TUGAS AKHIR – IT184802

EVALUASI TATA KELOLA KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 DENGAN MENGGUNAKAN MODEL SSE-CMM (*SYSTEM SECURITY ENGINEERING CAPABILITY MATURITY MODEL*) PADA PERUSAHAAN DAERAH AIR MINUM SURYA SEMBADA KOTA SURABAYA

DIMAS PRAMUDYA HAQQI

NRP 05311840000037

Dosen Pembimbing I

Ir. Khakim Ghozali, M.MT

NIP 196403051989031004

Dosen Pembimbing II

Dr.techn. Ir. Raden Venantius Hari Ginardi, M.Sc

NIP 196505181992031003

PROGRAM STUDI SARJANA

DEPARTEMEN TEKNOLOGI INFORMASI

Fakultas Teknologi Elektro dan Informatika Cerdas

Institut Teknologi Sepuluh Nopember

Surabaya

2022

TUGAS AKHIR – IT184802

EVALUASI TATA KELOLA KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 DENGAN MENGGUNAKAN MODEL SSE-CMM (*SYSTEM SECURITY ENGINEERING CAPABILITY MATURITY MODEL*) PADA PERUSAHAAN DAERAH AIR MINUM SURYA SEMBADA KOTA SURABAYA

DIMAS PRAMUDYA HAQQI

NRP 05311840000037

Dosen Pembimbing I

Ir. Khakim Ghozali, M.MT

NIP 196403051989031004

Dosen Pembimbing II

Dr.techn. Ir. Raden Venantius Hari Ginardi, M.Sc

NIP 196505181992031003

PROGRAM STUDI SARJANA

DEPARTEMEN TEKNOLOGI INFORMASI

Fakultas Teknologi Elektro dan Informatika Cerdas

Institut Teknologi Sepuluh Nopember

Surabaya

2022

FINAL PROJECT – IT184802

EVALUATION OF INFORMATION SECURITY GOVERNANCE BASED ON ISO/IEC 27001:2013 STANDARD USING SSE-CMM MODEL (SYSTEM SECURITY ENGINEERING CAPABILITY MATURITY MODEL) AT REGIONAL WATER COMPANY SURYA SEMBADA CITY OF SURABAYA

DIMAS PRAMUDYA HAQQI

NRP 05311840000037

Advisor I

Ir. Khakim Ghozali, M.MT

NIP 196403051989031004

Advisor II

Dr.techn. Ir. Raden Venantius Hari Ginardi, M.Sc

NIP 196505181992031003

STUDY PROGRAM BACHELOR

Department of Information Technology

Faculty of Intelligent Electrical and Informatics Technology

Institut Teknologi Sepuluh Nopember

Surabaya

2022

LEMBAR PENGESAHAN

EVALUASI TATA KELOLA KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 DENGAN MENGGUNAKAN MODEL SSE-CMM (*SYSTEM SECURITY ENGINEERING CAPABILITY MATURITY MODEL*) PADA PERUSAHAAN DAERAH AIR MINUM SURYA SEMBADA KOTA SURABAYA

TUGAS AKHIR

Diajukan untuk memenuhi salah satu syarat
memperoleh gelar Sarjana Komputer pada
Program Studi S-1 Departemen Teknologi Informasi
Fakultas Teknologi Elektro dan Informatika Cerdas
Institut Teknologi Sepuluh Nopember

Oleh : **DIMAS PRAMUDYA HAQQI**
NRP. 05311840000037

Disetujui oleh Tim Penguji Laporan Tugas Akhir:

1. Ir. Khakim Ghozali, M.MT — Pembimbing I

2. Dr.techn. Ir. Raden Venantius Hari Ginardi, M.Sc — Ko-pembimbing

3. Ir. Muchammad Husni, M.Kom — Penguji

4. Annisaa Sri Indrawanti, S. Kom., M. Kom — Penguji

SURABAYA
Juli, 2022

PERNYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini:

Nama mahasiswa / NRP	:	Dimas Pramudya Haqqi / 05311840000037
Program studi	:	S-1 Teknologi Informasi
Dosen Pembimbing I / NIP	:	Ir. Khakim Ghozali, M.MT / 196403051989031004
Dosen Pembimbing II / NIP	:	Dr.techn. Ir. Raden Venantius Hari Ginardi, M.Sc / 196505181992031003

dengan ini menyatakan bahwa Tugas Akhir dengan judul "EVALUASI TATA KELOLA KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 DENGAN MENGGUNAKAN MODEL SSE-CMM (*SYSTEM SECURITY ENGINEERING CAPABILITY MATURITY MODEL*) PADA PERUSAHAAN DAERAH AIR MINUM SURYA SEMBADA KOTA SURABAYA" adalah hasil karya sendiri, bersifat orisinal, dan ditulis dengan mengikuti kaidah penulisan ilmiah.

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan ini, maka saya bersedia menerima sanksi sesuai dengan ketentuan yang berlaku di Institut Teknologi Sepuluh Nopember.

Surabaya, 13 Juli 2022

Mengetahui,

Dosen Pembimbing I,	Dosen Pembimbing II,
Ir. Khakim Ghozali, M.MT	Dr.techn. Ir. Raden Venantius Hari Ginardi, M.Sc
NIP. 196403051989031004	NIP. 196505181992031003

Mahasiswa,

Dimas Pramudya Haqqi

NRP. 05311840000037

ABSTRAK

EVALUASI TATA KELOLA KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 DENGAN MENGGUNAKAN MODEL SSE-CMM (*SYSTEM SECURITY ENGINEERING CAPABILITY MATURITY MODEL*) PADA PERUSAHAAN DAERAH AIR MINUM SURYA SEMBADA KOTA SURABAYA

Nama Mahasiswa / NRP : **Dimas Pramudya Haqqi / 05311840000037**

Departemen : **Teknologi Informasi / FTEIC (ELECTICS) - ITS**

Dosen Pembimbing I : **Ir. Khakim Ghozali, M.MT**

Dosen Pembimbing II : **Dr.techn. Ir. Raden Venantius Hari Ginardi, M.Sc**

Abstrak

Seiring dengan perkembangan teknologi yang semakin pesat dan aktivitas digitalisasi data membuat ancaman terhadap keamanan sistem informasi semakin meningkat pesat. Kinerja tata kelola Teknologi Informasi (TI) akan mengalami berbagai macam gangguan jika informasi sebagai salah satu objek utama mengalami masalah pada keamanan informasi. PDAM Surya Sembada Kota Surabaya salah satu BUMD (Badan Usaha Milik Daerah) yang dimiliki oleh Pemerintah Kota Surabaya. Dalam memberikan pelayanan kepada pelanggan tentunya memerlukan Teknologi Informasi dan Sistem Informasi yang cukup memadai guna mendukung pelayanan prima kepada pelanggan, lebih-lebih di era digitalisasi saat ini. Untuk mengukur sejauh mana kemampuan PDAM Surya Sembada Kota Surabaya dalam hal tata kelola keamanan informasi maka perlu dilakukannya sebuah evaluasi tata kelola keamanan informasi. Tujuan penelitian ini adalah untuk mengetahui tingkat kematangan (*Maturity Level*) keamanan informasi, serta memberikan rekomendasi pada PDAM Surya Sembada Kota Surabaya berdasarkan evaluasi tersebut. Penelitian ini menggunakan metode skala *Systems Security Engineering Capability Maturity Model* (SSE-CMM). Perhitungan *Maturity Level* menggunakan 4 klausul yang telah ditentukan berdasarkan pada ISO/IEC 27001:2013 dan menggunakan skala *Systems Security Engineering Capability Maturity Model* (SSE-CMM). Hasil rata-rata nilai *Maturity Level* dari keseluruhan klausul sebesar 3,5 dan berada dalam *level* tiga yang mana merupakan kategori *Well Defined* artinya kinerja pada *level* ini dilakukan sesuai dengan persetujuan, sesuai dengan standar yang telah ada, dan proses telah didokumentasikan, direncanakan dan dikelola dengan menggunakan standar yang ditetapkan organisasi. Selain itu, penulis menemukan beberapa *gap* antara kondisi sebenarnya dengan standar ISO/IEC 27001:2013 dan telah diberikan rekomendasi. Hasil penelitian ini dapat bermanfaat sebagai bahan pertimbangan untuk memperbaiki *gap* yang ada sesuai dengan standar ISO/IEC 27001:2013. Sehingga kedepannya dapat digunakan sebagai dasar mengambil penilaian dan kebijakan manajemen PDAM Surya Sembada Kota Surabaya dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI) sesuai standar ISO/IEC 27001: 2013.

Kata kunci: ISO/IEC 27001:2013, Keamanan Informasi, Tingkat Kematangan

ABSTRACT

EVALUATION OF INFORMATION SECURITY GOVERNANCE BASED ON ISO/IEC 27001:2013 STANDARD USING SSE-CMM MODEL (SYSTEM SECURITY ENGINEERING CAPABILITY MATURITY MODEL) AT REGIONAL WATER COMPANY SURYA SEMBADA CITY OF SURABAYA

Student Name / NRP : Dimas Pramudya Haqqi / 05311840000037

Department : Information Technology / FTEIC (ELECTICS) - ITS

Advisor I : Ir. Khakim Ghozali, M.MT

Advisor II : Dr.techn. Ir. Raden Venantius Hari Ginardi, M.Sc

Abstract

Along with increasingly rapid technological developments and data digitization activities, threats to security systems are increasing rapidly. The performance of Information Technology (IT) governance will experience various kinds of disturbances if information as one of the main objects experiences problems with information security. PDAM Surya Sembada Surabaya City is one of the Regional Owned Enterprises (BUMD) owned by the Surabaya City Government. In providing services to customers, of course, requires adequate Information Technology and Information Systems to support excellent service to customers, especially in the current digitalization era. To measure the ability of PDAM Surya Sembada Surabaya City in terms of information security governance, it is necessary to seek an evaluation of information security governance. The purpose of this study was to determine the Maturity Level of information security, and to provide recommendations to PDAM Surya Sembada Surabaya City based on this evaluation. This study uses the Systems Security Engineering Capability Maturity Model (SSE-CMM) scale method. The calculation of the Maturity Level uses 4 predetermined clauses based on ISO/IEC 27001:2013 and uses the Systems Security Engineering Capability Maturity Model (SSE-CMM) scale. The average result of the Maturity Level value of the total clause is 3.5 and is in level three which is a Well Defined category. Performance at this level is carried out according to approval, in accordance with existing standards, and the process has been planned, planned and managed properly. using the standards set by the organization. In addition, the authors found several gaps between the actual conditions and the ISO/IEC 27001:2013 standard and have been given recommendations. The results of this study can be useful as consideration for correcting the existing gap in accordance with the ISO/IEC 27001:2013 standard. So that in the future it can be used as a basis for assessment and management policies of PDAM Surya Sembada Surabaya City in the application of Information Security Management System (ISMS) according to ISO/IEC 27001:2013 standards.

Keywords: ISO/IEC 27001:2013, Information Security, Maturity Level

KATA PENGANTAR

Puji syukur penulis panjatkan atas kehadirat Allah S.W.T atas segala berkat dan rahmat-Nya lah penulis dapat menyelesaikan laporan tugas akhir dengan judul "**EVALUASI TATA KELOLA KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 DENGAN MENGGUNAKAN MODEL SSE-CMM (*SYSTEM SECURITY ENGINEERING CAPABILITY MATURITY MODEL*) PADA PERUSAHAAN DAERAH AIR MINUM SURYA SEMBADA KOTA SURABAYA"** yang merupakan salah satu syarat kelulusan di Departemen Teknologi Informasi Informasi, Fakultas Teknologi Elektro dan Informatika Cerdas, Institut Teknologi Sepuluh Nopember Surabaya.

Secara khusus penulis akan menyampaikan ucapan terima kasih yang sedalam-dalamnya kepada:

1. Syukur alhamdulillah kehadirat Allah SWT, atas berkat dan rahmat-Nya penulis dapat menyelesaikan tugas akhir ini dengan semaksimal mungkin.
2. Drs. Sunarno dan Almh. Dra. Erlina Julianti selaku kedua orang tua, dan seluruh keluarga besar yang telah memberikan dukungan serta doa yang tiada henti kepada penulis dalam mengerjakan proposal Tugas Akhir.
3. Bapak Dr.techn. Ir. Raden Venantius Hari Ginardi, M.Sc selaku Kepala Departemen Teknologi Informasi FTEIC ITS yang telah memberi fasilitas selama pengerjaan laporan tugas akhir
4. Bapak Ir. Khakim Ghozali, M.MT dan Bapak Dr.techn. Ir. Raden Venantius Hari Ginardi, M.Sc selaku dosen pembimbing dengan penuh keikhlasan dan dedikasi tinggi telah membimbing penulis dalam mengerjakan laporan tugas akhir ini hingga selesai. Terima kasih atas kesediaan, waktu, semangat dan ilmu yang telah diberikan.
5. Semua teman-teman seperjuangan Departemen Teknologi Informasi ITS Angkatan 2018 yang telah memberi dukungan serta bertukar pikiran dalam mengerjakan laporan tugas akhir
6. Serta semua pihak yang telah membantu dalam pengerjaan Laporan Tugas Akhir ini yang belum mampu penulis sebutkan diatas.

Terima kasih atas segala bantuan, dukungan, serta doa yang diberikan. Semoga Allah SWT senantiasa memberikan kesehatan, keselamatan, karunia dan nikmat-Nya.

Penulis pun ingin memohon maaf karena Penulis menyadari bahwa Laporan Tugas Akhir ini masih belum sempurna dengan segala kekurangan di dalamnya. Selain itu penulis bersedia menerima kritik dan saran terkait dengan Laporan Tugas Akhir ini. Semoga Laporan Tugas Akhir ini dapat bermanfaat bagi seluruh pembaca.

Surabaya, Juli 2022
Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

Pada bab ini berisi mengenai gambaran umum tugas akhir meliputi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat tugas akhir

1.1 Latar Belakang

Pada era sekarang teknologi informasi (TI) sudah merupakan bagian yang memegang peranan penting di dunia industri. Beberapa macam kemudahan diberikan oleh teknologi informasi dalam menyelesaikan berbagai masalah yang dimiliki oleh setiap individu manusia di bidang industri. Namun, di sisi lain untuk membangun sebuah infrastruktur teknologi informasi yang handal memerlukan biaya yang tidak sedikit untuk membangunnya. Teknologi informasi dalam sektor perusahaan publik dan privat, administrasi publik dan bagian lain sangat rentan sekali dari berbagai ancaman siber, seperti misalnya *virus*, serangan *hacking* pada kegagalan sistem. Proses bisnis yang sedang berlangsung menjadi tidak berjalan dengan baik sebagai akibat dari ancaman oleh orang yang tidak bertanggung jawab. Secara periodik, teknologi informasi harus dilindungi agar resiko fungsional yang dimilikinya tidak menjadi rusak. Dalam masa implementasinya, biaya akan sangat diperlukan dan digunakan secara seefisien mungkin agar tidak terjadi pembengkakan biaya. Semuanya juga harus proporsional dan terukur serta dilakukan berdasarkan prediksi resiko-resiko yang mungkin akan terjadi (Bundesamt fur Sicherheit in der Informationstechnik, 2005).

Untuk itu Pentingnya nilai dari sebuah informasi menyebabkan informasi seringkali hanya boleh diakses oleh orang-orang tertentu saja yang sudah memiliki hak akses yang sudah ditentukan oleh administrator. Jatuhnya informasi ke tangan pihak lain yang tidak memiliki hak akses yang telah ditentukan oleh administrator akan menimbulkan dampak yang merugikan bagi pemilik informasi tersebut, oleh karena itu keamanan sistem informasi yang akan digunakan harus terjamin dalam batas yang sudah ditentukan atau batas yang dapat diterima (Bundesamt fur Sicherheit in der Informationstechnik, 2005). Masalah keamanan merupakan salah satu aspek sangat penting dari sebuah penggunaan sistem informasi. Sayang sekali jika permasalahan keamanan ini sering kali terabaikan dan tidak ada perhatian atau bahkan tidak disentuh sama sekali dari para pemilik dan pengelola dari sistem informasi itu sendiri. Dalam hal ini adalah melindungi beberapa *asset* digital yang dimiliki, serangan siber sangat bisa mempengaruhi kinerja bisnis, reputasi, dan kekayaan intelektual pada sebuah perusahaan, khususnya pada area yang berkembang sangat cepat dan membutuhkan evaluasi dan inovasi yang berkelanjutan nantinya. Tujuan serangan siber sendiri tak lebih ialah berkonsentrasi pada elemen manusia sebagai sasaran terlemah dalam postur keamanan *system* jaringan apapun (Torten et al., 2018).

Sehingga perlu dilakukannya sebuah evaluasi tata kelola keamanan informasi (*information security evaluation*). Kesadaran akan pentingnya menjaga keamanan informasi merupakan tahapan dari beberapa *factor* kepatuhan hukum (regulasi) dan penjagaan integritas dari data pengguna (Islami et al., 2016).

Menurut para ahli, Ransbotham dan Mitra mengungkapkan bahwa keamanan informasi harus dijadikan prioritas utama dalam berjalannya sebuah organisasi karena hal tersebut merupakan faktor yang sangat penting dalam menunjang berjalannya keamanan informasi pada suatu organisasi tersebut (ISO, 2013).

Tata kelola keamanan teknologi sebagai sarana sistem informasi, saat ini dapat dikatakan menjadi sebuah tuntutan dan kebutuhan yang harus dimiliki pada setiap instansi dan organisasi, baik itu didalam pemerintahan, industri, perusahaan, seluruh *level* pendidikan, seluruh aspek kesehatan, dan lainnya. Teknologi informasi bisa meningkatkan efisiensi juga

tingkat efektivitas dalam sebuah organisasi untuk menciptakan sebuah layanan yang berkualitas tinggi berdasarkan proses bisnisnya yang dimilikinya. Hambatan dan gangguan yang dapat terjadi untuk sebuah kegiatan aktivitas yang terkait pada *asset* organisasi adalah menjadi risiko apabila terjadinya sebuah gangguan pada keamanan informasi. Informasi yang selama ini dimiliki oleh pihak instansi dan organisasi bisa saja dicuri dan disalahgunakan untuk kepentingan pribadi maupun golongan untuk tindak kejahatan. Kekuatan keamanan informasi dapat dikontrol melalui Sistem Manajemen Keamanan Informasi (SMKI) agar dapat sesuai prosedur. Organisasi dapat menunjukkan bahwa mereka memiliki kontrol internal yang lebih baik dan yang tak kalah lebih penting bahwa mereka dapat membantu mengurangi risiko keamanan informasi dengan beroperasi di bawah satu sistem. Standar ISO/IEC 27001:2013 adalah standar yang diharapkan dapat digunakan untuk membantu terutama pihak manajemen perusahaan untuk merencanakan dan menerapkan keamanan informasi sesuai aturan standar (Ransbotham & Mitra, 2009).

Pemilihan PDAM Surya Sembada Kota Surabaya untuk penelitian ini didasari oleh sebuah kenyataan bahwasannya menurut informasi yang didapat oleh penulis pada sekitar bulan Oktober 2021 telah terjadi *hacking* pada *Data Center* PDAM Surya Sembada yang mengakibatkan sebagian data-data perusahaan hilang sehingga dengan segala daya upaya bagian IT melakukan beberapa langkah *recovery* data, untuk menyelamatkan data-data perusahaan yang telah dicuri oleh *hacker*. Menurut informasi yang telah didapat penulis, bahwa PDAM Surya Sembada Kota Surabaya belum memiliki kebijakan manajemen yang mengatur tentang keamanan informasi. Berangkat dari permasalahan tersebut, hal yang paling penting harus diketahui adalah posisi *level* kematangan PDAM Surya Sembada Kota Surabaya dalam hal keamanan informasi. Salah satu metode penelitian yang akan digunakan untuk melakukan evaluasi tata kelola keamanan informasi PDAM Surya Sembada Kota Surabaya adalah dengan menggunakan metode berdasarkan standar ISO/IEC 27001:2013.

Seperti yang kita ketahui bersama bahwasannya standar ISO/IEC 27001:2013 menyediakan bentuk kerangka kerja, untuk menjaga normalnya kegiatan menggunakan teknologi, sistem manajemen yang dapat memungkinkan perusahaan atau sebuah organisasi memastikan pengukuran tingkat keefektifan dalam keamanan informasi, menyimpan keamanan informasi yang rahasia, melindungi perusahaan dan organisasi, melindungi aset, pertukaran informasi yang aman, serta mengelola dan meminimalisir eksposur terhadap resiko. Keamanan informasi pada standar ISO/IEC 27001:2013 adalah kewajiban setiap instansi yang merupakan kebutuhan organisasi untuk menjaga keamanan informasi.

Tujuan penelitian tugas akhir ini adalah untuk mengetahui tingkat kematangan (*Maturity Level*) keamanan informasi dan menghasilkan sebuah rekomendasi dari hasil evaluasi untuk dasar kebijakan keamanan informasi yang dapat digunakan PDAM Surya Sembada Kota di PDAM Surya Sembada Kota Surabaya sesuai standar ISO/IEC 27001:2013

PDAM Surya Sembada Kota Surabaya merupakan sebuah perusahaan air minum yang dimiliki pemerintah daerah kota Surabaya yang mempunyai fungsi membangun infrastruktur guna meningkatkan kualitas produksi air bagi masyarakat khususnya wilayah Surabaya dan sekitarnya. Sehingga kedepannya dapat digunakan sebagai dasar mengambil penilaian dan kebijakan manajemen PDAM Surya Sembada Kota Surabaya dalam penerapan Sistem Manajemen Keamanan Informasi sesuai standar ISO/IEC 27001: 2013.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan di atas, maka berikut ini merupakan rumusan masalah yang akan diselesaikan pada penelitian ini adalah :

1. Berapa tingkat kematangan (*Maturity Level*) pada keamanan informasi di PDAM Surya Sembada Kota Surabaya?

2. Rekomendasi apa yang dapat diberikan penulis, setelah mengetahui tingkat kematangan (*Maturity Level*) setelah dilakukannya evaluasi tata kelola keamanan informasi di PDAM Surya Sembada Kota Surabaya?

1.3 Batasan Masalah

Berdasarkan rumusan masalah yang telah disebutkan di atas, berikut ini adalah batasan masalah yang diterapkan dalam pengerjaan tugas akhir ini:

1. Evaluasi Tata Kelola Keamanan Informasi pada *Data Center* perusahaan yang dilakukan pada PDAM Surya Sembada Kota Surabaya
2. *Framework* yang digunakan penulis dalam penelitian ini adalah standar ISO/IEC 27001:2013
3. Klausul pada standar ISO/IEC 27001:2013 yang digunakan penulis dalam menyusun penelitian, antara lain:
   a. Klausul A.9 (Kontrol Akses),
   b. Klausul A.11 (Keamanan Fisik dan Lingkungan),
   c. Klausul A.12 (Keamanan Operasi), dan
   d. Klausul A.16 (Manajemen Insiden Keamanan Informasi)
4. Langkah-langkah yang dilakukan untuk melakukan evaluasi tata kelola keamanan informasi dalam penelitian ini, penulis menggunakan metode SSE-CMM (*System Security Engineering Capability Maturity Model*) dengan 5 tingkat kemampuan, untuk mengukur tingkat kematangan (*Maturity Level*) keamanan informasi
5. Sistem Manajemen Keamanan Informasi (SMKI) dengan model *Plan*, *Do*, *Check* dan *Act* (PDCA) yang digunakan dalam penelitian evaluasi tata kelola keamanan informasi ini adalah tahapan *Check* dan *Act*
6. Data acuan yang digunakan oleh penulis dalam menyusun penelitian ini adalah hasil data wawancara dan kuesioner yang dilakukan pada PDAM Surya Sembada Kota Surabaya

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan di atas, maka tujuan yang dicapai dari tugas akhir ini adalah sebagai berikut:

1. Mengetahui tingkat kematangan (*Maturity Level*) keamanan informasi pada *Data Center* yang dimiliki oleh PDAM Surya Sembada Kota Surabaya.
2. Menghasilkan sebuah rekomendasi dari hasil evaluasi yang telah dilakukan, untuk dasar kebijakan keamanan informasi yang dapat digunakan PDAM Surya Sembada Kota Surabaya sesuai dengan standar ISO/IEC 27001:2013 di masa yang akan datang.

1.5 Manfaat Tugas Akhir

Manfaat yang diberikan dari dilaksanakannya penelitian tugas akhir ini adalah sebagai berikut:

1. Membantu mengetahui kondisi terkini pada tingkat kematangan (*Maturity Level*) keamanan informasi yang dimiliki oleh PDAM Surya Sembada Kota Surabaya
2. Menjadi sebuah rekomendasi dari hasil evaluasi yang telah dilakukan untuk kebijakan dan program perencanaan Sistem Manajemen Keamanan Informasi sesuai standar ISO/IEC 27001:2013 di PDAM Surya Sembada Kota Surabaya di masa yang akan datang.

BAB II
TINJAUAN PUSTAKA

Pada bab ini akan membahas mengenai tinjauan pustaka yang digunakan sebagai landasan dalam melakukan penelitian tugas akhir. Bab ini menjelaskan mengenai studi sebelumnya dan dasar teori yang terkait.

2.1 Hasil Penelitian Terdahulu

Dalam penelitian ini, digunakan beberapa penelitian terdahulu sebagai pedoman dan referensi dalam melaksanakan proses-proses dalam pengerjaan tugas akhir, informasi yang disampaikan dalam Tabel 2.1 berisi informasi penelitian sebelumnya, hasil penelitian dan hubungan terhadap tugas akhir.

Tabel 2.1 Studi Sebelumnya

No	Tahun, Penulis	Pembahasan
1	*Implementasi ISO/IEC 27001:2013 Untuk Sistem Manajemen Keamanan Informasi (SMKI) Pada Fakultas Teknik UIKA-Bogor* (Ritzkal et al., 2016)	
	Ritzkal, Arief Goeritno, A. Hendri Hendrawan (2016)	Jurnal ini membahas tentang analisis terhadap sistem manajemen keamanan informasi yang berada pada Fakultas Teknik Universitas Ibn Khaldun (UIKA) Bogor berdasarkan ISO/IEC 27001: 2013 dengan menggunakan Klausal 11, yaitu Kontrol Akses. Standardisasi ISO/IEC 27001:2013, ialah suatu standar berkenaan dengan Sistem Manajemen Keamanan Informasi (SMKI, ISMS: *Information Security Management System*) yang dipublikasikan pada 25 September 2013. Sistem Manajemen Keamanan informasi (SMKI), adalah pendekatan yang sistematis untuk pengelolaan informasi sensitif institusi, agar tetap pada kondisi *safety*. Di dalamnya terdapat orang, proses, dan sistem teknologi informasi melalui penerapan proses manajemen risiko. Analisis terhadap SMKI pada penelitian ini, penulis bertujuan untuk memperoleh taraf keamanan pada jaringan *hotspot* Fakultas Teknik berdasarkan standar tersebut. Dilakukan pembuatan suatu kuesioner menggunakan pendekatan metode *Plan-Do-Check-Act* (PDCA). Pengisian kuesioner ditujukan kepada dua jenis responden, yaitu pengguna serta manajemen. Responden pengguna pengisian kuesioner ini dibatasi pada 20 orang dengan sistem *sampling* dalam pengisian kuesioner, sedangkan manajemen mengarah satu orang pengelola jaringan *hotspot*. Diperoleh hasil, yaitu pengguna hanya mempercayai tingkat keamanan sebesar 49% dan pihak manajemen hanya mempercayai taraf keamanan sebesar 45%. berdasarkan hal itu dapat diambil keputusan, bahwa SMKI pada jaringan *hotspot* di Fakultas Teknik kurang *safety* berdasarkan Standarisasi ISO/IEC 27001:2013 pada penelitian kali ini.
2	*Assessment of ISMS Based On Standard ISO/IEC 27001:2013 at DISKOMINFO Depok City* (Nurbojatmiko et al., 2016)	
	Nurbojatmiko, Aries Susanto,	Jurnal ini membahas tentang penanganan masalah keamanan informasi yang dilakukan sesuai dengan kebutuhan dan sesuai dengan pengetahuan pegawai. Metode perencanaan SMKI dengan

No	Tahun, Penulis	Pembahasan
	Euis Shobariah (2016)	menggunakan PDCA (*Plan-Do-Check-Act*) sesuai dengan standar ISO/IEC 27001:2013:2013. Untuk itu diperlukan suatu penilaian terhadap Sistem Manajemen Keamanan Informasi (SMKI) yang ditujukan kepada Bagian Data dan Informasi pada Dinas Komunikasi dan Informatika Kota Depok (DISKOMINFO Kota Depok) dengan menggunakan beberapa klausul, yaitu: • Klausul 7 (Keamanan Sumber Daya Manusia) • Klausul 8 (Manajemen Aset) • Klausul 9 (Kontrol Akses) • Klausul 11 (Keamanan Fisik & Lingkungan) • Klausul 12 (Keamanan Operasi) • Klausul 16 (Pengelolaan Insiden) Serta didapatkan hasil *Maturity Level* pada setiap klausul, sebagai berikut: • Klausul 7 sebesar 1.25, • Klausul 8 sebesar 1.58, • Klausul 9 sebesar 1.53, • Klausul 11 sebesar 1.30, • Klausul 12 sebesar 1.26, • Dan klausul 16 sebesar 1.20.
3	*Analisis Sistem Manajemen Keamanan Informasi Menggunakan SNI ISO/IEC 27001:2013 Pada Pemerintahan Daerah Kota Sukabumi (Studi Kasus: Di Diskominfo Kota Sukabumi)* (Apriandari & Sasongko, 2018)	
	Winda Apriandari, Ashwin Sasongko (2018)	Jurnal ini membahas tentang kendala dalam mengelola keamanan data, antara lain karena kurangnya Sumber Daya Manusia, kurangnya kesadaran dan tanggung jawab serta penerapan keamanan informasi yang buruk sehingga menyebabkan insiden atau peretasan keamanan informasi khususnya di Sistem Informasi Kota Sukabumi. hal ini menyebabkan terganggunya proses pelayanan publik dan bisnis di DISKOMINFO. Sistem Manajemen Keamanan Informasi (SMKI) adalah sistem manajemen yang diterapkan oleh organisasi, terutama organisasi pemerintah, untuk mengamankan aset informasi dari ancaman yang ada dalam lingkup DISKOMINFO. Proses yang dilakukan menggunakan pendekatan siklus PDCA antara lain *Plan Do Check Act*. SMKI menangani aspek informasi seperti kerahasiaan, integritas, dan ketersediaan informasi. Analisis SMKI menggunakan basis manajemen risiko SNI ISO/IEC 27001:2013 dan SNI ISO/IEC 31000:2009. Analisis SMKI bertujuan untuk mengidentifikasi profil risiko dengan mengidentifikasi aset, ancaman, dan kerentanan serta mengevaluasi dan mengendalikan gangguan. SMKI menghasilkan manual keamanan informasi, prosedur keamanan informasi, instruksi kerja dan formulir keamanan informasi.

No	Tahun, Penulis	Pembahasan
4	*Audit Keamanan Sistem Informasi Berdasarkan Standar SNI-ISO/IEC 27001:2013 Pada Sistem Informasi Akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta* (Kusuma, 2014)	
	Riawan Arby Kusuma (2014)	Jurnal ini membahas tentang pengukuran kinerja sistem manajemen keamanan informasi dengan menggunakan standar SNI-ISO/IEC 27001:2013, pengukuran dengan menggunakan *Maturity Model* bertujuan untuk melihat representasi dari kondisi saat ini. Dari penelitian ini, dapat disimpulkan bahwa tingkat keamanan dari SIA UIN Sunan Kalijaga Yogyakarta tentang keamanan informasi memiliki skala kematangan dengan model skala 2 (*Repeatable but Intuitive*). Hal ini menunjukkan bahwa keamanan yang terkandung dalam SIA UIN Sunan Kalijaga telah dibakukan tetapi tidak ter dokumentasikan. Semua keamanan informasi yang berada pada SIA UIN Sunan Kalijaga Yogyakarta dilengkapi dengan sejumlah prosedur yang harus dijalankan oleh individu yang memiliki tugas bersama. UPT PTIPD selaku pengelola SIA UIN Sunan Kalijaga Yogyakarta belum mengadakan program pelatihan formal, yang memiliki tujuan untuk mengkomunikasikan prosedur dan tanggung jawab dari masing-masing individu.
5	*Audit Keamanan Sistem Informasi Berdasarkan SNI – ISO/IEC 27001:2013 Pada Sistem Informasi Akademik Universitas Pembangunan Nasional "Veteran" Jakarta* (Putra et al., 2020)	
	Darma Yanto Putra, Theresia Wati, I Wayan Widi (2020)	Jurnal ini membahas terjadinya kerusakan pada aset sistem informasi, tidak memiliki kebijakan tentang keamanan informasi yang memiliki keharusan diterapkan didalam keamanan juga pengawasan aset pelayanan informasi akademik, juga kemungkinan ancaman dan risiko terhadap dukungan sistem informasi. Penelitian ini memiliki tujuan untuk perencanaan Sistem Manajemen Keamanan Informasi (SMKI) dimana penggunaannya sebagai pedoman terhadap kebijakan keamanan informasi di UPT TIK UPN "Veteran" Jakarta. Bahasan dalam penelitian ini adalah analisis Sistem Manajemen Keamanan Informasi (SMKI) dengan ISO/IEC 27001 pada sistem informasi akademik UPT TIK UPN "Veteran" Jakarta. Penelitian ini menggunakan metode *Plan*, *Do*, *Check*, dan *Act* dalam kegiatan mengumpulkan, menganalisis, dan mengolah data. Hasil penelitian ini adalah tingkat kematangan ISO/IEC 27001:2013 dengan rata – rata berada di *level* dua, diharapkan penelitian ini sangat membantu memberikan rekomendasi terhadap kontrol keamanan informasi sebagai pedoman dan prosedur untuk menerapkan kebijakan keamanan informasi.

2.2 Dasar Teori

Berikut ini merupakan dasar teori yang digunakan dalam penelitian tugas akhir.

2.2.1 Data dan Informasi

Data merupakan fakta dan angka yang relatif tidak ada artinya bagi para penggunanya (McLeod & Schell, 2008). Definisi lain dari data adalah merupakan sebuah fakta mengenai peristiwa atau sebuah kenyataan lain yang mendukung pengetahuan untuk dijadikan dasaran

guna menyusun suatu keterangan, dalam pembuatan kesimpulan akhir dari suatu peristiwa dan kenyataan atau penetapan keputusan yang akan di ambil nantinya (Gondodiyoto & Hendarti, 2007). Dari dua definisi tersebut dapat di ambil kesimpulan bahwasannya sebuah data merupakan hasil observasi dalam bentuk fakta-fakta atau angka-angka yang relatif tidak ada artinya bagi penggunanya, akan tetapi dapat tergarap melalui proses-proses tertentu untuk menjadi sebuah pemahaman yang lebih bermanfaat bagi pemakainya. Sedangkan informasi merupakan adalah data yang telah diproses, atau data yang memiliki arti (McLeod & Schell, 2008). Definisi lain menyatakan bahwa informasi adalah sebuah hasil pengolahan dari data sehingga menambah kegunaan dan dapat dipakai untuk tujuan tertentu atau untuk penjabaran dan pengambilan keputusan nantinya (Gondodiyoto & Hendarti, 2007). Dari dua definisi informasi tersebut dapat di ambil kesimpulan bahwa informasi ialah hasil dari pemrosesan data berupa fakta-fakta atau angka-angka yang bermanfaat bagi penggunanya dalam melakukan suatu penjabaran dan dasar dalam pengambilan suatu keputusan nantinya.

2.2.2 Evaluasi

Definisi evaluasi dapat dijabarkan dengan secara bahasa ataupun secara harfiah. Definisi secara bahasa, kata evaluasi berasal dari kata bahasa inggris yaitu "*evaluation*" yang memiliki arti penaksiran atau penilaian. Sedangkan definisi secara harfiah, evaluasi adalah proses untuk menentukan nilai suatu hal atau objek beracuan tertentu untuk dapat menggapai tujuan tertentu. Evaluasi adalah sebuah kegiatan untuk menghimpun informasi mengenai tentang kinerja sesuatu (metode, manusia, peralatan), informasi tersebut akan dipergunakan dalam menentukan alternatif terbaik dalam membuat keputusan (Pengertian Ahli, n.d.).

Tahapan evaluasi dilaksanakan untuk mengukur seberapa besar usaha yang telah dilakukan dan untuk dapat menjadi bahan perbaikan pada usaha selanjutnya. Menurut KBBI, evaluasi memiliki arti penilaian atau memberikan penilaian (Kamus Besar Bahasa Indonesia (KBBI), n.d.). Sedangkan dalam kamus Oxford, evaluasi memiliki arti sebuah pembuatan keputusan tentang jumlah, angka/bilangan, atau nilai sesuatu (English Oxford Living Dictionary, n.d.).

Terdapat beberapa tahapan yang harus kita lewati pada saat waktu menjalankan proses evaluasi. Setiap proses evaluasi dimungkinkan mempunyai tahapan-tahapan yang berbeda, tetapi ada tahapan penting yang memiliki sifat umum dan sering digunakan dalam melakukan sebuah proses evaluasi (Umar, 2005). Tahapan tersebut antara lain :

1. Menetapkan apa saja yang akan dievaluasi, hal tersebut mengacu pada program kerja instansi/perusahaan.
2. Mendesain kegiatan evaluasi, sebelum melaksanakan evaluasi dilakukan desain evaluasi. Yaitu mendesain data apa saja yang dibutuhkan, tahapan kerja yang dilalui, siapa yang dilibatkan, apa yang akan dihasilkan agar menjadi jelas.
3. Menghimpun data, penghimpunan data dapat dilaksanakan berdasarkan dengan kaidah-kaidah ilmiah yang berlaku dan sesuai dengan kebutuhan & kemampuan.
4. Mengolah dan menganalisis data, data yang terkumpul diolah dan dikelompokkan lalu dianalisis dan menghasilkan fakta terpecaya. Fakta kemudian akan dibandingkan dengan harapan untuk menghasilkan *gap*.
5. Pelaporan hasil evaluasi, pemanfaatan evaluasi bagi pihak-pihak berkepentingan.

