	KMK479/KMK01/2010 Poin VIII -Web SPAN tentang DRC -Identifikasi Risiko -Analisis Risiko -Evaluasi Risiko (Foto **M-12, M-75, M-76, M-77 dan M-78**)
			Kesesuaian (Ada/Tidak)	Ada
			Tanggal kesesuaian	21 April 2014
4.12	III	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan / konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KMK 479/KMK.01/2010 Poin X telah menjelaskan kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan

				/konsideran keamanan informasi, termasuk uji-cobanya dengan focus pada penyusunan rencana kelangsungan kegiatan dan cakupan ujicoba termasuk simulasi, recovery, parallel recovery dan uji perangkat.
			Bukti	KMK 479/KMK.01/2010 KMK.260/KMK.01/2009 **(Foto M-8 dan M-12)**
			Kesesuaian (Ada/Tidak)	Ada
			Tanggal kesesuaian	21 April 2014
4.13	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Dalam Penerapan/ Diterapkan Sebagian

			Temuan	KMK 479/KMK.01/2010 Poin X telah menjelaskan kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan komposisi, peran, wewenang dan tanggung jawab tim dengan focus pada Unit Eselon I dan mencakup identifikasi risiko, identifikasi ase informasi, identifikasi sumber daya, memastikan keselamatan pegawai dan keamanan perangkat, pendokumentasian dan ujicoba secara berkala.
			Bukti	KMK 479/KMK.01/2010 KMK.260/KMK.01/2009 **(Foto M-8 dan M-12)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	20 April 2014

4.14	III	3	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	Dalam Penerapan/ Diterapkan Sebagian
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	Dalam Perencanaan
			Temuan	KMK 479/KMK.01/2010 Poin X telah menjelaskan kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan /konsideran keamanan informasi, termasuk uji-cobanya dengan focus tim keamanan informasi pada eselon I sehingga tidak ditemukan ujicoba pelaksanaan pada Eselon II.

			Bukti	KMK 479/KMK.01/2010 KMK.260/KMK.01/2009 **(Foto M-8 dan M-12)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	20 April 2014
4.15	IV	3	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	Dalam Penerapan/ Diterapkan Sebagian
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	Dalam Perencanaan

			Temuan	KMK 479/KMK.01/2010 Poin X telah menjelaskan kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mengharuskan analisis dampak kegiatan melibatkan pemilik proses bisnis dan dievaluasi secara berkala untuk memastikan efektifitasnya.Hal yang ditemui dalam observasi adalah focus tim keamanan informasi pada eselon I sehingga tidak ditemukan prosedur ujicoba berikut pembenahan pada Eselon II (Kanwil DJPBN Jawa Timur).
			Bukti	KMK 479/KMK.01/2010 KMK.260/KMK.01/2009 **(Foto M-8 dan M-12)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	20 April 2014

4.16	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	DJPBN telah menerapkan evaluasi seluruh kebijakan dan prosedur yang dilaksanakan sepenuhnya oleh Bagian Organisasi dan Tata Laksana dan untuk Kanwil DJPBN dilaksanakan oleh SKKI melalui LPPPI triwulanan yang merupakan gabungan seluruh laporan pengendalian internal KPPN. Namun belum ada penspesifikasian khusus terkait dengan keamanan informasi karena pengelolaan keamanan informasi dilaporkan sebgai bagian dari proses bisnis organisasi
			Bukti	PMK 184/PMK.01/2010 LPPPI Tw.3 Kanwil DJPBN LPPI Semester II KPPN
			Kesesuaian(Ada/Tidak)	Ada

			Tanggal Penyesuaian	20 April 2014
4.17	II	1	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisis risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Tingkatan kebijakan strategis dalam DJPBN umunya dituangkan dalam bentuk PP, PMK, KMK, KM dan peraturan yang setingkat. Esensi peraturan - peraturan tersebut adalah kebijakan dan standar yang menjadi bagan dari rencana kerja organisasi. Keseluruhan peraturan juga merupakan hasil analisis risiko dari sejumlah penerapan keamanan informasi yang masuk dalam lingkup TIK sebagai bagian penting dalam proses bisnis dan rencana kerja organisasi sehingga selalu memunculkan langkah pengendalian dan evaluasi berkala dalam tiap kebijakan yang ada.

			Bukti	KMK No.479/KMK.01/2010 KMK No.260/KMK.01/2009 KMK No.512/KMK.01/2010 KMK. No.350/KMK.01/2010 Prosedur-prosedur terkait dll (Foto **M-8, M-12,M-13 & M-15**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	20 April 2014
4.18	II	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Tingkatan kebijakan strategis dalam DJPBN umunya dituangkan dalam bentuk PP, PMK, KMK, KM dan peraturan yang setingkat. Esensi peraturan - peraturan tersebut adalah kebijakan dan standar yang menjadi bagan dari rencana kerja organisasi. Keseluruhan peraturan juga merupakan hasil analisis risiko

				sebagai konsekuensi logis dari kebutuhan dan perubahan profil risiko dari sejumlah penerapan keamanan informasi yang masuk dalam lingkup TIK sebagai bagian penting dalam proses bisnis dan rencana kerja organisasi sehingga selalu memunculkan langkah pengendalian dan evaluasi berkala dalam tiap kebijakan yang ada.
			Bukti	KMK No.479/KMK.01/2010 KMK No.260/KMK.01/2009 KMK No.512/KMK.01/2010 KMK. No.350/KMK.01/2010 Prosedur-prosedur terkait dll (Foto **M-8, M-12,M-13 & M-15**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	20 April 2014
4.19	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Dalam Penerapan/ Diterapkan Sebagian

			Temuan	Sebagaimana KMK dan PMK yang telah disampaikan sebelumnya. TIK juga menjadi sasaran strategis seluruh unit vertical DJPBN tentang Pemanfaatan TIK secara optimal. Disamping itu Rencana Strategis Kementerian Keuangan juga menyatakan perlunya kebijakan-kebijakan, standar, dan prosedur berkaitan dengan operasionalisasi teknologi informasi dan komunikasi seperti yang terkait dengan tata kelola yang baik (good IT governance),pengelolaan layanan (IT service management), pengelolaan kesinambungan bisnis (business continuity management) beserta seluruh kelengkapan seperti Disaster Recover Plan dan Disaster Recover Center, **keamanan sistem informasi** (IT security

				management), dan pengelolaan sumber daya informasi (termasuk yang berkaitan dengan masalah lisensi software) sebagai bagian dari pelaksanaan program kerja organisasi
			Bukti	Renstra Poin D TI Keuangan KMK.479/KMK.01/2010 LHPPPI (Sasaran UPR) (Foto **M-12, M-78 dan M-80**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	20 April 2014
4.20	III	2	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	Dalam Penerapan / Diterapkan Sebagian

			Temuan	Pelaksanaan audit internal lingkup DJPBN dilaksanakan oleh Inspektorat Jenderal berdasar Standar Audit Inspektorat Jenderal (SAINS). Cakupannya adalah seluruh aset, kebijakan, prosedur dan pelaksanaan. KANWIL DJPBN sendiri memiliki dan melaksanakan program audit internal yang dikenal dengan istilah pengendalian internal yang dilakukan oleh SKKI sebagai pihak independen dengan cakupan kepatuhan pelaksanaan kebijakan dan prosedur secara berkala
			Bukti	PMK.59/PMK.09/2010 Poin I.2 KMK.152/KMK.09/2011 KMK.296/KMK.09/2010 Kepdirjen No.85/PB/2012

				(Foto **M-103, M-104, M-105, dan M-106**)
			Kesesuaian (Ada/Tidak)	Ada
			Tanggal kesesuaian	21 April 2014
4.21	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?	Dalam Perencanaan
			Temuan	DJPBN sebagai pelaksana renstra kementerian keuangan telah merencanakan pengendalian internal untuk mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi yang diawali dengan

				pelaksanaan tes online keamanan informasi yang diselenggarakan melalui media website SPAN. Kedepan pengendalian keamanan informasi tercakup dalam bentuk pengendalian internal sambil menunggu juga audit keamanan informasi oleh Itjen yang menjadi program Kominfo pada seluruh Kementerian/Lembaga
			Bukti	LHPPI Kanwil Tw.3 LHPPI KPPN Semester I Tes Online Keamanan Informasi (Foto **M-21,M-22,M-78 & M-79**)
			Kesesuaian (Ada/Tidak)	Ada
			Tanggal kesesuaian	21 April 2014

4.22	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Dalam Perencanaan
			Temuan	DJPBN sebagai pelaksana renstra kementerian keuangan telah merencanakan pengendalian internal untuk mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi yang diawali dengan pelaksanaan tes online keamanan informasi yang diselenggarakan

				melalui media website SPAN. Kedepan pengendalian keamanan informasi tercakup dalam bentuk pengendalian internal sambil menunggu juga audit keamanan informasi oleh Itjen yang menjadi program Kominfo pada seluruh Kementerian/Lembaga
			Bukti	LHPPI Kanwil Tw.3 LHPPI KPPN Semester I Tes Online Keamanan Informasi (Foto **M-21,M-22,M-78 & M-79**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	20 April 2014
			Catatan	Pengendalian ataupun audit internal belum mengarah terlalu spesifik pada keamanan informasi, kontrol yang dibuat hanya berdasarkan proses bisnis yang ada seperti komplain atau layanan operasional seperti *backup data*

4.23	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Dalam Perencanaan
			Temuan	DJPBN sebagai pelaksana renstra kementerian keuangan telah merencanakan pengendalian internal untuk mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi yang diawali dengan pelaksanaan tes online keamanan informasi yang diselenggarakan melalui media website SPAN. Kedepan pengendalian keamanan

				informasi tercakup dalam bentuk pengendalian internal sambil menunggu juga audit keamanan informasi oleh Itjen yang menjadi program Kominfo pada seluruh Kementerian/Lembaga
			Bukti	LHPPI Kanwil Tw.3 LHPPI KPPN Semester I Tes Online Keamanan Informasi (Foto **M-21,M-22,M-78 & M-79**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	20 April 2014
			Catatan	Audit internal secara berkala akan dilaporkan kepada pimpinan seperti yang terdokumentasikan pada Kepdirjen.85/PB/2010, namun laporan secara resmi sebagai evaluasi audit khusus keamaann informasi memang masih perencanaan.

4.24	IV	3	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisis untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Dalam Penerapan / Diterapkan Sebagian
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisis untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Dalam Perencanaan

			Temuan	DJPBN dalam menetapkan suatu kebijakan dan prosedur pasti melakukan analisis untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya. SPAN sebagai wujud pengimplementasian perubahan dan struktur penganggran dan perbendaharaan sendiri ditunjang oleh kebijakan khusus dan infrastruiktur yang diatur tersendiri dan terpisah dari infrastruktur yang dimilki unit vertical DJPBN
			Bukti	PMK tentang Piloting SPAN Infrastruktur SPAN dengan Logo Perangkat SPAN di unit vertikal **(Foto M-40, M-107, Dan M-108)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	20 April 2014

			Catatan	Pada pemutakhiran kebijakan dan prosedur serta rencana strategis, focus utama adalah pada analisis kondisi eksisting dan perbaikan seluruh proses bisnis dengan ditunjang efisiensi anggaran dan infrastruktur Kementerian
4.25	V	3	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada untuk memastikan bahwa keseluruhan inisiatif tersebut telah diterapkan secara efektif?	Dalam Penerapan / Diterapkan Sebagian
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada untuk memastikan bahwa keseluruhan inisiatif tersebut telah diterapkan secara efektif?	Dalam Perencanaan

			Temuan	DJPBN sebagai pelaksana renstra kementerian keuangan telah merencanakan pengendalian internal untuk mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi yang diawali dengan pelaksanaan tes online keamanan informasi yang diselenggarakan melalui media website SPAN. Kedepan evaluasi keamanan informasi tercakup dalam bentuk pengendalian internal sambil menunggu juga audit kepatuhan keamanan informasi oleh Itjen yang menjadi program Kominfo pada seluruh Kementerian/Lembaga
			Bukti	LHPPI Kanwil Tw.3 LHPPI KPPN Semester I

				Tes Online Keamanan Informasi (Foto **M-21,M-22,M-78 & M-79**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	20 April 2014
4.26	V	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah / panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Dalam Penerapan / Diterapkan Sebagian
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah / panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Dalam Perencanaan

			Temuan	DJPBN sebagai pelaksana renstra kementerian keuangan telah merencanakan peningkatan keamanan dan evaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi yang diawali dengan pelaksanaan tes online keamanan informasi yang diselenggarakan melalui media website SPAN. Kedepan peningkatan keamanan informasi tercakup dalam bentuk strategis unit vertical melaui pembentukan tim keamanan informasi pada seluruh Kementerian / Lembaga
			Bukti	Renstra Poin D TI Keuangan KMK.479/KMK.01/2010 LHPPPI (Sasaran UPR) Test Online Keamanan Informasi (Foto **M-12, M-22, M-78 dan M-**

				80)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	20 April 2014
			Catatan	Program peningkatan keamanan informasi di sini rencananya dilkukan pada semua bidang termasuk peningkatan kompetensi SDM, manajerial dan teknikal. Pada kondisi sekarang KANWIL DJPBN melandaskan kegiatannya pada KMK No.479/KMK.01/2010 sehingga program peningkatan secara umum diharapkam dijabarkan dalam dokumen kebijakan organisasi vertical secara spesifik pada semua bidang

Lampiran F

F.1 Penilaian Aspek Kepatuhan Area IV - Pengelolaan Aset

Tabel F.14.1 Penilaian Aspek Kepatuhan Area IV - Pengelolaan Aset

5.1	II	1	Apakah tersedia daftar inventaris aset informasi yang lengkap dan akurat?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN telah menerapkan daftar aset informasi berupa Dokumen, Data, Hardware, Software dan Jaringan namun selain BMN (Barang Milik Negara) beerapa belum terbentuk dalam detail daftar inventaris aset informasi
			Bukti	Daftar Aset SIMAK BMN DIR (Daftar Inventaris Ruangan) (**Foto M-25 dan M-65**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
5.2	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?	Dalam Penerapan / Diterapkan Sebagian

			Temuan	KANWIL DJPBN telah menerapkan proses evaluasi dan klasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi termasuk alokasi pengguna perbidang dan seksi serta keperluan pengamanannya hanya saja masih terbatas kepada alokasi Hardware, Software dan Jaringan dan belum terbentuk dalam detail SOP pengamanan aset informasi
			Bukti	Daftar Aset (SIMAK BMN), DIR, dan Rincian Target Capaian Kinerja (Persentase Pemenuhan Sarana TIK) KMK.479/KMK.01/2010 Poin III (**Foto M-11, M-12, M-25 dan M-65**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
5.3	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dan matrix yang merekam alokasi akses tersebut	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN telah mendefinisikan tingkatan akses yang berbeda terutama dalam penggunaan aplikasi seuai dengan tingkat kewenangan untuk perekaman alokasi akses

				hanya terdapat di beberapa bagian tertentu tergantung tingkat kerahasiaan dan nilai aset informasi yang dituju
			Bukti	KMK.512/KMK.01/2009. Tingkat kewenangan aplikasi SPAN Hak Akses user (Aplikasi SPAN membagi user dan password dalam tingkat akses ttu) Kartu dan Buku Tamu **(Foto M-13, M-19, M-20, M-44, M-57, M-58, M-67 dan M-68)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
			Catatan	KANWIL DJPBN mempunyai matrik rekaman alokasi akses, namun secara umum akses di KANWIL DJPBN khususnya SPAN hanya menampilkan user pengguna. Tidak ada dalam list log user aktif di dalamnya. Alokasi akses antara lain user berbeda pada tiap hierarki dan sistem perangkat keamanan misal sidik jari, face recognition, kartu tamu dll Karena alasan privacy maka alokasi akses userdan password dimohon tidak ditampilkan

5.4	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	Dalam Penerapan /Diterapkan Sebagian
			Temuan	Karena pelaksanaan perubahan konfigurasi terbilang minim, maka implementasi masih menyesuaikan dengan KMK terkait untuk pelaksanaanya dan proses pengelolaan terhadap perubahan yang diterapkan secara formil di Kantor Pusat masih secara informal dilakukan di Kantor Wilayah DJPBN
			Bukti	Ip Configuration intranet DJPBN IP Configuration SPAN Penggantian akses user Kepala Seksi, Penggantian akses user Pelaksana (Foto **M-10, M-29, M-109 dan M-110**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

			Catatan	Prosedur konfigurasi untuk sementara ini masih belum ada, secara umum masih terbentuk dalam prosedur umum tindakan pengelolaan aset baik \yang terkait dengan BMN maupun teknologi. Pihak KANWIL DJPBN umumnya melakukan konfigurasi secara spontan tanpa panduan tertulis/ prosedur yang rinci pada aset-aset informasi ini. Terkait dengan SPAN seluruh konfigurasi tercatat pada sistem log terpusat.
5.5	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Dalam penerapan/ Diterapkan Sebagian
			Temuan	Karena pelaksanaan perubahan konfigurasi terbilang minim, maka implementasi masih menyesuaikan dengan KMK terkait untuk pelaksanaanya dan proses pengelolaan terhadap perubahan yang diterapkan secara formil di Kantor Pusat masih secara informal dilakukan di Kantor Wilayah DJPBN

			Bukti	Ip Configuration intranet DJPBN IP Configuration SPAN Penggantian akses user Kepala Seksi, Penggantian akses user Pelaksana (Foto **M-10, M-29, M-109 dan M-110**)
			Kesesuaian(Ada/Tidak)	Ada, beberapa
			Tanggal Penyesuaian	21 April 2014
			Catatan	Prosedur konfigurasi untuk sementara ini masih belum ada, secara umum masih terbentuk dalam prosedur umum tindakan pengelolaan aset baik \yang terkait dengan BMN maupun teknologi. Pihak KANWIL DJPBN umumnya melakukan konfigurasi secara spontan tanpa panduan tertulis/ prosedur yang rinci pada aset-aset informasi ini. Terkait dengan SPAN seluruh konfigurasi tercatat pada sistem log terpusat.
5.6	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Dalam Penerapan / Diterapkan Sebagian

			Temuan	Di KANWIL DJPBN telah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi. Untuk BMN maka pelaksanaanya dilakukan melalui aplikasi SIMAK BMN (Barang Milik Negara) dan akses pengguna dilaksanakan lewat pendaftaran melalui email Kementerian Keuangan ke Pusintek
			Bukti	Dokumen Berita Acara Serah Terima Berita Acara Penyerahan Barang SIMAK BMN Formulir Permintaan Akses User (Foto **M-65, M-100, M-109, M-110, M-111**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
			Catatan	Kondisi saat ini di KANWIL DJPBN telah mempunyai proses rilis aset, namun SOP belum sepenuhnya terbentuk. Umumnya pihak pelaksana secara otomatis memahami prosedur konvensi (belum tertulis) dalam melakukan sejumlah prasyarat pengaksesan ke sistem/aplikasi/aset terbaru

5.7	II	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak KANWIL DJPBN dalam proses untuk menerapkan definisi tanggung jawab pengamanan informasi secara individual untuk semua personil dengan pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Terdapat pula Larangan dan Sanksi sebagai control tiap individu.
			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2009 KMK.274/KMK.01/2010 KMK.350/KMK.01/2010 **(Foto M-12, M-13, M-18 dan M-113)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
5.8	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	Dalam Penerapan / Diterapkan Sebagian

			Temuan	Pihak KANWIL DJPBN telah menerapkan tata tertib penggunaan komputer, email, internet dan intranet melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Terdapat pula Larangan dan Sanksi sebagai control tiap individu
			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2009 KMK.274/KMK.01/2010 KMK.350/KMK.01/2010 **(Foto M-12, M-13, M-18 dan M-113)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
5.9	II	1	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin XI tentang HAKI

			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2009 KMK.274/KMK.01/2010 KMK.350/KMK.01/2010 **(Foto M-12, M-13, M-18 dan M-113)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
			Catatan	Untuk beberapa pengimplementasian belum terbentuknya prosedur detail dan hanya melaksanakan beberapa ketentuan terkait pengembangan sistem informasi dengan mendasarkan pada KMK.351/KMK.01/2011 dengan mematuhi HAKI sebagaimana diatur kemudian dalam KMK.479/KMK.01/2010
5.10	II	1	Peraturan pengamanan data pribadi	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin III & VI tentang aset & akses

			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2009 KMK.274/KMK.01/2010 KMK.350/KMK.01/2010 **(Foto M-12, M-13, M-18 dan M-113)**
			Kesesuaian(Ada/Tidak)	Ada, beberapa
			Tanggal Penyesuaian	21 April 2014
			Catatan	Secara umum, pihak KANWIL DJPBN melaksanakan himbauan secara menyeluruh keamanan pada semua file pribadi misal penggunaan enkripsi, penyimpanan data-data pada folder, dan lainnya namun belum mendokumentasikan prosedur dan himbauan tersebut secara tertulis.
5.11	II	1	Pengelolaan identitas elektronik dan proses otentikasi (*username & password*) termasuk kebijakan terhadap pelanggarannya	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/

				2010 Poin VII tentang Akses dan KMK.512 /KMK.01/2009 tentang Kebijakan dan Penggunaan Akun dan Kata Sandi Pengguna yang diikuti pula oleh Larangan dan Sanksi
			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2009 KMK.274/KMK.01/2010 KMK.350/KMK.01/2010 **(Foto M-12, M-13, M-18 dan M-113)**
			Kesesuaian(Ada/Tidak)	Ada, beberapa
			Tanggal Penyesuaian	21 April 2014
5.12	II	1	Persyaratan dan prosedur pengelolaan/ pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin VII tentang Pengendalian Akses dan Poin III tentang Aset Informasi

			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2009 KMK.274/KMK.01/2010 KMK.350/KMK.01/2010 **(Foto M-12, M-13, M-18 dan M-113)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
5.13	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin VI tentang media penyimpanan dan KMK.350/KMK.01/2010 Poin 5.5 tentang media Penyimpanan Data dan 5.5.3 ttg Penghancuran Media Penyimpanan Data

			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2009 KMK.274/KMK.01/2010 KMK.350/KMK.01/2010 **(Foto M-12, M-13, M-18 dan M-113)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
5.14	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin VI bagian 8 tentang pertukaran informasi dan KMK.274/KMK.01/2010 pada bag 5.2 Aplikasi Pertukaran Data Elektronik
			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2009 KMK.274/KMK.01/2010 KMK.350/KMK.01/2010

				(Foto M-12, M-13, M-18 dan M-113)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
5.15	II	1	Proses penyidikan / investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin IX tentang gangguan keamanan informasi dan GKN sendiri memilki SOP tentang penyelesaian gangguan layanan TIK
			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2009 KMK.274/KMK.01/2010 KMK.350/KMK.01/2010 SOP Pemulihan Layanan TIK SOP Penyelesaian Gangguan Layanan TIK SOP Penerapan Keamanan Informasi **(Foto M-12, M-13, M-18, M-86, M-87, M-**

				89 dan M-113)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
5.16	II	1	Prosedur *back-up* ujicoba pengembalian data (*restore*)	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin XI bag C.5 tentang Back-up dan KMK.350/KMK.01/2010 Poin 4.3.3 tentang Ketersediaan Data (*Availability*)
			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2009 KMK.274/KMK.01/2010 KMK.350/KMK.01/2010 **(Foto M-12, M-13, M-18 dan M-113)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

			Catatan	Back up data selalu dilakukan sebagai konvensi pengelola data. Belum adanya pemutakhiran prosedur back-up yang up to date lingkup Kanwil DJPBN
5.17	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin V tentang pengamaan fisik dan lingkungan khususnya akses ke aset informasi yang memiliki klasifikasi RAHASIA dan SANGAT RAHASIA
			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2009 KMK.274/KMK.01/2010 KMK.350/KMK.01/2010 **(Foto M-12, M-13, M-18 dan M-113)**
			Kesesuaian(Ada/Tidak)	Ada

			Tanggal Penyesuaian	21 April 2014
			Catatan	Pengamanan fisik belum diturunkan SOP detail untuk klasifikasi zona masing-masing seperti kritikal, sedang, ringan sesuai dengan pengelolaan risiko
5.18	III	2	Proses pengecekan latar belakang SDM	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin IV tentang SDM yang memiliki standar pengecekan latar belakang SDM dengan mengecek referensi hubungan kerja, kualifikasi akademik dan lain-lain.
			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2009 KMK.274/KMK.01/2010 KMK.350/KMK.01/2010 **(Foto M-12, M-13, M-18 dan M-113)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

			Catatan	Prosedur atau alur yang yang tertulis mengenai pengecekan latar belakang SDM adalah lingkup Kantor Pusat DJPBN
5.19	III	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin IX tentang gangguan keamanan informasi dan GKN sendiri memilki SOP tentang penyelesaian gangguan layanan TIK
			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2009 KMK.274/KMK.01/2010 KMK.350/KMK.01/2010 SOP Pemulihan Layanan TIK SOP Penyelesaian Gangguan Layanan TIK SOP Penerapan Keamanan Informasi **(Foto M-12, M-13, M-18, M-86, M-87, M-**

				89 dan M-113)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
			Catatan	KANWIL DJPBN sebagai pengguna GKN Surabaya I melakukan pelaporan insiden pada KPTIK GKN lisan dan tertulis secara informal, pada umumnya belum tersedia prosedur mengenai pelaporan terjadinya insiden keamanan informasi Kanwil, namun penanganan insiden secara umum sudah diatur pada SOP GKN Surabaya I
5.20	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin VI tentang media penyimpanan dan KMK.350/KMK.01/2010 Poin 5.5 tentang media Penyimpanan Data dan 5.5.3 ttg Penghancuran Media Penyimpanan Data

			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2009 KMK.274/KMK.01/2010 KMK.350/KMK.01/2010 **(Foto M-12, M-13, M-18 dan M-113)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
5.21	III	2	Prosedur kajian penggunaan akses (*user access review*) dan langkah pembenahan apabila terjadi ketidak sesuaian (*non-conformity*) terhadap kebijakan yang berlaku.	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin VII tentang Pengendalian Akses dan Poin III tentang Aset Informasi. KMK. 512/KMK.01/2010 sendiri mengatur bahwa pelanggran terhadap kebijakan dibenahi dengan pemberian sanksi teknis/administratif

			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2009 KMK.274/KMK.01/2010 KMK.350/KMK.01/2010 **(Foto M-12, M-13, M-18 dan M-113)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
5.22	III	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisis kepatuhan terhadap prosedur *backup*-nya?	Dalam Penerapan / Diterapkan Sebagian
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisis kepatuhan terhadap prosedur *backup*-nya?	Dalam Perencanaan
			Temuan	Saat ini seluruh data terkait Keuangan Negara tercatat lengkap dan di-*backup* secara berkala sebagai bentuk penerapan KMK.479 /KMK.01/2010 Poin VI bagian C.5 tentang *backup* dan KMK.350/KMK.01/2010 pada bag 5.3 yang menerapkan metode *system backup*, *full backup* dan *incremental backup* yang mendasarkan pelaksanaan *backup*

				berdasarkan tingkat kritikalitas data, namun untuk poin laporan analisis kepatuhan terhadap prosedur *backup* masih dalam perencanaan
			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2009 KMK.274/KMK.01/2010 KMK.350/KMK.01/2010 **(Foto M-12, M-13, M-18 dan M-113)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
5.23	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Saat ini pelaksanaan keamanan informasi menjadi bagian yang utuh dari proses bisnis dan evaluasi pelaksanaan diwujudkan dalam pengendalian internal yang dilakukan berkala Dalam pada itu, KANWIL DJPBN telah mempunyai daftar rekaman pelaksanaan pengendalian namun terbentuk secara

				terpisah (misal : manajemen komunikasi operasi berupa update antivirus dlm LPPI; pengendalian akses melaui form permintaan akun, perubahan akses user; pengelolaan insiden melalui laporan koordinasi pemulihan permasalahan) dan bentuk-bentuk pengamanan yang sesuai dengan tingkat kritikalitas data dan klasifikasinya
			Bukti	LPPI Kanwil Triwulan.3 Form Perminitaan Akun Laporan Koordinasi Pemulihan Layanan **(Foto M-79, M-96 dan M-114)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
5.24	III	3	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?	Dalam Penerapan / Diterapkan Sebagian

			Temuan	Di KANWIL DJPBN umumnya kebijakan\ prosedur penggunaan perangkat pengolah informasi mengikuti KMK.479/KMK.01/ 2010 baik itu untuk perangkat kantor atau milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dan terkait dengan memastikan aspek HAKI dan pengamanan akses yang digunakan dilaksankan melalui perjanjian lisensi, kepemilikan source code dan HAKI yang diatur dalam Poin 8 bag 5.d
			Bukti	LPPI Kanwil Triwulan.3 Form Perminitaan Akun Laporan Koordinasi Pemulihan Layanan **(Foto M-79, M-96 dan M-114)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

5.25	II	1	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?	Diterapkan Secara Menyeluruh
			Temuan	KANWIL DJPBN dalam proses menerapkan secara menyeluruh pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang
			Bukti	Foto kartu tamu, buku tamu. Fingerprint, face recognition, satpam, cctv, foto ruang arsip data, foto fire extinguisher, foto pendeteksi asap **(Foto M-27, M-49, M-51, M-52, M-67, M-68, M-115, M-116, M-117 dan M-118)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

5.26	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Diterapkan Secara Menyeluruh
			Temuan	Di KANWIL DJPBN sedang dalam proses penerapan penuh pengelolaan alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik
			Bukti	Foto kartu tamu, buku tamu. Fingerprint, face recognition, satpam, cctv, foto kunci akses server depan, foto kunci akses server belakang. **(Foto M-51, M-52, M-54, M-55, M-67, M-68, M-70)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
			Catatan	Di KANWIL DJPBN khususnya akses ke ruang dengan tingkat kritikalitas tinggi sudah mempunyai pengelolaan kunci ruang (fisik dan elektronik). Namun memang secara utuh belum terlihat report aktivitas lengkap dan masih disiapkan log aktivitas lengkap untuk aset fisik sebagai pelengkap pengamanan.

5.27	II	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	Diterapkan Secara Menyeluruh
			Temuan	DI KANWIL DJPBN secara menyeluruh sudah mempunyai infrastruktur komputasi yang terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya
			Bukti	Foto Hasil Cek Lingkungan Perangkat (berdasar ketentuan pengamanan perangkat dalam KMK.479/KMK.01/2010), Foto Smoke Detector, Foto Fire Extinguisher **(Foto M-49, M-59, M-117, dan M-118)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

5.28	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Diterapkan Secara Menyeluruh
			Temuan	KANWIL DJPBN secara menyeluruh memastikan infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir
			Bukti	Daya terpasang saat ini GKN 2250 KVA Foto ruang genset, Foto Saklar Ruangan **(Foto F-48, M-119)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
5.29	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN menstandarkan peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor) pada Poin V

				Pengendalian Fisik dan Lingkungan bag.e yang menjelaskan perangkat yang digunakan di luar lingkungan Kementerian Keuangan harus disetujui oleh Pihak Yang Berwenang dan ketentuan lainnya dalam Pedoman Pengamanan Perangkat
			Bukti	KMK.479/KMK.01/2010 Pedoman Pengaman Perangkat (Foto M-12, M-98)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

5.30	II	2	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	Diterapkan Secara Menyeluruh

			Temuan	KANWIL DJPBN menyiapkan secara penuh konstruksi ruang penyimpanan perangkat pengolah informasi penting dengan menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai
			Bukti	KIB Gedung Keuangan Negara I Fire Extinguisher, Hydrant, Smoke Detector, Indikator Suhu, Cek Lingkungan Perangkat, **(Foto F-49, M-50, M-59, M-60, M-117, M-118, M-121 dan M-122)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

5.31	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Diterapkan Secara Menyeluruh
			Temuan	KANWIL DJPBN telah mempunyai beberapa proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting
			Bukti	Juknis Pengelolaan S-9339, Foto pelaksanaan maintenance, Foto cek perangkat dan lingkungan perangkat, SOP Pengelolaan Jaringan dan Infratruktur, ST Maintenance perangkat, Laporan Koordinasi gangguan layanan TIK, SOP-SOP lainnya. **(Foto M-5, M-56, M-59, M-86, M-87, M-88, M-89, M-90, M-95 dan M-114)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

5.32	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Diterapkan Secara Menyeluruh
			Temuan	Di KANWIL DJPBN telah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga dimana pengiriman dilengkapi dengan Surat Pengantar dan Surat Tugas dari Instansi /Organisasi yang memberi tugas pengiriman barang dan /atau Surat Tugas Pemuatan Barang dari dalam lingkungan gedung dan/atau bangunan. Khusus Dokumen dilengkapi pula dengan Sistem 4 Amplop
			Bukti	KMK. NOMOR 21/KMK.01/2012 Tentang PEDOMAN PENGAMANAN BARANG MILIK NEGARA DI LINGKUNGAN KEMENTERIAN KEUANGAN **(Foto M-123)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

5.33	II	2	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)	Dalam Penerapan / Diterapkan Sebagian
			Temuan	DI KANWIL DJPBN telah tersedia beberapa peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi dengan mendasar kepada KMK.479/KMK.01/2010 Poin VI dimana menjelaskan perlunya pengamanan fisik yang memadai melalui penggunaan pintu elektronik, sistem pemadam, alarm dan aksesibilitas ke ruang dengan klasifikasi RAHASIA hanya diberikan kepada pegawai yang berwenang, dll

			Bukti	KMK 479/KMK.01/2010 Buku Tamu untukIzin kepada KPTIK Surat Tugas Maintenance Server **(Foto M-12, M-68 dan M-95)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
5.34	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?	Diterapkan Secara Menyeluruh
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Di KANWIL DJPBN telah mempunyai proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi dimana pihak ketiga yang memasuki ruang server,

				pusat data, dan area kerja yang berisikan aset informasi yang RAHASIA harus didampingi pegawai unit TIK sepanjang waktu kunjungan. Waktu keluar masuk serta maksud kedatangan harus dicatat dalam buku catatan kunjungan (KMK.479/KMK01/2010)
			Bukti	KMK 479/KMK.01/2010 Buku Tamu untuk Izin kepada KPTIK Maksud dan Tujuan Kunjungan KPTIK Surat Tugas Maintenance Server **(Foto M-12, M-68, M-124 dan M-95)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

Halaman ini sengaja dikosongkan

Lampiran G

G.1 Penilaian Aspek Kepatuhan Area V - Teknologi

Tabel G.15.1 Penilaian Aspek Kepatuhan Area V - Teknologi

6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Di KANWIL DJPBN telah menerapkan layanan TIK (sistem komputer) yang menggunakan internet untuk dilindungi dengan lebih dari 1 lapis pengamanan (proxy dan firewall)
			Bukti	Screenshot proxy (Firewall dikelola Pusintek, belum ada keterangan dari KPTIK) **(Foto M-61 dan M-62)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?	Diterapkan Secara Menyeluruh

			Temuan	KANWIL DJPBN secara menyeluruh telah tersedia jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)
			Bukti	Foto Kewenangan Akses User SPAN, Foto Kewenangan Akses pada Revisi DIPA CW, Penggantian Akses User Seksi/Pelaksana (**M-19, M-20, M-109, M-110**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
			Catatan	Pembagian kewenangan ini berguna untuk mengakses jaringan SPAN untuk semua aplikasi internal DJPBN dengan peruntukan pada masing-masing seksi dan petugas.
6.3	II	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset komputer dan perangkat jaringan, yang dimutakhirkan sesuai perkembangan dan kebutuhan?	Diterapkan Secara Menyeluruh

			Temuan	KANWIL DJPBN secara menyeluruh telah mempunyai konfigurasi standar untuk keamanan sistem bagi keseluruhan aset komputer dan perangkat jaringan, yang dimutakhirkan sesuai perkembangan dan kebutuhan terutama untuk SPAN yang melakukan pembatasan akses IP (*banned Ipconfig*)
			Bukti	Dokumen Juknis, Akses User dan Password SPAN, Modul Panduan Keamanan Tenologi Informasi, Ipconfig SPAN, Ipconfig Intranet (**M-5, M-10, M-19, M-29**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
6.4	II	1	Apakah Instansi anda secara rutin menganalisis kepatuhan penerapan konfigurasi standar yang ada?	Diterapkan Secara Menyeluruh
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	

			Apakah Instansi anda secara rutin menganalisis kepatuhan penerapan konfigurasi standar yang ada?	Dalam Penerapan/ Diterapkan Sebagian
			Temuan	KANWIL DJPBN telah menerapkan secara rutin analisis kepatuhan penerapan konfigurasi standar yang ada di beberapa perangkat TIK
			Bukti	Hasil cek *network configuration* (Foto **M-53**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
6.5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Diterapkan Secara Menyeluruh
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Dalam Penerapan/ Diterapkan Sebagian

			Temuan	Jaringan, sistem dan aplikasi yang digunakan di KANWIL DJPBN dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi melalui pengecekan pada network configuration, bandwith, ping, dll namun untuk pengecekan celah kelemahan pada aplikasi umumnya dilaksanakan Kantor Pusat, SPAN & Pusintek
			Bukti	Screenshot tampilan bandwith meter Cek network Configuration Maintenance Rutin pada Jaringan **(Foto M-53, M-56 dan M-125)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

6.6	II	1	Apakah keseluruhan infrastruktur dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Diterapkan Secara Menyeluruh

			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah keseluruhan infrastruktur dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Keseluruhan infrastruktur masih sebagaian yang dalam penerapan untuk dimonitor dan memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada berdasarkan KMK479/KMK01/2010 Poin VI agar terus memantau penggunaan perangkat pengolah informasi dan membuat perkiraan pertumbuhan kedepan untuk memastikan ketersediaan kapasitas
			Bukti	KMK.479/KMK.01/2010 Screenshot tampilan bandwith meter (Foto M-12, M-125)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
6.7	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh

			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Dalam Penerapan/ Diterapkan Sebagian
			Temuan	Setiap perubahan dalam sistem informasi secara otomatis dan menyeluruh terekam di dalam log, namun sistem informasi yang dibagi pada unit vertical tidak bisa melihat / tidak dibuatkan menu untuk melihat listing rekapitulasi log misal : rekap log user pada akses SPAN sehingga permintaan data rekap log harus melalui permohonan lagi pada Kantor Pusat dan SPAN
			Bukti	Screenshot Akses User Nama Screenshot Akses User NIP **(Foto M-57 dan M-58)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
6.8	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh

			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Dalam Penerapan/ Diterapkan Sebagian
			Temuan	Secara sistem semua aktivitas terekam di dalam log karena dibutuhkan input pengguna yang diset secara khusus, namun kejadian ini belum pernah ditemukan sehingga tidak ada report log tentang pengaksesan oleh yang tidak berhak dan sistem tersebut nantinya akan terhubung dengan sistem SPAN melalui VPN. Selain dari itu, komputer tersebut tidak dapat terhubung dengan jaringan internet luar. Ini juga merupakan salah satu bentuk pengamanan untuk mengantisipi tindakan-tindakan hacking oleh pihak yang tidak bertanggungjawab
			Bukti	User akses SPAN Web SPAN tentang Data Centre

				Screenshot Akses User Nama Screenshot Akses User NIP **(Foto M-19,M-57, M-58 dan M-92)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
6.9	II	1	Apakah semua log dianalisis secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Diterapkan Secara Menyeluruh
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah semua log dianalisis secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Secara sistem SPAN menganalisis secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik) berdasarkan KMK.479/ KMK.01/2010 Poin VI, namun report evaluasi berkala sistem SPAN

				tidak disampaikan pada Kantor vertical kecuali terjadi insiden dan gangguan sistem lainnya.
			Bukti	KMK.479/KMK.01/2010 S-62/PB.08/2014 User & Pass SPAN User akses SPAN Web SPAN tentang Data Centre Screenshot Akses User Nama Screenshot Akses User NIP **(Foto M-19,M-57, M-58 dan M-92)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
6.10	II	1	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Diterapkan Secara Menyeluruh
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Dalam Perencanaan

			Temuan	DJPBN telah menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada berdasarkan KMK.479/ KMK.01/2010 Poin VIII bag D.3 Pengelolaan Keamanan Jaringan. SPAN sendiri memanfaatkan penggunaan enkripsi namun tidak terdefinisikan dalam dokumen/ website mengenai enkripsi tersebut
			Bukti	KMK.479/KMK.01/2010 S-62/PB.08/2014 User & Pass SPAN User akses SPAN Web SPAN tentang Data Centre Screenshot Akses User Nama Screenshot Akses User NIP **(Foto M-19,M-57, M-58 dan M-92)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
6.11	III	2	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	Diterapkan Secara Menyeluruh
			STATUS : DUGAAN	

			Pengubahan Status Kepatuhan	
			Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	Dalam Perencanaan
			Temuan	DJPBN telah menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada berdasarkan KMK.479/ KMK.01/2010 Poin VI bag D.4 Pengelolaan Keamanan Jaringan. SPAN sendiri memanfaatkan penggunaan enkripsi namun tidak terdefinisikan dalam dokumen/ website mengenai enkripsi tersebut
			Bukti	KMK.479/KMK.01/2010 S-62/PB.08/2014 User & Pass SPAN User akses SPAN Web SPAN tentang Data Centre Screenshot Akses User Nama Screenshot Akses User NIP **(Foto M-19,M-57, M-58 dan M-92)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

6.12	III	2	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Diterapkan Secara Menyeluruh
			STATUS ; DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Dalam Perencanaan
			Temuan	DJPBN telah menerapkan enkripsi sesuai kebijakan pengelolaan yang ada berdasarkan KMK.479/ KMK.01/2010 Poin VI bag D.4 Pengelolaan Keamanan Jaringan. SPAN sendiri memanfaatkan penggunaan enkripsi namun tidak terdefinisikan dalam dokumen/ website mengenai enkripsi tersebut
			Bukti	KMK.479/KMK.01/2010 S-62/PB.08/2014 User & Pass SPAN User akses SPAN Web SPAN tentang Data Centre

				Screenshot Akses User Nama Screenshot Akses User NIP **(Foto M-19,M-57, M-58 dan M-92)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

6.13	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas / panjangnya dan penggunaan kembali *password* lama?	Diterapkan Secara Menyeluruh
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menonaktifkan *password*, mengatur kompleksitas /panjangnya dan penggunaan kembali *password* lama?	Dalam Penerapan / Diterapkan Sebagian

			Temuan	Semua sistem termasuk SPAN dan sejumlah aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas / panjangnya dan penggunaan kembali *password* lama berdasarkan KMK No.512/KMK.01/ 2010
			Bukti	KMK.479/KMK.01/2010 KMK.512/KMK.01/2010 S-62/PB.08/2014 User & Pass SPAN User akses SPAN Web SPAN tentang Data Centre Screenshot Akses User Nama Screenshot Akses User NIP **(Foto M-19,M-57, M-58 dan M-92)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
6.14	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Diterapkan Secara Menyeluruh

			Temuan	Akses yang digunakan untuk mengelola sistem (administrasi sistem) pada SPAN secara menyeluruh telah menggunakan bentuk pengamanan khusus yang berlapis
			Bukti	Screenshot proxy, KMK.479/KMK.01/2010 KMK.512/KMK.01/2010 S-62/PB.08/2014 User & Pass SPAN User akses SPAN Web SPAN tentang Data Centre Screenshot Akses User Nama Screenshot Akses User NIP **(Foto M-19, M-29, M-57, M-58, M-62 dan M-92)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

			Catatan	Bentuk pengamanan admisnistrasi sistem dilakukan berlapis mulai dari tingkat rendah hingga tinggi. Untuk tingkat rendah diawali dengan penggunaan proxy untuk jaringan intranet sedangkan yang tinggi otentikasi username dan password untuk masuk sistem. Namun untuk pengelolaan bentuk pengamanan sistem belum terdokumentasi secara tertulis.
6.15	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?	Diterapkan Secara Menyeluruh
			Temuan	Sistem dan aplikasi yang digunakan lingkup Kanwil sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login, dan penarikan akses. Akses interface SPAN sendiri melakukan timeouts, lockout dan penarikan akses

			Bukti	Screenshot proxy, KMK.479/KMK.01/2010 KMK.512/KMK.01/2010 S-62/PB.08/2014 User & Pass SPAN User akses SPAN Web SPAN tentang Data Centre Screenshot Akses User Nama Screenshot Akses User NIP **(Foto M-19, M-29, M-57, M-58, M-62 dan M-92)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

6.16	III	2	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Diterapkan Secara Menyeluruh
			Temuan	Pengamanan data dan informasi pada SPAN dilengkapi dengan hal-hal berikut, diantaranya : Firewall, Bluecoat Web Filter, Anti SPAM sebagai perangkat pengamanan lalu

				lintas data internet dan intranet dengan komputer-komputer client, Access Control Server, Access Concentrator, sebagai perangkat keamanan dan manajemen konektivitas data, Vaccine Server, Security Server. Untuk akses jaringan nirkabel sendiri dipastikan menggunakan dua pengamanan yakni proxy depkeu, dan password wifi dan akses hanya diberikan jika melakukan permohonan user akses ke KPTIK GKN Surabaya I
			Bukti	Ipconfig Proxy untuk intranet DJPBN Pengamanan Web SPAN Permohonan Akses User (Foto **M-10, M-61, M-92 dan M-96**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

6.17	II	1	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	Diterapkan Secara Menyeluruh
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	Dalam Penerapan/ Diterapkan Sebagian
			Temuan	Pengamanan data dan informasi pada SPAN dilengkapi dengan hal-hal berikut, diantaranya : Firewall, Bluecoat Web Filter, Anti SPAM sebagai perangkat pengamanan lalu lintas data internet dan intranet dengan komputer-komputer client, Access Control Server, Access Concentrator, sebagai perangkat keamanan dan manajemen konektivitas data, Vaccine Server, Security Server. Untuk akses jaringan nirkabel sendiri dipastikan menggunakan dua pengamanan

				yakni proxy depkeu, dan password wifi dan akses hanya diberikan jika melakukan permohonan user akses ke KPTIK GKN Surabaya I. namun belum ada dokumentasi khusus prosedur permohonan akses dari luar instansi. Dan pengamanan ke unit-unit pelayanan juga dilaksanakan sebagaimana umumnya dengan menggunakan Buku Tamu, kartu Tamu dan Satpam
			Bukti	Buku Tamu Kartu Tamu Satuan pengamanan (Foto **M-67, M-68, M-69 dan M-70**)
			Kesesuaian(Ada/Tidak)	Ada, beberapa
			Tanggal Penyesuaian	21 April 2014
6.18	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Dalam Penerapan / Diterapkan Sebagian

			Temuan	Sistem operasi untuk setiap perangkat *desktop* dan *server* umumnya dimutakhirkan dengan versi terkini, namun tidak dapat dijadikan acuan karena sistem SPAN sebagai tulang punggung proses bisnis berbasiskan web dengan jalur yang dibangun secara khusus
			Bukti	Interface SPAN Custom Web Pemrosesan SPAN Cek Waktu utk Proses Kerja SPAN (Foto **M-6, M-43 dan M-71**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
6.19	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Diterapkan Secara Menyeluruh
			Temuan	Setiap *desktop* dan *server* secara menyeluruh dilindungi dari penyerangan virus (*malware*)
			Bukti	Screennshot antivirus komputer FO Antivirus Komputer semua bidang **(Foto M-30 dan M-31)**

			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
6.20	III	2	Apakah ada rekaman dan hasil analisis (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus telah dimutakhirkan secara rutin dan sistematis?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	DI KANWIL DJPBN terdapat rekaman dan hasil analisis (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus telah dimutakhirkan secara rutin dan sistematis karena update antivirus selain menjadi pengamanan informasi juga dilaporkan dalam bentuk pengendalian internal secara berjenjang dan berkala
			Bukti	Dokumen analisis risiko LPPI KPPN semester 1 LPPI Kanwil Tw.3 Dokumen evaluasi risiko **(Foto M-76, M-78,M-79 dan M-81)**
			Kesesuaian(Ada/Tidak)	Ada

			Tanggal Penyesuaian	21 April 2014

6.21	III	2	Apakah adanya laporan penyerangan virus yang gagal/sukses ditindaklanjuti dan diselesaikan?	Diterapkan Secara Menyeluruh
			STATUS : DUGAAN	
			Pengubahan Status Kepatuhan	
			Apakah adanya laporan penyerangan virus yang gagal/sukses ditindaklanjuti dan diselesaikan?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN telah menerapkan pelaporan penyerangan virus jika insiden tersebut mengganggu kinerja proses bisnis sebagaimaan kebijakan dalam KMK.479/KMK.01/2010 namun masih dilakukan secara informal dan tidak terdokumentasi
			Bukti	Dokumen analisis risiko LPPI KPPN semester 1 LPPI Kanwil Tw.3 Dokumen evaluasi risiko Laporan Gangguan Layanan TIK **(Foto M-76, M-78,M-79, M-81 dan M-114)**
			Kesesuaian(Ada/Tidak)	Ada

			Tanggal Penyesuaian	21 April 2014
			Catatan	KANWIL DJPBN secara resmi belum mempunyai laporan mengenai penyerangan antivirus dalam bentuk dokumen. Gangguan Layanan TIK yang masuk ke KPTIK pun umunya terkait jaringan.
6.22	III	2	Apakah keseluruhan sistem (aplikasi, perangkat komputer dan jaringan) sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	Keseluruhan sistem (aplikasi, perangkat komputer dan jaringan) wajib menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada namun belum ada evaluasi akurasi antara aplikasi, sistem dan jaringan. Standarisasi waktu saat ini menggunakan standar aplikasi SPAN

			Bukti	Screenshot aplikasi SPAN, Waktu optimasi SPAN **(Foto M-43 dan M-120)**
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014
6.23	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi keamanan yang diverifikasi/validasi pada saat pengembangan dan uji-coba?	Diterapkan Secara Menyeluruh
			Temuan	Setiap aplikasi yang ada secara menyeluruh memiliki spesifikasi keamanan yang diverifikasi/validasi pada saat pengembangan dan uji-coba sebagaimana diatur dalam KMK.479/KMK.01/2010 Poin VIII
			Bukti	KMK.479/KMK.01/2010 Strategi dan Metode Pengujian UAT (Foto **M-12 dan M-126**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

6.24	IV	3	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Dalam Penerapan / Diterapkan Sebagian
			Temuan	KANWIL DJPBN juga melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin berdasarkan KMK.479/ KMK.01/2010 dan KMK.351/KMK. 01/ 2011 dengan semua metode testing yang ada, namun disebabkan aplikasi yang dikembangkan umumnya adalah terkait aplikasi keuangan Negara maka keterlibatan lebih difokuskan kepada pengguna internal DJPBN / FO dan MO KPPN
			Bukti	KMK.479/KMK.01/2010 Strategi dan Metode Pengujian UAT (Foto **M-12 dan M-126**)
			Kesesuaian(Ada/Tidak)	Ada
			Tanggal Penyesuaian	21 April 2014

Lampiran H

Halaman ini sengaja dikosongkan

H.1 CPAR Area I Tata Kelola

Form 16.1 CPAR Tata Kelola 2.1

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Pimpinan intansi dalam hal ini Kepala Kanwil dan Kepala Bagian Umum serta Kepala Bidang secara resmi bertanggung jawab terhadap pelaksanaan pengamanan informasi, namun untuk lebih spesifik pada kebijakan keamanan secara teknis belum dirinci.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Sebagai pengimplementasian KMK 479/KMK.01/2010 maka diharapkan dibentuk fungsi dan kewenangan tertulis untuk *Chief Information Security Officer* Eselon II, *Information Security Manager* Eselon II dan Tim Keamanan Informasi secara formal pada Kanwil DJPBN yang bertanggungjawab kepada Kepala Kanwil DJPBN Jawa Timur.