2.2.3 Keamanan Informasi

Keamanan informasi memberikan perlindungan terhadap informasi dari 3 aspek keamanan informasi, yaitu *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan), dan juga memberikan perlindungan terhadap sistem serta perangkat keras yang digunakan untuk menyimpan atau mentransmisi informasi tersebut melalui penerapan kebijakan, program pelatihan dan penyadaran serta teknologi (Whitman & Mattord, 2014). Keamanan informasi memiliki sebuah definisi yang artinya perlindungan aset organisasi (mis.,

Informasi) dari pengungkapan yang tidak sah dan modifikasi yang tidak sah dan tidak disengaja, dan memastikan informasi tersebut siap digunakan saat diperlukan (Arnason & Willet, 2008).

Adapun jenis keamanan informasi dapat dibagi menjadi beberapa bagian sebagai berikut (Whitman & Mattord, 2014)

1. *Physical Security* (Keamanan Fisik)
   Physical Security memiliki fokus untuk memberikan perlindungan kepada karyawan atau *staff* organisasi, aset fisik, ataupun tempat kerja apabila sedang terjadi sesuatu yang dapat mengancam seperti insiden kebakaran, adanya akses tanpa otorisasi / tidak sah atau akses ilegal, dan bencana alam lainnya yang tidak dapat terduga
2. *Operational Security*
   Operational Security berfokus untuk memberi perlindungan kepada gangguan yang mungkin akan mengganggu organisasi dalam melaksanakan kegiatan operasional.
3. *Communications Security*
   Communications Security berfokus untuk memberi perlindungan kepada perusahaan dalam menggunakan media komunikasi, teknologi komunikasi, serta konten yang ada di dalamnya untuk mencapai tujuan dalam sebuah organisasi.
4. *Network Security*
   Network Security berfokus untuk memberikan perlindungan kepada perusahaan dalam menggunakan jaringan yang terdiri atas perangkat jaringan, koneksi dan konten yang tersedia pada jaringan untuk mencapai fungsi komunikasi data organisasi tersebut.

2.2.4 Tujuan Keamanan Informasi

Tiap-tiap organisasi atau perusahaan mengenakan sistem informasi berbasis komputer guna meraih tujuan tertentu. Oleh karenanya perusahaan dituntut untuk membuat sistem keamanan untuk mengamankan aset yang dimilikinya yakni berupa *hardware* dan *software* dari sistem informasi tersebut. Memiliki tujuan untuk meyakinkan kerahasiaan, ketersediaan, dan integritas dari pengolahan data. Biaya yang akan dikeluarkan oleh perusahaan untuk melakukan pengamanan terhadap sistem komputer tentunya harus wajar jika mempunyai keinginan untuk meminimalkan seminimal mungkin dari risiko-risiko dan memelihara keamanan sistem komputerisasi di suatu tingkat atau *level* yang dapat diterima. Karenanya masyarakat akan menilai reputasi organisasi dari tiga aspek diatas yakni integritas, kerahasiaan, dan ketersediaan informasi (IBISA, 2011).

Implementasi upaya operasional dan didukung oleh prosedur dan kebijakan yang baik dapat diperoleh dari keamanan informasi. Prosesnya diawali dengan pengidentifikasian kontrol yang akan dipakai dalam organisasi yang dimana kontrol tersebut harus beralaskan analisis kebutuhan aspek keamanan informasi dalam organisasi. Selanjutnya setelah prosedur, kebijakan dan panduan operasional tentang kontrol yang diterapkan dalam organisasi dibuat, berikutnya akan dilakukan sosialisasi kepada seluruh bagian organisasi guna meraih dukungan dan komitmen dari seluruh elemen dalam organisasi (Sarno & Iffano, 2009).

2.2.5 Aspek Keamanan Informasi

Aspek keamanan informasi dari organisasi memiliki keharusan untuk dikontrol, diperhatikan dan di implementasi. Untuk memenuhi semua aspek keamanan informasi dilakukan dengan bertujuan untuk memberikan perlindungan pada informasi. Aspek-aspek yang berkaitan dengan *user* pada keamanan informasi, yakni sebagai berikut (Sarno & Iffano, 2009):

1. *Privacy*
   Beberapa informasi yang berada di dalam organisasi hanya dipergunakan oleh pihak yang memiliki tujuan tertentu khususnya bagi pemilik data. Aspek keamanan informasi yaitu *privacy* dapat menjamin keamanan data dari pihak lain yang tidak memiliki kepentingan untuk mengaksesnya.

2. *Identification*
   Aspek keamanan informasi salah satunya adalah *identification* dapat memberi jaminan bahwasannya sebuah informasi mempunyai karakteristik untuk mengidentifikasi jika suatu informasi bisa mengenali pemiliknya. Aspek *identification* ini adalah awalan dalam mendapatkan hak akses ke dalam informasi yang diamankan.
3. *Authentication*
   Autentikasi dalam halnya aspek keamanan informasi dapat terjadi waktu sistem membuktikan bahwasannya yang memakai dan menggunakan sebuah informasi tersebut memang benar pemilik yang memiliki identitas yang sesuai dengan yang di klaim oleh pemilik aslinya yang sesuai dengan identitasnya.
4. *Authorization*
   Aspek *Authorization* adalah aspek yang tersedia setelah identitas pengguna sudah melakukan auntentikasi, lalu kemudian terjadi sebuah proses autorisasi yang menyediakan jaminan pemakainya dalam halnya adalah manusia ataupun komputer. Jika telah mendapatkan autorisasi maka pengguna dapat mengakses, mengubah, atau menghapus isi informasi.
5. *Accountability*
   Aspek *Accountability* dapat terpenuhi apabila sebuah sistem dapat menunjukkan data kegiatan pada informasi yang telah dilakukan dan oleh siapa saja yang melakukan kegiatan tersebut.

Keamanan informasi juga mempunyai tiga pilar untuk mendukungnya, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*), tujuan keamanan informasi juga merupakan kerahasiaan, integritas dan ketersediaan. Tiga pilar pendukung tersebut dapat dikenal juga sebagai pilar CIA dalam keamanan informasi.

Macam-macam pilar keamanan informasi adalah sebagai berikut (Whitman & Mattord, 2014):

1. Pilar Kerahasiaan (*confidentiality*) adalah karakteristik informasi khusus mereka yang mempunyai hak istimewa yang dapat tercukupi dan kebutuhan yang ditunjukkan dapat mengaksesnya. Bahwa hanya personil yang berwenang yang dapat mengakses informasi, pihak lain tidak dapat mengaksesnya yang dapat memastikan kerahasiaannya.
2. Pilar Integritas (*Integrity*) adalah keadaan menjadi utuh, lengkap, dan tidak rusak. Integritas sebuah informasi mendapatkan ancaman apabila terpapar korupsi, kerusakan, kehancuran, atau gangguan lainnya dari negara asal. Pilar keamanan informasi yakni integritas menjadikan informasi tetap dalam format pencipta informasi yang dimaksud. Karena informasi menjadi bernilai sedikit atau tidak bernilai jika integritasnya tidak dapat diverifikasi. Pilar Integritas informasi adalah landasan dalam sebuah keamanan informasi.
3. Pilar Ketersediaan (*availability*) dalam keamanan informasi terjadi pada saat pengguna mempunyai akses ke format yang dapat dipergunakan, tanpa adanya gangguan atau hambatan-hambatan. Ketersediaan tidak dapat menggambarkan bahwasannya informasi tersebut dapat diakses pada pengguna mana pun, tetapi dapat diakses pada pengguna yang memiliki kewenangan. Pilar ketersediaan (*availability*) dalam keamanan informasi ini memastikan informasi telah siap dipakai. Hilangnya ketersediaan pada keamanan informasi dapat menyebabkan gangguan akses atau penggunaan informasi atau teknologi informasi.

2.2.6 *Framework* Keamanan Tata Kelola TI

Alfantookh (2009) (Alfantookh, 2009) dalam Susanto (2011) (Susanto, 2011) mengartikan bahwasannya tersedia 11 kontrol penting tata kelola keamanan teknologi informasi yang harus diterapkan oleh sebuah organisasi dalam melakukan pengukuran atau

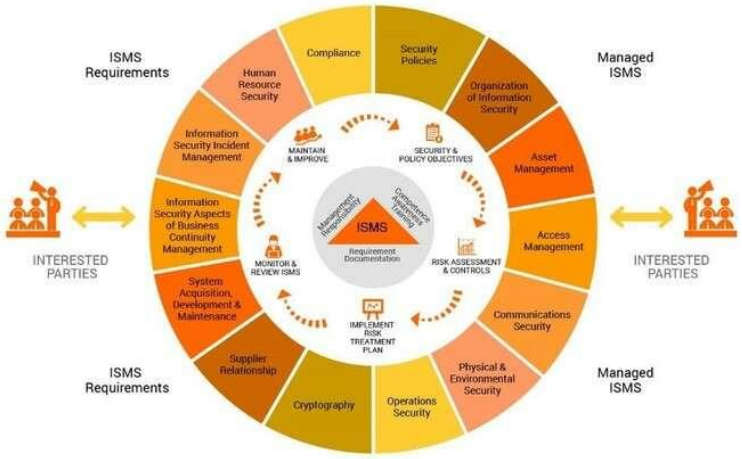
evaluasi. Adapun 11 kontrol penting dalam tata Kelola keamanan teknologi informasi adalah sebagai berikut :

1. *Information Security Policy*
   Sebagaimana sebuah organisasi dalam melakukan keamanan informasi, dengan cara memberikan pernyataan yang memiliki niatan untuk mengamankan informasi, memberikan arahan pada manajemen, staf maupun pemangku saham untuk membahas pentingnya sebuah keamanan informasi dalam organisasi.
2. *Communication & Operations Management*
   Sebagaimana sebuah organisasi bisa menentukan suatu kebijakan keamanan informasi yang dapat mengurangi risiko keamanan dan memvalidasi perhitungan yang benar dalam halnya prosedur operasional, kontrol, dan tanggung jawab yang telah ditetapkan dengan baik.
3. *Access Control*
   Access control mempunyai definisi sebagai sistem yang dimungkinkan mendapatkan otoritas dalam organisasi untuk dapat mengontrol akses ke area dan sumber daya dalam fasilitas fisik tertentu atau sistem informasi berbasis komputer.
4. *Information System Acquisition, Development and Maintenance*
   Sebuah proses yang terintegrasi dapat menunjukkan batas-batas dan sistem informasi teknis, diawali dengan akuisisi, mengembangkan dan memelihara sistem informasi.
5. *Organization of Information Security*
   Organization of Information Security dapat diartikan sebagai struktur yang dimiliki organisasi dalam menerapkan keamanan informasi yang terdiri atas komitmen manajemen terhadap keamanan informasi, koordinasi keamanan informasi, proses otorisasi untuk fasilitas pemrosesan informasi.
6. *Asset Management*
   Sebagaimana sebuah organisasi dapat melakukan pengamanan pada asetnya dengan cara melakukan pengidentifikasian, melacak, mengelompokkan, dan ketetapan kepemilikan untuk aset yang paling penting dalam sebuah organisasi.
7. *Information Security Incident Management*
   Suatu kegiatan untuk melakukan antisipasi terhadap insiden yang dimungkinkan dapat terjadi. Kegiatan ini melibatkan suatu pengidentifikasian kepada sumber daya yang dibutuhkan untuk menangani insiden yang dapat terjadi. Dalam manajemen insiden yang baik juga dapat akan membantu dengan melakukan pencegahan terhadap insiden di masa depan.
8. *Business Continuity Incident Management*
   Suatu organisasi dapat memastikan keberlangsungan operasional dalam situasi abnormal atau yang tidak semestinya terjadi. Memastikan ketersiapan sebuah organisasi untuk memulihkan jika terjadi sebuah peristiwa yang dapat merugikan, meminimalisir dampak yang dapat terjadi, dan menyediakan sarana saat keadaan darurat terjadi.
9. *Human Resources Security*
   Human Resources Security dapat memastikan bahwasannya seluruh karyawan telah memenuhi syarat-syarat serta dapat paham atas peran dan tanggung jawab dalam pekerjaan yang mereka ampu, dan akses yang diberikan dihapus saat pekerjaan telah selesai.
10. *Physical and Environment Security*
    Langkah-langkah yang diambil untuk melindungi sistem, bangunan, dan infrastruktur pendukung terkait terhadap ancaman yang terkait dengan lingkungan fisik, bangunan termasuk ruangan yang menampung sistem informasi dan teknologi informasi.

11. *Compliance*

    Compliance terbagi menjadi dua area, yaitu area yang pertama melibatkan kepatuhan terhadap undang-undang, peraturan, dan persyaratan kontrak. Sedangkan untuk area kedua adalah kepatuhan terhadap kebijakan, standar, dan proses keamanan.

2.2.7 ISO/IEC 27001 & ISO/IEC 27001:2013



Gambar 2.1 ISO/IEC 27001 (*ECC International*)
Diakses dari: **Error! Hyperlink reference not valid.** information-security-management-*system* (ECC International, n.d.)

ISO/IEC 27001 adalah salah satu seri yang diterbitkan oleh *The International Organization for Standarization* yang dalamnya berisi tentang spesifikasi atau syarat yang harus dipenuhi untuk membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini memiliki sifat independen kepada produk teknologi informasi, mensyaratkan penggunaan melakukan pendekatan yang berbasis manajemen risiko, serta dibentuk untuk dapat melakukan penjaminan terhadap kontrol keamanan yang telah dipilih perusahaan dapat melindungi aset informasi dari berbagai macam risiko dan memberikan keyakinan terhadap tingkat keamanan bagi pihak yang berkepentingan (Direktorat Keamanan Informasi, 2017).

Menurut Arnason & Willet (2008) selain memberikan panduan untuk diterapkannya Sistem Manajemen Keamanan Informasi (SMKI), ISO/IEC 27001:2013 juga dipergunakan oleh perusahaan dalam meraih sertifikat internasional pihak ketiga untuk pembuktian bahwasannya kontrol keamanan yang telah beroperasi di perusahaan telah terstandarisasi dengan persyaratan standar yang ada (Arnason & Willet, 2008). ISO/IEC 27001:2013 memberikan suatu gambaran terhadap Sistem Manajemen Keamanan Informasi dengan menggunakan suatu pendekatan risiko bisnis untuk dapat menetapkan, menerapkan, mengoperasikan, memantau serta memelihara SMKI tersebut (Arnason & Willet, 2008).

ISO/IEC 27001:2013 mempunyai arahan terhadap tentang bagaimana cara membangun sebuah sistem manajemen yang menetapkan disiplin dalam cara menunjuk sebuah kontrol dan cara untuk menetapkan praktik yang sebaiknya dapat diterapkan dalam kontrol keamanan. Tata cara untuk mengimplementasi kontrol keamanan juga menyesuaikan terhadap kondisi sebuah organisasi entah dari segi lingkungan fisik maupun dari segi teknis. Ini bertujuan untuk membangun sebuah kesadaran keamanan, membangun infrastruktur sebuah organisasi, serta melakukan perencanaan, penerapan dan pemeliharaan terhadap kontrol keamanan (Arnason & Willet, 2008).

ISO/IEC 27001:2013 adalah standar versi yang paling baru dari standar ISO seri 27001 yang dirilis oleh *The International Organization for Standarization* pada waktu tahun 2013.

Standar ISO/IEC 27001:2013 ini menyediakan persyaratan-persyaratan yang dapat dipergunakan untuk menetapkan, mengimplementasi, mempertahankan serta terus meningkatkan sistem manajemen keamanan informasi (SMKI) di suatu organisasi. Pengangkatan sebuah sistem manajemen keamanan informasi ini merupakan keputusan yang sangat strategis oleh organisasi yang tentunya telah berdasarkan oleh adanya kebutuhan dan tujuan organisasi, persyaratan keamanan, dan struktur organisasi yang tentunya akan dapat berubah seiring mengikuti perkembangan waktu. Dalam Sistem manajemen keamanan informasi tersebut juga menjaga 3 aspek keamanan informasi yakni *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan) pada informasi dengan diterapkannya proses manajemen risiko untuk memberi kepercayaan kepada para *stakeholder* perusahaan bahwasannya risiko telah dilakukan pengelolaan secara baik dan benar. Standar Internasional ini dipergunakan oleh pihak internal, serta eksternal perusahaan untuk melaksanakan penilaian kepada kemampuan organisasi untuk memenuhi persyaratan keamanan informasi sebuah organisasi itu sendiri (ISO, 2013).

2.2.8 Klausul ISO/IEC 27001:2013

Pada standar ISO/IEC 27001:2013 mempunyai 14 klausul, 35 objektif kontrol dan 144 kontrol keamanan. Tabel 2.2. adalah tabel penjelasan dari klausul obyektif kontrol dan kontrol keamanan yang terdapat dalam standar ISO/IEC 27001:2013

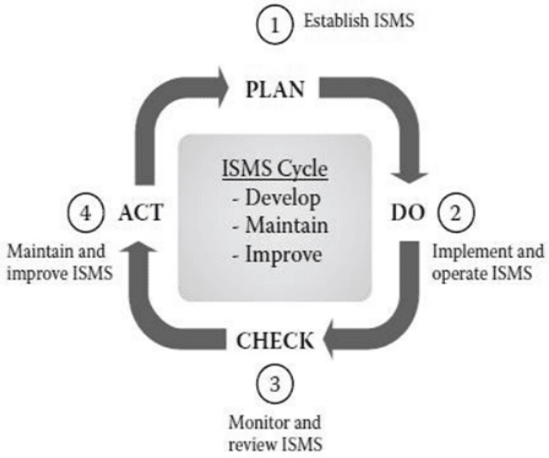
Tabel 2.2 Klausul ISO/IEC 27001:2013 (ISO, 2013)

Klausul	Objektif Kontrol
A.5. Kebijakan Keamanan Informasi	A.5.1 Arahan Manajemen Untuk Keamanan Informasi
A.6. Organisasi Keamanan Informasi	A.6.1 Organisasi Internal
	A.6.2 Perangkat Seluler Dan *Teleworking*
A.7. Keamanan Sumber Daya Manusia	A.7.1 Sebelum Bekerja
	A.7.2 Selama Bekerja
	A.7.3 Pemutusan Hubungan Kerja Dan Perubahan Pekerjaan
A.8. Manajemen Aset	A.8.1 Tanggung Jawab Untuk Aset
	A.8.2 Klasifikasi Informasi
	A.8.3 Penanganan Media
A.9. Kontrol Akses	A.9.1 Persyaratan Bisnis Terhadap Kontrol Akses
	A.9.2 Manajemen Akses *User*
	A.9.3 Tanggung Jawab Pengguna
	A.9.4 Kontrol Akses Sistem Dan Aplikasi
A.10. Kriptografi	A.10.1 Kontrol Kriptografi
A.11. Keamanan Fisik Dan Lingkungan	A.11.1 Area Aman
	A.11.2 Peralatan
A.12. Keamanan Operasi	A.12.1 Prosedur Dan Tanggung Jawab Operasional
	A.12.2 Perlindungan Dari *Malware*
	A.12.3 *Backup*
	A.12.4 Pencatatan Dan Pemantauan
	A.12.5 Kontrol Perangkat Lunak Operasional
	A.12.6 Pengelolaan Kerentanan Teknis
	A.12.7 Pertimbangan Audit Sistem Informasi
A.13.	A.13.1 Manajemen Keamanan Jaringan

Klausul	Objektif Kontrol
Keamanan Komunikasi	A.13.2 Transfer Informasi
A.14. Akuisisi Sistem, Pengembangan, Dan Pemeliharaan	A.14.1 Persyaratan Keamanan Sistem Informasi
	A.14.2 Keamanan Dalam Proses Pengembangan Dan Dukungan
	A.14.3 Uji Data
A.15. Hubungan Pemasok	A.15.1 Keamanan Informasi Dalam Hubungan Pemasok
	A.15.2 Manajemen Pengiriman Layanan Pemasok
A.16. Manajemen Insiden Keamanan Informasi	A.16.1 Manajemen Insiden Keamanan Informasi Dan Perbaikan

2.2.9 Model PDCA (*Plan-Do-Check-Act*)

Model ini merupakan model yang dipergunakan dalam penerapan sistem manajemen keamanan informasi atau dapat disebut juga sebagai siklus SMKI. Model PDCA dirancang untuk mendorong perbaikan yang berkelanjutan. Dan menerapkan SMKI sebagaimana yang telah ditentukan dalam standar ISO/IEC 27001:2013, sebuah organisasi dapat menggunakan model PDCA (Arnason & Willet, 2008). Di bawah ini adalah gambar yang menunjukkan siklus PDCA



Gambar 2.2 Siklus PDCA (ISO, 2013)

Dalam proses siklusnya, organisasi dapat menetapkan sebuah ruang lingkup SMKI, pengumpulan rincian-rincian aset dalam ruang lingkup SMKI, melaksanakan sebuah penilaian risiko kepada fungsi bisnis dan aset dalam halnya yakni ruang lingkup SMKI, dan melakukan penilaian kepada kontrol keamanan dari ISO/IEC 27001:2013 (Arnason & Willet, 2008).

Penjelasan model PDCA yang diimplementasikan pada proses SMKI akan dijabarkan sebagai berikut (Sarno & Iffano, 2009):

1. *Plan*

   Tahapan *plan* ini merupakan tahap yang dilaksanakan untuk membuat perencanaan serta merancang sebuah sistem manajemen keamanan informasi (SMKI) di suatu perusahaan. Supaya penerapan SMKI telah sesuai dengan keinginan atau kebutuhan suatu perusahaan ada beberapa tahapan yang harus dilewati yakni: membangun komitmen, kebijakan, kontrol, prosedur, serta instruksi kerja. Pada tahapan ini komitmen manajemen sangat dibutuhkan untuk melakukan perencanaan sistem manajemen sistem manajemen

keamanan informasi yang telah sesuai dengan keinginan. Oleh karena itu, manajemen juga harus memiliki keterlibatan yang aktif dalam memberi masukan, dan dalam meninjau dan menyetujui semua dokumen kebijakan (Williams, 2013).

2. *Do*
   Tahap tersebut berisikan kegiatan untuk melakukan penerapan dan pengoperasian dari kebijakan, kontrol, proses dan prosedur sistem manajemen keamanan informasi (SMKI) yang telah terencana pada tahap plan sebelumnya.
3. *Check*
   Tahap ini adalah tahap untuk memantau pelaksanaan SMKI melalui kegiatan audit atau evaluasi terhadap SMKI. Tahap ini dilaksanakan untuk mengetahui apakah SMKI yang diterapkan telah sesuai dengan keinginan perusahaan dan untuk mencari solusi untuk perbaikan jika kinerja SMKI yang berada pada saat ini kurang sesuai dengan keinginan perusahaan
4. *Act*
   Tahap ini merupakan kegiatan yang dilakukan untuk melakukan perbaikan serta mengembangkan dari SMKI berdasarkan hasil audit atau evaluasi yang ada pada tahap *check* sebelumnya. Hal tersebut juga dapat diartikan sebagai perbaikan berkelanjutan yang seharusnya dilakukan terhadap SMKI untuk menyesuaikan dengan standarisasi prosedur yang baru.

Berdasarkan penjelasan tersebut diatas, maka untuk evaluasi keamanan informasi dapat menggunakan tahapan *check* dan *act*.

2.2.10 *Systems Security Engineering Capability Maturity Model* (SSE-CMM)

SSE-CMM adalah gambaran referensi proses yang memiliki fokus pada persyaratan guna mengimplementasikan keamanan dalam serangkaian sistem terkait yang merupakan domain keamanan teknologi informasi. SSE-CMM mempromosikan integrasi tersebut, mengambil pandangan bahwa keamanan tersebar di semua ilmu teknik. Model ini pertama kali dikembangkan oleh Carnegie Mellon University pada tahun 1995. Saat ini versi SSE-CMM yang terbaru adalah Versi 3 yang dirilis pada tahun 2003 (CMU, 2003). Tujuan Carnegie Mellon University mengembangkan SSE-CMM ini adalah untuk memajukan rekayasa keamanan yang terdefinisi, matang, dan terukur. SSE-CMM dikembangkan untuk memajukan praktik-praktik keamanan dengan tujuan meningkatkan kualitas dan ketersediaan dan mengurangi biaya pengiriman sistem yang aman, produk terpercaya, dan layanan rekayasa keamanan.

2.2.11 *Level Capability* SSE-CMM *(Systems Security Engineering Capability Maturity Model)*

Menurut Sarno & Iffano (2009) penilaian harus dilakukan untuk menentukan tingkat kemampuan masing-masing daerah proses. Hal ini menunjukkan bahwa area proses yang berbeda dapat dan mungkin akan ada pada berbagai tingkat kemampuan. Organisasi kemudian akan dapat menggunakan informasi-informasi tertentu ini sebagai sarana untuk fokus perbaikan prosesnya. Prioritas dan urutan kegiatan organisasi untuk meningkatkan proses yang harus memperhitungkan tujuan bisnisnya (Sarno & Iffano, 2009).

Tujuan bisnis adalah pendorong utama dalam menafsirkan model seperti SSE-CMM. Tapi, ada urutan dasar kegiatan dan prinsip- prinsip dasar yang mendorong urutan logis dari upaya perbaikan yang khas. Agar kegiatan ini dinyatakan dalam fitur-fitur umum dan praktik generik sisi tingkat kemampuan arsitektur SSE-CMM (Sarno & Iffano, 2009).

Level capability SSE-CMM (*System Security Enginering Capability Maturity Model*) memiliki 5 tingkat dalam SSE-CMM yaitu (CMU, 2013):

1. *Level* 1 "*Performed Informally*"
   Level 1 yaitu sebuah praktek dasar yang pada umumnya wajib dikerjakan. Kinerja praktek dasar ini belum sepenuhnya terencana dan dilacak. Performa dapat tergantung pada pengetahuan individu dan organisasi. Hasil performa dari *level* ini menghasilkan untuk kinerja organisasi. Hasil dari kinerja diidentifikasi untuk proses selanjutnya.
2. *Level* 2 "*Planned and Tracked*"
   Pada tingkat 2 "*Planned and Tracked*", kinerja sesuai prosedur yang sudah terverifikasi. *Level* ini memiliki fokus pada definisi, perencanaan, dan masalah kinerja tingkat proyek. Hasil kerja sesuai pada standar yang telah ditetapkan dan sesuai pada persyaratan. *Level* 2 memiliki perbedaan dengan *level* 1 yakni bahwasannya pada kinerja *level* 2 proses kinerja sudah terencana dan dikelola.
3. *Level* 3 "*Well Defined*"
   Pada *level* ini memiliki fokus pada penyesuaian disiplin dari proses yang talah ditetapkan pada tingkat organisasi. *Level* ini menggunakan persetujuan, sesuai dengan standar yang telah ada, dan proses telah didokumentasikan. Dalam kinerjanya *level* 3 dengan kinerja *level* 2 memiliki perbedaan yaitu bahwa proses kinerja ini direncanakan dan dikelola dengan menggunakan proses standar organisasi.
4. *Level* 4 "*Quantitatively Controlled*"
   Level ini berfokus pada pengukuran yang dihubungkan dengan tujuan bisnis organisasi. Meskipun penting untuk memulai menghimpun dan menggunakan Langkah proyek dasar sejak dini, pengukuran dan penggunaan data tidak diharapkan secara luas sampai tingkat yang lebih tinggi telah dicapai. Langkah detail pada proses kinerja dapat dikumpulkan dan dianalisis. Perbedaan dengan kinerja *level* 3 adalah, bahwa proses kinerja *level* 4 didefinisikan, dipahami dan dikendalikan secara kuantitatif.
5. *Level* 5 "*Continously Improving*"
   Level 5 "*Continously Improving*" ini menghasilkan pengungkitan dari semua peningkatan praktik manajemen yang terlihat pada tingkat sebelumnya, lalu ditekankan perubahan budaya yang dapat mempertahankan hasil yang telah dibuat. Adanya proses perbaikan secara berkesinambungan karena mendapatkan *feedback* kuantitatif dari melakukan proses yang telah didefinisikan. Perbedaan utama dari kinerja proses *level* 4 adalah bahwa proses telah terdefinisi dan proses yang telah sesuai standar menjalani perbaikan berkelanjutan dan dilakukannya peningkatan, berdasarkan pada pemahaman kuantitatif dari dampak perubahan proses.

Tabel 2.3 *Capability Level* SSE-CMM (CMU, 2013)

Keterangan	***Level***
Performed Informally	1
Planned and Tracked	2
Well Defined	3
Quantitatively Controlled	4
Continuously Improving	5

2.2.12 Perhitungan *Maturity Level*

Hasil dari perhitungan kuesioner yang dibuat rekapitulasi untuk dapat mempresentasikan presentase dan *Maturity Level* (Surendro, 2009).

Nilai *Maturity Level* didapatkan dari rata-rata seluruh kontrol keamanan yang telah dihitung *level* kemampuannya. Setiap klausul memiliki beberapa objektif kontrol, dan setiap objektif kontrol memiliki beberapa kontrol keamanan informasi dan rata-rata yang dari kontrol keamanan itulah yang diambil untuk menghasilkan nilai *Maturity Level* setiap objektif kontrol.

Sedangkan nilai *Maturity Level* tiap klausul diambil berdasarkan rata-rata objektif kontrol yang digunakan yang pada klausul tersebut.

Dalam penelitian ini pembedaan istilah antara nilai kematangan dan tingkat kematangan. Nilai kematangan dapat bernilai tidak bulat (desimal), yang mempresentasikan proses pencapaian menuju suatu tingkat kapabilitas tertentu. Sedangkan tingkat kapabilitas lebih menunjukkan tahapan atau kelas yang dicapai dalam proses kapabilitas yang dinyatakan dalam bilangan bulat (Surendro, 2009).

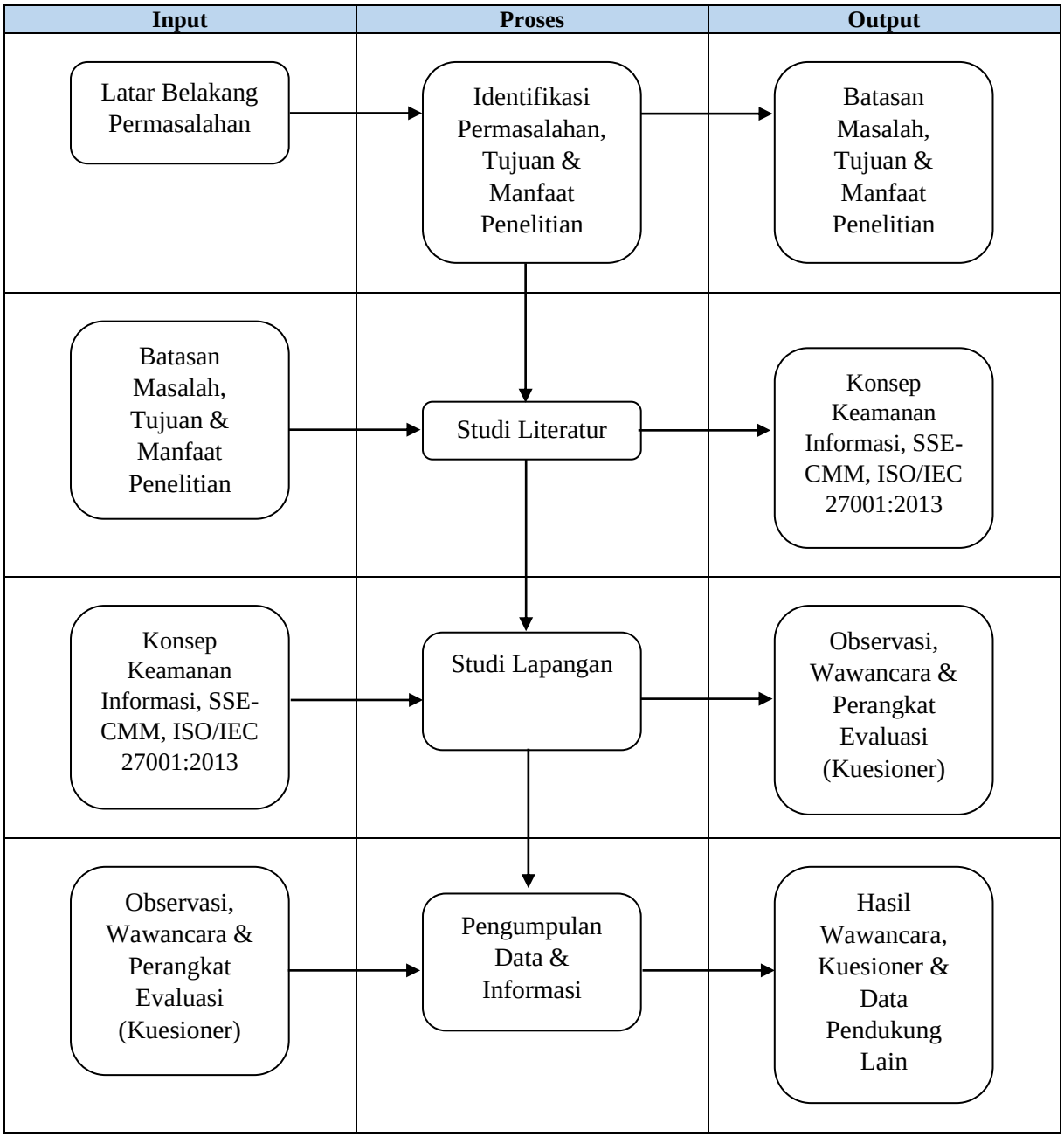
Dari penjabaran teori diatas terkait *System Security Engineering Capability Maturity Model* (SSE-CMM) adalah model yang dapat digunakan untuk penerapan keamanan di dalam sistem teknologi informasi. Adapun kelebihan dari SSE-CMM dibandingkan model lainnya adalah tujuan berfokus pada pendifinisian, peningkatan dan penilaian keamanan pada kemampuan teknik dengan pendekatan model kematangan keamanan pada keberlangsungan teknik dan metode penilaian. Tingkat kemampuan pada SSE-CMM dibagi menjadi lima bagian yaitu *performed informally*, *planned and tracked*, *well defined*, *quantitatively controlled*, dan *continuously improving*.

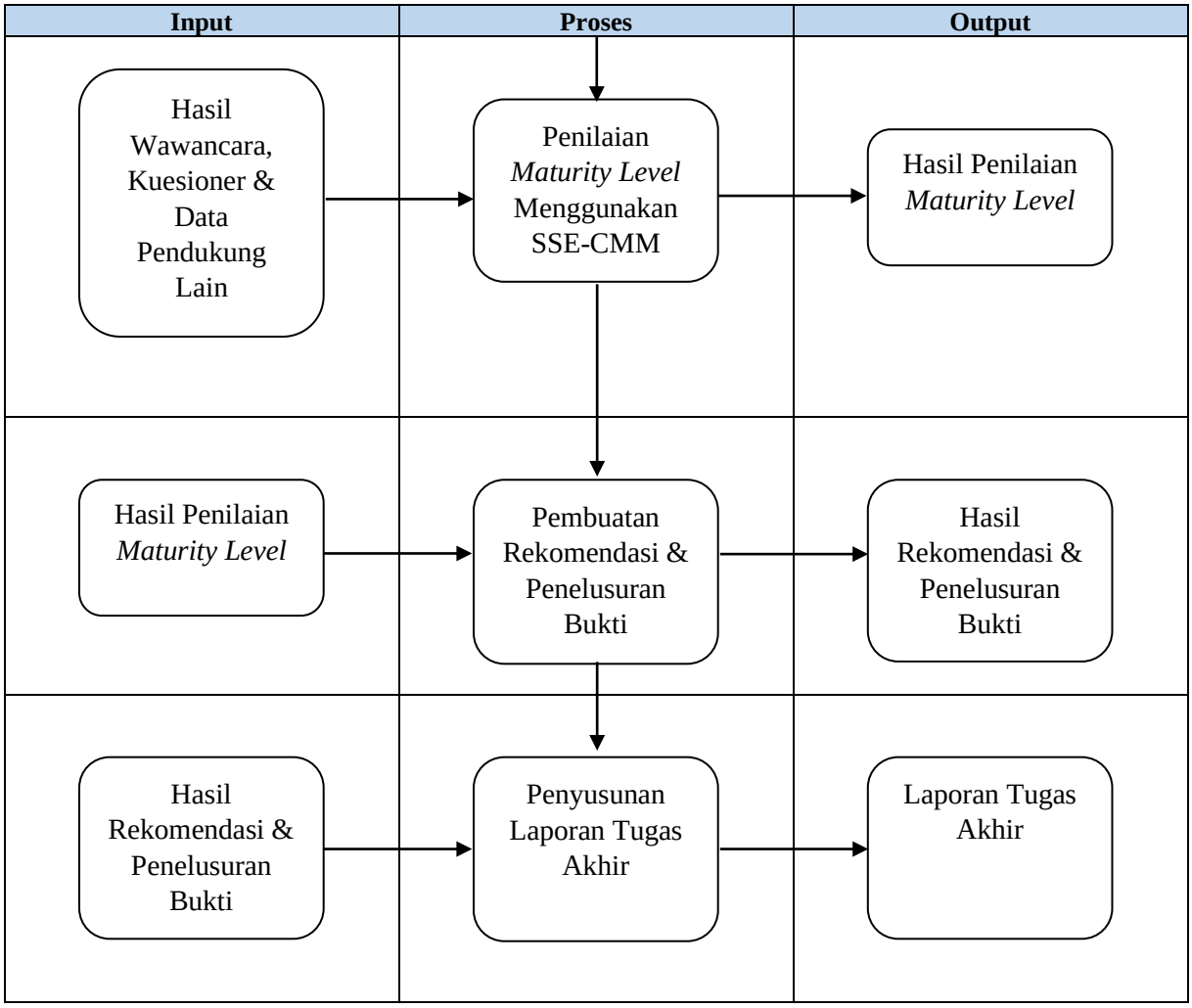
BAB III
METODOLOGI

Pada bab ini akan membahas mengenai metodologi yang berisi tahapan-tahapan yang dilakukan dalam pengerjaan tugas akhir, deskripsi dari setiap tahapan.

3.1 Tahapan Metodologi Penelitian

Pada sub bab ini membahas mengenai metodologi yang digunakan dalam pengerjaan tugas akhir. Metodologi yang digunakan dalam penelitian ini dapat dilihat pada Gambar 3.1.





Gambar 3.1 Metode Penelitian

3.2 Deskripsi Metodologi Penelitian

Pada bagian ini akan dijelaskan secara lebih rinci mengenai tahapan pada metode yang akan digunakan dalam pelaksanaan tugas akhir:

3.2.1 Identifikasi Permasalahan

Pada tahap ini akan dilakukan kegiatan mencari permasalahan yang ada. Setelah permasalahan ditemukan, langkah selanjutnya adalah mencari solusi yang dapat digunakan untuk menyelesaikan permasalahan tersebut. Hasil dari tahap ini merupakan permasalahan dan usulan solusi yang dapat diangkat menjadi topik tugas akhir.

3.2.2 Studi Literatur

Pada tahapan ini akan dilakukan mencari referensi teori yang relefan dengan kasus atau penemuan permasalahan yang akan menunjang kelancaran proses pengerjaan tugas akhir. Pencarian data dan informasi dari buku, jurnal, maupun laporan penelitian yang sebelumnya dan berkaitan mengenai keamanan informasi, cara pengukurannya, dan variabel yang digunakan. Selain itu, dilakukan pencarian informasi mengenai klausul-klausul dalam ISO/IEC 27001:2013 dan Analisa tingkat kematangan (*Level Maturity*) keamanan informasi dengan menggunakan metode/indek SSE-CMM. Dari tahap ini, penulis juga mulai menyusun instrumen penelitian berupa kuesioner yang akan digunakan dalam penelitian.

3.2.3 Pengumpulan Data dan Informasi

Pada tahap ini dilakukan pengumpulan data dan informasi yang berkaitan dengan pengerjaan tugas akhir. Penulis membutuhkan data serta informasi yang lengkap sebagai bahan untuk mendukung teori-teori yang telah dijelaskan pada Bab sebelumnya, metode pengumpulan data yang digunakan mencakup studi pustaka, studi lapangan yang terdiri dari observasi, wawancara, dan kuesioner, serta studi literatur sejenis.

3.2.4 Studi Lapangan

Studi lapangan dilakukan penulis secara langsung di Kantor Pusat PDAM Surya Sembada Kota Surabaya yang berada pada Jl. Mayjend. Prof. Dr. Moestopo No. 2 Surabaya. Studi lapangan merupakan studi yang dilakukan secara langsung ke tempat penelitian yang sudah ditentukan penulis. Studi lapangan ini antara lain meliputi:

1. Observasi
   Observasi lebih dari sekedar melakukan pengamatan pada lingkungan sekitar untuk memperoleh ide untuk penelitian, namun observasi adalah proses dilakukannya pengukuran yang cermat dan akurat, yang merupakan fitur pembeda penyelidikan ilmiah yang dilakukan dengan baik (Marczyk, 2005). Metode observasi yang dilakukan penulis pada penelitian tugas akhir ini dengan pengamatan secara langsung di Kantor Pusat PDAM Surya Sembada Kota Surabaya Bagian Teknologi Sistem Informasi (TSI), dengan melihat proses sistem keamanan informasi dan proses untuk mendapatkan data yang dibutuhkan pada bagian Teknologi Sistem Informasi (TSI). Kegiatan observasi ini dimulai pada bulan Maret sampai dengan bulan April 2022.
2. Wawancara
   Teknik pengumpulan data dimana pewawancara dalam mengumpulkan data mengajukan pertanyaan kepada yang diwawancarai adalah definisi dari wawancara (Sugiyono, 2014). Wawancara tergolong ke dalam metode pengumpulan data kualitatif. Dalam penelitian ini penulis melakukan wawancara secara langsung terhadap pejabat di bagian Teknologi Sistem Informasi pada PDAM Surya Sembada Kota Surabaya
3. Kuesioner
   Kuesioner adalah cara untuk mengumpulkan data yang dapat dilakukan dengan cara memberikan beberapa pertanyaan atau pernyataan tertulis yang ditujukan ke responden yang telah ditentukan untuk dijawabnya (Sugiyono, 2014). Dalam penelitian ini kuesioner termasuk ke dalam metode pengumpulan data kualitatif. Dalam melakukan pengumpulan data dan penyebaran kuesioner penulis melakukan pada bagian Teknologi dan Sistem Informasi di PDAM Surya Sembada Kota Surabaya. Pertanyaan atau pernyataan pada kuesioner yang telah ditetapkan memiliki acuan pada klausul-klausul yang dipilih penulis pada standar ISO/IEC 27001:2013. Selanjutnya akan dilakukan Analisa tingkat kematangan (*Level Maturity*) keamanan informasi. Pelaksanaan kuesioner dilakukan pada tanggal 7 April 2022 s/d 11 April 2022

3.2.5 Menentukan Ruang Lingkup SMKI

Dalam melakukan pengumpulan data untuk menentukan ruang lingkup SMKI diperlukan hal-hal, sebagai berikut:

1. Mempelajari karakteristik dari PDAM Surya Sembada Kota Surabaya dimulai dari profil perusahaan, visi dan misi perusahaan serta tujuan yang ingin dicapai oleh PDAM Surya Sembada Kota Surabaya
2. Menghimpun informasi berkaitan dengan teknologi informasi serta teknologi apa saja yang dimiliki oleh PDAM Surya Sembada Kota Surabaya yang berupa informasi *database* dan infrastruktur lainnya.

3.2.6 Pemilihan Objektif Kontrol dan Kontrol Keamanan Berdasarkan ISO/IEC 27001:2013

Memilih objektif kontrol dan kontrol keamanan informasi yang akan diimplementasikan di PDAM Surya Sembada Kota Surabaya. Selanjutnya melakukan Pemetaan ISO/IEC 27001:2013 yang akan digunakan dalam Penelitian

Penulis memilih beberapa kontrol yang sesuai dengan kondisi dan masukan dari pihak Bagian Teknologi Sistem Informasi (TSI) PDAM Surya Sembada Kota Surabaya. Tabel 3.1 merupakan klausul yang penulis gunakan dalam penelitian ini.

Tabel 3.1 Klausul ISO/IEC 27001:2013 yang Digunakan

Klausul	Objektif Kontrol	Kontrol Keamanan
A.9. Kontrol Akses	A.9.1 Persyaratan Bisnis Terhadap Kontrol Akses	A.9.1.1 Kebijakan Kontrol Akses
		A.9.1.2 Akses ke jaringan dan layanan jaringan
A.11. Keamanan Fisik dan Lingkungan	A.11.1 Area Aman	A.11.1.2 Kontrol Entri Fisik
		A.11.1.3 Mengamankan kantor, ruangan, dan fasilitas
		A.11.1.4 Melindungi Terhadap Ancaman Eksternal dan Lingkungan
	A.11.2 Peralatan	A.11.2.2 Utilitas Pendukung
		A.11.2.3 Keamanan Kabel
		A.11.2.4 Pemeliharaan Peralatan
A.12 Keamanan Operasi	A.12.2 Perlindungan dari *Malware*	A.12.2.1 Kontrol terhadap *Malware*
	A.12.3 *Backup*	A.12.3.1 *Backup* Informasi
A.16. Pengelolaan Insiden Keamanan Informasi	A.16.1 Manajemen Insiden Keamanan Informasi dan Pebaikan	A.16.1.2 Pelaporan Peristiwa keamanan informasi
		A.16.1.3 Pelaporan kelemahan keamanan informasi
		A.16.1.4 Penilaian dan keputusan tentang kejadian keamanan informasi
		A.16.1.5 Respon terhadap insiden keamanan informasi
		A.16.1.6 Belajar dari Insiden Keamanan Informasi

3.2.7 Penilaian *Maturity Level* Menggunakan SSE-CMM

Dalam penilaian *Maturity Level*, penulis menggunakan *System Security Engineering Capability Maturity Model* (SSE-CMM). Langkah-langkah yang dilakukan sebelum melakukan penilaian *Maturity Level* adalah sebagai berikut:

1. Pembuatan pernyataan
   Setelah menentukan objektif kontrol dan kontrol keamanan informasi apa saja yang akan diimplementasikan, selanjutnya penulis membuat pernyataan berdasarkan kontrol keamanan dari setiap objektif kontrol yang dipilih untuk diimplementasikan di PDAM

Surya Sembada Kota Surabaya. Pernyataan ini dibuat dan disesuaikan dengan berdasarkan standar ISO/IEC 27001:2013 yang memiliki isi panduan implementasi dari tiap kontrol keamanan yang dipilih.

2. Penentuan nilai tingkat kemampuan (*Capability Level*)
   Untuk menilai *level* kemampuan keamanan pada tiap pernyataan digunakan model *System Security Engineering Capability Maturity Model* (SSE-CMM).

Tabel 3.2 *Level* Kemampuan SSE-CMM (CMU, 2013)

Tingkat Kemampuan	Deskripsi
1	*Performed Informally* (Dilakukan Informal)
2	*Planned and Tracked* (Direncanakan dan Dilacak)
3	*Well Defined* (Didefinisikan dengan Baik)
4	*Quantitatively Controlled* (Dikendalikan secara kuantitatif)
5	*Continuously Improving* (Ditingkatkan terus-menerus)

3. Perhitungan Tingkat Kematangan (*Maturity Level*)
   Nilai *Maturity Level* bisa diperoleh dari rata-rata seluruh kontrol keamanan yang telah dihitung sebelumnya pada *level* kemampuannya. Sedangkan untuk pemberian pembobotan pada setiap pernyataan kontrol keamanan, menurut Sarno dan Iffano (2009) bahwa pembobotan pada setiap pernyataan kontrol keamanan yang digunakan mengacu pada resiko yang akan terjadi. Dalam hubungannya dengan SMKI, resiko adalah dampak yang ditimbulkan atas terjadinya sesuatu yang mengancam keamanan informasi di organisasi, sehingga setiap pernyataan akan diberikan bobot sesuai dengan nilai resiko yang akan terjadi apabila tidak diterapkan (Sarno & Iffano, 2009). Setiap klausul memiliki beberapa objektif kontrol, dan setiap objektif kontrol memiliki beberapa kontrol keamanan informasi dan rata-rata yang diperolah dari kontrol keamanan itulah yang diambil untuk menghasilkan nilai *Maturity Level* pada setiap objektif kontrol. Sedangkan nilai *Maturity Level* tiap klausul diambil berdasarkan rata-rata objektif kontrol yang digunakan pada klausul tersebut.

3.2.8 Pemberian Rekomendasi

Tahapan ini terdiri dari tahap penelusuran bukti dan tahap pemberian rekomendasi.

1. Penelusuran Bukti
   Pada tahap ini dilakukan penelusuran bukti berdasarkan hasil penilaian *Maturity Level*. Ini bertujuan untuk menyelaraskan hasil perhitungan *Maturity Level* agar sesuai dengan kondisi sebenarnya dari keamanan informasi di PDAM Surya Sembada Kota Surabaya. Serta untuk mengetahui apakah ada *gap* antara kondisi saat ini dengan panduan implementasi kontrol keamanan yang ada pada ISO/IEC 27001:2013, bahwa ISO/IEC 27001:2013 hanya sebagai panduan saja, tidak mengukur tingkat kematangan implementasi atau nilai *gap*. Untuk mengukur tingkat kematangan dipergunakan *framework* selain ISO/IEC 27001:2013 (ISO, 2013) (CMU, 2003).
2. Pemberian Rekomendasi
   Tahap ini bertujuan untuk memberikan usulan perbaikan serta pengembangan terhadap Sistem Manajemen Keamanan Informasi di PDAM Surya Sembada Kota Surabaya. Rekomendasi yang diberikan beracuan pada standar ISO/IEC 27001: 2013 yang memiliki isi panduan implementasi tiap kontrol keamanan yang ada pada ISO/IEC 27001: 2013.

3.2.9 Hasil dan Pembahasan

Pada tahap ini penulis akan melakukan pembahasan dari hasil tahap-tahap yang sudah dilewati oleh penulis sebelumnya. Yang dimulai dari pembahasan mengenai pemilihan domain

penentuan klausul ISO/IEC 27001:2013, hasil perhitungan *Maturity Level*, rekomendasi serta usulan bagi PDAM Surya Sembada Kota Surabaya, implikasi penelitian serta keterbatasan studi.

3.2.10 Penyusunan Laporan Tugas Akhir

Tahap ini adalah tahap terakhir dalam pengerjaan tugas akhir, yaitu penyusunan laporan tugas akhir. Pada tahap ini setiap tahapan dalam tugas akhir akan didokumentasikan serta menyimpulkan setiap langkah dan keputusan yang diambil dalam proses pembuatannya. Penyusunan buku tugas akhir ini mengikuti format yang telah ditetapkan oleh Direktorat Pendidikan ITS

1. Bab I Pendahuluan
   Pada bab ini dijelaskan tentang latar belakang, perumusan masalah, batasan, tujuan, manfaat tugas akhir.
2. Bab II Tinjauan Pustaka
   Pada bab ini dijelaskan mengenai penelitian serupa yang telah dilakukan dan dasar teori yang mendukung penyelesaian permasalahan pada tugas akhir.
3. Bab III Metodologi
   Bab ini menjelaskan tentang tahapan – tahapan yang dilakukan dalam mengerjakan tugas akhir.
4. Bab IV Hasil dan Pembahasan
   Bab ini berisi tentang analisis dan pembahasan dalam penyelesaian permasalahan yang dibahas pada tugas akhir.
5. Bab V Kesimpulan dan Saran
   Bab ini akan berisi kesimpulan dan saran yang ditunjukkan sebagai pelengkap untuk menyempurnakan tugas akhir ini.

BAB IV
HASIL DAN PEMBAHASAN

Bab ini berisi tentang analisis dan pembahasan dalam penyelesaian permasalahan yang dibahas pada tugas akhir.

4.1 Ruang Lingkup Sistem Manajemen Keamanan Informasi (SMKI)

4.1.1 Gambaran Umum Perusahaan

Gambar 4.1 Logo PDAM Surya Sembada Kota Surabaya

Sebagai BUMD yang melaksanakan mandat tanggung jawab dari Pemerintah Kota untuk penyediaan air minum bagi penduduk Kota Surabaya PDAM Surya Sembada Kota Surabaya memiliki posisi yang sangat strategis serta dituntut untuk selalu mampu memenuhi tuntutan kebutuhan penduduk Surabaya khususnya pelanggan secara memuaskan. Pada tahun 1890, air minum untuk penduduk kota Surabaya pertama kali diambil dari sumber mata air desa Purut Pasuruan yang diangkut dengan menggunakan kereta api. Seiring dengan perkembangan zaman, pada tahun 1903 dilakukan pemasangan pipa dari Pandaan oleh NV. Biernie selama tiga tahun lamanya hingga jumlah pelanggan ±1.500 sambungan. Kebutuhan masyarakat akan air bersih terus meningkat sehingga pada tahun 1922 dibangunlah Instalasi Penjernihan Air Minum (IPAM) Ngagel I dengan kapasitas 60 liter/detik, yang kemudian ditingkatkan menjadi 180 liter/detik pada tahun 1942. Delapan tahun kemudian tepatnya pada tahun 1950, Pemerintah Belanda menyerahkan Perusahaan Air Minum pada Pemerintah Republik Indonesia (Kota Praja Surabaya). Dengan meningkatkan populasi jumlah penduduk di kota Surabaya, maka sebagai solusinya kapasitas IPAM Ngagel ditingkatkan menjadi 350 liter/detik pada tahun 1954. Setelah berhasil membangun IPAM Ngagel I, pada tahun 1959 dibangunlah IPAM Ngagel II dengan kapasitas 1.000 liter/detik yang didesain dan dilaksanakan oleh Degremont Fa dari Perancis.

Pada tahun 1976, Perusahaan Air Minum disahkan menjadi Perusahaan Daerah dan dituangkan di dalam Perda No. 7 tanggal 30 Maret 1976. Setahun kemudian kapasitas IPAM Ngagel I ditingkatkan menjadi 500 liter/detik. Status Perusahaan Daerah dialihkan pada tahun 1978 menjadi Perusahaan Daerah Air Minum dari Dinas Air Minum berdasarkan SK Walikotamadya Dati II Surabaya No. 657/WK/77 tanggal 30 Desember 1977. Peningkatan kapasitas IPAM Ngagel I kembali dilakukan pada tahun 1980 menjadi 1.000 liter/detik. Peningkatan jumlah penduduk kota Surabaya menggugah hati pemerintah untuk melaksanakan pembangunan IPAM Ngagel III, IPAM Karangpilang I, II dan III. Pembangunan IPAM Ngagel III dengan kapasitas 1.000 liter/detik atas lisensi dari Neptune Microfloc (Amerika Serikat). Selain itu, IPAM Karangpilang I telah dibangun pada tahun 1990 dengan kapasitas 1.000 liter/detik dengan dana Loan IBRD. No.2362 IND. Adapun visi dan misi dari perusahaan adalah:

Visi

Menjadi Perusahaan Air Minum Modern

Misi

1. Memastikan pengelolaan keuangan yang transparan untuk kesejahteraan masyarakat
2. Membangun masyarakat yang bijak dalam penggunaan air

3. Menyediakan air minum yang efisien dan berkelanjutan
4. Membangun lingkungan kerja yang memprioritaskan integritas dan prestasi

PDAM Surya Sembada Kota Surabaya memiliki kantor pusat dan dua unit produksi. Kantor pusat PDAM Surya Sembada Kota Surabaya berada di Jalan Mayjen Prof. Dr. Moestopo No.2 Surabaya. Lokasi dua unit produksi berada di tempat yang berbeda. Unit Produksi tersebut adalah unit produksi IPAM Ngagel dan IPAM Karangpilang. Pada unit produksi IPAM Ngagel terdapat tiga instalasi, yaitu IPAM Ngagel I, II, dan III. Ketiga instalasi tersebut berada di Jalan Penjernihan nomor 1 Surabaya. Unit produksi IPAM Karangpilang juga terdapat tiga instalasi yang berada di Jalan Mastrip nomor 56 Karangpilang Surabaya.

Gambar 4.2 Kantor Pusat PDAM Surya Sembada Kota Surabaya

Tujuan didirikan PDAM Surya Sembada Kota Surabaya ini adalah:

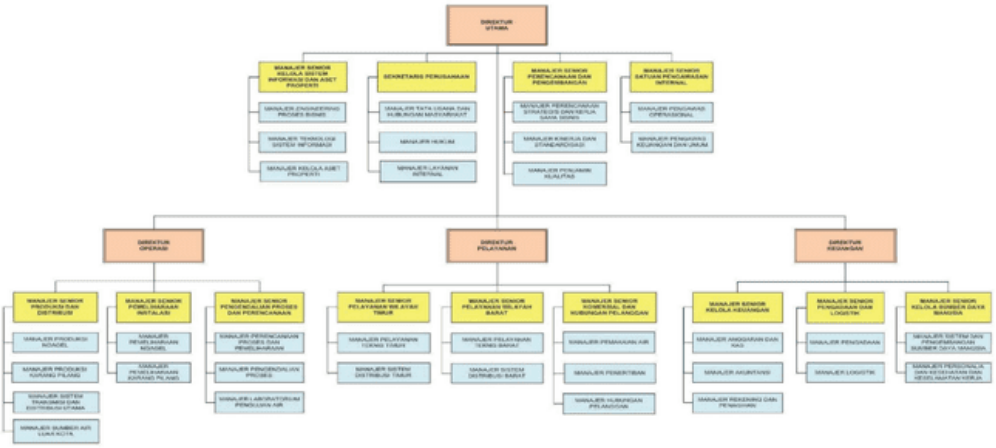
1. Menyediakan pelayanan kepada masyarakat sesuai dengan ruang lingkup usahanya.
2. Memberikan kontribusi pada Pendapatan Asli Daerah.
3. Turut serta meningkatkan perekonomian daerah.

Untuk memberikan pelayanan prima kepada pelanggan, PDAM Surya Sembada Kota Surabaya memiliki Budaya Kerja antara lain:

1. *Satisfaction* : Mengutamakan kepuasan dalam melayani pelanggan.
2. *Morale* : Memiliki semangat juang yang gigih dan pantang menyerah dalam upaya mencapai kesuksesan.
3. *Integrity* : Memahami komitmen untuk mewujudkan loyalitas.
4. *Leadership* : Berjiwa kepemimpinan sebagai teladan dalam sikap, kompetensi dan jati diri.
5. *Entrepreneurship* : Memiliki keberanian dalam mengambil risiko dengan perhitungan yang masuk akal dan terkendali.

4.1.2 Struktur Organisasi Perusahaan

Guna mendukung berjalannya aktifitas di perusahaan, PDAM Surya Sembada Kota Surabaya memiliki susunan organisasi sebagai berikut:



Gambar 4.3 Struktur Organisasi PDAM Surya Sembada Kota Surabaya

Tugas Pokok dan Fungsi Bagian TSI

Pada penelitian ini, penulis melakukan penelitian pada bagian Teknologi dan Sistem Informasi (TSI). Bagian Teknologi Sistem Informasi (TSI) dipimpin oleh Manajer Teknologi Sistem Informasi yang bertanggung jawab kepada Manajer Senior Teknologi Sistem Informasi dan Aset Properti. Manajer Teknologi Sistem Informasi membawahi:

1. *Supervisor* Infrastruktur;
2. *Supervisor* Sistem Informasi;
3. *Supervisor* Pengembangan Teknologi Informasi
4. *Supervisor* Kontrol Digital dan Instrumentasi.

a. Manajer Teknologi Sistem Informasi bertugas:
   1) Mengelola dan mengoordinasikan infrastruktur teknologi informasi yang meliputi penyediaan, monitoring operasional, serta pemeliharaan fasilitas komputer, jaringan komputer, *server*, *Data Center*, *disaster recovery center*, *command center*, dan surat elektronik/*e-mail;*
   2) Mengelola dan mengoordinasikan sistem kontrol digital dan instrumentasi yang meliputi penyediaan, monitoring operasional, serta pemeliharaan HMI, SCADA, *Online Monitoring*, *sensor*, *controller*, dan lain-lain*;*
   3) Mengelola dan mengoordinasikan penyediaan, monitoring operasional, pemeliharaan, perubahan, dan penyempurnaan aplikasi teknologi informasi sesuai model dan proses bisnis perusahaan;
   4) Mengelola dan mengoordinasikan pengembangan teknologi informasi yang meliputi pembuatan aplikasi dan infrastruktur baru sesuai perkembangan bisnis perusahaan;
   5) Mengelola dan mengoordinasikan sistem pengamanan data-data perusahaan.

b. Subbagian Infrastruktur

   Subbagian Infrastruktur dipimpin oleh *Supervisor* Infrastruktur yang bertanggung jawab kepada Manajer Teknologi Sistem Informasi. *Supervisor* Infrastruktur membawahi Staf Senior dan Staf. Subbagian Infrastruktur bertugas :
   1) Melaksanakan dan mengawas instalasi perawatan, dan perbaikan komputer, *printer*, dan perlengkapannya;
   2) Melaksanakan dan mengawasi instalasi, perawatan, dan perbaikan jaringan komputer lokal dan jaringan komputer antarkantor;
   3) Melaksanakan dan mengawasi instalasi, perawatan, dan perbaikan *server fisikal* serta virtual beserta *storage system;*
   4) Melaksanakan dan mengawasi pemindahan *Backup* data ke media eksternal dan *Disaster Recovery Center (DRC)*;

5) Melaksanakan dan mengawasi pengamanan operasional *server*, komputer, dan jaringan komputer dari ancaman virus dan *hacker;*
6) Melaksanakan dan mengawasi penyediaan layanan sistem surat elektronik/*e- mail.*

c. Subbagian Sistem Informasi

Subbagian Sistem Informasi dipimpin oleh *Supervisor* Sistem Informasi yang bertanggung jawab kepada Manajer Teknologi Sistem Informasi. *Supervisor* Sistem Informasi membawahi Staf Senior dan Staf. *Supervisor* Sistem Informasi bertugas:

1) Melaksanakan dan mengawasi pemeliharaan dan perbaikan aplikasi sistem informasi;
2) Melaksanakan dan mengawasi proses analisis dan pembuatan desain pengembangan aplikasi yang sudah ada (*existing*), antara lain *billing system*, *payment online*, SKA, GIS, HRIS, dan lain-lain;
3) Melaksanakan dan mengawasi penambahan fitur-fitur aplikasi sistem informasi yang sudah ada (*existing*), antara lain *billing system*, *payment online*, SKA, GIS, HRIS, dan lain-lain;
4) Melaksanakan dan mengawasi pengevaluasian terhadap aplikasi sistem informasi yang sudah ada (*existing*) secara berkala;
5) Melaksanakan dan mengawasi *Backup* seluruh aplikasi dan *source code* secara reguler;
6) Melaksanakan dan mengawasi perbaikan data pada *database*.

d. Subbagian Pengembangan Teknologi Informasi

Subbagian Pengembangan Teknologi Informasi dipimpin oleh *Supervisor* Pengembangan Teknologi Informasi yang bertanggung jawab kepada Manajer Teknologi Sistem Informasi. *Supervisor* Pengembangan Teknologi Informasi membawahi Staf Senior dan Staf. *Supervisor* Pengembangan Teknologi Informasi bertugas:

1) Melaksanakan da mengawasi pengembangan aplikasi baru sesuai kebutuhan dan perkembangan bisnis perusahaan;
2) Melaksanakan dan mengawasi penyusunan standardisasi *software*, aplikasi, dan infrastruktur yang dapat diimplementasikan di perusahaan;
3) Melaksanakan dan mengawasi pemeliharaan dan pengembangan *database* sesuai perkembangan bisnis perusahaan;
4) Melaksanakan dan mengawasi *Backup store database* utama ke pengaman aplikasi;
5) Melaksanakan dan mengawasi penggunaan perangkat lunak yang legal;
6) Melaksanakan dan mengawasi penyediaan *helpdesk support*.

e. Subbagian Kontrol Digital dan Instrumentasi

Subbagian Kontrol Digital dan Instrumentasi Informasi dipimpin oleh *Supervisor* Kontrol Digital dan Instrumentasi yang bertanggung jawab kepada Manajer Teknologi Sistem Informasi. *Supervisor* Kontrol Digital dan Instrumentasi membawahi Staf Senior dan Staf. *Supervisor* Kontrol Digital dan Instrumentasi bertugas:

1) Melaksanakan dan mengawasi instalasi, perawatan, perbaikan, dan peremajaan peralatan kontrol digital dan instrumentasi yang meliputi *HMI*, *SCADA*, *Online Monitoring*, *sensor*, *controller*, dan lain-lain;
2) Melaksanakan dan mengawasi penelitian dan pengembangan sistem kontrol digital dan instrumentasi;
3) Melaksanakan dan mengawasi *monitoring* terhadap akuisisi dan akurasi peralatan kontrol digital.

4.2 Pengumpulan Data dan Informasi

Pada tahap ini dilakukan pengumpulan data dan informasi yang dibutuhkan untuk mengetahui kondisi perusahaan menggunakan metode wawancara dengan narasumber yang sudah dipilih sesuai kebutuhan. Selain pengumpulan data dan informasi dengan metode wawancara juga dilakukan dengan metode penyebaran kuesioner guna mengetahui nilai *Maturity Level* dari setiap klausul kepada beberapa pegawai bagian TSI PDAM Surya Sembada Kota Surabaya yang sudah dipetakan

4.2.1 Wawancara

Metode wawancara pada tahap ini memiliki peran penting dalam hal pengumpulan data yang akan membantu keberlangsungan pengerjaan tugas akhir. Kegiatan wawancara dilaksanakan dengan melakukan tanya jawab secara langsung kepada Manajer Teknologi Sistem Informasi (TSI) PDAM Surya Sembada Kota Surabaya di Kantor Pusat PDAM Surya Sembada Kota Surabaya. Untuk mengetahui penerapan sistem keamanan informasi dan permasalahan-permasalahan yang terjadi pada perusahaan yang berkaitan dengan sistem keamanan informasi.

Tabel 4.1 Tujuan Wawancara

Tujuan	Narasumber
Mengetahui kondisi terkini perusahaan terkait dengan keamanan informasi	Nasrul Amir
Mengetahui gambaran umum perusahaan serta tugas pokok dan fungsi bagian TSI	Nasrul Amir

Tabel 4.2 Daftar Pelaksanaan Wawancara

No	Hari/Tanggal	Tempat	Narasumber	Jabatan
1	Selasa, 5 April 2022	Ruang Bagian Teknologi Sistem Informasi (TSI)	Nasrul Amir	Manajer TSI
2	Rabu, 6 April 2022	Ruang SOCC (*Service and Operation Command Center*)	Nasrul Amir	Manajer TSI

4.2.2 Pemetaan Responden

Untuk pelaksanaan pengisian pernyataan dan pertanyaan dalam kuesioner, penulis melalukan pemetaan responden yang dilakukan bersama dengan Manajer Teknologi Sistem Informasi (TSI) hal tersebut bertujuan agar pernyataan dan pertanyaan tiap klausul ISO/IEC 27001:2013, dijawab tepat sasaran sesuai dengan tupoksi pengelolaan keamanan sistem infomasi pada PDAM Surya Sembada Kota Surabaya.

Tabel 4.3 Pemetaan Responden dengan Kontrol Keamanan ISO/IEC 27001:2013

No	Nama Responden	Jabatan	Kontrol Keamanan ISO/IEC 27001:2013
1.	Eko Yudha Prasetya	*Supervisor* Pengembangan Teknologi Informasi	A.9.1.1 Kebijakan Kontrol Akses A.12.3.1 *Backup* Informasi
2.	Dedy Purwanto	*Supervisor* Infrastruktur	A.9.1.2 Akses ke Jaringan dan Layanan Jaringan A.11.1.2 Kontrol Entri Fisik A.11.1.3 Mengamankan Kantor, Ruangan, dan Fasilitas A.11.1.4 Melindungi Terhadap Ancaman Eksternal dan Lingkungan

No	Nama Responden	Jabatan	Kontrol Keamanan ISO/IEC 27001:2013
			A.11.2.2 Utilitas Pendukung A.11.2.3 Keamanan Kabel A.11.2.4 Pemeliharaan Peralatan
3.	Ira Nuraini	*Supervisor* Sistem Informasi	A.12.2.1 Kontrol Terhadap *Malware* A.16.1.2 Pelaporan Peristiwa Keamanan Informasi A.16.1.3 Pelaporan Kelemahan Keamanan Informasi A.16.1.4 Penilaian dan Keputusan tentang Kejadian Keamanan Informasi A.16.1.5 Respon Terhadap Insiden Keamanan Informasi A.16.1.6 Belajar dari Insiden Keamanan Informasi

4.2.3 Alasan Pemilihan Klausul Berdasarkan ISO/IEC 27001:2013

Penulis memilih beberapa kontrol yang sesuai dengan kondisi dan masukan dari pihak Bagian Teknologi Sistem Informasi (TSI) PDAM Surya Sembada Kota Surabaya dengan beberapa alasan yang mendukung. Tabel 4.4 merupakan alasan pemilihan klausul yang penulis gunakan dalam penelitian ini.

Tabel 4.4 Alasan Pemilihan Klausul Berdasarkan ISO/IEC 27001:2013

A.9	**Kontrol Akses**
A.9.1	**Persyaratan Bisnis Terhadap Kontrol Akses**
A.9.1.1	**Kebijakan Kontrol Akses**
Alasan: Kontrol keamanan A.9.1.1 kontrol yang berkaitan dengan penetapan, pendokumentasian, dan peninjauan kebijakan akses mengacu bisnis dan kebutuhan keamanan informasi.	
A.9.1.2	**Akses ke jaringan dan layanan jaringan**
Alasan: Kontrol keamanan A.9.1.2 kontrol yang berkaitan dengan Akses ke dalam jaringan dan menggunakan layanan jaringan, yang menerangkan bahwa *user* hanya boleh diijinkan akses ke jaringan dan layanan jaringan yang telah secara khusus diizinkan untuk digunakan oleh *user*	
A.11	**Keamanan Fisik dan Lingkungan**
A.11.1	**Area Aman**
A.11.1.2	**Kontrol Entri Fisik**
Alasan: Kontrol keamanan A.11.1.2 kontrol Area aman harus dilindungi oleh kontrol entri yang tepat untuk memastikan bahwa hanya personel yang berwenang yang diperbolehkan mengakses	
A.11.1.3	**Mengamankan Kantor, Ruangan, dan Fasilitas**
Alasan: Kontrol keamanan A.11.1.3 kontrol bahwa keamanan fisik untuk kantor, kamar dan fasilitas harus dirancang dan diterapkan untuk prosedur bekerja	
A.11.1.4	**Melindungi Terhadap Ancaman Eksternal dan Lingkungan**
Alasan: Kontrol keamanan A.11.1.4 kontrol bahwa perlindungan fisik terhadap bencana alam, serangan atau kecelakaan yang berbahaya harus dirancang dan diterapkan	

A.11.2	**Peralatan**
A.11.2.2	**Utilitas Pendukung**
Alasan: Kontrol keamanan A.11.2.2 kontrol bahwa peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dalam mendukung utilitas	
A.11.2.3	**Keamanan Kabel**
Alasan: Kontrol keamanan A.11.2.3 kontrol yang menangani perlindungan terhadap daya dan kabel telekomunikasi atau layanan pendukung informasi	
A.11.2.4	**Pemeliharaan Peralatan**
Alasan: Kontrol keamanan A. 11.2.4 kontrol yang menangani pemeliharaan peralatan bahwa peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya yang berkelanjutan	
A.12	**Keamanan Operasi**
A.12.2	**Perlindungan dari *Malware***
A.12.2.1	**Kontrol Terhadap *Malware***
Alasan: Kontrol keamanan A.12.2.1 kontrol untuk perlindungan terhadap *Malware* dengan pendeteksian, pencegahan, dan pemulihan kontrol yang dikombinasikan secara tepat.	
A.12.3	***Backup***
A.12.3.1	***Backup* Informasi**
Alasan: Kontrol keamanan A. 12.3.1 kontrol untuk *Backup* informasi, Salinan cadangan informasi, perangkat lunak dan gambar sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan yang disepakati	
A.16	**Manajemen Insiden Keamanan Informasi**
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**
A.16.1.2	**Pelaporan Peristiwa Keamanan Informasi**
Alasan: Kontrol keamanan A.16.1.2 kontrol untuk pelaporan peristiwa keamanan informasi, bahwa kejadian keamanan informasi harus dilaporkan melalui saluran manajemen yang tepat secepat mungkin	
A.16.1.3	**Pelaporan Kelemahan Keamanan Informasi**
Alasan: Kontrol keamanan A.16.1.3 kontrol untuk pelaporan kelemahan keamanan informasi, pengguna (*user*) yang menggunakan sistem informasi dan layanan organisasi harus diminta untuk mencatat dan melaporkan setiap kelemahan keamanan sistem atau layanan yang diamati atau dicurigai	
A.16.1.4	**Penilaian dan Keputusan tentang Kejadian Keamanan Informasi**
Alasan: Kontrol keamanan A.16.1.4 kontrol untuk Penilaian dan Keputusan tentang kejadian keamanan informasi, bahwa kejadian keamanan informasi harus dinilai dan harus diputuskan apakah mereka harus diklasifikasikan sebagai insiden keamanan informasi	
A.16.1.5	**Respon Terhadap Insiden Keamanan Informasi**
Alasan: Kontrol keamanan A.16.1.5 kontrol Respon Terhadap Insiden Keamanan Informasi , bahwa insiden keamanan informasi harus ditanggapi sesuai dengan prosedur dan terdokumentasi	
A.16.1.6	**Belajar Dari Insiden Keamanan Informasi**
Alasan: Kontrol keamanan A.16.1.6 kontrol untuk Belajar dari Insiden Keamanan Informasi, bahwa pengetahuan yang diperoleh dari menganalisa dan menyelesaikan insiden keamanan informasi harus digunakan untuk mengurangi kemungkinan atau dampak dari insiden masa depan	

4.3 Penilaian *Maturity Level* Menggunakan SSE-CMM (*System Security Engineering Capability Maturity Level*)

Tahap ini merupakan tahap untuk menggambarkan sudah sejauh mana PDAM Surya Sembada Kota Surabaya dapat memenuhi proses pengelolaan keamanan informasi berdasarkan standar ISO/IEC 27001:2013 dan dilakukan terhadap masing-masing kontrol keamanan yang sudah dijabarkan pada sub bab 4.2.

Daftar pernyataan yang penulis gunakan di dalam penelitian ini dibuat berdasarkan kontrol keamanan dari setiap objektif kontrol yang dipilih untuk melakukan evaluasi tata kelola keamanan informasi PDAM Surya Sembada Kota Surabaya. Daftar penyataan yang penulis gunakan dibuat berdasarkan standar ISO/IEC 27001:2013 yang berisi tentang panduan implementasi dari masing-masing kontrol keamanan yang sudah diuraikan di atas. Dalam penelitian ini penulis menggunakan *System Security Engineering Capability Maturity Level* (SSE-CMM) untuk mengukur *Maturity Level* proses pengelolaan keamanan informasi berdasarkan standar ISO/IEC 27001:2013.

Di bawah ini merupakan kerangka kerja perhitungan nilai *Maturity Level* serta hasil perhitungan tingkat kematangan dari masing-masing kontrol kemanan informasi.

4.3.1 Klausul A.9 Kontrol Akses

Tabel 4.5 Kerangka Kerja Perhitungan *Maturity Level* Klausul A.9 Kontrol Akses

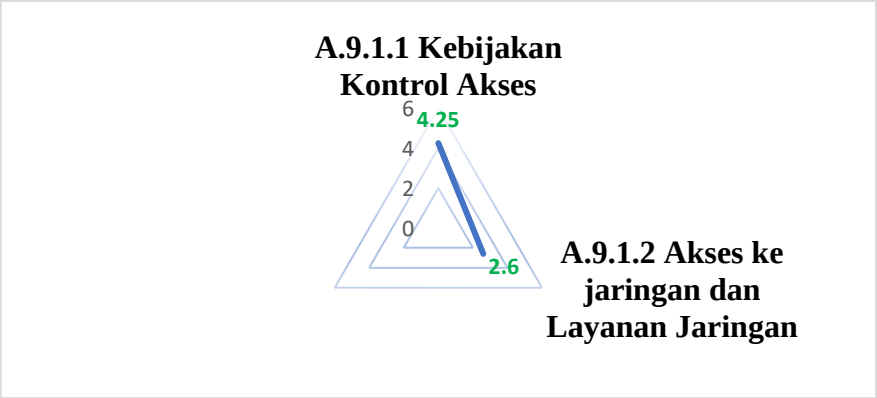
A.9	**Kontrol Akses**						
A.9.1	**Persyaratan Bisnis Terhadap Kontrol Akses**						
A.9.1.1	**Kebijakan Kontrol Akses**						
Kontrol: Kebijakan kontrol akses harus ditetapkan, didokumentasikan dan ditinjau berdasarkan persyaratan keamanan bisnis dan informasi							
No	**Pernyataan**	**Bobot**	**Tingkat Kemampuan**				**Nilai**
			1	**2**	**3**	**4**	**5**	
1.	Pemilik aset dapat menetapkan aturan akses kontrol yang tepat, hak akses dan pembatasan aturan pengguna terhadap aset yang dimiliki	1					✓	5
2.	Tersedianya kebijakan kontrol akses yang bersifat fisik dan logis yang baik dan sudah dipertimbangakan secara bersama-sama	1				✓		4
3.	Terdapat kebijakan yang relevan dan kewajiban kontraktual apapun yang berkaitan dengan pembatasan akses ke data atau layanan	1				✓		4
4.	Terdapat tinjauan kembali hak akses secara berkala dan hak akses dihapus apabila tidak sesuai	1				✓		4
Total Bobot		4						4,25
A.9	**Kontrol Akses**							
A.9.1	**Persyaratan Bisnis Terhadap Kontrol Akses**							
A.9.1.2	**Akses ke Jaringan dan Layanan Jaringan**							
Kontrol: Pengguna hanya boleh diberikan akses ke jaringan dan layanan jaringan yang telah secara khusus diizinkan untuk digunakan.								