Dibentuk suatu Dokumen Kebijakan Keamanan Informasi sebagai penjabaran atas Kebijakan Keamanan Informasi sebagaimana tertuang dalam KMK.479/KMK.01/2010, dipublikasikan dan dikomunikasikan kepada seluruh pegawai dan pihak-pihak lain yang relevan

Berdasarkan hasil skor penilaian bahwa Tingkat Kematangan bagian ini di level II maka peningkatannya diharapkan untuk dilakukan, dimana segenap pimpinan Kanwil DJPBN sebaiknya secara formal mengawasi pelaksanaan pengamanan dengan melakukan monitoring dan evaluasi rutin secara berkala. Monitoring

dan evaluasi didokumentasikan dengan rapi guna pembelajaran untuk pembuatan keputusan kebijakan keamanan informasi selanjutnya.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera.			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 16.2 CPAR Tata Kelola 2.2

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Pelaksanaan yang terkait dengan teknologi informasi umumnya dilakukan oleh Supervisi Teknis Aplikasi pada Bidang SKKI termasuk sebagian pengelolaan keamanan informasi. Untuk pengamanan yang lebih spesifik diserahkan pada tiap bagian dan seksi. Namun secara garis besar KANWIL DJPBN diharapkan memiliki unit keamanan informasi untuk melaksanakan fungsi atau bagian yang secara spesifik mengenai tugas dan tanggung jawab untuk keamanan informasi secara formal.

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Membuat renstra dan kebijakan dalam keamanan informasi dalam tingkat institusi Eselon II serta dijabarkan dalam tingkat teknis sebagaimana pelaksanaan SFO (*strategy focused organization*) yang selama ini sudah dilakukan.
Mendokumentasikan renstra dan kebijakan keamanan informasi secara tertulis. Mengkomunikasikan dokumentasi tersebut kepada pihak internal terkait (Kepala Bidang, Kepala Seksi dan Pelaksana) serta pihak ketiga.
Membentuk Tim Keamanan Informasi yang dikoordinasikan oleh Ketua Tim Keamanan Informasi dengan tugas, wewenang dan tanggungjawab meliputi seluruh pengamanan informasi untuk menjalankan renstra dan kebijakan diatas
Tugas, Wewenang dan Tanggung Jawab Tim Keamanan Informasi merupakan perwujudan Tugas, Wewenang dan Tanggung Jawab berdasarkan KMK.479/KMK.01/2010
Fungsi Tim Keamanan Informasi ini harus dikomunikasikan, dan

<table>
<tr><td colspan="4">disosialisasikan kepada Pimpinan, Kepala Bidang, Kepala Seksi dan seluruh Pelaksana serta pihak ketiga.
Guna peningkatan pengelolaan keamanan informasi, maka KANWIL DJPBN sebaiknya senantiasa melakukan monitoring dan evaluasi baik kebijakan atau rencana strategi dan terdokumentasikan dalam suatu laporan perubahan secara resmi dan tertulis..</td></tr>
<tr><td>Nama & TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
<tr><td colspan="4">Section 4 : Tindak lanjut dan verifikasi</td></tr>
<tr><td colspan="4">Ditingkatkan, disempurnakan lagi fungsi teknis Tim Keamanan Informasi dan dilaksanakan segera</td></tr>
<tr><td>Nama & TTD</td><td colspan="2">Disposisi oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
</table>

Form 16.3 CPAR Tata Kelola 2.3

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Pelaksanaan pengelolaan informasi umumnya dilakukan oleh Supervisi Teknis Aplikasi pada Kanwil DJPBN dan pelaksanaan pengamanan sudah dilakukan sebagian besar pada beberapa kontrol informasi yang dibutuhkan, namun wewenang penjaminan kepatuhan belum didefinisikan secara lengkap dan terstruktur dan tidak didelegasikan secara resmi pada Seksi Supervisi Teknis Aplikasi bidang SKKI

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Berdasarkan faktor di atas maka Kanwil DJPBN sebaiknya membentuk Tim Keamanan Informasi sebagai Pelaksana Pengamanan Informasi beserta dengan tugas, wewenang dan tanggungjawab sebagaimana usulan sebelumnya pada CPAR 2.2

Selanjutnya sebelum melakukan program kepatuhan, Kanwil DJPBN sebaiknya mendefinisikan kontrol kepatuhan seperti record data, log aktivitas, formulir prosedur, dll sebagai alat kewenangan pengelolaan keamanan informasi

Melakukan penjadwalan serta evaluasi kontrol seara berkala sesuai kebijakan unit atau instansi.

Bentuk evaluasi kepatuhan sebaiknya terdokumentasikan sehingga dapat dipakai sebagai pertimbangan untuk menetapkan keputusan kebijakan di masa depan. Selain itu evaluasi merupakan upaya Kanwil DJPBN dalam meningkatkan kualitas pengendalian internal.

Selain sebagai program kepatuhan (*compliance*) semua kontrol diperlukan dalam aktvitas audit.

Hasil evaluasi pengelolaan keamanan informasi sebagai suatu informasi public hendaknya dilaporkan secara berkala kepada pimpinan, dikomunikasikan, dan disosialisasikan di lingkup Kanwil DJPBN Jawa Timur			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 16.4 CPAR Tata Kelola 2.4

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Alokasi sumberdaya dalam pelaksanaan pengamanan sudah dilakukan sebagian besar pada beberapa kontrol informasi yang dibutuhkan namun alokasi sumberdaya untuk penjaminan kepatuhan belum didefinisikan secara lengkap dan terstruktur dan tidak didelegasikan secara resmi pada Seksi Supervisi Teknis Aplikasi bidang SKKI

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mengkategorikan dan mendefinisikan keamanan informasi berdasarkan kebutuhan, aset dan personel

Memiliki daftar kebutuhan sumberdaya pengamanan informasi meliputi :

- Data / Informasi (*softcopy* & *hardcopy*)
- Software (aplikasi, O/S, *tools/utility*, dsb)
- Akses pada *Hardware* & Infrastruktur Jaringan
- Sarana Pendukung
- SDM

Selain itu juga berdasarkan pengamanan berdasarkan tingkat kesulitan dan keamanannya

Mengukur secara umum tingkat risiko masing-masing aset

Mengalokasikan sumber daya manusia yang sesuai berdasarkan histori sebelumnya

Untuk menjamin keamanan, DJPBN secara umum menetapkan kesepakatan dengan karyawan terekrut berdasarkan perjanjian termasuk NDA karyawan.

Untuk meningkatkan level Tingkat Kematangan menjadi III hingga V maka

KANWIL DJPBN sebaiknya mengevaluasi kinerja SDM secara berkala serta memonitoring setiap tindakan pelaksanaan pengamanan. Hal ini dapat dilakukan dengan *checklist*, serta laporan *compliance* instruksi kerja pelaksana.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 16.5 CPAR Tata Kelola 2.5

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Peran pelaksanaan pengamanan informasi mencakup kebutuhan dipetakan secara umum berdasarkan konvensi / kesepahaman antar bidang dan antar seksi dengan pelaksana pada Supervisi Teknis Aplikasi kecuali untuk hal-hal yang diatur dalam pengendalian internal SKKI

Pemetaan hanya berdasarkan unit, belum berdasarkan kebutuhan audit internal serta wewenang yang bertanggung jawab pada aset informasi tersebut

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan peran serta tanggung jawab pelaksana pengamanan informasi secara jelas dalam bentuk dokumen tertulis atau bentuk perjanjian

Mengkoordinasikan tanggung jawab pengelolaan keamanan informasi dengan tim/personel pengamanan informasi

Jika untuk kebutuhan audit, maka dapat dibentuk tim pengamanan sendiri guna kebutuhan audit namun tidak harus terpisah dengan unit yang ada.

Untuk meningkatkan peran pengelolaan keamanan informasi menuju Tingkat Kematangan level III hingga V, maka KANWIL DJPBN sebaiknya melakukan evaluasi secara berkala pada tiap kinerja pelaksanaan pengamanan informasi. Selain itu, KANWIL DJPBN sebaiknya melakukan perubahan struktur peran pelaksana tanggung jawab jika memang dibutuhkan.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 16.6 CPAR Tata Kelola 2.6

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Persyaratan dan standar kompetensi sudah dijabarkan pada kebijakan di dokumen Indikator Kinerja Utama. Namun untuk kesesuaian atau tidak masih belum dijelaskan sehingga perlu adanya mekanisme peninjauan ulang pengecekan kompetensi tim keamanan informasi dengan kriteria SDM

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan semua peran pengamanan serta tanggung jawabnya
Melakukan verifikasi personel atau pelaksana yang ada dengan kesesuaian peran dan tanggungjawab yang telah dibuat
Jika perlu penunjukan melalui surat tugas mengenai pengelolaan keamanan aset informasi yang ada
Melaksanakan uji kompetensi pengelolaan keamanan informasi secara berkala baik offline maupun online
Menyelenggarakan evaluasi atas uji kompetensi
Melaksanakan bimbingan teknis (BIMTEK) untuk memperbesar kuantitas personil yang berkompeten terkait keamanan informasi
Untuk meningkatkan Tingkat Kematangan level III hingga V, maka KANWIL DJPBN sebaiknya melakukan evaluasi secara berkala pada tiap kinerja pelaksana. Selain itu, KANWIL DJPBN sebaiknya melakukan perubahan struktur peran pelaksana / tanggung jawab jika memang dibutuhkan..

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 16.7 CPAR Tata Kelola 2.7

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Pelaksana pengendalian internal di DJPBN khususnya yang dilakukan oleh Kanwil DJPBN sudah memiliki kompetensi dan keahlian yang memadai sesuai persyaratan / standar yang berlaku dan diterapkan secara menyeluruh namun untuk keamanan informasi secara khusus masih menunggu evaluasi tes online keamanan informasi DJPBN

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Melakukan verifikasi personel atau pelaksanan yang ada dengan kesesuaian yang telah dibuat
Jika perlu melakukan kontrak atau perjanjian mengenai keamanan aset yang ada
Jika ada temuan kemampuan / kapasitas yang tidak sesuai maka perlu dilakukan kebijakan seperti adanya sosialisasi atau pelatihan guna menunjang kemampuan sesuai kriteria tanggung jawab yang akan diemban nantinya
Untuk meningkatkan Tingkat Kematangan level III hingga V, maka KANWIL DJPBN sebaiknya melakukan evaluasi tiap personel untuk mengetahui wawasan mengenai keamanan informasi
Evaluasi pelaksana pengelolaan keamaan informasi seharusnya dapat dilakukan berkala dan dapat pula dilakukan setelah proses training.
Dibutuhkan adanya suatu dokumentasi pelaporan atas seluruh proses evaluasi

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 16.8 CPAR Tata Kelola 2.8

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Organsiasi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

DJPBN dan khususnya KANWIL DJPBN sudah melakukan peningkatan pemahaman keamanan informasi dengan adanya sosialisasi, tes online, pelatihan atau sertifikasi bagi para pelaksananya. Namun pelatihan pada KANWIL DJPBN belum terstruktur dan terjadwal secara berkala, pelatihan dilakukan berdasarkan kebutuhan semata dan kadang tidak adanya laporan tertulis sesuai dengan rencana strategis sebagaimana SFO yang telah dirancang

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Guna kepentingan sosialisasi dan pelatihan, pihak manajerial baiknya mengkomunikasikan terlebih dahulu kepada pelaksana mengenai bahan dan materi pelatihan yang akan dilaksanakan.
Merencanakan materi serta jadwal pelatihan secara berkala misal tiap triwulan sekali, didokumentasikan dan disosialisasikan
Menyusun langkah evaluasi pelaksanaan sosialisasi dan pelatihan baik dari sisi pelaksana ataupun manajerial.
Untuk meningkatkan peran ke Tingkat Kematangan level III hingga V, maka KANWIL DJPBN sebaiknya melakukan evaluasi tiap personel untuk mengetahui wawasan mengenai keamanan dan mendokumentasikannya sebagai analisis SDM organisasi.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 16.9 CPAR Tata Kelola 2.9

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Program sosialisasi dan pelatihan bagi pelaksana telah dilakukan namun kurang dijadwalkan secara rutin. Sosialisasi dan training hanya dilaksanakan jika ada kebutuhan

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Melakukan penjadwalan program atau pelatihan guna meningkatkan kompetensi serta keahlian pelaksana (misal setiap3 bulan dilakukan training)
Melakukan upgrade keahlian pelaksana sebagai upaya *controlling* dan *monitoring* SDM Kanwil DJPBN
Melakukan test praktik keamanan informasi sebagai evaluasi kemampuan pencegahan seperti ujicoba *testing hacking* pada sistem untuk mengetahui tingkat kompetensi pelaksanan pada *vulnerability* atau kerawanan dari sistem.
Untuk meningkatkan Tingkat Kematangan level III hingga V, maka KANWIL DJPBN sebaiknya melakukan evaluasi tiap personel untuk mengetahui wawasan mengenai keamanan informasi
Evaluasi ini dapat dilakukan setelah proses training atau pelatihan.
Melakukan pendokumentasian hasil evaluasi terhadap kompetensi pelaksana / pengelola keamanan informasi
Melakukan identifikasi dan analisis SDM berdasarkan laporan hasil evaluasi peningkatan kemampuan pelaksana

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 16.10 CPAR Tata Kelola 2.10

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal maupun eksternal untuk mengidentifikasikan persyaratan/kebutuhan pengamanan dan menyelesaikan permasalahan yang ada

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

DJPBN untuk masa sekarang dalam proses menerapkan tanggung jawab pengelolaan keamanan informasi dengan pihak pengelola / pengguna aset informasi secara internal maupun eksternal berdasarkan KMK.479 /KMK 01/ 2010 termasuk kontrak kerjasama dengan pihak ketiga dan kontrak kerjasama dengan satuan pengamanan Kanwil DJPBN

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Melakukan peninjauan ulang kerja sama dengan pihak internal KPTIK terhadap seluruh bentuk tanggung jawab pengamanan informasi misal : jaringan, infrastruktur dll dengan definisi tugas yang jelas.

Melakukan penyiapan *standar operating procedure* untuk tiap bentuk pencegahan pengamanan informasi dengan mendefinisikan tugas pengamanan informasi dalam skala manajerial dan operasional.

Untuk sistem informasi dengan skala besar dan melibatkan banyak pihak misal : SPAN, sebaiknya selain menerima penyerahan barang dan penugasan operasional; diharuskan juga meminta report / laporan untuk beberapa hal yang menjadi kendala dimana penyelesaiannya dilakukan oleh SPAN Pusat sekaligus sebagai feedback kepada pimpinan mengenai penanganan permasalahan keamanan informasi dan operasionalisasi

Menentukan dan memisahkan tanggung jawab yang jelas jika bekerja sama dengan pihak eksternal termasuk penyiapan langkah prosedural, misal : *vendor hardware* yang melakukan *maintenance* berkala..

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 16.11 CPAR Tata Kelola 2.11

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Pihak DJPBN khususnya Kanwil DJPBN secara menyeluruh menerapkan koordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan) dan pihak eksternal terkait yang berkepentingan (aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Melakukan pengkajian ulang kerja sama dengan pihak internal dan eksternal terhadap bentuk tanggung jawab pengelolaan pengamanan misal Satpam (Satuan Pengamanan) terkait dengan definisi tugas yang lebih jelas.
Melakukan pendefinisian dengan jelas bentuk pencegahan pengamanan informasi khususnya penanganan aset informasi dengan klasifikasi RAHASIA dan SANGAT RAHASIA baik dengan pihak internal maupun eksternal
Menentukan dan mendefinisikan prosedur dan tanggung jawab yang jelas jika bekerja sama dengan pihak eksternal, misal : untuk vendor hardware yang melakukan maintenance berkala.
Melakukan koordinasi pengarsipan kebutuhan pengamanan dan dokumen bentuk – bentuk pengamanan lingkup KANWIL DJPBN yang terkait dengan satker atau unit lain.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 16.12 CPAR Tata Kelola 2.12

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

DJPBN telah menerapkan tanggung jawab mengenai pengelolaan 11 domain area keamanan informasi berdasar KMK 479/KMK.01/2010 dan BCM berdasar KMK. 260/KMK. 01/2009 serta Analisis Resiko namun pihak Kanwil DJPBN sebagai unit vertical belum secara spesifik mendefinisikan mekanisme *disaster recovery plan* serta tingkat kepentingan dan probabilitasnya

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Memasukkan pendefinisian keamanan informasi dalam proses manajemen kelangsungan bisnis
Identifikasi kejadian-kejadian yang mengganggu proses bisnis melalui kegiatan risk assessment.
Mendaftar kemungkinan *disaster* atau bencana yang muncul pada setiap aset
Mendefinisikan kerugian serta dampak terjadinya bencana
Merecanakan tindakan mitigasi
Menyusun dan menerapkan rencana kelangsungan dan pemulihan operasi untuk menjamin ketersediaan proses bisnis kritikal pada tingkat tertentu
Membuat *Formulir Recovery Plan* (RP)
Menyediakan Kerangka *Business Continuity Planning* (BCP), termasuk skenario kegagalan yang mungkin dan langkah perbaikannya.
Melakukan pengujian, pemeliharaan dan revisi (jika perlu) agar dokumen BCP tetap valid
Untuk menuju tingkat kematangan III dan IV, KANWIL DJPBN sebaiknya melakukan *monitoring* berkala dengan menyusun *checklist* RP.

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 16.13 CPAR Tata Kelola 2.13

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Kanwil DJPBN telah melaksanakan mekanisme pelaporan kondisi kinerja/ efektivitas dan kepatuhan program melalui laporan pengendalian internal kepada pimpinan instansi secara rutin namun tidak secara spesifik dan khusus untuk pengelolaan keamanan informasi karena pengamanan informasi terlihat menjadi bagian *report* yang menyatu dengan proses bisnis Kanwil DJPBN

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan kategori dan prioritas kepatuhan yang ada pada lingkup Kanwil DJPBN

Memastikan kebutuhan pelaporan kepatuhan untuk semua pengelolaan keamanan yang terjadi di lapangan seperti adanya *logbook*, *checklist*, ataupun *record* yang wajib ada dalam penilaian kepatuhan

Melakukan pengimplementasian prosedur-prosedur yang tepat untuk memastikan kesesuaiannya dengan perundangan, peraturan dan perjanjian kontrak

Memastikan proteksi data dan privasi sesuai dengan peraturan dan regulasi yang ada

Menyusun prosedur pelaporan pengamanan informasi yang telah diatur dalam kebijakan.

Melakukan pengumpulan data atas keseluruhan bukti laporan sebagai upaya pendisiplinan pelaporan

Melakukan sistem *reward* dan *punishment*.

Melaksanakan evaluasi kepatuhan secara berkala

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 16.14 CPAR Tata Kelola 2.14

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

DJPBN berdasar KMK 479/ KMK.01/2010 melaksanakan evaluasi atas seluruh rekomendasi terkait TIK dan wujud nyatanya adalah SPAN sebagai program khusus untuk sasaran strategis TIK termasuk pengamanan informasi berdasar Renstra KMK.40/KMK.01/2010 hal. 66 dst. Khusus pada Kanwil DJPBN hal-hal yang mencakup pengelolaan informasi menjadi konsideran khusus bagi Seksi STA (Supervisi Teknis Aplikasi) SKKI. Kedepannya perlu diperhatikan pengembangan pengelolaan keamanan informasi sebagai konsideran dalam SFO organisasi

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Untuk membuat rancangan rencana strategis ke depannya sebaiknya dibedakan antara rencana strategis organisasi dengan rencana strategis sistem informasi
Rencana strategis keamanan informasi sebaiknya lebih mendetailkan ruang lingkup, tujuan, serta risiko yang berkaitan dan diselaraskan dengan tujuan unit KANWIL DJPBN dan umumnya DJPBN
Jika sudah dirancang, maka sebaiknya KANWIL DJPBN melakukan sosialisasi dan komunikasi kepada pihak-pihak yang akan bertanggung jawab di dalamnya seperti pelaksana pada bagiannya masing-masing.
Sebagai upaya peningkatan Tingkat Kematangan level III hingga level V maka KANWIL DJPBN sebaiknya melakukan evaluasi terhadap kebijakan atau renstra sesuai kondisi pengelolaan saat ini. Jika ditemukan kelemahan saat mengevaluasi sebaiknya membuat laporan perubahan serta pemutakhiran kebijakan.

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 16.15 CPAR Tata Kelola 2.15

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Pimpinan satuan kerja di Kanwil DJPBN diharuskan melakukan penetapan program khusus untuk pengamanan informasi namun saat ini belum ada penerapan di tingkat Kanwil karena kurangnya penjelasan rinci dari KMK.479 /KMK.01.2010 dan KMK.350/ KMK.01/2010 yang sebelumnya telah mensyaratkan kepatuhan pengamanan informasi yang juga menjadi tanggungjawab secara menyeluruh institusi.program khusus ini belum dilakukan secara formal oleh Kanwil DJPBN

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Untuk merencanakan program khusus sebagai kepatuhan terhadap keamanan informasi maka pihak KANWIL DJPBN perlu mendefinisikan ruang lingkup keamanan informasi dalam bentuk rencana strategis keamanan informasi

Selain itu, perlu adanya program dengan sistem *reward* dan *punishment* sebagaimana yang dimiliki untuk proses bisnis pelayanan sebagai upaya penegakkan kedisiplinan.

Untuk meningkatkan Tingkat Kematangan ke level III, maka KANWIL DJPBN sebaiknya melakukan dokumentasi resmi SMKI yang minimum mempunyai Kebijakan Keamanan Informasi, peran dan tanggung jawab keamanan organisasi, klasifikasi informasi, kebijakan pengamanan fisik dan logic, manajemen risiko serta pengelolaan sumber daya TI yang terkait.

Untuk meningkatkan ke level III hingga V maka KANWIL DJPBN sebaiknya juga menyusun prosedur dan instruksi kerja serta *checklist* guna proses evaluasi secara berkala.

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 16.16 CPAR Tata Kelola 2.16

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda sudah mendefinisikan paramater, metrik dan mekanisme pengukuran kinerja pengelolaan keamanan informasi

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Pimpinan satuan kerja di Kanwil DJPBN diharuskan mendefinisikan parameter, metric dan mekanisme untuk pengamanan informasi, namun saat ini belum ada penerapan di tingkat Kanwil karena kurangnya penjelasan rinci dari KMK.479 /KMK.01.2010 dan KMK.350/ KMK.01/2010 yang sebelumnya telah mensyaratkan kepatuhan pengamanan informasi yang juga menjadi tanggungjawab secara menyeluruh institusi.

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Melakukan survei, observasi dan analisis mengenai proses bisnis yang erat kaitannya dengan pengukuran kinerja keamanan informasi
Menentukan *framework* atau acuan dalam pengukuran kinerja
Menentukan tujuan pengukuran yang relevan dengan keamanan informasi
Menentukan indikator dalam bentuk kualitatif dan kuantitatif guna memudahkan pencapaian indikator
Mendefinisikan subjek metrik dalam proses bisnis pengendalian internal keamanan informasi KANWIL DJPBN. Termasuk kemungkinan adanya satker atau pihak eksternal / pihak ketiga yang masih dan perlu bertanggung jawab dalam keamanan informasi.
Sebaiknya pengukuran disusun berdasarkan bentuk kontrol atau pengendalian yang telah dibuat.
Untuk kepentingan eskalasi Tingkat Kematangan ke level III, maka metode atau mekanisme pengukuran sebaiknya didokumentasikan secara resmi dalam SMKI.
Menyusun seluruh bentuk pengendalian internal berdasarkan pengelolaan risiko

keamanan informasi. Untuk eskalasi menuju level III hingga V maka KANWIL DJPBN juga perlu berbenah diri dalam melakukan monitoring berkala dari penerapan efektivitas metode pengukuran yang ada, apakah diperlukan pemutakhiran atau tidak.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 16.17 CPAR Tata Kelola 2.17

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Pimpinan satuan kerja di Kanwil DJPBN diharuskan mendefinisikan program penilaian kinerja untuk pengamanan informasi dalam penilaian hard competency, namun saat ini belum ada penerapan di tingkat Kanwil karena kurangnya penjelasan rinci dari KMK.479 /KMK.01.2010 dan KMK.350/ KMK.01/2010 yang sebelumnya telah mensyaratkan kepatuhan pengamanan informasi yang juga menjadi tanggungjawab secara menyeluruh dalam institusi.Pertanyaan atau topik yang terdapat pada penilaian kinerja masih umum dan belum secara spesifik mengarah pada tanggung jawab masing-masing pelaksana

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mensyaratkan seluruh pegawai, kontraktor atau pihak ketiga untuk mengaplikasikan keamanan informasi seuai dengan kebijakan dan prosedur keamanan informasi yang telah dibuat

Memberikan sosialisasi dan pelatihan berkala terkait keamanan informasi

Jika memang terdapat sistem penilaian secara terpusat semua pegawai atau tenaga kerja di DJPBN, maka untuk mengetahui seberapa jauh kinerja pegawai maka perlu dilakukan juga penilaian per bagian dan per unit atau penyediaan pertinggal pelaporan sistem penilaian kepatuhan tersebut.

Penilaian kinerja per bagian dilakukan berdasarkan :

- *Timeline* waktu kerja
- Cakupan tugas dan tanggung jawab
- Kepatuhan mengenai program keamanan informasi dari KANWIL DJPBN dan Kantor Pusat

Untuk meningkatkan ke Tingkat Kematangan level III hingga V, maka KANWIL DJPBN sebaiknya melakukan evaluasi tiap personel untuk mengetahui wawasan mengenai keamanan informasi sebagaimana yang pernah dilaksanakan sebelumnya Evaluasi kepatuhan ini dapat dilakukan setelah proses training atau pelatihan secara berkala, didokumentasikan dan dijadikan bahan analisis pimpinan.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 16.18 CPAR Tata Kelola 2.18

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan dan mengevaluasi pencapaiannya secara rutin, termasuk pelaporannya kepada pimpinan Instansi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Pimpinan satuan kerja di Kanwil DJPBN diharuskan mendefinisikan target dan sasaran untuk pengelolaan pengamanan informasi termasuk evaluasinya secara rutin, namun saat ini belum ada penerapan di tingkat Kanwil karena kurangnya penjelasan rinci dari KMK.479 /KMK.01.2010 dan KMK.350/KMK.01/2010 yang sebelumnya telah mensyaratkan kepatuhan pengamanan informasi dan juga penetapan target dan sasaran pengeloaaan keamanan informasi dalam institusi.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Menurunkan kebijakan selama ini kedalam dokumen kebijakan keamanan informasi Kanwil DJPBN, didokumentasikan, dikomunikasikan dan dipublikasikan kepada seluruh pegawai dan pihak-pihak lain yang relevan
Menciptakan rencana strategis organisasi terkait keamanan informasi
Target dan sasaran diturunkan dari rencana strategis dan kebijakan organisasi (KANWIL DJPBN) terkait pengelolaan keamanan informasi
Menyusun indikator kuantitatif guna dapat menghitung capaian tiap target pengelolaan keamanan informasi yang ada.
Target dan sasaran yang sudah ditetapkan sebaiknya dikomunikasikan dan dipublikasikan kepada pihak terkait seperti pihak pelaksana dan pihak ketiga.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 16.19 CPAR Tata Kelola 2.19

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda sudah mengidentifikasi legislasi dan perangkat hukum lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisis tingkat kepatuhannya

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Pimpinan satuan kerja di Kanwil DJPBN diharuskan mendefinisikan analisis tingkat kepatuhan untuk pengelolaan pengamanan informasi termasuk legislasi dan perangkat hukumnya, namun saat ini belum ada analisis tingkat kepatuhan di tingkat Kanwil karena kurangnya penjelasan rinci dari KMK.479 /KMK.01.2010 dan KMK.350/ KMK.01/2010 yang sebelumnya telah mensyaratkan kepatuhan pengamanan informasi dan juga penetapan analisis tingkat kepatuhan pengeloaaan keamanan informasi dalam institusi.

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mengidentifikasi perangkat legislasi dan hukum lainnya yang merupakan turunan dari rencana strategis keamanan informasi sebagaimana dibahas pada CPAR sebelumnya

Melengkapi semua perangkat dan dokumen yang dibutuhkan guna kelengkapan hukum dan legislasi

Setelah itu, mendefinisikan berdasarkan kekayaan aset yang ada sehingga mampu memprediksi nilai kerugian/loss jika terdapat pelanggaran keamanan informasi yang terlihat.

Menganalisis tingkat kepatuhan pengelolaan keamanan informasi secara berkala

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 16.20 CPAR Tata Kelola 2.20

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Kebijakan terkait keamanan informasi dan langkah penanggulanagan insiden telah didefinisikan namun pelanggaran hukum hanya ditemukan pada KMK.512/ KMK.01/2010 yang mengatur Sanksi Administratif dan Sanksi Teknis

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Menghubungkan tujuan pengelolaan keamanan informasi dengan proses bisnis unit dan bagian dengan tujuan mengidentifikasi insiden yang terkait.
Mengidentifikasi kemunculan insiden, tingkat kemungkinan, termasuk di dalamnya kategorisasi dan prioritisasi insiden
Membuat langkah korektif insiden berdasarkan kategori dan prioritasnya
Secara proaktif berkoordinasi dengan satker terkait (Legal/Hukum) dan pihak eksternal yang berkepentingan (aparat keamanan)
Membuat legislasi serta perangkat hukum untuk menjamin kepatuhan pada pelaksanaannya (*tools* identifikasi jika ada pelanggaran).
Sebagai upaya peningkatan menuju Tingkat Kematangan level III hingga V maka KANWIL DJPBN sebaiknya menyusun kebijakan serta pemetaan hukum di dalamnya. Guna efektivitas penyusunan, maka KANWIL DJPBN sebaiknya melakukan evaluasi kebijakan sebagaimana rencana strategi yang telah disusun.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Lampiran I

Halaman ini sengaja dikosongkan

I.1 CPAR Area II Pengelolaan Risiko

Form 17.1 CPAR Pengelolaan Risiko 3.1

<table>
<tr><td colspan="4">KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR
GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640</td></tr>
<tr><td colspan="4">Section 1 : Obyek</td></tr>
<tr><td colspan="4">Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan</td></tr>
<tr><td>Nama & TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
<tr><td colspan="4">Section 2 : Penyebab / Pendukung</td></tr>
<tr><td colspan="4">Kanwil DJPBN telah memiliki dokumen pengelolaan risiko untuk proses bisnis pelayanan perbendaharaan. Untuk membuat program kerja pengelolaan risiko pengelolaan keamanan informasi, KANWIL DJPBN sebaiknya mempunyai dokumen identifikasi risiko beserta evaluasi dan analisis risiko keamanan informasi yang khusus dan terpisah dari kerangka pengendalian risiko proses bisnis yang dilaksanakan selama ini. Dokumen kerangka kerja pengelolaan risiko keamanan informasi secara inisiatif harus dilakukan sesegera mungkin..</td></tr>
<tr><td>Nama & TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
<tr><td colspan="4">Section 3 : Usulan tindakan perbaikan</td></tr>
<tr><td colspan="4">Membuat daftar risiko dalam proses bisnis terkait keamanan informasi
Membuat skala risiko hingga tingkat probablitas kejadiannya
Menentukan tindakan mitigasi dan pengendalian risiko
Membuat kontrol pengendalian seperti log, form, dll
Untuk menuju tingkat kematangan III atau yang lebih tinggi maka KANWIL DJPBN harus mempunyai kerangka kerja risiko terdokumentasi secara resmi yang mengacu pada KMK.479/KMK.01/2010.</td></tr>
<tr><td>Nama & TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
</table>

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis pengelolaan risiko dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 17.2 CPAR Pengelolaan Risiko 3.2

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Kanwil DJPBN telah memiliki dokumen pengelolaan risiko untuk proses bisnis pelayanan perbendaharaan. Untuk membuat kerangka kerja pengelolaan risiko pengelolaan keamanan informasi, KANWIL DJPBN sebaiknya mempunyai dokumen identifikasi risiko beserta evaluasi dan analisis risiko keamanan informasi yang khusus dan terpisah dari kerangka pengendalian risiko proses bisnis yang dilaksanakan selama ini. Dokumen kerangka kerja pengelolaan risiko keamanan informasi secara inisiatif harus dilakukan sesegera mungkin..

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Membuat daftar risiko dalam proses bisnis terkait keamanan informasi
Membuat skala risiko hingga tingkat probablitas kejadiannya
Menentukan tindakan mitigasi dan pengendalian risiko keamanan informasi
Membuat kontrol pengendalian seperti log, *checklist*, form, laporan dll
Menyajikannya secara berkala sebagai bentuk pelaporan kepada pimpinan dan dikomunikasikan serta disosialisasikan kepada seluruh pelaksana untuk mendapat tindak lanjut perbaikan yang lebih baik
Menginventarisir seluruh laporan dan melakukan kajian efektivitas kontrol.
Untuk menuju tingkat kematangan III atau yang lebih tinggi maka KANWIL DJPBN harus mempunyai kerangka kerja risiko terdokumentasi secara resmi yang mengacu kepada KMK.479/KMK.01/2010.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 17.3 CPAR Pengelolaan Risiko 3.3

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Kanwil DJPBN telah memiliki dokumen pengelolaan risiko untuk proses bisnis pelayanan perbendaharaan. Untuk membuat kerangka kerja pengelolaan risiko pengelolaan keamanan informasi, KANWIL DJPBN sebaiknya mempunyai dokumen identifikasi risiko beserta evaluasi dan analisis risiko keamanan informasi yang khusus dan terpisah dari kerangka pengendalian risiko proses bisnis yang dilaksanakan selama ini. Dokumen kerangka kerja pengelolaan risiko keamanan informasi secara inisiatif harus dilakukan sesegera mungkin..

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Membuat daftar seluruh risiko keamanan informasi yang terkait dengan aset informasi berdasarkan definisi serta tingkat klasifikasi aset
Misal : Aset komputer mempunyai berbagai risiko terkait penggunaannya.
Membuat tingkat ancaman atau kerugian jika risiko aset terjadi serta level probabilitas terjadinya risiko tersebut
Menentukan dampak terkait dengan ancaman yang terjadi serta bobot ancaman
Mendefinisikan risiko berdasarkan aset per unit
Misal : Risiko antivirus yang tidak terupdate di bagian Front Office (FO)
Membuat kontrol pengendalian seperti adanya prosedur, log, form
Misal : logbook *maintenance* jaringan tiap bulan, prosedur pemeliharaan, formulir pemeliharaan
Untuk menuju ke tingkat kematangan III atau yang lebih tinggi maka KANWIL DJPBN harus mempunyai kerangka kerja risiko terdokumentasi secara resmi yang detailnya seperti yang telah dijelaskan dalam KMK.479/KMK.01/2010.

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 17.4 CPAR Pengelolaan Risiko 3.4

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN dalam proses penyesuaian berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi digunakan termasuk penetapan ambang batas risiko terhadap performa DJPBN berdasarkan level risiko, level konsekuensi, kategori risiko, level frekuensi dan personal judgement (LR, LK, C, LF) untuk menentukan apakah Fraud, Srategis, Operasional, Compliance&Finansial), namun hal ini berlaku pada pengendalian internal terkait proses bisnis dan belum secara khusus dalam pengendalian pengelolaan keamanan informasi Kanwil DJJPBN

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Menetapkan PIC (*person in charge*) atau penanggung jawab dari aset informasi yang ada
Membuat mekanisme/prosedur penilaian ambang bats risiko berdasarkan aset informasi yang ada
Untuk kepentingan eskalasi Tingkat Kematangan ke level III, maka KANWIL DJPBN perlu mendefinisikan kepemilikan serta menetapkan pihak pengelola (custodian) aset pada kebijakan atau rencana strategis keamanan informasi tingkat Kanwil DJPBN
Untuk menyusun bentuk kontrol sebagaimana CPAR sebelumnya maka sebaiknya disesuaikan dengan aset informasi yang telah ditentukan
Guna eskalasi ke level III hingga level V, maka perlu dilakukan evaluasi berkala penetapan ambang batas tingkat resiko
Evaluasi harus dilaporkan, didokumentasikan dan dikomunikasikan

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 17.5 CPAR Pengelolaan Risiko 3.5

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN dalam proses penyesuaian berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang dokumen didalamnya termasuk Tabel Rancangan Pengendalian yang terdokumentasi dan secara resmi digunakan termasuk pengendalian aset informasi yang didalamnya berisi aplikasi pendukung dan dokumen pendukung sebagai aset informasi, pelaksana pengendalian sebagai pengelola dan unsur pengendalian lainnya terhadap performa DJPBN berdasarkan jenis kegiatan, keluaran, tujuan dan identifikasinya. Namun kesemua pengendalian butuh dispesifikasikan lagi dalam hal keterkaitannya dengan aset informasi yang menjadi aspek utama dalam pengendalian keamanan informasi

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Menetapkan PIC (*person in charge*) atau penanggung jawab dari aset yang ada
Membuat prosedur pengelolaan dan pengendalian berdasarkan aset serta pihak pengelola/*custodian* yang ada
Untuk kepentingan eskalasi Tingkat Kematangan ke level III, maka KANWIL DJPBN perlu mendefinisikan kepemilikan serta pihak pengelola (*custodian*) aset ke dalam kebijakan atau rencana strategis keamanan informasi lingkup Kanwil DJPBN
Untuk menyusun bentuk kontrol maka sebaiknya disesuaikan dengan aset yang telah ditentukan
Guna eskalasi ke level III hingga level V, maka perlu dilakukan evaluasi kepemilikan berdasarkan histori pelaksanaan pengamanan tiap pengelola aset.

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 17.6 CPAR Pengelolaan Risiko 3.6

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN dalam proses penyesuaian berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan aset informasi pengendalian yang didalamnya berisi aplikasi pendukung dan dokumen pendukung sebagai aset informasi. Namun belum dilakukan pembedaan secara detil tentang aset utama karena seluruh komponen pengendalian masuk dalam kategori aset utama

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Membuat daftar ancaman dan kelemahan berdasarkana Aset informasi yang ada di KANWIL DJPBN

Misal : Aset komputer mempunyai berbagai ancaman dan kelemahan terkait dengan risiko yang terjadi

Membuat tingkat atau level ancaman atau kerugian jika risiko aset terjadi serta probabilitas terjadinya risiko tersebut

Menentukan penilaian dari tingkat probabilitas terjadinya ancaman

Membuat kerangka kerja pengelolaan aset infomasi berdasarkan ancaman dan kelemahan dengan detail di dalamnya.

- Daftar aset
- Daftar ancaman dan kelemahan
- Tingkat atau level ancaman dan kelemahan
- Probabilitas atau tingkat kemungkinan munculnya ancaman
- Kontrol atau pengendalian berupa prosedur, log, form

Misal : logbook *maintenance* jaringan tiap bulan, prosedur pemeliharaan, formulir pemeliharaan dan pengendalian lain yang terkait.

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 17.7 CPAR Pengelolaan Risiko 3.7

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN dalam sebagai unit pelaksana vertical DJPBN telah mengimplementasikan PMK.191/ PMK .08/2008 yang melaksanakan suatu kerangka kerja pengelolaan risiko dimana dokumen didalamnya termasuk analisis risiko aset informasi yang dideskripsikan pada Analisis Risiko. Namun identifikasi berdasarkan aset informasi perlu menjadi perhatian khusus disamping identifikasi berdasarkan sasaran unit penilaian risiko.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan klasifikasi aset
Mengklasifikasikan aset utama dalam pengelolaan
Mendefinisikan dampak risiko/ kerugian berdasarkan aset informasi yang ada
Mendefinisikan tingkat vulnerability dari setiap aset yang biasa disebut dengan Risk Register
Dari hasil definisi tersebut, dapat dilakukan analisis risiko tiap aset
Membuat analisis perhitungan risiko mulai dari level rendah hingga level tinggi pada risiko
Melakukan tindakan pengendalian contoh formulir, logbook, dan prosedur
Agar dapat menaikkan nilai tingkat penerapan maka dilakukan evaluasi berkala dari semua tindakan pengendalian yang ada dalam bentuk laporan yang juga disosialisasikan berkala minimal pada tiap bagian.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 17.8 CPAR Pengelolaan Risiko 3.8

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda sudah menjalankan inisiatif analisis/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN dalam sebagai unit pelaksana vertical DJPBN telah mengimplementasikan PMK.191/ PMK .08/2008 yang melaksanakan suatu kerangka kerja pengelolaan risiko dimana dokumen didalamnya termasuk analisis risiko aset informasi yang dideskripsikan pada Analisis Risiko. Namun identifikasi berdasarkan aset informasi perlu menjadi perhatian khusus disamping identifikasi berdasarkan sasaran unit penilaian risiko.

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan klasifikasi aset pada Kanwil DJPBN
Mengklasifikasikan aset utama dalam pengelolaan.
Mendefinisikan dampak risiko/ kerugian berdasarkan aset informasi yang ada
Mendefinisikan tingkat vulnerability dari setiap aset yang biasa disebut dengan Risk Register
Dari hasil definisi tersebut, dapat dilakukan analisis risiko tiap aset
Membuat analisis perhitungan risiko mulai dari level rendah hingga level tinggi pada risiko
Melakukan proiritisasi risiko berdasarkan analisis risiko diatas.
Melakukan tindakan pengendalian contoh formulir, logbook, dan prosedur
Agar dapat menaikkan nilai tingkat penerapan maka usulan dilakukan evaluasi berkala dari semua tindakan pengendalian yang ada dalam bentuk laporan yang didokumentasikan
Laporan evaluasi juga disosialisasikan berkala pada tiap bagian.

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 17.9 CPAR Pengelolaan Risiko 3.9

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN dalam proses penyesuaian berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi digunakan mencakup definisi dan hubungan tingkat klasifikasi risiko, sistem pengendalian, pilihan opsi penanganan dan opsi penanganan terpilih terkait dengan performa DJPBN. Namun perlu dilakukan analisis risiko yang lebih spesifik kepada keamanan informasi secara berkala terkait pengimplementasian KMK.479/KMK.01/2010

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan klasifikasi risiko pada Kanwil DJPBN
Mengklasifikasikan risiko keamanan informasi dalam pengelolaan.
Mendefinisikan dampak risiko/ kerugian berdasarkan aset informasi yang ada
Mendefinisikan tingkat vulnerability dari setiap risiko
Dari hasil definisi tersebut, dapat dilakukan analisis risiko keamanan informasi
Membuat analisis perhitungan risiko mulai dari level rendah hingga level tinggi
Melakukan proiritisasi risiko berdasarkan analisis risiko diatas.
Melakukan tindakan pengendalian contoh formulir, logbook, dan prosedur
Agar dapat menaikkan nilai tingkat penerapan maka usulan dilakukan evaluasi berkala dari semua tindakan pengendalian yang ada dalam bentuk laporan
Laporan evaluasi juga disosialisasikan berkala pada tiap bagian.