No	Pernyataan	Bobot	Tingkat Kemampuan					Nilai
			1	2	3	4	5	
1.	Terdapat kebijakan yang mengatur jaringan dan layanan jaringan mana yang diizinkan untuk diakses	1			✓			3
2.	Terdapat kebijakan yang mengatur otorisasi untuk menetapkan siapa yang diizinkan untuk mengakses jaringan atau layanan jaringan tertentu	1			✓			3
3.	Tersedianya kebijakan yang mengatur tentang sarana yang dipakai untuk mengakses jaringan dan layanan jaringan (misalnya penggunaan VPN atau jaringan nirkabel)	1			✓			3
4.	Terdapat kebijakan yang mengatur syarat untuk autentikasi (validasi) pengguna untuk mengakses berbagai layanan jaringan	1		✓				2
5.	Terdapat kebijakan yang mengatur pemantauan penggunaan layanan jaringan	1		✓				2
Total Bobot		5						2,60

Tabel 4.6 Hasil Perhitungan *Maturity Level* Klausul A.9 Kontrol Akses

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
A.9 Kontrol Akses	A.9.1 Persyaratan Bisnis Terhadap Kontrol Akses	A.9.1.1 Kebijakan Kontrol Akses	4,25	3,42
		A.9.1.2 Akses ke Jaringan dan Layanan Jaringan	2,60	
	***Maturity Level* Klausul A.9**			**3,42**

Berdasarkan hasil perhitungan *Maturity Level* yang sudah penulis lakukan pada Klausul A.9 Kontrol Akses, maka didapatkan nilai *Maturity Level* di PDAM Surya Sembada Kota Surabaya sebesar 3,42. Dari hasil nilai *Maturity Level* tersebut termasuk dalam *level* 3 yaitu *Well Defined* (Didefinisikan dengan baik). Hasil itu dapat diperoleh karena pada kontrol keamanan A.9.1.1 terdapat 4 pernyataan mendapat nilai tingkat kemampuan 4,25 serta 5 pernyataan pada kontrol keamanan A.9.1.2 mendapat nilai tingkat kemampuan 2,6. Di bawah ini merupakan grafik yang merepresentasikan nilai *Maturity Level* klausul A.9 Kontrol Akses



Gambar 4.4 Representasi Nilai *Maturity Level* Klausul A.9 Kontrol Akses

4.3.2 Klausul A.11 Keamanan Fisik dan Lingkungan

Tabel 4.7 Kerangka Kerja Perhitungan *Maturity Level* Klausul A.11 Keamanan Fisik dan Lingkungan

A.11	**Keamanan Fisik dan Lingkungan**							
A.11.1	**Area Aman**							
A.11.1.2	**Kontrol Entri Fisik**							
Kontrol: Area aman harus dilindungi oleh kontrol entri yang tepat untuk memastikan bahwa hanya personel yang berwenang yang diperbolehkan mengakses								
No	**Pernyataan**	**Bobot**	**Tingkat Kemampuan**					**Nilai**
			1	**2**	**3**	**4**	**5**	
1.	Terdapat pencatatan tanggal dan waktu masuk dan keluarnya pengunjung dan terdapat pengawasan terhadap pengunjung	1				✓		4
2.	Akses ke daerah-daerah tempat informasi rahasia diproses atau disimpan (Contoh: Ruang *server*) harus dibatasi untuk individu yang berwenang dengan menerapkan kontrol akses yang sesuai (Contoh: menggunakan kartu akses atau *fingerprint*)	1				✓		4
3.	Pemantauan dan penjagaan buku masuk fisik atau jejak audit elektronik dari semua akses	1				✓		4
4.	Semua pegawai atau pihak eksternal memakai tanda pengenal	1				✓		4
5.	Perbaharuan secara berkala tentang aturan hak akses untuk mengamankan daerah yang aman	1				✓		4
Total Bobot		5						4,00
A.11	**Keamanan Fisik dan Lingkungan**							
A.11.1	**Area Aman**							
A.11.1.3	**Mengamankan Kantor, Ruangan, dan Fasilitas**							
Kontrol: Keamanan fisik untuk kantor, kamar dan fasilitas harus dirancang dan diterapkan								

No	Pernyataan	Bobot	Tingkat Kemampuan					Nilai
			1	2	3	4	5	
1.	Fasilitas utama ditempatkan di tempat yang aman dan tidak dapat diakses oleh publik	1				✓		4
2.	Terdapat tanda baik di dalam atau di luar bangunan yang menunjukkan terdapat tempat pengelolaan dan pengolahan data atau informasi	1	✓					1
Total Bobot		2						2,50
A.11	**Keamanan Fisik dan Lingkungan**							
A.11.1	**Area Aman**							
A.11.1.4	**Melindungi Terhadap Ancaman Eksternal dan Lingkungan**							

Kontrol: Perlindungan fisik terhadap bencana alam, serangan atau kecelakaan yang berbahaya harus dirancang dan diterapkan.

No	Pernyataan	Bobot	Tingkat Kemampuan					Nilai
			1	2	3	4	5	
1.	Terdapat suatu rancangan atau penerapan perlindungan secara fisik kepada aset dari adanya bencana alam, serangan atau kecelakaan yang berbahaya	1			✓			3
2.	Terdapat saran-saran dari ahli mengenai bagaimana cara untuk menghindari kerusakan dari segala ancaman seperti kebakaran, banjir, gempa bumi, ledakan, atau ancaman lain	1			✓			3
Total Bobot		2						3,00
A.11	**Keamanan Fisik dan Lingkungan**							
A.11.2	**Peralatan**							
A.11.2.2	**Utilitas Pendukung**							

Kontrol: Peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dalam mendukung utilitas

No	Pernyataan	Bobot	Tingkat Kemampuan					Nilai
			1	2	3	4	5	
1.	Tersedianya peraturan tentang sarana pendukung yang sesuai dengan spesifikasi peralatan dan persyaratan hukum organisasi	1			✓			3
2.	Penilaian sarana pendukung dilakukan secara teratur	1			✓			3
3.	Pemeriksaan dan pengujian aturan tentang sarana pendukung dilakukan secara teratur	1	✓					1
Total Bobot		3						2,33
A.11	**Keamanan Fisik dan Lingkungan**							

A.11.2	Peralatan
A.11.2.3	Keamanan Kabel

Kontrol: Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung harus dilindungi dari intersepsi, interferensi atau kerusakan

No	Pernyataan	Bobot	Tingkat Kemampuan					Nilai
			1	2	3	4	5	
1.	Terdapat peraturan tentang listrik dan jalur telekomunikasi ke fasilitas pengolahan informasi yang menyatakan harus dibawah tanah	1			✓			3
2.	Terdapat peraturan pemisahan antara kabel listrik dengan kabel komunikasi	1			✓			3
Total Bobot		2						3,00

A.11	Keamanan Fisik dan Lingkungan
A.11.2	Peralatan
A.11.2.4	Pemeliharaan Peralatan

Kontrol: Peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya yang berkelanjutan

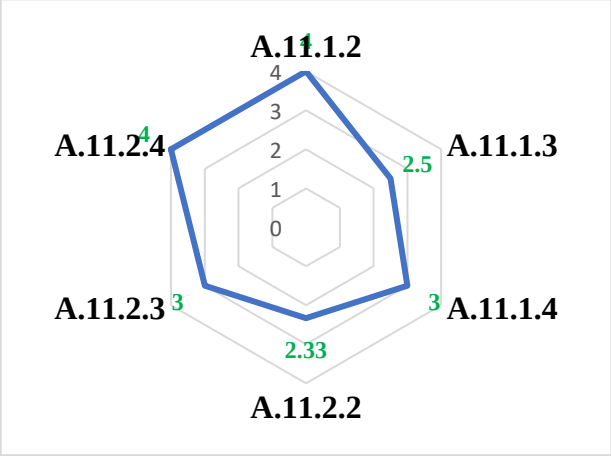
No	Pernyataan	Bobot	Tingkat Kemampuan					Nilai
			1	2	3	4	5	
1.	Terdapat peraturan mengenai spesifikasi peralatan dan pemeliharaan peralatan dalam *interval* yang direkomendasikan pemasok	1				✓		4
2.	Pemeliharaan atau perbaikan peralatan dilakukan oleh petugas yang berwenang	1				✓		4
3.	Pastikan seluruh peralatan berfungsi dengan baik sebelum mengoperasikan kembali setelah proses pemeriksaan dan pemeliharaan	1				✓		4
Total Bobot		3						4,00

Tabel 4.8 Hasil Perhitungan *Maturity Level* Klausul A.11 Keamanan Fisik dan Lingkungan

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
A.11 Keamanan Fisik dan Lingkungan	A.11.1 Area Aman	A.11.1.2 Kontrol Entri Fisik	4,00	3,16
		A.11.1.3 Mengamankan Kantor, Ruangan, dan Fasilitas	2,50	
		A.11.1.4 Melindungi Terhadap Ancaman Eksternal dan Lingkungan	3,00	
	A.11.2	A.11.2.2	2,33	3,11

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
	Peralatan	Utilitas Pendukung		
		A.11.2.3 Keamanan Kabel	3,00	
		A.11.2.4 Pemeliharaan Peralatan	4,00	
	***Maturity Level* Klausul A.11**			**3,13**

Berdasarkan hasil perhitungan *Maturity Level* yang penulis lakukan pada Klausul A.11 Keamanan Fisik dan Lingkungan, maka didapatkan nilai *Maturity Level* di PDAM Surya Sembada Kota Surabaya sebesar 3,13. Dari perolehan hasil nilai *Maturity Level* tersebut termasuk dalam *level* 3 yaitu *Well Defined* (Didefinisikan dengan baik). Hasil tersebut didapat karena pada kontrol keamanan A.11.1.2 terdapat 5 pernyataan mendapat nilai tingkat kemampuan 4, serta pada kontrol keamanan A.11.1.3 terdapat 2 pernyataan mendapat nilai tingkat kemampuan 2,5 pada kontrol keamanan A.11.1.4 terdapat 2 pernyataan dengan nilai tingkat kemampuan 3,0 serta pada kontrol kemanan A.11.2.2 terdapat 3 pernyataan mendapat nilai tingkat kemampuan 2,33, kontrol keamanan A.11.2.3 terdapat 2 pernyataan mendapat nilai tingkat kemampuan 3, dan pada kontrol keamanan A.11.2.4 terdapat 3 pernyataan mendapat nilai tingkat kemampuan 4. Di bawah ini merupakan grafik yang merepresentasikan nilai *Maturity Level* klausul A.11 Keamanan Fisik dan Lingkungan



Gambar 4.5 Representasi Nilai *Maturity Level* Klausul A.11 Keamanan Fisik dan Lingkungan

4.3.3 Klausul A.12 Keamanan Operasi

Tabel 4.9 Kerangka Kerja Perhitungan *Maturity Level* Klausul A.12 Keamanan Operasi

A.12	**Keamanan Operasi**			
A.12.2	**Perlindungan dari *Malware***			
A.12.2.1	**Kontrol Terhadap *Malware***			
Kontrol: Kontrol deteksi, pencegahan, dan pemulihan untuk melindungi terhadap *Malware* harus diterapkan, dikombinasikan dengan kesadaran pengguna yang sesuai				
No	**Pernyataan**	**Bobot**	**Tingkat Kemampuan**	**Nilai**

			1	2	3	4	5	
1.	Terdapat kebijakan mengenai penggunaan perangkat lunak yang resmi beserta pengontrolannya	1				✓		4
2.	Terdapat kontrol guna mencegah dan mendeteksi perangkat lunak yang tidak sah (*illegal*) serta penggunaan situs berbahaya yang dicurigai	1	✓					1
3.	Terdapat peraturan terkait dengan sumber yang digunakan untuk mendapatkan *file* dan *software* untuk mencegah risiko	1				✓		4
4.	Terdapat manajemen kerentanan terhadap *Malware*	1			✓			3
5.	Meninjau rutin perangkat lunak dan konten data sistem yang mendukung proses bisnis yang penting	1	✓					1
6.	Instalasi dan pembaharuan rutin *software* pendeteksi *Malware* serta perbaikan perangkat lunak untuk memindai komputer dan media	1				✓		4
7.	Terdapat SOP dan tanggung jawab untuk menangani perlindungan *Malware* pada sistem, pelatihan dalam penggunaan, pelaporan dan perbaikan dari serangan *Malware*	1				✓		4
8.	Terdapat prosedur mengumpulkan informasi tentang *Malware* baru secara teratur	1			✓			3
9.	Prosedur untuk memverifikasi informasi yang berkaitan dengan *Malware*	1			✓			3
Total Bobot		9						3,00
A.12	**Keamanan Operasi**							
A.12.3	***Backup***							
A.12.3.1	***Backup* Informasi**							

Kontrol: Salinan cadangan informasi, perangkat lunak dan gambar sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan yang disepakati

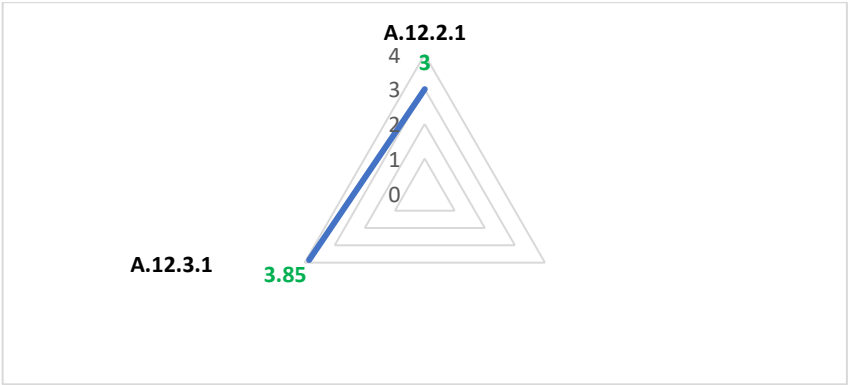
No	Pernyataan	Bobot	Tingkat Kemampuan					Nilai
			1	2	3	4	5	
1.	Kebijakan *Backup* informasi yang mencakup pertahanan dan perlindungan infrormasi	1				✓		4
2.	Tersedianya fasilitas *Backup* informasi yang memadai untuk memastikan informasi penting dapat dipulihkan setelah terjadi bencana atau kegagalan	1				✓		4

	media							
3.	Pencatatan *Backup* informasi yang akurat dan lengkap serta dokumentasi prosedur perbaikan	1				✓		4
4.	*Backup* di simpan di tempat yang aman dan jarak yang cukup	1				✓		4
5.	Tingkat perlindungan fisik dan lingkungan *Backup* informasi yang konsisten sesuai dengan standar yang diterapkan pada lokasi utama organisasi	1				✓		4
6.	Pengujian media *Backup* secara berkala	1				✓		4
7.	*Backup* menggunakan enkripsi dalam keadaan kerahasiaan sangat penting	1			✓			3
Total Bobot		7						3,85

Tabel 4.10 Hasil Perhitungan *Maturity Level* Klausul A.12 Keamanan Operasi

Klausul	**Objektif Kontrol**	**Kontrol Keamanan**	**Tingkat Kemampuan**	**Rata-rata Objektif Kontrol**
A.12 Keamanan Operasi	A.12.2 Perlindungan dari *Malware*	A.12.2.1 Kontrol Terhadap *Malware*	3,00	3,00
	A.12.3 *Backup*	A.12.3.1 *Backup* Informasi	3,85	3,85
	***Maturity Level* Klausul A.12**			**3,42**

Berdasarkan hasil perhitungan *Maturity Level* yang penulis lakukan pada Klausul A.12 Keamanan Operasi, maka didapatkan nilai *Maturity Level* di PDAM Surya Sembada Kota Surabaya sebesar 3,42. Dari hasil nilai *Maturity Level* tersebut termasuk dalam *level* 3 yaitu *Well Defined* (Didefinisikan dengan baik). Hasil itu didapat karena pada kontrol keamanan A.12.2.1 terdapat 9 pernyataan mendapat nilai tingkat kemampuan 3, serta pada kontrol keamanan A.12.3.1 terdapat 7 pernyataan mendapat nilai tingkat kemampuan 3,85 Di bawah ini merupakan grafik yang merepresentasikan nilai *Maturity Level* klausul A.12 Keamanan Operasi



Gambar 4.6 Representasi Nilai *Maturity Level* Klausul A.12 Keamanan Operasi

4.3.4 Klausul A.16 Manajemen Insiden Keamanan Informasi

Tabel 4.11 Kerangka Kerja Perhitungan *Maturity Level* Klausul A.16 Manajemen Insiden Keamanan Informasi

A.16	**Manajemen Insiden Keamanan Informasi**
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**
A.16.1.2	**Pelaporan Peristiwa Keamanan Informasi**

Kontrol: Kejadian keamanan informasi harus dilaporkan melalui saluran manajemen yang tepat secepat mungkin

No	**Pernyataan**	**Bobot**	**Tingkat Kemampuan**					**Nilai**
			1	**2**	**3**	**4**	**5**	
1.	Pegawai menyadari akan tanggung jawabnya untuk melaporkan kejadian keamanan informasi secepat mungkin	1				✓		4
2.	Terdapat prosedur untuk melaporkan kejadian keamanan informasi terkait dengan pelanggaran akses, malfungsi perangkat lunak atau perangkat keras, adanya perubahan sistem yang tidak terkendali	1				✓		4
Total Bobot		2						4,00

A.16	**Manajemen Insiden Keamanan Informasi**
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**
A.16.1.3	**Pelaporan Kelemahan Keamanan Informasi**

Kontrol: Karyawan dan kontraktor yang menggunakan sistem informasi dan layanan organisasi harus diminta untuk mencatat dan melaporkan setiap kelemahan keamanan sistem atau layanan yang diamati atau dicurigai

No	**Pernyataan**	**Bobot**	**Tingkat Kemampuan**					**Nilai**
			1	**2**	**3**	**4**	**5**	
1.	Terdapat arahan bagi karyawan maupun kontraktor untuk mencatat kelemahan keamanan sistem yang dicurigai	1				✓		4
2.	Terdapat mekanisme pelaporan kelemahan keamanan informasi yang mudah diakses	1				✓		4
Total Bobot		2						4,00

A.16	**Manajemen Insiden Keamanan Informasi**
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**
A.16.1.4	**Penilaian dan Keputusan tentang Kejadian Keamanan Informasi**

Kontrol: Kejadian keamanan informasi harus dinilai dan harus diputuskan apakah mereka harus diklasifikasikan sebagai insiden keamanan informasi

No	**Pernyataan**	**Bobot**	**Tingkat Kemampuan**					**Nilai**
			1	**2**	**3**	**4**	**5**	
1.	Penilaian titik kontak setiap peristiwa keamanan informasi menggunakan kejadiankeamanan informasi yang disepakati	1				✓		4
2.	Pengklasifikasian dan penentuan prioritas insiden dari skala klasifikasi insiden dilakukan	1				✓		4
3.	Hasil penilaian dan keputusan reasesmen	1	✓					1

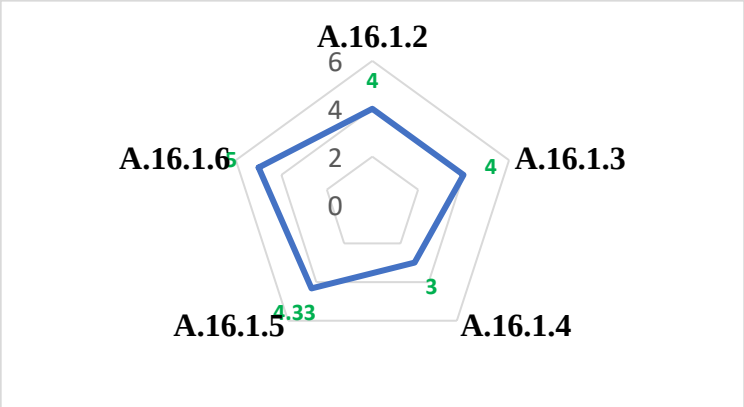
	dicatat secara rinci							
Total Bobot		3						3,00
A.16	**Manajemen Insiden Keamanan Informasi**							
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**							
A.16.1.5	**Respon Terhadap Insiden Keamanan Informasi**							
Kontrol: Insiden keamanan informasi harus ditanggapi sesuai dengan prosedur terdokumentasi								
No	**Pernyataan**	**Bobot**	**Tingkat Kemampuan**					**Nilai**
			1	**2**	**3**	**4**	**5**	
1.	Terdapat pengumpulan bukti sesegera mungkin setelah terjadinya insiden keamanan informasi	1				✓		4
2.	Terdapat prosedur untuk mengkomunikasikan keberadaan insiden keamanan informasi	1					✓	5
3.	Terdapat pencatatan insiden keamanan informasi untuk selanjutnya dilakukan analisis penyebab insiden keamanan infomasi	1				✓		4
Total Bobot		3						4,33
A.16	**Manajemen Insiden Keamanan Informasi**							
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**							
A.16.1.6	**Belajar Dari Insiden Keamanan Informasi**							
Kontrol: Pengetahuan yang diperoleh dari menganalisa dan menyelesaikan insiden keamanan informasi harus digunakan untuk mengurangi kemungkinan atau dampak dari insiden masa depan								
No	**Pernyataan**	**Bobot**	**Tingkat Kemampuan**					**Nilai**
			1	**2**	**3**	**4**	**5**	
1.	Terdapat mekanisme yang digunakan untuk mengukur dan memonitor jenis, frekuensi dan biaya insiden keamanan informasi	1					✓	5
2.	Evaluasi insiden keamanan informasi digunakan untuk meningkatkan kinerja keamanan serta membatasi frekuensi, kerusakan dan biaya kejadian di masa depan	1					✓	5
Total Bobot		2						5,00

Tabel 4.12 Hasil Perhitungan *Maturity Level* Klausul A.16 Manajemen Insiden Keamanan Informasi

Klausul	**Objektif Kontrol**	**Kontrol Keamanan**	**Tingkat Kemampuan**	**Rata-rata Objektif Kontrol**
A.16 Manajemen Insiden Keamanan Informasi	A.16.1 Manajemen Insiden Keamanan Informasi dan Perbaikan	A.16.1.2 Pelaporan Peristiwa Keamanan Informasi	4,00	4,06
		A.16.1.3 Pelaporan Kelemahan Keamanan Informasi	4,00	
		A.16.1.4	3,00	

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
		Penilaian dan Keputusan tentang Kejadian Keamanan Informasi		
		A.16.1.5 Respon Terhadap Insiden Keamanan Informasi	4,33	
		A.16.1.6 Belajar Dari Insiden Keamanan Informasi	5,00	
	***Maturity Level* Klausul A.16**			**4,06**

Berdasarkan hasil perhitungan *Maturity Level* yang penulis lakukan pada Klausul A.16 Manajemen Insiden Keamanan Informasi, didapatkan nilai *Maturity Level* di PDAM Surya Sembada Kota Surabaya sebesar 4,06. Dari hasil nilai *Maturity Level* tersebut maka termasuk dalam *level* 4 yaitu *Quantitatively Controlled* (Dikendalikan secara kuantitatif). Hasil itu didapat karena pada kontrol keamanan A.16.1.2 terdapat 2 pernyataan mendapat nilai tingkat kemampuan 4, serta pada kontrol keamanan A.16.1.3 terdapat 2 pernyataan mendapat nilai tingkat kemampuan 4, serta pada kontrol keamanan A.16.1.4 terdapat 3 pernyataan mendapat nilai tingkat kemampuan 3, kemudian pada kontrol keamanan A.16.1.5 terdapat 3 pernyataan mendapat nilai tingkat kemampuan 4,33 dan kontrol keamanan A.16.1.6 terdapat 2 pernyataan mendapat nilai tingkat kemampuan 5,0. Di bawah ini merupakan grafik yang merepresentasikan nilai *Maturity Level* klausul A.16 Manajemen Insiden Keamanan Informasi.



Gambar 4.7 Representasi Nilai *Maturity Level* Klausul A.16 Manajemen Insiden Keamanan Informasi

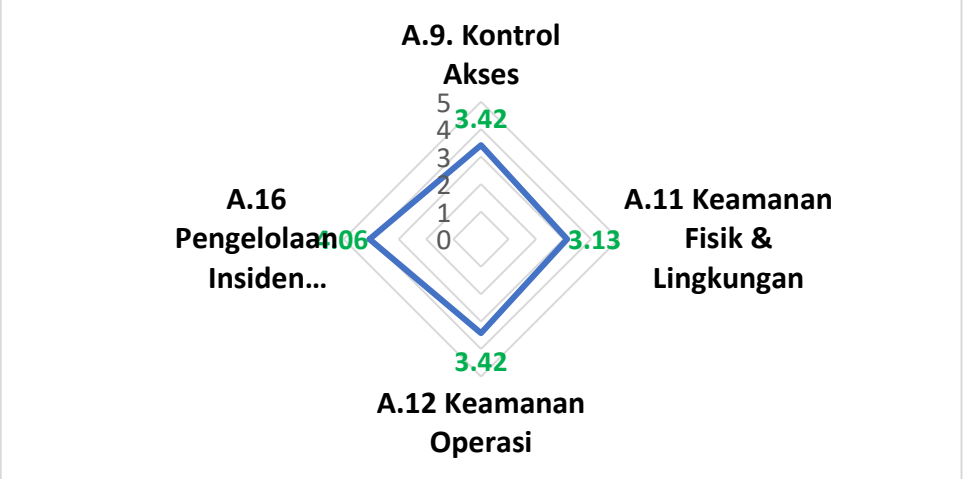
4.4 Penelusuran Bukti dan Rekomendasi

Setelah mengukur *Maturity Level* dari tiap-tiap objektif kontrol serta kontrol keamanan pada PDAM Surya Sembada Kota Surabaya, langkah selanjutnya yaitu melakukan penelusuran bukti terhadap pernyataan-pernyataan yang ada pada kontrol keamanan. Penelusuran bukti ini berguna untuk mensinkronkan / mencocokkan hasil nilai *Maturity Level* yang sudah diberikan oleh beberapa responden melalui kuesioner dengan kondisi sebenarnya yang ada pada PDAM Surya Sembada Kota Surabaya. Setelah tahap penelusuran bukti selesai dilakukan, maka langkah berikutnya adalah memberikan rekomendasi kepada PDAM Surya Sembada Kota

Surabaya untuk dapat mempebaiki serta meningkatkan kontrol keamanan informasi yang sesuai dengan standar ISO/IEC 27001:2013. Ringkasan perhitungan nilai rata-rata *Maturity Level* dari seluruh klausul yang ada pada sub bagian 4.3 akan dijelaskan di bawah ini.

Tabel 4.13 Hasil Perhitungan Nilai *Maturity Level* Seluruh Klausul

Klausul	***Maturity Level***
A.9 Kontrol Akses	3,42
A.11 Keamanan Fisik dan Lingkungan	3,13
A.12 Keamanan Operasi	3,42
A.16 Manajemen Insiden Keamanan Informasi	4,06
Nilai *Maturity Level*	**3,50 (*Well Defined*)**



Gambar 4.8 Representasi Nilai *Maturity Level* Seluruh Klausul

Dari hasil perhitungan keseluruhan klausul yang penulis gunakan didapatkan hasil nilai *Maturity Level* keseluruhan sebesar 3,5 yang artinya *Maturity Level* pada PDAM Surya Sembada Kota Surabaya berada dalam kategori *Well Defined* artinya kinerja pada *level* ini dilakukan sesuai dengan persetujuan, sesuai dengan standar yang telah ada, dan proses telah didokumentasikan, direncanakan dan dikelola dengan menggunakan standar yang ditetapkan organisasi, kinerja yang dilakukan telah mengacu pada standar ISO/IEC 27001:2013 tentang *system* manajemen keamanan informasi dalam tata kelola keamanan informasi, meskipun masih ada beberapa kontrol keamanan yang masih perlu ditingkatkan.

4.4.1 Penulusuran Bukti

Setelah melakukan penilaian *Maturity Level* serta merepresentasikan dalam bentuk grafik di atas, penulis melakukan penelusuran bukti terhadap dokumen

Tabel 4.14 Penelusuran Bukti Pada Klasul A.9 Kontrol Akses

A.9	**Kontrol Akses**
A.9.1	**Persyaratan Bisnis Terhadap Kontrol Akses**
A.9.1.1	**Kebijakan Kontrol Akses**
Kontrol: Kebijakan kontrol akses harus ditetapkan, didokumentasikan dan ditinjau	

berdasarkan persyaratan keamanan bisnis dan informasi					
No	**Pertanyaan**	**Dilakukan**		**Bukti**	***Gap***
		Ya	**Tidak**		
1.	Apakah pemilik aset menetapkan aturan akses kontrol yang tepat, hak akses dan pembatasan aturan pengguna terhadap aset yang dimiliki	✓		Terdapat formulir daftar akses terotorisasi (F-TIF-12-01) yang berisi nomor, nama, fungsi/jabatan, hak akses (R. NOC (*Network Operation Center*), R. Utilitas, R. *Networking*, R. *Server*, Ijin akses pihak ketiga), daftar akses terotorisasi terbagi menjadi 2 yaitu akses otorisasi pada *Data Center* dan aplikasi	-
2.	Apakah tersedia kebijakan kontrol akses yang bersifat fisik dan logis yang baik dan sudah dipertimbangakan secara bersama-sama	✓		Terdapat SOP pengelolaan akses pengguna *system* pada TSI (SOP-TIF-11) yang berisi pengelolaan pedoman pelaksanaan kegiatan pengelolaan akses pengguna *system* pada TSI dengan ruang lingkup bagian TSI	-
3.	Apakah terdapat kebijakan yang relevan dan kewajiban kontraktual apapun yang berkaitan dengan pembatasan akses ke data atau layanan	✓		Terdapat SOP pengelolaan akses pengguna *system* pada TSI (SOP-TIF-11) yang berisi pengelolaan pedoman pelaksanaan kegiatan pengelolaan akses pengguna *system* pada TSI dengan ruang lingkup bagian TSI	-
4.	Apakah terdapat tinjauan kembali hak akses secara berkala dan hak akses dihapus apabila tidak sesuai	✓		Terdapat form *review* hak akses (F-TIF-12-02) untuk me*review* hak akses apakah ada penambahan / pengurangan *user* pada aplikasi (cater dan e-proc) dan *Data Center*	-
A.9	**Kontrol Akses**				
A.9.1	**Persyaratan Bisnis Terhadap Kontrol Akses**				
A.9.1.2	**Akses ke Jaringan dan Layanan Jaringan**				
Kontrol: Pengguna hanya boleh diberikan akses ke jaringan dan layanan jaringan yang telah secara khusus diizinkan untuk digunakan.					
No	**Pertanyaan**	**Dilakukan**		**Bukti**	***Gap***
		Ya	**Tidak**		
1.	Apakah terdapat kebijakan yang mengatur jaringan dan layanan jaringan mana yang diizinkan untuk diakses	✓		Terdapat dokumen Standar keamanan jaringan (STD-TIF-04) yang berisi bahwa jaringan PDAM secara	-

				memadai dikelola dan dikendalikan untuk dilindungi dari ancaman, dan menjaga keamanan untuk *system* dan aplikasi yang menggunakan jaringan, dan penting untuk memastikan bahwa pelaksaanaan pengendalian keamanan jaringan di PDAM sudah konsisten	
2.	Apakah terdapat kebijakan yang mengatur otorisasi untuk menetapkan siapa yang diizinkan untuk mengakses jaringan atau layanan jaringan tertentu	✓		Terdapat dokumen Standar keamanan jaringan (STD-TIF-04) yang berisi bahwa jaringan PDAM secara memadai dikelola dan dikendalikan untuk dilindungi dari ancaman, dan menjaga keamanan untuk *system* dan aplikasi yang menggunakan jaringan, dan penting untuk memastikan bahwa pelaksaanaan pengendalian keamanan jaringan di PDAM sudah konsisten	-
3.	Apakah tersedia kebijakan yang mengatur tentang sarana yang dipakai untuk mengakses jaringan dan layanan jaringan (misalnya penggunaan VPN atau jaringan nirkabel)	✓		Terdapat dokumen Standar keamanan jaringan (STD-TIF-04) yang berisi bahwa jaringan PDAM secara memadai dikelola dan dikendalikan untuk dilindungi dari ancaman, dan menjaga keamanan untuk *system* dan aplikasi yang menggunakan jaringan, dan penting untuk memastikan bahwa pelaksaanaan pengendalian keamanan jaringan di PDAM sudah konsisten	-
4.	Apakah terdapat kebijakan yang mengatur syarat untuk autentikasi (validasi) pengguna untuk mengakses berbagai layanan jaringan	✓		Terdapat dokumen Standar keamanan jaringan (STD-TIF-04) yang berisi bahwa jaringan PDAM secara memadai dikelola dan dikendalikan untuk dilindungi dari ancaman, dan menjaga keamanan untuk	-

				system dan aplikasi yang menggunakan jaringan, dan penting untuk memastikan bahwa pelaksaanaan pengendalian keamanan jaringan di PDAM sudah konsisten	
5.	Apakah terdapat kebijakan yang mengatur pemantauan penggunaan layanan jaringan	✓		Terdapat dokumen standar manajemen *log* (STD-TIF-09) yang berisi agar bagian TSI mempunyai persyaratan minimal dalam hal audit *review log* untuk memantau sumber daya TI secara efektif dan efisien untuk mendeteksi potensi gangguan *security*, transaksi yang tidak sah dan kerusakan perangkat di PDAM, ruang lingkup bagaimana menangani kemanan jaringan di PDAM termasuk jaringan, *server*, dan *system* keamanan internet, kebijakan *firewall* serta hak admin	-

Tabel 4.15 Penelusuran Bukti Pada Klasul A.11 Keamanan Fisik dan Lingkungan

A.11	**Keamanan Fisik dan Lingkungan**				
A.11.1	**Area Aman**				
A.11.1.2	**Kontrol Entri Fisik**				
Kontrol: Area aman harus dilindungi oleh kontrol entri yang tepat untuk memastikan bahwa hanya personel yang berwenang yang diperbolehkan mengakses					
No	**Pertanyaan**	**Dilakukan**		**Bukti**	***Gap***
		Ya	**Tidak**		
1.	Apakah terdapat pencatatan tanggal dan waktu masuk dan keluarnya pengunjung dan terdapat pengawasan terhadap pengunjung	✓		Adanya buku tamu pada *Data Center* yang berisi tanggal dan waktu masuk / keluar kunjungan pada *Data Center*	-
2.	Apakah akses ke dalam tempat informasi rahasia diproses atau disimpan (Contoh: Ruang *server*) dibatasi untuk individu yang berwenang dengan menerapkan kontrol akses yang sesuai (Contoh: menggunakan kartu akses	✓		Adanya mesin *fingerprint* untuk akses masuk ke dalam *Data Center*	-

	atau *fingerprint*)				
3.	Apakah terdapat pemantauan dan penjagaan buku masuk fisik atau jejak audit elektronik dari semua akses	✓		Adanya buku tamu dan mesin *fingerprint* sebelum masuk kedalam ruangan	-
4.	Apakah semua pegawai atau pihak eksternal memakai tanda pengenal	✓		Terdapat kebijakan mengenai penggunaan kartu tanda pengenal / *name tag* untuk pegawai dan eksternal	-
5.	Apakah terdapat perbaharuan secara berkala tentang aturan hak akses untuk mengaman kan daerah yang aman	✓		Adanya SOP pengelolaan hak akses ruang *Data Center* (SOP-TIF-12), sebagai pedoman dalam proses manajemen hak akses ruang *Data Center* di PDAM, dengan ruang lingkup, bagian TSI dalam mengelola hak akses ruang *Data Center* sesuai *flowchart*, dan formulir daftar akses terotorisasi (F-TIF-12-01) yang berisi nomor, nama, fungsi/jabatan, hak akses (R. NOC, R. Utilitas, R. *Networking*, R. *Server*, Ijin akses pihak ketiga), daftar akses terotorisasi terbagi menjadi 2 yaitu akses otorisasi pada *Data Center* dan aplikasi dan form *review* hak akses (F-TIF-12-02) untuk me*review* hak akses apakah ada penambahan / pengurangan *user* pada aplikasi (cater dan e-proc) dan *Data Center*	-
A.11	**Keamanan Fisik dan Lingkungan**				
A.11.1	**Area Aman**				
A.11.1.3	**Mengamankan Kantor, Ruangan, dan Fasilitas**				
Kontrol: Keamanan fisik untuk kantor, kamar dan fasilitas harus dirancang dan diterapkan					

No	**Pertanyaan**	**Dilakukan**		**Bukti**	***Gap***
		Ya	**Tidak**		
1.	Apakah fasilitas utama telah ditempatkan di tempat yang aman dan tidak dapat diakses oleh publik	✓		Fasilitas utama yaitu *Data Center* telah ditempatkan di tempat tersembunyi dari jangkauan	-

				orang, dan tidak diketahui oleh umum	
2.	Apakah terdapat tanda baik di dalam atau di luar bangunan yang menunjukkan terdapat tempat pengelolaan dan pengolahan data atau informasi		✓	-	Berdasarkan kontrol pada A.11.1.3 keamanan fisik untuk bangunan harus diterapkan, untuk menunjukkan terdapat tempat pengelolaan dan pengolahan data atau informasi
A.11	**Keamanan Fisik dan Lingkungan**				
A.11.1	**Area Aman**				
A.11.1.4	**Melindungi Terhadap Ancaman Eksternal dan Lingkungan**				

Kontrol: Perlindungan fisik terhadap bencana alam, serangan atau kecelakaan yang berbahaya harus dirancang dan diterapkan.

No	**Pertanyaan**	**Dilakukan**		**Bukti**	***Gap***
		Ya	**Tidak**		
1.	Apakah terdapat suatu rancangan atau penerapan perlindungan secara fisik kepada aset dari adanya bencana alam, serangan atau kecelakaan yang berbahaya	✓		Terdapat SOP yang berisikan tentang SMK3 (Sistem Manajemen Keselamatan & Kesehatan Kerja) yang memuat perlindungan secara fisik kepada aset dari adanya bencana alam, serangan atau kecelakaan yang berbahaya	-
2.	Apakah terdapat saran-saran dari ahli mengenai bagaimana cara untuk menghindari kerusakan dari segala ancaman seperti kebakaran, banjir, gempa bumi, ledakan, atau ancaman lain	✓		Terdapat SOP yang berisikan tentang SMK3 (Sistem Manajemen Keselamatan & Kesehatan Kerja) yang memuat perlindungan secara fisik kepada aset dari adanya bencana alam, serangan atau kecelakaan yang berbahaya	-

A.11	Keamanan Fisik dan Lingkungan				
A.11.2	Peralatan				
A.11.2.2	Utilitas Pendukung				
Kontrol: Peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dalam mendukung utilitas					
No	**Pertanyaan**	**Dilakukan**		**Bukti**	***Gap***
		Ya	**Tidak**		
1.	Apakah tersedia peraturan tentang sarana pendukung yang sesuai dengan spesifikasi peralatan dan persyaratan hukum organisasi	✓		Adanya standar ruang *server* (STD-TIF-13) yang berisi panduan dalam mempersiapkan ruang *server* yang menjadi tanggung jawab bagian TSI, pedoman ini juga sebagai landasan dalam upaya meningkatkan keamanan dan kerahasaiaan *asset* di PDAM	-
2.	Apakah penilaian sarana pendukung telah dilakukan secara teratur	✓		Adanya standar ruang *server* (STD-TIF-13) yang berisi panduan dalam mempersiapkan ruang *server* yang menjadi tanggung jawab bagian TSI, pedoman ini juga sebagai landasan dalam upaya meningkatkan keamanan dan kerahasaiaan *asset* di PDAM	
3.	Apakah pemeriksaan dan pengujian aturan tentang sarana pendukung telah dilakukan secara teratur		✓	-	Berdasarkan kontrol A.11.2.2 peralatan harus diperiksa dan dilindungi dari segala gangguan untuk mencegah kegagalan dalam utilitas
A.11	**Keamanan Fisik dan Lingkungan**				

A.11.2	Peralatan
A.11.2.3	Keamanan Kabel

Kontrol: Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung harus dilindungi dari intersepsi, interferensi atau kerusakan

No	Pertanyaan	Dilakukan		Bukti	*Gap*
		Ya	Tidak		
1.	Apakah terdapat peraturan tentang listrik dan jalur telekomunikasi ke fasilitas pengolahan informasi yang menyatakan harus dibawah tanah	✓		Adanya standar ruang *server* (STD-TIF-13) yang berisi panduan dalam mempersiapkan ruang *server* yang menjadi tanggung jawab bagian TSI, pedoman ini juga sebagai landasan dalam upaya meningkatkan keamanan dan kerahasaiaan *asset* di PDAM	-
2.	Apakah terdapat peraturan pemisahan antara kabel listrik dengan kabel komunikasi	✓		Adanya standar ruang *server* (STD-TIF-13) yang berisi panduan dalam mempersiapkan ruang *server* yang menjadi tanggung jawab bagian TSI, pedoman ini juga sebagai landasan dalam upaya meningkatkan keamanan dan kerahasaiaan *asset* di PDAM	-

A.11	Keamanan Fisik dan Lingkungan
A.11.2	Peralatan
A.11.2.4	Pemeliharaan Peralatan

Kontrol: Peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya yang berkelanjutan

No	Pertanyaan	Dilakukan		Bukti	*Gap*
		Ya	Tidak		
1.	Apakah terdapat peraturan mengenai spesifikasi peralatan dan pemeliharaan peralatan dalam interval yang direkomendasikan pemasok	✓		Adanya surat perjanjian kontrak (SPK) untuk maintenance *Data Center* pada pihak ketiga, dikarenakan *maintenance* dilakukan oleh pihak ketiga / vendor	-
2.	Apakah pemeliharaan atau perbaikan peralatan dilakukan oleh petugas yang berwenang	✓		Adanya surat perjanjian kontrak (SPK) untuk maintenance *Data Center* pada pihak ketiga, dikarenakan *maintenance*	-

				dilakukan oleh pihak ketiga / vendor	
3.	Apakah telah dipastikan untuk seluruh peralatan berfungsi dengan baik sebelum mengoperasikan kembali setelah proses pemeriksaan dan pemeliharaan	✓		Adanya surat perjanjian kontrak (SPK) untuk maintenance *Data Center* pada pihak ketiga, dikarenakan *maintenance* dilakukan oleh pihak ketiga / vendor	-

Tabel 4.16 Penelusuran Bukti pada Klasul A.12 Keamanan Operasi

A.12	**Keamanan Operasi**				
A.12.2	**Perlindungan dari *Malware***				
A.12.2.1	**Kontrol Terhadap *Malware***				
Kontrol: Kontrol deteksi, pencegahan, dan pemulihan untuk melindungi terhadap *Malware* harus diterapkan, dikombinasikan dengan kesadaran pengguna yang sesuai					
No	**Pertanyaan**	**Dilakukan**		**Bukti**	***Gap***
		Ya	**Tidak**		
1.	Apakah terdapat kebijakan mengenai penggunaan perangkat lunak yang resmi beserta pengontrolannya	✓		Adanya dokumen *IT Policy* yang berisi tentang menggunakan perangkat lunak resmi	-
2.	Apakah terdapat kontrol guna mencegah dan mendeteksi perangkat lunak yang tidak sah (*illegal*) serta penggunaan situs berbahaya yang dicurigai		✓	-	Berdasarkan kontrol 12.2.1 harus ada kontrol yang diterapkan untuk mendeteksi serta melarang apabila ada yang menggunakan *software* yang *illegal* serta *phising* / situs berbahaya yang dicurigai
3.	Apakah terdapat peraturan terkait dengan sumber yang digunakan untuk mendapatkan *file* dan *software* untuk mencegah risiko	✓		Adanya dokumen *IT Policy* yang berisi tentang menggunakan perangkat lunak resmi dan adanya standar identifikasi *asset* informasi, *register* resiko	-

				dan rencana penanganan resiko keamanan informasi (STD-TIF-15) yang berisi menetapkan tanggung jawab dan proses identifikasi *asset* infromasi, *register* resiko keamanan informasi dan menetapkan rencana penanganan resiko keamanan informasi dan pemantauan resiko dengan ruang lingkup untuk semua kegiatan di PDAM	
4.	Apakah terdapat manajemen kerentanan terhadap *Malware*	✓		Terdapat standar anti *Malware* (STD-TIF-01) yang berisi melindungi informasi perusahaan terhadap ancaman dan gangguan *mailicious code* / *Malware* (*virus*, *worms*, *spyware* dll) di PDAM dengan dilakukannya *penetration testing*	-
5.	Apakah telah melakukan tinjauan rutin ke perangkat lunak dan konten data sistem yang mendukung proses bisnis yang penting		✓	-	Berdasarkan kontrol 12.2.1 seharusnya ada tinjauan rutin ke perangkat lunak

					dan konten data sistem yang mendukung proses bisnis yang penting dalam jangka waktu tertentu untuk memastikan *software* yang digunakan sesuai dengan kebutuhan organisasi
6.	Apakah telah dilakukannya instalasi dan pembaharuan rutin *software* pendeteksi *Malware* serta perbaikan perangkat lunak untuk memindai komputer dan media	✓		Pembaruan pada patch anti virus yang digunakan oleh perusahaan pada setiap tahunnya	-
7.	Apakah terdapat SOP dan tanggung jawab untuk menangani perlindungan *Malware* pada sistem, pelatihan dalam penggunaan, pelaporan dan perbaikan dari serangan *Malware*	✓		Terdapat standar anti *Malware* (STD-TIF-01) berisi melindungi informasi perusahaan terhadap ancaman dan gangguan *mailicious code* / *Malware* (*virus*, *worms*, *spyware* dll) di PDAM	-
8.	Apakah terdapat prosedur mengumpulkan informasi tentang *Malware* baru secara teratur	✓		Terdapat standar anti *Malware* (STD-TIF-01) berisi melindungi informasi perusahaan terhadap ancaman dan gangguan *mailicious code* / *Malware* (*virus*, *worms*, *spyware* dll) di PDAM	-

9.	Apakah terdapat prosedur untuk memverifikasi informasi yang berkaitan dengan *Malware*	✓		Terdapat standar anti *Malware* (STD-TIF-01) berisi melindungi informasi perusahaan terhadap ancaman dan gangguan *mailicious code* / *Malware* (*virus*, *worms*, *spyware* dll) di PDAM	-
A.12	**Keamanan Operasi**				
A.12.3	***Backup***				
A.12.3.1	***Backup* Informasi**				
Kontrol: Salinan cadangan informasi, perangkat lunak dan gambar sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan yang disepakati					
No	**Pertanyaan**	**Dilakukan**		**Bukti**	***Gap***
		Ya	**Tidak**		
1.	Apakah tersedia kebijakan *Backup* informasi yang mencakup pertahanan dan perlindungan informasi	✓		Terdapat standar *Backup* dan *restore* (STD-TIF-02) yang berisi bila terjadi masalah pada data asli yang mengakibatkan data asli tidak bisa diakses maka masih dapat mengakses data duplikasinya dan mengembalikan data seperti semula	-
2.	Apakah tersedia fasilitas *Backup* informasi yang memadai untuk memastikan informasi penting dapat dipulihkan setelah terjadi bencana atau kegagalan media	✓		Menggunakan aplikasi veeam untuk *Backup* informasi untuk memastikan informasi penting dapat dipulihkan setelah terjadi bencana atau kegagalan media	-
3.	Apakah terdapat pencatatan *Backup* informasi yang akurat dan lengkap serta dokumentasi prosedur perbaikan	✓		Adanya *indicator Backup* informasi setiap bulannya pada *Key Performance Indicator* (KPI) untuk *Backup* & *restore data*	-
4.	Apakah *Backup* telah di simpan di tempat yang aman dan jarak yang cukup	✓		Penerapan *Disaster Recovery Center* (DRC) untuk *Backup* informasi, yang berada di Jakarta dan di tempat yang aman	-

5.	Apakah tingkat perlindungan fisik dan lingkungan *Backup* informasi konsisten sesuai dengan standar yang diterapkan pada lokasi utama organisasi	✓		Penerapan *Disaster Recovery Center* (DRC) untuk *Backup* informasi, yang berada di Jakarta dan di tempat yang aman	-
6.	Apakah terdapat pengujian media *Backup* secara berkala	✓		Adanya indicator menguji media yang talah di *Backup* secara berkala, sebagaimana tertera pada *Key Performance Indicator* (KPI) untuk *restore database*	-
7.	Apakah *Backup* telah menggunakan enkripsi dalam keadaan kerahasiaan sangat penting	✓		Menggunakan aplikasi veeam untuk *Backup* informasi dengan enkripsi SSL (*Secure Socket Layer*)	-

Tabel 4.17 Penelusuran Bukti pada Klasul A.16 Manajemen Insiden Keamanan Informasi

A.16	**Manajemen Insiden Keamanan Informasi**				
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**				
A.16.1.2	**Pelaporan Peristiwa Keamanan Informasi**				
Kontrol: Kejadian keamanan informasi harus dilaporkan melalui saluran manajemen yang tepat secepat mungkin					
No	**Pertanyaan**	**Dilakukan**		**Bukti**	***Gap***
		Ya	**Tidak**		
1.	Apakah pegawai telah menyadari akan tanggung jawabnya untuk melaporkan kejadian keamanan informasi secepat mungkin	✓		Adanya training mengenai kesadaran akan sistem manajemen keamanan informasi (SMKI) untuk menyadari akan tanggung jawabnya untuk melaporkan kejadian keamanan informasi dan dokumen pakta integritas mengenai keamanan informasi	-
2.	Apakah terdapat prosedur untuk melaporkan kejadian keamanan informasi terkait dengan pelanggaran akses, malfungsi perangkat lunak atau perangkat keras, adanya perubahan sistem yang tidak terkendali	✓		Terdapat aplikasi IT Support untuk melaporkan kejadian keamanan informasi terkait dengan pelanggaran akses, malfungsi perangkat lunak atau perangkat keras, adanya perubahan sistem yang tidak terkendali	-
A.16	**Manajemen Insiden Keamanan Informasi**				
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**				
A.16.1.3	**Pelaporan Kelemahan Keamanan Informasi**				

Kontrol: Karyawan dan kontraktor yang menggunakan sistem informasi dan layanan organisasi harus diminta untuk mencatat dan melaporkan setiap kelemahan keamanan sistem atau layanan yang diamati atau dicurigai					
No	**Pertanyaan**	**Dilakukan**		**Bukti**	***Gap***
		Ya	**Tidak**		
1.	Apakah terdapat arahan bagi karyawan maupun kontraktor untuk mencatat kelemahan keamanan sistem yang dicurigai	✓		Adanya training mengenai kesadaran akan sistem manajemen keamanan informasi (SMKI) untuk mencatat kelemahan keamanan sistem yang dicurigai	-
2.	Apakah terdapat mekanisme pelaporan kelemahan keamanan informasi yang mudah diakses	✓		Terdapat SOP penanganan insiden keamanan informasi (SOP-TIF-22) yang berisi panduan dalam menentukan Langkah-langkah penanganan untuk mencegah berulangnya suatu insiden dikemudian hari, dan memastikan penanggulangan insiden dapat berjalan sesuai rencana dan IT *support* untuk pelaporan kelemahan pada keamanan informasi	-
A.16	**Manajemen Insiden Keamanan Informasi**				
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**				
A.16.1.4	**Penilaian dan Keputusan tentang Kejadian Keamanan Informasi**				
Kontrol: Kejadian keamanan informasi harus dinilai dan harus diputuskan apakah mereka harus diklasifikasikan sebagai insiden keamanan informasi					
No	**Pertanyaan**	**Dilakukan**		**Bukti**	***Gap***
		Ya	**Tidak**		
1.	Apakah telah dilakukan penilaian titik kontak setiap peristiwa keamanan informasi menggunakan kejadian keamanan informasi yang disepakati	✓		Terdapat form laporan insiden (F-TIF-22-01) yang berisi nama insiden, lokasi insiden dan keterangan dan form *checklist* evaluasi insiden keamanan informasi (F-TIF-22-02) berisi nama insiden, penyebab insiden asal insiden, tingkat prioritas insiden	-

				dan Tindakan perbaikan	
2.	Apakah terdapat pengklasifikasian dan penentuan prioritas insiden dari skala klasifikasi insiden dilakukan	✓		Adanya standar identifikasi *asset* informasi, *register* resiko dan rencana penanganan resiko keamanan informasi (STD-TIF-15) berisi untuk menetapkan tanggung jawab dan proses identifikasi *asset* infromasi, *register* resiko keamanan informasi dan menetapkan rencana penanganan resiko keamanan informasi dan pemantauan resiko dengan ruang lingkup untuk semua kegiatan di PDAM	-
3.	Apakah terdapat hasil penilaian dan keputusan reasesmen dicatat secara rinci		✓	-	Berdasarkan kontrol 16.1.4 dokumen hasil penilaian dan keputusan reasesmen dari insiden yang pernah terjadi harus dicatat secara rinci.
A.16	**Manajemen Insiden Keamanan Informasi**				
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**				
A.16.1.5	**Respon Terhadap Insiden Keamanan Informasi**				
Kontrol: Insiden keamanan informasi harus ditanggapi sesuai dengan prosedur terdokumentasi					

No	**Pertanyaan**	**Dilakukan**		**Bukti**	***Gap***
		Ya	**Tidak**		

1.	Apakah terdapat pengumpulan bukti sesegera mungkin setelah terjadinya insiden keamanan informasi	✓		Terdapat form laporan insiden (F-TIF-22-01) yang berisi nama insiden, lokasi insiden dan keterangan dan form *checklist* evaluasi insiden keamanan informasi (F-TIF-22-02) berisi nama insiden, penyebab insiden asal insiden, tingkat prioritas insiden dan tindakan perbaikan	-
2.	Apakah terdapat prosedur untuk mengkomunikasikan keberadaan insiden keamanan informasi	✓		Terdapat SOP penanganan insiden keamanan informasi (SOP-TIF-22) yang berisi panduan dalam menentukan langkah-langkah penanganan untuk mencegah berulangnya suatu insiden dikemudian hari, dan memastikan penanggulangan insiden dapat berjalan sesuai rencana	-
3.	Apakah terdapat pencatatan insiden keamanan informasi untuk selanjutnya dilakukan analisis penyebab insiden keamanan infomasi	✓		Terdapat form laporan insiden (F-TIF-22-01) yang berisi nama insiden, lokasi insiden dan keterangan	-
A.16	**Manajemen Insiden Keamanan Informasi**				
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**				
A.16.1.6	**Belajar Dari Insiden Keamanan Informasi**				
Kontrol: Pengetahuan yang diperoleh dari menganalisa dan menyelesaikan insiden keamanan informasi harus digunakan untuk mengurangi kemungkinan atau dampak dari insiden masa depan					
No	**Pertanyaan**	**Dilakukan**		**Bukti**	***Gap***
		Ya	**Tidak**		
1.	Apakah terdapat mekanisme yang digunakan untuk mengukur dan memonitor jenis, frekuensi dan biaya insiden keamanan informasi	✓		Terdapat SOP penanganan insiden keamanan informasi (SOP-TIF-22) yang berisi panduan dalam menentukan langkah-langkah penanganan untuk mencegah berulangnya suatu insiden dikemudian hari, dan memastikan penanggulangan insiden dapat berjalan sesuai rencana	-
2.	Apakah telah dilakukan suatu evaluasi insiden keamanan informasi	✓		Adanya form *checklist* evaluasi insiden keamanan informasi (F-TIF-22-02)	-

	digunakan untuk meningkatkan kinerja keamanan serta membatasi frekuensi, kerusakan dan biaya kejadian di masa depan			berisi nama insiden, penyebab insiden, asal insiden, tingkat prioritas insiden dan tindakan perbaikan	

4.4.2 Rekomendasi

Sebelum memberikan rekomendasi pada perusahaan, penulis menemukan beberapa *gap* untuk mengetahui apakah ada *gap* antara kondisi saat ini dengan panduan implementasi kontrol keamanan yang ada pada ISO/IEC 27001:2013, bahwa ISO/IEC 27001:2013 hanya sebagai panduan saja, tidak mengukur tingkat kematangan implementasi atau nilai *gap*. Untuk mengukur tingkat kematangan dipergunakan *framework* selain ISO/IEC 27001:2013 (ISO, 2013) (CMU, 2003). Berikut adalah tabel ringkasan *gap* yang ditemukan

Tabel 4.18 Ringkasan Gap yang Ditemukan

No	Kontrol Keamanan	*Gap*
1	A.11.1.3 Mengamankan Kantor, Ruangan, dan Fasilitas	Berdasarkan kontrol pada A.11.1.3 keamanan fisik untuk bangunan harus diterapkan, untuk menunjukkan terdapat tempat pengelolaan dan pengolahan data atau informasi
2	A.11.2.2 Utilitas Pendukung	Berdasarkan kontrol A.11.2.2 peralatan harus diperiksa dan dilindungi dari segala gangguan untuk mencegah kegagalan dalam utilitas
3	A.12.2.1 Kontrol Terhadap *Malware*	Berdasarkan kontrol A.12.2.1 harus ada kontrol yang diterapkan untuk mendeteksi serta melarang apabila ada yang menggunakan software yang *illegal* serta *phising* / situs berbahaya yang dicurigai dan Berdasarkan kontrol A.12.2.1 seharusnya ada tinjauan rutin ke perangkat lunak dan konten data sistem yang mendukung proses bisnis yang penting dalam jangka waktu tertentu untuk memastikan *software* yang digunakan sesuai dengan kebutuhan organisasi
4	A.16.1.4 Penilaian dan Keputusan tentang Kejadian Keamanan Informasi	Berdasarkan kontrol A.16.1.4 dokumen hasil penilaian dan keputusan reasesmen dari insiden yang pernah terjadi harus dicatat secara rinci

Mengacu dari *gap* yang ada dari 4 kontrol keamanan antara lain kontrol keamanan A.11.1.3 (Mengamankan Kantor, Ruangan, dan Fasilitas), A.11.2.2 (Utilitas Pendukung), A.12.2.1 (Kontrol Terhadap *Malware*), A.16.1.4 (Penilaian dan Keputusan tentang Kejadian Keamanan Informasi), selanjutnya penulis memberikan beberapa rekomendasi.

Tabel 4.19 merupakan beberapa rekomendasi yang dapat penulis berikan untuk dapat memperbaiki *gap* yang ada pada PDAM Surya Sembada Kota Surabaya.

Tabel 4.19 Rekomendasi untuk Memperbaiki *Gap* yang Ada di PDAM Surya Sembada Kota Surabaya

A.11	**Keamanan Fisik dan Lingkungan**
A.11.1	**Area Aman**
A.11.1.3	**Mengamankan Kantor, Ruangan, dan Fasilitas**
Rekomendasi	
- Berkaitan dengan kontrol A.11.1.3 sebaiknya pengelola memberikan petunjuk berupa tanda yang menerangkan bahwa terdapat tempat pengelolaan dan pengolahan data / informasi	
A.11	**Keamanan Fisik dan Lingkungan**
A.11.2	**Peralatan**
A.11.2.2	**Utilitas Pendukung**
Rekomendasi	
- Utilitas pendukung harus dinilai secara teratur untuk memastikan utilitas pendukung tersebut masih layak atau tidak	
A.12	**Keamanan Operasi**
A.12.2	**Perlindungan dari *Malware***
A.12.2.1	**Kontrol Terhadap *Malware***
Rekomendasi	
- Adanya peninjauan rutin terhadap *software* yang digunakan untuk memastikan *software* yang digunakan tersebut memang digunakan untuk mendukung kegiatan - Membuat peraturan tentang penggunaan perangkat lunak yang resmi karena masih ada beberapa komputer yang memakai perangkat lunak tidak resmi. - Membuat peraturan tentang *website* mana saja yang dapat digunakan apabila ingin men *download software*	
A.16	**Manajemen Insiden Keamanan Informasi**
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**
A.16.1.4	**Penilaian dan Keputusan tentang Kejadian Keamanan Informasi**
Rekomendasi	
- Menyediakan dokumen klasifikasi insiden apa saja yang menjadi prioritas utama	

Dari rekomendasi yang telah diberikan penulis tersebut dapat digunakan sebagai langkah untuk mengantisipasi dampak yang ditimbulkan jika suatu waktu terjadi insiden *hacking*. Dari rekomendasi yang telah diberikan penulis juga dapat digunakan sebagai dasaran untuk memperbaiki *gap* yang ada pada kontrol keamanan ISO/IEC 27001:2013 sebagai bahan untuk merencanakan SMKI sesuai standar ISO/IEC 27001:2013.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Pada penelitian ini penulis melakukan Evaluasi Tata kelola keamanan Informasi berdasar standar ISO/IEC 27001:2013 dengan menggunakan model / index SSE-CMM. Berdasarkan hasil pembahasan yang telah di bahas pada bab sebelumnya, maka dapat diambil kesimpulan, sebagai berikut:

1. Dari hasil perhitungan *Maturity Level* didapatkan hasil rata-rata dari 4 klausul ISO/IEC 27001:2013 yang digunakan adalah sebesar 3,5 yang mana hasil perhitungan *Maturity Level* tersebut menunjukkan kedalam kategori *Well Defined* artinya kinerja pada *level* ini dilakukan sesuai dengan persetujuan, sesuai dengan standar yang telah ada, dan proses telah didokumentasikan, direncanakan dan dikelola dengan menggunakan standar yang ditetapkan organisasi
2. Ditemukan beberapa *gap* yang ditemukan oleh penulis, diantaranya pada kontrol keamanan A.11.1.3 (Mengamankan Kantor, Ruangan, dan Fasilitas), A.11.2.2 (Utilitas Pendukung), A.12.2.1 (Kontrol Terhadap *Malware*), A.16.1.4 (Penilaian dan Keputusan tentang Kejadian Keamanan Informasi)
3. Beberapa *gap* yang ditemukan oleh penulis disebabkan karena adanya kegiatan pada bidang IT PDAM Surya Sembada Kota Surabaya belum memiliki peraturan dan prosedur pelaksanaan kegiatan secara tertulis dalam pengimplementasiannya
4. Dari hasil penelitian yang telah dilakukan oleh penulis, maka diberikan suatu rekomendasi pada beberapa kontrol keamanan, seperti kontrol keamanan A.11.1.3 (Mengamankan Kantor, Ruangan, dan Fasilitas), A.11.2.2 (Utilitas Pendukung), A.12.2.1 (Kontrol Terhadap *Malware*), A.16.1.4 (Penilaian dan Keputusan tentang Kejadian Keamanan Informasi) hal tersebut diatas untuk evaluasi terhadap insiden guna mencegah terjadinya insiden serupa yang pernah terjadi.

5.2 Saran

Berdasarkan kesimpulan dan analisa yang yang telah dilakukan sebelumnya, maka penulis memberikan saran, sebagai berikut:

1. Untuk dapat ditingkatkan dan ditekankan *core value* perusahaan yang dapat mempertahankan hasil yang telah dicapai.
2. Melakukan *monitoring* dan evaluasi tata kelola keamanan informasi untuk ditingkatkan terus menerus serta adanya proses perbaikan secara ber kesinambungan untuk mencapai *maturity level* yang lebih tinggi (*level* 4 atau *level* yang paling tinggi yaitu *level* 5)
3. Evaluasi Tata kelola Keamanan Informasi dalam penelitian ini menggunakan *framework* ISO 27001:2013 dan penilaian *maturity level* dengan menggunakan model SSE-CMM, maka untuk pengembangan penelitian selanjutnya disarankan dapat menggunakan penilaian *maturity level* dengan model lain, yaitu *Capability Maturity Model for Integration* (CMMI) COBIT sebagai bahan perbandingan.

DAFTAR PUSTAKA

Alfantookh, A. (2009). *An approach for the assessment of the application of ISO/IEC 27001:2013 essential information security controls*. Riyadh: King Saud University.

Apriandari, W., & Sasongko, A. (2018). Analisis sistem manajemen keamanan informasi menggunakan SNI ISO/IEC 27001:2013 pada Pemerintahan Daerah Kota Sukabumi (studi kasus: di Diskominfo Kota Sukabumi). *Santika Jurnal Ilmiah Sains dan Teknologi*, *8*(1), 715-729. https://doi.org/10.37150/jsa.v8i1.391

Arnason, S., & Willet, K. (2008). *How to achieve 27001 certification: An example of applied compliance management*. Auerbach Publications.

Bundesamt fur Sicherheit in der Informationstechnik. (2005). *IT security audit material for site surveys in critical infrastructures*. Jerman: Bundesamt fur Sicherheit in der Informationstechnik.

CMU. (2003). *A systems engineering capability maturity model (SE-CMM)*. Carnegie Mellon University.

CMU. (2013). *Systems security engineering capability maturity model (SSE-CMM)*. Carnegie Mellon University.

Direktorat Keamanan Informasi. (2017). *Panduan penerapan sistem manajemen keamanan informasi berbasis indeks keamanan informasi (indeks KAMI).* Jakarta: Direktorat Keamanan Informasi.

ECC International. (n.d.). *Information security management system*. Retrieved February 7, 2022, from https://eccinternational.com/consulting/data-security-management/information-security-management-*system*/

English Oxford Living Dictionary. (n.d.). *Evaluation*. Retrieved February 7, 2022, from https://en.oxforddictionaries.com/definition/evaluation

Gondodiyoto, S., & Hendarti, H. (2007). *Audit sistem informasi: Pendekatan cobIT*. Jakarta: Mitra Wacana Media.

IBISA. (2011). *Keamanan sistem informasi*. Yogyakarta: ANDI.

Islami, D. C., Bunga, K., & Candiwan. (2016). Kesadaran keamanan informasi pada pegawai bank X di Bandung Indonesia awareness information security employees X bank in Bandung Indonesia. *Jurnal INKOM*, *10*(1), 19-26. https://doi.org/10.14203/j.inkom.428

ISO. (2008). ISO/IEC 27005:2018: Information technology - Security techniques – Information security risk management. *IEC*, *27005*(27005).

ISO. (2013). ISO/IEC 27001:2013: Information technology - Security techniques - Information security management *system*s - Requirements. *IEC*, *27001*(27001).

Kamus Besar Bahasa Indonesia (KBBI). (n.d.). *Evaluasi*. Retrieved February 7, 2022, from https://kbbi.web.id/evaluasi

Kusuma, R. A. (2014). *Audit keamanan sistem informasi berdasarkan standar SNI-ISO/IEC 27001:2013 pada sistem informasi akademik Universitas Islam Negeri Sunan Kalijaga Yogyakarta*. Yogyakarta: UIN Sunan Kalijaga.

Marczyk, G. R. (2005). *Essentials of research design and methodology*. John Wiley & Sons.

McLeod, R., & Schell, G. P. (2008). *Management information systems*. Pearson/Prentice Hall.

Nurbojatmiko, Susanto, A., & Shobariah, E. (2016). Assessment of ISMS based on standard ISO/IEC 27001:2013 at DISKOMINFO Depok City. *2016 4th International Conference on Cyber and IT Service Management*, 1-6. https://doi.org/10.1109/CITSM.2016.7577471

Pengertian Ahli. (n.d.). *Pengertian evaluasi: Apa itu evaluasi?* Retrieved February 7, 2022, from https://pengertianahli.id/pengertian-evaluasi-apa-itu-evaluasi/

Putra, D. Y., Wati, T., & Widi, I. W. (2020). Audit keamanan sistem informasi berdasarkan SNI - ISO/IEC 27001:2013 pada sistem informasi akademik Universitas Pembangunan Nasional "Veteran" Jakarta. *SINAPTIKA, 1*(1), 1-18.

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information System Research*, *20*(1), 121-139. https://doi.org/10.1287/isre.1080.0174

Ritzkal, Goeritno, A., & Hendrawan, A. H. (2016). Implementasi ISO/IEC 27001:2013 untuk sistem manajemen keamanan informasi (SMKI) pada Fakultas Teknik UIKA-Bogor. *Seminar Nasional Sains dan Teknologi*, 1-5.

Sarno, R., & Iffano, I. (2009). *Sistem manajemen keamanan informasi berbasis ISO27001*. Surabaya: ITS Press.

Sugiyono. (2013). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Bandung: Alfabeta.

Sugiyono. (2014). *Metode penelitian pendidikan pendekatan kuantitatif. kualitatif, dan R&D*. Bandung: Alfabeta.

Surendro, K. (2009). *Implementasi tata kelola teknologi informasi*. Bandung: Informatika.

Susanto, H. (2011). I-SolFramework views on ISO/IEC 27001:2013: Information security management *system*: Refinement integrated solution's six domains. *Asian Transactions on Computers*, *1*(3), 1-10.

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awarness on information technology professionals' behavior. *Computers & Security*, *79*, 68-79. https://doi.org/10.1016/j.cose.2018.08.007

Umar, H. (2005). *Evaluasi kinerja perusahaan*. Jakarta: Gramedia Pustaka Utama.

Whitman, M. E., & Mattord, H. J. (2014). *Principles of information security*. Cengage Learning.

Williams, B. K. (2013). *Using information technology: A practical introduction to computers & communications*. McGraw-Hill.

LAMPIRAN A
PELAKSANAAN WAWANCARA

Responden	Nasrul Amir
Jabatan	Manajer Teknologi Sistem Informasi
Pewawancara	Dimas Pramudya Haqqi
Tanggal	5 April 2022
Tempat	Ruang TSI PDAM Surya Sembada Kota Surabaya

1	**P:**	Apakah tugas dari Bagian Teknologi Sistem Informasi (TSI) pada PDAM Surya Sembada Kota Surabaya?
	J:	Bagian yang mengelola Infrastruktur serta Sistem Informasi terkait *server*, pusat data, aplikasi , perangkat IT serta jaringan computer
2	**P:**	*Data Center*apa yang di kelola pada bagian Teknologi dan Sistem Informasi di PDAM Surya Sembada Kota Surabaya?
	J:	Semua data pelanggan dan perusahaan PDAM SURYA SEMBADA KOTA SURABAYA
3	**P:**	Apa saja contoh Tindakan untuk menjaga keamanan informasi yang sudah dilakukan?
	J:	Mengacu standar ISO/IEC 27001:2013 tentang Sistem Manajemen Keamanan Informasi
4	**P:**	Apakah ada SOP tertulis mengenai manajemen keamanan informasi?
	J:	Ada SOP yang dibuat untuk manajemen keamanan informasi
5	**P:**	Pada PDAM Surya Sembada Kota Surabaya pernakah terjadi ancaman atau insiden terkait dengan keamanan informasi? Insidennya sepertiapa, dan kapan?
	J:	Serangan *Ransomeware*, tahun 2021
6	**P:**	Adakah dampak/kerugian yang ditimbulkan dari ancaman/insiden yang pernah terjadi sebelumnya?
	J:	Dampak atau kerugian adalah kehilangan beberapa data yang belum sempat ter *Backup*

Responden	Nasrul Amir
Jabatan	Manajer Teknologi Sistem Informasi
Pewawancara	Dimas Pramudya Haqqi
Tanggal	6 April 2022
Tempat	SOCC PDAM Surya Sembada Kota Surabaya

1	**P:**	Apabila pernah terjadi insiden terkait dengan keamanan informasi, adakah langkah yang dilakukan untuk memperbaikinya? Dan apakah memerlukan biaya untuk memperbaikinya?

	J:	Memperkuat *system* keamanan di jaringan dan *firewall*, untuk memperbaiki ada yang butuh biaya ada yang tidak
2	**P:**	Apakah sejauh ini PDAM Surya Sembada Kota Surabaya pernah di evaluasi tata kelola dengan framework-framework yang ada? (Contoh menggunakan ISO/IEC 27001:2013, Cobit dll)
	J:	Menggunakan ISO/IEC 27001:2013 untuk persiapan penerapan SMKI
5	**P:**	Menurut anda perlukah dilakukan evaluasi terhadap *system* manajemen keamanan informasipada PDAM Surya Sembada ?
	J:	Perlu, karena harus dievaluasi untuk perbaikan yang berkelanjutan terkait *system* manajemen keamanan informasi
6	**P:**	Apakah pada PDAM Surya Sembada ini pernah melakukan edukasi dan pelatihan terhadap keamanan informasi kepada pegawai ?
	J:	Pernah melakukan *Awareness* terkait keamanan informasi dan penggunaan kata sandi
7	**P:**	Untuk *server* di PDAM Surya Sembada apakah ada *Backup* rutin untuk menjaga apabila suatu saat terjadi kerusakan *server* lagi, seperti yang pernah terjadi sebelumnya?
	J:	*Backup server* dan *database* rutin selalu dilakukan setiap hari

LAMPIRAN B
DAFTAR PERANGKAT EVALUASI TATA KELOLA KEAMANAN INFORMASI

A.9	**Kontrol Akses**
A.9.1	**Persyaratan Bisnis Terhadap Kontrol Akses**
A.9.1.1	**Kebijakan Kontrol Akses**

Kontrol: Kebijakan kontrol akses harus ditetapkan, didokumentasikan dan ditinjau berdasarkan persyaratan keamanan bisnis dan informasi

No	Pernyataan	Bobot	Tingkat Kemampuan					Nilai
			1	2	3	4	5	
1.	Pemilik aset dapat menetapkan aturan akses kontrol yang tepat, hak akses dan pembatasan aturan pengguna terhadap aset yang dimiliki							
2.	Tersedianya kebijakan kontrol akses yang bersifat fisik dan logis yang baik dan sudah dipertimbangakan secara bersama-sama							
3.	Terdapat kebijakan yang relevan dan kewajiban kontraktual apapun yang berkaitan dengan pembatasan akses ke data atau layanan							
4.	Terdapat tinjauan kembali hak akses secara berkala dan hak akses dihapus apabila tidak sesuai							
Total Bobot								

A.9	**Kontrol Akses**
A.9.1	**Persyaratan Bisnis Terhadap Kontrol Akses**
A.9.1.2	**Akses ke Jaringan dan Layanan Jaringan**

Kontrol: Pengguna hanya boleh diberikan akses ke jaringan dan layanan jaringan yang telah secara khusus diizinkan untuk digunakan.

No	Pernyataan	Bobot	Tingkat Kemampuan					Nilai
			1	2	3	4	5	
1.	Terdapat kebijakan yang mengatur jaringan dan layanan jaringan mana yang diizinkan untuk diakses							
2.	Terdapat kebijakan yang mengatur otorisasi untuk menetapkan siapa yang diizinkan untuk mengakses jaringan atau layanan jaringan tertentu							
3.	Tersedianya kebijakan yang mengatur tentang sarana yang dipakai untuk mengakses jaringan dan layanan jaringan (misalnya penggunaan VPN atau jaringan nirkabel)							
4.	Terdapat kebijakan yang mengatur syarat untuk autentikasi (validasi) pengguna untuk mengakses berbagai layanan jaringan							

5.	Terdapat kebijakan yang mengatur pemantauan penggunaan layanan jaringan							
Total Bobot								

A.11	**Keamanan Fisik dan Lingkungan**
A.11.1	**Area Aman**
A.11.1.2	**Kontrol Entri Fisik**

Kontrol: Area aman harus dilindungi oleh kontrol entri yang tepat untuk memastikan bahwa hanya personel yang berwenang yang diperbolehkan mengakses

No	**Pernyataan**	**Bobot**	**Tingkat Kemampuan**					**Nilai**
			1	**2**	**3**	**4**	**5**	
1.	Terdapat pencatatan tanggal dan waktu masuk dan keluarnya pengunjung dan terdapat pengawasan terhadap pengunjung							
2.	Akses ke daerah-daerah tempat informasi rahasia diproses atau disimpan (Contoh: Ruang *server*) harus dibatasi untuk individu yang berwenang dengan menerapkan kontrol akses yang sesuai (Contoh: menggunakan kartu akses atau *fingerprint*)							
3.	Pemantauan dan penjagaan buku masuk fisik atau jejak audit elektronik dari semua akses							
4.	Semua pegawai atau pihak eksternal memakai tanda pengenal							
5.	Perbaharuan secara berkala tentang aturan hak akses untuk mengamankan daerah yang aman							
Total Bobot								

A.11	**Keamanan Fisik dan Lingkungan**
A.11.1	**Area Aman**
A.11.1.3	**Mengamankan Kantor, Ruangan, dan Fasilitas**

Kontrol: Keamanan fisik untuk kantor, kamar dan fasilitas harus dirancang dan diterapkan

No	**Pernyataan**	**Bobot**	**Tingkat Kemampuan**					**Nilai**
			1	**2**	**3**	**4**	**5**	
1.	Fasilitas utama ditempatkan di tempat yang aman dan tidak dapat diakses oleh publik							
2.	Terdapat tanda baik di dalam atau di luar bangunan yang menunjukkan terdapat tempat pengelolaan dan pengolahan data atau informasi							
Total Bobot								

A.11	**Keamanan Fisik dan Lingkungan**
A.11.1	**Area Aman**
A.11.1.4	**Melindungi Terhadap Ancaman Eksternal dan Lingkungan**

Kontrol: Perlindungan fisik terhadap bencana alam, serangan atau kecelakaan yang berbahaya harus dirancang dan diterapkan.