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 17.10 CPAR Pengelolaan Risiko 3.10

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas biaya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN dalam proses penyesuaian berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi digunakan mencakup definisi dan hubungan tingkat klasifikasi risiko, sistem pengendalian, pilihan opsi penanganan dan opsi penanganan terpilih terkait dengan performa DJPBN. Namun perlu dilakukan analisis risiko yang lebih spesifik kepada keamanan informasi secara berkala terkait pengimplementasian KMK.479/KMK.01/2010

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan klasifikasi risiko pada Kanwil DJPBN
Mengklasifikasikan risiko keamanan informasi dalam pengelolaan.
Mendefinisikan dampak risiko/ kerugian berdasarkan aset informasi yang ada
Mendefinisikan tingkat vulnerability dari setiap risiko
Dari hasil definisi tersebut, dapat dilakukan analisis risiko keamanan informasi
Membuat analisis perhitungan risiko mulai dari level rendah hingga level tinggi
Melakukan proiritisasi risiko berdasarkan analisis risiko diatas.
Melakukan tindakan pengendalian contoh formulir, logbook, dan prosedur
Agar dapat menaikkan nilai tingkat penerapan maka usulan dilakukan evaluasi berkala dari semua tindakan pengendalian yang ada dalam bentuk laporan
Laporan evaluasi juga disosialisasikan berkala pada tiap bagian.
Menentukan ambang batas risiko dan menguji apakah langkah pengendalian yang kita lakukan efektif menurunkan level frekuensi risiko

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 17.11 CPAR Pengelolaan Risiko 3.11

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN dalam proses penyesuaian berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi digunakan mencakup definisi dan hubungan tingkat klasifikasi risiko, sistem pengendalian, pilihan opsi penanganan dan opsi penanganan terpilih terkait dengan performa DJPBN. Namun perlu dilakukan analisis risiko yang lebih spesifik kepada keamanan informasi secara berkala terkait pengimplementasian KMK.479/KMK.01/2010

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan klasifikasi risiko pada Kanwil DJPBN
Mengklasifikasikan risiko keamanan informasi dalam pengelolaan.
Mendefinisikan dampak risiko/ kerugian berdasarkan aset informasi yang ada
Mendefinisikan tingkat vulnerability dari setiap risiko
Dari hasil definisi tersebut, dapat dilakukan analisis risiko keamanan informasi
Membuat analisis perhitungan risiko mulai dari level rendah hingga level tinggi
Melakukan proiritisasi risiko berdasarkan analisis risiko diatas.
Melakukan tindakan pengendalian contoh formulir, logbook, dan prosedur
Agar dapat menaikkan nilai tingkat penerapan maka usulan dilakukan evaluasi berkala dari semua tindakan pengendalian yang ada dalam bentuk laporan
Laporan evaluasi juga dikomunikasikan dan disosialisasikan berkala pada seluruh pelaksanan di tiap bagian.
Menentukan ambang batas risiko keamanan informasi dan menguji apakah langkah pengendalian yang kita lakukan efektif menurunkan level frekuensi risiko

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 17.12 CPAR Pengelolaan Risiko 3.12

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi untuk memastikan konsistensi dan efektifitasnya

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN dalam proses penyesuaian berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi digunakan mencakup definisi dan hubungan tingkat klasifikasi risiko, sistem pengendalian, pilihan opsi penanganan dan opsi penanganan terpilih terkait dengan performa DJPBN. Namun perlu dilakukan analisis risiko yang lebih spesifik kepada keamanan informasi secara berkala terkait pengimplementasian KMK.479/KMK.01/2010

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan klasifikasi risiko pada Kanwil DJPBN
Mengklasifikasikan risiko keamanan informasi dalam pengelolaan.
Mendefinisikan dampak risiko/ kerugian berdasarkan aset informasi yang ada
Mendefinisikan tingkat vulnerability dari setiap risiko
Dari hasil definisi tersebut, dapat dilakukan analisis risiko keamanan informasi
Membuat analisis perhitungan risiko mulai dari level rendah hingga level tinggi
Melakukan proiritisasi risiko berdasarkan analisis risiko diatas.
Melakukan tindakan pengendalian contoh formulir, logbook, dan prosedur
Agar dapat menaikkan nilai tingkat penerapan maka usulan dilakukan evaluasi berkala dari semua tindakan pengendalian yang ada dalam bentuk laporan
Laporan evaluasi juga dikomunikasikan dan disosialisasikan berkala pada seluruh pelaksanan di tiap bagian.
Menentukan ambang batas risiko keamanan informasi dan menguji apakah langkah pengendalian yang kita lakukan efektif menurunkan level frekuensi risiko

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 17.13 CPAR Pengelolaan Risiko 3.13

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN dalam proses penyesuaian berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi digunakan mencakup definisi dan hubungan tingkat klasifikasi risiko, sistem pengendalian, pilihan opsi penanganan dan opsi penanganan terpilih terkait dengan performa DJPBN. Namun perlu dilakukan analisis risiko yang lebih spesifik kepada keamanan informasi secara berkala terkait pengimplementasian KMK.479/KMK.01/2010

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan klasifikasi risiko pada Kanwil DJPBN
Mengklasifikasikan risiko keamanan informasi dalam pengelolaan.
Mendefinisikan dampak risiko/ kerugian berdasarkan aset informasi yang ada
Mendefinisikan tingkat vulnerability dari setiap risiko
Dari hasil definisi tersebut, dapat dilakukan analisis risiko keamanan informasi
Membuat analisis perhitungan risiko mulai dari level rendah hingga level tinggi
Melakukan proiritisasi risiko berdasarkan analisis risiko diatas.
Melakukan tindakan pengendalian contoh formulir, logbook, dan prosedur
Agar dapat menaikkan nilai tingkat penerapan maka usulan dilakukan evaluasi berkala dari semua tindakan pengendalian yang ada dalam bentuk laporan
Laporan evaluasi juga dikomunikasikan dan disosialisasikan berkala pada seluruh pelaksanan di tiap bagian.
Menentukan ambang batas risiko keamanan informasi dan menguji apakah

langkah pengendalian yang kita lakukan efektif menurunkan level frekuensi risiko Melaksanakan perubahan tindakan pengendalian untuk langkah-langkah pengendalian yang menunjukkan tren level frekuensi risiko tetap/meningkat dengan langkah-langkah pengendalian dengan kemampuan efektivitas yang lebih baik			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 17.14 CPAR Pengelolaan Risiko 3.14

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN dalam proses penyesuaian berdasarkan PMK.191 / PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi digunakan mencakup definisi dan hubungan tingkat klasifikasi risiko, sistem pengendalian, pilihan opsi penanganan dan opsi penanganan terpilih terkait dengan performa DJPBN. Namun perlu dilakukan analisis risiko yang lebih spesifik kepada keamanan informasi secara berkala terkait pengimplementasian KMK.479/KMK.01/2010

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan klasifikasi risiko pada Kanwil DJPBN
Mengklasifikasikan risiko keamanan informasi dalam pengelolaan.
Mendefinisikan dampak risiko/ kerugian berdasarkan aset informasi yang ada
Mendefinisikan tingkat vulnerability dari setiap risiko
Dari hasil definisi tersebut, dapat dilakukan analisis risiko keamanan informasi
Membuat analisis perhitungan risiko mulai dari level rendah hingga level tinggi
Melakukan proiritisasi risiko berdasarkan analisis risiko diatas.
Melakukan tindakan pengendalian contoh formulir, logbook, dan prosedur
Agar dapat menaikkan nilai tingkat penerapan maka usulan dilakukan evaluasi berkala dari semua tindakan pengendalian yang ada dalam bentuk laporan
Laporan evaluasi juga dikomunikasikan dan disosialisasikan berkala pada seluruh pelaksanan di tiap bagian.
Menentukan ambang batas risiko keamanan informasi dan menguji apakah langkah pengendalian yang kita lakukan efektif menurunkan level frekuensi risiko

Melaksanakan perubahan tindakan pengendalian untuk langkah-langkah pengendalian yang menunjukkan tren level frekuensi risiko tetap/meningkat dengan langkah-langkah pengendalian dengan kemampuan efektivitas yang lebih baik			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Apakah pimpinan Instansi anda secara prinsip dan resmi kebijakan terkait?			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 17.15 CPAR Pengelolaan Risiko 3.15

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN dalam proses pelaksanaan berdasarkan PMK.191 /PMK.08/2008 melaksanakan suatu kerangka kerja pengelolaan risiko yang terdokumentasi dan secara resmi dilaporkan berkala kepada pimpinan terkait performa DJPBN berdasarkan level risiko, level konsekuensi, kategori risiko, level frekuensi dan personal judgement (LR, LK, C, LF) untuk menentukan apakah Fraud, Srategis, Operasional, Compliance & Finansial). Tindakan penilaian untuk meningkatkan efektifitas pengendalian risiko dan mendorong tingkat risiko menuju ke trend yg lebih kecil/lebih rendah umunya dilakukan dengan memperhatikan dasar pemilihan opsi penanganan dan dilaporkan secara berkala untuk mendapatkan masukan dari kebijakan yang lebih tinggi. Masuknya unsur penilaian persentase laporan mitigasi risiko dan laporan pengendalian internal dalam IKU SKKI memastikan unsur ini dalam indicator kinerja untuk proses bisnis Kanwil DJPBN

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan klasifikasi risiko pada Kanwil DJPBN
Mengklasifikasikan risiko keamanan informasi dalam pengelolaan.
Mendefinisikan dampak risiko/ kerugian berdasarkan aset informasi yang ada
Mendefinisikan tingkat vulnerability dari setiap risiko
Dari hasil definisi tersebut, dapat dilakukan analisis risiko keamanan informasi
Membuat analisis perhitungan risiko mulai dari level rendah hingga level tinggi
Melakukan proiritisasi risiko berdasarkan analisis risiko diatas.
Melakukan tindakan pengendalian contoh formulir, logbook, dan prosedur
Agar dapat menaikkan nilai tingkat penerapan maka usulan dilakukan evaluasi

berkala dari semua tindakan pengendalian yang ada dalam bentuk laporan Laporan evaluasi juga dikomunikasikan dan disosialisasikan berkala pada seluruh pelaksanan di tiap bagian. Menentukan ambang batas risiko keamanan informasi dan menguji apakah langkah pengendalian yang kita lakukan efektif menurunkan level frekuensi risiko Melaksanakan perubahan tindakan pengendalian untuk langkah-langkah pengendalian yang menunjukkan tren level frekuensi risiko tetap/meningkat dengan langkah-langkah pengendalian dengan kemampuan efektivitas yang lebih baik			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Lampiran J

Halaman ini sengaja dikosongkan

J.1 CPAR Area III Kerangka Kerja

Form 18.1 CPAR Kerangka Kerja 4.1

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Kebijakan dan prosedur keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

DJPBN sudah memiliki sejumlah kebijakan terkait pengelolaan keamanan informasi dan telah melaksanakan sejumlah tindakan pengamanan berdasarkan kepada KMK.479/KMK.01/2010 tentang kebijakan dan prosedur keamanan informasi namun sejumlah kebijakan (berdasar 11 area) belum semuanya memiliki petunjuk teknis dan prosedur pelaksanaan pengamanan pada tingkat Eselon II Kanwil DJPBN Jawa Timur

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan tujuan serta ruang lingkup keamanan informasi yang ada di KANWIL DJPBN terutama untuk cakupan yang lebih spesifik terkait dengan pelaksanaan teknis pengelolaan keamanan informasi

Menentukan kesesuaian kebijakan dan prosedur keamanan infomasi dengan kebijakan dan keamanan infomasi DJPBN secara umum berdasarkan undang-undang

Mendefinisikan peran dan tanggung jawab keamanan infomasi di dalamnya berdasarkan KMK No.479/KMK.01/2010 tentang peran dan tanggungjawab pengelola keamanan informasi termasuk peran dan tanggungjawab Information Security (IS) Manager dan Information Security (IS) Officer

Merujuk referensi dari peraturan instansi, serta peraturan kepatuhan keamanan informasi lain yang terkait.

Membuat kontrol pengendalian pengelolaan keamanan informasi sesuai dengan proses bisnis KANWIL DJPBN dalam bentuk prosedur, instruksi kerja, petunjuk pelaksanaan (juklak), petunjuk teknis (juknis) berdasarkan Pengendalian Umum KMK No.479/KMK.01/2010 Untuk dapat menuju pada tingkat keamanan yang lebih tinggi, kepatuhan pada kebijakan dan prosedur sebaiknya dievaluasi berkala tiap bulan atau semester. Setiap laporan evaluasi hendaknya didokumentasikan secara resmi dan dikomunikasikan serta disosialisasikan kepada semua pihak pelaksana DJPBN			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.2 CPAR Kerangka Kerja 4.2

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Kebijakan keamanan informasi telah sebagian ditetapkan secara formal, dipublikasikan kepada pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya, namun belum terdapat kesediaan semua pihak untuk mengetahui lebih lanjut perihal keamanan informasi dan masih mjemiliki anggapan bahwa pelaksanaannya merupakan tanggung jawab suatu Seksi misal : STA atau suatu Bidang saja misal : SKKI

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Melakukan penghimpunan perundang-undangan, peraturan dan prosedur terkait keamanan informasi dalam satu buku sebagaimana dilakukan pada perundang-undangan terkait organisasi yang dihimpun selama ini.
Menggandakan keseluruhan perundang-undangan dalam jumlah yang dibutuhkan untuk dimiliki oleh setiap Pelaksana pada tiap Seksi
Menyiapkan seluruh kebijakan terkait dengan keamanan informasi pada website Kanwil DJPBN dan meminta kesediaan admin website untuk selalu mengupdate informasi terkait keamanan informasi secaraberkala
Mendefinisikan peran dan tanggung jawab pelaksana untuk keamanan infomasi di dalam lingkup Kanwil DJPBN
Menghimbau peran serta aktif seluruh pelaksana untuk mengetahui referensi pengamanan informasi dari peraturan instansi, serta peraturan kepatuhan keamanan informasi lain yang terkait. Misal : kebijakan dan himnbauan terkait keamanan informasi dari Kominfo, dan peraturan hukum lainnya terkait pengamaan informasi institusi pemerintah

Untuk dapat menuju pada tingkat keamanan yang lebih tinggi, kepatuhan pada kebijakan dan prosedur sebaiknya dievaluasi berkala tiap bulan atau tiap semester. Setiap laporan evaluasi harus didokumentasikan secara resmi dan dikomunikasikan kepada semua pihak pelaksana Kanwil DJPBN			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.3 CPAR Kerangka Kerja 4.3

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Mekanisme pengelolaan dokumen kebijakan dan prosedur organisasi sudah diterapkan namun untuk yang spesifik mengenai keamanan informasi masih tidak menjadi perhatian khusus dalam proses pengelolaan dokumen di KANWIL DJPBN. Selain itu, kendala kondisi saat ini, kebijakan dan prosedur belum diperbarui atau dimutakhirkan berdasarkan kebutuhan spesifik Kanwil DJPBN Jawa Timur.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Melaksanakan mekanisme pengelolaan keseluruhan dokumen terkait keamanan informasi berdasarkan KMK.21/KMK.01/2012 dengan sejumlah penyempurnaan agar pengendalian internal pada pengelolaan keamanan informasi menjadi lebih baik,.

Mengevaluasi rancangan kebijakan /rancangan prosedur sesuai dengan hasil review kebijakan / prosedur sebelumnya

Melakukan pengelolaan peredaran dokumen kebijakan dan prosedur keamanan berdasarkan tiap bagiannya.

Penggunaan daftar induk nomor registrasi dokumen secara khusus / spesifik agar memudahkan pemilahannya dari dokumen pengelolaan lainnya

Penggunaan list / daftar dokumen yang selalu diupdate setiap kali terjadi penambahan dokumen terkait pengelolaan keamanan informasi

Melaksanakan pengelolaan kontrol akses dokumen kebijakan dan prosedur terutama untuk pihak ketiga yang terkait di dalamnya.

Sebagai upaya meningkatkan Tingkat Kematangan level III hingga level V,

maka KANWIL DJPBN sebaiknya melakukan evaluasi berkala terhadap mekanisme atau prosedur pengelolaan dokumen kebijakan pengelolaan keamanan informasi sekaligus sebagai pembaruan terhadap kebijakan yang dipandang perlu untuk direvisi/ditarik peredarannya.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.4 CPAR Kerangka Kerja 4.4

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia mekanisme untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Pihak bagian KANWIL DJPBN sudah mempunyai mekanisme untuk mengkomunikasikan kebijakan-kebijakan namun belum secara spesifik mengarahkan pengkomunikasian pada keamanan informasi untuk pihak terkait serta pihak ketiga serta masih diatur secara insidentil (maintenance, sosialisasi, rapat dll), belum terdokumentasikan kedalam prosedur tertulis secara berkala

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan pihak ketiga yang terkait beserta tingkat availabilitas misal : pihak ketiga yang masih se-instansi dan eksternal non-instansi
Menentukan tingkat sekuritas dari tiap definisi pihak ketiga yang ada
Menetukan kontrol akses berdasarkan tingkat sekuritas pihak ketiga
Menyiapkan saluran komunikasi secara lebih luas untuk setiap perubahan kebijakan dan prosedur terkait keamanan informasi bagi pihak ketiga
Untuk perubahan dan rancangan kebijakan dan prosedur disosialisakan kepada pihak ketiga yang terlibat dalam pengadaan, pengembangan dan pemeliharaan sistem informasi secara tertulis
Guna keperluan peningkatan ke Tingkat Kematangan pada level III hingga V maka pihak KANWIL DJPBN sebaiknya melakukan evaluasi berkala terhadap pendokumentasian kebijakan dan prosedur terkait pengelolaan keamanan informasi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 18.5 CPAR Kerangka Kerja 4.5

<table>
<tr><td colspan="4"> 

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR
GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640</td></tr>
<tr><td colspan="4">Section 1 : Obyek</td></tr>
<tr><td colspan="4">Keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi</td></tr>
<tr><td>Nama & TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
<tr><td colspan="4">Section 2 : Penyebab / Pendukung</td></tr>
<tr><td colspan="4">DJPBN dalam proses menerapkan prosedur keamanan informasi wajib merefleksikan kebutuhan mitigasi dari kerangka kerja pengelolaan risiko (mis : KMK. 479/KMK.01/2010 Poin VI Pengelolaan Komunikasi dan Operasional merefleksikan pengendalian scanning sebelum mengupload ADK Bank/Pos Persepsi dalam TRP dan instalasi antivirus terupdate pada LHPPI.</td></tr>
<tr><td>Nama & TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
<tr><td colspan="4">Section 3 : Usulan tindakan perbaikan</td></tr>
<tr><td colspan="4">Mendefinisikan tujuan serta ruang lingkup keamanan informasi yang ada di KANWIL DJPBN
Menentukan kesesuaian kebijakan dan prosedur keamanan infomasi dengn kebijakan dan keamanan infomasi organisasi secara umum
Mendefinisikan peran dan tanggung jawab keamanan infomasi di dalamnya
Merujuk analisis kebijakan dan prosedur pengelolaan keamanan informasi pada seluruh referensi dari peraturan instansi, serta peraturan kepatuhan keamanan informasi lain yang terkait. Misal : KMK.479/KMK.01/2010, KMK.512.KMK.01/2010, dan peraturan hukum lainnya
Merujuk dari hasil identifikasi risiko sebagaimana CPAR pada Area Risiko
Membuat kontrol pengendalian sesuai dengan proses bisnis Kanwil DJPBN
Mengkomunikasikan rancangan dan hasil kebijakan dan prosedur keamanan informasi dengan seluruh pelaksana serta pihak ketiga yang terkait.</td></tr>
<tr><td>Nama & TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
</table>

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 18.6 CPAR Kerangka Kerja 4.6

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset tercantum dalam kontrak dengan pihak ketiga

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Pihak DJPBN telah menerapkan sejumlah aspek keamanan informasi seperti pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset sebagaiaman tercantum dalam KMK.479 Poin XI, KMK.512, KMK.351 dan sejumlah peraturan lainnya namun pengimplementasian dalam kontrak pihak ketiga yang dikelola Kanwil masih dilakukan secara informal & belum tertulis.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan pihak ketiga yang terkait beserta tingkat availabilitas pihak ketiga tersebut, misal : pihak ketiga yang masih se-instansi dan eksternal non-instansi

Menentukan tingkat sekuritas dari tiap definisi pihak ketiga yanga tertuang dalam kontrak

Menetukan kontrol akses berdasarkan tingkat sekuritas pihak ketiga

Untuk perubahan dan rancangan kebijakan dan prosedur keamanan informasi wajib disosialisakan kepada pihak ketiga

Menentukan aset yang terkait dengan pihak ketiga

Menyusun *checklist review* mengenai proses *change management* dari kebijakan dan prosedur yang telah disusun oleh organisasi.

Guna keperluan eskalasi ke Tingkat Kematangan pada level III hingga V maka pihak KANWIL DJPBN sebaiknya melakukan evaluasi berkala terhadap *checklis*t. Jika terdapat kelemahan, maka segera dilakukan perubahan terhadap kebijakan / prosedur tersebut

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.7 CPAR Kerangka Kerja 4.7

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

DJPBN dalam proses menerapkan sebagian sanksi atau konsekuesi pelanggaran kebijakan keamanan informasi berdasarkan perundang-undangan. Belum ditemukan hingga saat ini pelanggaran terkait keamanan informasi namun jika ditemukan dilakukan penerapan Sanksi berdasar KMK 512/KMK.01/2010 poin 5 yakni Sanksi Teknis berupa penonaktifan akses dan Sanksi Administratif sesuai PP 30 th 1980 sebagaimana telah diubah dengan PP 53 Tahun 2010 tentang Peraturan Disiplin Pegawai Negeri Sipil

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan tujuan serta ruang lingkup keamanan informasi yang ada di lingkup Kanwil DJPBN
Menentukan kesesuaian kebijakan dan prosedur keamanan infomasi dengn kebijakan dan keamanan infomasi organisasi secara umum
Mendefinisikan peran dan tanggung jawab pelaksanaan keamanan infomasi di dalamnya
Merujuk kebijakan dan prosedur pada referensi dari peraturan instansi, serta peraturan kepatuhan keamanan informasi lain yang terkait. Misal : KMK.512/KMK.01/2010 beserta seluruh aturan tentang larangan dan sanksinya, peraturan hukum lain yang terkait
Merujuk pada hasil identifikasi risiko
Membuat kontrol pengendalian sesuai dengan proses bisnis Kanwil DJPBN
Mengkomunikasikan rancangan dan hasil kebijakan dan prosedur keamanan informasi termasuk konsekwensi pelanggaran kebijakan keamanan informasi dengan pelaksana serta pihak ketiga terkait

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.8 CPAR Kerangka Kerja 4.8

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

DJPBN dalam proses menerapkan sebagian sanksi atau konsekuesi pelanggaran kebijakan keamanan informasi berdasarkan perundang-undangan. Belum ditemukan hingga saat ini pelanggaran terkait keamanan informasi namun jika ditemukan dilakukan penerapan Sanksi berdasar KMK 512/KMK.01/2010 poin 5 yakni Sanksi Teknis berupa penonaktifan akses dan Sanksi Administratif sesuai PP 30 th 1980 sebagaimana telah diubah dengan PP 53 Tahun 2010 tentang Peraturan Disiplin Pegawai Negeri Sipil

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan tujuan serta ruang lingkup keamanan informasi yang ada di lingkup Kanwil DJPBN
Menentukan kesesuaian kebijakan dan prosedur keamanan infomasi dengn kebijakan dan keamanan infomasi organisasi secara umum
Mendefinisikan peran dan tanggung jawab pelaksanaan keamanan infomasi di dalamnya
Merujuk kebijakan dan prosedur pada referensi dari peraturan instansi, serta peraturan kepatuhan keamanan informasi lain yang terkait. Misal : KMK.512/KMK.01/2010 beserta seluruh aturan tentang larangan dan sanksinya, peraturan hukum lain yang terkait
Merujuk pada hasil identifikasi risiko
Membuat kontrol pengendalian sesuai dengan proses bisnis Kanwil DJPBN
Mengkomunikasikan rancangan dan hasil kebijakan dan prosedur keamanan informasi termasuk konsekwensi pelanggaran kebijakan keamanan informasi dengan pelaksana serta pihak ketiga terkait

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.9 CPAR Kerangka Kerja 4.9

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi security patch, alokasi tanggungjawab untuk memonitor adanya rilis security patch baru, memastikan pemasangannya dan melaporkannya

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Pihak KANWIL DJPBN masih dalam proses menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi security patch, alokasi tanggung jawab, serta rilis security patch baru dan memastikan pemasangan serta pelaporan berdasarkan KMK 479/KMK.01/2010 Poin VIII &X. Pada umumnya hal-hal yang terkait dengan security patch dilaksanakan oleh Kantor Pusat DJPBN dan Pusintek

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefiinisikan dan menentukan daftar aplikasi atau sistem operasi serta versi lama dan terbarunya

Mengidentifikasi kelemahan rilis terbaru dan *security patch*-nya serta kesesuaian dengan kebutuhan proses bisnis Kanwil DJPBN khususnya pada aplikasi di luar SPAN yang masih beroperasi secara berkala

Mendaftar atau menyusun database aplikasi atau sistem operasi yang akan atau sudah di-*patch*

Melakukan *testing patch* sebelum diimplementasikan ke semua perangkat

Mendefinsiikan PIC bagian security (misal : tim keamanan informasi) guna mengkomunikasikan kepada semua pelaksana teknis.

Melakukan deploying pada semua perangkat sesuai daftar aset yang akan dideploy

Guna keperluan eskalasi ke Tingkat Kematangan pada level III hingga V maka pihak KANWIL DJPBN sebaiknya membuat laporan pengelolaan serta evaluasi

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.10 CPAR Kerangka Kerja 4.10

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Sistem terbaru yang diimplementasikan dalam lingkup DJPBN adalah SPAN. Namun sebagai sistem dengan tingkat pemenuhan kebutuhan lintas Direktorat maka evaluasi resiko dilakukan oleh Satker SPAN pada Kantor Pusat dengan mitigasi risiko yang tertuang dalam web SPAN yang menjelaskan tentang adanya DRC (Disaster Recovery Centre) SPAN sementara pada lingkup vertical identifikasi risiko terkait SPAN telah dilakukan namun belum ada mitigasi risko secara detil (implementasi SPAN berada pada masa transisi untuk 7 Kanwil & KPPN-KPPN yang diliputinya)

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mengidentifikasi pemasalahan yang ada pada sistem baru, apakah telah menunjukkan kesiapan untuk dilakukan rilis
Mendefiinisikan dan menentukan daftar sistem operasi serta klasifikasi versi lama dan terbarunya sesuai solusi permasalahan yang ada
Melakukan perencananaan finansial (investasi) serta evaluasi kelayakan sistem
Mengidentifikasi kelemahan sistem terbaru, tingkat kerentanan terhadap permasalahan, serta kesesuaiannya dengan kebutuhan proses bisnis Kanwil DJPBN
Mendaftar atau menyusun database sistem apa saja yang diperbarui
Melakukan *testing* sistem baru sebelum diimplementasikan pada semua perangkat yang terkena masalah
Mendefinsiikan PIC bagian *security* (misal : tim keamanan informasi) guna mengkomunikasikan kepada semua pelaksana teknis

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.11 CPAR Kerangka Kerja 4.11

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

KMK479/KMK01/2010 Poin VIII bagian 6 menyatakan kerentanan teknis dengan sejumlah pengamanan dan langkah-langkah jika patch tidak tersedia, namun tidak dijabarkan secara terperinci langkah–langkah tersebut dan jadwal penyelesaiannya dan di tingkat vertical belum dibuatkan juknis lebih lanjut. Fakta terkini tentang sistem terbaru yang diimplementasikan dalam lingkup DJPBN adalah SPAN. Untuk sementara pada lingkup vertical identifikasi risiko terkait SPAN telah dilakukan namun belum ada mitigasi risko secara detil berikut waktu penyelesaiannya (misal : implementasi SPAN yang berada pada masa transisi untuk 7 Kanwil & KPPN-KPPN yang diliputinya)

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mengidentifikasi risiko yang terjadi dari penerapan sistem baru
Mendefinisikan tindakan mitigasi sekaligus tindakan pengamanan baru atau *compensating control*
Menghitung kerugiana aset yang ada
Melakukan penjadwalan penyelesain masalah (tindakan korektif)
Melaksanakan langkah standar sebagaimana tertuang dalam KMK No.479 /KMK.01/2010 tentang Pengembangan Sistem Informasi dan Penanganan Insiden Keamanan Informasi lingkup DJPBN
Guna keperluan eskalasi ke Tingkat Kematangan pada level III hingga V maka pihak KANWIL DJPBN sebaiknya melakukan pemantauan dengan menyusun kontrol antara lain formulir tindakan mitigasi, *checklist* akibat dan dampak.

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.12 CPAR Kerangka Kerja 4.12

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

KMK 479/KMK.01/2010 Poin X telah menjelaskan kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan /konsideran keamanan informasi, termasuk uji-cobanya dengan fokus pada penyusunan rencana kelangsungan kegiatan dan cakupan ujicoba termasuk simulasi, *recovery*, *parallel recovery* dan uji perangkat. Namun untuk DJPBN hanya dilaksanakan pada Kantor Pusat dan tidak diturunkan perencanaan dan pelaksanaan DRP pada tingkat Eselon II

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Memahami risiko organisasi serta tingkat probabilitas
Mengidientifikasi semua aset yang kritis sesuai dengan proses bisnis yang ada
Menetukan dampak serta insiden yang kemungkinan akan muncul.
Mempertimbangkan jaminan atau garansi aset sebagai proses *business continuity plan*
Memastikan keamanan data dan informasi internal dari personel atau pelaksana keamanan
Mendokumentasikan *business continuity plan*
Melakukan testing serta update *business continuity plan*
Melaksanakan pelaporan secara berkala terhadap dokumen *business continuity plan* dan hasil testing serta update *business continuity plan*

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama &			

TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.13 CPAR Kerangka Kerja 4.13

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KMK 479/KMK.01/2010 Poin X telah menjelaskan kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan komposisi, peran, wewenang dan tanggung jawab tim dengan focus pada Unit Eselon I dan mencakup identifikasi risiko, identifikasi aset informasi, identifikasi sumber daya, memastikan keselamatan pegawai dan keamanan perangkat, pendokumentasian dan ujicoba secara berkala. Namun untuk lingkup Kanwil DJPBN belum diimplementasikan

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Menentukan tujuan dan ruang lingkup Disaster Recovery Plan atau yang biasa disebut DRP
Menentukan tim pembentuk DRP
Melakukan penilaian risiko bencana dari kerangka kerja pengelolaan risiko sebelumnya
Mengidentifikasi Daftar layanan TI yang dipandang kritikal
Menetapkan kunci bisnis kritis dari KANWIL DJPBN sebagai upaya proses implementasi DRP nantinya
Mendefinisikan kebutuhan perencanaan seperti risiko serta tindakan mitigasi yang terdapat pada dokumen kerangka kerja pengelolaan risiko
Merujuk referensi dari dokumen BCP serta mengintegrasikan antara keduanya
Melakukan testing pada level disaster yang rendah
Melakukan evaluasi dan pelaporan sebagai upaya menuju peningkatan ke Tingkat Kematangan level III hingga V.

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.14 CPAR Kerangka Kerja 4.14

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Uji-coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah dilakukan sesuai jadwal

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**

Section 2 : Penyebab / Pendukung

KMK 479/KMK.01/2010 Poin X telah menjelaskan kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan /konsideran keamanan informasi, termasuk uji-cobanya dengan focus tim keamanan informasi pada eselon I sehingga tidak ditemukan ujicoba pelaksanaan pada Eselon II.

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**

Section 3 : Usulan tindakan perbaikan

Menentukan tujuan dan ruang lingkup Disaster Recovery Plan atau yang biasa disebut DRP
Menentukan tim pembentuk DRP
Melakukan penilaian risiko bencana dari kerangka kerja pengelolaan risiko sebelumnya
Menetapkan kunci bisnis kritis dari KANWIL DJPBN sebagai upaya proses implementasi DRP nantinya
Mendefinisikan kebutuhan perencanaan seperti risiko serta tindakan mitigasi yang terdapat pada dokumen kerangka kerja pengelolaan risiko
Merujuk referensi dari dokumen BCP serta mengintegrasikan antara keduanya
Melakukan testing pada level disaster yang rendah
Melakukan evaluasi dan pelaporan sebagai upaya menuju peningkatan ke Tingkat Kematangan level III hingga V.

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 18.15 CPAR Kerangka Kerja 4.15

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Hasil dari perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KMK 479/KMK.01/2010 Poin X telah menjelaskan kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mengharuskan analisis dampak kegiatan melibatkan pemilik proses bisnis dan dievaluasi secara berkala untuk memastikan efektifitasnya.Hal yang ditemui dalam observasi adalah focus tim keamanan informasi pada eselon I sehingga tidak ditemukan prosedur ujicoba berikut pembenahan pada Eselon II (Kanwil DJPBN Jawa Timur).

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Melakukan testing pada level disaster yang rendah
Melakukan evaluasi dan pelaporan
Jika terdapat kegagalan, maka perlu adanya *change management* pada *update* DRP sesuai dengan kompleksitas permasalahan yang ada
Untuk meningkatkan Tingkat Kematangan level III hingga level V maka KANWIL DJPBN sebaiknya menyusun dokumen DRP berdasarkan risiko dan disaster yang ada
Dokumen DRP hendaknya dikomunikasikan, dan disosialisasikan pada seluruh pelaksana Kanwil DJPBN

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 18.16 CPAR Kerangka Kerja 4.16

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

DJPBN telah menerapkan evaluasi seluruh kebijakan dan prosedur yang dilaksanakan sepenuhnya oleh Bagian Organisasi dan Tata Laksana dan untuk Kanwil DJPBN dilaksanakan oleh SKKI melalui LPPPI triwulanan yang merupakan gabungan seluruh laporan pengendalian internal KPPN. Namun belum ada penspesifikasian khusus terkait dengan keamanan informasi karena pengelolaan keamanan informasi dilaporkan sebgai bagian dari proses bisnis organisasi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Melaksanakan mekanisme pengelolaan keseluruhan dokumen terkait keamanan informasi berdasarkan KMK.21/KMK.01/2012 dengan sejumlah penyempurnaan agar pengendalian internal pada pengelolaan keamanan informasi menjadi lebih baik,.

Mengevaluasi rancangan kebijakan /rancangan prosedur sesuai dengan hasil review kebijakan / prosedur sebelumnya

Melakukan pengelolaan peredaran dokumen kebijakan dan prosedur keamanan berdasarkan tiap bagiannya.

Penggunaan daftar induk nomor registrasi dokumen secara khusus / spesifik agar memudahkan pemilahannya dari dokumen pengelolaan lainnya

Penggunaan list / daftar dokumen yang selalu diupdate setiap kali terjadi penambahan dokumen terkait pengelolaan keamanan informasi

Melaksanakan pengelolaan kontrol akses dokumen kebijakan dan prosedur terutama untuk pihak ketiga yang terkait di dalamnya.

Sebagai upaya meningkatkan Tingkat Kematangan level III hingga level V,

maka KANWIL DJPBN sebaiknya melakukan evaluasi berkala terhadap mekanisme atau prosedur pengelolaan dokumen kebijakan pengelolaan keamanan informasi sekaligus sebagai pembaruan terhadap kebijakan yang dipandang perlu untuk direvisi/ditarik peredarannya.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.17 CPAR Kerangka Kerja 4.17

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisis risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Tingkatan kebijakan strategis dalam DJPBN umunya dituangkan dalam bentuk PP, PMK, KMK, KM dan peraturan yang setingkat. Esensi peraturan - peraturan tersebut adalah kebijakan dan standar yang menjadi bagan dari rencana kerja organisasi. Keseluruhan peraturan juga merupakan hasil analisis risiko dari sejumlah penerapan keamanan informasi yang masuk dalam lingkup TIK sebagai bagian penting dalam proses bisnis dan rencana kerja organisasi sehingga selalu memunculkan langkah pengendalian dan evaluasi berkala dalam tiap kebijakan yang ada.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan tujuan serta ruang lingkup keamanan informasi yang ada di KANWIL DJPBN

Menentukan kesesuaian kebijakan dan prosedur keamanan infomasi dengn kebijakan dan keamanan infomasi organisasi secara umum

Mendefinisikan peran dan tanggung jawab keamanan infomasi di dalamnya

Merujuk analisis kebijakan dan prosedur pengelolaan keamanan informasi pada seluruh referensi dari peraturan instansi, serta peraturan kepatuhan keamanan informasi lain yang terkait. Misal : KMK.479/KMK.01/2010, KMK.512.KMK.01/2010, dan peraturan hukum lainnya

Standar keamanan infomasi atau yang biasa disebut SMKI merupakan satu kesatuan dalam kebijakan, prosedur, program, BCP, dan DRP serta berbagai aspek manajemen serta teknis dalam keamanan informasi

Merujuk pada hasil identifikasi risiko sebagaimana CPAR pada Area Risiko

Membuat daftar risiko dalam proses bisnis terkait Membuat skala risiko hingga tingkat probablitas kejadiannya Menentukan tindakan mitigasi dan pengendalian risiko Membuat kontrol pengendalian sesuai dengan proses bisnis Kanwil DJPBN Mengkomunikasikan rancangan pengendalian dan hasil kebijakan dan prosedur keamanan informasi berdasarkan analisis risiko dengan seluruh pelaksana serta pihak ketiga yang terkait.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.18 CPAR Kerangka Kerja 4.18

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Tingkatan kebijakan strategis dalam DJPBN umunya dituangkan dalam bentuk PP, PMK, KMK, KM dan peraturan yang setingkat. Esensi peraturan - peraturan tersebut adalah kebijakan dan standar yang menjadi bagan dari rencana kerja organisasi. Keseluruhan peraturan juga merupakan hasil analisis risiko sebagai konsekuensi logis dari kebutuhan dan perubahan profil risiko dari sejumlah penerapan keamanan informasi yang masuk dalam lingkup TIK sebagai bagian penting dalam proses bisnis dan rencana kerja organisasi sehingga selalu memunculkan langkah pengendalian dan evaluasi berkala dalam tiap kebijakan yang ada.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan tujuan serta ruang lingkup keamanan informasi yang ada di KANWIL DJPBN

Menentukan kesesuaian kebijakan dan prosedur keamanan infomasi dengn kebijakan dan keamanan infomasi organisasi secara umum

Mendefinisikan peran dan tanggung jawab keamanan infomasi di dalamnya

Merujuk analisis kebijakan dan prosedur pengelolaan keamanan informasi pada seluruh referensi dari peraturan instansi, serta peraturan kepatuhan keamanan informasi lain yang terkait. Misal : KMK.479/KMK.01/2010, KMK.512.KMK.01/2010, dan peraturan hukum lainnya

Standar keamanan infomasi atau yang biasa disebut SMKI merupakan satu kesatuan dalam kebijakan, prosedur, program, BCP, dan DRP serta berbagai aspek manajemen serta teknis dalam keamanan informasi

Merujuk pada hasil identifikasi risiko sebagaimana CPAR pada Area Risiko Membuat daftar risiko dalam proses bisnis terkait Membuat skala risiko hingga tingkat probablitas kejadiannya Menentukan tindakan mitigasi dan pengendalian risiko Membuat kontrol pengendalian sesuai dengan proses bisnis Kanwil DJPBN Mengkomunikasikan rancangan pengendalian dan hasil kebijakan dan prosedur keamanan informasi berdasarkan analisis risiko dengan seluruh pelaksana serta pihak ketiga yang terkait.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.19 CPAR Kerangka Kerja 4.19

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Sebagaimana KMK dan PMK yang telah disampaikan sebelumnya. TIK juga menjadi sasaran strategis seluruh unit vertical DJPBN tentang Pemanfaatan TIK secara optimal. Disamping itu Rencana Strategis Kementerian Keuangan juga menyatakan perlunya kebijakan-kebijakan, standar, dan prosedur berkaitan dengan operasionalisasi teknologi informasi dan komunikasi seperti yang terkait dengan tata kelola yang baik (good IT governance),pengelolaan layanan (IT service management), pengelolaan kesinambungan bisnis (business continuity management) beserta seluruh kelengkapan seperti Disaster Recover Plan dan Disaster Recover Center, keamanan sistem informasi (IT security management), dan pengelolaan sumber daya informasi (termasuk yang berkaitan dengan masalah lisensi software) sebagai bagian dari pelaksanaan program kerja organisasi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan tujuan serta ruang lingkup keamanan informasi yang ada di KANWIL DJPBN

Menentukan kesesuaian kebijakan dan prosedur keamanan infomasi dengn kebijakan dan keamanan infomasi organisasi secara umum

Mendefinisikan peran dan tanggung jawab keamanan infomasi di dalamnya

Merujuk analisis kebijakan dan prosedur pengelolaan keamanan informasi pada seluruh referensi dari peraturan instansi, serta peraturan kepatuhan keamanan informasi lain yang terkait. Misal : KMK.479/KMK.01/2010, KMK.512.KMK.01/2010, dan peraturan hukum lainnya

Standar keamanan infomasi atau yang biasa disebut SMKI merupakan satu

kesatuan dalam kebijakan, prosedur, program, BCP, dan DRP serta berbagai aspek manajemen serta teknis dalam keamanan informasi Merujuk pada hasil identifikasi risiko sebagaimana CPAR pada Area Risiko Membuat daftar risiko dalam proses bisnis terkait Membuat skala risiko hingga tingkat probablitas kejadiannya Menentukan tindakan mitigasi dan pengendalian risiko Membuat kontrol pengendalian sesuai dengan proses bisnis Kanwil DJPBN Mengkomunikasikan rancangan pengendalian dan hasil kebijakan dan prosedur keamanan informasi berdasarkan analisis risiko dengan seluruh pelaksana serta pihak ketiga yang terkait. Menjadikan keseluruhan strategi penerapan keamanan informasi sebagai bagian dari pelaksanaan program kerja organisasi yang tertuang dalam SS (sasaaran strategis) dan dirincikan dalam SFO (*strategy focused organization*)			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.20 CPAR Kerangka Kerja 4.20

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Pelaksanaan audit internal lingkup DJPBN dilaksanakan oleh Inspektorat Jenderal berdasar Standar Audit Inspektorat Jenderal (SAINS). Cakupannya adalah seluruh aset, kebijakan, prosedur dan pelaksanaan. KANWIL DJPBN sendiri memiliki dan melaksanakan program audit internal yang dikenal dengan istilah pengendalian internal yang dilakukan oleh SKKI sebagai pihak independen dengan cakupan kepatuhan pelaksanaan kebijakan dan prosedur secara berkala namun dibutuhkan pula sebuah audit internal yang spesifik terkait dengan pengelolaan keamanan informasi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan peran serta tanggung jawab pelaksana pengamanan informasi secara jelas dalam bentuk dokumen tertulis
Mengkoordinasikan tanggung jawab pengelolaan keamanan informasi dengan tim/personel pengamanan informasi
Jika untuk kebutuhan audit, maka dapat dibentuk tim pengamanan sendiri guna kebutuhan audit namun tidak harus terpisah dengan unit yang ada.
Melakukan internal audit Kanwil DJPBN mengenai strategi manajemen keamanan informasi yang telah disusun. Namun tidak hanya internal, audit juga dilaksanakan oleh pihak eksternal
Mempersiapkan perlengkapan kebutuhan audit seperti kontrol audit berdasarkan SMKI
Mendokumentasikan hasil serta review dari audit internal

<table>
<tr><td colspan="4">Mendefinisikan tindakan kesesuaian (validasi) sesuai bukti yang ada
Menentukan tindakan korektif serta mitigasi
Untuk meningkatkan peran pengelolaan keamanan informasi menuju Tingkat Kematangan level III hingga V, maka KANWIL DJPBN sebaiknya melakukan evaluasi secara berkala pada tiap kinerja pelaksanaan pengamanan informasi. Selain itu, Kanwil DJPBN sebaiknya melakukan evaluasi kebijakan berkala untuk menyesuaikan dengan kebutuhan bisnisnya dan melakukan perubahan struktur peran pelaksana / tanggung jawab jika memang dibutuhkan.</td></tr>
<tr><td>Nama
&
TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
<tr><td colspan="4">Section 4 : Tindak lanjut dan verifikasi</td></tr>
<tr><td colspan="4">Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera</td></tr>
<tr><td>Nama
&
TTD</td><td colspan="2">Disposisi oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
</table>

Form 18.21 CPAR Kerangka Kerja 4.21

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

DJPBN sebagai pelaksana renstra kementerian keuangan telah merencanakan pengendalian internal untuk mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi yang diawali dengan pelaksanaan tes online keamanan informasi yang diselenggarakan melalui media website SPAN. Kedepan pengendalian keamanan informasi diharuskan tercakup dalam bentuk pengendalian internal sambil menunggu juga audit keamanan informasi oleh Itjen yang menjadi program Kominfo pada seluruh Kementerian/Lembaga

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan peran serta tanggung jawab pelaksana pengamanan informasi secara jelas dalam bentuk dokumen tertulis
Mengkoordinasikan tanggung jawab pengelolaan keamanan informasi dengan tim/personel pengamanan informasi
Jika untuk kebutuhan audit, maka dapat dibentuk tim pengamanan sendiri guna kebutuhan audit namun tidak harus terpisah dengan unit yang ada.
Melakukan internal audit Kanwil DJPBN mengenai strategi manajemen keamanan informasi yang telah disusun. Namun tidak hanya internal, audit juga dilaksanakan oleh pihak eksternal
Mempersiapkan perlengkapan kebutuhan audit seperti kontrol audit berdasarkan SMKI
Mendokumentasikan hasil serta review dari audit internal
Mendefinisikan tindakan kesesuaian (validasi) sesuai bukti yang ada
Menentukan tindakan korektif serta mitigasi
Untuk meningkatkan peran pengelolaan keamanan informasi menuju Tingkat

Kematangan level III hingga V, maka KANWIL DJPBN sebaiknya melakukan evaluasi secara berkala pada tiap kinerja pelaksanaan pengamanan informasi untuk menganalisis tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi . Selain itu, Kanwil DJPBN sebaiknya melakukan evaluasi kebijakan berkala untuk menyesuaikan dengan kebutuhan bisnisnya dan melakukan perubahan struktur peran pelaksana / tanggung jawab jika memang dibutuhkan.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.22 CPAR Kerangka Kerja 4.22

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

DJPBN sebagai pelaksana renstra kementerian keuangan telah merencanakan pengendalian internal untuk mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi yang diawali dengan pelaksanaan tes online keamanan informasi yang diselenggarakan melalui media website SPAN. Kedepan pengendalian keamanan informasi tercakup dalam bentuk pengendalian internal sambil menunggu juga audit keamanan informasi oleh Itjen yang menjadi program Kominfo pada seluruh Kementerian/Lembaga

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan peran serta tanggung jawab pelaksana pengamanan informasi secara jelas dalam bentuk dokumen tertulis
Mengkoordinasikan tanggung jawab pengelolaan keamanan informasi dengan tim/personel pengamanan informasi
Jika untuk kebutuhan audit, maka dapat dibentuk tim pengamanan sendiri guna kebutuhan audit namun tidak harus terpisah dengan unit yang ada.
Melakukan internal audit Kanwil DJPBN mengenai strategi manajemen keamanan informasi yang telah disusun. Namun tidak hanya internal, audit juga dilaksanakan oleh pihak eksternal
Mempersiapkan perlengkapan kebutuhan audit seperti kontrol audit berdasarkan SMKI
Mendokumentasikan hasil serta review dari audit internal
Mendefinisikan tindakan kesesuaian (validasi) sesuai bukti yang ada
Menentukan tindakan korektif serta mitigasi

Untuk meningkatkan peran pengelolaan keamanan informasi menuju Tingkat Kematangan level III hingga V, maka KANWIL DJPBN sebaiknya melakukan evaluasi secara berkala pada tiap kinerja pelaksanaan pengamanan informasi untuk menganalisis tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi . Selain itu, Kanwil DJPBN sebaiknya melakukan evaluasi kebijakan berkala untuk mengidentifikasi langkah pembenahan dan pencegahan, dan melakukan perubahan struktur peran pelaksana / tanggung jawab beserta inisiatif peningkatan kinerja keamanan informasi jika memang dibutuhkan.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.23 CPAR Kerangka Kerja 4.23

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

DJPBN sebagai pelaksana renstra kementerian keuangan telah merencanakan pengendalian internal untuk mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi yang diawali dengan pelaksanaan tes online keamanan informasi yang diselenggarakan melalui media website SPAN. Kedepan pengendalian keamanan informasi tercakup dalam bentuk pengendalian internal sambil menunggu juga audit keamanan informasi oleh Itjen yang menjadi program Kominfo pada seluruh Kementerian/Lembaga

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan peran serta tanggung jawab pelaksana pengamanan informasi secara jelas dalam bentuk dokumen tertulis
Mengkoordinasikan tanggung jawab pengelolaan keamanan informasi dengan tim/personel pengamanan informasi
Jika untuk kebutuhan audit, maka dapat dibentuk tim pengamanan sendiri guna kebutuhan audit namun tidak harus terpisah dengan unit yang ada.
Melakukan internal audit Kanwil DJPBN mengenai strategi manajemen keamanan informasi yang telah disusun. Namun tidak hanya internal, audit juga dilaksanakan oleh pihak eksternal
Mempersiapkan perlengkapan kebutuhan audit seperti kontrol audit berdasarkan SMKI
Mendokumentasikan dan melaporkan hasil serta review dari audit internal
Mendefinisikan tindakan kesesuaian (validasi) sesuai bukti yang ada
Menentukan tindakan korektif serta mitigasi
Untuk meningkatkan peran pengelolaan keamanan informasi menuju Tingkat

Kematangan level III hingga V, maka KANWIL DJPBN sebaiknya melakukan evaluasi secara berkala pada tiap kinerja pelaksanaan pengamanan informasi untuk menganalisis tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi . Selain itu, Kanwil DJPBN sebaiknya melakukan evaluasi kebijakan berkala untuk mengidentifikasi langkah pembenahan dan pencegahan, dan melakukan perubahan struktur peran pelaksana / tanggung jawab beserta inisiatif peningkatan kinerja keamanan informasi jika memang dibutuhkan.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.24 CPAR Kerangka Kerja 4.24

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisis untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

DJPBN dalam menetapkan suatu kebijakan dan prosedur pasti melakukan analisis untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya. SPAN sebagai wujud pengimplementasian perubahan dan struktur penganggaran dan perbendaharaan sendiri ditunjang oleh kebijakan khusus dan infrastruktur yang diatur tersendiri dan terpisah dari infrastruktur yang dimiliki unit vertical DJPBN. Terlepas dari kebijakan yang umumnya ditentukan oleh Kantor Pusat, prosedur dan panduan di tingkat Kanwil seharusnya memunculkan analisis aspek finansial, analisis terhadap infrastruktur dan analisis pengelolaan perubahan

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Jika terdapat pengubahan dalam kebijakan / prosedur, atau pengelolaan keamanan, maka langkah awal adalah mendaftar semua perubahan yang ada
Mendefinisikan aset atau sistem yang terkenadampak perubahan
Menentukan tindakan korektif perubahan
Melakukan perencanaan secara strategis mengenai kondisi eksisting, finansial serta kebutuhan proses bisnis saat ini
Melakukan reviu untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan
Memastikan rencana dan anggaran *annual support* yang mencakup reviu dan sistem testing dari perubahan

Memastikan pemberitahuan pada perubahan dilakukan dalam jangka waktu yang tepat untuk memastikan tes dan reviu telah dilaksanakan sebelum implementasi Memastikan bahwa perubahan telah diselaraskan dengan rencana kelangsungan kegiatan (BCM).			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 18.25 CPAR Kerangka Kerja 4.25

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada untuk memastikan bahwa keseluruhan inisiatif tersebut telah diterapkan secara efektif

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

DJPBN sebagai pelaksana renstra kementerian keuangan telah merencanakan pengendalian internal untuk mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi yang diawali dengan pelaksanaan tes online keamanan informasi yang diselenggarakan melalui media website SPAN. Kedepan evaluasi keamanan informasi tercakup dalam bentuk pengendalian internal sambil menunggu juga audit kepatuhan keamanan informasi oleh Itjen yang menjadi program Kominfo pada seluruh Kementerian/ Lembaga. Secara pasti, Kanwil DJPBN belum mempunyai prosedur lengkap sebagai turunan SMKI yang menjadi pedoman keamanan informasi tingkat Kanwil sehingga masih belum adanya tindakan "*compliance testing*" yang spesifik bagi pelaksana pengaman informasi

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan kategori dan prioritas kepatuhan yang ada pada lingkup Kanwil DJPBN

Memastikan kebutuhan pelaporan kepatuhan untuk semua pengelolaan keamanan yang terjadi di lapangan seperti adanya logbook, checklist, ataupun record yang wajib ada dalam penilaian kepatuhan

Melakukan pengimplementasian prosedur-prosedur yang tepat untuk memastikan kesesuaiannya dengan perundangan, peraturan dan perjanjian kontrak

Memastikan kepatuhan terhadap persyaratan hukum, kepatuhan terhadap kebijakan keamanan informasi, dan kepatuhan terhadap spesifikasi teknis

<table>
<tr><td colspan="4">keamanan informasi sesuai dengan peraturan dan regulasi yang ada
Menyusun prosedur pelaporan pengamanan informasi yang telah diatur dalam kebijakan.
Menjalankan audit / pengendalian internal, mendokumentasikannya dan melaporkan kepada pimpinan
Melakukan pengumpulan data atas keseluruhan bukti laporan sebagai upaya pendisiplinan pelaporan
Melakukan sistem reward dan punishment.
Melaksanakan evaluasi kepatuhan secara berkala</td></tr>
<tr><td>Nama & TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
<tr><td colspan="4">Section 4 : Tindak lanjut dan verifikasi</td></tr>
<tr><td colspan="4">Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera</td></tr>
<tr><td>Nama & TTD</td><td colspan="2">Disposisi oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
</table>

Form 18.26 CPAR Kerangka Kerja 4.26

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN telah mempunyai perencanaan jangka panjang (1-3-5 tahun) sebagai turunan dari strategis intansi (DJPBN) namun memang program keamanan informasi masih diterapkan sebagian (belum terdokumentasi secararesmi)

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Menentukan standar SMKI yang akan dipakai dalam hal ini KMK No.479 /KMK.01/2010
Menentukan tujuan serta ruang lingkup strategi keamanan informasi di KANWIL DJPBN
Menurunkan kebijakan selama ini kedalam dokumen kebijakan keamanan informasi Kanwil DJPBN, didokumentasikan, dikomunikasikan dan dipublikasikan kepada seluruh pegawai dan pihak-pihak lain yang relevan
Menciptakan rencana strategis organisasi terkait keamanan informasi
Target dan sasaran diturunkan dari rencana strategis dan kebijakan organisasi (KANWIL DJPBN) terkait pengelolaan keamanan informasi
Menyusun indikator kuantitatif guna dapat menghitung capaian tiap target pengelolaan keamanan informasi yang ada.
Target dan sasaran yang sudah ditetapkan sebaiknya dikomunikasikan dan dipublikasikan kepada pihak terkait seperti pihak pelaksana dan pihak ketiga.
Untuk menuju tingkat kematangan III atau yang lebih tinggi maka KANWIL DJPBN harus juga mempunyai kerangka kerja risiko terdokumentasi secara resmi yang detailnya seperti tersebut di atas. Selain itu terdapat proses evaluasi

berkala seperti kontrol pengendalian yang dilaporkan secara mingguan, bulanan, atau secara umum tahunan			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Lampiran K

Halaman ini sengaja dikosongkan

K.1 CPAR Area IV Pengelolaan Aset

Form 19.1 CPAR Pengelolaan Aset 5.1

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia daftar inventaris aset informasi yang lengkap dan akurat

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN telah menerapkan daftar aset informasi berupa Dokumen, Data, Hardware, Software dan Jaringan namun selain BMN (Barang Milik Negara) beberapa aset informasi belum terbentuk dalam detail daftar inventaris aset informasi

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Untuk memudahkan proses inventarisasi maka KANWIL DJPBN sebaiknya menghimpun tim inventarisasi aset informasi terupdate.
Menghitung jumlah aset tetap per sub sub kelompok barang
Mencatat aset tetap ke dalam kertas kerja inventarisasi
Mengupdate aset tetap ke dalam SIMAK BMN
Menempelkan label pada aset tetap yang telah dihitung
Menentukan kondisi aset tetap dengan kriteria baik, rusak ringan, atau rusak berat
Menyusun laporan hasil inventarisasi
Membandingkan laporan hasil inventerisasi dengan dokumen aset tetap yang ada
Membuat daftar seluruh aset tetap yang tidak ditemukan, belum pernah dicatat, dan rusak berat serta daftar koreksi nilai
Sebaiknya setiap pengelolaan aset didetailkan mengenai pengelola dan penanggung jawab aset tiap bagiannya.