No	Pernyataan	Bobot	Tingkat Kemampuan					Nilai
			1	2	3	4	5	
1.	Terdapat suatu rancangan atau penerapan perlindungan secara fisik kepada aset dari adanya bencana alam, serangan atau kecelakaan yang berbahaya							
2.	Terdapat saran-saran dari ahli mengenai bagaimana cara untuk menghindari kerusakan dari segala ancaman seperti kebakaran, banjir, gempa bumi, ledakan, atau ancaman lain							
Total Bobot								
A.11	**Keamanan Fisik dan Lingkungan**							
A.11.2	**Peralatan**							
A.11.2.2	**Utilitas Pendukung**							

Kontrol: Peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dalam mendukung utilitas

No	Pernyataan	Bobot	Tingkat Kemampuan					Nilai
			1	2	3	4	5	
1.	Tersedianya peraturan tentang sarana pendukung yang sesuai dengan spesifikasi peralatan dan persyaratan hukum organisasi							
2.	Penilaian sarana pendukung dilakukan secara teratur							
3.	Pemeriksaan dan pengujian aturan tentang sarana pendukung dilakukan secara teratur							
Total Bobot								
A.11	**Keamanan Fisik dan Lingkungan**							
A.11.2	**Peralatan**							
A.11.2.3	**Keamanan Kabel**							

Kontrol: Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung harus dilindungi dari intersepsi, interferensi atau kerusakan

No	Pernyataan	Bobot	Tingkat Kemampuan					Nilai
			1	2	3	4	5	
1.	Terdapat peraturan tentang listrik dan jalur telekomunikasi ke fasilitas pengolahan informasi yang menyatakan harus dibawah tanah							
2.	Terdapat peraturan pemisahan antara kabel listrik dengan kabel komunikasi							
Total Bobot								
A.11	**Keamanan Fisik dan Lingkungan**							
A.11.2	**Peralatan**							
A.11.2.4	**Pemeliharaan Peralatan**							

Kontrol: Peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya yang berkelanjutan

No	Pernyataan	Bobot	Tingkat Kemampuan	Nilai

			1	2	3	4	5	
1.	Terdapat peraturan mengenai spesifikasi peralatan dan pemeliharaan peralatan dalam interval yang direkomendasikan pemasok							
2.	Pemeliharaan atau perbaikan peralatan dilakukan oleh petugas yang berwenang							
3.	Pastikan seluruh peralatan berfungsi dengan baik sebelum mengoperasikan kembali setelah proses pemeriksaan dan pemeliharaan							
Total Bobot								
A.12	**Keamanan Operasi**							
A.12.2	**Perlindungan dari *Malware***							
A.12.2.1	**Kontrol Terhadap *Malware***							

Kontrol: Kontrol deteksi, pencegahan, dan pemulihan untuk melindungi terhadap *Malware* harus diterapkan, dikombinasikan dengan kesadaran pengguna yang sesuai

No	Pernyataan	Bobot	Tingkat Kemampuan					Nilai
			1	2	3	4	5	
1.	Terdapat kebijakan mengenai penggunaan perangkat lunak yang resmi beserta pengontrolannya							
2.	Terdapat kontrol guna mencegah dan mendeteksi perangkat lunak yang tidak sah (*illegal*) serta penggunaan situs berbahaya yang dicurigai							
3.	Terdapat peraturan terkait dengan sumber yang digunakan untuk mendapatkan *file* dan *software* untuk mencegah risiko							
4.	Terdapat manajemen kerentanan terhadap *Malware*							
5.	Meninjau rutin perangkat lunak dan konten data sistem yang mendukung proses bisnis yang penting							
6.	Instalasi dan pembaharuan rutin *software* pendeteksi *Malware* serta perbaikan perangkat lunak untuk memindai komputer dan media							
7.	Terdapat SOP dan tanggung jawab untuk menangani perlindungan *Malware* pada sistem, pelatihan dalam penggunaan, pelaporan dan perbaikan dari serangan *Malware*							
8.	Terdapat prosedur mengumpulkan informasi tentang *Malware* baru secara teratur							
9.	Prosedur untuk memverifikasi informasi yang berkaitan dengan *Malware*							
Total Bobot								
A.12	**Keamanan Operasi**							

A.12.3	***Backup***
A.12.3.1	***Backup* Informasi**

Kontrol: Salinan cadangan informasi, perangkat lunak dan gambar sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan yang disepakati

No	Pernyataan	Bobot	Tingkat Kemampuan					Nilai
			1	2	3	4	5	
1.	Kebijakan *Backup* informasi yang mencakup pertahanan dan perlindungan infrormasi							
2.	Tersedianya fasilitas *Backup* informasi yang memadai untuk memastikan informasi penting dapat dipulihkan setelah terjadi bencana atau kegagalan media							
3.	Pencatatan *Backup* informasi yang akurat dan lengkap serta dokumentasi prosedur perbaikan							
4.	*Backup* di simpan di tempat yang aman dan jarak yang cukup							
5.	Tingkat perlindungan fisik dan lingkungan *Backup* informasi yang konsisten sesuai dengan standar yang diterapkan pada lokasi utama organisasi							
6.	Pengujian media *Backup* secara berkala							
7.	*Backup* menggunakan enkripsi dalam keadaan kerahasiaan sangat penting							
Total Bobot								

A.16	**Manajemen Insiden Keamanan Informasi**
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**
A.16.1.2	**Pelaporan Peristiwa Keamanan Informasi**

Kontrol: Kejadian keamanan informasi harus dilaporkan melalui saluran manajemen yang tepat secepat mungkin

No	Pernyataan	Bobot	Tingkat Kemampuan					Nilai
			1	2	3	4	5	
1.	Pegawai menyadari akan tanggung jawabnya untuk melaporkan kejadian keamanan informasi secepat mungkin							
2.	Terdapat prosedur untuk melaporkan kejadian keamanan informasi terkait dengan pelanggaran akses, malfungsi perangkat lunak atau perangkat keras, adanya perubahan sistem yang tidak terkendali							
Total Bobot								

A.16	**Manajemen Insiden Keamanan Informasi**
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**
A.16.1.3	**Pelaporan Kelemahan Keamanan Informasi**

Kontrol: Karyawan dan kontraktor yang menggunakan sistem informasi dan layanan organisasi harus diminta untuk mencatat dan melaporkan setiap kelemahan keamanan sistem atau layanan yang diamati atau dicurigai

No	Pernyataan	Bobot	Tingkat Kemampuan	Nilai

			1	2	3	4	5	
1.	Terdapat arahan bagi karyawan maupun kontraktor untuk mencatat kelemahan keamanan sistem yang dicurigai							
2.	Terdapat mekanisme pelaporan kelemahan keamanan informasi yang mudah diakses							
Total Bobot								
A.16	**Manajemen Insiden Keamanan Informasi**							
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**							
A.16.1.4	**Penilaian dan Keputusan tentang Kejadian Keamanan Informasi**							
Kontrol: Kejadian keamanan informasi harus dinilai dan harus diputuskan apakah mereka harus diklasifikasikan sebagai insiden keamanan informasi								
No	**Pernyataan**	**Bobot**	**Tingkat Kemampuan**					**Nilai**
			1	**2**	**3**	**4**	**5**	
1.	Penilaian titik kontak setiap peristiwa keamanan informasi menggunakan kejadian keamanan informasi yang disepakati							
2.	Pengklasifikasian dan penentuan prioritas insiden dari skala klasifikasi insiden dilakukan							
3.	Hasil penilaian dan keputusan reasesmen dicatat secara rinci							
Total Bobot								
A.16	**Manajemen Insiden Keamanan Informasi**							
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**							
A.16.1.5	**Respon Terhadap Insiden Keamanan Informasi**							
Kontrol: Insiden keamanan informasi harus ditanggapi sesuai dengan prosedur terdokumentasi								
No	**Pernyataan**	**Bobot**	**Tingkat Kemampuan**					**Nilai**
			1	**2**	**3**	**4**	**5**	
1.	Terdapat pengumpulan bukti sesegera mungkin setelah terjadinya insiden keamanan informasi							
2.	Terdapat prosedur untuk mengkomunikasikan keberadaan insiden keamanan informasi							
3.	Terdapat pencatatan insiden keamanan informasi untuk selanjutnya dilakukan analisis penyebab insiden keamanan infomasi							
Total Bobot								

A.16	**Manajemen Insiden Keamanan Informasi**
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**
A.16.1.6	**Belajar Dari Insiden Keamanan Informasi**
Kontrol: Pengetahuan yang diperoleh dari menganalisa dan menyelesaikan insiden keamanan informasi harus digunakan untuk mengurangi kemungkinan atau dampak dari insiden masa depan	

No	**Pernyataan**	**Bobot**	**Tingkat Kemampuan**	**Nilai**

			1	2	3	4	5	
1.	Terdapat mekanisme yang digunakan untuk mengukur dan memonitor jenis, frekuensi dan biaya insiden keamanan informasi							
2.	Evaluasi insiden keamanan informasi digunakan untuk meningkatkan kinerja keamanan serta membatasi frekuensi, kerusakan dan biaya kejadian di masa depan							
Total Bobot								

LAMPIRAN C
DAFTAR PENELUSURAN BUKTI EVALUASI TATA KELOLA KEAMANAN INFROMASI

A.9	**Kontrol Akses**
A.9.1	**Persyaratan Bisnis Terhadap Kontrol Akses**
A.9.1.1	**Kebijakan Kontrol Akses**

Kontrol: Kebijakan kontrol akses harus ditetapkan, didokumentasikan dan ditinjau berdasarkan persyaratan keamanan bisnis dan informasi

No	Pertanyaan	Dilakukan		Bukti	*Gap*
		Ya	Tidak		
1.	Apakah pemilik aset menetapkan aturan akses kontrol yang tepat, hak akses dan pembatasan aturan pengguna terhadap aset yang dimiliki				
2.	Apakah tersedia kebijakan kontrol akses yang bersifat fisik dan logis yang baik dan sudah dipertimbangakan secara bersama-sama				
3.	Apakah terdapat kebijakan yang relevan dan kewajiban kontraktual apapun yang berkaitan dengan pembatasan akses ke data atau layanan				
4.	Apakah terdapat tinjauan kembali hak akses secara berkala dan hak akses dihapus apabila tidak sesuai				

A.9	**Kontrol Akses**
A.9.1	**Persyaratan Bisnis Terhadap Kontrol Akses**
A.9.1.2	**Akses ke Jaringan dan Layanan Jaringan**

Kontrol: Pengguna hanya boleh diberikan akses ke jaringan dan layanan jaringan yang telah secara khusus diizinkan untuk digunakan.

No	Pertanyaan	Dilakukan		Bukti	*Gap*
		Ya	Tidak		
1.	Apakah terdapat kebijakan yang mengatur jaringan dan layanan jaringan mana yang diizinkan untuk diakses				
2.	Apakah terdapat kebijakan yang mengatur otorisasi untuk menetapkan siapa yang diizinkan untuk mengakses jaringan atau layanan jaringan tertentu				
3.	Apakah tersedia kebijakan yang mengatur tentang sarana yang dipakai untuk mengakses jaringan				

	dan layanan jaringan (misalnya penggunaan VPN atau jaringan nirkabel)				
4.	Apakah terdapat kebijakan yang mengatur syarat untuk autentikasi (validasi) pengguna untuk mengakses berbagai layanan jaringan				
5.	Apakah terdapat kebijakan yang mengatur pemantauan penggunaan layanan jaringan				
A.11	**Keamanan Fisik dan Lingkungan**				
A.11.1	**Area Aman**				
A.11.1.2	**Kontrol Entri Fisik**				
Kontrol: Area aman harus dilindungi oleh kontrol entri yang tepat untuk memastikan bahwa hanya personel yang berwenang yang diperbolehkan mengakses					
No	**Pertanyaan**	**Dilakukan**		**Bukti**	***Gap***
		Ya	**Tidak**		
1.	Apakah terdapat pencatatan tanggal dan waktu masuk dan keluarnya pengunjung dan terdapat pengawasan terhadap pengunjung				
2.	Apakah akses ke dalam tempat informasi rahasia diproses atau disimpan (Contoh: Ruang *server*) dibatasi untuk individu yang berwenang dengan menerapkan kontrol akses yang sesuai (Contoh: menggunakan kartu akses atau *fingerprint*)				
3.	Apakah terdapat pemantauan dan penjagaan buku masuk fisik atau jejak audit elektronik dari semua akses				
4.	Apakah semua pegawai atau pihak eksternal memakai tanda pengenal				
5.	Apakah terdapat perbaharuan secara berkala tentang aturan hak akses untuk mengamankan daerah yang aman				
A.11	**Keamanan Fisik dan Lingkungan**				
A.11.1	**Area Aman**				
A.11.1.3	**Mengamankan Kantor, Ruangan, dan Fasilitas**				
Kontrol: Keamanan fisik untuk kantor, kamar dan fasilitas harus dirancang dan diterapkan					

No	Pertanyaan	Dilakukan		Bukti	*Gap*
		Ya	Tidak		
1.	Apakah fasilitas utama telah ditempatkan di tempat yang aman dan tidak dapat diakses oleh publik				
2.	Apakah terdapat tanda baik di dalam atau di luar bangunan yang menunjukkan terdapat tempat pengelolaan dan pengolahan data atau informasi				
A.11	**Keamanan Fisik dan Lingkungan**				
A.11.1	**Area Aman**				
A.11.1.4	**Melindungi Terhadap Ancaman Eksternal dan Lingkungan**				

Kontrol: Perlindungan fisik terhadap bencana alam, serangan atau kecelakaan yang berbahaya harus dirancang dan diterapkan.

No	Pertanyaan	Dilakukan		Bukti	*Gap*
		Ya	Tidak		
1.	Apakah terdapat suatu rancangan atau penerapan perlindungan secara fisik kepada aset dari adanya bencana alam, serangan atau kecelakaan yang berbahaya				
2.	Apakah terdapat saran-saran dari ahli mengenai bagaimana cara untuk menghindari kerusakan dari segala ancaman seperti kebakaran, banjir, gempa bumi, ledakan, atau ancaman lain				
A.11	**Keamanan Fisik dan Lingkungan**				
A.11.2	**Peralatan**				
A.11.2.2	**Utilitas Pendukung**				

Kontrol: Peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dalam mendukung utilitas

No	Pertanyaan	Dilakukan		Bukti	*Gap*
		Ya	Tidak		
1.	Apakah tersedia peraturan tentang sarana pendukung yang sesuai dengan spesifikasi peralatan dan persyaratan hukum organisasi				
2.	Apakah penilaian sarana pendukung telah dilakukan secara teratur				

3.	Apakah pemeriksaan dan pengujian aturan tentang sarana pendukung telah dilakukan secara teratur				
A.11	**Keamanan Fisik dan Lingkungan**				
A.11.2	**Peralatan**				
A.11.2.3	**Keamanan Kabel**				

Kontrol: Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung harus dilindungi dari intersepsi, interferensi atau kerusakan

No	**Pertanyaan**	**Dilakukan**		**Bukti**	***Gap***
		Ya	**Tidak**		
1.	Apakah terdapat peraturan tentang listrik dan jalur telekomunikasi ke fasilitas pengolahan informasi yang menyatakan harus dibawah tanah				
2.	Apakah terdapat peraturan pemisahan antara kabel listrik dengan kabel komunikasi				
A.11	**Keamanan Fisik dan Lingkungan**				
A.11.2	**Peralatan**				
A.11.2.4	**Pemeliharaan Peralatan**				

Kontrol: Peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya yang berkelanjutan

No	**Pertanyaan**	**Dilakukan**		**Bukti**	***Gap***
		Ya	**Tidak**		
1.	Apakah terdapat peraturan mengenai spesifikasi peralatan dan pemeliharaan peralatan dalam interval yang direkomendasikan pemasok				
2.	Apakah pemeliharaan atau perbaikan peralatan dilakukan oleh petugas yang berwenang				
3.	Apakah telah dipastikan untuk seluruh peralatan berfungsi dengan baik sebelum mengoperasikan kembali setelah proses pemeriksaan dan pemeliharaan				
A.12	**Keamanan Operasi**				
A.12.2	**Perlindungan dari *Malware***				
A.12.2.1	**Kontrol Terhadap *Malware***				

Kontrol: Kontrol deteksi, pencegahan, dan pemulihan untuk melindungi terhadap *Malware* harus diterapkan, dikombinasikan dengan kesadaran pengguna yang sesuai

No	Pertanyaan	Dilakukan		Bukti	*Gap*
		Ya	Tidak		
1.	Apakah terdapat kebijakan mengenai penggunaan perangkat lunak yang resmi beserta pengontrolannya				
2.	Apakah terdapat kontrol guna mencegah dan mendeteksi perangkat lunak yang tidak sah (*illegal*) serta penggunaan situs berbahaya yang dicurigai				
3.	Apakah terdapat peraturan terkait dengan sumber yang digunakan untuk mendapatkan *file* dan *software* untuk mencegah risiko				
4.	Apakah terdapat manajemen kerentanan terhadap *Malware*				
5.	Apakah telah melakukan tinjauan rutin ke perangkat lunak dan konten data sistem yang mendukung proses bisnis yang penting				
6.	Apakah telah dilakukannya instalasi dan pembaharuan rutin *software* pendeteksi *Malware* serta perbaikan perangkat lunak untuk memindai komputer dan media				
7.	Apakah terdapat SOP dan tanggung jawab untuk menangani perlindungan *Malware* pada sistem, pelatihan dalam penggunaan, pelaporan dan perbaikan dari serangan *Malware*				
8.	Apakah terdapat prosedur mengumpulkan informasi tentang *Malware* baru secara teratur				
9.	Apakah terdapat prosedur untuk memverifikasi informasi yang berkaitan dengan *Malware*				
A.12	**Keamanan Operasi**				
A.12.3	***Backup***				
A.12.3.1	***Backup* Informasi**				
Kontrol: Salinan cadangan informasi, perangkat lunak dan gambar sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan yang disepakati					

No	Pertanyaan	Dilakukan		Bukti	*Gap*
		Ya	Tidak		
1.	Apakah tersedia kebijakan *Backup* informasi yang mencakup pertahanan dan perlindungan informasi				
2.	Apakah tersedia fasilitas *Backup* informasi yang memadai untuk memastikan informasi penting dapat dipulihkan setelah terjadi bencana atau kegagalan media				
3.	Apakah terdapat pencatatan *Backup* informasi yang akurat dan lengkap serta dokumentasi prosedur perbaikan				
4.	Apakah *Backup* telah di simpan di tempat yang aman dan jarak yang cukup				
5.	Apakah tingkat perlindungan fisik dan lingkungan *Backup* informasi konsisten sesuai dengan standar yang diterapkan pada lokasi utama organisasi				
6.	Apakah terdapat pengujian media *Backup* secara berkala				
7.	Apakah *Backup* telah menggunakan enkripsi dalam keadaan kerahasiaan sangat penting				
A.16	**Manajemen Insiden Keamanan Informasi**				
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**				
A.16.1.2	**Pelaporan Peristiwa Keamanan Informasi**				

Kontrol: Kejadian keamanan informasi harus dilaporkan melalui saluran manajemen yang tepat secepat mungkin

No	Pertanyaan	Dilakukan		Bukti	*Gap*
		Ya	Tidak		
1.	Apakah pegawai telah menyadari akan tanggung jawabnya untuk melaporkan kejadian keamanan informasi secepat mungkin				
2.	Apakah terdapat prosedur untuk melaporkan kejadian keamanan informasi terkait dengan pelanggaran akses, malfungsi perangkat lunak atau perangkat keras, adanya perubahan sistem yang tidak terkendali				

A.16	Manajemen Insiden Keamanan Informasi
A.16.1	Manajemen Insiden Keamanan Informasi dan Perbaikan
A.16.1.3	Pelaporan Kelemahan Keamanan Informasi

Kontrol: Karyawan dan kontraktor yang menggunakan sistem informasi dan layanan organisasi harus diminta untuk mencatat dan melaporkan setiap kelemahan keamanan sistem atau layanan yang diamati atau dicurigai

No	Pertanyaan	Dilakukan		Bukti	*Gap*
		Ya	Tidak		
1.	Apakah terdapat arahan bagi karyawan maupun kontraktor untuk mencatat kelemahan keamanan sistem yang dicurigai				
2.	Apakah terdapat mekanisme pelaporan kelemahan keamanan informasi yang mudah diakses				

A.16	Manajemen Insiden Keamanan Informasi
A.16.1	Manajemen Insiden Keamanan Informasi dan Perbaikan
A.16.1.4	Penilaian dan Keputusan tentang Kejadian Keamanan Informasi

Kontrol: Kejadian keamanan informasi harus dinilai dan harus diputuskan apakah mereka harus diklasifikasikan sebagai insiden keamanan informasi

No	Pertanyaan	Dilakukan		Bukti	*Gap*
		Ya	Tidak		
1.	Apakah telah dilakukan penilaian titik kontak setiap peristiwa keamanan informasi menggunakan kejadian keamanan informasi yang disepakati				
2.	Apakah terdapat pengklasifikasian dan penentuan prioritas insiden dari skala klasifikasi insiden dilakukan				
3.	Apakah terdapat hasil penilaian dan keputusan reasesmen dicatat secara rinci				

A.16	Manajemen Insiden Keamanan Informasi
A.16.1	Manajemen Insiden Keamanan Informasi dan Perbaikan
A.16.1.5	Respon Terhadap Insiden Keamanan Informasi

Kontrol: Insiden keamanan informasi harus ditanggapi sesuai dengan prosedur terdokumentasi

No	Pertanyaan	Dilakukan		Bukti	*Gap*
		Ya	Tidak		
1.	Apakah terdapat pengumpulan bukti sesegera mungkin setelah terjadinya insiden keamanan informasi				

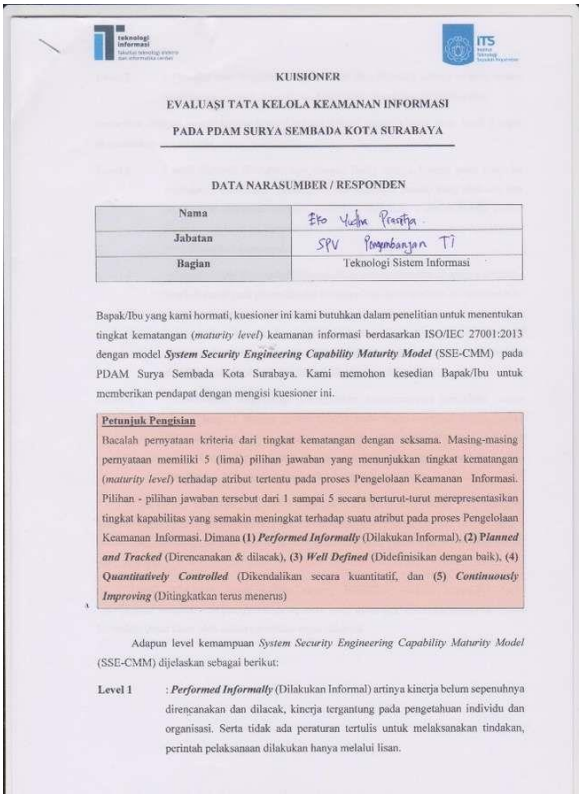
2.	Apakah terdapat prosedur untuk mengkomunikasikan keberadaan insiden keamanan informasi				
3.	Apakah terdapat pencatatan insiden keamanan informasi untuk selanjutnya dilakukan analisis penyebab insiden keamanan infomasi				
A.16	**Manajemen Insiden Keamanan Informasi**				
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**				
A.16.1.6	**Belajar Dari Insiden Keamanan Informasi**				

Kontrol: Pengetahuan yang diperoleh dari menganalisa dan menyelesaikan insiden keamanan informasi harus digunakan untuk mengurangi kemungkinan atau dampak dari insiden masa depan

No	**Pertanyaan**	**Dilakukan**		**Bukti**	***Gap***
		Ya	**Tidak**		
1.	Apakah terdapat mekanisme yang digunakan untuk mengukur dan memonitor jenis, frekuensi dan biaya insiden keamanan informasi				
2.	Apakah telah dilakukan suatu evaluasi insiden keamanan informasi digunakan untuk meningkatkan kinerja keamanan serta membatasi frekuensi, kerusakan dan biaya kejadian di masa depan				

LAMPIRAN D
DOKUMEN FISIK PENGISIAN PERANGKAT EVALUASI TATA KELOLA KEAMANAN INFORMASI

Supervisor Pengembangan Teknologi Informasi



KUISIONER

EVALUASI TATA KELOLA KEAMANAN INFORMASI

PADA PDAM SURYA SEMBADA KOTA SURABAYA

DATA NARASUMBER / RESPONDEN

Nama	Eko Yudha Pratama
Jabatan	SPV Pengembangan TI
Bagian	Teknologi Sistem Informasi

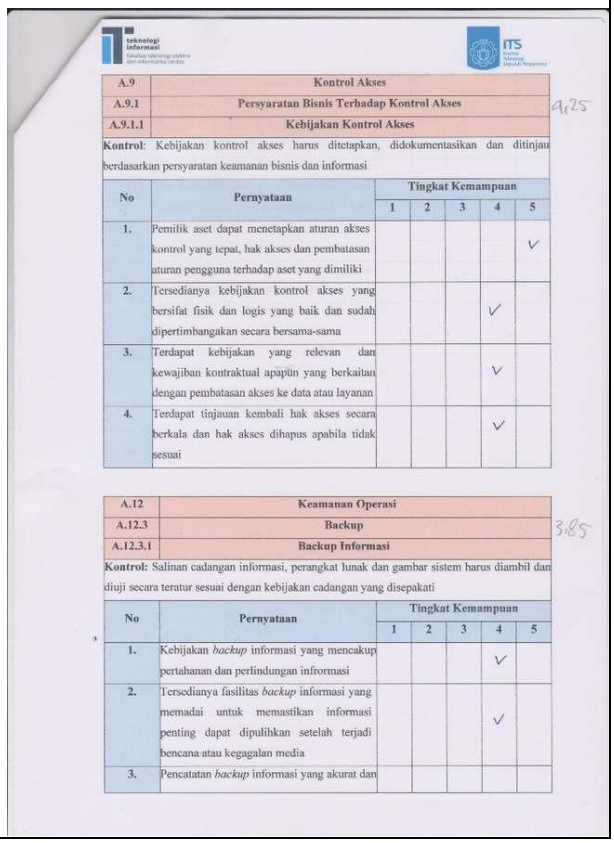
Bapak/Ibu yang kami hormati, kuesioner ini kami butuhkan dalam penelitian untuk menentukan tingkat kematangan (*maturity level*) keamanan informasi berdasarkan ISO/IEC 27001:2013 dengan model ***System Security Engineering Capability Maturity Model*** (SSE-CMM) pada PDAM Surya Sembada Kota Surabaya. Kami memohon kesedian Bapak/Ibu untuk memberikan pendapat dengan mengisi kuesioner ini.

Petunjuk Pengisian

Bacalah pernyataan kriteria dari tingkat kematangan dengan seksama. Masing-masing pernyataan memiliki 5 (lima) pilihan jawaban yang menunjukkan tingkat kematangan (*maturity level*) terhadap atribut tertentu pada proses Pengelolaan Keamanan Informasi. Pilihan - pilihan jawaban tersebut dari 1 sampai 5 secara berturut-turut merepresentasikan tingkat kapabilitas yang semakin meningkat terhadap suatu atribut pada proses Pengelolaan Keamanan Informasi. Dimana **(1)** ***Performed Informally*** (Dilakukan Informal), **(2)** ***Planned and Tracked*** (Direncanakan & dilacak), **(3)** ***Well Defined*** (Didefinisikan dengan baik), **(4)** ***Quantitatively Controlled*** (Dikendalikan secara kuantitatif, dan **(5)** ***Continuously Improving*** (Ditingkatkan terus menerus)

Adapun level kemampuan *System Security Engineering Capability Maturity Model* (SSE-CMM) dijelaskan sebagai berikut:

Level 1 : ***Performed Informally*** (Dilakukan Informal) artinya kinerja belum sepenuhnya direncanakan dan dilacak, kinerja tergantung pada pengetahuan individu dan organisasi. Serta tidak ada peraturan tertulis untuk melaksanakan tindakan, perintah pelaksanaan dilakukan hanya melalui lisan.



A.9	Kontrol Akses
A.9.1	Persyaratan Bisnis Terhadap Kontrol Akses
A.9.1.1	Kebijakan Kontrol Akses

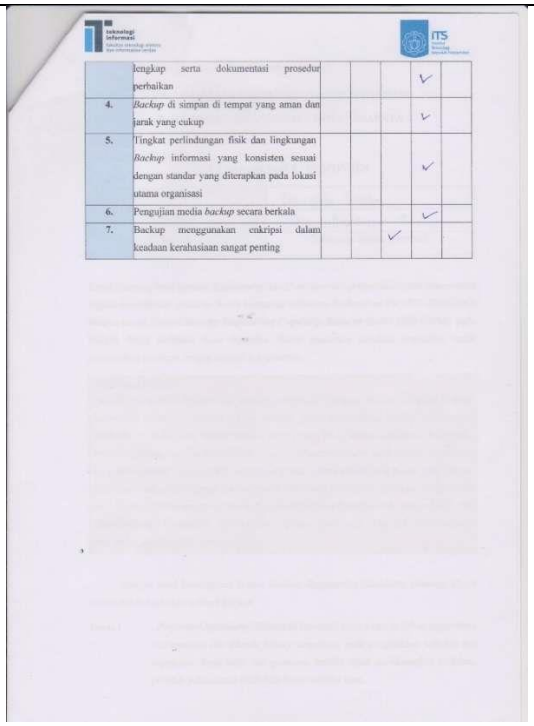
Kontrol: Kebijakan kontrol akses harus ditetapkan, didokumentasikan dan ditinjau berdasarkan persyaratan keamanan bisnis dan informasi

No	Pernyataan	Tingkat Kemampuan				
		1	2	3	4	5
1.	Pemilik aset dapat menetapkan aturan akses kontrol yang tepat, hak akses dan pembatasan aturan pengguna terhadap aset yang dimiliki					✓
2.	Tersedianya kebijakan kontrol akses yang bersifat fisik dan logis yang baik dan sudah dipertimbangakan secara bersama-sama				✓	
3.	Terdapat kebijakan yang relevan dan kewajiban kontraktual apapun yang berkaitan dengan pembatasan akses ke data atau layanan				✓	
4.	Terdapat tinjauan kembali hak akses secara berkala dan hak akses dihapus apabila tidak sesuai				✓	

A.12	Keamanan Operasi
A.12.3	Backup
A.12.3.1	Backup Informasi

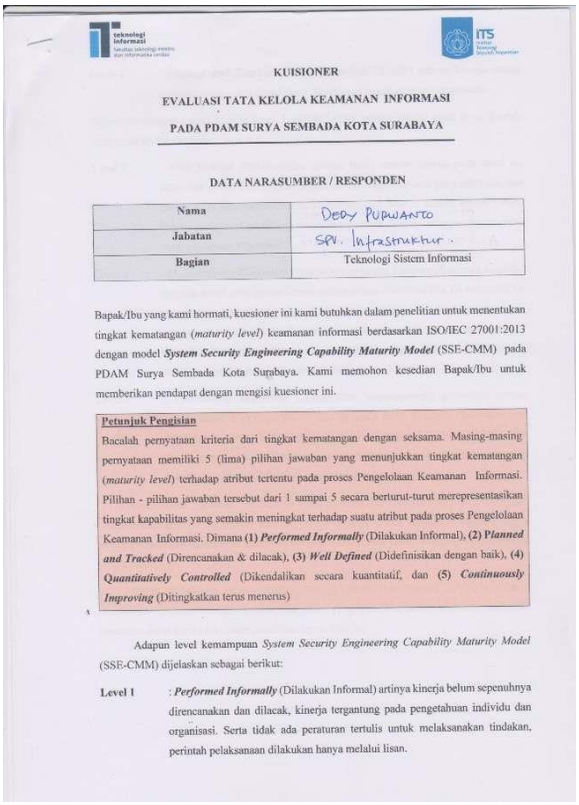
Kontrol: Salinan cadangan informasi, perangkat lunak dan gambar sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan yang disepakati

No	Pernyataan	Tingkat Kemampuan				
		1	2	3	4	5
1.	Kebijakan *backup* informasi yang mencakup pertahanan dan perlindungan infromasi				✓	
2.	Tersedianya fasilitas *backup* informasi yang memadai untuk memastikan informasi penting dapat dipulihkan setelah terjadi bencana atau kegagalan media				✓	
3.	Pencatatan *backup* informasi yang akurat dan					



	lengkap serta dokumentasi prosedur perbaikan				✓	
4.	*Backup* di simpan di tempat yang aman dan jarak yang cukup				✓	
5.	Tingkat perlindungan fisik dan lingkungan *Backup* informasi yang konsisten sesuai dengan standar yang diterapkan pada lokasi utama organisasi				✓	
6.	Pengujian media *backup* secara berkala				✓	
7.	Backup menggunakan enkripsi dalam keadaan kerahasiaan sangat penting			✓		

Supervisor Infrastruktur



KUISIONER

EVALUASI TATA KELOLA KEAMANAN INFORMASI

PADA PDAM SURYA SEMBADA KOTA SURABAYA

DATA NARASUMBER / RESPONDEN

Nama	Dedy Purwanto
Jabatan	Spv. Infrastruktur.
Bagian	Teknologi Sistem Informasi

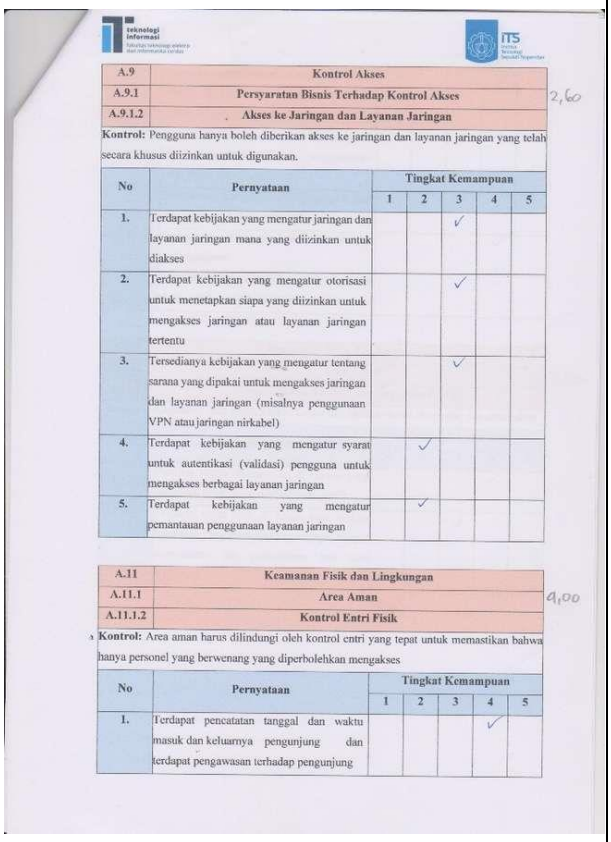
Bapak/Ibu yang kami hormati, kuesioner ini kami butuhkan dalam penelitian untuk menentukan tingkat kematangan (*maturity level*) keamanan informasi berdasarkan ISO/IEC 27001:2013 dengan model ***System Security Engineering Capability Maturity Model*** (SSE-CMM) pada PDAM Surya Sembada Kota Surabaya. Kami memohon kesedian Bapak/Ibu untuk memberikan pendapat dengan mengisi kuesioner ini.

Petunjuk Pengisian

Bacalah pernyataan kriteria dari tingkat kematangan dengan seksama. Masing-masing pernyataan memiliki 5 (lima) pilihan jawaban yang menunjukkan tingkat kematangan (*maturity level*) terhadap atribut tertentu pada proses Pengelolaan Keamanan Informasi. Pilihan - pilihan jawaban tersebut dari 1 sampai 5 secara berturut-turut merepresentasikan tingkat kapabilitas yang semakin meningkat terhadap suatu atribut pada proses Pengelolaan Keamanan Informasi. Dimana **(1)** ***Performed Informally*** (Dilakukan Informal), **(2)** ***Planned and Tracked*** (Direncanakan & dilacak), **(3)** ***Well Defined*** (Didefinisikan dengan baik), **(4)** ***Quantitatively Controlled*** (Dikendalikan secara kuantitatif, dan **(5)** ***Continuously Improving*** (Ditingkatkan terus menerus)

Adapun level kemampuan *System Security Engineering Capability Maturity Model* (SSE-CMM) dijelaskan sebagai berikut:

Level 1 : ***Performed Informally*** (Dilakukan Informal) artinya kinerja belum sepenuhnya direncanakan dan dilacak, kinerja tergantung pada pengetahuan individu dan organisasi. Serta tidak ada peraturan tertulis untuk melaksanakan tindakan, perintah pelaksanaan dilakukan hanya melalui lisan.



A.9	Kontrol Akses
A.9.1	Persyaratan Bisnis Terhadap Kontrol Akses
A.9.1.2	Akses ke Jaringan dan Layanan Jaringan

2,60

Kontrol: Pengguna hanya boleh diberikan akses ke jaringan dan layanan jaringan yang telah secara khusus diizinkan untuk digunakan.

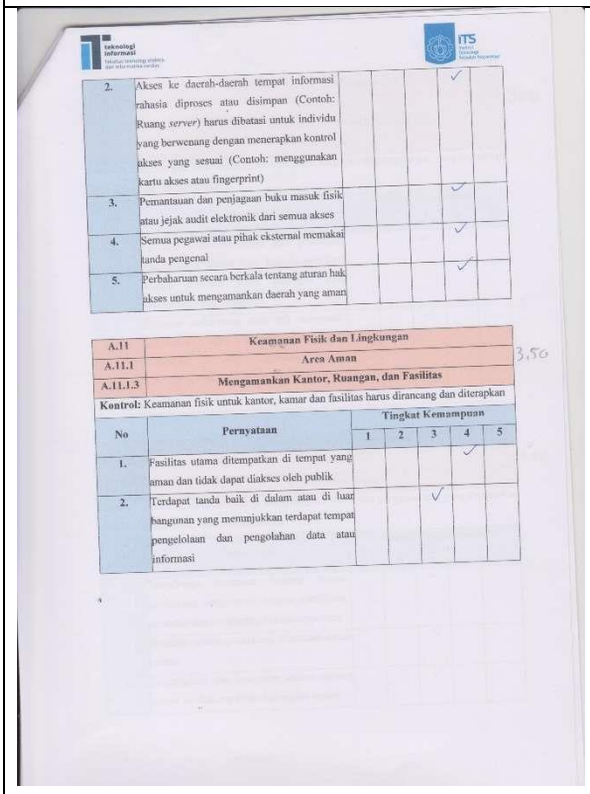
No	Pernyataan	Tingkat Kemampuan				
		1	2	3	4	5
1.	Terdapat kebijakan yang mengatur jaringan dan layanan jaringan mana yang diizinkan untuk diakses			✓		
2.	Terdapat kebijakan yang mengatur otorisasi untuk menetapkan siapa yang diizinkan untuk mengakses jaringan atau layanan jaringan tertentu			✓		
3.	Tersedianya kebijakan yang mengatur tentang sarana yang dipakai untuk mengakses jaringan dan layanan jaringan (misalnya penggunaan VPN atau jaringan nirkabel)			✓		
4.	Terdapat kebijakan yang mengatur syarat untuk autentikasi (validasi) pengguna untuk mengakses berbagai layanan jaringan		✓			
5.	Terdapat kebijakan yang mengatur pemantauan penggunaan layanan jaringan		✓			

A.11	Keamanan Fisik dan Lingkungan
A.11.1	Area Aman
A.11.1.2	Kontrol Entri Fisik

4,00

Kontrol: Area aman harus dilindungi oleh kontrol entri yang tepat untuk memastikan bahwa hanya personel yang berwenang yang diperbolehkan mengakses

No	Pernyataan	Tingkat Kemampuan				
		1	2	3	4	5
1.	Terdapat pencatatan tanggal dan waktu masuk dan keluarnya pengunjung dan terdapat pengawasan terhadap pengunjung				✓	



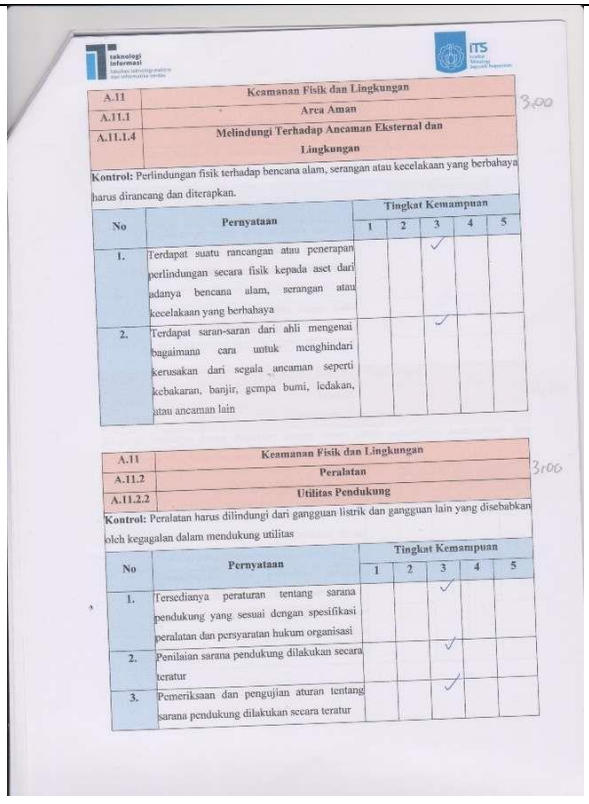
2.	Akses ke daerah-daerah tempat informasi rahasia diproses atau disimpan (Contoh: Ruang *server*) harus dibatasi untuk individu yang berwenang dengan menerapkan kontrol akses yang sesuai (Contoh: menggunakan kartu akses atau fingerprint)				✓	
3.	Pemantauan dan penjagaan buku masuk fisik atau jejak audit elektronik dari semua akses				✓	
4.	Semua pegawai atau pihak eksternal memakai tanda pengenal				✓	
5.	Perbaharuan secara berkala tentang aturan hak akses untuk mengamankan daerah yang aman				✓	

A.11	Keamanan Fisik dan Lingkungan
A.11.1	Area Aman
A.11.1.3	Mengamankan Kantor, Ruangan, dan Fasilitas

3,50

Kontrol: Keamanan fisik untuk kantor, kamar dan fasilitas harus dirancang dan diterapkan

No	Pernyataan	Tingkat Kemampuan				
		1	2	3	4	5
1.	Fasilitas utama ditempatkan di tempat yang aman dan tidak dapat diakses oleh publik				✓	
2.	Terdapat tanda baik di dalam atau di luar bangunan yang menunjukkan terdapat tempat pengelolaan dan pengolahan data atau informasi			✓		



A.11	Keamanan Fisik dan Lingkungan
A.11.1	Area Aman
A.11.1.4	Melindungi Terhadap Ancaman Eksternal dan Lingkungan

3,00

Kontrol: Perlindungan fisik terhadap bencana alam, serangan atau kecelakaan yang berbahaya harus dirancang dan diterapkan.

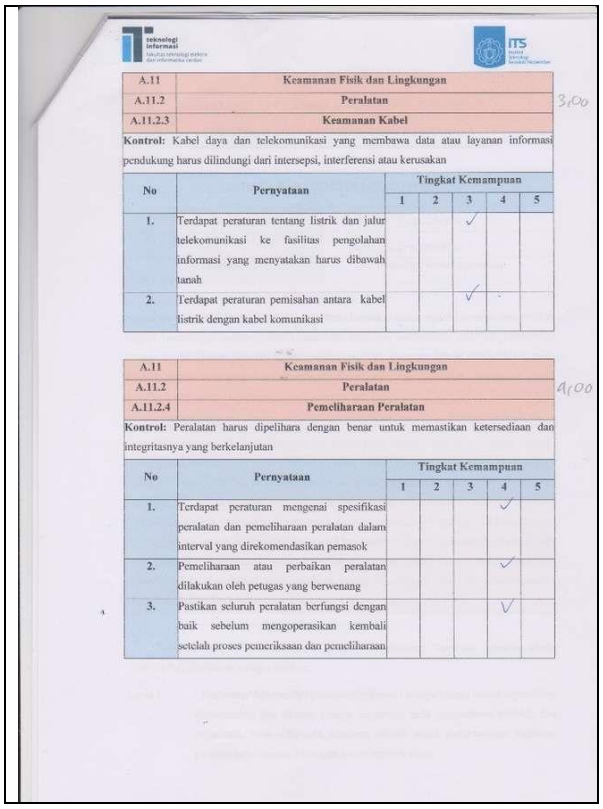
No	Pernyataan	Tingkat Kemampuan				
		1	2	3	4	5
1.	Terdapat suatu rancangan atau penerapan perlindungan secara fisik kepada aset dari adanya bencana alam, serangan atau kecelakaan yang berbahaya			✓		
2.	Terdapat saran-saran dari ahli mengenai bagaimana cara untuk menghindari kerusakan dari segala ancaman seperti kebakaran, banjir, gempa bumi, ledakan, atau ancaman lain			✓		

A.11	Keamanan Fisik dan Lingkungan
A.11.2	Peralatan
A.11.2.2	Utilitas Pendukung

3,00

Kontrol: Peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dalam mendukung utilitas

No	Pernyataan	Tingkat Kemampuan				
		1	2	3	4	5
1.	Tersedianya peraturan tentang sarana pendukung yang sesuai dengan spesifikasi peralatan dan persyaratan hukum organisasi			✓		
2.	Penilaian sarana pendukung dilakukan secara teratur			✓		
3.	Pemeriksaan dan pengujian aturan tentang sarana pendukung dilakukan secara teratur			✓		



A.11	Keamanan Fisik dan Lingkungan
A.11.2	Peralatan
A.11.2.3	Keamanan Kabel

Kontrol: Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung harus dilindungi dari intersepsi, interferensi atau kerusakan

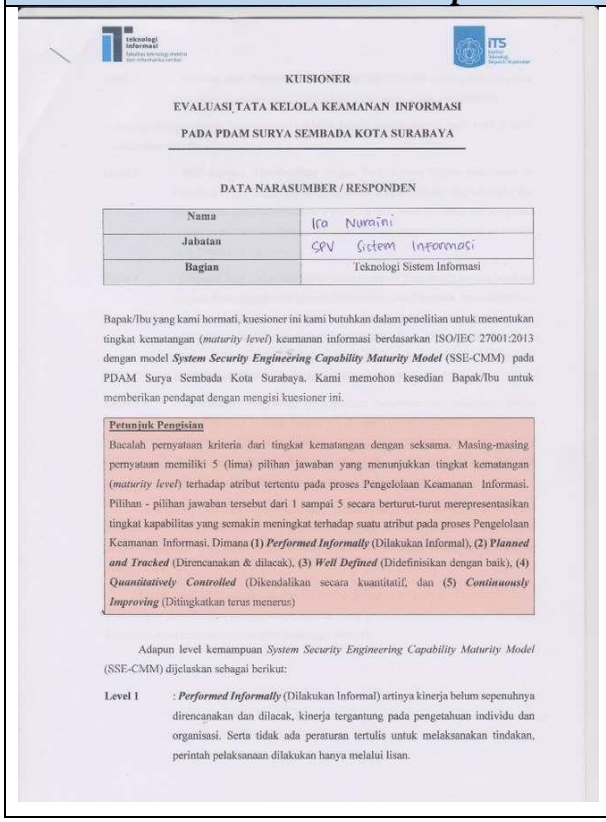
No	Pernyataan	Tingkat Kemampuan				
		1	2	3	4	5
1.	Terdapat peraturan tentang listrik dan jalur telekomunikasi ke fasilitas pengolahan informasi yang menyatakan harus dibawah tanah			✓		
2.	Terdapat peraturan pemisahan antara kabel listrik dengan kabel komunikasi			✓		

A.11	Keamanan Fisik dan Lingkungan
A.11.2	Peralatan
A.11.2.4	Pemeliharaan Peralatan

Kontrol: Peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya yang berkelanjutan

No	Pernyataan	Tingkat Kemampuan				
		1	2	3	4	5
1.	Terdapat peraturan mengenai spesifikasi peralatan dan pemeliharaan peralatan dalam interval yang direkomendasikan pemasok				✓	
2.	Pemeliharaan atau perbaikan peralatan dilakukan oleh petugas yang berwenang				✓	
3.	Pastikan seluruh peralatan berfungsi dengan baik sebelum mengoperasikan kembali setelah proses pemeriksaan dan pemeliharaan				✓	

Supervisor Sistem Informasi



KUISIONER

EVALUASI TATA KELOLA KEAMANAN INFORMASI

PADA PDAM SURYA SEMBADA KOTA SURABAYA

DATA NARASUMBER / RESPONDEN

Nama	Ira Nuraini
Jabatan	SPV Sistem Informasi
Bagian	Teknologi Sistem Informasi

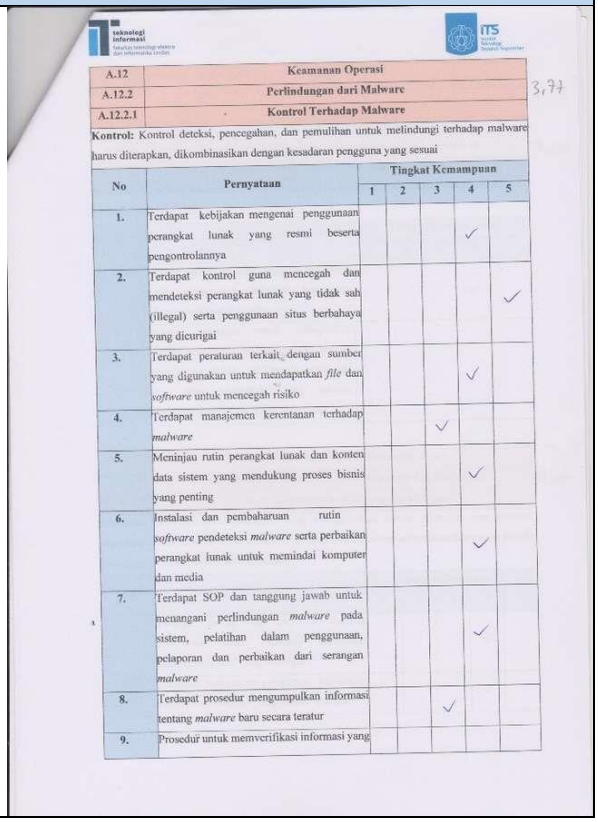
Bapak/Ibu yang kami hormati, kuesioner ini kami butuhkan dalam penelitian untuk menentukan tingkat kematangan (*maturity level*) keamanan informasi berdasarkan ISO/IEC 27001:2013 dengan model ***System Security Engineering Capability Maturity Model*** (SSE-CMM) pada PDAM Surya Sembada Kota Surabaya. Kami memohon kesedian Bapak/Ibu untuk memberikan pendapat dengan mengisi kuesioner ini.

Petunjuk Pengisian

Bacalah pernyataan kriteria dari tingkat kematangan dengan seksama. Masing-masing pernyataan memiliki 5 (lima) pilihan jawaban yang menunjukkan tingkat kematangan (*maturity level*) terhadap atribut tertentu pada proses Pengelolaan Keamanan Informasi. Pilihan - pilihan jawaban tersebut dari 1 sampai 5 secara berturut-turut merepresentasikan tingkat kapabilitas yang semakin meningkat terhadap suatu atribut pada proses Pengelolaan Keamanan Informasi. Dimana **(1)** ***Performed Informally*** (Dilakukan Informal), **(2)** ***Planned and Tracked*** (Direncanakan & dilacak), **(3)** ***Well Defined*** (Didefinisikan dengan baik), **(4)** ***Quantitatively Controlled*** (Dikendalikan secara kuantitatif, dan **(5)** ***Continuously Improving*** (Ditingkatkan terus menerus)

Adapun level kemampuan *System Security Engineering Capability Maturity Model* (SSE-CMM) dijelaskan sebagai berikut:

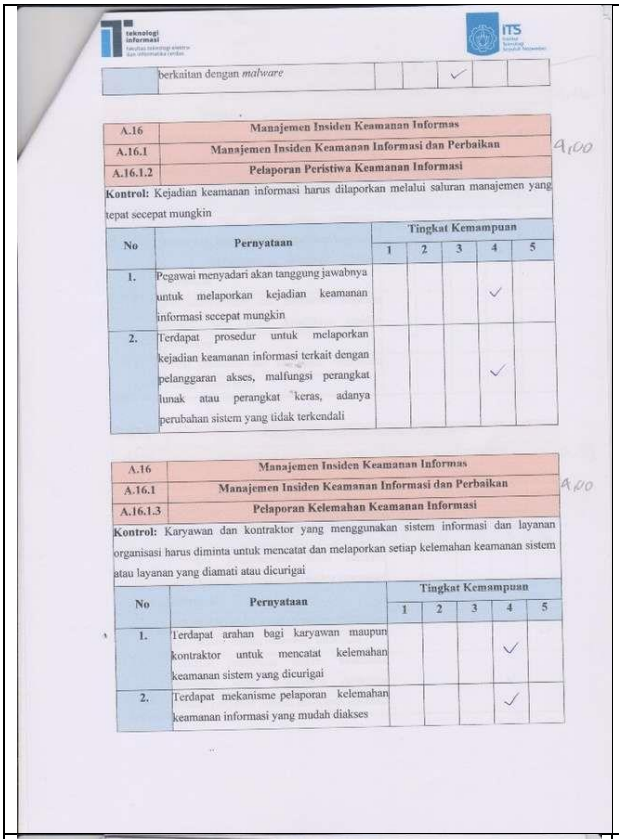
Level 1 : ***Performed Informally*** (Dilakukan Informal) artinya kinerja belum sepenuhnya direncanakan dan dilacak, kinerja tergantung pada pengetahuan individu dan organisasi. Serta tidak ada peraturan tertulis untuk melaksanakan tindakan, perintah pelaksanaan dilakukan hanya melalui lisan.



A.12	Keamanan Operasi
A.12.2	Perlindungan dari Malware
A.12.2.1	Kontrol Terhadap Malware

Kontrol: Kontrol deteksi, pencegahan, dan pemulihan untuk melindungi terhadap malware harus diterapkan, dikombinasikan dengan kesadaran pengguna yang sesuai

No	Pernyataan	Tingkat Kemampuan				
		1	2	3	4	5
1.	Terdapat kebijakan mengenai penggunaan perangkat lunak yang resmi beserta pengontrolannya				✓	
2.	Terdapat kontrol guna mencegah dan mendeteksi perangkat lunak yang tidak sah (illegal) serta penggunaan situs berbahaya yang dicurigai					✓
3.	Terdapat peraturan terkait dengan sumber yang digunakan untuk mendapatkan *file* dan *software* untuk mencegah risiko				✓	
4.	Terdapat manajemen kerentanan terhadap *malware*			✓		
5.	Meninjau rutin perangkat lunak dan konten data sistem yang mendukung proses bisnis yang penting				✓	
6.	Instalasi dan pembaharuan rutin *software* pendeteksi *malware* serta perbaikan perangkat lunak untuk memindai komputer dan media				✓	
7.	Terdapat SOP dan tanggung jawab untuk menangani perlindungan *malware* pada sistem, pelatihan dalam penggunaan, pelaporan dan perbaikan dari serangan *malware*				✓	
8.	Terdapat prosedur mengumpulkan informasi tentang *malware* baru secara teratur			✓		
9.	Prosedur untuk memverifikasi informasi yang					



	berkaitan dengan *malware*			✓		

A.16	Manajemen Insiden Keamanan Informas
A.16.1	Manajemen Insiden Keamanan Informasi dan Perbaikan
A.16.1.2	Pelaporan Peristiwa Keamanan Informasi

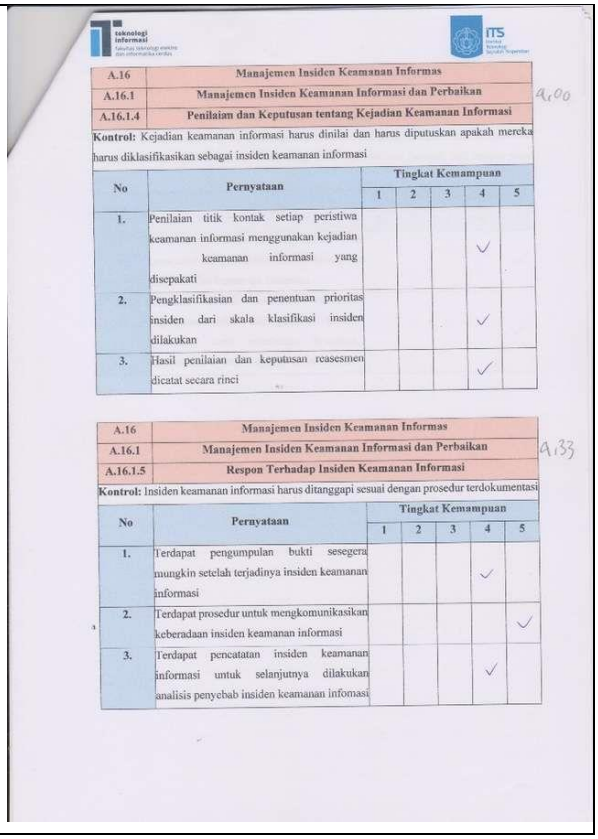
Kontrol: Kejadian keamanan informasi harus dilaporkan melalui saluran manajemen yang tepat secepat mungkin

No	Pernyataan	Tingkat Kemampuan				
		1	2	3	4	5
1.	Pegawai menyadari akan tanggung jawabnya untuk melaporkan kejadian keamanan informasi secepat mungkin				✓	
2.	Terdapat prosedur untuk melaporkan kejadian keamanan informasi terkait dengan pelanggaran akses, malfungsi perangkat lunak atau perangkat keras, adanya perubahan sistem yang tidak terkendali				✓	

A.16	Manajemen Insiden Keamanan Informas
A.16.1	Manajemen Insiden Keamanan Informasi dan Perbaikan
A.16.1.3	Pelaporan Kelemahan Keamanan Informasi

Kontrol: Karyawan dan kontraktor yang menggunakan sistem informasi dan layanan organisasi harus diminta untuk mencatat dan melaporkan setiap kelemahan keamanan sistem atau layanan yang diamati atau dicurigai

No	Pernyataan	Tingkat Kemampuan				
		1	2	3	4	5
1.	Terdapat arahan bagi karyawan maupun kontraktor untuk mencatat kelemahan keamanan sistem yang dicurigai				✓	
2.	Terdapat mekanisme pelaporan kelemahan keamanan informasi yang mudah diakses				✓	



A.16	Manajemen Insiden Keamanan Informas
A.16.1	Manajemen Insiden Keamanan Informasi dan Perbaikan
A.16.1.4	Penilaian dan Keputusan tentang Kejadian Keamanan Informasi

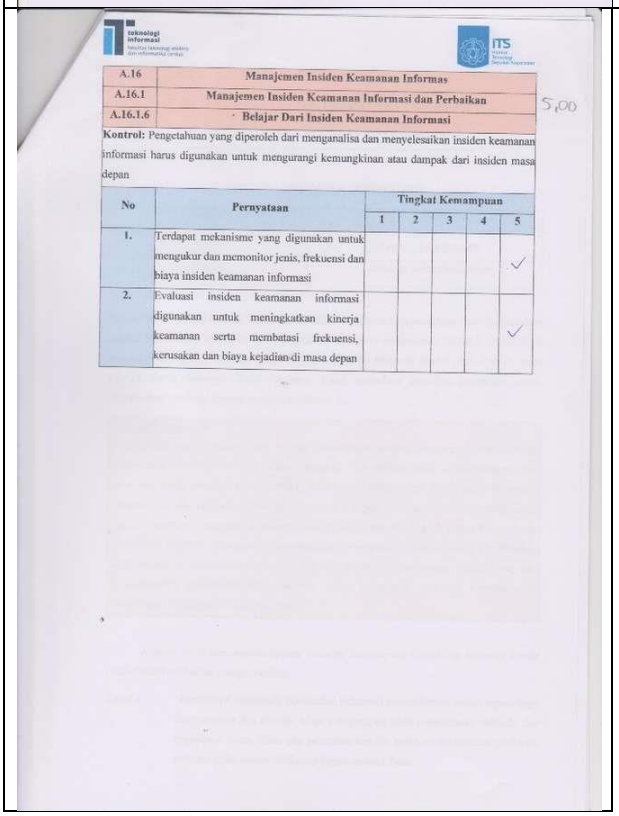
Kontrol: Kejadian keamanan informasi harus dinilai dan harus diputuskan apakah mereka harus diklasifikasikan sebagai insiden keamanan informasi

No	Pernyataan	Tingkat Kemampuan				
		1	2	3	4	5
1.	Penilaian titik kontak setiap peristiwa keamanan informasi menggunakan kejadian keamanan informasi yang disepakati				✓	
2.	Pengklasifikasian dan penentuan prioritas insiden dari skala klasifikasi insiden dilakukan				✓	
3.	Hasil penilaian dan keputusan reasesmen dicatat secara rinci				✓	

A.16	Manajemen Insiden Keamanan Informas
A.16.1	Manajemen Insiden Keamanan Informasi dan Perbaikan
A.16.1.5	Respon Terhadap Insiden Keamanan Informasi

Kontrol: Insiden keamanan informasi harus ditanggapi sesuai dengan prosedur terdokumentasi

No	Pernyataan	Tingkat Kemampuan				
		1	2	3	4	5
1.	Terdapat pengumpulan bukti sesegera mungkin setelah terjadinya insiden keamanan informasi				✓	
2.	Terdapat prosedur untuk mengkomunikasikan keberadaan insiden keamanan informasi					✓
3.	Terdapat pencatatan insiden keamanan informasi untuk selanjutnya dilakukan analisis penyebab insiden keamanan infomasi				✓	

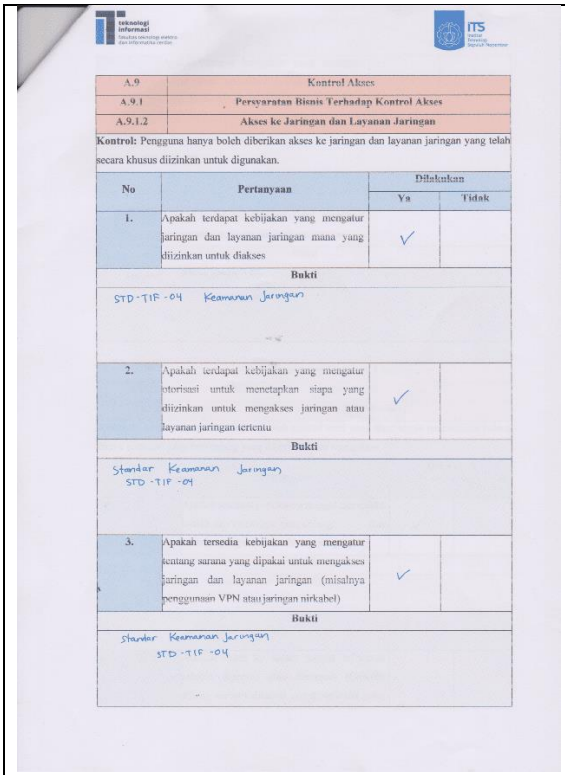


A.16	Manajemen Insiden Keamanan Informas
A.16.1	Manajemen Insiden Keamanan Informasi dan Perbaikan
A.16.1.6	Belajar Dari Insiden Keamanan Informasi

Kontrol: Pengetahuan yang diperoleh dari menganalisa dan menyelesaikan insiden keamanan informasi harus digunakan untuk mengurangi kemungkinan atau dampak dari insiden masa depan

No	Pernyataan	Tingkat Kemampuan				
		1	2	3	4	5
1.	Terdapat mekanisme yang digunakan untuk mengukur dan memonitor jenis, frekuensi dan biaya insiden keamanan informasi					✓
2.	Evaluasi insiden keamanan informasi digunakan untuk meningkatkan kinerja keamanan serta membatasi frekuensi, kerusakan dan biaya kejadian di masa depan					✓

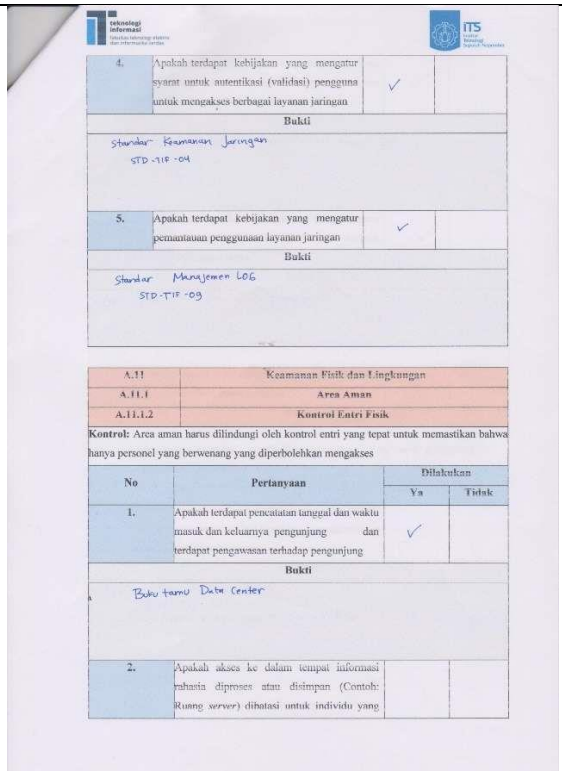
LAMPIRAN E
DOKUMEN FISIK DAFTAR PENELUSURAN BUKTI EVALUASI TATA KELOLA KEAMANAN INFORMASI



A.9	Kontrol Akses
A.9.1	Persyaratan Bisnis Terhadap Kontrol Akses
A.9.1.2	Akses ke Jaringan dan Layanan Jaringan

Kontrol: Pengguna hanya boleh diberikan akses ke jaringan dan layanan jaringan yang telah secara khusus diizinkan untuk digunakan.

No	Pertanyaan	Dilakukan	
		Ya	Tidak
1.	Apakah terdapat kebijakan yang mengatur jaringan dan layanan jaringan mana yang diizinkan untuk diakses	✓	
	Bukti		
	STD-TIF-04 Keamanan Jaringan		
2.	Apakah terdapat kebijakan yang mengatur otorisasi untuk menetapkan siapa yang diizinkan untuk mengakses jaringan atau layanan jaringan tertentu	✓	
	Bukti		
	Standar Keamanan Jaringan STD-TIF-04		
3.	Apakah tersedia kebijakan yang mengatur tentang sarana yang dipakai untuk mengakses jaringan dan layanan jaringan (misalnya penggunaan VPN atau jaringan nirkabel)	✓	
	Bukti		
	Standar Keamanan Jaringan STD-TIF-04		

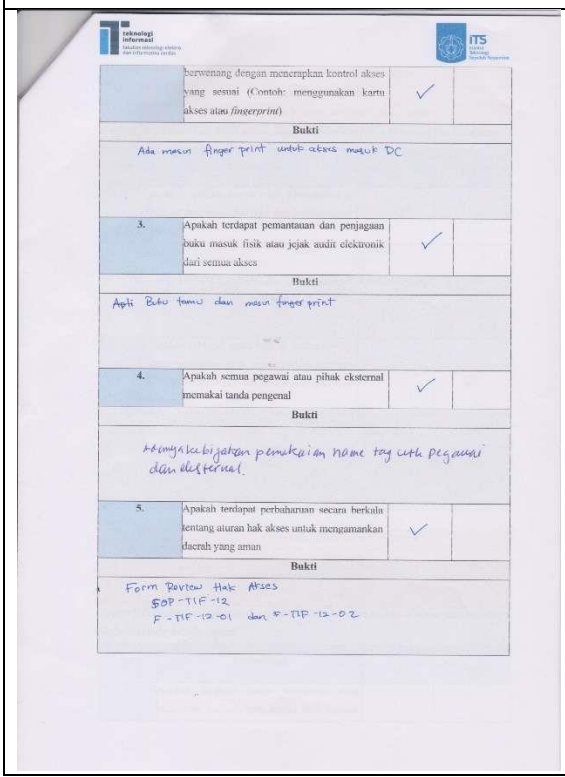


4.	Apakah terdapat kebijakan yang mengatur syarat untuk autentikasi (validasi) pengguna untuk mengakses berbagai layanan jaringan	✓	
	Bukti		
	Standar Keamanan Jaringan STD-TIF-04		
5.	Apakah terdapat kebijakan yang mengatur pemantauan penggunaan layanan jaringan	✓	
	Bukti		
	Standar Manajemen Log STD-TIF-09		

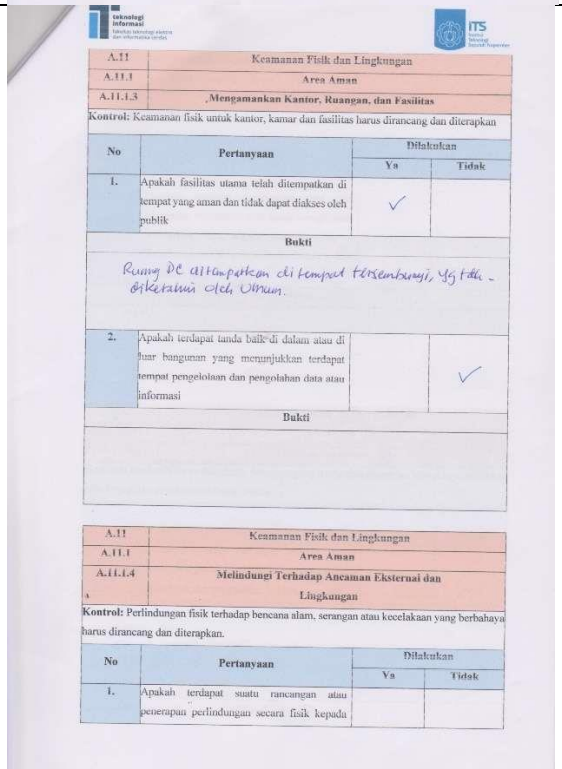
A.11	Keamanan Fisik dan Lingkungan
A.11.1	Area Aman
A.11.1.2	Kontrol Entri Fisik

Kontrol: Area aman harus dilindungi oleh kontrol entri yang tepat untuk memastikan bahwa hanya personel yang berwenang yang diperbolehkan mengakses

No	Pertanyaan	Dilakukan	
		Ya	Tidak
1.	Apakah terdapat pencatatan tanggal dan waktu masuk dan keluarnya pengunjung dan terdapat pengawasan terhadap pengunjung	✓	
	Bukti		
	Buku tamu Data Center		
2.	Apakah akses ke dalam tempat informasi rahasia diproses atau disimpan (Contoh: Ruang *server*) dibatasi untuk individu yang		



	berwenang dengan menerapkan kontrol akses yang sesuai (Contoh: menggunakan kartu akses atau *fingerprint*)	✓	
	Bukti		
	Ada mesin finger print untuk akses masuk DC		
3.	Apakah terdapat pemantauan dan penjagaan buku masuk fisik atau jejak audit elektronik dari semua akses	✓	
	Bukti		
	Apti Buku tamu dan mesin finger print		
4.	Apakah semua pegawai atau pihak eksternal memakai tanda pengenal	✓	
	Bukti		
	Adanya kebijakan pemakaian name tag untuk pegawai dan eksternal.		
5.	Apakah terdapat perbaharuan secara berkala tentang aturan hak akses untuk mengamankan daerah yang aman	✓	
	Bukti		
	Form Review Hak Akses SOP-TIF-12 F-TIF-12-01 dan F-TIF-12-02		



A.11	Keamanan Fisik dan Lingkungan
A.11.1	Area Aman
A.11.1.3	Mengamankan Kantor, Ruangan, dan Fasilitas

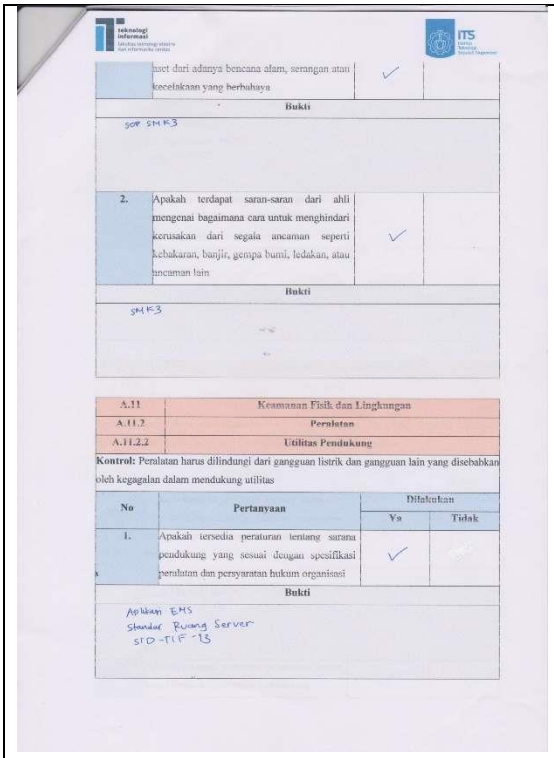
Kontrol: Keamanan fisik untuk kantor, kamar dan fasilitas harus dirancang dan diterapkan

No	Pertanyaan	Dilakukan	
		Ya	Tidak
1.	Apakah fasilitas utama telah ditempatkan di tempat yang aman dan tidak dapat diakses oleh publik	✓	
	Bukti		
	Ruang DC ditempatkan di tempat tersembunyi, yg tdk diketahui oleh Umum.		
2.	Apakah terdapat tanda baik di dalam atau di luar bangunan yang menunjukkan terdapat tempat pengelolaan dan pengolahan data atau informasi		✓
	Bukti		

A.11	Keamanan Fisik dan Lingkungan
A.11.1	Area Aman
A.11.1.4	Melindungi Terhadap Ancaman Eksternal dan Lingkungan

Kontrol: Perlindungan fisik terhadap bencana alam, serangan atau kecelakaan yang berbahaya harus dirancang dan diterapkan.