Menyampaikan hasil inventarisasi kepada pengelola aset secara berkala di lingkup KANWIL DJPBN			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.2 CPAR Pengelolaan Aset 5.2

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN telah menerapkan proses evaluasi dan klasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi termasuk alokasi pengguna perbidang dan seksi serta keperluan pengamanannya hanya saja masih terbatas kepada alokasi Hardware, Software dan Jaringan dan belum terbentuk dalam detail SOP pengamanan aset informasi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinsikan aset dan inventaris semua bagian di KANWIL DJPBN
Mendefinisikan kepemilikan/ penanggungjawab pengelolaan untuk setiap aset yang dimiliki oleh KANWIL DJPBN
Melakukan panduan klasifikasi aset mulai dari kepentingan aset & utilisasi aset
Menyusun prosedur panduan pengelolaan pengamanan aset serta labelling terhadap seluruh aset di KANWIL DJPBN. Contoh : Penggunaan labeling pada PC di seluruh ruang bidang dan seksi
Untuk meningkatkan ke Tingkat Kematangan level III, sebaiknya KANWIL DJPBN senantiasa melakukan update labeling aset informasi guna analisis kebutuhan KANWIL DJPBN saat ini
Menuju Tingkat Kematangan level III hingga V maka KANWIL DJPBN perlu melakukan evaluasi secara keseluruhan pada aset atau inventaris yang ada sehingga proses update kontrol labeling dapat diterapkan sesuai kondisi terkini.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 19.3 CPAR Pengelolaan Aset 5.3

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia definisi tingkatan akses yang berbeda dan matrix yang merekam alokasi akses tersebut

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN telah mendefinisikan tingkatan akses yang berbeda terutama dalam penggunaan aplikasi seuai dengan tingkat kewenangan untuk perekaman alokasi akses yang terdapat di beberapa bagian tertentu tergantung tingkat kerahasiaan dan nilai aset informasi yang dituju

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Menginventarisir kepemilikan untuk setiap aset informasi misal : PC personal dan akses yang dimiliki oleh KANWIL DJPBN
Mendefinisikan tanggung jawab dari pengelola aset
Menyusun matriks pengguna aset dengan kategori :

- Pemilik Aset
- Pengelola Aset
- Pengguna umum

Melakukan penyesuaian prosedur untuk pengelolaan Hak Akses yang juga memuat penentuan dari klasifikasi penggunahak akses tersebut.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi

Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera

Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 19.4 CPAR Pengelolaan Aset 5.4

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia proses pengelolaan perubahan terhadap sistem (termasuk perubahan konfigurasi) yang diterapkan secara konsisten

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Karena pelaksanaan perubahan konfigurasi terbilang minim, maka implementasi masih menyesuaikan dengan KMK terkait untuk pelaksanaanya dan proses pengelolaan terhadap perubahan yang diterapkan secara formil di Kantor Pusat masih secara informal dilakukan di Kantor Wilayah DJPBN

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan bagian dari manajemen konfigurasi yang akan dikelola di KANWIL DJPBN contoh konfigurasi untuk Kontrol akses, Update software atau sistem operasi

Menyusun petunjuk pengelolaan konfigurasi untuk masing-masing bagian

Menyusun dokumen perubahan (*change management document*) sebagai hasil evaluasi konfigurasi

Untuk menuju pada Tingkat Kematangan level III hingga level V, maka perlu adanya evaluasi petunjuk atau prosedur yang runtut tersusun serta proses penerapannya yag disesuaikan dengan kondisi saat ini di KANWIL DJPBN

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi

Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera

Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 19.5 CPAR Pengelolaan Aset 5.5

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Karena pelaksanaan perubahan konfigurasi terbilang minim, maka implementasinya dilaksankan oleh Kantor Pusat dan menyesuaikan dengan KMK terkait untuk pelaksanaanya. Selain itu, proses pengelolaan terhadap perubahan yang diterapkan secara formil di Kantor Pusat, masih dijalankan secara informal di Kantor Wilayah DJPBN karena minimnya pelaksanaan operasionalisasi perubahan dan minimnya prosedur/panduan yang dibutuhkan untuk melakukan perubahan / konfigurasi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Memastikan permintaan perubahan / konfigurasi diajukan oleh pihak yang berwenang
Mendefinisikan bagian dari manajemen konfigurasi yang akan dikelola di KANWIL DJPBN misal : konfigurasi untuk Kontrol akses dan Update software atau sistem operasi
Melakukan identifikasi terhadap perangkat lunak, informasi, basis data, dan perangkat keras yang perlu dikonfigurasi
Menyusun petunjuk pengelolaan konfigurasi untuk masing-masing bagian
Memastikan pihak yang berwenang menerima perubahan yang diminta sebelum dilakukan implementasi
Memastikan bahwa dokumentasi perubahan termutakhir dan dokumen sebelumnya disimpan
Memelihara versi perubahan
Memelihara jejak audit (*audit trails*) perubahan
Memastikan bahwa implementasi perubahan dilakukan pada waktu yang tepat dan tidak mengganggu kegiatan operasional.

Menyusun dokumen perubahan (*change document*) sebagai hasil evaluasi konfigurasi Untuk menuju pada Tingkat Kematangan level III hingga level V maka perlu adanya evaluasi petunjuk atau prosedur yang telah disusun serta proses penerapannya saat ini di KANWIL DJPBN.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.6 CPAR Pengelolaan Aset 5.6

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Di KANWIL DJPBN telah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi. Untuk BMN maka pelaksanaanya dilakukan melalui aplikasi SIMAK BMN (Barang Milik Negara) dan akses pengguna dilaksanakan lewat pendaftaran melalui email Kementerian Keuangan ke Pusintek.
Selain BMN, setiap update aplikasi atau sistem yang memenuhi proses bisnis dan kebutuhan KANWIL DJPBN akan dilakukan update atau proses pemutakhiran. Namun kondisi sekarang di KANWIL DJPBN belum mempunyai prosedur pengelolaan konfigurasi.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Memastikan permintaan perubahan aset informasi terbaru diajukan oleh pihak yang berwenang
Mendefinisikan bagian dari manajemen konfigurasi yang akan dikelola di KANWIL DJPBN misal : konfigurasi untuk Kontrol akses dan Update software atau sistem operasi
Melakukan identifikasi terhadap perangkat lunak, informasi, basis data, dan perangkat keras yang perlu dikonfigurasi
Menyusun petunjuk pengelolaan konfigurasi untuk masing-masing bagian
Memastikan pihak yang berwenang menerima perubahan yang diminta sebelum dilakukan implementasi
Memastikan bahwa dokumentasi perubahan aset informasi terbaru dan dokumen sebelumnya disimpan
Memelihara versi perubahan aset informasi terbaru

Memelihara jejak audit (*audit trails*) perubahan aset informasi terbaru Memastikan bahwa implementasi aset informasi terbaru dilakukan pada waktu yang tepat dan tidak mengganggu kegiatan operasional. Menyusun dokumen perubahan (*change document*) aset informasi terbaru sebagai hasil evaluasi konfigurasi Untuk menuju pada Tingkat Kematangan level III hingga level V maka perlu adanya evaluasi petunjuk atau prosedur yang telah disusun serta proses penerapannya saat ini di KANWIL DJPBN.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.7 CPAR Pengelolaan Aset 5.7

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Pihak KANWIL DJPBN dalam proses untuk menerapkan definisi tanggung jawab pengamanan informasi secara individual untuk semua personil dengan pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Terdapat pula Larangan dan Sanksi sebagai control tiap individu.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan tujuan serta ruang lingkup keamanan informasi yang ada di KANWIL DJPBN (lingkup yang lebih spesifik dengan pelaksanaan teknis)
Menentukan kesesuaian kebijakan dan prosedur keamanan infomasi dengn kebijakan dan keamanan infomasi DJPBN secara umum
Mendefinisikan kepentingan pengamanan informasi serta penanggung jawabnya
Mendefinisikan peran dan tanggung jawab keamanan infomasi di dalamnya
Memverifikasi latar belakang semua personil
Menggunakan kontrak keamanan aset yang dikelola oleh personil atau penanggung jawabnya
Merujuk referensi dari peraturan instansi, serta peraturan kepatuhan keamanan informasi lain yang terkait.
Membuat kontrol pengendalian sesuai dengan proses bisnis KANWIL DJPBN
Untuk menuju pada Tingkat Kematangan level III hingga level V maka perlu adanya pembuatan mekanisme penanggung jawab pengaman informasi, mereview serta mengevaluasi kinerja tiap penanggung jawab secara individual.
Untuk mengevaluasi, KANWIL DJPBN perlu memeriksa kesesuaian intruksi

kerja dengan formulir tiap tindakan Untuk dapat menuju pada tingkat kepatuhan yang lebih tinggi, maka kepatuhan pada kebijakan dan prosedur sebaiknya dievaluasi berkala tiap bulan atau semester. Setiap laporan evaluasi yang didokumentasikan secara resmi dan dikomunikasikan serta disosialisasikan kepada semua pihak pelaksana DJPBN			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.8 CPAR Pengelolaan Aset 5.8

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tata tertib penggunaan komputer, email, internet dan intranet

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Pihak KANWIL DJPBN telah menerapkan tata tertib penggunaan komputer, email, internet dan intranet melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Terdapat pula Larangan dan Sanksi sebagai control tiap individu

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mengupdate tata tertib penggunaan komputer, internet, dan intranet dan perangkat keamanan informasi yang ada di KANWIL DJPBN (lingkup yang lebih spesifik dengan pelaksanaan teknis)
Menentukan kesesuaian tata tertib penggunaan komputer, internet, dan intranet dengan kebijakan dan keamanan infomasi DJPBN secara umum
Mendefinisikan pentingnya pengamanan informasi dalam penggunaan komputer, internet, dan intranet
Menyampaikan peran dan tanggung jawab keamanan infomasi di dalam penggunaan komputer, internet, dan intranet
Menggunakan kontrak pengendalian untuk menjamin kepatuhan tata tertib penggunaan komputer, internet, dan intranet seluruh personil
Merujuk referensi dari peraturan instansi, serta peraturan kepatuhan keamanan informasi lain yang terkait.
Membuat kontrol pengendalian penggunaan komputer, internet, dan intranet sesuai dengan proses bisnis Kanwil DJPBN
Untuk menuju pada Tingkat Kematangan level III hingga level V maka tata tertib yang telah ter-*update* disosialisasikan dan dikomunikasikan kepada semua pihak.
Menyusun seluruh tata tertib secara tertulis dan mendokumentasikannya

sebagai arsip. Selain itu, mengevaluasi serta memonitoring proses penerapannya Untuk dapat menuju pada tingkat kepatuhan yang lebih baik, maka kepatuhan pada tata tertib dan prosedur sebaiknya dievaluasi berkala tiap bulan atau semester. Setiap laporan evaluasi yang ada didokumentasikan secara resmi dan dikomunikasikan serta disosialisasikan kepada semua pihak pelaksana DJPBN			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.9 CPAR Pengelolaan Aset 5.9

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin XI tentang HAKI. Masalah umumnya adalah belum adanya *cascading* prosedur yang terdokumentasi ntuk mengatur tata tertib tersebut.

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan semua aset instansi yang terkait HAKI
Menyusun tata tertib pengamanan dan penggunaan aset instansi terkait keamanan informasi yang ada di KANWIL DJPBN (lingkup yang lebih spesifik dengan pelaksanaan teknis)
Menentukan kesesuaian tata tertib pengamanan dan penggunaan aset Instansi dengan kebijakan dan keamanan infomasi DJPBN secara umum
Mendefinisikan pentingnya pengamanan informasi dalam pengamanan dan penggunaan aset Instansi
Menyampaikan peran dan tanggung jawab keamanan infomasi di dalam pengamanan dan penggunaan aset Instansi
Menggunakan kontrak pengendalian untuk menjamin kepatuhan tata tertib pengamanan dan penggunaan aset Instansi seluruh personil
Merujuk referensi dari peraturan instansi, termasuk semua peraturan dari HAKI dalam menyusun peraturan atau panduan pengamanan serta peraturan kepatuhan keamanan informasi lain yang terkait.
Membuat kontrol pengendalian pengamanan dan penggunaan aset Instansi sesuai dengan proses bisnis Kanwil DJPBN
Menetapkan sanksi dan pelanggaran terhadap peraturan yang telah dibuat

Untuk menuju pada Tingkat Kematangan level III hingga level V maka tata tertib yang telah ter-update disosialisasikan dan dikomunikasikan kepada semua pihak. Menyusun seluruh tata tertib secara tertulis dan mendokumentasikannya sebagai arsip. Selain itu, mengevaluasi serta memonitoring proses penerapannya Untuk dapat menuju pada tingkat kepatuhan yang lebih baik, maka kepatuhan pada tata tertib dan prosedur sebaiknya dievaluasi berkala tiap bulan atau semester. Setiap laporan evaluasi yang ada didokumentasikan secara resmi dan dikomunikasikan serta disosialisasikan kepada semua pihak pelaksana DJPBN			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.10 CPAR Pengelolaan Aset 5.10

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Peraturan pengamanan data pribadi

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.512/KMK.01/2010 dan KMK.479/KMK.01/ 2010 Poin III & VI tentang aset & akses

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan semua aset informasi (pribadi dan instansi)
Menyusun kategori peraturan pengamanan data pribadi termasuk penggunaan akun dan kata sandi terkait keamanan informasi yang ada di KANWIL DJPBN (lingkup yang lebih spesifik dengan pelaksanaan teknis)
Melaksanakan standar pengamanan akun dan kata sandi yaitu :

- Memakai kata sandi yang tidak mudah ditebak
- Mengubah kata sandi yang telah diberikan oleh unit TIK Eselon I pada saat pertama kali digunakan
- Mengubah kata sandi secara berkala, dan paling lama dalam jangka waktu 90 (Sembilan puluh) hari.
- Melindungi informasi penting miliki Kementerian keuangan yang ada dalam perangkat computer dengan cara memakai screen saver yang aktif setelah 10 (sepuluh) menit tidak digunakan
- Mengaktifkan konfigurasi yang akan mematikan perangkat computer setelah 30 (tiga puluh) menit tidak digunakan

Menghindari hal-hal yang telah datur dalam larangan penggunayaitu :

- Mengungkapkan atau berbagi kata sandi melalui media apapun
- Membuat kata sandi sama di sistem TIK di lingkungan Kementerian Keuangan dengan kata sandi yang digunakan di luar sistem TIK

Kementerian Keuangan

- Menggunakan fasilitas ingat kata sandi (*remember password*) dalam mengakses sistem operasi, surat elektronik, sistem jaringan/ internet
- Menuliskan kata sandi dimanapun dan/atau menyimpan kata sandi di berkas elektronik pada setiap sistem komputer

Menetapkan sanksi dan pelanggaran terhadap peraturan yang telah dibuat sebagaimana diatur KMK.512/KMK.01/2010

Untuk menuju pada Tingkat Kematangan level III hingga level V maka tata tertib harus disosialisasikan dan dikomunikasikan kepada semua pihak.

Menyusun seluruh tata tertib secara tertulis dan mendokumentasikannya sebagai arsip. Selain itu, mengevaluasi serta memonitoring proses penerapannya

Untuk dapat menuju pada tingkat kepatuhan yang lebih baik, maka kepatuhan pada tata tertib sebaiknya dievaluasi berkala tiap bulan atau semester. Setiap laporan evaluasi yang ada didokumentasikan secara resmi dan dikomunikasikan serta disosialisasikan kepada semua pihak pelaksana DJPBN

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**

Section 4 : Tindak lanjut dan verifikasi

Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera

Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 19.11 CPAR Pengelolaan Aset 5.11

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Pengelolaan identitas elektronik dan proses otentikasi (username&password) termasuk kebijakan terhadap pelanggarannya

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin VII tentang Akses dan KMK.512 /KMK.01/2009 tentang Kebijakan dan Penggunaan Akun dan Kata Sandi Pengguna yang diikuti pula oleh Larangan dan Sanksi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan semua aset informasi (pribadi dan instansi)
Menyusun kategori peraturan pengamanan data pribadi termasuk penggunaan akun dan kata sandi terkait keamanan informasi yang ada di KANWIL DJPBN (lingkup yang lebih spesifik dengan pelaksanaan teknis)
Melaksanakan standar pengamanan akun dan kata sandi yaitu :

a. Memakai kata sandi yang tidak mudah ditebak
b. Mengubah kata sandi yang telah diberikan oleh unit TIK Eselon I pada saat pertama kali digunakan
c. Mengubah kata sandi secara berkala, dan paling lama dalam jangka waktu 90 (Sembilan puluh) hari.
d. Melindungi informasi penting miliki Kementerian keuangan yang ada dalam perangkat computer dengan cara memakai screen saver yang aktif setelah 10 (sepuluh) menit tidak digunakan
e. Mengaktifkan konfigurasi yang akan mematikan perangkat computer setelah 30 (tiga puluh) menit tidak digunakan

Menghindari hal-hal yang telah datur dalam larangan penggunayaitu :

a. Mengungkapkan atau berbagi kata sandi melalui media apapun
b. Membuat kata sandi sama di sistem TIK di lingkungan Kementerian Keuangan dengan kata sandi yang digunakan di luar sistem TIK Kementerian Keuangan
c. Menggunakan fasilitas ingat kata sandi (remember password) dalam mengakses sistem operasi, surat elektronik, sistem jaringan/ internet
d. Menuliskan kata sandi dimanapun dan/atau menyimpan kata sandi di berkas elektronik pada setiap sistem komputer

Menetapkan sanksi dan pelanggaran terhadap peraturan yang telah dibuat sebagaimana diatur KMK.512/KMK.01/2010

Untuk menuju pada Tingkat Kematangan level III hingga level V maka tata tertib harus disosialisasikan dan dikomunikasikan kepada semua pihak.

Menyusun seluruh tata tertib secara tertulis dan mendokumentasikannya sebagai arsip. Selain itu, mengevaluasi serta memonitoring proses penerapannya

Untuk dapat menuju pada tingkat kepatuhan yang lebih baik, maka kepatuhan pada tata tertib sebaiknya dievaluasi berkala tiap bulan atau semester. Setiap laporan evaluasi yang ada didokumentasikan secara resmi dan dikomunikasikan serta disosialisasikan kepada semua pihak pelaksana DJPBN

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**

Section 4 : Tindak lanjut dan verifikasi

Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera

Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 19.12 CPAR Pengelolaan Aset 5.12

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin VII tentang Pengendalian Akses dan Poin III tentang Aset Informasi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan semua aset informasi (pribadi dan instansi)
Menyusun kategori peraturan pengamanan data pribadi termasuk penggunaan akun dan kata sandi terkait keamanan informasi yang ada di KANWIL DJPBN (lingkup yang lebih spesifik dengan pelaksanaan teknis)
Melaksanakan standar pengamanan akun dan kata sandi yaitu :

- Memakai kata sandi yang tidak mudah ditebak
- Mengubah kata sandi yang telah diberikan oleh unit TIK Eselon I pada saat pertama kali digunakan
- Mengubah kata sandi secara berkala, dan paling lama dalam jangka waktu 90 (Sembilan puluh) hari.
- Melindungi informasi penting miliki Kementerian keuangan yang ada dalam perangkat computer dengan cara memakai screen saver yang aktif setelah 10 (sepuluh) menit tidak digunakan
- Mengaktifkan konfigurasi yang akan mematikan perangkat computer setelah 30 (tiga puluh) menit tidak digunakan

Menghindari hal-hal yang telah datur dalam larangan penggunayaitu :

- Mengungkapkan atau berbagi kata sandi melalui media apapun
- Membuat kata sandi sama di sistem TIK di lingkungan Kementerian

Keuangan dengan kata sandi yang digunakan di luar sistem TIK Kementerian Keuangan
- Menggunakan fasilitas ingat kata sandi (remember password) dalam mengakses sistem operasi, surat elektronik, sistem jaringan/ internet
- Menuliskan kata sandi dimanapun dan/atau menyimpan kata sandi di berkas elektronik pada setiap sistem komputer

Menetapkan sanksi dan pelanggaran terhadap peraturan yang telah dibuat sebagaimana diatur KMK.512/KMK.01/2010

Untuk menuju pada Tingkat Kematangan level III hingga level V maka tata tertib harus disosialisasikan dan dikomunikasikan kepada semua pihak.

Menyusun seluruh tata tertib secara tertulis dan mendokumentasikannya sebagai arsip. Selain itu, mengevaluasi serta memonitoring proses penerapannya

Untuk dapat menuju pada tingkat kepatuhan yang lebih baik, maka kepatuhan pada tata tertib sebaiknya dievaluasi berkala tiap bulan atau semester. Setiap laporan evaluasi yang ada didokumentasikan secara resmi dan dikomunikasikan serta disosialisasikan kepada semua pihak pelaksana DJPBN

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 4 : Tindak lanjut dan verifikasi

Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera

	Disposisi oleh :	**Tanggal :**
Nama & TTD	**Kepala Bagian Umum**	

Form 19.13 CPAR Pengelolaan Aset 5.13

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin VI tentang media penyimpanan dan KMK.350/KMK.01/2010 Poin 5.5 tentang media Penyimpanan Data dan 5.5.3 ttg Penghancuran Media Penyimpanan Data

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan tingkat prioritas aset berdasarkan kebutuhan atau proses bisnis KANWIL DJPBN
Menentukan tingkat hidup (*lifetime*) dari data atau infomasi tersebut
Menyisihkan arsip data non aktif dengan data aktif
Membuat daftar arsip yang akan dipindahkan dan dimusnahkan
Membuat berita acara pemusnahan arsip
Membuat persetujuan pemusnahan arsip dengan pihak terkait misal pimpinan Kanwil DJPBN dan pihak eksternal yang terkait
Untuk arsip data yang tersimpan dalam media penyimpanan data, maka penghancuran media penyimpanan data harus mempertimbangkan hal-hal berikut :

- Media yang berisi data dengan klasifikasi Sangat Rahasia, Rahasia atau Terbats harus dimusnahkan secara aman, misalnya dibakar atau dihancurkan
- Membuat dan menerapkan prosedur untuk mengidentifikasi media yang mungkin memerlukan pemusnahan secara aman

• Pemusnahan media penyimpanan yang berisi data dengan klasifikasi Sangat Rahasia, Rahasia atau Terbatas harus tercatat dalam *audit trail* Sebagai upaya pengendalian, maka disusun formulir pemusnahan pengendalian serta laporan evaluasi yang terdokumentasi			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.14 CPAR Pengelolaan Aset 5.14

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin VI bagian 8 tentang pertukaran informasi dan KMK.274/KMK.01/2010 pada bag 5.2 Aplikasi Pertukaran Data Elektronik

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Menerapkan kebijakan pengamanan mengenai informasi dan data
Menentukan kebutuhan pengendalian kontrol untuk memastikan perlindungan aset informasi
Jika berkaitan dengan proses layanan oleh pihak ketiga, maka sebaiknya Kanwil DJPBN menentukan tingkatan layanan yang dapat diterima oleh Kanwil DJPBN. (Keterkaitan dengan pelindungan aset internal)
Melakukan persetujuan atau kontrak perjanjian secara resmi
Pertukaran informasi dan perangkat lunak antara Kementerian Keuangan dan pihak ketiga hanya dilakukan atas kesepakatan tertulis kedua belah pihak
Kanwil DJPBN harus melakukan penilaian risiko yang memadai sebelum melaksanakan pertukaran informasi
Kanwil DJPBN harus menerapkan pengendalian keamanan informasi untuk pengiriman informasi melalui surat elektronik atau pengiriman informasi melalui jasa layanan pengiriman dalam rangka menghindari akses oleh yang tidak berwenang
Untuk melangkah ke tingkat kematangan selanjutnya maka Kanwil DJPBN diharapkan menerapkan prosedur pertukaran informasi bila menggunakan perangkat elektronik, pertukaran informasi yang tidak menggunakan perangkat

komunikasi elektronik, pengendalian pertukaran informasi. Mendokumentasikan keseluruhan kebijakan dan prosedur secara tertulis, mengkomunikasikan dan mensosialisasikan kepada seluruh pegawai Kanwil DJPBN dan pihak ketiga.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.15 CPAR Pengelolaan Aset 5.15

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin IX tentang gangguan keamanan informasi dan GKN sendiri memilki SOP tentang penyelesaian gangguan layanan TIK

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Sebelum melakukan penyidikan, KANWIL DJPBN sebaiknya menyusun mekanisme /prosedur manajemen insiden di lingkungan Kanwil DJPBN
Penyusunan mekanisme atau prosedur penyidikan merujuk dari kebijakan manajemen insiden
Mendefinisikan insiden yang terjadi dan yang akan dilaporkan
Membuat fomulir pelaporan insiden yang didialamnya terdapat detail eskalasi (kenaikan level) , kendali perubahan, dll.
Menyusun rencana tindakan penanggulangan dini (termasuk keperluan eskalasi selanjutnya), bersama-sama dengan pemilik aset informasi dan Petugas Keamanan Informasi.
Melakukan review terhadap rencana tindakan penanggulangan dini, dan apabila diperlukan, merevisi rencana tersebut.
Melaporkan insiden yang ditemukan di lingkungan sistem yang dikelolanya kepada KPTIK dan menindaklanjutinya.
Menindaklanjuti permintaan eskalasi pelaporan insiden dari KPTIK yang melibatkan sistem yang dikelolanya.
Melakukan investigasi singkat untuk menetapkan klasifikasi insiden yang

ditindaklanjutinya. Dan untuk insiden berat akan melaporkan langsung kepada pemilik aset dan Petugas Keamanan Informasi. Apabila insiden tersebut ternyata tidak terbukti, petugas keamanan informasi / KPTIK mencatat hasil investigasi (*log*) dan menginformasikan kepada atasannya, Tim Keamanan Informasi dan penggungjawab aset informasi. Apabila ternyata ditemukan bukti pendukung insiden tersebut, ataupun masih terdapat ketidakjelasan atas kecurigaan terjadinya insiden, maka petugas keamanan informasi harus membahas hal tersebut dengan atasannya			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.16 CPAR Pengelolaan Aset 5.16

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Prosedur back-up ujicoba pengembalian data (restore)

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin VI bag C.5 tentang Back-up dan KMK.350/KMK.01/2010 Poin 4.3.3 tentang Ketersediaan Data (Availability)

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Menentukan proses *backup* apakah dilakukan secara manual atau menggunakan tools

Jika menggunakan *tools*, Mekanisme *back-up* atau *restore* data sebaiknya disesuaikan dengan *tools* yang akan dipakai oleh KANWIL DJPBN

Menyusun mekanisme *backup /restore* berdasarkan *tools* yang dipakai

Metode *backup*, meliputi tetapi tidak terbats pada :

- *System Backup*
- *Full Backup*
- *Incremental Backup*

Mengatur konfigurasi *tools* untuk melakukan *backup* secara rutin

Harus dibuat catatan / *log backup* yang berisi informasi sekurang-kurangnya meliputi tapi tidak terbatas pada :

- Nama media yang digunakan
- Isi
- Metode *backup*
- Status *backup* (berhasil / gagal)
- Waktu pelaksanaan *backup*
- Lokasi media *backup* disimpan, tanggal pemindahan dan petugas

yang memindahkan Jika dilakukan manual, maka disusun prosedur backup secara berkala minimal 1 (satu) bulan sekali Mendefinisikan data atau aset yang di*backup* Baik manual atau *tools*, secara berkala dilakukan pelaporan berbentuk *checklist*			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.17 CPAR Pengelolaan Aset 5.17

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin V tentang pengamaan fisik dan lingkungan khususnya akses ke aset informasi yang memiliki klasifikasi RAHASIA dan SANGAT RAHASIA

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan semua aset informasi (pribadi dan instansi)
Menentukan tingkat prioritas aset yang terdapat di KANWIL DJPBN
Menyusun kategori peraturan pengamanan asset informasi (data, informasi, software, hardware, jaringan dan perangkat lainnya) terkait keamanan informasi yang ada di KANWIL DJPBN (lingkup yang lebih spesifik dengan pelaksanaan teknis)
Mengklasifikasikan zona pengamanan berdasarkan aset yang ada
Menyusun kebijakan pengamanan fisik berdasarkan klasifikasi zona
Menetapkan sanksi dan pelanggaran terhadap peraturan yang telah dibuat sebagaimana diatur oleh KMK.512/KMK.01/2010
Untuk menuju pada Tingkat Kematangan level III hingga level V maka tata tertib harus disosialisasikan dan dikomunikasikan kepada semua pihak.
Menyusun seluruh tata tertib secara tertulis dan mendokumentasikannya sebagai arsip. Selain itu, mengevaluasi serta memonitoring proses penerapannya
Untuk dapat menuju pada tingkat kepatuhan yang lebih baik, maka kepatuhan pada tata tertib sebaiknya dievaluasi berkala tiap bulan atau semester. Setiap

laporan evaluasi yang ada didokumentasikan secara resmi dan dikomunikasikan serta disosialisasikan kepada semua pihak pelaksana DJPBN			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.18 CPAR Pengelolaan Aset 5.18

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Proses pengecekan latar belakang SDM

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin IV tentang SDM yang memiliki standar pengecekan latar belakang SDM dengan mengecek referensi hubungan kerja, kualifikasi akademik dan lain-lain.

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan semua peran pengamanan serta tanggung jawabnya
Melakukan verifikasi personel atau pelaksana yang ada dengan kesesuaian peran dan tanggungjawab yang telah dibuat
Jika perlu penunjukan melalui surat tugas mengenai pengelolaan keamanan aset informasi yang ada
Melaksanakan uji kompetensi pengelolaan keamanan informasi secara berkala baik offline maupun online
Menyelenggarakan evaluasi atas uji kompetensi
Jika ada temuan yang tidak sesuai maka perlu dilakukan kebijakan seperti adanya sosialisasi atau pelatihan guna menunjang kemampuan sesuai kriteria tanggung jawab yang akan diemban nantinya
Melakukan praktik keamanan informasi sebagai tindakan pencegahan seperti testing hacking pada sistem KANWIL DJPBN untuk mengetahui tingkat vulnerability atau kerawanan dari sistem.
Melaksanakan bimbingan teknis (BIMTEK) untuk memperbesar kuantitas personil yang kompeten terkait keamanan informasi
Untuk meningkatkan Tingkat Kematangan level III hingga V, maka KANWIL DJPBN sebaiknya melakukan evaluasi secara berkala pada tiap kinerja

pelaksana. Selain itu, KANWIL DJPBN sebaiknya melakukan perubahan struktur peran pelaksana / tanggung jawab jika memang dibutuhkan..Untuk menuju pada Tingkat Kematangan level III hingga level V maka perlu adanya evaluasi petunjuk atau prosedur yang telah disusun serta proses penerapannya saat ini di KANWIL DJPBN.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.19 CPAR Pengelolaan Aset 5.19

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin IX tentang gangguan keamanan informasi dan GKN sendiri memilki SOP tentang penyelesaian gangguan/insiden layanan TIK. Proses penanganan insidenpun sudah diterapkan namun memang belum ada pelaporan secara resmi kepada pihak terkait baik internal atau eksternal

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Menggarisbawahi KMK.479/KMK.01/2010, KANWIL DJPBN sebaiknya menyusun kebijakan manajemen insiden di lingkup KANWIL DJPBN
Menghubungkan tujuan pengelolaan keamanan informasi dengan proses bisnis unit dan bagian dengan tujuan mengidentifikasi insiden yang saling terkait.
Penyusunan mekanisme atau prosedur pelaporan insiden merujuk dari kebijakan manajemen insiden
Mendefinisikan insiden yang terjadi dan yang akan dilaporkan
Membuat fomulir pelaporan insiden yang didialamnya terdapat detail eskalasi (level), tindakan penyelesaian, dll.
Mengidentifikasi kemunculan insiden, tingkat kemungkinan, termasuk di dalamnya kategorisasi dan prioritisasi insiden
Membuat langkah korektif insiden berdasarkan kategori dan prioritasnya
Untuk menuju pada Tingkat Kematangan level III hingga level V maka perlu adanya evaluasi formulir pelaporan insiden yang telah disusun secara berkala dan dilaporkan kepada pimpin serta disosialisasikan untuk seluruh pelaksana

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.20 CPAR Pengelolaan Aset 5.20

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Prosedur penghancuran data/aset yang sudah tidak diperlukan

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN telah mempunyai prosedur penghancuran data atau aset namun belum mempunyai klasifikasi serta peryaratan aset

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan tingkat prioritas aset berdasarkan kebutuhan atau poses bisnis KANWIL DJPBN
Menentukan tingkat hidup (lifetime)dari data atau infomasi tersebut
Menyisihkan arsip data non aktif dengan data aktif
Membuat daftar arsip yang akan dipindahkan dan dimusnahkan
Membuat berita acara pemusnahan arsip
Membuat persetujuan pemusnahan arsip dengan pihak terkait misal pimpinan KANWIL DJPBN dan pihak eksternal yang terkait
Untuk arsip data yang tersimpan dalam media penyimpanan data, maka penghancuran media penyimpanan data harus mempertimbangkan hal-hal berikut :

- Media yang berisi data dengan klasifikasi Sangat Rahasia, Rahasia atau Terbats harus dimusnahkan secara aman, misalnya dibakar atau dihancurkan
- Membuat dan menerapkan prosedur untuk mengidentifikasi media yang mungkin memerlukan pemusnahan secara aman
- Pemusnahan media penyimpanan yang berisi data dengan klasifikasi Sangat Rahasia, Rahasia atau Terbatas harus tercatat dalam audit trail

Sebagai upaya pengendalian, maka disusun formulir pemusnahan pengendalian serta laporan evaluasi yang terdokumentasiSebagai upaya pengendalian, maka disusun formulir pemusnahan pengendalian serta laporan evaluasi yang

terdokumentasi secara tertulis Untuk menuju pada Tingkat Kematangan level II hingga level V maka perlu adanya formulir yang disusun serta laporan penerapan pengamanan			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.21 CPAR Pengelolaan Aset 5.21

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Prosedur kajian penggunaan akses (*user access review*) dan langkah pembenahan apabila terjadi ketidak sesuaian (*non-conformity*) terhadap kebijakan yang berlaku.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN belum mempunyai kajian penggunaan akses serta langkah pembaharuannya. Pengerjaan prosedur tersebut dialihkan kepada tim proyek eksternal KANWIL DJPBN namun masih satu instansi yang terdiri dari dosen dan karyawan. Kendala yang berarti adalah kurang pahamnya mengenai proses bisnis KANWIL DJPBN oleh karena itu dilakukan pengggalian data dan informasi dengan wawacara rutin dengan pihak KANWIL DJPBN.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan semua aset informasi aplikasi (jaringan dan *standalone*)
Mendefinisikan pengguna menjadi super administrator, administrator, dan pengguna umum untuk semua sistem dan aplikasi (selain SPAN yang telah diatur secara khusus oleh Kementerian Keuangan)
Untuk aplikasi dan sistem yang vital sebaiknya hanya diberlakukan super administrator dan administrator
Untuk aplikasi pendukung dapat digunakan akses ketiganya
Penyusunan prosedur kajian penggunaan akses dan tindakan pembenahan insiden akses informasi
Penggunaan kebijakan *login attempts* untuk membatasi kesalahan masukan user
Penggunaan *session lock* guna mengunci akun jika diketahui tidak terdapat aktivitas selama waktu tertentu
Penyusunan prosedur disesuaikan dengan kebijakan pengamanan informasi yang dibuat, sehingga dapat disusun langkah - langkah pembaharuan mengenai aspek yang tidak sesuai di dalamnya.

Menetapkan sanksi dan pelanggaran terhadap peraturan yang telah dibuat sebagaimana pula diatur KMK.512/KMK.01/2010 Untuk menuju pada Tingkat Kematangan level III hingga level V maka perlu adanya evaluasi kebijakan dan prosedur yang telah disusun serta proses penerapannya saat ini di KANWIL DJPBN Untuk dapat menuju pada tingkat kepatuhan yang lebih baik, maka kepatuhan pada prosedur sebaiknya dievaluasi berkala tiap bulan atau semester. Setiap laporan evaluasi yang ada didokumentasikan secara resmi dan dikomunikasikan serta disosialisasikan kepada semua pihak pelaksana DJPBN			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.22 CPAR Pengelolaan Aset 5.22

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia daftar data/informasi yang harus di-backup dan laporan analisis kepatuhan terhadap prosedur backup-nya

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Saat ini seluruh data terkait Keuangan Negara tercatat lengkap dan di-backup secara berkala sebagai bentuk penerapan KMK.479 /KMK.01/2010 Poin VI bagian C.5 tentang backup dan KMK.350/KMK.01/2010 pada bag 5.3 yang menerapkan metode system backup, full backup dan incremental backup yang mendasarkan pelaksanaan backup berdasarkan tingkat kritikalitas data, namun untuk poin laporan analisis kepatuhan terhadap prosedur backup masih dalam perencanaan, namun belum tersedianya laporan analisis kepatuhan terhadap prosedur backup sehingga hasil evaluasi mengenai proses backup tidak dapat dinilai

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan tingkat prioritas aset berdasarkan kebutuhan atau poses bisnis KANWIL DJPBN
Menentukan tingkat hidup (lifetime) dari data atau infomasi tersebut
Mendefinisikan data atau aset yang dibackup
Menentukan proses backup apakah dilakukan secara manual atau menggunakan tools
Jika menggunakan tools, Mekanisme back-up atau restore data sebaiknya disesuaikan dengan tools yang akan dipakai oleh KANWIL DJPBN
Menyusun mekanisme backup /restore berdasarkan tools yang dipakai
Metode backup, meliputi tetapi tidak terbats pada :

- System Backup
- Full Backup
- Incremental Backup

Mengatur konfigurasi tools untuk melakukan backup secara rutin
Harus dibuat catatan / log backup yang berisi informasi sekurang-kurangnya meliputi tapi tidak terbatas pada :

- Nama media yang digunakan
- Isi
- Metode backup
- Status backup (berhasil / gagal)
- Waktu pelaksanaan backup
- Lokasi media backup disimpan, tanggal pemindahan dan petugas yang memindahkan

Jika dilakukan manual, maka disusun prosedur backup secara berkala minimal 1 (satu) bulan sekali
Baik manual atau tools, secara berkala dilakukan pelaporan berbentuk checklist
Guna kepentingan eskalasi Tingkat Kematangan level II hingga level V maka perlu adanya penyusunan prosedur dan instruksi kerja mengenai back-up data serta evaluasi secaraberkala guna pengukuran efektivitas prosedur yang telah disusun

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**

Section 4 : Tindak lanjut dan verifikasi

Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera

Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 19.23 CPAR Pengelolaan Aset 5.23

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Saat ini pelaksanaan keamanan informasi menjadi bagian yang utuh dari proses bisnis dan evaluasi pelaksanaan diwujudkan dalam pengendalian internal yang dilakukan berkala Dalam pada itu, KANWIL DJPBN telah mempunyai daftar rekaman pelaksanaan pengendalian namun terbentuk secara terpisah (misal : manajemen komunikasi operasi berupa update antivirus dlm LPPI; pengendalian akses melaui form permintaan akun, perubahan akses user; pengelolaan insiden melalui laporan koordinasi pemulihan permasalahan) dan bentuk-bentuk pengamanan yang sesuai dengan tingkat kritikalitas data dan klasifikasinya, namun KANWIL DJPBN belum mempunyai prosedur standar keamanan manajemen informasi maka daftar rekaman pelaksanaan pengamanan masih disusun secara umum sebagai aktivitas operasional KANWIL DJPBN.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Melakukan survei, observasi dan analisis mengenai proses bisnis yang erat kaitannya dengan pengukuran kinerja keamanan informasi
Menentukan framework atau acuan dalam pengukuran kinerja
Menentukan tujuan pengukuran yang relevan dengan keamanan informasi
Menentukan indikator dalam bentuk kualitatif dan kuantitatif guna memudahkan pencapaian indikator
Mendefinisikan subjek metrik dalam proses bisnis pengendalian internal keamanan informasi KANWIL DJPBN. Termasuk kemungkinan adanya satker atau pihak eksternal / pihak ketiga yang masih dan perlu bertanggung jawab dalam keamanan informasi.

Sebaiknya pengukuran disusun berdasarkan bentuk kontrol atau pengendalian yang telah dibuat. Untuk kepentingan eskalasi Tingkat Kematangan ke level III, maka metode atau mekanisme pengukuran sebaiknya didokumentasikan secara resmi dalam SMKI. Menyusun seluruh bentuk pengendalian internal berdasarkan pengelolaan risiko keamanan informasi. Untuk eskalasi menuju level III hingga V maka KANWIL DJPBN perlu berbenah diri dalam melakukan monitoring sebagai bentuk perekaman berkala dari penerapan efektivitas metode pengamanan yang ada, apakah diperlukan pemutakhiran atau tidak.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.24 CPAR Pengelolaan Aset 5.24

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Pihak KANWIL DJPBN telah menerapkan tata tertib melalui pengimplementasian sejumlah kebijakan sebagaimana tertuang dalam PMK, KMK dan KEPDIRJEN. Khususnya Penerapan KMK.479/KMK.01/ 2010 Poin XI tentang HAKI, namun masih belum tersedianya prosedur penggunaan perangkat informasi milik pihak ketiga dengan memastikan aspek HAKI

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan kepemilikan aset pihak ketiga
Mendaftar semua aset atau perangkat informasi milik pihak ketiga
Melakukan pengendalian dengan bentuk kontrol berupa :

- Formulir penggunaan oleh pihak KANWIL DJPBN yang harus melalui persetujuan
- Daftar pengguna
- Kebutuhan penggunaan

Melakukan evaluasi serta menyusun pelaporan penggunaan asset/perangkat pihak ketiga.
Memisahkan data dan melakukan backup secara regular guna memastikan tidak bercampurnya data dan informasi guna menjaaga keamanan informasi KANWIL DJPBN
Melakukan pengecekan secara berkala terhadap aset untuk memastikan keamanan informasi.
Melaksanakan pelaporan berkala terhadap penggunaan asset informasi milik pihak ketiga baik berupa perangkat, data, software dll

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.25 CPAR Pengelolaan Aset 5.25

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN dalam proses menerapkan secara menyeluruh pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang, dan meski pengamanan fasilitas fisik pada lokasi kerja sudah diterapkan namun untuk dokumen kontrol pengendalian masih dirasa kurang.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Menentukan tingkat prioritas aset yang terdapat di KANWIL DJPBN
Mendaftar semua fasilitas pengamanan fisik di KANWIL DJPBN per bagian
Mengklasifikasikan fasilitas berdasarkan tingkat prioritas atau prioritas keamanan aset
Menyusun kategori peraturan pengamanan asset informasi (data, informasi, software, hardware, jaringan dan perangkat lainnya) terkait keamanan informasi yang ada di KANWIL DJPBN (lingkup yang lebih spesifik dengan pelaksanaan teknis)
Mengklasifikasikan zona pengamanan berdasarkan aset yang ada
Menyusun kebijakan pengamanan fisik berdasarkan klasifikasi zona
Menyusun bentuk kontrol seperti formulir, checklist, logbook
Menetapkan sanksi dan pelanggaran terhadap peraturan yang telah dibuat sebagaimana diatur oleh KMK.512/KMK.01/2010
Untuk menuju pada Tingkat Kematangan level III hingga level V maka tata tertib harus disosialisasikan dan dikomunikasikan kepada semua pihak.
Menyusun seluruh tata tertib secara tertulis dan mendokumentasikannya

sebagai arsip. Selain itu, mengevaluasi serta memonitoring proses penerapannya Untuk dapat menuju pada tingkat kepatuhan yang lebih baik, maka kepatuhan pada tata tertib sebaiknya dievaluasi berkala sehingga dapat dilakukan secara cepat mengenai pembaharuan atau perbaikan aset jika memang diperlukan sebagai upaya peningkatan tiap bulan atau semester. Setiap laporan evaluasi yang ada didokumentasikan secara resmi dan dikomunikasikan serta disosialisasikan kepada semua pihak pelaksana DJPBN			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.26 CPAR Pengelolaan Aset 5.26

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Di KANWIL DJPBN sedang dalam proses penerapan penuh pengelolaan alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik. Alokasi kunci masuk yang diterapkan secara fisik meliputi kartu tamu, buku tamu. satpam, sedangkan kunci elektronik meliputi Fingerprint, face recognition, cctv, kunci elektronik akses server depan, kunci elektronik akses server belakang. Pengelolaan penggunaan cukup baik namun belum adanya laporan detil pengelolaan akses pada asset / fasilitas dan evaluasi berkala mengenai pengelolaan tersebut.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Menentukan tingkat prioritas aset yang terdapat di KANWIL DJPBN
Mendaftar semua fasilitas pengamanan fisik di KANWIL DJPBN per bagian
Mengklasifikasikan fasilitas berdasarkan tingkat prioritas atau prioritas keamanan aset
Menyusun kategori pengamanan asset informasi (data, informasi, software, hardware, jaringan dan perangkat lainnya) terkait akses ke fasilitas fisik yang ada di KANWIL DJPBN (baik fisik dan elektronik)
Mengklasifikasikan zona pengamanan berdasarkan aset yang ada
Menyusun kebijakan pengamanan fisik berdasarkan klasifikasi zona
Menyusun bentuk kontrol seperti formulir, checklist, logbook
Menetapkan sanksi dan pelanggaran terhadap peraturan yang telah dibuat sebagaimana diatur oleh KMK.512/KMK.01/2010
Untuk menuju pada Tingkat Kematangan level III hingga level V maka tata tertib harus disosialisasikan dan dikomunikasikan kepada semua pihak.

Menyusun seluruh tata tertib secara tertulis dan mendokumentasikannya sebagai arsip. Selain itu, mengevaluasi serta memonitoring proses penerapannya Untuk dapat menuju pada tingkat kepatuhan yang lebih baik, maka kepatuhan pada tata tertib sebaiknya dievaluasi berkala sehingga dapat dilakukan secara cepat mengenai pembaharuan atau perbaikan aset jika memang diperlukan sebagai upaya peningkatan tiap bulan atau semester. Setiap laporan evaluasi yang ada didokumentasikan secara resmi dan dikomunikasikan serta disosialisasikan kepada semua pihak pelaksana DJPBN			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.27 CPAR Pengelolaan Aset 5.27

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Di KANWIL DJPBN secara menyeluruh sudah mempunyai infrastruktur komputasi yang terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya namun masih belum adanya mekanisme KANWIL DJPBN mengenai laporan evaluasi prasyarat pemeliharaan infrastruktur

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Melakukan identifikasi terhadap asset informasi perangkat keras infrastruktur komputasi sebagai BMN (Barang Milik Negara)
Menyusun mekanisme prasyarat infrastruktur setiap perangkat berdasarkan petunjuk manual aset
Menyusun petunjuk pengelolaan infrastruktur komputasi untuk masing-masing bagian sesuai KMK.21/KMK.01/2012 tentang pengelolaan BMN
Memastikan pihak yang berwenang menerima data infrastruktur yang diminta
Memastikan bahwa dokumentasi BMN termasuk aset informasi didalamnya beserta dokumen disimpan
Menyusun bentuk kontrol seperti logbook serta formulir pemeliharaan infrastruktur
Melakukan monitoring berkala sehingga dapat dilakukan tindakan secara cepat mengenai pembaharuan atau perbaikan aset BMN jika memang diperlukan sebagai upaya peningkatan pengamanan asset informasi
Untuk menuju pada Tingkat Kematangan level III hingga level V maka perlu adanya evaluasi pengelolaan BMN khususnya terkait dengan infrastruktur

komputasi yang telah disusun serta proses penerapannya saat ini di KANWIL DJPBN.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.28 CPAR Pengelolaan Aset 5.28

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Di KANWIL DJPBN secara menyeluruh sudah mempunyai infrastruktur komputasi yang terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya namun masih belum adanya mekanisme KANWIL DJPBN mengenai laporan evaluasi prasyarat pemeliharaan infrastruktur

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Melakukan identifikasi terhadap asset informasi perangkat keras infrastruktur komputasi sebagai BMN (Barang Milik Negara)
Menyusun mekanisme prasyarat infrastruktur setiap perangkat berdasarkan petunjuk manual aset
Menyusun petunjuk pengelolaan infrastruktur komputasi untuk masing-masing bagian sesuai KMK.21/KMK.01/2012 tentang pengelolaan BMN
Memastikan pihak yang berwenang menerima data infrastruktur yang diminta
Memastikan bahwa dokumentasi BMN termasuk aset informasi didalamnya beserta dokumen disimpan
Menyusun bentuk kontrol seperti logbook serta formulir pemeliharaan infrastruktur
Melakukan monitoring berkala sehingga dapat dilakukan tindakan secara cepat mengenai pembaharuan atau perbaikan aset BMN jika memang diperlukan sebagai upaya peningkatan pengamanan asset informasi
Untuk menuju pada Tingkat Kematangan level III hingga level V maka perlu adanya evaluasi pengelolaan BMN khususnya terkait dengan infrastruktur komputasi yang telah disusun serta proses penerapannya saat ini di KANWIL

DJPBN.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.29 CPAR Pengelolaan Aset 5.29

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN menstandarkan peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor) pada Poin V Pengendalian Fisik dan Lingkungan bag.e yang menjelaskan perangkat yang digunakan di luar lingkungan Kementerian Keuangan harus disetujui oleh Pihak Yang Berwenang dan ketentuan lainnya dalam Pedoman Pengamanan Perangkat, namun belum tersedia petunjuk mekanisme / prosedur pengamanan perangkat komputasi KANWIL DJPBN jika digunakan di luar lokasi kerja resmi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan kepemilikan aset KANWIL DJPBN yang akan dipinjam
Mendaftar semua aset atau perangkat informasi milik KANWIL DJPBN
Menyususn prosedur penggunaan BMN milik instansi yang digunakan di luar lokasi kerja resmi miliki pemerintah dengan memperhatikan aspek :

a. Izin penggunaan
b. Nomor asset BMN yang digunakan
c. Kategori asset
d. Jangka waktu penggunaan
e. Klausul penggunaan

Melakukan pengendalian dengan bentuk kontrol berupa :

- Formulir penggunaan dari pihak KANWIL DJPBN
- Daftar pengguna
- Kebutuhan penggunaan

Melakukan evaluasi serta menyusun pelaporan penggunaan

Memisahkan akses penggunaan perangkat komputasi internal dengan eksternal. Untuk penggunaan eksternal sebaiknya dilakukan pembatasan akses dengan tingkatan lebih rendah daripada penggunaan internal Pengguna perangkat komputasi di luar lingkungan kerja resmi wajib melaporkan secara berkala kepada pihak KANWIL DJPBN mengenai perangkat instansi yang digunakan secara tertulis			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.30 CPAR Pengelolaan Aset 5.30

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN menyiapkan secara penuh konstruksi ruang penyimpanan perangkat pengolah informasi penting dengan menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Melakukan identifikasi terhadap asset informasi perangkat keras komputasi sebagai BMN (Barang Milik Negara) sekaligus kebutuhan konstruksi ruang penyimpanan

Menyusun mekanisme prasyarat penempatan setiap perangkat berdasarkan petunjuk manual aset dengan tingkat risiko terendah berdasar KMK.479/KMK.01/2010 berdasarkan aspek :

- Akses
- Lokasi
- Tujuan penggunaan asset
- Otorisasi

Menyusun petunjuk pengelolaan pengamanan perangkat untuk masing-masing bagian sesuai KMK.21/KMK.01/2012 tentang pengelolaan BMN

Memastikan pihak yang berwenang menerima data penempatan perangkat yang diminta

Memastikan bahwa dokumentasi BMN termasuk aset informasi didalamnya beserta dokumen disimpan Menyusun bentuk kontrol seperti logbook serta formulir pemeliharaan infrastruktur Melakukan monitoring berkala sehingga dapat dilakukan tindakan secara cepat mengenai pembaharuan atau perbaikan aset BMN jika memang diperlukan sebagai upaya peningkatan pengamanan asset informasi Untuk menuju pada Tingkat Kematangan level III hingga level V maka perlu adanya evaluasi pengelolaan BMN khususnya terkait dengan infrastruktur komputasi yang telah disusun serta proses penerapannya saat ini di KANWIL DJPBN.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 19.31 CPAR Pengelolaan Aset 5.31

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN telah mempunyai beberapa proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting, dokumentasi proses inspeksi dan perawatan perangkat komputer dalam proses diterapkan namun masih kurangnya bentuk kontrol pengendaliannya.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Melakukan identifikasi terhadap asset informasi perangkat keras komputasi sebagai BMN (Barang Milik Negara) sekaligus kebutuhan konstruksi ruang penyimpanan

Menyusun mekanisme prasyarat penempatan setiap perangkat berdasarkan petunjuk manual aset dengan tingkat risiko terendah berdasar KMK.479/KMK.01/2010 berdasarkan aspek :

- Akses
- Lokasi
- Tujuan penggunaan asset
- Otorisasi

Menyusun petunjuk pengelolaan pengamanan perangkat untuk masing-masing bagian sesuai KMK.21/KMK.01/2012 tentang pengelolaan BMN

Memastikan pihak yang berwenang menerima data penempatan perangkat yang diminta

Memastikan bahwa dokumentasi BMN termasuk aset informasi didalamnya

<table>
<tr><td colspan="4">beserta dokumen disimpan
Menyusun bentuk kontrol seperti logbook serta formulir pemeliharaan infrastruktur
Melakukan monitoring berkala sehingga dapat dilakukan tindakan secara cepat mengenai pembaharuan atau perbaikan aset BMN jika memang diperlukan sebagai upaya peningkatan pengamanan asset informasi
Untuk menuju pada Tingkat Kematangan level III hingga level V maka perlu adanya evaluasi pengelolaan BMN khususnya terkait dengan infrastruktur komputasi yang telah disusun serta proses penerapannya saat ini di KANWIL DJPBN.</td></tr>
<tr><td>Nama & TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
<tr><td colspan="4">Section 4 : Tindak lanjut dan verifikasi</td></tr>
<tr><td colspan="4">Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera</td></tr>
<tr><td>Nama & TTD</td><td colspan="2">Disposisi oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
</table>

Form 19.32 CPAR Pengelolaan Aset 5.32

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Di KANWIL DJPBN telah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga dimana pengiriman dilengkapi dengan Surat Pengantar dan Surat Tugas dari Instansi /Organisasi yang memberi tugas pengiriman barang dan /atau Surat Tugas Pemuatan Barang dari dalam lingkungan gedung dan/atau bangunan. Khusus Dokumen dilengkapi pula dengan Sistem 4 Amplop

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan kepemilikan dokumen pihak ketiga
Mendaftar semua aset atau informasi milik pihak ketiga
Melaksanakan mekanisme pengelolaan keseluruhan dokumen dan perangkat BMN terkait keamanan informasi berdasarkan KMK.21/KMK.01/2012 dengan sejumlah penyempurnaan agar pengendalian internal pada pengelolaan keamanan asset informasi menjadi lebih baik,.
Mengevaluasi rancangan kebijakan /rancangan prosedur sesuai dengan hasil review kebijakan / prosedur sebelumnya
Melakukan pengelolaan peredaran dokumen pengiriman terkait kebijakan dan prosedur keamanan berdasarkan tiap bagiannya.
Melaksanakan pengikatan kontrak terkait pengiriman asset informasi dengan pihak ketiga
Penggunaan daftar induk nomor registrasi dokumen pengiriman secara khusus / spesifik agar memudahkan pemilahannya dari dokumen pengelolaan lainnya
Penggunaan list / daftar dokumen pengiriman yang selalu diupdate setiap kali terjadi penambahan dokumen terkait pengiriman asset informasi dan

<table>
<tr><td colspan="4">pengelolaan keamanan informasinya
Melaksanakan pengelolaan kontrol akses berdasar dokumen kebijakan dan prosedur terutama untuk pihak ketiga yang terkait di dalamnya.
Sebagai upaya meningkatkan Tingkat Kematangan level III hingga level V, maka KANWIL DJPBN sebaiknya melakukan evaluasi berkala terhadap mekanisme atau prosedur pengelolaan pengiriman asset dan dokumen pengiriman terkait kebijakan pengelolaan keamanan informasi sekaligus sebagai pembaruan terhadap kebijakan yang dipandang perlu untuk direvisi/ditarik peredarannya.</td></tr>
<tr><td>Nama
&
TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
<tr><td colspan="4">Section 4 : Tindak lanjut dan verifikasi</td></tr>
<tr><td colspan="4">Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera</td></tr>
<tr><td>Nama
&
TTD</td><td colspan="2">Disposisi oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
</table>

Form 19.33 CPAR Pengelolaan Aset 5.33

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

DI KANWIL DJPBN telah tersedia beberapa peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi dengan mendasar kepada KMK.479/KMK.01/2010 Poin VI dimana menjelaskan perlunya pengamanan fisik yang memadai melalui penggunaan pintu elektronik, sistem pemadam, alarm dan aksesibilitas ke ruang dengan klasifikasi RAHASIA hanya diberikan kepada pegawai yang berwenang, dll. Permasalaahannya tata tertib pengamanan masih berupa peraturan secara umum belum didefinisikan berdasarkan kepentingan aset yang dimiliki oleh KANWIL DJPBN

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Melakukan identifikasi terhadap asset informasi perangkat keras komputasi sebagai BMN (Barang Milik Negara) sekaligus kebutuhan konstruksi ruang penyimpanan

Menyusun mekanisme prasyarat penempatan setiap perangkat berdasarkan petunjuk manual aset dengan tingkat risiko terendah berdasar KMK.479/KMK.01/2010 berdasarkan aspek :

- Akses
- Lokasi
- Tujuan penggunaan asset
- Otorisasi

Mendefinsikan risiko yang terjadi dengana adanya penggunaan perangkat TI yang membahayakan aset informasi di KANWIL DJPBN. Seperti penggunaan alat elektronik, perangkat digital seperti micro SD, USB, kamera/handycam, dll
Menyusun tata tertib baru bagi penggunaan lokasi kerja baik oleh pihak internal ataupun pihak eksternal
Melaksanakan bentuk pengamanan baru dengan kontrol pengendalian yang lebih ketat seperti :

- Pemberlakuan adanya logbook pengunjung
- Penggunaan kamera CCTV serta penangung jawab sesuai jadwal yang telah dibuat.

Menyusun petunjuk pengelolaan pengamanan perangkat untuk masing-masing bagian sesuai KMK.21/KMK.01/2012 tentang pengelolaan BMN
Memastikan pihak yang berwenang menerima data penempatan perangkat yang diminta
Memastikan bahwa dokumentasi BMN termasuk aset informasi didalamnya beserta dokumen disimpan
Menyusun bentuk kontrol seperti logbook serta formulir pemeliharaan infrastruktur
Melakukan monitoring berkala sehingga dapat dilakukan tindakan secara cepat mengenai pembaharuan atau perbaikan aset BMN jika memang diperlukan sebagai upaya peningkatan pengamanan asset informasi
Untuk menuju pada Tingkat Kematangan level III hingga level V maka perlu adanya evaluasi pengelolaan BMN khususnya terkait dengan infrastruktur komputasi yang telah disusun serta proses penerapannya saat ini di KANWIL DJPBN.

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**

Section 4 : Tindak lanjut dan verifikasi

Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera

Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 19.34 CPAR Pengelolaan Aset 5.34

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Di KANWIL DJPBN telah mempunyai proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi dimana pihak ketiga yang memasuki ruang server, pusat data, dan area kerja yang berisikan aset informasi yang RAHASIA harus didampingi pegawai unit TIK sepanjang waktu kunjungan. Waktu keluar masuk serta maksud kedatangan harus dicatat dalam buku catatan kunjungan (KMK.479 /KMK01/2010)

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Menyusun mekanisme prasyarat akses lokasi/wilayah kerja sesuai KMK No.479 /KMK.01/2010 berdasarkan aspek :

- Akses
- Lokasi
- Tujuan
- Otorisasi

Menyusun petunjuk pengelolaan pengamanan perangkat untuk masing-masing bagian sesuai KMK.21/KMK.01/2012 tentang pengelolaan BMN

Menyusun kontrol pengendalian seperti :

- Peninjauan latar belakang pihak ketiga
- Logbook pengunjung

Jika berkaitan dengan pemeliharaan sistem oleh pihak ketiga, maka memishakan data penting dan tidak pada sistem atau aplikasi.

Menjamin keamanan dengan kontrak perjanjian berasaskan HAKI dan ketentuan hukum yang belaku.

Melakukan monitoring berkala sehingga dapat dilakukan tindakan secara cepat mengenai pembaharuan atau perbaikan aset BMN jika memang diperlukan sebagai upaya peningkatan pengamanan asset informasi Untuk menuju pada Tingkat Kematangan level III hingga level V maka perlu adanya evaluasi pengelolaan BMN khususnya terkait dengan akses pada asset informasi di lingkungan kerja yang telah disusun serta proses penerapannya saat ini di KANWIL DJPBN.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Lampiran L

Halaman ini sengaja dikosongkan

L.1 CPAR Area V Teknologi

Form 20.1 CPAR Teknologi 6.1

<table>
<tr><td colspan="4">KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR
GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640</td></tr>
<tr><td colspan="4">Section 1 : Obyek</td></tr>
<tr><td colspan="4">Layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan</td></tr>
<tr><td>Nama & TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
<tr><td colspan="4">Section 2 : Penyebab / Pendukung</td></tr>
<tr><td colspan="4">Di KANWIL DJPBN telah menerapkan layanan TIK (sistem komputer) yang menggunakan internet untuk dilindungi dengan lebih dari 1 lapis pengamanan (proxy dan firewall)</td></tr>
<tr><td>Nama & TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
<tr><td colspan="4">Section 3 : Usulan tindakan perbaikan</td></tr>
<tr><td colspan="4">Mendefinisikan pembatasan berdasarkan hak akses
Menyusun mekanisme pengelolaan pengamanan (SOP) berdasarkan hak akses
Membuat rekomendasi dokumentasi pengelolaan pengamanan tersebut baik secara teknologi atau fisik (faktor manusia) pada KPTIK
Dokumentasi dibedakan menjadi dua pengguna antara lain untuk tim penanggungjawab pengelolaan keamanan dan pengguna umum
- Bagi tim penanggungjawab pengelolaan keamanan, pengelolaan berlapis didetailkan menjadi konfigurasi sistem proxy, otentikasi sistem atau aplikasi
- Bagi pengguna umum (non admin) maka dokumentasi lebih pada panduan pengamanan penggunaan akses TIK</td></tr>
<tr><td>Nama & TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
</table>

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 20.2 CPAR Teknologi 6.2

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN secara menyeluruh telah menyediakan jaringan komunikasi yang disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan tingkatan hak akses pengguna
Menginventarisir hak akses – hak akses seluruh pelaksana
Mendokumentasikan seluruh hak akses – hak akses pada semua aset TIK
Menentukan bentuk pengamanan tiap hak akses pengguna
Mendokumentasikan bentuk pengamana secara tertulis terkait pengelolaan hak akses tersebut
Dokumentasi pengamanan dibedakan menjadi dua pengguna antara lain tim penanggungjawab pengelolaan keamanan TIK dan pengguna umum

- Bagi tim penanggungjawab pengelolaan keamanan, pengelolaan berlapis didetailkan menjadi konfigurasi sistem proxy, otentikasi sistem atau aplikasi
- Bagi pengguna umum (non admin) maka dokumentasi lebih pada panduan pengamanan pribadi

Untuk meningkatkan Tingkat Keamanan menjadi level III hingga V, maka sebaiknya dokumentasi yang disusun dilakukan monitoring berkala

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 20.3 CPAR Teknologi 6.3

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset komputer dan perangkat jaringan, yang dimutakhirkan sesuai perkembangan dan kebutuhan

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN secara menyeluruh telah mempunyai konfigurasi standar untuk keamanan sistem bagi keseluruhan aset komputer dan perangkat jaringan, yang dimutakhirkan sesuai perkembangan dan kebutuhan terutama untuk SPAN yang melakukan pembatasan akses IP

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan kebutuhan sistem yang ada termasuk konfigurasinya
Menginventarisir avalaibilitas aplikasi sistem yang dipakai di KANWIL DJPBN
Merekomendasikan sistem atau aplikasi terbaru (selain SPAN) yang disesuaikan dengan kebutuhan sistem informasi yang terdapat di KANWIL DJPBN
Mendefinisikan perencanaan pemutakhiran dengan :

- Mendefinsikan risiko implementasi
- Perencanaan finansial implementasi
- Kelayakan perangkat dalam meningkatkan efisiensi dan efektifitas proses bisnis yang ada

Untuk meningkatkan Tingkat Keamanan menjadi level III hingga V, maka sebaiknya dibuatkan secara tertulis prosedur dan instruksi kerja

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 20.4 CPAR Teknologi 6.4

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda secara rutin menganalisis kepatuhan penerapan konfigurasi standar yang ada

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN telah menerapkan secara rutin analisis kepatuhan penerapan konfigurasi standar yang ada di beberapa perangkat TIK namun tidak terdokumentasikan secara detail dan resmi perubahan konfigurasi dan penjelasan tambahan untuk seluruh perangkat

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan teknologi atau sistem yang akan dilakukan konfigurasi
Menggunakan *tools* pengelolaan konfigurasi
Menyusun kontrol pengendalian mengenai perubahan konfigurasi atau tindakan korektif akan adanya insiden pada saat melakukan konfigurasi seperti formulir, laporan (report), dan *checklist* yang termasuk di dalamnya dalam keterlibatan *people*, *process*, dan *technologies*.
Untuk meningkatkan Tingkat Keamanan menjadi level III hingga V, maka sebaiknya dilakukan monitoring semua kontrol pengendalian terhadap semua perubahan / konfigurasi.

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 4 : Tindak lanjut dan verifikasi

Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera

Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 20.5 CPAR Teknologi 6.5

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan / keutuhan konfigurasi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Jaringan, sistem dan aplikasi yang digunakan di KANWIL DJPBN dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi melalui pengecekan pada *network configuration*, *bandwith*, *ping*, dll namun untuk pengecekan celah kelemahan pada aplikasi umumnya dilaksanakan Kantor Pusat, SPAN & Pusintek. Sedangkan pengecekan jaringan pada KPTIK terhadap sistem intranet belum melakukan pengecekan celah kelemahan dan perubahan konfigurasi yang dilakukan pihak yang tidak bertanggungjawab.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan sistem apa saja yang akan dilakukan pemindaian secara berkala
Jika proses dokumentasi pemindaian harus berdasarkan konfigurasi maka perlu adanya panduan konfigurasi pemindaian (SOP)
Mendokumentasikan pelaporan pemindaian jika terdapat kelemahan atau insiden.
Untuk meningkatkan peran pengelolaan Tingkat Keamanan menjadi level III hingga V, maka sebaiknya pelaporan pengecekan kelemahan dan perubahan dituliskan sebagai masukan untuk pimpinan dalam melaksanakan kebijakan selanjutnya

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 20.6 CPAR Teknologi 6.6

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Keseluruhan infrastruktur dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN secara menyeluruh melakukan proses pemindaian atau monitoring bandwith, virus, dan server. Namun untuk proses pemindaian tersebut, memang dilakuka secara otomatis dalam sistem sehingga tidak ada proses dokumentasi di dalamnya.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan sistem apa saja yang akan dilakukan pemindaian secara berkala
Menginventarisir sistem yang akan dilakukan pemindaian secara berkala
Jika proses dokumentasi pemindaian harus berdasarkan konfigurasi maka perlu adanya panduan konfigurasi pemindaian (SOP) termasuk mekanisme pelaporan dan pihak-pihak yang wajib menerima hasil pelaporan tersebut
Mendokumentasikan pelaporan pemindaian jika terdapat kelemahan atau insiden.
Untuk meningkatkan poin pengelolaan keamanan informasi ke Tingkat Keamanan menjadi level III hingga V, maka sebaiknya pelaporan dituliskan secara terstruktur.
Seluruh mekanisme diatas termasuk pendokumentasiannya hendaknya dilakukan berkala, diuji efektivitasnya dan dijadikan report sebagai bahan pertimbangan kebutuhan kapasitas, kebutuhan pengamanan dan kebutuhan konfigurasi yang memenuhi kebutuhan masa mendatang

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 20.7 CPAR Teknologi 6.7

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Setiap perubahan dalam sistem informasi secara otomatis dan menyeluruh terekam di dalam log, namun sistem informasi yang dibagi pada unit vertical tidak bisa melihat / tidak dibuatkan menu untuk melihat listing rekapitulasi log misal : rekap log user pada akses SPAN sehingga permintaan data rekap log harus melalui permohonan lagi pada Kantor Pusat dan SPAN

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Berdasarkan analisis tersebut maka usulan / rekomendasinya adalah :
Menyusun prosedur mengenai proses *change management* (perubahan) yang terdokumentasi dan telah terdefinsikan.
Dokumentasi perubahan disesuaikan berdasarkan prosedur serta tanggung jawab sumber daya manusia (SDM)
Selain itu, prosedur tersebut diklasifikasikan berdasarkan aset atau infrastruktur
Terdapat beberapa fase dalam prosedur manajemen perubahan antara lain :

a. Permintaan perubahan (*request of change*)
b. Identifikasi, prioritasi, inisiasi perubahan
c. Otorisasi kelayakan perubahan
d. Pendekatan proses perubahan
e. Testing perubahan
f. Testing user
g. Dokumentasi
h. Monitoring perubahan
i. Mendefinisikan tanggung jawab otoritisasi personel dan pengguna sistem atau aplikasi tersebut
j. Pelaporan perubahan

Untuk meningkatkan Tingkat Keamanan menjadi level III hingga V, maka sebaiknya semua mekanisme yang disusun dilakukan monitoring serta evaluasi. Selain itu terdapat adanya penanganan lebih lanjut jika ada identifikasi kelemahan pada saat proses monitoring			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 20.8 CPAR Teknologi 6.8

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Upaya-upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Secara sistem semua aktivitas terekam di dalam log karena dibutuhkan input pengguna yang diset secara khusus, namun kejadian ini belum pernah ditemukan sehingga tidak ada report log tentang pengaksesan oleh yang tidak berhak dan sistem tersebut nantinya akan terhubung dengan sistem SPAN melalui VPN. Selain dari itu, komputer tersebut tidak dapat terhubung dengan jaringan internet luar. Ini juga merupakan salah satu bentuk pengamanan untuk mengantisipi tindakan-tindakan hacking oleh pihak yang tidak bertanggungjawab. Di tingkat Kanwil DJPBN, belum adanya laporan resmi mengenai insiden serta tindakan korektif atas insiden yang terjadi namun semua tindakan penyimpangan terekam otomatis dalam log aktivitas sistem.

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Berdasarkan *Handbook CISRT sub section Log-Files Analysis* maka berikut usulan terkait

Mendefinisikan kriteria record data dan informasi pada logfile seperti :

- User atau pengguna yang logon pada sistem
- Media logon yang digunakan
- Insiden atau problem yang terjadi (jika ada)
- Timestamp yaitu waktu pada record tersebut. Biasanya untuk sinkronisasi maka dilakukan dengan menggunakan software NTP (Net Work Protocol) guna menyamakan bagian waktu untuk semua daerah di dunia
- Keaslian log seperti nama internet, mac address, nomor software, dll
- Otentikasi log biasanya dihasilkan sesuai dengan waktu file diambil

Mendefinisikan jenis log dalam berbagai kategori seperti file yang tergolong *harm* atau *event file* dengan menggunakan alarm Menentukan tim personel guna mengkaji *logfile* yang ada serta melakukan pelaporan resmi kepada bagian atau unit terkait Kanwil DJPBN.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 20.9 CPAR Teknologi 6.9

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Semua log dianalisis secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Secara sistem SPAN menganalisis secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik) berdasarkan KMK.479/ KMK.01/2010 Poin VI, namun report evaluasi berkala sistem SPAN tidak disampaikan pada Kantor vertical kecuali terjadi insiden dan gangguan sistem lainnya. Di tingkat Kanwil DJPBN log belum dianalisis secara berkala dan dijadikan rujukan hanya jika terdapat celah kelemahan pada sistem atau aplikasi. Log belum didokumentasikan sebagai laporan tertulis.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Pemeriksaan data masukan (standar KMK.479/KMK.01/2010) dengan mempertimbangkan :

- Pengkajian secara berkala terhadap field kunci (*key field*) untuk mengkonfirmasi keabsahan dan integritas data
- Memeriksa dokumen *hardcopy* untuk memastikan tidak adanya perubahan yang tidak melalui otorisasi
- Menampilkan pesan dalam menanggapi kesalahan validasi
- Prosedur untuk menguji kewajaran data masukan
- Menguraikan tanggungjawab dari seluruh pegawai yang terkait perekaman data

Mendefinisikan log yang akan dianalisis.
Menentukan jangka waktu pelaporan /log.
Menganalisis log apakah terdapat celah kelemahan sehingga dapat dijadikan pertimbangan pada saat pengambilan keputusan.
Untuk meningkatkan ke Tingkat Kematangan selanjutnya bagi Kanwil DJPBN

khususnya bagi tim pengamaan informasi, maka log tersebut dimonitoring, dikaji dan dilaporkan secara tertulis			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 20.10 CPAR Teknologi 6.10

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

DJPBN telah menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada berdasarkan KMK.479/ KMK.01/2010 Poin VI bag D.4 Pengelolaan Keamanan Jaringan. SPAN sendiri memanfaatkan penggunaan enkripsi namun tidak terdefinisikan dalam dokumen / website mengenai enkripsi tersebut

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

(Berdasarkan analisis pada KMK.479/KMK.01/2010) :

Mengidentifikasi kondisi dari suatu kegiatan / aset yang menetukan bahwa isi informasi harus dilindungi seperti risiko kegiatan, media pengiriman informasi dan tingkat perlindungan yang dibutuhkan

Menyusun prosedur penerapan enkripsi berdasarkan sistem atau aplikasi dimana keperluan enkripsi untuk perlindungan informasi yang sifatnya SANGAT RAHASAI, RAHASIA dan TERBATAS yang melalui perangkat *mobile computing*, *removable media*, atau jalur komunikasi

Menerapkan standar minimal untuk penggunaan enkripsi berdasarkan penilaian risiko, antara lain jenis, kekuatan, dan kualitas dari algoritma enkripsi yang digunakan

Melaksanakan pengelolaan *kriptografi key*, seperti perlindungan *kriptografi key*, pemulihan informasi terenkripsi dalam hal kehilangan atau kerusakan *kriptografi key*, dan

Sebelum dirilis, sebaiknya dilakukan proses testing enkripsi baik aktif atau pasif guna mengecek kehandalan enkripsi terkait pemeriksaan suatu konten dan kecepatan pemrosesan pada sistem.

Melakukan pelaporan berkala penggunaan enkripsi guna mengecek kelemahan sistem			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 20.11 CPAR Teknologi 6.11

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda mempunyai standar dalam menggunakan enkripsi

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

DJPBN telah menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada berdasarkan KMK.479/ KMK.01/2010 Poin VI bag D.4 Pengelolaan Keamanan Jaringan. SPAN sendiri memanfaatkan penggunaan enkripsi namun tidak terdefinisikan dalam dokumen/ website mengenai enkripsi tersebut

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

(Berdasarkan analisis pada KMK.479/KMK.01/2010) :

Mengidentifikasi kondisi dari suatu kegiatan / aset yang menetukan bahwa isi informasi harus dilindungi seperti risiko kegiatan, media pengiriman informasi dan tingkat perlindungan yang dibutuhkan

Tim pengamanan informasi / unit TIK pusat harus menetapkan, mengembangkan dan menerapkan sistem kriptografi untuk perlindungan informasi dan membuat rekomendasi yang tepat bagi penerapannya

Menyusun prosedur penerapan enkripsi berdasarkan sistem atau aplikasi dimana keperluan enkripsi untuk perlindungan informasi yang sifatnya SANGAT RAHASAI, RAHASIA dan TERBATAS yang melalui perangkat *mobile computing*, *removable media*, atau jalur komunikasi

Menerapkan standar minimal untuk penggunaan enkripsi berdasarkan penilaian risiko, antara lain jenis, kekuatan, dan kualitas dari algoritma enkripsi yang digunakan

Melaksanakan pengelolaan *kriptografi key*, seperti perlindungan *kriptografi key*, pemulihan informasi terenkripsi dalam hal kehilangan atau kerusakan *kriptografi key*, dan

Sebelum dirilis, sebaiknya dilakukan proses testing enkripsi baik aktif atau

<table>
<tr><td colspan="4">pasif guna mengecek kehandalan enkripsi terkait pemeriksaan suatu konten dan kecepatan pemrosesan pada sistem.
Melakukan pelaporan berkala penggunaan enkripsi guna mengecek kelemahan sistem</td></tr>
<tr><td>Nama & TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
<tr><td colspan="4">Section 4 : Tindak lanjut dan verifikasi</td></tr>
<tr><td colspan="4">Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera</td></tr>
<tr><td>Nama & TTD</td><td colspan="2">Disposisi oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
</table>

Form 20.12 CPAR Teknologi 6.12

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

DJPBN telah menerapkan enkripsi sesuai kebijakan pengelolaan yang ada berdasarkan KMK.479/ KMK.01/2010 Poin VI bag D.4 Pengelolaan Keamanan Jaringan. SPAN sendiri memanfaatkan penggunaan enkripsi namun tidak terdefinisikan dalam dokumen/ website mengenai enkripsi tersebut

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

(Berdasarkan analisis pada KMK.479/KMK.01/2010) :
Mengidentifikasi kondisi dari suatu kegiatan / aset yang menetukan bahwa isi informasi harus dilindungi seperti risiko kegiatan, media pengiriman informasi dan tingkat perlindungan yang dibutuhkan
Tim pengamanan informasi / unit TIK pusat harus menetapkan, mengembangkan dan menerapkan sistem kriptografi untuk perlindungan informasi dan membuat rekomendasi yang tepat bagi penerapannya
Menyusun prosedur penerapan enkripsi berdasarkan sistem atau aplikasi dimana keperluan enkripsi untuk perlindungan informasi yang sifatnya SANGAT RAHASAI, RAHASIA dan TERBATAS yang melalui perangkat *mobile computing, removable media*, atau jalur komunikasi
(Jika perlu untuk layanan yang membutuhkan privasi tinggi maka perlu adanya sertifikat elektronik)
Menerapkan standar minimal untuk penggunaan enkripsi berdasarkan penilaian risiko, antara lain jenis, kekuatan, dan kualitas dari algoritma enkripsi yang digunakan
Melaksanakan pengelolaan *kriptografi key*, seperti perlindungan *kriptografi*

key, pemulihan informasi terenkripsi dalam hal kehilangan atau kerusakan *kriptografi key*, dan Sebelum dirilis, sebaiknya dilakukan proses testing enkripsi baik aktif atau pasif guna mengecek kehandalan enkripsi terkait pemeriksaan suatu konten dan kecepatan pemrosesan pada sistem. Melakukan pelaporan berkala penggunaan enkripsi guna mengecek kelemahan sistem sekaligus untuk menetukan siklusnya apakah tetap digunakan, dimodifikasi, diganti atau dihapuskan.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 20.13 CPAR Teknologi 6.13

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 2 : Penyebab / Pendukung

Semua sistem termasuk SPAN dan sejumlah aplikasi secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas / panjangnya dan penggunaan kembali password lama berdasarkan KMK No.512/KMK.01/ 2010

	Diajukan oleh :	**Disetujui oleh :**	**Tanggal :**
Nama & TTD	**(Mustaqim Siga)**	**Kepala Bagian Umum**	

Section 3 : Usulan tindakan perbaikan

Mendefinisikan semua aset informasi (pribadi dan instansi)
Menyusun kategori peraturan pengamanan data pribadi termasuk penggunaan akun dan kata sandi terkait keamanan informasi yang ada di KANWIL DJPBN (lingkup yang lebih spesifik dengan pelaksanaan teknis)
Penyusunan prosedur otomatisasi penggantian usename dan password dengan melihat aspek seperti di bawah ini :

- Prioritas siste atau aplikasi yang menerapkan otomatisasi
- (jangka waktu) username dan password lama

Melaksanakan standar pengamanan akun dan kata sandi yaitu :

a. Memakai kata sandi yang tidak mudah ditebak
b. Mengubah kata sandi yang telah diberikan oleh unit TIK Eselon I pada saat pertama kali digunakan
c. Mengubah kata sandi secara berkala, dan paling lama dalam jangka waktu 90 (Sembilan puluh) hari.
d. Melindungi informasi penting miliki Kementerian keuangan yang ada dalam perangkat computer dengan cara memakai screen saver yang aktif setelah 10 (sepuluh) menit tidak digunakan

e. Mengaktifkan konfigurasi yang akan mematikan perangkat computer setelah 30 (tiga puluh) menit tidak digunakan

Menghindari hal-hal yang telah datur dalam larangan penggunayaitu :

a. Mengungkapkan atau berbagi kata sandi melalui media apapun
b. Membuat kata sandi sama di sistem TIK di lingkungan Kementerian Keuangan dengan kata sandi yang digunakan di luar sistem TIK Kementerian Keuangan
c. Menggunakan fasilitas ingat kata sandi (remember password) dalam mengakses sistem operasi, surat elektronik, sistem jaringan/ internet
d. Menuliskan kata sandi dimanapun dan/atau menyimpan kata sandi di berkas elektronik pada setiap sistem komputer

Menetapkan sanksi dan pelanggaran terhadap peraturan yang telah dibuat sebagaimana diatur KMK.512/KMK.01/2010

Untuk menuju pada Tingkat Kematangan level III hingga level V maka tata tertib harus disosialisasikan dan dikomunikasikan kepada semua pihak.

Menyusun seluruh tata tertib secara tertulis dan mendokumentasikannya sebagai arsip. Selain itu, mengevaluasi serta memonitoring proses penerapannya

Untuk dapat menuju pada tingkat kepatuhan yang lebih baik, maka kepatuhan pada tata tertib sebaiknya dievaluasi berkala tiap bulan atau semester. Setiap laporan evaluasi yang ada didokumentasikan secara resmi dan dikomunikasikan serta disosialisasikan kepada semua pihak pelaksana DJPBN

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**

Section 4 : Tindak lanjut dan verifikasi

Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera

Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 20.14 CPAR Teknologi 6.14

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**

Section 2 : Penyebab / Pendukung

Akses yang digunakan untuk mengelola sistem (administrasi sistem) pada SPAN secara menyeluruh telah menggunakan bentuk pengamanan khusus yang berlapis

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**

Section 3 : Usulan tindakan perbaikan

Menetapkan PIC (*person in charge*) atau penanggung jawab dari aset sistem yang ada
Menentukan bentuk pengamanan (kategori khusus yang berlapis) sesuai aset sistem atau aplikasi yang ada di Kanwil DJPBN
Menentukan aset berdasarkan prioritas risiko
Melakukan kajian risiko sebelum memberikan hak akses kepada pihak ketiga dan menetapkan kontrol keamanan berdasarkan hasil kajian tersebut
Membuat prosedur pengamanan dan pengendalian berdasarkan aset sistem serta pihak pengelola/*custodian* yang ada
Secara berkala pelaksana melakukan monitoring terhadap pengelolaan akses sistem
Membuat pelaporan monitoring guna mengetahui tindakan yang diambil untuk pengelolaan akses sistem selanjutnya sebagai upaya peningkatan control secara berkelanjutan
Untuk menyusun bentuk kontrol maka sebaiknya disesuaikan dengan aset yang telah ditentukan
Untuk kepentingan eskalasi Tingkat Kematangan ke level III dan IV, maka KANWIL DJPBN perlu melakukan evaluasi pengelola / kepemilikan berdasarkan histori pelaksanaan pengamanan tiap pengelola aset sistem ke

dalam kebijakan / prosedur atau rencana strategis keamanan informasi lingkup Kanwil DJPBN.			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 20.15 CPAR Teknologi 6.15

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login,dan penarikan akses

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Sistem dan aplikasi yang digunakan lingkup Kanwil sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login, dan penarikan akses. Akses interface SPAN sendiri melakukan timeouts, lockout dan penarikan akses. Di tingkat Kanwil, penerapan sistem atau aplikasi belum secara otomatis menggunakan proses otomatisasi waktu akses , *timeout*, serta *lockout*.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

(Berdasar KMK.479/KMK.01/2010)
Prosedur pengendalian akses ke sistem dan aplikasi dengan memperhatikan :
Prosedur akses yang aman
Identifikasi dan otorisasi pengguna dimana pengguna harus memiliki akun yang unik dan hanya digunakan untuk peruntukannya dmana proses otorisasi menggunakan teknik autentifikasi yang sesuai untuk memvalidasi identitas pengguna
Sistem pengelolaan kata sandi
Penyusunan prosedur otomatisasi penggantian *usename dan password* dengan melihat aspek seperti di bawah ini

- Prioritas sistem atau aplikasi yang menerapkan otomatisasi
- (jangka waktu) username dan password lama
- Pengguna aplikasi (umum ataukah admin)

Lock outs dimana sistem akan mengunci akses kepada aplikasi jika pengguna salah 3 (tiga) kali memasukkan username dan password

<table>
<tr><td colspan="4">Penghapusan atau penonaktifan akses pelaksana yang telah berubah tugas dan/atau fungsinya setelah penugasan berakhir atau mutasi
Pemeriksaan, penghapusan atau penonaktifan akun pelaksana secara berkala dan untuk pengguna yang memiliki lebih dari 1 (satu) akun
Penggunaan system utilities dimana unit TIK harus membatasi dan mengendalikan penggunaan system utilities
Fasilitas session time-out harus diaktifkan dimana sistem dan aplikasi menutup dan mengunci layar computer, aplikasi dan koneksi jaringan apabila tidak ada aktivitas penggunaan setelah periode tertentu
Pembatasan waktu koneksi, unit TIK harus membatasi waktu koneksi untuk sistem informasi dan aplikasi yang memiliki klasifikasi RAHASIA dan SANGAT RAHASIA
Prosedur tersebut harus didokumentasikan secara tertulis serta dikomunikasikan secara internal pada bagian tertentu yang terkait
Untuk meningkatkan ke Tingkat Kematangan level III hingga level selanjutnya maka KANWIL DJPBN sebaiknya melakukan monitoring serta pelaporan berkala</td></tr>
<tr><td>Nama & TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
<tr><td colspan="4">Section 4 : Tindak lanjut dan verifikasi</td></tr>
<tr><td colspan="4">Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera</td></tr>
<tr><td>Nama & TTD</td><td colspan="2">Disposisi oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
</table>

Form 20.16 CPAR Teknologi 6.16

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Pengamanan data dan informasi pada SPAN dilengkapi dengan hal-hal berikut, diantaranya : Firewall, Bluecoat Web Filter, Anti SPAM sebagai perangkat pengamanan lalu lintas data internet dan intranet dengan komputer-komputer client, Access Control Server, Access Concentrator, sebagai perangkat keamanan dan manajemen konektivitas data, Vaccine Server, Security Server. Untuk akses jaringan nirkabel sendiri dipastikan menggunakan dua pengamanan yakni proxy depkeu, dan password wifi dan akses hanya diberikan jika melakukan permohonan user akses ke KPTIK GKN Surabaya I. Bentuk pengamanan pengecekan penggunaan akses jaringan tidak resmi masih dalam perencanaan dan belum secara menyeluruh diterapkan di KANWIL DJPBN. Proses pendeteksian dilakukan dengan penelusuran melalui log file aplikasi lain.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Berdasarkan kendala tersebut maka KANWIL DJPBN sebaiknya :
Menentukan risiko infrastruktur termasuk kabel/nirkabel akses jaringan
Menentukan bentuk pengamanan baik secara sistem/ aplikasi dan pengelolaannya
Jika dalam bentuk sistem/aplikasi dan pengelolaan, maka harus dianalisis terlebih dahulu mengenai semua kebutuhan berdasarkan risiko di atas
Menentukan sistem perekrutan tim apakah secara outsourcing atau insourcing (internal)
Merencanakan kebutuhan finansial
Memonitoring jalannya pembuatan aplikasi atau pengelolaannya.

Mensosialisasikan kepada pihak terkait yaitu bagian terkait mengenai aplikasi, manajerial organisasi			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 20.17 CPAR Teknologi 6.17

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Bentuk pengamanan data dan informasi pada SPAN dilengkapi dengan hal-hal berikut, diantaranya : Firewall, Bluecoat Web Filter, Anti SPAM sebagai perangkat pengamanan lalu lintas data internet dan intranet dengan komputer-komputer client, Access Control Server, Access Concentrator, sebagai perangkat keamanan dan manajemen konektivitas data, Vaccine Server, Security Server. Untuk akses jaringan nirkabel sendiri dipastikan menggunakan dua pengamanan yakni proxy depkeu, dan password wifi dan akses hanya diberikan jika melakukan permohonan user akses ke KPTIK GKN Surabaya I. namun belum ada dokumentasi khusus prosedur permohonan akses dari luar instansi. Dan pengamanan ke unit-unit pelayanan juga dilaksanakan sebagaimana umumnya (manual) dengan menggunakan Buku Tamu, Kartu Tamu dan Satpam.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Menentukan pihak eksternal yang terkait baik secara langsung dan tidak langsung dalam proses bisnis di KANWIL DJPBN
Membuat klasifikasi risisko (*risk classification*) berdasarkan dampak akses ke pihak eksternal
Menerapkan bentuk pengamanan baik secara manajemen atau dari sistem / aplikasi dan mendokumentasikannya secara tertulis.
Mengkomunikasikan kebijakan / prosedur kepada pihak internal dan pihak eksternal KANWIL DJPBN
Bentuk monitoring dalam bentuk formulir harus tersedia dan wajib disiapkan misal : formulir peminjaman perangkat TI, dalam bentuk kontrak kerja sama

pengadaan, dll Melakukan monitoring pengamanan secara berkala			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 20.18 CPAR Teknologi 6.18

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Sistem operasi untuk setiap perangkat desktop dan server umumnya dimutakhirkan dengan versi terkini, namun tidak dapat dijadikan acuan karena sistem SPAN sebagai tulang punggung proses bisnis berbasiskan web dengan jalur yang dibangun secara khusus. Di tingkat Kanwil tidak semua sistem operasi dimutakhirkan sesuai kondisi terupdate namun disesuaikan dengan kebutuhan pada KANWIL DJPBN.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Memastikan permintaan update aset informasi terbaru diajukan oleh pihak yang berwenang
Menyusun kelemahan dan kelebihan sistem operasi yang terbaru
Melakukan mapping kondisi sistem versi update dengan kebutuhan organisasi saat ini
Menyusun formulir update sistem operasi terbaru
Melakukan identifikasi terhadap perangkat lunak, informasi, basis data, dan perangkat keras yang perlu diupdate
Menyusun petunjuk pengelolaan konfigurasi untuk masing-masing bagian
Memastikan pihak yang berwenang menerima perubahan yang diminta sebelum dilakukan update
Memastikan bahwa dokumentasi update aset informasi terbaru dan dokumen versi sebelumnya disimpan
Memelihara versi update aset informasi terbaru
Memelihara jejak audit (audit trails) aset informasi terbaru
Memastikan bahwa update aset informasi terbaru dilakukan pada waktu yang

<table>
<tr><td colspan="4">tepat dan tidak mengganggu kegiatan operasional.
Menyusun dokumen perubahan (change document) aset informasi terbaru sebagai hasil evaluasi konfigurasi pasca diupdate
Untuk menuju pada Tingkat Kematangan level III hingga level V maka perlu adanya evaluasi petunjuk atau prosedur yang telah disusun serta proses penerapannya saat ini di KANWIL DJPBN.
Melakukan evaluasi berkala terhadap formulir update sistem yang telah disusun sebagai upaya peningkatan dan pelaporan</td></tr>
<tr><td>Nama
&
TTD</td><td>Diajukan oleh :

(Mustaqim Siga)</td><td>Disetujui oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
<tr><td colspan="4">Section 4 : Tindak lanjut dan verifikasi</td></tr>
<tr><td colspan="4">Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera</td></tr>
<tr><td>Nama
&
TTD</td><td colspan="2">Disposisi oleh :

Kepala Bagian Umum</td><td>Tanggal :</td></tr>
</table>

Form 20.19 CPAR Teknologi 6.19

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Setiap desktop dan server dilindungi dari penyerangan virus (malware)

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Setiap desktop dan server secara menyeluruh dilindungi dari penyerangan virus (malware). Belum adanya dokumentasi mengenai bentuk pengamanan desktop dan server dari malware.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Berdasarkan KMK.479/KMK.01/2010 maka Kanwil DJPBN sebaiknya melakukan :
Pendefinisian risiko malware atau virus yang kemungkinan menyerang
Menentukan tingkat prioritas kehandalan virus atau malware
Mendefinsikan kebutuhan pengamanan berdasarkan klasifikasi risiko virus atau malware
Menerapkan sistem yang dapat melakukan pendeteksian, pencegahan dan pemulihan sebagai bentuk perlindungan terhadap ancaman program yang membahayakan (*malicious code*)
Penyusunan dokumentasi bentuk pengamanan baik secara teknikal atau manajemen
Jika dalam bentuk sistem/aplikasi dan pengelolaan, maka harus dianalisis terlebih dahulu mengenai semua kebutuhan berdasarkan risiko di atas.
Pelaporan rutin mengenai update antivirus
Mendokumentasikan kelemahan serta kendala saat melakukan update atau pemutakhiran antivirus

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 20.20 CPAR Teknologi 6.20

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Ada rekaman dan hasil analisis (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus telah dimutakhirkan secara rutin dan sistematis

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

DI KANWIL DJPBN terdapat rekaman dan hasil analisis (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus telah dimutakhirkan secara rutin dan sistematis karena update antivirus selain menjadi pengamanan informasi juga dilaporkan dalam bentuk pengendalian internal secara berjenjang dan berkala. Kendala utama di sini belum adanya pelaporan tertulis mengenai pemutakhiran antivirus secara berkala di KANWIL DJPBN.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Berdasarkan KMK.479/KMK.01/2010 maka Kanwil DJPBN sebaiknya melakukan :
Pendefinisian risiko malware atau virus yang kemungkinan menyerang
Menentukan tingkat prioritas kehandalan virus atau malware
Mendefinsikan kebutuhan pengamanan berdasarkan klasifikasi risiko virus atau malware
Menerapkan sistem yang dapat melakukan pendeteksian, pencegahan dan pemulihan sebagai bentuk perlindungan terhadap ancaman program yang membahayakan (*malicious code*)
Penyusunan dokumentasi bentuk pengamanan baik secara teknikal atau manajemen
Jika dalam bentuk sistem/aplikasi dan pengelolaan, maka harus dianalisis terlebih dahulu mengenai semua kebutuhan berdasarkan risiko di atas.
Pelaporan rutin mengenai update antivirus
Mendokumentasikan kelemahan serta kendala saat melakukan update atau pemutakhiran antivirus

Pelaporan ditujukan kepada koordinator pelaksana serta pimpinan			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 20.21 CPAR Teknologi 6.21

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Adanya laporan penyerangan virus yang gagal/sukses ditindaklanjuti dan diselesaikan

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN telah menerapkan pelaporan penyerangan virus jika insiden tersebut mengganggu kinerja proses bisnis sebagaimaan kebijakan dalam KMK.479/KMK.01/2010 namun masih dilakukan secara informal dan tidak terdokumentasi jika terdapat kelemahan atau kegagalan antivirus.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Berdasarkan KMK.479/KMK.01/2010 maka Kanwil DJPBN sebaiknya melakukan :
Pendefinisian risiko malware atau virus yang kemungkinan menyerang
Menentukan tingkat prioritas kehandalan virus atau malware
Mendefinsikan kebutuhan pengamanan berdasarkan klasifikasi risiko virus atau malware
Menerapkan sistem yang dapat melakukan pendeteksian, pencegahan dan pemulihan sebagai bentuk perlindungan terhadap ancaman program yang membahayakan (*malicious code*)
Penyusunan dokumentasi bentuk pengamanan baik secara teknikal atau manajemen
Jika dalam bentuk sistem/aplikasi dan pengelolaan, maka harus dianalisis terlebih dahulu mengenai semua kebutuhan berdasarkan risiko di atas.
Pelaporan rutin mengenai update antivirus
Mendokumentasikan kelemahan serta kendala saat melakukan update atau pemutakhiran antivirus
Pelaporan ditujukan kepada koordinator pelaksana serta pimpinan untuk ditindak lanjuti

Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 20.22 CPAR Teknologi 6.22

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Keseluruhan sistem (aplikasi, perangkat komputer dan jaringan) sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Keseluruhan sistem (aplikasi, perangkat komputer dan jaringan) wajib menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada namun belum ada evaluasi akurasi antara aplikasi, sistem dan jaringan. Standarisasi waktu saat ini menggunakan waktu standar pada aplikasi SPAN

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Sesuai KMK.479/KMK.01/2010, KANWIL DJPBN sebaiknya melakukan hal-hal seperti di bawah ini :

Mendefinisikan risiko jika terdapat penyalahgunaan akurasi waktu pada sistem

Menentukan aplikasi dalam menangani sinkronisasi misal dalam bentuk SNTP, NTP yang ditanam pada server

Melakukan konfigurasi waktu secara menyeluruh untuk semua sistem di KANWIL DJPBN

Jika standarisasi waktu yang digunakan adalah standar pada sistem SPAN maka seluruh sistem pada wilayah operasional menggunakan konfigurasi waktu yang sama

Melakukan pengecekan secara berkala, diutamakan dengan rentang / *timestamp* yang pendek misal setiap hari guna mengantisipasi kesalahan konfigurasi

Setiap ada kegiatan maintenance terhadap perangkat / sistem, maka harus dilakukan sinkronisasi ulang waktu setelah kegiatan maintenance

Melakukan monitoring dalam bentuk formulir atau *checklist*

Melakukan pelaporan tertulis yang ditujukan kepada bagian koordinator dan

pimpinan			
Nama & TTD	**Diajukan oleh :** **(Mustaqim Siga)**	**Disetujui oleh :** **Kepala Bagian Umum**	**Tanggal :**
Section 4 : Tindak lanjut dan verifikasi			
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera			
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**		**Tanggal :**

Form 20.23 CPAR Teknologi 6.23

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Setiap aplikasi yang ada memiliki spesifikasi keamanan yang diverifikasi/validasi pada saat pengembangan dan uji-coba

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

Setiap aplikasi yang ada secara menyeluruh memiliki spesifikasi keamanan yang diverifikasi/validasi pada saat pengembangan dan uji-coba sebagaimana diatur dalam KMK.479/KMK.01/2010 Poin VIII, namun KANWIL DJPBN belum mempunyai spesifikasi keamanan dari Kantor Pusat untuk aplikasi yang diverifikasi/divalidasi saat proses testing.

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Berdasarkan KMK.479/KMK.01/2010, maka KANWIL DJPBN sebaiknya :
Mendefinisikan kebutuhan aplikasi apa saja yang dibutuhkan di KANWIL DJPBN
Melakukan pengembangan aplikasi baik secara insourcing atau outsourcing
Menentukan metode pengembangan aplikasi yang akan dikembangkan
Mendefinisikan tingkat sekuritas aplikasi
Menenentukan indikator keamanan pada aplikasi yang akan diuji coba
Menentukan kalkulasi jangka waktu proses deployment aplikasi
Melakukan penyusunan prosedur proses uji coba berdasarkan tingkat sekuritas aplikasi
Menyusun pelaporan hasil verifikasi atau validasi saat uji coba
Mendokumentasikan seluruh pelaksanaan verifikasi / validasi dan menyampaikannya pada pihak terkait

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Form 20.24 CPAR Teknologi 6.24

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

GKN Surabaya I Jl. Indrapura No.5 Surabaya 60175
Telp. (031) 3523093 Fax. (031) 3558640

Section 1 : Obyek

Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 2 : Penyebab / Pendukung

KANWIL DJPBN juga melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin berdasarkan KMK.479/ KMK.01/2010 dan KMK.351/KMK. 01/ 2011 dengan semua metode testing yang ada, namun disebabkan aplikasi yang dikembangkan umumnya adalah terkait aplikasi keuangan Negara maka keterlibatan lebih difokuskan kepada pengguna internal DJPBN / FO dan MO KPPN

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 3 : Usulan tindakan perbaikan

Berdasarkan kendala di atas maka sebaikanya KANWIL DJPBN menerapkan
Penyusunan prosedur keamanan informasi mengenai kerja sama dengan pihak eksternal
Prosedur tersebut berkenaaan dengan pembagian data dan informasi, status aset sistem atau aplikasi di KANWIL DJPBN
Melakukan surat kerja sama dan perjanjian seperti pakta integritas berdasarkan hukum yang berlaku serta asas HAKI.
Untuk meningkatkan Tingkat Kematangan unuk level III hingga selanjutnya maka prosedur kerja sama yang telah disusun hendaknya didokumentasikan, dikomunikasikan pada pimpinan dan disosialisasikan. Selain itu juga mengevaluasi proses penerapan prosedur serta mengidenifikasi apakah terdapat celah atau kelemahan pada

	Diajukan oleh :	Disetujui oleh :	Tanggal :
Nama & TTD	(Mustaqim Siga)	Kepala Bagian Umum	

Section 4 : Tindak lanjut dan verifikasi		
Ditingkatkan, disempurnakan lagi fungsi kebijakan teknis dan dilaksanakan segera		
Nama & TTD	**Disposisi oleh :** **Kepala Bagian Umum**	**Tanggal :**

Lampiran M

Halaman ini sengaja dikosongkan

M.1 Bukti Pendukung

Tabel M.21.1 Bukti Pendukung

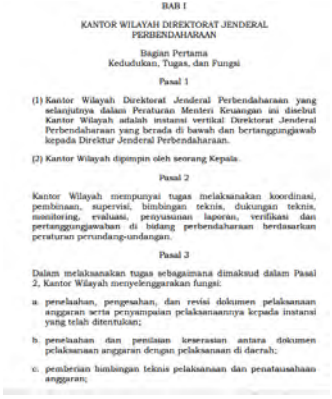
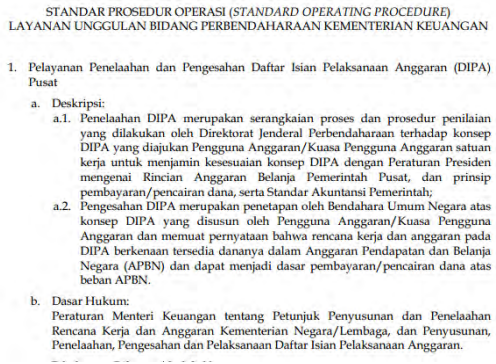
Foto M-1	Foto M-2
Tanggal validasi : 28 April 2014	Tanggal validasi :28 April 2014
 BAB I KANTOR WILAYAH DIREKTORAT JENDERAL PERBENDAHARAAN Bagian Pertama Kedudukan, Tugas, dan Fungsi Pasal 1 (1) Kantor Wilayah Direktorat Jenderal Perbendaharaan yang selanjutnya dalam Peraturan Menteri Keuangan ini disebut Kantor Wilayah adalah instansi vertikal Direktorat Jenderal Perbendaharaan yang berada di bawah dan bertanggungjawab kepada Direktur Jenderal Perbendaharaan. (2) Kantor Wilayah dipimpin oleh seorang Kepala. Pasal 2 Kantor Wilayah mempunyai tugas melaksanakan koordinasi, pembinaan, supervisi, bimbingan teknis, dukungan teknis, monitoring, evaluasi, penyusunan laporan, verifikasi dan pertanggungjawaban di bidang perbendaharaan berdasarkan peraturan perundang-undangan. Pasal 3 Dalam melaksanakan tugas sebagaimana dimaksud dalam Pasal 2, Kantor Wilayah menyelenggarakan fungsi: a. penelaahan, pengesahan, dan revisi dokumen pelaksanaan anggaran serta penyampaian pelaksanaannya kepada instansi yang telah ditentukan; b. penelaahan dan penilaian keserasian antara dokumen pelaksanaan anggaran dengan pelaksanaan di daerah; c. pemberian bimbingan teknis pelaksanaan dan penatausahaan anggaran;	 STANDAR PROSEDUR OPERASI (*STANDARD OPERATING PROCEDURE*) LAYANAN UNGGULAN BIDANG PERBENDAHARAAN KEMENTERIAN KEUANGAN 1. Pelayanan Penelaahan dan Pengesahan Daftar Isian Pelaksanaan Anggaran (DIPA) Pusat a. Deskripsi: a.1. Penelaahan DIPA merupakan serangkaian proses dan prosedur penilaian yang dilakukan oleh Direktorat Jenderal Perbendaharaan terhadap konsep DIPA yang diajukan Pengguna Anggaran/Kuasa Pengguna Anggaran satuan kerja untuk menjamin kesesuaian konsep DIPA dengan Peraturan Presiden mengenai Rincian Anggaran Belanja Pemerintah Pusat, dan prinsip pembayaran/pencairan dana, serta Standar Akuntansi Pemerintah; a.2. Pengesahan DIPA merupakan penetapan oleh Bendahara Umum Negara atas konsep DIPA yang disusun oleh Pengguna Anggaran/Kuasa Pengguna Anggaran dan memuat pernyataan bahwa rencana kerja dan anggaran pada DIPA berkenaan tersedia dananya dalam Anggaran Pendapatan dan Belanja Negara (APBN) dan dapat menjadi dasar pembayaran/pencairan dana atas beban APBN. b. Dasar Hukum: Peraturan Menteri Keuangan tentang Petunjuk Penyusunan dan Penelaahan Rencana Kerja dan Anggaran Kementerian Negara/Lembaga, dan Penyusunan, Penelaahan, Pengesahan dan Pelaksanaan Daftar Isian Pelaksanaan Anggaran.
Screenshot tupoksi KANWIL DJPBN	Dokumen Petunjuk Operasional DJPBN semua unit

Foto M-3	**Foto M-4**
Tanggal validasi : 28 April 2014	Tanggal validasi : 28 April 2014

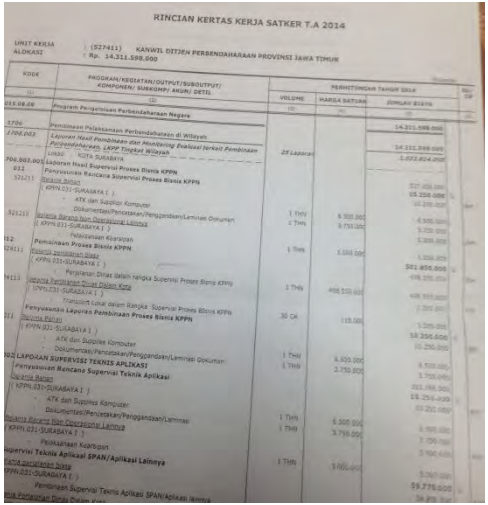
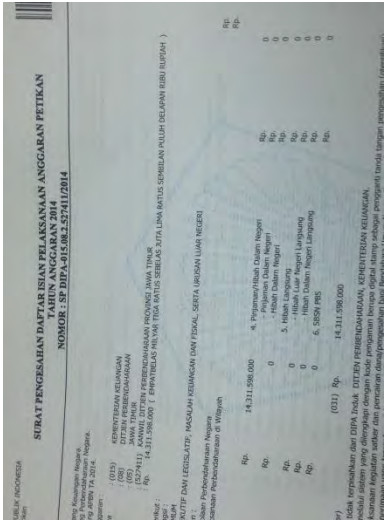

	

Foto Jumlah Anggaran (RKAKL) tahun 2014	Foto Daftar Isian Pelaksanaan Anggaran

RINCIAN KERTAS KERJA SATKER T.A 2014

UNIT KERJA : (527411) KANWIL DITJEN PERBENDAHARAAN PROVINSI JAWA TIMUR
ALOKASI : Rp. 14.311.598.000

SURAT PENGESAHAN DAFTAR ISIAN PELAKSANAAN ANGGARAN PETIKAN
TAHUN ANGGARAN 2014
NOMOR : SP DIPA-015.08.2.527411/2014

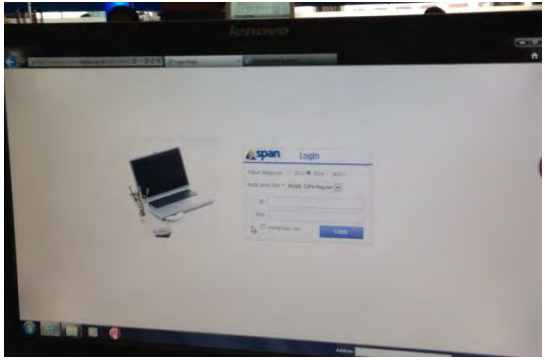
KEMENTERIAN KEUANGAN
DIREKTORAT JENDERAL PERBENDAHARAAN
KANWIL DITJEN PERBENDAHARAAN PROVINSI JAWA TIMUR
Rp. 14.311.598.000 (EMPAT BELAS MILYAR TIGA RATUS SEBELAS JUTA LIMA RATUS SEMBILAN PULUH DELAPAN RIBU RUPIAH)

KUTIP DAN LEGALISIR/ MASALAH KEUANGAN DAN FISKAL SERTA LAHJSAN LUAR NEGERI

Rp. 14.311.598.000
Rp. 0
Rp. 0
Rp. 0
Rp. 0

4. Penjaman/Hibah Dalam Negeri
- Hibah Dalam Negeri
5. Hibah Langsung
- Hibah Luar Negeri Langsung
- Hibah Dalam Negeri Langsung
6. 5859/ PKS

(031) Rp. 14.311.598.000

Foto M-5	Foto M-6
Tanggal validasi : 28 April 2014	Tanggal validasi :28 April 2014
	
Dokumen Juknis Pengelolaan Server, Jaringan & Database	Foto Interface Sistem Perbendaharaan Anggaran Negara Custom Web

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
DIREKTORAT SISTEM PERBENDAHARAAN
GEDUNG PRIJADI PRAPTOSUHARDJO II LANTAI 3-4, JALAN BUDI UTOMO NOMOR 8, JAKARTA, 10710
TELEPON (021) 3864781, 3864776 EXT. 5303, 5304 FAKSIMILE (021) 3864781

Nomor : S-9239/PB.7/2011
Sifat : Segera
Lampiran : 2 (dua) lembar
Hal : Petunjuk Teknis Pengelolaan Server, Sistem Jaringan, dan Database

4 Oktober 2011

Yth. 1. Para Kepala Kantor Wilayah Ditjen Perbendaharaan
2. Para Kepala Kantor Pelayanan Perbendaharaan Negara
Di seluruh Indonesia

Dalam rangka pengelolaan server, sistem jaringan, dan database khususnya da menghadapi pelaksanaan tugas pada akhir tahun anggaran 2011, dengan ini dim perhatian Saudara akan hal-hal sebagai berikut :

1. Pengelolaan server, sistem jaringan, dan database merupakan kegiatan yang p mendapatkan perhatian khusus mengingat fungsi dan kegunaan perangkat tekno informasi tersebut sangat penting dalam menunjang kelancaran pelaksanaan tugas-tu kantor;
2. Mengingat semakin meningkatnya proses transaksi dan volume data khusus menjelang akhir tahun anggaran, sehingga seluruh peralatan teknologi inform dinarapkan dapat berfungsi dengan baik, termasuk tata kelola aplikasi dan data agar da dikelola secara aman dan lancar. Khusus untuk pengamanan database hendak menjadi prioritas disamping pengamanan perangkat teknologi informasi yang lain, sep proses backup data, serta pengiriman data ke Kantor Pusat Ditjen Perbendaharaan ha dilaksanakan sesuai prosedur.

Berkenaan dengan hal-hal tersebut diatas, dan sebagai upaya agar pengelol server, sistem jaringan, dan database pada Kanwil Ditjen Perbendaharaan dan KPPN da

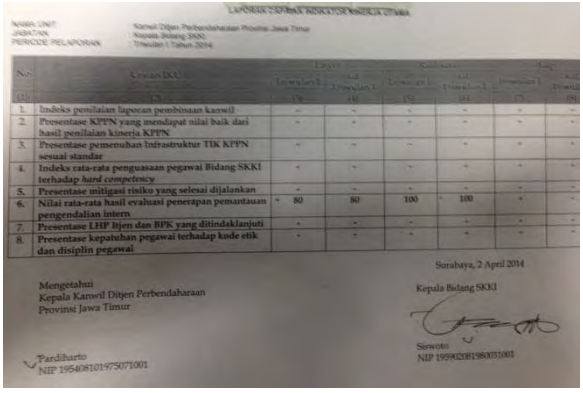
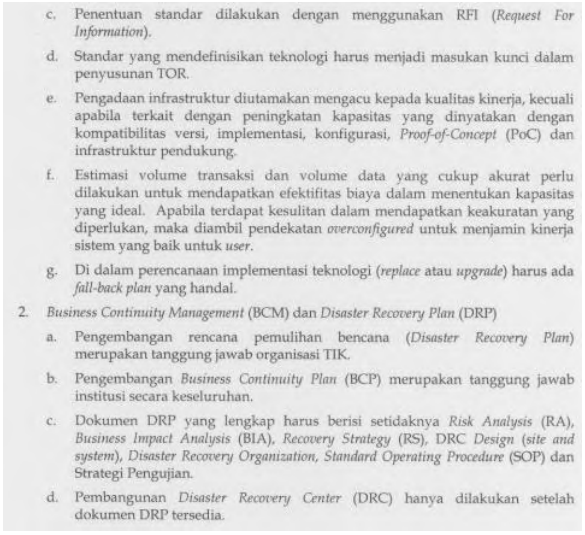
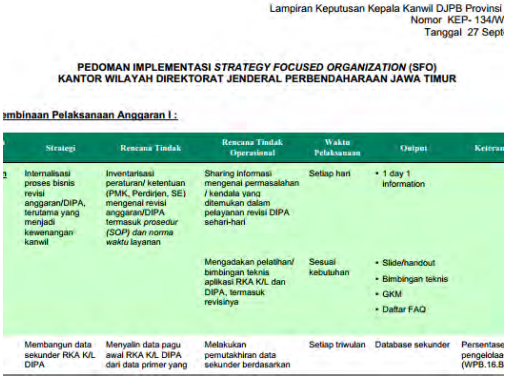
Foto M-7	**Foto M-8**
Tanggal validasi : 28 April 2014  Dokumen Capaian Indikator Kinerja Utama (IKU)	Tanggal validasi : 28 April 2014  KMK No.260/KMK.01/2009 (Kebijakan, DRP, BCM, Pengelolaan risiko)

Foto M-9

Tanggal validasi : 28 April 2014



Lampiran Keputusan Kepala Kanwil DJPB Provinsi
Nomor KEP- 134/W
Tanggal 27 Sept

PEDOMAN IMPLEMENTASI *STRATEGY FOCUSED ORGANIZATION* (SFO)
KANTOR WILAYAH DIREKTORAT JENDERAL PERBENDAHARAAN JAWA TIMUR

ımbinaan Pelaksanaan Anggaran I :

Strategi	Rencana Tindak	Rencana Tindak Operasional	Waktu Pelaksanaan	Output	Keteran
Internalisasi proses bisnis revisi anggaran/DIPA, terutama yang menjadi kewenangan kanwil	Inventarisasi peraturan/ ketentuan (PMK, Perdirjen, SE) mengenai revisi anggaran/DIPA termasuk *prosedur (SOP) dan norma waktu* layanan	Sharing informasi mengenai permasalahan / kendala yang ditemukan dalam pelayanan revisi DIPA sehari-hari	Setiap hari	• 1 day 1 information	
		Mengadakan pelatihan/ bimbingan teknis aplikasi RKA K/L dan DIPA, termasuk revisinya	Sesuai kebutuhan	• Slide/handout • Bimbingan teknis • GKM • Daftar FAQ	
Membangun data sekunder RKA K/L DIPA	Menyalin data pagu awal RKA K/L DIPA dari data primer yang	Melakukan pemutakhiran data sekunder berdasarkan	Setiap triwulan	Database sekunder	Persentase pengelolaa (WPB.16.B

Foto *Strategy Focused Organization* (Strategi, Kebijakan, Supervisi Aplikasi, Pengelolaan risiko)

Foto M-10

Tanggal validasi :28 April 2014

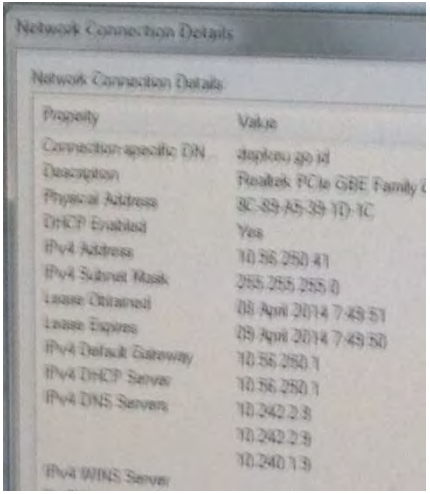


Foto Ipconfig DJPBN untuk semua unit

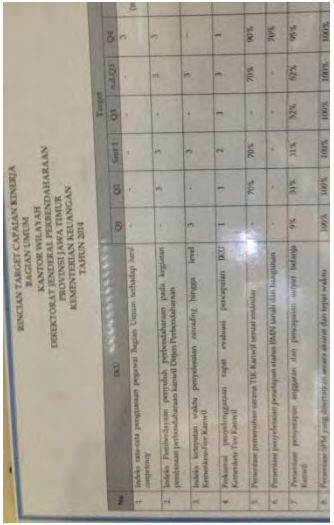
Foto M-11	**Foto M-12**
Tanggal validasi : 28 April 2014	Tanggal validasi : 28 April 2014
	Menetapkan : KEPUTUSAN MENTERI KEUANGAN TENTANG KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN KEMENTERIAN KEUANGAN. PERTAMA : Menetapkan Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di Lingkungan Kementerian Keuangan, yang selanjutnya disebut Kebijakan dan Standar SMKI di Lingkungan Kementerian Keuangan sebagaimana ditetapkan dalam Lampiran yang tidak terpisahkan dari Keputusan Menteri Keuangan ini. KEDUA : Kebijakan dan Standar SMKI di Lingkungan Kementerian Keuangan sebagaimana dimaksud dalam Diktum PERTAMA terdiri dari 11 (sebelas) sasaran pengendalian yaitu: 1. Umum; 2. Organisasi Keamanan Informasi; 3. Pengelolaan Aset Informasi; 4. Keamanan Sumber Daya Manusia; 5. Keamanan Fisik dan Lingkungan; 6. Pengelolaan Komunikasi dan Operasional; 7. Akses; 8. Keamanan Informasi dalam Pengadaan, Pengembangan, dan Pemeliharaan Sistem Informasi; 9. Pengelolaan Gangguan Keamanan Informasi; 10. Keamanan Informasi dalam Pengelolaan Kelangsungan Kegiatan; dan 11. Kepatuhan.
Dokumen Rincian Target Capaian Kinerja per Bidang	Dokumen KMK.479/KMK.01/2010 (11 domain area pengelolaan keamanan informasi)

Foto M-13

Tanggal validasi : 6 April 2014

KEBIJAKAN DAN STANDAR PENGGUNAAN AKUN DAN KATA SANDI, SURAT ELEKTRONIK, DAN INTERNET DI LINGKUNGAN DEPARTEMEN KEUANGAN

MENTERI KEUANGAN,

Menimbang : a. bahwa dalam rangka melindungi aset informasi Departemen Keuangan dari berbagai bentuk ancaman keamanan informasi baik dari dalam maupun luar, berdasar pada prinsip kerahasiaan, keutuhan, dan ketersediaan layanan Teknologi Informasi dan Komunikasi (TIK), dipandang perlu mengatur penggunaan Akun dan Kata Sandi, Surat Elektronik, dan Internet di lingkungan Departemen Keuangan;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Keputusan Menteri Keuangan tentang Kebijakan Dan Standar Penggunaan Akun Dan Kata Sandi, Surat Elektronik, Dan Internet Di Lingkungan Departemen Keuangan;

Mengingat : 1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843);

2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);

3. Peraturan Pemerintah Nomor 30 Tahun 1980 tentang Peraturan Disiplin Pegawai Negeri Sipil (Lembaran Negara Republik Indonesia Tahun 1980 Nomor 50, Tambahan Lembaran Negara

KMK 512/KMK.01/2009 (Akun, Kata Sandi, Email, Internet, Larangan, Sanksi dan Domain)

Foto M-14

Tanggal validasi : 6 April 2014

Foto Gugus Kendali Mutu Kanwil DJPBN

Foto M-15	Foto M-16
Tanggal validasi : 6 April 2014	Tanggal validasi : 28 April 2014

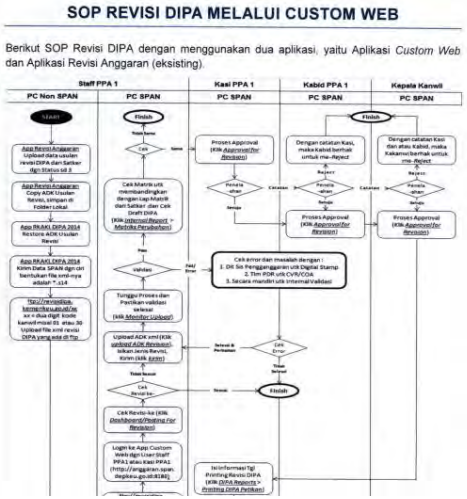
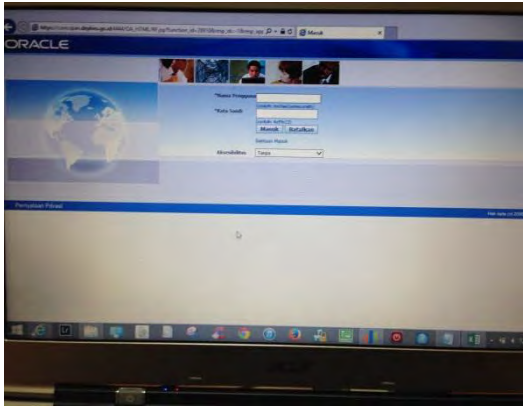
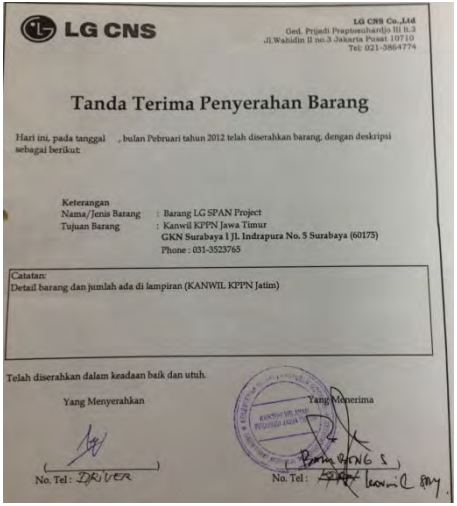
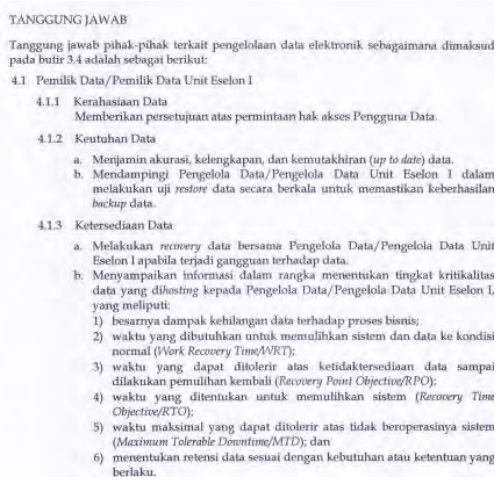

	

Foto prosedur revisi DIPA melalui Custom Web	Foto Aplikasi Sistem Perbendaharaan Anggaran Negara

Foto M-17	Foto M-18
Tanggal validasi : 28 April 2014	Tanggal validasi : 28 April 2014
	
Contoh Daftar Berita Acara Penyerahan Barang	KMK 350/KMK.01/2010 (Kebijakan dan Tanggungjawab CIA Data)

LG CNS

LG CNS Co.,Ltd
Ged. Prijadi Praptosuhardjo III lt.3
Jl.Wahidin II no.3 Jakarta Pusat 10710
Tel: 021-3864774

Tanda Terima Penyerahan Barang

Hari ini, pada tanggal , bulan Pebruari tahun 2012 telah diserahkan barang, dengan deskripsi sebagai berikut:

Keterangan
Nama/Jenis Barang : Barang LG SPAN Project
Tujuan Barang : Kanwil KPPN Jawa Timur
GKN Surabaya I Jl. Indrapura No. 5 Surabaya (60175)
Phone : 031-3523765

Catatan:
Detail barang dan jumlah ada di lampiran (KANWIL KPPN Jatim)

Telah diserahkan dalam keadaan baik dan utuh.

Yang Menyerahkan

( )
No. Tel : DRIVER

Yang Menerima

( )
No. Tel :

TANGGUNG JAWAB

Tanggung jawab pihak-pihak terkait pengelolaan data elektronik sebagaimana dimaksud pada butir 3.4 adalah sebagai berikut:

4.1 Pemilik Data/Pemilik Data Unit Eselon I

4.1.1 Kerahasiaan Data
Memberikan persetujuan atas permintaan hak akses Pengguna Data.

4.1.2 Keutuhan Data

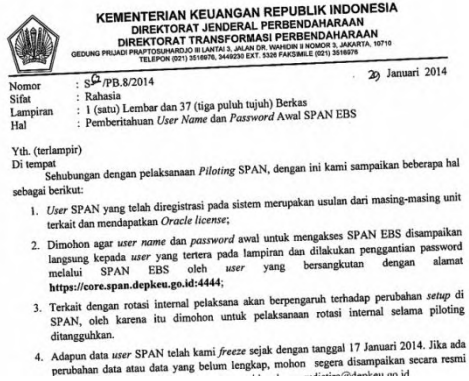
a. Menjamin akurasi, kelengkapan, dan kemutakhiran (*up to date*) data.
b. Mendampingi Pengelola Data/Pengelola Data Unit Eselon I dalam melakukan uji *restore* data secara berkala untuk memastikan keberhasilan *backup* data.

4.1.3 Ketersediaan Data

a. Melakukan *recovery* data bersama Pengelola Data/Pengelola Data Unit Eselon I apabila terjadi gangguan terhadap data.
b. Menyampaikan informasi dalam rangka menentukan tingkat kritikalitas data yang *dihosting* kepada Pengelola Data/Pengelola Data Unit Eselon I, yang meliputi:
   1) besarnya dampak kehilangan data terhadap proses bisnis;
   2) waktu yang dibutuhkan untuk memulihkan sistem dan data ke kondisi normal (*Work Recovery Time/WRT*);
   3) waktu yang dapat ditolerir atas ketidaktersediaan data sampai dilakukan pemulihan kembali (*Recovery Point Objective/RPO*);
   4) waktu yang ditentukan untuk memulihkan sistem (*Recovery Time Objective/RTO*);
   5) waktu maksimal yang dapat ditolerir atas tidak beroperasinya sistem (*Maximum Tolerable Downtime/MTD*); dan
   6) menentukan retensi data sesuai dengan kebutuhan atau ketentuan yang berlaku.

Foto M-19

Tanggal validasi : 28 April 2014



KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
DIREKTORAT TRANSFORMASI PERBENDAHARAAN
GEDUNG PRIJADI PRAPTOSUHARDJO III LANTAI 3, JALAN DR. WAHIDIN II NOMOR 3, JAKARTA, 10710
TELEPON (021) 3518976, 3449230 EXT. 5326 FAKSIMILE (021) 3518976

Nomor : S-/PB.8/2014 20 Januari 2014
Sifat : Rahasia
Lampiran : 1 (satu) Lembar dan 37 (tiga puluh tujuh) Berkas
Hal : Pemberitahuan *User Name* dan *Password* Awal SPAN EBS

Yth. (terlampir)
Di tempat

Sehubungan dengan pelaksanaan *Piloting* SPAN, dengan ini kami sampaikan beberapa hal sebagai berikut:

1. *User* SPAN yang telah diregistrasi pada sistem merupakan usulan dari masing-masing unit terkait dan mendapatkan *Oracle license*;
2. Dimohon agar *user name* dan *password* awal untuk mengakses SPAN EBS disampaikan langsung kepada *user* yang tertera pada lampiran dan dilakukan penggantian password melalui SPAN EBS oleh *user* yang bersangkutan dengan alamat **https://core.span.depkeu.go.id:4444**;
3. Terkait dengan rotasi internal pelaksana akan berpengaruh terhadap perubahan *setup* di SPAN, oleh karena itu dimohon untuk pelaksanaan rotasi internal selama piloting ditangguhkan.
4. Adapun data *user* SPAN telah kami *freeze* sejak dengan tanggal 17 Januari 2014. Jika ada perubahan data atau data yang belum lengkap, mohon segera disampaikan secara resmi

Akses User dan Password SPAN awal
(Nama, Email, Login, Password)

Foto M-20

Tanggal validasi : 28 April 2014

2. User Aplikasi Custom Web

User minimal yang sudah disediakan oleh DJA sebayak delapan user, yaitu :

a. Kepala Kanwil - KWL(kodekanwil)
b. Kepala Bidang PPA I - KWL(kodekanwil)PP1
c. Kepala Seksi PPA I A -KWL(kodekanwil)PP1_41
d. Staff 1 Seksi PPA I A - KWL(kodekanwil)PP1_41staf1
e. Staff 2 Seksi PPA I A - KWL(kodekanwil)PP1_41staf2
f. Kepala Seksi PPA I B - KWL(kodekanwil)PP1_42
g. Staff 1 Seksi PPA I B - KWL(kodekanwil)PP1_42staf1
h. Staff 2 Seksi PPA I B - KWL(kodekanwil)PP1_42staf2

User dapat ditambah sesuai dengan Jumlah Seksi pada Bidang PPA I. Penambahan user dapat disampaikan melalui email ke DJA

3. Alamat Aplikasi Custom Web

Aplikasi *Custom Web* dapat diakses melalui jaringan SPAN di alamat http://anggaran.span.depkeu.go.id:8180

4. Aplikasi Pendukung Custom Web

a. Aplikasi Revisi Revisi Anggaran
b. Aplikasi RKAKL DIPA TA 2014
c. FTP Upload dan Download Data SPAN (ftp://revisidipa.kemenkeu.go.id/xx(xx = dua digit kode kanwil)), dan login menggunakan akses yang sama ketika login ke alamat ftp://www.anggaran.depkeu.go.id

Tingkat Kewenangan Akses User SPAN Custom Web level Kanwil DJPBN

Foto M-21

Tanggal validasi : 28 April 2014

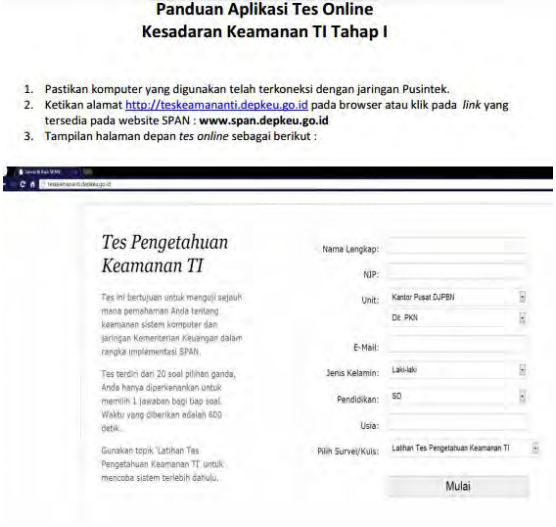
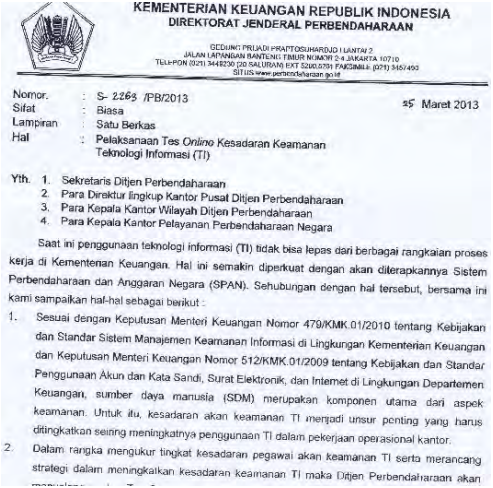


Foto Form Tes Kesadaran Keamanan IT

Foto M-22

Tanggal validasi : 28 April 2014


KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN

GEDUNG PRIJADI PRAPTOSUHARDJO I LANTAI 2
JALAN LAPANGAN BANTENG TIMUR NOMOR 2-4 JAKARTA 10710
TELEPON (021) 3448230 (20 SALURAN) EXT 5200,5701 FAKSIMILI: (021) 3457493
SITUS www.perbendaharaan.go.id

Nomor. : S- 2263 /PB/2013
Sifat : Biasa
Lampiran : Satu Berkas
Hal : Pelaksanaan Tes *Online* Kesadaran Keamanan Teknologi Informasi (TI)

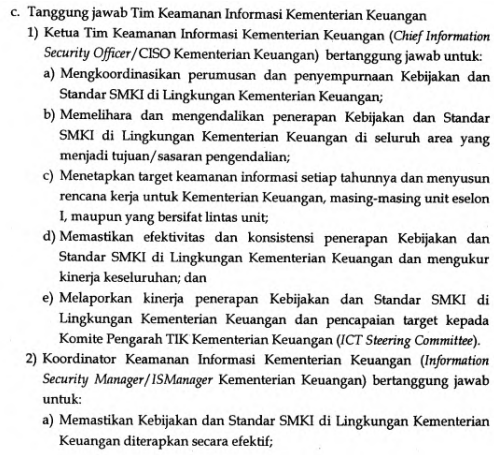
25 Maret 2013

Yth. 1. Sekretaris Ditjen Perbendaharaan
2. Para Direktur lingkup Kantor Pusat Ditjen Perbendaharaan
3. Para Kepala Kantor Wilayah Ditjen Perbendaharaan
4. Para Kepala Kantor Pelayanan Perbendaharaan Negara

Saat ini penggunaan teknologi informasi (TI) tidak bisa lepas dari berbagai rangkaian proses kerja di Kementerian Keuangan. Hal ini semakin diperkuat dengan akan diterapkannya Sistem Perbendaharaan dan Anggaran Negara (SPAN). Sehubungan dengan hal tersebut, bersama ini kami sampaikan hal-hal sebagai berikut :

1. Sesuai dengan Keputusan Menteri Keuangan Nomor 479/KMK.01/2010 tentang Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di Lingkungan Kementerian Keuangan dan Keputusan Menteri Keuangan Nomor 512/KMK.01/2009 tentang Kebijakan dan Standar Penggunaan Akun dan Kata Sandi, Surat Elektronik, dan Internet di Lingkungan Departemen Keuangan, sumber daya manusia (SDM) merupakan komponen utama dari aspek keamanan. Untuk itu, kesadaran akan keamanan TI menjadi unsur penting yang harus ditingkatkan seiring meningkatnya penggunaan TI dalam pekerjaan operasional kantor.
2. Dalam rangka mengukur tingkat kesadaran pegawai akan keamanan TI serta merancang strategi dalam meningkatkan kesadaran keamanan TI maka Ditjen Perbendaharaan akan

Pelaksanaan Tes Online Kesadaran Keamanan TI

Foto M-23	**Foto M-24**
Tanggal validasi : 28 April 2014	Tanggal validasi : 28 April 2014
	
Modul Prosedur Panduan Keamanan TI DJPBN	Tanggung jawab CISO dan Tim Keamanan Informasi dalam KMK 479/KMK.01/2010

c. Tanggung jawab Tim Keamanan Informasi Kementerian Keuangan

1) Ketua Tim Keamanan Informasi Kementerian Keuangan (*Chief Information Security Officer*/CISO Kementerian Keuangan) bertanggung jawab untuk:
   a) Mengkoordinasikan perumusan dan penyempurnaan Kebijakan dan Standar SMKI di Lingkungan Kementerian Keuangan;
   b) Memelihara dan mengendalikan penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Keuangan di seluruh area yang menjadi tujuan/sasaran pengendalian;
   c) Menetapkan target keamanan informasi setiap tahunnya dan menyusun rencana kerja untuk Kementerian Keuangan, masing-masing unit eselon I, maupun yang bersifat lintas unit;
   d) Memastikan efektivitas dan konsistensi penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Keuangan dan mengukur kinerja keseluruhan; dan
   e) Melaporkan kinerja penerapan Kebijakan dan Standar SMKI di Lingkungan Kementerian Keuangan dan pencapaian target kepada Komite Pengarah TIK Kementerian Keuangan (*ICT Steering Committee*).
2) Koordinator Keamanan Informasi Kementerian Keuangan (*Information Security Manager*/*ISManager* Kementerian Keuangan) bertanggung jawab untuk:
   a) Memastikan Kebijakan dan Standar SMKI di Lingkungan Kementerian Keuangan diterapkan secara efektif;

Foto M-25

Tanggal validasi : 6 April 2014

DAFTAR BARANG RUANGAN

NAMA UPB : KANWIL DITJEN PBN PROVINSI JAWA TIMUR
KODE UPB : 019.08.15.527411.000.KD

NAMA RUANGAN : RUANG SERVER PPA-I
KODE RUANGAN : 2.1.3

No.	No Urut Pendaft	Nama Barang	Identitas Barang			Jumlah Barang	Penguasaan	Keterangan
			Merk/Type	Kd Barang	Thn Perl			
1	2	3	4	5	6	7	8	9
21	3	Server	SERIES 226-KBON 3 GHz HP ML370 T03 Server SAS CTO	3.10.02.04.001	2009	1 Buah	Milik Sendiri	Monitor LCD HP
22	4	Server	HP PROLIANT ML180 G6	3.10.02.04.001	2009	1 Buah	Milik Sendiri	MEMORY
23	1	Router	Cisco 1760-V	3.10.02.04.002	2008	1 Buah	Milik Sendiri	
24	1	Raid Server		3.10.02.04.014	2011	1 Buah	Milik Sendiri	

Tidak diperkenankan memindahkan barang-barang yang ada pada daftar ini tanpa sepengetahuan penanggung jawab Unit Akuntansi Kuasa Pengguna Barang (UAKPB) dan penanggung jawab ruangan ini

Foto Daftar Inventaris Ruang Data Center

Foto M-26

Tanggal validasi : 6 April 2014

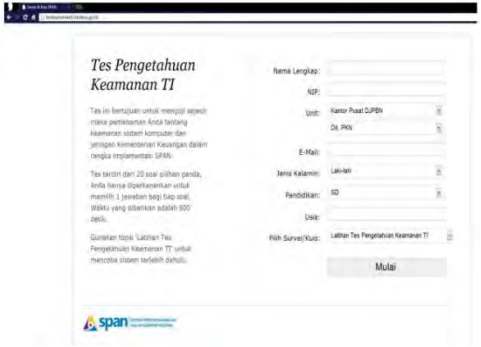


Foto tes online website

Foto M-27	**Foto M-28**
Tanggal validasi : 6 April 2014	Tanggal validasi : 17 April 2014

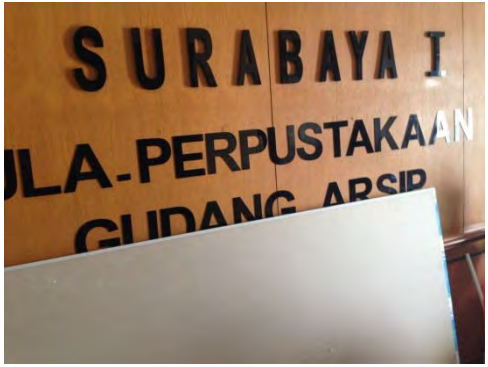



Foto ruang penyimpanan arsip	Foto server data center lama

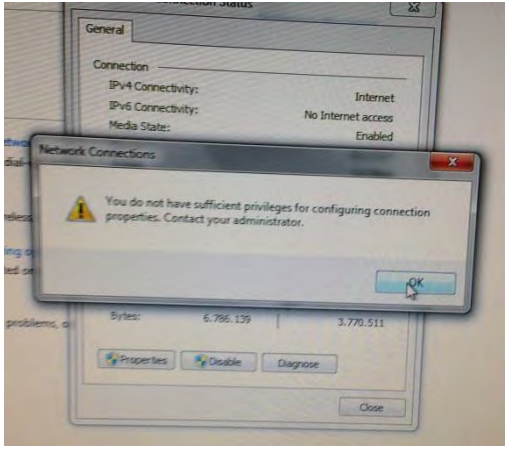
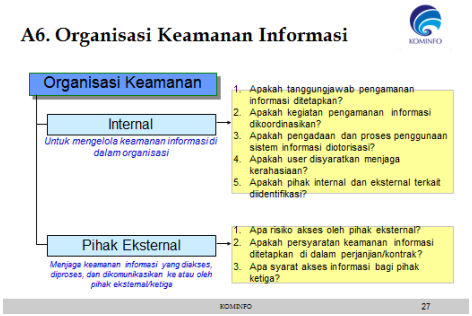
Foto M-29	Foto M-30
Tanggal validasi : 28 April 2014	Tanggal validasi : 28 April 2014
	
Screenshot banned IPCONFIG untuk SPAN	Foto antivirus Kaspersky FO

Foto M-31	Foto M-32
Tanggal validasi : 28 April 2014	Tanggal validasi : 28 April 2014
	
Foto antivirus seluruh Bidang	Foto Sertifikat Bimbingan Teknis

Foto M-33

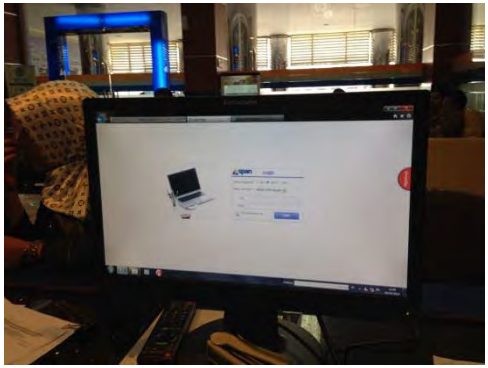
Tanggal validasi : 12 Mei 2014



Slide Penetapan Organisasi Keamanan Informasi Kominfo

Foto M-34

Tanggal validasi : 12 Mei 2014



Pelayanan Revisi DIPA Satker dengan SPAN

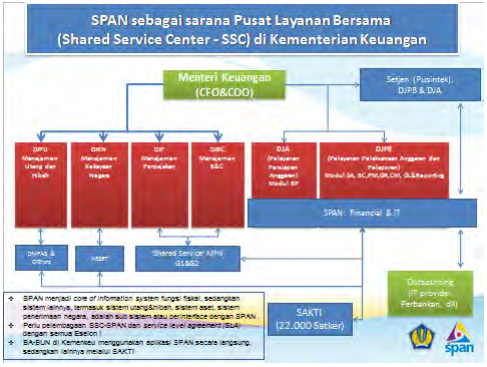
Foto M-35	Foto M-36
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Screenshot Fungsionalitas SPAN dalam Keuangan Negara	Skala Transformasi SPAN dengan lingkup pada seluruh Satker secara Nasional

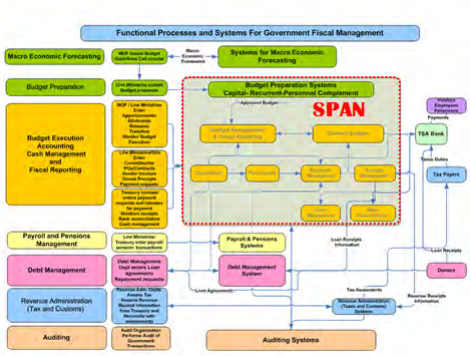
Foto M-37	Foto M-38
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Kompleksitas SPAN dalam Keuangan Negara	HImpunan RKAKL-DIPA dengan lingkup pada seluruh Kementerian secara Nasional

Foto M-39	**Foto M-40**
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Referensi Perundang-Undangan SPAN dalam Keuangan Negara	PMK tentang Pelaksanaan Piloting SPAN

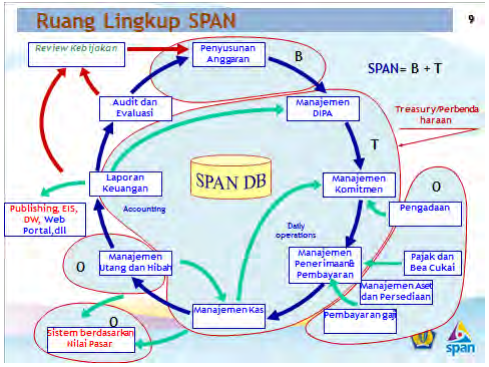
Foto M-41	Foto M-42
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Suasana Layanan Kanwil DJPBN Jawa Timur	Ruang Lingkup Pelaksanaan Piloting SPAN

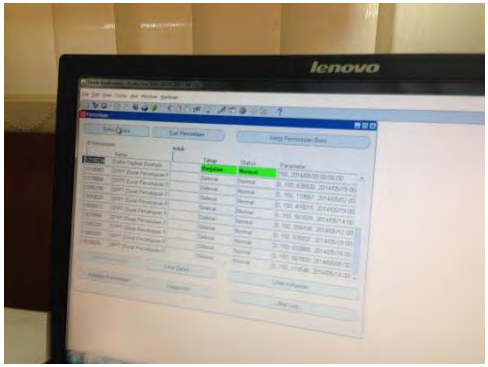
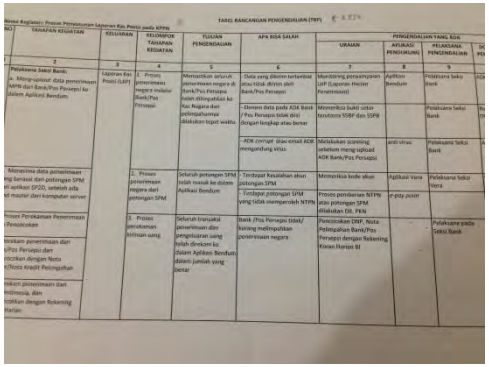
Foto M-43	Foto M-44
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Pemrosesan SPAN dilengkapi dengan rentang waktu fungsionalitas sistem	Tingkatan Hak Akses SPAN

Foto M-45	Foto M-46
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Daftar Uji Pengendalian Utama	Tabel Rancangan Pengendalian (TRP)

DAFTAR UJI PENGENDALIAN UTAMA

Nama Kegiatan : Penerbitan atau Pencairan Dana SP2D Non Belanja Pegawai
Pengendalian Utama : Instalasi antivirus yang ter-update di komputer FO
Disusun Oleh : Widiastuti
Bulan : April 2013

No (1)	Nomor Komputer FO (2)	Pertanyaan 1 (3)	Keterangan (4)
01	2.12.01.82.001.77	V	V
02	2.12.01.82.001.78	V	V
03	2.12.01.82.001.79	V	V
04	2.12.01.82.001.80	V	V
05	2.12.01.82.001.81	V	V
06	2.12.01.82.001.82	V	V

Jumlah komputer yang ada di FO = 8 komputer

Pelaksana Pemantauan KPPN Surabaya I

Widiastuti

Foto M-47	**Foto M-48**
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Laporan Triwulan III Pemantauan Pengendalian Utama	Ruang Generating Set GKN

LAPORAN AKHIR TRIWULAN III
PEMANTAUAN PENGENDALIAN UTAMA UNIT KERJA
KANTOR WILAYAH DIREKTORAT JENDERAL PERBENDAHARAAN PROVINSI JAWA TIMUR
Periode Januari - September 2013

NO	Pengendalian Utama *)	Populasi	Sampel	Jumlah Kepatuhan	Tingkat Kepatuhan	Jumlah Temuan	Jumlah Rekomendasi	Jumlah Tindak Lanjut Belum Tuntas
1	2	3	4	5	6	7	8	9
1	Penelitian berjenjang dari Kepala Seksi dan Kepala Bidang PA	634	100%	634	100%	nihil	nihil	nihil
2	Instalasi antivirus yang *ter-update* di komputer FO	14	100%	14	100%			
	Rata rata tingkat kepatuhan kegiata				100%			
Total								

Surabaya, 9 Oktober 2013

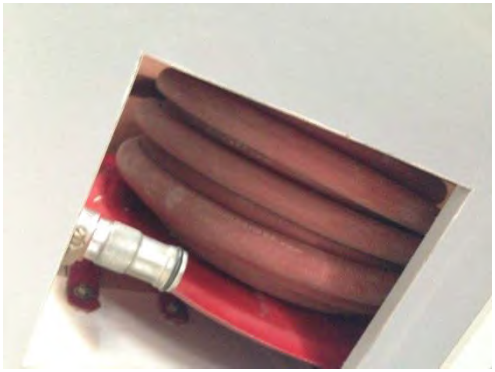
Foto M-49	Foto M-50
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Fire Extinguisher	Selang Hydrant

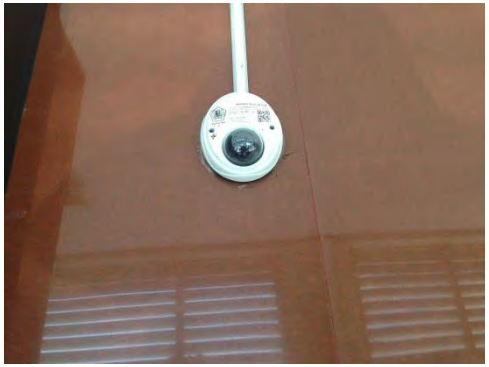
Foto M-51	**Foto M-52**
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Akses Sidik Jari Pegawai dan Akses PIN Tamu	Face Recognition

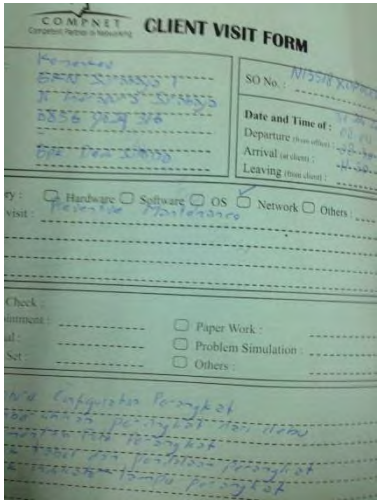
Foto M-53	Foto M-54
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Network Configuration / Preventive Maintenance	Kunci Akses Server Depan

Foto M-55	Foto M-56
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Akses Server Belakang	Maintenace Perangkat

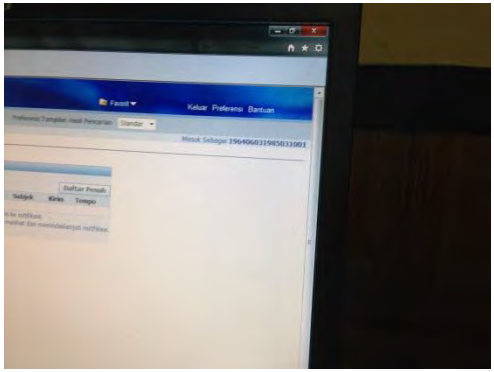
Foto M-57	Foto M-58
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Log Akses SPAN	Log Akses SPAN Nama

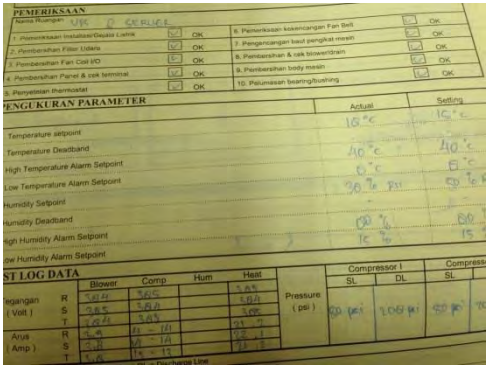
Foto M-59	**Foto M-60**
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Pengecekan Kondisi dan Lingkungan Perangkat	Indikator Suhu

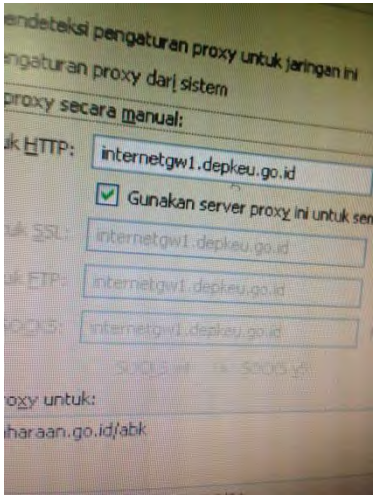
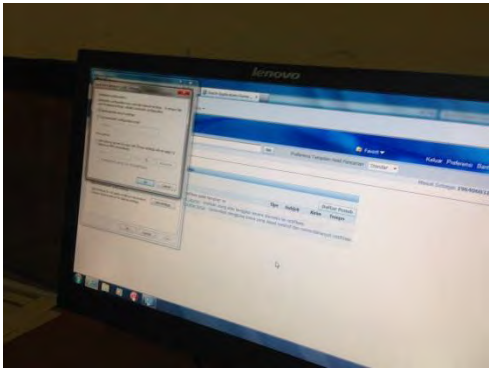
Foto M-61	Foto M-62
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Proxy Intra DJPBN	Proxy Jalur SPAN

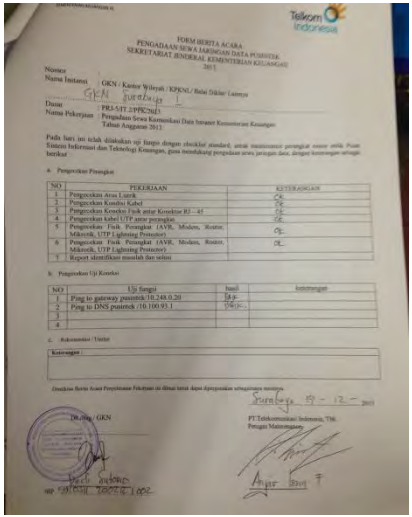
Foto M-63	**Foto M-64**
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Sewa Jaringan Internet	Ping gateway Pusintek

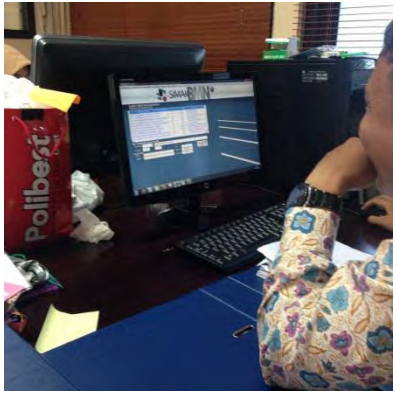
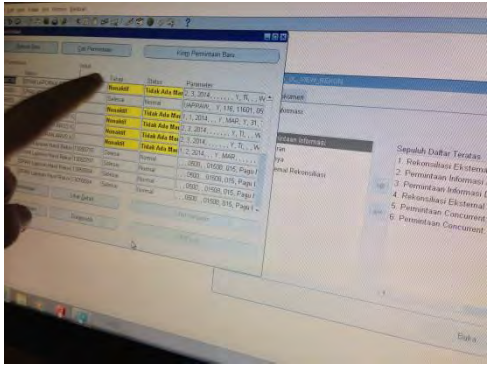
Foto M-65	Foto M-66
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
SIMAK BMN	Proses Sistem Aplikasi SPAN

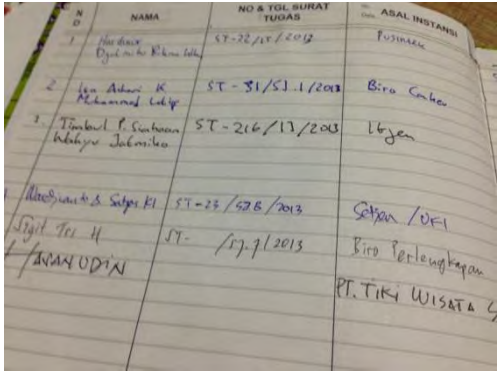
Foto M-67	**Foto M-68**
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Kartu Tamu / Visitor	Buku Tamu

Foto M-69	Foto M-70
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
Yang bertanda tangan dibawah ini : Nama : ROSIDI Jabatan : Petugas Satpam GKN Surabaya I Alamat : Jl. Petukangan no.48 Surabaya Dengan ini menyatakan dengan sebenarnya bahwa, dengan diterimanya kami sebagai Tenaga Satpam Kantor Pengelolaan TIK dan BMN Surabaya pada Gedung Keuangan Negara Surabaya I, kami sanggup memenuhi ketentuan yang berlaku sesuai Surat Perjanjian dan Persetujuan Kerja Nomor : SPPK- /TIKBMN.03/2013 tanggal 2 Januari 2014 dan **kami tidak akan menuntut untuk dapat diangkat menjadi Pegawai Negeri Sipil pada Departemen Keuangan RI.** Demikian surat pernyataan ini kami buat dengan sebenarnya untuk dapat dipergunakan seperlunya. Surabaya, 2 Januari 2014 Yang membuat pernyataan ROSIDI	
SK Satuan Pengamanan (SATPAM)	Satuan Pengamanan (SATPAM)

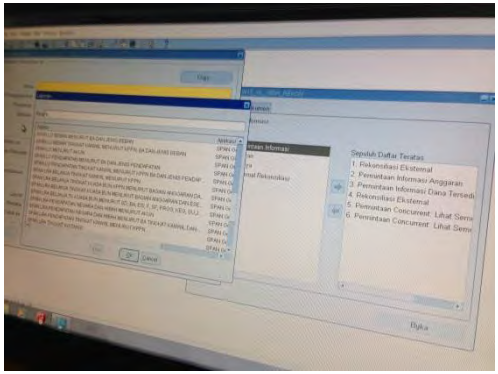
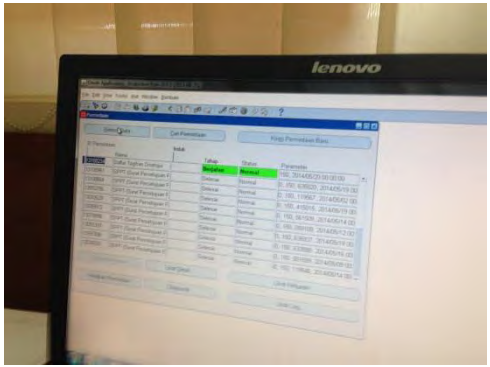
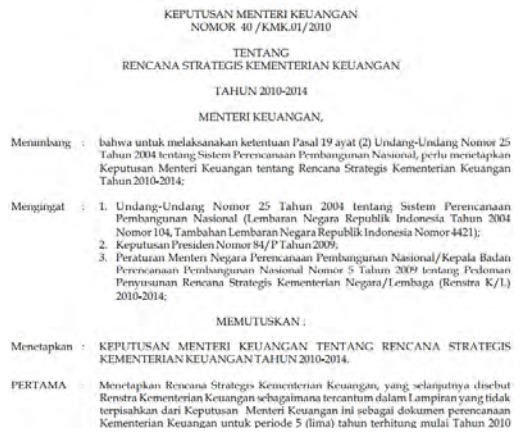
Foto M-71	Foto M-72
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Aplkasi SPAN (Proses Kerja Rekonsiliasi Wilayah) Kanwil DJPBN	Cek Waktu Untuk Proses Kerja Aplikasi SPAN

Foto M-73

Tanggal validasi : 12 Mei 2014



KEPUTUSAN MENTERI KEUANGAN
NOMOR 40 /KMK.01/ 2010

TENTANG
RENCANA STRATEGIS KEMENTERIAN KEUANGAN

TAHUN 2010-2014

MENTERI KEUANGAN,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 19 ayat (2) Undang-Undang Nomor 25 Tahun 2004 tentang Sistem Perencanaan Pembangunan Nasional, perlu menetapkan Keputusan Menteri Keuangan tentang Rencana Strategis Kementerian Keuangan Tahun 2010-2014;

Mengingat : 1. Undang-Undang Nomor 25 Tahun 2004 tentang Sistem Perencanaan Pembangunan Nasional (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 104, Tambahan Lembaran Negara Republik Indonesia Nomor 4421);
2. Keputusan Presiden Nomor 84/P Tahun 2009;
3. Peraturan Menteri Negara Perencanaan Pembangunan Nasional/Kepala Badan Perencanaan Pembangunan Nasional Nomor 5 Tahun 2009 tentang Pedoman Penyusunan Rencana Strategis Kementerian Negara/Lembaga (Renstra K/L) 2010-2014;

MEMUTUSKAN :

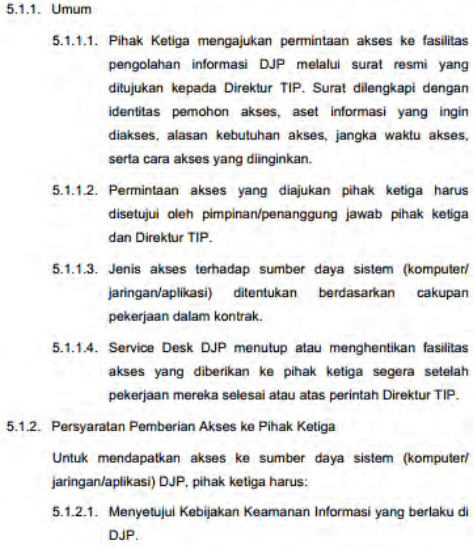
Menetapkan : KEPUTUSAN MENTERI KEUANGAN TENTANG RENCANA STRATEGIS KEMENTERIAN KEUANGAN TAHUN 2010-2014.

PERTAMA : Menetapkan Rencana Strategis Kementerian Keuangan, yang selanjutnya disebut Renstra Kementerian Keuangan sebagaimana tercantum dalam Lampiran yang tidak terpisahkan dari Keputusan Menteri Keuangan ini sebagai dokumen perencanaan Kementerian Keuangan untuk periode 5 (lima) tahun terhitung mulai Tahun 2010

KMK. 40/ KMK.01/2010 Rencana Strategis Kementerian Keuangan

Foto M-74

Tanggal validasi : 12 Mei 2014



5.1.1. Umum

5.1.1.1. Pihak Ketiga mengajukan permintaan akses ke fasilitas pengolahan informasi DJP melalui surat resmi yang ditujukan kepada Direktur TIP. Surat dilengkapi dengan identitas pemohon akses, aset informasi yang ingin diakses, alasan kebutuhan akses, jangka waktu akses, serta cara akses yang diinginkan.

5.1.1.2. Permintaan akses yang diajukan pihak ketiga harus disetujui oleh pimpinan/penanggung jawab pihak ketiga dan Direktur TIP.

5.1.1.3. Jenis akses terhadap sumber daya sistem (komputer/ jaringan/aplikasi) ditentukan berdasarkan cakupan pekerjaan dalam kontrak.

5.1.1.4. Service Desk DJP menutup atau menghentikan fasilitas akses yang diberikan ke pihak ketiga segera setelah pekerjaan mereka selesai atau atas perintah Direktur TIP.

5.1.2. Persyaratan Pemberian Akses ke Pihak Ketiga

Untuk mendapatkan akses ke sumber daya sistem (komputer/ jaringan/aplikasi) DJP, pihak ketiga harus:

5.1.2.1. Menyetujui Kebijakan Keamanan Informasi yang berlaku di DJP.

Pedoman Akses Pihak Ketiga

Foto M-75

Tanggal validasi : 12 Mei 2014

T JENDERAL PERBENDAHARAAN KEMENTERIAN KEUANGAN
JEN PERBENDAHARAAN PROVINSI JAWA TIMUR
3AYA I

SECOND RISK ASSESSMENT / PENILAIAN RISIKO I
Untuk Time Horizon I

Formulir 2.0 Risk Register A - Proses Identifikasi Risiko

	:	KPPN SURABAYA I
gkup Proses	:	KPPN SURABAYA I
aktu Proses	:	1 Januari s.d. 30 Juni 2014 (1 Time Horizon)
oses	:	Identifikasi Risiko
ngjawab Proses	:	KEPALA KPPN SURABAYA I
	:	22-Jan-14

kasi Risiko

n UPR	Kategori risiko	Risiko			
		Apa yang mungkin terjadi	Penyebab terjadinya	Kapan terjadinya	
n Belanja Optimal ional	Operasional	1. Penyerapan belanja DIPA satker tidak sesuai target 2. Pola penarikan dana dalam DIPA tidak tepat	1. Kurangnya pemahaman K/L terhadap Undang-undang 2. Sosialisasi manajemen	Sepanjang tahun	Pe Ne m te da ek

Identifikasi Risiko DJPBN Jawa Timur

Foto M-76

Tanggal validasi : 12 Mei 2014

ANWIL DITJEN PERBENDAHARAAN PROVINSI JAWA TIMUR
PPN SURABAYA I

SECOND RISK ASSESSMENT / PENILAIAN RISIKO I
Untuk Time Horizon I

Formulir 3.0 Risk Register B - Proses Analisis Risiko

1	Unit Kerja	:	KPPN SURABAYA I
2	Ruang Lingkup Proses	:	KPPN SURABAYA I
3	Jangka Waktu Proses	:	1 Januari s.d. 30 Juni 2014 (1 Time Horizon)
4	Tujuan Proses	:	Analisis Risiko
5	Penanggungjawab Proses	:	Kepala KPPN Surabaya I
6	Tanggal	:	22 Januari 2014

abel Analisis dan Profil Risiko

o	Kategori risiko	Sasaran UPR	Risiko			Deskripsi konsekuensi risiko	Sistem Pengendalian yang ada	Tingkat Konsekuensi risiko
			Apa yang mungkin terjadi	Penyebab terjadinya	Kapan terjadinya			
	Operasional	SS.KPPN.1: Pelaksanaan Belanja Negara yang Optimal dan Proporsional	1. Penyerapan belanja DIPA Satker tidak sesuai target 2. Pola Penarikan dana dalam DIPA tidak tepat	1. Kurangnya pemahaman K/L terhadap Undang-undang 2. Sosialisasi manajemen keuangan kurang 3. Dokumen	Sepanjang Tahun	Penyerapan Belanja Negara tidak optimal yang mengakibatkan terganggunya pertunbuhan ekonomi	Laporan Bulanan	rendah

Analisis Risiko DJPBN Jawa Timur

Foto M-77

Tanggal validasi : 12 Mei 2014

Infrastruktur pada Data Center (DC) dan Disaster Recovery Center SPAN

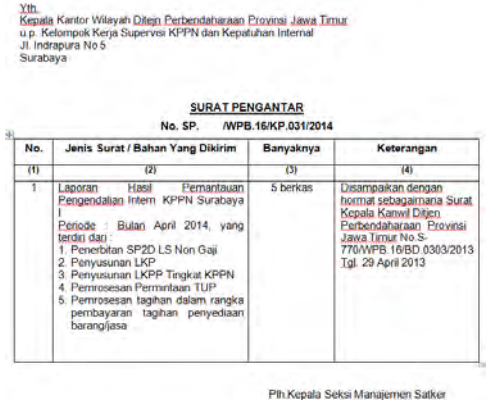
Data Center (DC) SPAN berfungsi sebagai pemroses dan penyimpan data utama dalam sistem. Jika server utama *down* karena bencana atau hal-hal yang tidak diinginkan, pemrosesan dan penyimpanan informasi dialihkan ke *Disaster Recovery Center (DRC)*. Berikut beberapa komponen pada DC dan DRC SPAN:

- *Server*
  Server sebagai "komputer induk" dari sistem SPAN secara umum dibagi 3 sesuai fungsinya, meliputi:
  - Server Utama/Production merupakan server utama dalam implementasi SPAN, salah satunya yaitu server aplikasi EBS dan server hyperion.
  - Server pada DMZ (*Demilitarized Zone*) yaitu server yang sengaja disediakan agar dapat diakses oleh pihak di luar SPAN, seperti server interface untuk interkoneksi perbankan dan SAKTI.
  - Server Development, yaitu server yang berfungsi sebagai tempat pengujian, seperti server test aplikasi EBS Module, dan Server Test Oracle Database.
- Perangkat *Security*
  Pengamanan data dan informasi pada DC dan DRC SPAN dilengkapi dengan hal-hal berikut, diantaranya:
  - Firewall, Bluecoat Web Filter, Anti SPAM sebagai perangkat pengamanan lalu lintas data internet dan intranet dengan komputer-komputer *client*.
  - Access Control Server, Access Concentrator, sebagai perangkat keamanan dan manajemen konektivitas data,
  - Vaccine Server,
  - Security Server.

Infrastruktur Data Centre dan DRC SPAN

Foto M-78

Tanggal validasi : 12 Mei 2014



Yth.
Kepala Kantor Wilayah Ditjen Perbendaharaan Provinsi Jawa Timur
u.p. Kelompok Kerja Supervisi KPPN dan Kepatuhan Internal
Jl. Indrapura No 5
Surabaya

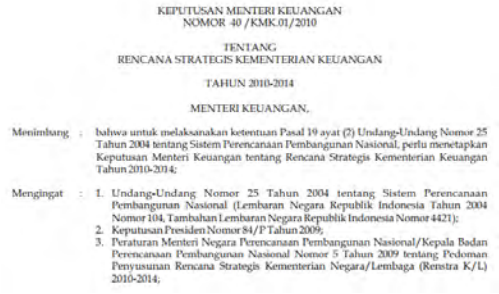
SURAT PENGANTAR

No. SP. /WPB.16/KP.031/2014

No.	Jenis Surat / Bahan Yang Dikirim	Banyaknya	Keterangan
(1)	(2)	(3)	(4)
1	Laporan Hasil Pemantauan Pengendalian Intern KPPN Surabaya I Periode : Bulan April 2014, yang terdiri dari : 1. Penerbitan SP2D LS Non Gaji 2. Penyusunan LKP 3. Penyusunan LKPP Tingkat KPPN 4. Pemrosesan Permintaan TUP 5. Pemrosesan tagihan dalam rangka pembayaran tagihan penyediaan barang/jasa	5 berkas	Disampaikan dengan hormat sebagaimana Surat Kepala Kanwil Ditjen Perbendaharaan Provinsi Jawa Timur No.S-770/WPB.16/BD.0303/2013 Tgl. 29 April 2013

Plh.Kepala Seksi Manajemen Satker

Laporan Hasil Pemantauan Pengendalian KPPN

Foto M-79	**Foto M-80**
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Laporan PPPI Kanwil DJPBN	Rencana Strategis Kementerian Keuangan (SPAN terletak pada hal.66)

Sekretaris Ditjen Perbendaharaan
Unit Kepatuhan Internal
apangan Banteng Timur No.2-4
rta

09 Oktober 2013

SURAT PENGANTAR
NOMOR : SP- 533 /WPB.16/BD.0303/2013

Uraian	Banyaknya	Keterangan
Bersama ini kami sampaikan Laporan tanggal 09 September 2013 No. SP-533/WPB.16/BD.0303/2013 Laporan Pelaksanaan Pemantauan Pengendalian Internal Triwulan III (Januari sd September 2013)	1 (satu) berkas	Memenuhi Keputusan Dirjen PBN No. KEP.34/PB/2013 dan Surat Dirjen PBN No. S-5334/PB.1/2013. Disampaikan dengan hormat, sebagai laporan, dengan permintaan setelah berkas diterima, lembar kedua Surat Pengantar ini mohon dikirimkan kembali ke Unit Kepatuhan Internal (UKI) Bidang Supervisi Kepatuhan Internal Kanwil DJPBN Provinsi Jawa Timur.

Kepala Kantor Wilayah,

PARDIARTO
NIP. 19540810197507100

KEPUTUSAN MENTERI KEUANGAN
NOMOR 40 /KMK.01/2010

TENTANG
RENCANA STRATEGIS KEMENTERIAN KEUANGAN

TAHUN 2010-2014

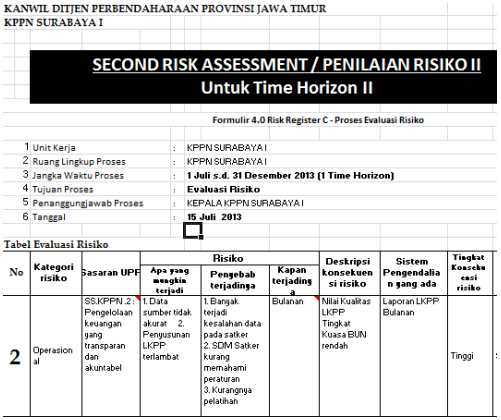
MENTERI KEUANGAN,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 19 ayat (2) Undang-Undang Nomor 25 Tahun 2004 tentang Sistem Perencanaan Pembangunan Nasional, perlu menetapkan Keputusan Menteri Keuangan tentang Rencana Strategis Kementerian Keuangan Tahun 2010-2014;

Mengingat :
1. Undang-Undang Nomor 25 Tahun 2004 tentang Sistem Perencanaan Pembangunan Nasional (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 104, Tambahan Lembaran Negara Republik Indonesia Nomor 4421);
2. Keputusan Presiden Nomor 84/P Tahun 2009;
3. Peraturan Menteri Negara Perencanaan Pembangunan Nasional/Kepala Badan Perencanaan Pembangunan Nasional Nomor 5 Tahun 2009 tentang Pedoman Penyusunan Rencana Strategis Kementerian Negara/Lembaga (Renstra K/L) 2010-2014;

Foto M-81

Tanggal validasi : 12 Mei 2014



KANWIL DITJEN PERBENDAHARAAN PROVINSI JAWA TIMUR
KPPN SURABAYA I

SECOND RISK ASSESSMENT / PENILAIAN RISIKO II
Untuk Time Horizon II

Formulir 4.0 Risk Register C - Proses Evaluasi Risiko

1	Unit Kerja	:	KPPN SURABAYA I
2	Ruang Lingkup Proses	:	KPPN SURABAYA I
3	Jangka Waktu Proses	:	**1 Juli s.d. 31 Desember 2013 (1 Time Horizon)**
4	Tujuan Proses	:	**Evaluasi Risiko**
5	Penanggungjawab Proses	:	KEPALA KPPN SURABAYA I
6	Tanggal	:	**15 Juli 2013**

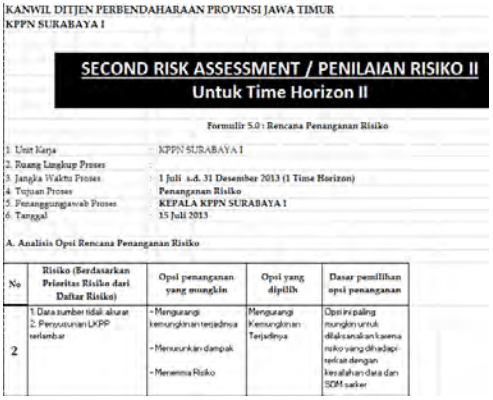
Tabel Evaluasi Risiko

No	Kategori risiko	Sasaran UPP	Risiko			Deskripsi konsekuensi risiko	Sistem Pengendalian yang ada	Tingkat Kosekuensi risiko
			Apa yang mungkin terjadi	Pengebab terjadinya	Kapan terjadinya			
2	Operasional	SS:KPPN .2. Pengelolaan keuangan yang transparan dan akuntabel	1. Data sumber tidak akurat 2. Penyusunan LKPP terlambat	1. Banyak terjadi kesalahan data pada satker 2. SDM Satker kurang memahami peraturan 3. Kurangnya pelatihan	Bulanan	Nilai Kualitas LKPP Tingkat Kuasa BUN rendah	Laporan LKPP Bulanan	Tinggi

Evaluasi Risiko Time Horizon II

Foto M-82

Tanggal validasi : 12 Mei 2014



KANWIL DITJEN PERBENDAHARAAN PROVINSI JAWA TIMUR
KPPN SURABAYA I

SECOND RISK ASSESSMENT / PENILAIAN RISIKO II
Untuk Time Horizon II

Formulir 5.0 : Rencana Penanganan Risiko

1.	Unit Kerja	KPPN SURABAYA I
2.	Ruang Lingkup Proses	
3.	Jangka Waktu Proses	1 Juli s.d. 31 Desember 2013 (1 Time Horizon)
4.	Tujuan Proses	Penanganan Risiko
5.	Penanggungjawab Proses	KEPALA KPPN SURABAYA I
6.	Tanggal	15 Juli 2013

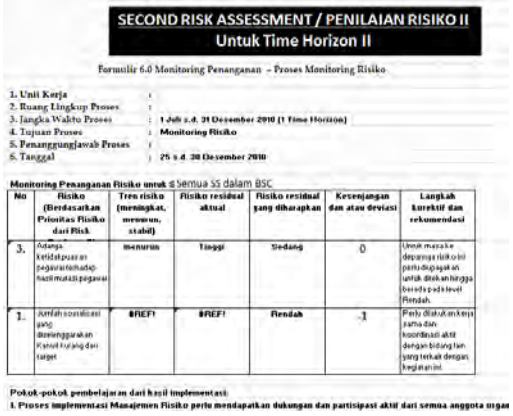
A. Analisis Opsi Rencana Penanganan Risiko

No	Risiko (Berdasarkan Peristiwa Risiko dari Daftar Risiko)	Opsi penanganan yang mungkin	Opsi yang dipilih	Dasar pemilihan opsi penanganan
2	1. Data sumber tidak akurat 2. Penyusunan LKPP terlambat	- Mengurangi kemungkinan terjadinya - Menurunkan dampak - Menerima Risiko	Mengurangi Kemungkinan Terjadinya	Opsi ini paling mungkin untuk dilaksanakan karena risiko yang dihadapi terkait dengan kesalahan data dan SDM satker

Penanganan Risiko Time Horizon II

Foto M-83

Tanggal validasi : 12 Mei 2014



SECOND RISK ASSESSMENT / PENILAIAN RISIKO II
Untuk Time Horizon II

Formulir 6.0 Monitoring Penanganan – Proses Monitoring Risiko

1. Unit Kerja :
2. Ruang Lingkup Proses :
3. Jangka Waktu Proses : 1 Juli s.d. 31 Desember 2010 (1 Time Horizon)
4. Tujuan Proses : Monitoring Risiko
5. Penanggungjawab Proses :
6. Tanggal : 25 s.d. 30 Desember 2010

Monitoring Penanganan Risiko untuk 6 Semua 5S dalam BSC

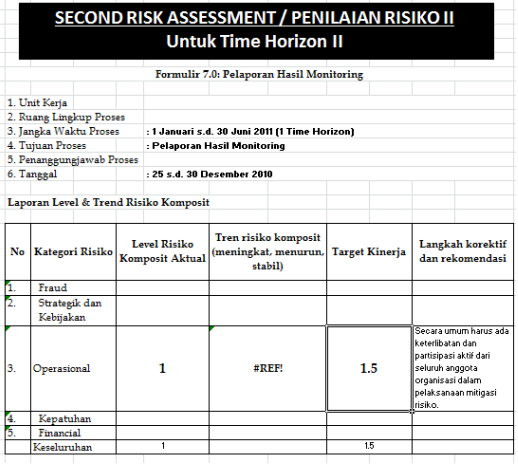
No	Risiko (Berdasarkan Prioritas Risiko dari Risk	Tren risiko (meningkat, menurun, stabil)	Risiko residual aktual	Risiko residual yang diharapkan	Kesenjangan dan atau deviasi	Langkah korektif dan rekomendasi
3.	Adanya ketidakpuasan pegawai terhadap hasil mutasi pegawai	menurun	Tinggi	Sedang	0	Untuk masa ke depannya risiko ini perlu dipantau untuk diturunkan hingga berada pada level Rendah.
1.	Jumlah sosialisasi yang diselenggarakan Kurang/ lebih dari target	#REF!	#REF!	Rendah	-1	Perlu ditunjukkan kerja sama dan koordinasi aktif dengan bidang lain yang terkait dengan kegiatan ini.

Pokok-pokok pembelajaran dari hasil implementasi:
1. Proses implementasi Manajemen Risiko perlu mendapatkan dukungan dan partisipasi aktif dari semua anggota organ

Monitoring Risiko Time Horizon II

Foto M-84

Tanggal validasi : 12 Mei 2014



SECOND RISK ASSESSMENT / PENILAIAN RISIKO II
Untuk Time Horizon II

Formulir 7.0: Pelaporan Hasil Monitoring

1. Unit Kerja
2. Ruang Lingkup Proses
3. Jangka Waktu Proses : 1 Januari s.d. 30 Juni 2011 (1 Time Horizon)
4. Tujuan Proses : Pelaporan Hasil Monitoring
5. Penanggungjawab Proses
6. Tanggal : 25 s.d. 30 Desember 2010

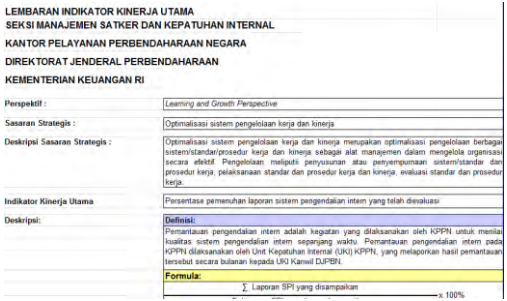
Laporan Level & Trend Risiko Komposit

No	Kategori Risiko	Level Risiko Komposit Aktual	Tren risiko komposit (meningkat, menurun, stabil)	Target Kinerja	Langkah korektif dan rekomendasi
1.	Fraud				
2.	Strategik dan Kebijakan				
3.	Operasional	1	#REF!	1.5	Secara umum harus ada keterlibatan dan partisipasi aktif dari seluruh anggota organisasi dalam pelaksanaan mitigasi risiko.
4.	Kepatuhan				
5.	Financial				
	Keseluruhan	1		1.5	

Laporan Hasil Monitoring

Foto M-85

Tanggal validasi : 12 Mei 2014



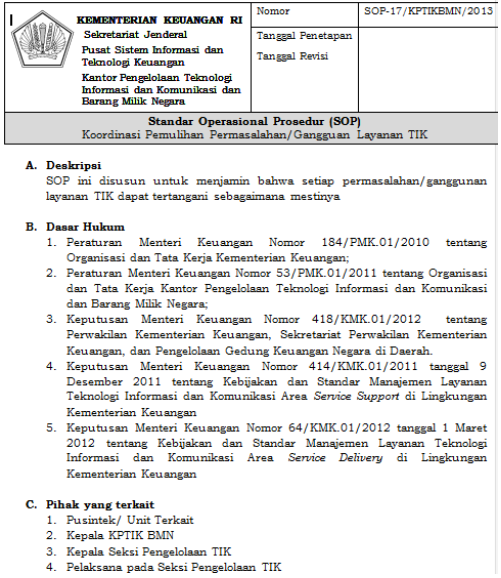
LEMBARAN INDIKATOR KINERJA UTAMA
SEKSI MANAJEMEN SATKER DAN KEPATUHAN INTERNAL
KANTOR PELAYANAN PERBENDAHARAAN NEGARA
DIREKTORAT JENDERAL PERBENDAHARAAN
KEMENTERIAN KEUANGAN RI

Perspektif :	*Learning and Growth Perspective*
Sasaran Strategis :	Optimalisasi sistem pengelolaan kerja dan kinerja
Deskripsi Sasaran Strategis :	Optimalisasi sistem pengelolaan kerja dan kinerja merupakan optimalisasi pengelolaan berbagai sistem/standar/prosedur kerja dan kinerja sebagai alat manajemen dalam mengelola organisasi secara efektif. Pengelolaan meliputi penyusunan atau penyempurnaan sistem/standar dan prosedur kerja, pelaksanaan standar dan prosedur kerja dan kinerja, evaluasi standar dan prosedur kerja.
Indikator Kinerja Utama	Persentase pemenuhan laporan sistem pengendalian intern yang telah dievaluasi
Deskripsi:	**Definisi:** Pemantauan pengendalian intern adalah kegiatan yang dilaksanakan oleh KPPN untuk menilai kualitas sistem pengendalian intern sepanjang waktu. Pemantauan pengendalian intern pada KPPN dilaksanakan oleh Unit Kepatuhan Internal (UKI) KPPN, yang melaporkan hasil pemantauan tersebut secara bulanan kepada UKI Kanwil DJPBN. **Formula:** ∑ Laporan SPI yang disampaikan / ∑ Laporan SPI yang harus disampaikan x 100%

IKU Pengendalian Internal Kanwil DJPBN

Foto M-86

Tanggal validasi : 12 Mei 2014



KEMENTERIAN KEUANGAN RI Sekretariat Jenderal Pusat Sistem Informasi dan Teknologi Keuangan Kantor Pengelolaan Teknologi Informasi dan Komunikasi dan Barang Milik Negara	Nomor	SOP-17/KPTIKBMN/2013
	Tanggal Penetapan Tanggal Revisi	

Standar Operasional Prosedur (SOP)
Koordinasi Pemulihan Permasalahan/Gangguan Layanan TIK

A. Deskripsi

SOP ini disusun untuk menjamin bahwa setiap permasalahan/gangguan layanan TIK dapat tertangani sebagaimana mestinya

B. Dasar Hukum

1. Peraturan Menteri Keuangan Nomor 184/PMK.01/2010 tentang Organisasi dan Tata Kerja Kementerian Keuangan;
2. Peraturan Menteri Keuangan Nomor 53/PMK.01/2011 tentang Organisasi dan Tata Kerja Kantor Pengelolaan Teknologi Informasi dan Komunikasi dan Barang Milik Negara;
3. Keputusan Menteri Keuangan Nomor 418/KMK.01/2012 tentang Perwakilan Kementerian Keuangan, Sekretariat Perwakilan Kementerian Keuangan, dan Pengelolaan Gedung Keuangan Negara di Daerah.
4. Keputusan Menteri Keuangan Nomor 414/KMK.01/2011 tanggal 9 Desember 2011 tentang Kebijakan dan Standar Manajemen Layanan Teknologi Informasi dan Komunikasi Area *Service Support* di Lingkungan Kementerian Keuangan
5. Keputusan Menteri Keuangan Nomor 64/KMK.01/2012 tanggal 1 Maret 2012 tentang Kebijakan dan Standar Manajemen Layanan Teknologi Informasi dan Komunikasi Area *Service Delivery* di Lingkungan Kementerian Keuangan

C. Pihak yang terkait

1. Pusintek/ Unit Terkait
2. Kepala KPTIK BMN
3. Kepala Seksi Pengelolaan TIK
4. Pelaksana pada Seksi Pengelolaan TIK

SOP Pemulihan Layanan TIK

Foto M-87

Tanggal validasi : 12 Mei 2014

KEMENTERIAN KEUANGAN RI Sekretariat Jenderal Pusat Sistem Informasi dan Teknologi Keuangan Kantor Pengelolaan Teknologi Informasi dan Komunikasi dan Barang Milik Negara	Nomor	SOP-23/KPTIKBMN/2013
	Tanggal Penetapan Tanggal Revisi	
Standar Operasional Prosedur (SOP) Penyelesaian Gangguan Layanan TIK		

A. Deskripsi

SOP ini disusun untuk menjamin bahwa setiap gangguan TIK dapat diselesaikan

B. Dasar Hukum

1. Peraturan Menteri Keuangan Nomor 184/PMK.01/2010 tentang Organisasi dan Tata Kerja Kementerian Keuangan;
2. Peraturan Menteri Keuangan Nomor 53/PMK.01/2011 tentang Organisasi dan Tata Kerja Kantor Pengelolaan Teknologi Informasi dan Komunikasi dan Barang Milik Negara;
3. Keputusan Menteri Keuangan Nomor 418/KMK.01/2012 tentang Perwakilan Kementerian Keuangan, Sekretariat Perwakilan Kementerian Keuangan, dan Pengelolaan Gedung Keuangan Negara di Daerah.
4. Keputusan Menteri Keuangan Nomor 414/KMK.01/2011 tanggal 9 Desember 2011 tentang Kebijakan dan Standar Manajemen Layanan Teknologi Informasi dan Komunikasi Area *Service Support* di Lingkungan Kementerian Keuangan
5. Keputusan Menteri Keuangan Nomor 64/KMK.01/2012 tanggal 1 Maret 2012 tentang Kebijakan dan Standar Manajemen Layanan Teknologi Informasi dan Komunikasi Area *Service Delivery* di Lingkungan Kementerian Keuangan

C. Pihak yang terkait

1. Unit Terkait
2. Pusintek
3. Kepala KPTIKBMN
4. Kepala Seksi Pengelolaan TIK

SOP Penyelesaian Gangguan Layanan TIK

Foto M-88

Tanggal validasi : 12 Mei 2014

KEMENTERIAN KEUANGAN RI Sekretariat Jenderal Pusat Sistem Informasi dan Teknologi Keuangan Kantor Pengelolaan Teknologi Informasi dan Komunikasi dan Barang Milik Negara	Nomor	SOP-16/KPTIKBMN/2013
	Tanggal Penetapan Tanggal Revisi	
Standar Operasional Prosedur (SOP) Pengelolaan Jaringan Dan Infrastruktur		

A. Deskripsi

SOP ini disusun untuk menjamin kelancaran arus informasi melalui jaringan intranet dan internet.

B. Dasar Hukum

1. Peraturan Menteri Keuangan Nomor 184/PMK.01/2010 tentang Organisasi dan Tata Kerja Kementerian Keuangan;
2. Peraturan Menteri Keuangan Nomor 53/PMK.01/2011 tentang Organisasi dan Tata Kerja Kantor Pengelolaan Teknologi Informasi dan Komunikasi dan Barang Milik Negara;
3. Keputusan Menteri Keuangan Nomor 418/KMK.01/2012 tentang Perwakilan Kementerian Keuangan, Sekretariat Perwakilan Kementerian Keuangan, dan Pengelolaan Gedung Keuangan Negara di Daerah.
4. Keputusan Menteri Keuangan Nomor 414/KMK.01/2011 tanggal 9 Desember 2011 tentang Kebijakan dan Standar Manajemen Layanan Teknologi Informasi dan Komunikasi Area *Service Support* di Lingkungan Kementerian Keuangan
5. Keputusan Menteri Keuangan Nomor 64/KMK.01/2012 tanggal 1 Maret 2012 tentang Kebijakan dan Standar Manajemen Layanan Teknologi Informasi dan Komunikasi Area *Service Delivery* di Lingkungan Kementerian Keuangan

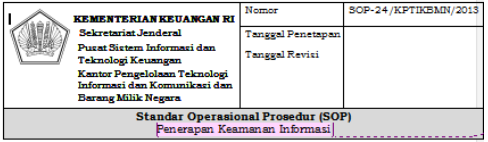
C. Pihak yang terkait

1. Pusintek
2. Kepala KPTIK BMN
3. Kepala Seksi Pengelolaan TIK
4. Pelaksana

SOP Pengelolaan Jaringan & Infrastruktur

Foto M-89

Tanggal validasi : 12 Mei 2014



KEMENTERIAN KEUANGAN RI Sekretariat Jenderal Pusat Sistem Informasi dan Teknologi Keuangan Kantor Pengelolaan Teknologi Informasi dan Komunikasi dan Barang Milik Negara	Nomor	SOP-24/KPTIKBMN/2013
	Tanggal Penetapan Tanggal Revisi	

Standar Operasional Prosedur (SOP)
Penerapan Keamanan Informasi

A. Deskripsi
SOP ini disusun untuk menjamin pelaksanaan penerapan keamanan informasi

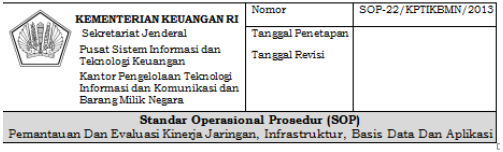
B. Dasar Hukum
1. Peraturan Menteri Keuangan Nomor 184/PMK.01/2010 tentang Organisasi dan Tata Kerja Kementerian Keuangan;
2. Peraturan Menteri Keuangan Nomor 53/PMK.01/2011 tentang Organisasi dan Tata Kerja Kantor Pengelolaan Teknologi Informasi dan Komunikasi dan Barang Milik Negara;
3. Keputusan Menteri Keuangan Nomor 418/KMK.01/2012 tentang Perwakilan Kementerian Keuangan, Sekretariat Perwakilan Kementerian Keuangan, dan Pengelolaan Gedung Keuangan Negara di Daerah
4. Keputusan Menteri Keuangan Nomor 512/KMK.01/2009 tanggal 28 Desember 2009 tentang Kebijakan dan Standar Penggunaan Akun dan Kata Sandi, Surat Elektronik, dan Internet di Lingkungan Departemen Keuangan
5. Keputusan Menteri Keuangan Nomor 350/KMK.01/2010 tanggal 27 Agustus 2010 tentang Kebijakan dan Standar Pengelolaan Data Elektronik di Lingkungan Kementerian Keuangan
6. Keputusan Menteri Keuangan Nomor 479/KMK.01/2010 tanggal 13 Desember 2010 tentang Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di Lingkungan Kementerian Keuangan

C. Pihak yang terkait
1. Pusintek
2. Kepala KPTIK BMN
3. Kepala Seksi Pengelolaan TIK
4. Seksi Pengelolaan BMN/ Subbagian Tata Usaha

SOP Penerapan Keamanan Informasi

Foto M-90

Tanggal validasi : 12 Mei 2014



KEMENTERIAN KEUANGAN RI Sekretariat Jenderal Pusat Sistem Informasi dan Teknologi Keuangan Kantor Pengelolaan Teknologi Informasi dan Komunikasi dan Barang Milik Negara	Nomor	SOP-22/KPTIKBMN/2013
	Tanggal Penetapan Tanggal Revisi	

Standar Operasional Prosedur (SOP)
Pemantauan Dan Evaluasi Kinerja Jaringan, Infrastruktur, Basis Data Dan Aplikasi

A. Deskripsi
SOP ini disusun untuk menjamin kegiatan pemantauan dan evaluasi kinerja jaringan, infrastruktur, basis data, dan aplikasi

B. Dasar Hukum
1. Peraturan Menteri Keuangan Nomor 184/PMK.01/2010 tentang Organisasi dan Tata Kerja Kementerian Keuangan;
2. Peraturan Menteri Keuangan Nomor 53/PMK.01/2011 tentang Organisasi dan Tata Kerja Kantor Pengelolaan Teknologi Informasi dan Komunikasi dan Barang Milik Negara;
3. Keputusan Menteri Keuangan Nomor 418/KMK.01/2012 tentang Perwakilan Kementerian Keuangan, Sekretariat Perwakilan Kementerian Keuangan, dan Pengelolaan Gedung Keuangan Negara di Daerah.
4. Keputusan Menteri Keuangan Nomor 414/KMK.01/2011 tanggal 9 Desember 2011 tentang Kebijakan dan Standar Manajemen Layanan Teknologi Informasi dan Komunikasi Area *Service Support* di Lingkungan Kementerian Keuangan
5. Keputusan Menteri Keuangan Nomor 64/KMK.01/2012 tanggal 1 Maret 2012 tentang Kebijakan dan Standar Manajemen Layanan Teknologi Informasi dan Komunikasi Area *Service Delivery* di Lingkungan Kementerian Keuangan

C. Pihak yang terkait
1. Pusintek
2. Kepala KPTIK BMN
3. Kepala Seksi Pengelolaan TIK
4. Pelaksana pada Seksi Pengelolaan TIK

SOP Pemantauan Evaluasi Jaringan, Basis Data

Foto M-91	Foto M-92
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Website SEKJEN Kementerian Keuangan	Menu Pustaka berisi Peraturan/Perundang-undangan pada Website SPAN

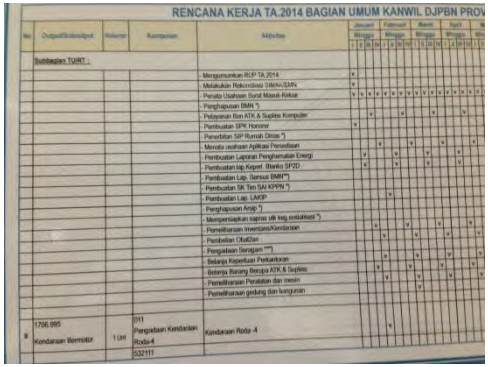
Foto M-93	Foto M-94
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Rencana kerja TA.2014	Peraturan/Perundang-undangan dan Dokumen Output Kanwil DJPBN

Foto M-95

Tanggal validasi : 12 Mei 2014

Kepada Yth.
Kepala
GKN Surabaya I
Jl.Indrapura No. 5 Lt. 1 Surabaya 60175

Perihal : Surat Tugas Maintenance Perangkat

Dengan Hormat,

Menindaklanjuti :
Kontrak nomor : PRJ-6/IT.2/PPK/2014 tentang Sewa Komunikasi Intranet Pusintek Tahun 2014 tanggal 15 Januari 2014 dimana PT Telekomunikasi Indonesia, Tbk. telah ditunjuk sebagai Penyedia Jasa untuk pelaksanaan pekerjaan tersebut.

Sehubungan dengan hal tersebut dalam rangka pemeliharaan Router di lingkungan Kementerian Keuangan, bersama ini kami mohon kesediaan Bapak/ibu untuk dapat memberikan izin Petugas Telkom sebagai berikut untuk melaksanakan pekerjaan pemeliharaan router di lokasi GKN Surabaya I

Nama : Anjar Isna Fadillah
Jabatan : Service Point Engineer (SPE)

Demikian disampaikan, atas perhatian dan kerjasama yang diberikan kami ucapkan terima kasih.

Hormat kami,

Telkom Indonesia

Guruh Adhi Laksana
Senior Enterprise Account Manager

Surat Tugas Maintenance Perangkat

Foto M-96

Tanggal validasi : 12 Mei 2014

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
SEKRETARIAT JENDERAL
PUSAT SISTEM INFORMASI DAN TEKNOLOGI KEUANGAN

Formulir Permintaan Alamat Surat Elektronik Grup

Usulan nama grup :
Berlaku s.d. / / 20

Penanggung Jawab Struktural
Nama :
NIP :
Jabatan :
Unit kerja :
Alamat kantor :
Nomor telepon : internal
Nomor HP :
Alamat surat elektronik :

Formulir Permintaan Alamat Email untuk Akses ke Jaringan

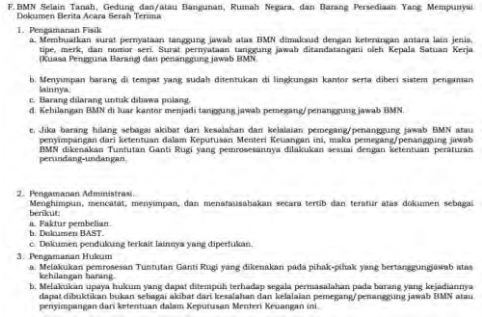
Foto M-97	Foto M-98
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	 F. BMN Selain Tanah, Gedung dan/atau Bangunan, Rumah Negara, dan Barang Persediaan Yang Mempunyai Dokumen Berita Acara Serah Terima 1. Pengamanan Fisik a. Membuatkan surat pernyataan tanggung jawab atas BMN dimaksud dengan keterangan antara lain jenis, tipe, merk, dan nomor seri. Surat pernyataan tanggung jawab ditandatangani oleh Kepala Satuan Kerja (Kuasa Pengguna Barang) dan penanggung jawab BMN. b. Menyimpan barang di tempat yang sudah ditentukan di lingkungan kantor serta diberi sistem pengaman lainnya. c. Barang dilarang untuk dibawa pulang. d. Kehilangan BMN di luar kantor menjadi tanggung jawab pemegang/penanggung jawab BMN. e. Jika barang hilang sebagai akibat dari kesalahan dari kelalaian pemegang/penanggung jawab BMN atau penyimpangan dari ketentuan dalam Keputusan Menteri Keuangan ini, maka pemegang/penanggung jawab BMN dikenakan Tuntutan Ganti Rugi yang pemrosesannya dilakukan sesuai dengan ketentuan peraturan perundang-undangan. 2. Pengamanan Administrasi. Menghimpun, mencatat, menyimpan, dan menatausahakan secara tertib dan teratur atas dokumen sebagai berikut: a. Faktur pembelian. b. Dokumen BAST. c. Dokumen pendukung terkait lainnya yang diperlukan. 3. Pengamanan Hukum a. Melakukan pemrosesan Tuntutan Ganti Rugi yang dikenakan pada pihak-pihak yang bertanggungjawab atas kehilangan barang. b. Melakukan upaya hukum yang dapat ditempuh terhadap segala permasalahan pada barang yang kejadiannya dapat dibuktikan bukan sebagai akibat dari kesalahan dan kelalaian pemegang/penanggung jawab BMN atau penyimpangan dari ketentuan dalam Keputusan Menteri Keuangan ini.
Unduh peraturan pada Web DJPBN	PEDOMAN PENGAMANAN BARANG MILIK NEGARA KEMENTERIAN KEUANGAN

Foto M-99

Tanggal validasi : 12 Mei 2014

MENTERI KEUANGAN
REPUBLIK INDONESIA
SALINAN

KEPUTUSAN MENTERI KEUANGAN

NOMOR 351/KMK.01/2011

TENTANG

KEBIJAKAN DAN STANDAR SIKLUS PENGEMBANGAN SISTEM INFORMASI DI LINGKUNGAN KEMENTERIAN KEUANGAN

MENTERI KEUANGAN,

Menimbang : a. bahwa dalam rangka mendukung pengembangan sistem informasi yang efektif dan efisien, diperlukan adanya pedoman siklus pengembangan sistem informasi di lingkungan Kementerian Keuangan;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Keputusan Menteri Keuangan tentang Kebijakan Dan Standar Siklus Pengembangan Sistem Informasi Di Lingkungan Kementerian Keuangan;

Mengingat : 1. Keputusan Presiden Nomor 56/P Tahun 2010;

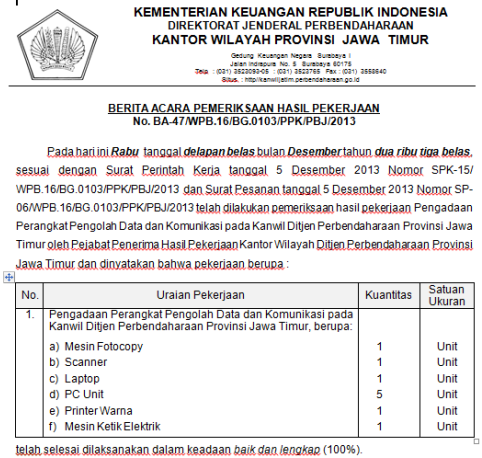
2. Peraturan Menteri Keuangan Nomor 184/PMK.01/2010 tentang Organisasi Dan Tata Kerja Kementerian Keuangan;

3. Keputusan Menteri Keuangan Nomor 260/KMK.01/2009 tentang Kebijakan Pengelolaan Teknologi Informasi Dan Komunikasi Di Lingkungan Departemen Keuangan;

KMK.351/KMK.01/2011 Kebijakan Pengembangan Sistem Informasi

Foto M-100

Tanggal validasi : 12 Mei 2014



KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN
KANTOR WILAYAH PROVINSI JAWA TIMUR

Gedung Keuangan Negara Surabaya I
Jalan Indrapura No. 8 Surabaya 60175
Telp. (031) 3523092-05 ; (031) 3522766 Fax. (031) 3559840
Situs : http://kanwil.jatim.perbendaharaan.go.id

BERITA ACARA PEMERIKSAAN HASIL PEKERJAAN
No. BA-47/WPB.16/BG.0103/PPK/PBJ/2013

Pada hari ini ***Rabu*** tanggal ***delapan belas*** bulan ***Desember*** tahun ***dua ribu tiga belas***, sesuai dengan Surat Perintah Kerja tanggal 5 Desember 2013 Nomor SPK-15/WPB.16/BG.0103/PPK/PBJ/2013 dan Surat Pesanan tanggal 5 Desember 2013 Nomor SP-06/WPB.16/BG.0103/PPK/PBJ/2013 telah dilakukan pemeriksaan hasil pekerjaan Pengadaan Perangkat Pengolah Data dan Komunikasi pada Kanwil Ditjen Perbendaharaan Provinsi Jawa Timur oleh Pejabat Penerima Hasil Pekerjaan Kantor Wilayah Ditjen Perbendaharaan Provinsi Jawa Timur dan dinyatakan bahwa pekerjaan berupa :

No.	Uraian Pekerjaan	Kuantitas	Satuan Ukuran
1.	Pengadaan Perangkat Pengolah Data dan Komunikasi pada Kanwil Ditjen Perbendaharaan Provinsi Jawa Timur, berupa:		
	a) Mesin Fotocopy	1	Unit
	b) Scanner	1	Unit
	c) Laptop	1	Unit
	d) PC Unit	5	Unit
	e) Printer Warna	1	Unit
	f) Mesin Ketik Elektrik	1	Unit

telah selesai dilaksanakan dalam keadaan *baik dan lengkap* (100%).

Demikian Berita Acara Pemeriksaan Hasil Pekerjaan ini dibuat untuk dipergunakan sebagaimana mestinya.

Berita Acara Serah Terima Pekerjaan

Foto M-101

Tanggal validasi : 12 Mei 2014

Bagian Kesatu
Berlakunya Hukuman Disiplin

Pasal 43

Hukuman disiplin yang dijatuhkan oleh:

a. Presiden;
b. Pejabat Pembina Kepegawaian untuk jenis hukuman disiplin sebagaimana dimaksud dalam Pasal 7 ayat (2), ayat (3), dan ayat (4) huruf a, huruf b, dan huruf c;
c. Gubernur selaku wakil pemerintah untuk jenis hukuman disiplin sebagaimana dimaksud dalam Pasal 7 ayat (4) huruf b dan huruf c;
d. Kepala Perwakilan Republik Indonesia; dan
e. Pejabat yang berwenang menghukum untuk jenis hukuman disiplin sebagaimana dimaksud dalam Pasal 7 ayat (2), mulai berlaku sejak tanggal keputusan ditetapkan.

Pasal 44

(1) Hukuman disiplin yang dijatuhkan oleh pejabat selain sebagaimana dimaksud dalam Pasal 43, apabila tidak diajukan keberatan maka mulai berlaku pada hari ke 15 (lima belas) setelah keputusan hukuman disiplin diterima.
(2) Hukuman disiplin yang dijatuhkan oleh pejabat selain sebagaimana dimaksud dalam Pasal 43, apabila diajukan keberatan maka mulai berlaku pada tanggal ditetapkannya keputusan atas keberatan.

Pasal 45

(1) Hukuman disiplin yang dijatuhkan oleh Pejabat Pembina Kepegawaian atau Gubernur selaku wakil pemerintah untuk jenis hukuman disiplin sebagaimana dimaksud dalam Pasal 7 ayat (4) huruf d dan huruf e, apabila tidak diajukan banding administratif maka mulai berlaku pada hari ke 15 (lima belas) setelah keputusan hukuman disiplin diterima.
(2) Hukuman disiplin yang dijatuhkan oleh Pejabat Pembina Kepegawaian atau Gubernur selaku wakil pemerintah untuk jenis hukuman disiplin sebagaimana dimaksud dalam Pasal 7 ayat (4) huruf d dan huruf e, apabila diajukan banding administratif maka mulai berlaku pada tanggal ditetapkannya keputusan banding administratif.

PP 53 Tahun 2010 Peraturan Disiplin Bagi Pegawai Negeri Sipil

Foto M-102

Tanggal validasi : 12 Mei 2014

a. koordinasi kegiatan direktorat jenderal;
b. koordinasi penyusunan peraturan perbendaharaan;
c. penyelenggaraan pengelolaan urusan organisasi dan ketatalaksanaan, kepegawaian, dan keuangan, serta pembinaan jabatan fungsional pada direktorat jenderal;
d. pelaksanaan pengembangan pegawai direktorat jenderal;
e. koordinasi penyusunan rencana kerja, rencana strategik, dan laporan akuntabilitas kinerja direktorat jenderal;
f. koordinasi dan pemantauan tindak lanjut hasil pemeriksaan aparat pengawasan fungsional dan pengawasan masyarakat;
g. pelaksanaan tata usaha, kearsipan, dan dokumentasi direktorat jenderal; dan
h. pelaksanaan urusan rumah tangga dan perlengkapan direktorat jenderal.

Pasal 826

Sekretariat Direktorat Jenderal terdiri atas:

a. Bagian Organisasi dan Tata Laksana;
b. Bagian Administrasi Kepegawaian;
c. Bagian Pengembangan Pegawai;
d. Bagian Keuangan;
e. Bagian Umum; dan
f. Kelompok Jabatan Fungsional.

Pasal 827

Bagian Organisasi dan Tata Laksana mempunyai tugas melaksanakan penataan organisasi dan ketatalaksanaan, koordinasi penyusunan peraturan, pengembangan organisasi dan kinerja, penyusunan pembakuan standar sarana dan prasarana kerja, penyusunan rencana strategis, rencana kinerja tahunan, pemantauan akuntabilitas kinerja, pelaporan, evaluasi tindak lanjut hasil pemeriksaan aparat pengawasan fungsional dan pengawasan masyarakat dan pengendalian pelaksanaan tugas kantor vertikal.

PMK 184/PMK.01/2010

Foto M-103

Tanggal validasi : 12 Mei 2014

2) Penerapan Standar Audit Inspektorat Jenderal (SAINS)

Tujuan pengawasan adalah membantu Inspektorat Jenderal untuk:

a) meningkatkan kualitas pengawasan/audit; dan

b) membuat interpretasi untuk menyamakan persepsi atas penerapan Standar Audit Inspektorat Jenderal (SAINS).

3) Program Modernisasi Manajemen Internal Audit Berdasarkan Arah Peraturan Pemerintah Nomor 60 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah

Tujuan pengawasan adalah:

a) mengembangkan perangkat dan prosedur penilaian kinerja;

b) mengembangkan *Blue Print* Penilaian Kinerja Pegawai sebagai panduan arah pengembangan kinerja pegawai Inspektorat Jenderal; dan

c) melakukan perbaikan/standardisasi tata kerja audit dengan cara membuat satu pedoman metodologi kegiatan audit internal dalam rangka reorientasi peran Inspektorat Jenderal dan upaya menjadi benchmark bagi Aparat Pengawasan Intern Pemerintah lainnya.

4) Program Dukungan Peningkatan Kualitas Laporan Keuangan Kementerian Negara/Lembaga Lain

Tujuan pengawasan adalah membantu Kementerian/Lembaga lain dalam peningkatan kualitas laporan keuangan.

m.Pencegahan dan Penindakan Korupsi, Kolusi, dan Nepotisme

1) Pencegahan Korupsi (Sosialisasi dan Survei Pencegahan Korupsi)

Tujuan pengawasan adalah:

a) menumbuhkan sikap tidak korupsi; dan

b) meningkatkan kesadaran untuk berani melaporkan dugaan korupsi.

2) *Surveillance* atas Penyimpangan dalam Pelayanan Publik dan Pengadaan Barang/Jasa

Tujuan pengawasan adalah:

a) mengumpulkan data dan informasi terkait praktik penyimpangan kegiatan pelayanan publik dan pengadaan barang/jasa;

PMK No.59/PMK.09/2010

Foto M-104

Tanggal validasi : 12 Mei 2014

TAHAPAN PENUNJUKAN PELAKSANA PEMANTAUAN

A. Prinsip Penunjukan

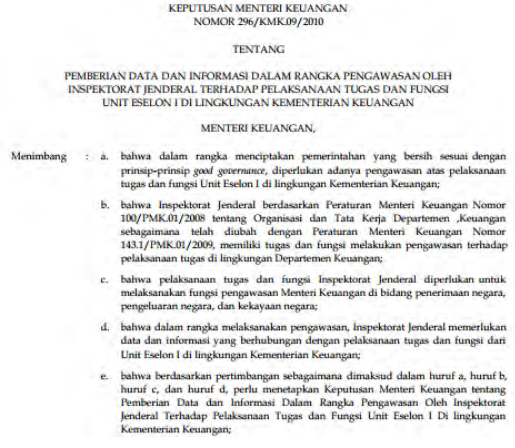
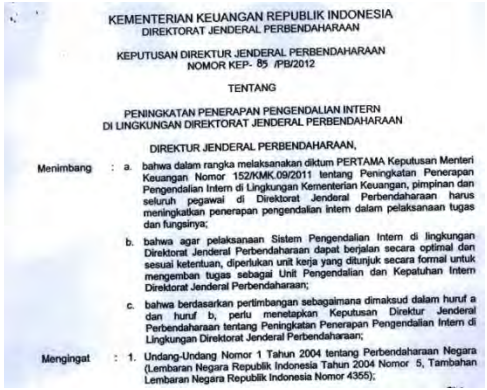
Pelaksana Pemantauan ditunjuk oleh Menteri Keuangan sebagaimana ditetapkan dalam Lampiran I Keputusan Menteri Keuangan ini. Penunjukan tersebut dilaksanakan dengan memperhatikan beban kerja (*workload*) dan independensi terhadap kegiatan yang dipantau (tidak menjalankan kegiatan utama organisasi).

B. Level Pelaksana Pemantauan

1. Untuk unit Eselon I yang tidak memiliki satuan kerja vertikal, salah satu unit eselon II berikut salah satu unit eselon III di bawahnya ditunjuk sebagai Pelaksana Pemantauan tingkat Eselon I untuk melaksanakan tugas pemantauan pengendalian intern bagi seluruh satuan kerja Eselon I tersebut. Level Pelaksana Pemantauan tersebut digambarkan sebagai berikut.

Gambar 1. Level Pelaksana Pemantauan Eselon I Tanpa Unit Vertikal

KMK 152/KMK.09/2011

Foto M-105	Foto M-106
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
KMK.296/KMK.09/2010	KEPDIRJEN No.85/PB/2012

KEPUTUSAN MENTERI KEUANGAN
NOMOR 296/KMK.09/2010

TENTANG

PEMBERIAN DATA DAN INFORMASI DALAM RANGKA PENGAWASAN OLEH INSPEKTORAT JENDERAL TERHADAP PELAKSANAAN TUGAS DAN FUNGSI UNIT ESELON I DI LINGKUNGAN KEMENTERIAN KEUANGAN

MENTERI KEUANGAN,

Menimbang : a. bahwa dalam rangka menciptakan pemerintahan yang bersih sesuai dengan prinsip-prinsip *good governance*, diperlukan adanya pengawasan atas pelaksanaan tugas dan fungsi Unit Eselon I di lingkungan Kementerian Keuangan;

b. bahwa Inspektorat Jenderal berdasarkan Peraturan Menteri Keuangan Nomor 100/PMK.01/2008 tentang Organisasi dan Tata Kerja Departemen ,Keuangan sebagaimana telah diubah dengan Peraturan Menteri Keuangan Nomor 143.1/PMK.01/2009, memiliki tugas dan fungsi melakukan pengawasan terhadap pelaksanaan tugas di lingkungan Departemen Keuangan;

c. bahwa pelaksanaan tugas dan fungsi Inspektorat Jenderal diperlukan untuk melaksanakan fungsi pengawasan Menteri Keuangan di bidang penerimaan negara, pengeluaran negara, dan kekayaan negara;

d. bahwa dalam rangka melaksanakan pengawasan, Inspektorat Jenderal memerlukan data dan informasi yang berhubungan dengan pelaksanaan tugas dan fungsi dari Unit Eselon I di lingkungan Kementerian Keuangan;

e. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, huruf c, dan huruf d, perlu menetapkan Keputusan Menteri Keuangan tentang Pemberian Data dan Informasi Dalam Rangka Pengawasan Oleh Inspektorat Jenderal Terhadap Pelaksanaan Tugas dan Fungsi Unit Eselon I Di lingkungan Kementerian Keuangan;

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PERBENDAHARAAN

KEPUTUSAN DIREKTUR JENDERAL PERBENDAHARAAN
NOMOR KEP- 85 /PB/2012

TENTANG

PENINGKATAN PENERAPAN PENGENDALIAN INTERN
DI LINGKUNGAN DIREKTORAT JENDERAL PERBENDAHARAAN

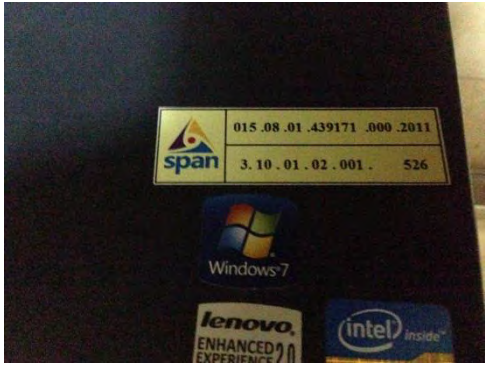
DIREKTUR JENDERAL PERBENDAHARAAN,

Menimbang : a. bahwa dalam rangka melaksanakan diktum PERTAMA Keputusan Menteri Keuangan Nomor 152/KMK.09/2011 tentang Peningkatan Penerapan Pengendalian Intern di Lingkungan Kementerian Keuangan, pimpinan dan seluruh pegawai di Direktorat Jenderal Perbendaharaan harus meningkatkan penerapan pengendalian intern dalam pelaksanaan tugas dan fungsinya;

b. bahwa agar pelaksanaan Sistem Pengendalian Intern di lingkungan Direktorat Jenderal Perbendaharaan dapat berjalan secara optimal dan sesuai ketentuan, diperlukan unit kerja yang ditunjuk secara formal untuk mengemban tugas sebagai Unit Pengendalian dan Kepatuhan Intern Direktorat Jenderal Perbendaharaan;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Keputusan Direktur Jenderal Perbendaharaan tentang Peningkatan Penerapan Pengendalian Intern di Lingkungan Direktorat Jenderal Perbendaharaan;

Mengingat : 1. Undang-Undang Nomor 1 Tahun 2004 tentang Perbendaharaan Negara (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 5, Tambahan Lembaran Negara Republik Indonesia Nomor 4355);

Foto M-107	**Foto M-108**
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Infrastruktur SPAN dengan logo khusus pada AKLAP Kanwil DJPBN	Perangkat SPAN pada lingkup Kantor vertical DJPBN yaitu Kanwil DJPBN dan KPPN

Perangkat pada lingkup Kantor Vertikal DJPB, yaitu Kanwil DJPB dan KPPN

Pada level yang lebih luas lagi, SPAN akan diakses dari seluruh Indonesia melalui kantor-kantor vertikal DJPB di daerah seperti Kanwil dan KPPN. Kantor-kantor ini tersebar di 30 provinsi se-Indonesia dari Sabang sampai Merauke dengan jumlah 30 Kanwil dan 177 KPPN. Beban kerjanya pun beragam. Karenanya, persebaran infrastrukturnya pun berbeda-beda. Berikut pembagiannya:

Kanwil dikategorikan menjadi:

- Kanwil Large (Jakarta, Jateng, Jatim, Sumut) mendapat jatah 8 komputer dan 5 printer
- Kanwil Medium (Jabar, Sumsel, dll) mendapat jatah 7 komputer 4 printer
- Kanwil Small (Yogyakarta, Banten, dll) mendapat jatah 6 komputer 4 printer

KPPN dikategorikan menjadi:

- KPPN Mega (Jakarta, kecuali jakarta VI) mendapat jatah 25 komputer 15 printer
- KPPN Large (Banda Aceh, Padang, dll) mendapat jatah 15 komputer 10 printer
- KPPN Medium (Tangerang, Bogor, dll) mendapat jatah 12 komputer 7 printer
- KPPN Small (Karawang, Sumedang, dll) mendapat jatah 8 komputer 5 printer

Komputer-komputer tersebut nantinya akan terhubung dengan sistem SPAN melalui VPN. Selain dari itu, komputer tersebut tidak dapat terhubung dengan jaringan internet luar. Ini juga merupakan salah satu bentuk pengamanan untuk mengantisipi tindakan-tindakan *hacking* oleh pihak yang tidak bertanggungjawab.

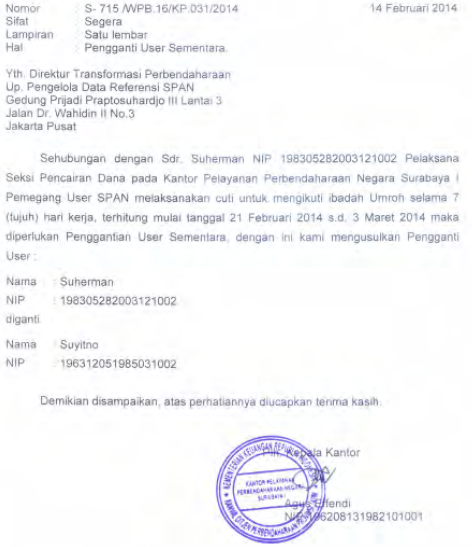
Foto M-109	Foto M-110
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Penggantian Akses User Kepala Seksi	Penggantian Akses User Pelaksana

Foto M-111	**Foto M-112**
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Tanda Terima Penyerahan Barang	Pelaksanaan Kegiatan TOT SPAN

Foto M-113

Tanggal validasi : 12 Mei 2014

4.3.4. Mengelola layanan pertukaran data elektronik sesuai dengan standar dan prosedur pertukaran data elektronik;
4.3.5. Membuat laporan pengelolaan layanan pertukaran data elektronik secara periodik untuk disampaikan ke CIO Kementerian Keuangan;
4.3.6. Mengubah hak akses Pengguna Data atas permintaan pihak terkait;
4.3.7. Menindaklanjuti laporan masalah infrastruktur pertukaran data elektronik;
4.3.8. Meneruskan laporan kejanggalan/anomali data kepada Pemilik Data;
4.3.9. Menjamin ketersediaan infrastruktur pertukaran data elektronik agar proses pertukaran data elektronik berjalan dengan baik; dan
4.3.10. Dalam hal infrastruktur pertukaran data elektronik belum tersedia atau mengalami gangguan, Kustodian Pertukaran Data menyampaikan data kepada Pengguna Data sesuai prosedur pertukaran data elektronik secara *offline*.

4.4. Apabila ada pihak yang tidak bisa memenuhi tanggung jawabnya, maka pihak terkait menyampaikan kepada CIO Kementerian Keuangan untuk ditindaklanjuti.

5. STANDAR

5.1. Infrastruktur Pertukaran Data Elektronik
Infrastruktur pertukaran data elektronik sekurang-kurangnya meliputi, tetapi tidak terbatas pada:
5.1.1. Perangkat keras antara lain: *server, client;*
5.1.2. Perangkat Jaringan antara lain: *switch, modem, router;* dan
5.1.3. Perangkat lunak antara lain: sistem operasi, sistem aplikasi pertukaran data elektronik.

KMK. 274/KMK.01/2010 Kebijakan dan Standar Pertukaran Data Elektronik

Foto M-114

Tanggal validasi : 12 Mei 2014

Laporan Koordinasi Pemulihan Permasalahan/Gangguan Layanan TIK
Gangguan Jaringan Internet

A. Laporan Gangguan/Permasalahan

Beberapa pegawai Kantor Pengelolaan TIK dan BMN Surabaya termasuk pegawai dari LPSE Surabaya mulai merasakan lambatnya jaringan internet sejak hari Jumat, 14 Maret 2014 termasuk untuk membuka aplikasi intranet seperti aplikasi persuratan (*http://workflow.depkeu.go.id*) dan aplikasi monitoring absen (*http://orpeg-absen.depkeu.go.id*). Website dan aplikasi yang dituju tidak terbuka sama sekali.

B. Investigasi Gangguan/Permasalahan

Seksi Pengelolaan TIK mencoba menelusuri dan mencari penyebab adanya gangguan dimaksud, beberapa hal yang dilakukan adalah:

1. Melakukan pengecekan fisik perangkat jaringan diantaranya perangkat wireless LAN, perangkat switch di ruangan Sekretariat KPTIK dan BMN dan perangkat switch di shufle kamar mandi lantai 2, semua perangkat dipastikan dalam kondisi aktif.
2. Melakukan pengujian koneksi ke IP Gateway 10.56.4.254, hasilnya *reply* dengan response time TTL yang cukup baik.
3. Melakukan pengujian koneksi ke IP DNS Server 10.100.93.1 dan 10.100.93.2, hasilnya reply namun dengan response time TTL hanya 56.

Atas dasar investigasi tersebut kami mencoba menarik kesimpulan bahwa perangkat jaringan di KPTIK dan BMN Surabaya tidak mengalami masalah dan kemungkinan besar gangguan terjadi di kantor pusat atau perangkat yang ada di kantor pusat.

Laporan Koordinasi Pemulihan Permasalahan/ Gangguan Layanan TIK

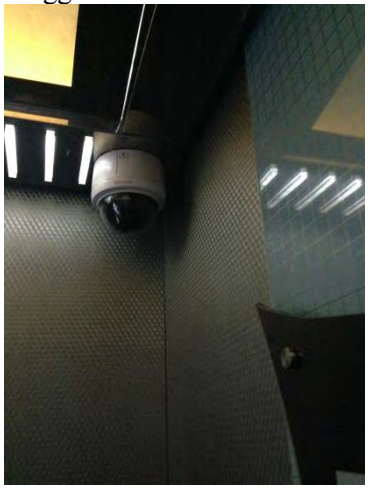
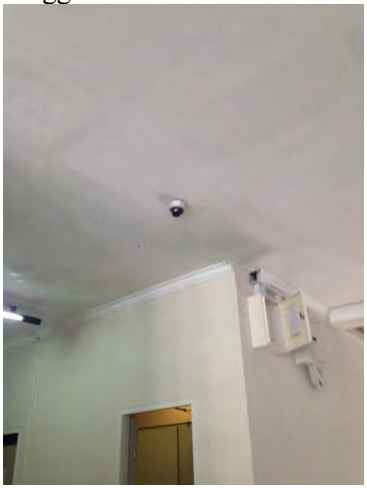
Foto M-115	**Foto M-116**
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
CCTV dalam Lift Kanwil DJPBN	CCTV seluruh Ruangan pada Kanwil DJPBN

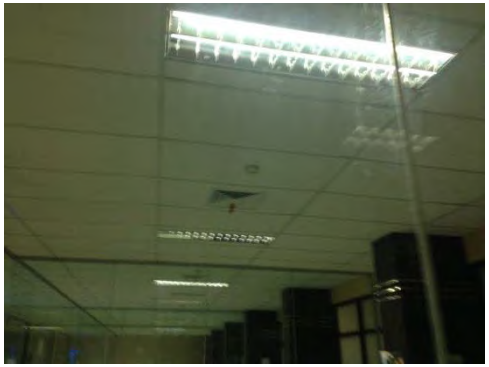
Foto M-117	Foto M-118
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Smoke Detector seluruh gedung Kanwil DJPBN	Smoke Detector Ruangan pada Kanwil DJPBN

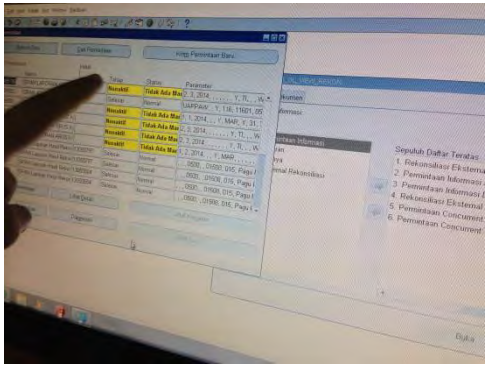
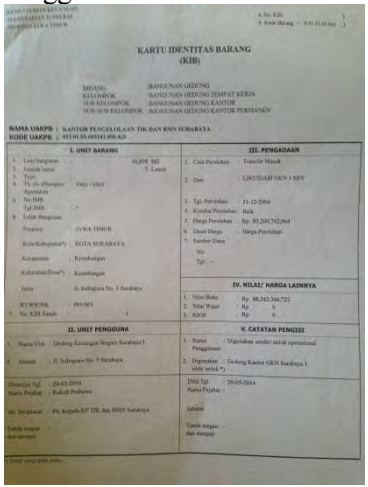
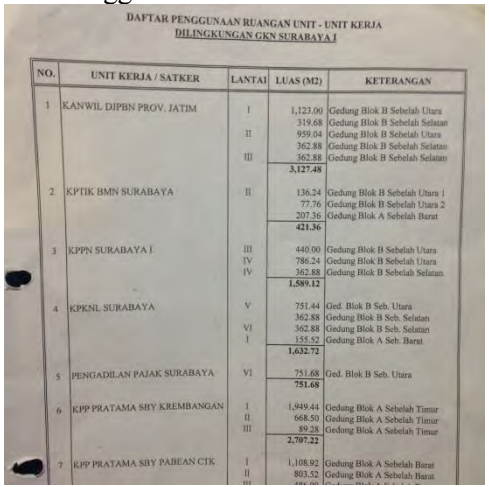
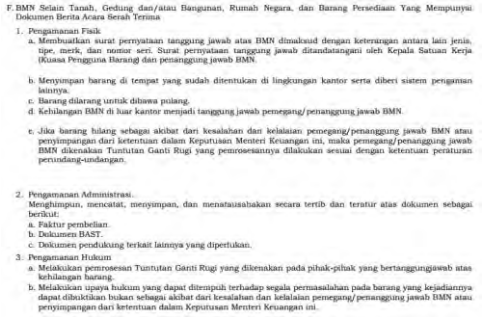
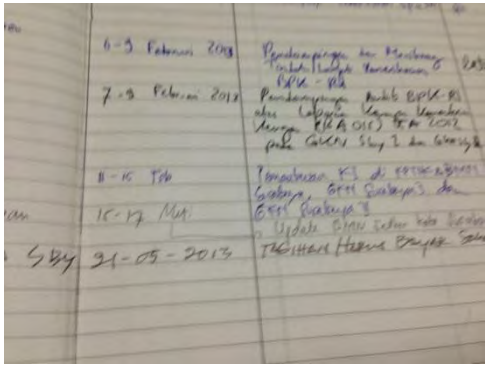
Foto M-119	**Foto M-120**
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Saklar Listrik Gedung lt.2 Kanwil DJPBN	Waktu Optimasi Proses SPAN pada Kanwil DJPBN

Foto M-121	Foto M-122
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
KIB (Kartu Identitas Barang) Gedung Keuangan Negara I	Daftar Pengguna Ruangan Unit-Unit Kerja Gedung Keuangan Negara I

KARTU IDENTITAS BARANG
(KIB)

DAFTAR PENGGUNAAN RUANGAN UNIT - UNIT KERJA
DILINGKUNGAN GKN SURABAYA I

NO.	UNIT KERJA / SATKER	LANTAI	LUAS (M2)	KETERANGAN
1	KANWIL DJPBN PROV. JATIM	I	1,123.00	Gedung Blok B Sebelah Utara
			319.68	Gedung Blok B Sebelah Selatan
		II	959.04	Gedung Blok B Sebelah Utara
			362.88	Gedung Blok B Sebelah Selatan
		III	362.88	Gedung Blok B Sebelah Selatan
			3,127.48	
2	KPTIK BMN SURABAYA	II	136.24	Gedung Blok B Sebelah Utara 1
			77.76	Gedung Blok B Sebelah Utara 2
			207.36	Gedung Blok A Sebelah Barat
			421.36	
3	KPPN SURABAYA I	III	440.00	Gedung Blok B Sebelah Utara
		IV	786.24	Gedung Blok B Sebelah Utara
		IV	362.88	Gedung Blok B Sebelah Selatan
			1,589.12	
4	KPKNL SURABAYA	V	751.44	Ged. Blok B Seb. Utara
			362.88	Gedung Blok B Seb. Selatan
		VI	362.88	Gedung Blok B Seb. Selatan
		I	155.52	Gedung Blok A Seb. Barat
			1,632.72	
5	PENGADILAN PAJAK SURABAYA	VI	751.68	Ged. Blok B Seb. Utara
			751.68	
6	KPP PRATAMA SBY KREMBANGAN	I	1,949.44	Gedung Blok A Sebelah Timur
		II	668.50	Gedung Blok A Sebelah Timur
		III	89.28	Gedung Blok A Sebelah Timur
			2,707.22	
7	KPP PRATAMA SBY PABEAN CTK	I	1,108.92	Gedung Blok A Sebelah Barat
		II	803.52	Gedung Blok A Sebelah Barat

Foto M-123	**Foto M-124**
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
KMK.21/KMK.01/2012 tentang Pedoman Pengamanan Barang Milik Negara	Maksud dan Tujuan Kunjuungan pada KPTIK Gedung Keuangan Negara I

F. BMN Selain Tanah, Gedung dan/atau Bangunan, Rumah Negara, dan Barang Persediaan Yang Mempunyai Dokumen Berita Acara Serah Terima

1. Pengamanan Fisik
   a. Membuatkan surat pernyataan tanggung jawab atas BMN dimaksud dengan keterangan antara lain jenis, tipe, merk, dan nomor seri. Surat pernyataan tanggung jawab ditandatangani oleh Kepala Satuan Kerja (Kuasa Pengguna Barang) dan penanggung jawab BMN.
   b. Menyimpan barang di tempat yang sudah ditentukan di lingkungan kantor serta diberi sistem pengaman lainnya.
   c. Barang dilarang untuk dibawa pulang.
   d. Kehilangan BMN di luar kantor menjadi tanggung jawab pemegang/penanggung jawab BMN.
   e. Jika barang hilang sebagai akibat dari kesalahan dan kelalaian pemegang/penanggung jawab BMN atau penyimpangan dari ketentuan dalam Keputusan Menteri Keuangan ini, maka pemegang/penanggung jawab BMN dikenakan Tuntutan Ganti Rugi yang pemrosesannya dilakukan sesuai dengan ketentuan peraturan perundang-undangan.
2. Pengamanan Administrasi.
   Menghimpun, mencatat, menyimpan, dan menatausahakan secara tertib dan teratur atas dokumen sebagai berikut:
   a. Faktur pembelian.
   b. Dokumen BAST.
   c. Dokumen pendukung terkait lainnya yang diperlukan.
3. Pengamanan Hukum
   a. Melakukan pemrosesan Tuntutan Ganti Rugi yang dikenakan pada pihak-pihak yang bertanggungjawab atas kehilangan barang.
   b. Melakukan upaya hukum yang dapat ditempuh terhadap segala permasalahan pada barang yang kejadiannya dapat dibuktikan bukan sebagai akibat dari kesalahan dan kelalaian pemegang/penanggung jawab BMN atau penyimpangan dari ketentuan dalam Keputusan Menteri Keuangan ini.

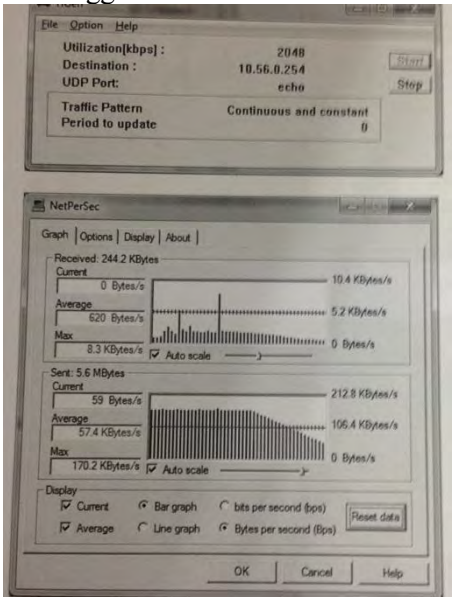
Foto M-125	Foto M-126
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
Bandwith Meter pada TIGen	Strategi dan Metode Pengujian pada span.depkeu.go.id

Foto M-127	Foto M-128
Tanggal validasi : 12 Mei 2014	Tanggal validasi : 12 Mei 2014
	
UU KIP No.14 Tahun 2008	KMK. 138/ KMK.01/2011 CIO

UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR 14 TAHUN 2008

TENTANG

KETERBUKAAN INFORMASI PUBLIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

PRESIDEN REPUBLIK INDONESIA

Menimbang :

a. bahwa informasi merupakan kebutuhan pokok setiap Orang bagi pengembangan pribadi dan lingkungan sosialnya serta merupakan bagian penting bagi ketahanan nasional;
b. bahwa hak memperoleh informasi merupakan hak asasi manusia dan keterbukaan Informasi Publik merupakan salah satu ciri penting negara demokratis yang menjunjung tinggi kedaulatan rakyat untuk mewujudkan penyelenggaraan negara yang baik;
c. bahwa keterbukaan Informasi Publik merupakan sarana dalam mengoptimalkan pengawasan publik terhadap penyelenggaraan negara dan Badan Publik lainnya dan segala sesuatu yang berakibat pada kepentingan publik;
d. bahwa pengelolaan Informasi Publik merupakan salah satu upaya untuk mengembangkan masyarakat informasi;
e. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, huruf c, dan huruf d perlu membentuk Undang-Undang tentang Keterbukaan Informasi Publik.

MENTERI KEUANGAN
REPUBLIK INDONESIA
SALINAN

KEPUTUSAN MENTERI KEUANGAN

NOMOR 138/KMK.01/2011

TENTANG

PENETAPAN *CHIEF INFORMATION OFFICER* KEMENTERIAN KEUANGAN

MENTERI KEUANGAN,

Menimbang :

a. bahwa dalam rangka pelaksanaan tata kelola Teknologi Informasi dan Komunikasi (TIK) di lingkungan Kementerian Keuangan yang efektif, perlu menetapkan *Chief Information Officer* Kementerian Keuangan;
b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Keputusan Menteri Keuangan tentang Penetapan *Chief Information Officer* Kementerian Keuangan;

Mengingat :

1. Keputusan Presiden Nomor 56/P Tahun 2010;
2. Peraturan Menteri Keuangan Nomor 184/PMK.01/2010 tentang Organisasi dan Tata Kerja Kementerian Keuangan;

BIODATA PENULIS

Penulis bernama lengkap Mustaqim Siga yang biasa dipanggil dengan nama Akim dilahirkan di Manado tanggal 2 Maret 1983 merupakan anak bungsu dari 5 (lima) bersaudara.

Penulis menempuh pendidikan formal yaitu di TK Aisyiyah Manado, SDN N 50 Manado, SMP Negeri 3 Manado, dan SMA Negeri 1 Mlati Sleman. Selepas lulus dari SMA, tahun 2002 penulis melanjutkan pendidikan jenjang D3 dengan mengikuti Seleksi Nasional Ujian Saringan Masuk STAN (Sekolah Tinggi Akuntansi Negara) dan diterima di Jurusan Perbendaharaan.

Penulis mengikuti program beasiswa internal DJPBN dan diterima pada Sistem Informasi Fakultas Teknologi Informasi ITS Surabaya pada tahun 2011 dan terdaftar dengan NRP 5211105703. Selain itu, penulis juga aktif dalam kegiatan ekstra kemahasiswaan antara lain ISGC dan ISGD.

Jika ada pertanyaan mengenai tugas akhir ini, penulis dapat dihubungi melalui email mustaqim.siga@gmail.com