No	Pertanyaan	Dilakukan	
		Ya	Tidak
1.	Apakah terdapat suatu rancangan atau penerapan perlindungan secara fisik kepada		



	hasil dari adanya bencana alam, serangan atau kecelakaan yang berbahaya	✓	

Bukti

SOP SMK3

2.	Apakah terdapat saran-saran dari ahli mengenai bagaimana cara untuk menghindari kerusakan dari segala ancaman seperti kebakaran, banjir, gempa bumi, ledakan, atau ancaman lain	✓	

Bukti

SMK3

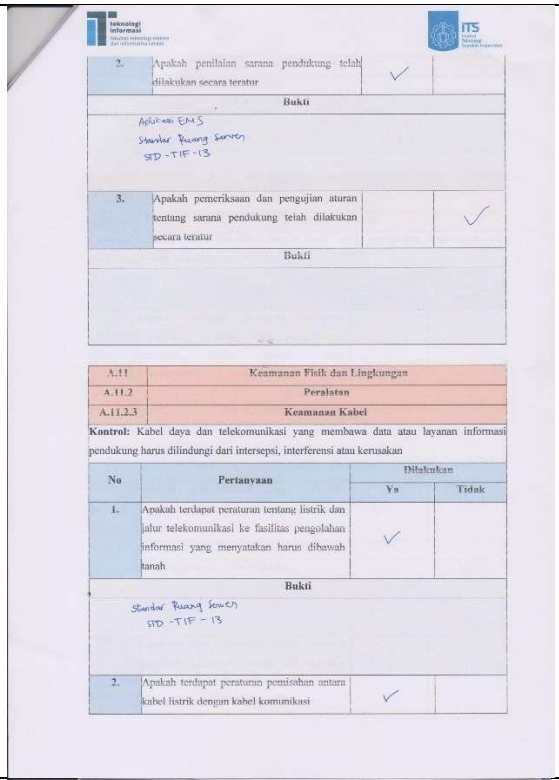
A.11	Keamanan Fisik dan Lingkungan
A.11.2	Peralatan
A.11.2.2	Utilitas Pendukung

Kontrol: Peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dalam mendukung utilitas

No	Pertanyaan	Dilakukan	
		Ya	Tidak
1.	Apakah tersedia peraturan tentang sarana pendukung yang sesuai dengan spesifikasi peralatan dan persyaratan hukum organisasi	✓	

Bukti

Aplikasi EMS
Standar Ruang Server
STD-TIF-13



2.	Apakah penilaian sarana pendukung telah dilakukan secara teratur	✓	

Bukti

Aplikasi EMS
Standar Ruang Server
STD-TIF-13

3.	Apakah pemeriksaan dan pengujian aturan tentang sarana pendukung telah dilakukan secara teratur		✓

Bukti

A.11	Keamanan Fisik dan Lingkungan
A.11.2	Peralatan
A.11.2.3	Keamanan Kabel

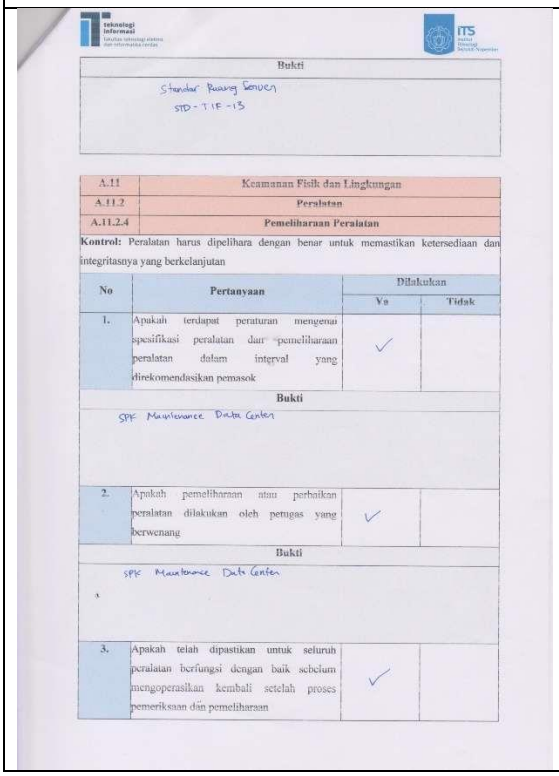
Kontrol: Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung harus dilindungi dari intersepsi, interferensi atau kerusakan

No	Pertanyaan	Dilakukan	
		Ya	Tidak
1.	Apakah terdapat peraturan tentang listrik dan jalur telekomunikasi ke fasilitas pengolahan informasi yang menyatakan harus dibawah tanah	✓	

Bukti

Standar Ruang Server
STD-TIF-13

2.	Apakah terdapat peraturan pemisahan antara kabel listrik dengan kabel komunikasi	✓	



Bukti

Standar Ruang Server
STD-TIF-13

A.11	Keamanan Fisik dan Lingkungan
A.11.2	Peralatan
A.11.2.4	Pemeliharaan Peralatan

Kontrol: Peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya yang berkelanjutan

No	Pertanyaan	Dilakukan	
		Ya	Tidak
1.	Apakah terdapat peraturan mengenai spesifikasi peralatan dan pemeliharaan peralatan dalam interval yang direkomendasikan pemasok	✓	

Bukti

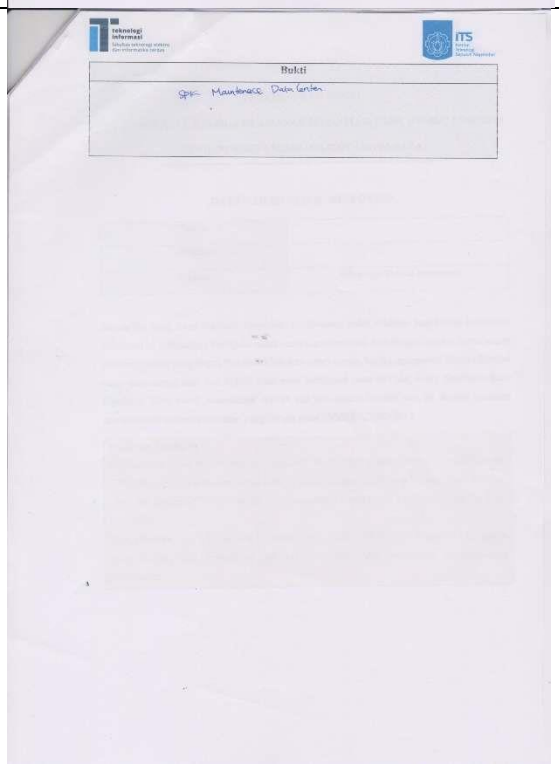
SPK Maintenance Data Center

2.	Apakah pemeliharaan atau perbaikan peralatan dilakukan oleh pengas yang berwenang	✓	

Bukti

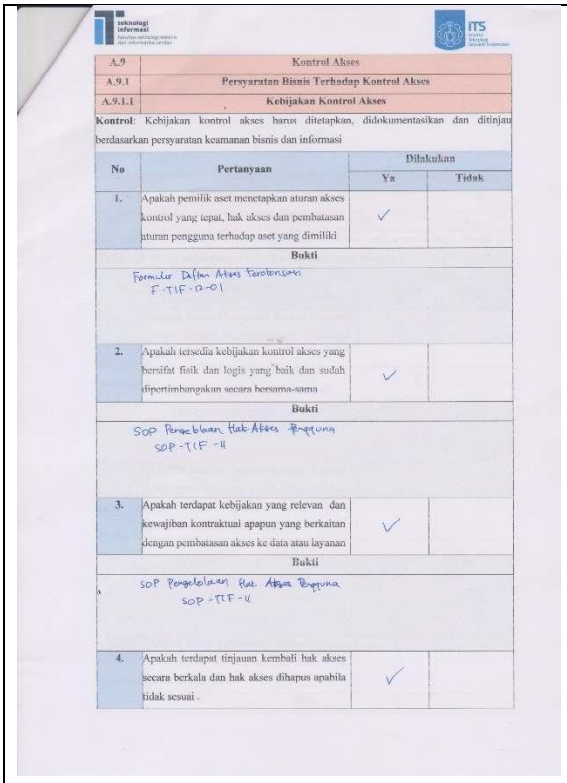
SPK Maintenance Data Center

3.	Apakah telah dipastikan untuk seluruh peralatan berfungsi dengan baik sebelum mengoperasikan kembali setelah proses pemeriksaan dan pemeliharaan	✓	



Bukti

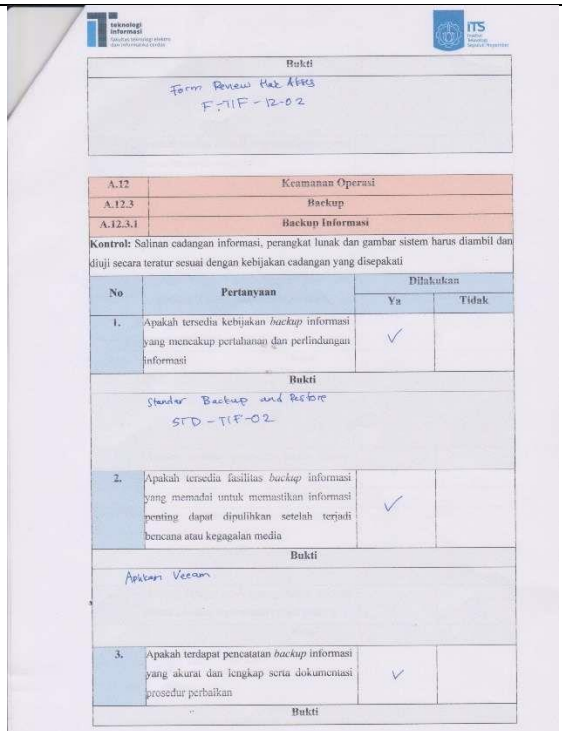
SPK Maintenance Data Center



A.9	Kontrol Akses
A.9.1	Persyaratan Bisnis Terhadap Kontrol Akses
A.9.1.1	Kebijakan Kontrol Akses

Kontrol: Kebijakan kontrol akses harus ditetapkan, didokumentasikan dan ditinjau berdasarkan persyaratan keamanan bisnis dan informasi

No	Pertanyaan	Dilakukan	
		Ya	Tidak
1.	Apakah pemilik aset menetapkan aturan akses kontrol yang tepat, hak akses dan pembatasan aturan pengguna terhadap aset yang dimiliki	✓	
	Bukti		
	Formulir Dalam Akses Terotorisasi F-TIF-12-01		
2.	Apakah tersedia kebijakan kontrol akses yang bersifat fisik dan logis yang baik dan sudah dipertimbangakan secara bersama-sama	✓	
	Bukti		
	SOP Pengelolaan Hak Akses Pengguna SOP-TIF-4		
3.	Apakah terdapat kebijakan yang relevan dan kewajiban kontraktual apapun yang berkaitan dengan pembatasan akses ke data atau layanan	✓	
	Bukti		
	SOP Pengelolaan Hak Akses Pengguna SOP-TIF-4		
4.	Apakah terdapat tinjauan kembali hak akses secara berkala dan hak akses dihapus apabila tidak sesuai .	✓	

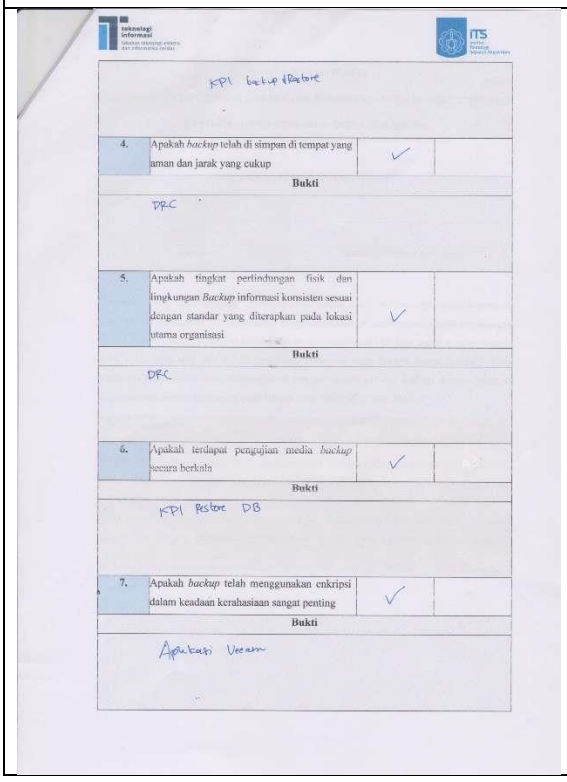


Bukti	
Form Review Hak Akses F-TIF-12-02	

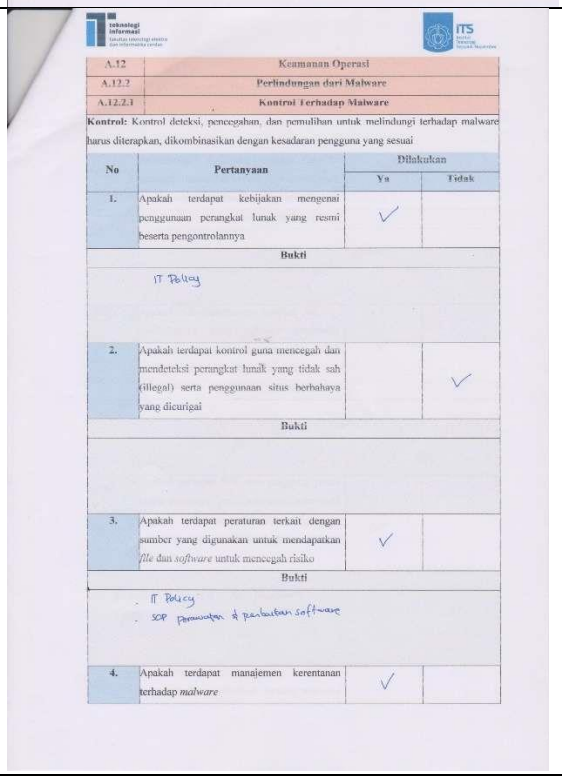
A.12	Keamanan Operasi
A.12.3	Backup
A.12.3.1	Backup Informasi

Kontrol: Salinan cadangan informasi, perangkat lunak dan gambar sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan yang disepakati

No	Pertanyaan	Dilakukan	
		Ya	Tidak
1.	Apakah tersedia kebijakan *backup* informasi yang mencakup pertahanan dan perlindungan informasi	✓	
	Bukti		
	Standar Backup and Restore STD-TIF-02		
2.	Apakah tersedia fasilitas *backup* informasi yang memadai untuk memastikan informasi penting dapat dipulihkan setelah terjadi bencana atau kegagalan media	✓	
	Bukti		
	Aplikasi Veeam		
3.	Apakah terdapat pencatatan *backup* informasi yang akurat dan lengkap serta dokumentasi prosedur perbaikan	✓	
	Bukti		



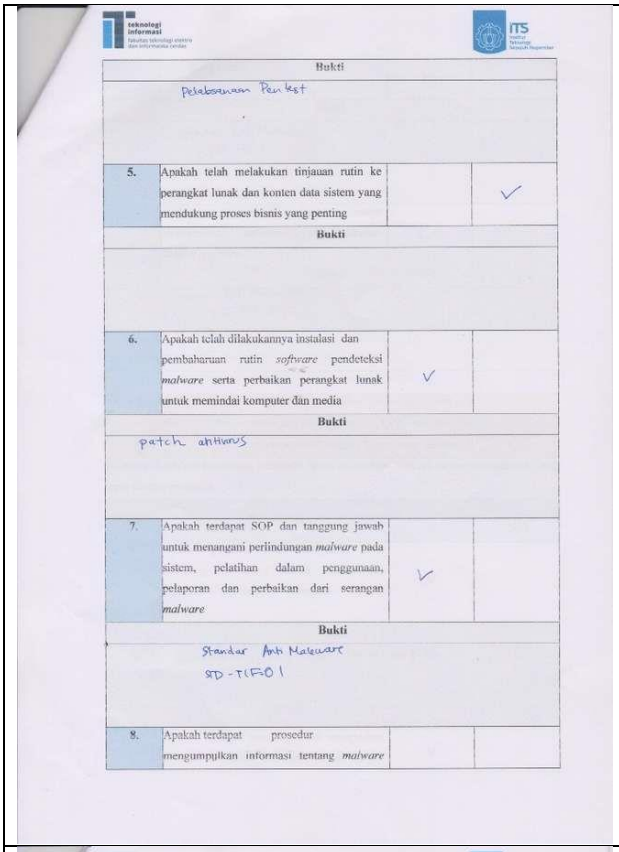
	KPI backup Restore
4. Apakah *backup* telah di simpan di tempat yang aman dan jarak yang cukup	✓
Bukti	
DRC	
5. Apakah tingkat perlindungan fisik dan lingkungan *Backup* informasi konsisten sesuai dengan standar yang diterapkan pada lokasi utama organisasi	✓
Bukti	
DRC	
6. Apakah terdapat pengujian media *backup* secara berkala	✓
Bukti	
KPI Restore DB	
7. Apakah *backup* telah menggunakan enkripsi dalam keadaan kerahasiaan sangat penting	✓
Bukti	
Aplikasi Veeam	



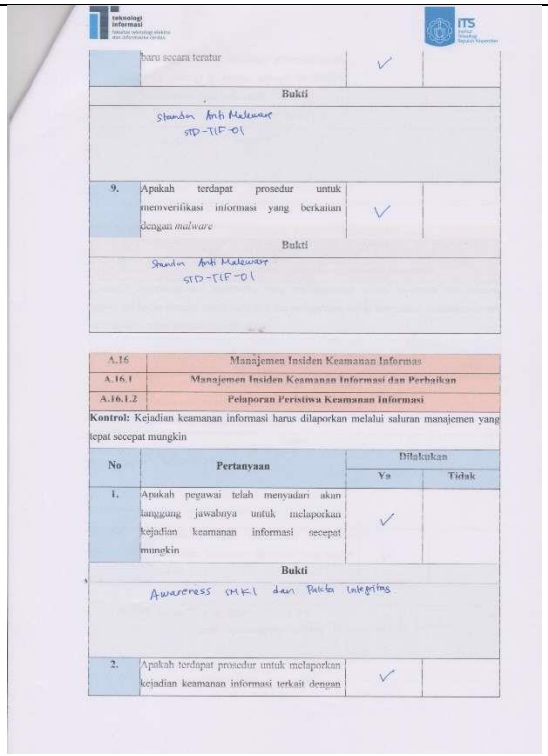
A.12	Keamanan Operasi
A.12.2	Perlindungan dari Malware
A.12.2.1	Kontrol Terhadap Malware

Kontrol: Kontrol deteksi, pencegahan, dan pemulihan untuk melindungi terhadap malware harus diterapkan, dikombinasikan dengan kesadaran pengguna yang sesuai

No	Pertanyaan	Dilakukan	
		Ya	Tidak
1.	Apakah terdapat kebijakan mengenai penggunaan perangkat lunak yang resmi beserta pengontrolannya	✓	
	Bukti		
	IT Policy		
2.	Apakah terdapat kontrol guna mencegah dan mendeteksi perangkat lunak yang tidak sah (illegal) serta penggunaan situs berbahaya yang dicurigai		✓
	Bukti		
3.	Apakah terdapat peraturan terkait dengan sumber yang digunakan untuk mendapatkan *file* dan *software* untuk mencegah risiko	✓	
	Bukti		
	. IT Policy . SOP Pemasangan & perbaikan software		
4.	Apakah terdapat manajemen kerentanan terhadap *malware*	✓	



	Bukti		
	Pelaksanaan Pen test		
5.	Apakah telah melakukan tinjauan rutin ke perangkat lunak dan konten data sistem yang mendukung proses bisnis yang penting		✓
	Bukti		
6.	Apakah telah dilakukannya instalasi dan pembaharuan rutin *software* pendeteksi *malware* serta perbaikan perangkat lunak untuk memindai komputer dan media	✓	
	Bukti		
	patch antivirus		
7.	Apakah terdapat SOP dan tanggung jawab untuk menangani perlindungan *malware* pada sistem, pelatihan dalam penggunaan, pelaporan dan perbaikan dari serangan *malware*	✓	
	Bukti		
	Standar Anti Malware STD-TIF-01		
8.	Apakah terdapat prosedur mengumpulkan informasi tentang *malware*		

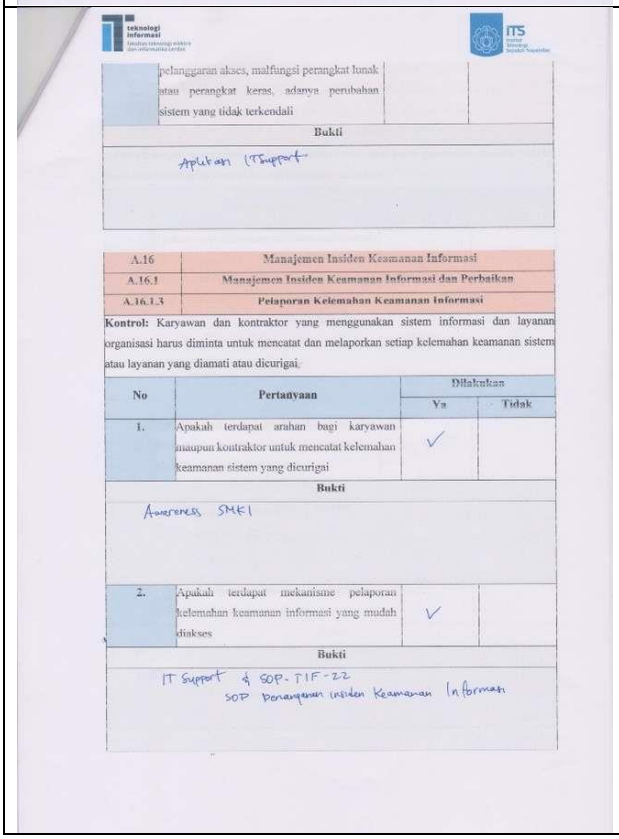


	baru secara teratur	✓	
	Bukti		
	Standar Anti Malware STD-TIF-01		
9.	Apakah terdapat prosedur untuk memverifikasi informasi yang berkaitan dengan *malware*	✓	
	Bukti		
	Standar Anti Malware STD-TIF-01		

A.16	Manajemen Insiden Keamanan Informas
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**
A.16.1.2	**Pelaporan Peristiwa Keamanan Informasi**

Kontrol: Kejadian keamanan informasi harus dilaporkan melalui saluran manajemen yang tepat secepat mungkin

No	Pertanyaan	Dilakukan	
		Ya	Tidak
1.	Apakah pegawai telah menyadari akan tanggung jawabnya untuk melaporkan kejadian keamanan informasi secepat mungkin	✓	
	Bukti		
	Awareness SMKI dan Pakta Integritas		
2.	Apakah terdapat prosedur untuk melaporkan kejadian keamanan informasi terkait dengan	✓	

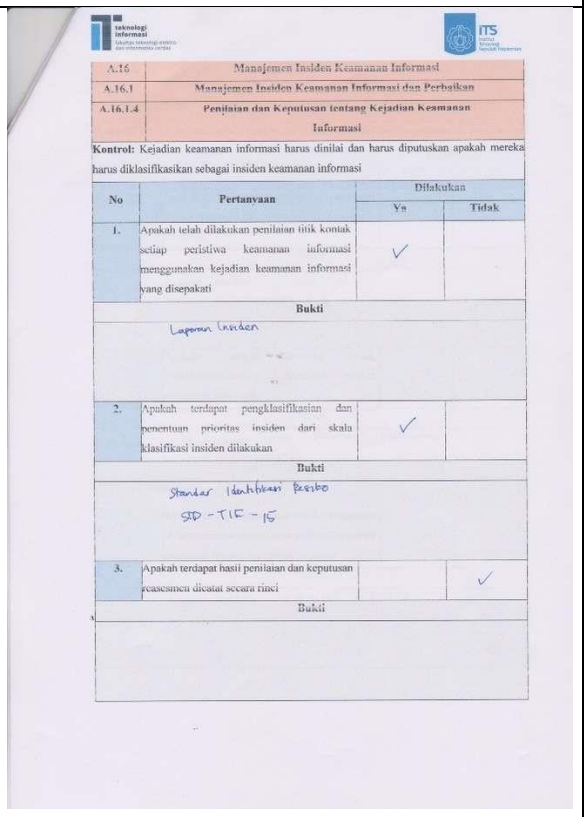


	pelanggaran akses, malfungsi perangkat lunak atau perangkat keras, adanya perubahan sistem yang tidak terkendali		
	Bukti		
	Aplikasi ITSupport		

A.16	Manajemen Insiden Keamanan Informasi
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**
A.16.1.3	**Pelaporan Kelemahan Keamanan Informasi**

Kontrol: Karyawan dan kontraktor yang menggunakan sistem informasi dan layanan organisasi harus diminta untuk mencatat dan melaporkan setiap kelemahan keamanan sistem atau layanan yang diamati atau dicurigai.

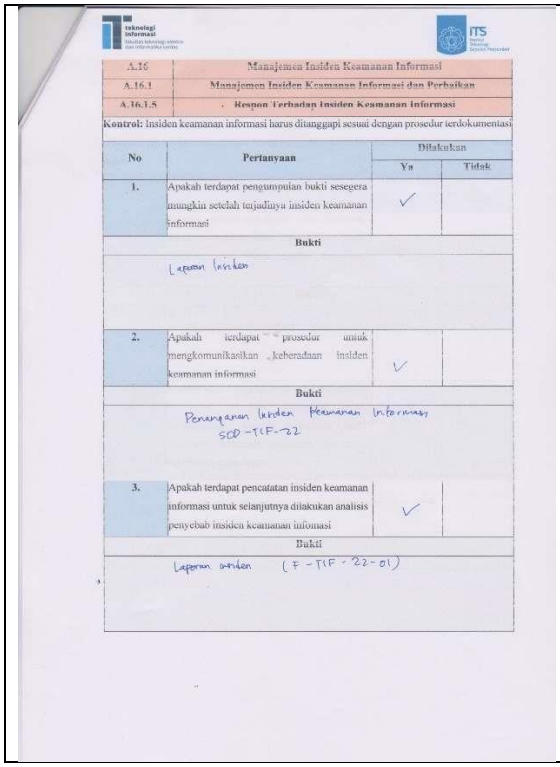
No	Pertanyaan	Dilakukan	
		Ya	Tidak
1.	Apakah terdapat arahan bagi karyawan maupun kontraktor untuk mencatat kelemahan keamanan sistem yang dicurigai	✓	
	Bukti		
	Awareness SMKI		
2.	Apakah terdapat mekanisme pelaporan kelemahan keamanan informasi yang mudah diakses	✓	
	Bukti		
	IT Support & SOP-TIF-22 SOP Penanganan Insiden Keamanan Informasi		



A.16	Manajemen Insiden Keamanan Informasi
A.16.1	**Manajemen Insiden Keamanan Informasi dan Perbaikan**
A.16.1.4	**Penilaian dan Keputusan tentang Kejadian Keamanan Informasi**

Kontrol: Kejadian keamanan informasi harus dinilai dan harus diputuskan apakah mereka harus diklasifikasikan sebagai insiden keamanan informasi

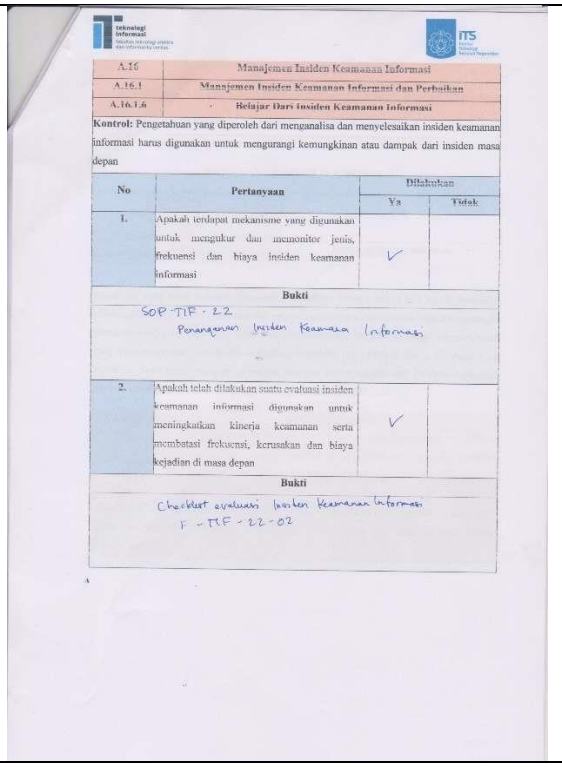
No	Pertanyaan	Dilakukan	
		Ya	Tidak
1.	Apakah telah dilakukan penilaian titik kontak setiap peristiwa keamanan informasi menggunakan kejadian keamanan informasi yang disepakati	✓	
	Bukti		
	Laporan Insiden		
2.	Apakah terdapat pengklasifikasian dan penentuan prioritas insiden dari skala klasifikasi insiden dilakukan	✓	
	Bukti		
	Standar Identifikasi Risiko STD-TIF-15		
3.	Apakah terdapat hasil penilaian dan keputusan reasesmen dicatat secara rinci		✓
	Bukti		



A.16	Manajemen Insiden Keamanan Informasi
A.16.1	Manajemen Insiden Keamanan Informasi dan Perbaikan
A.16.1.5	Respon Terhadap Insiden Keamanan Informasi

Kontrol: Insiden keamanan informasi harus ditanggapi sesuai dengan prosedur terdokumentasi

No	Pertanyaan	Dilakukan	
		Ya	Tidak
1.	Apakah terdapat pengumpulan bukti sesegera mungkin setelah terjadinya insiden keamanan informasi	✓	
	Bukti		
	Laporan Insiden		
2.	Apakah terdapat prosedur untuk mengkomunikasikan keberadaan insiden keamanan informasi	✓	
	Bukti		
	Penanganan Insiden Keamanan Informasi SOP-TIF-22		
3.	Apakah terdapat pencatatan insiden keamanan informasi untuk selanjutnya dilakukan analisis penyebab insiden keamanan informasi	✓	
	Bukti		
	Laporan insiden (F-TIF-22-01)		



A.16	Manajemen Insiden Keamanan Informasi
A.16.1	Manajemen Insiden Keamanan Informasi dan Perbaikan
A.16.1.6	Belajar Dari Insiden Keamanan Informasi

Kontrol: Pengetahuan yang diperoleh dari menganalisa dan menyelesaikan insiden keamanan informasi harus digunakan untuk mengurangi kemungkinan atau dampak dari insiden masa depan

No	Pertanyaan	Dilakukan	
		Ya	Tidak
1.	Apakah terdapat mekanisme yang digunakan untuk mengukur dan memonitor jenis, frekuensi dan biaya insiden keamanan informasi	✓	
	Bukti		
	SOP-TIF-22 Penanganan Insiden Keamanan Informasi		
2.	Apakah telah dilakukan suatu evaluasi insiden keamanan informasi digunakan untuk meningkatkan kinerja keamanan serta membatasi frekuensi, kerusakan dan biaya kejadian di masa depan	✓	
	Bukti		
	Checklist evaluasi insiden keamanan informasi F-TIF-22-02		

LAMPIRAN F
SURAT DAN DOKUMEN PERIJINAN

Surat Pengantar Permohonan Pengambilan Data Tugas Akhir Mahasiswa

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET, DAN TEKNOLOGI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
FAKULTAS TEKNOLOGI ELEKTRO DAN INFORMATIKA CERDAS
DEPARTEMEN TEKNOLOGI INFORMASI
Gedung Perpustakaan Lantai 6, Ruang TU IT601, Kampus ITS, keputih, Sukolilo, Surabaya, 60111
Telepon: 031-5994251-54, 5947274, PABX:1396
Fax:

Surat Pengantar
Nomor : **1227/IT2.IX.5.1.6/B/PN.05/2022**

Perihal : **Permohonan Pengambilan Data Tugas Akhir Mahasiswa**

Kepada Yth.
Ir. Arief Wisnu Cahyono, ST
Direktur Utama PDAM Surya Sembada
PDAM Surya Sembada Kota Surabaya
Jl. Mayjen Prof. Dr. Moestopo No. 2 Pacar Keling - Tambaksari
Surabaya Jawa Timur 60131

Terkait dengan rencana pelaksanaan Tugas Akhir mahasiswa Departemen Teknologi Informasi, Fakultas Teknologi Elektro dan Informatika Cerdas – Institut Teknologi Sepuluh Nopember atas nama :

NRP : 05311840000037
Nama : Dimas Pramudya Haqqi
Dosen Pembimbing : Ir. Khakim Ghozali, M.MT
Dr.techn. Ir. Raden Venantius Hari Ginardi, M.Sc

Judul Tugas Akhir : EVALUASI KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 DENGAN MENGGUNAKAN MODEL SSE-CMM (SYSTEM SECURITY ENGINEERING CAPABILITY MATURITY MODEL) PADA PERUSAHAAN DAERAH AIR MINUM SURYA SEMBADA KOTA SURABAYA

Dengan ini kami mohon mahasiswa tersebut diperkenankan untuk melakukan penelitian / mencari data pada mengenai :

1. Data terkait keamanan informasi untuk dilakukan sebuah evaluasi
2. Data dokumen terkait keamanan informasi guna penelusuran bukti

Pelaksanaan direncanakan pada tanggal 28 Maret s.d 16 Juni 2022

Demikian surat ini kami sampaikan, atas perhatian dan kerjasamanya kami ucapkan terima kasih.

Surabaya, 14 Maret 2022
Kepala Departemen Teknologi Informasi,

Dr.techn. Ir. Raden Venantius Hari Ginardi, M.Sc.
196505181992031003

Surat Perijinan Permohonan Pengambilan Data Tugas Akhir Mahasiswa

PERUSAHAAN DAERAH AIR MINUM
SURYA SEMBADA
KOTA SURABAYA

Surabaya, 25 MAR 2022

Nomor : 072/235/PDAM/2022.
Sifat : -
Lampiran : satu berkas
Hal : Penelitian

Yth.Kepala Departemen
Teknologi Informasi
Fakultas Teknologi Elektro dan
Informatika Cerdas ITS
Surabaya

Sehubungan dengan surat Saudara Nomor: 1227/IT2.IX.5.1.6/B/PN.05/2022 tanggal 14 Maret 2022 perihal Permohonan Pengambilan Data Tugas Akhir, bersama ini kami menginformasikan bahwa permohonan Saudara terkait permohonan Penelitian kami terima dan dilaksanakan secara ***online dan tatap muka (offline)*** dengan jadwal sebagai berikut :

Tanggal : 28 Maret 2022.s.d. 16 Juni 2022.
Pukul : 07.30 WIB.s.d.Selesai.
Jumlah Peserta : Satu Orang.
Tempat : Bagian Teknologi Sistem Informasi.
Kantor PDAM Surya Sembada Kota Surabaya
Jl.Prof.Dr.Moestopo No.2 Surabaya

Catatan :
1. Selama masa pandemi bimbingan dengan Pembimbing dilokasi Penelitian dilakukan secara jarak dekat/jauh dengan memanfaatkan Media sosial.(e-email,whatshapp,zoom dll) Hal ini termasuk permintaan data/dokumen.
2. Dokumentasi Visual(foto,video)dari tempat KP sangat ditekankan dan merupakan point penting penilaian.Mahasiswa didorong utk melakukan komunikasi dengan baik dengan pembimbing ditempat Penelitian untuk memohon dokumentasi -dokumentasi.
3. Hasil Kerja Praktik/**Penelitian**/Kunjungan agar Diserahkan kepada PDAM dan tidak Mempublikasikan tanpa izin/sepengetahuan PDAM Surya Sembada Kota Surabaya.

Narahubung : Hendro N.(088217948174).

Demikian atas perhatian dan kerjasama, kami menyampaikan terima kasih.

A.n. Direksi Perusahaan Daerah Air Minum
Surya Sembada Kota Surabaya,
Sekretaris Perusahaan

Drs. BAMBANG EKO SAKTI
MPP. 19.92.00780

Tembusan ;
Yth. 1. Direktur Utama;
2. Manajer Teknologi Sistem Informasi;
3. Manajer Tata Usaha & Humas;
PDAM Surya Sembada Kota Surabaya.
Mahasiswa bersangkutan/terkait
a.n.Dimas Pramudya H; ITS - Surabaya

Kantor :
Jl. Mayjen. Prof. Dr. Moestopo No. 2, Telp. 031-5039373, 5039676, Fax 031-5030100, Surabaya 60131
Website : www.pdam-sby.go.id Call Center : 0800 192 6666 (bebas pulsa) Layanan WA : 08123316666
ISO 9001 : 2015
ISO/IEC 17025 : 2017

Surat Keterangan Penelusuran Bukti Terbatas

PERUSAHAAN DAERAH AIR MINUM
SURYA SEMBADA
KOTA SURABAYA

SURAT KETERANGAN

Nomor :097/K/TSI/IV/2022

Yang bertanda tangan dibawah ini:

Nama : Nasrul Amir, S. Kom

Jabatan : Manager Teknologi Sistem Informasi

Bagian : Teknologi Sistem Informasi

Terkait dengan pelaksanaan Tugas Akhir mahasiswa Departemen Teknologi Informasi, Fakultas Teknologi Elektro dan Informatika Cerdas – Institut Teknologi Sepuluh Nopember atas nama:

Nama : Dimas Pramudya Haqqi

NRP : 05311840000037

Judul Tugas Akhir : EVALUASI TATA KELOLA KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 DENGAN MENGGUNAKAN MODEL SSE-CMM (*SYSTEM SECURITY ENGINEERING CAPABILITY MATURITY MODEL*) PADA PERUSAHAAN DAERAH AIR MINUM SURYA SEMBADA KOTA SURABAYA

Menerangkan bahwa bukti-bukti dokumen pendukung untuk evaluasi tata kelola keamanan informasi berdasarkan ISO/IEC 27001:2013 pada PDAM Surya Sembada Kota Surabaya guna keperluan penelitian Tugas Akhir, mahasiswa / peneliti hanya diijinkan untuk melihat bukti dokumen pendukung tersebut secara fisik / terbatas dan tidak diijinkan untuk di fotokopi, difoto atau di publikasi dalam bentuk apapun untuk kepentingan umum.

Demikian surat keterangan ini dibuat, untuk digunakan sebagaimana mestinya.

Surabaya,22 April 2022

Mengetahui,
Manager Teknologi Sistem Informasi
PDAM Surya Sembada Kota Surabaya

Nasrul Amir, S. Kom
Nip. 1 680 498

Kantor :
Jl. Mayjen. Prof. Dr. Moestopo No. 2, Telp. 031-5039373, 5039676, Fax 031-5030100, Surabaya 60131 ISO 9001 : 2015
Website : www.pdam-sby.go.id Call Center : 0800 192 6666 (bebas pulsa) Layanan SMS/WA : 081.2331-6666 ISO/IEC 17025 : 2017

Lembar Pengesahan Perusahaan

PERUSAHAAN DAERAH AIR MINUM
SURYA SEMBADA
KOTA SURABAYA

LEMBAR PENGESAHAN PERUSAHAAN

EVALUASI TATA KELOLA KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 DENGAN MENGGUNAKAN MODEL SSE-CMM (*SYSTEM SECURITY ENGINEERING CAPABILITY MATURITY MODEL*) PADA PERUSAHAAN DAERAH AIR MINUM SURYA SEMBADA KOTA SURABAYA

LAPORAN TUGAS AKHIR

Menyatakan bahwa isi laporan Tugas Akhir dengan judul tersebut, sudah diketahui dan sesuai dengan kondisi maupun kebutuhan perusahaan.

Oleh : **DIMAS PRAMUDYA HAQQI**
NRP. 05311840000037

Mengetahui,
Manager Teknologi Sistem Informasi
PDAM Surya Sembada Kota Surabaya

Nasrul Anuar S. Kom
Nip. 1.08.01498

Kantor :
Jl. Mayjen. Prof. Dr. Moestopo No. 2, Telp. 031-5039373, 5039676, Fax 031-5030100, Surabaya 60131
Website : www.pdam-sby.go.id Call Center : 0800 192 6666 (bebas pulsa) Layanan SMS/WA : 081.2331-6666
ISO 9001 : 2015
ISO/IEC 17025 : 2017

Surat Persetujuan Hasil Rekomendasi

PERUSAHAAN DAERAH AIR MINUM
SURYA SEMBADA
KOTA SURABAYA

SURAT KETERANGAN

Nomor: 102/ K / TSI / VII / 2022

Terkait dengan pelaksanaan Tugas Akhir mahasiswa Departemen Teknologi Informasi, Fakultas Teknologi Elektro dan Informatika Cerdas – Institut Teknologi Sepuluh Nopember atas nama:

Nama	: Dimas Pramudya Haqqi
NRP	: 05311840000037
Judul Tugas Akhir	: EVALUASI TATA KELOLA KEAMANAN INFORMASI BERDASARKAN STANDAR ISO/IEC 27001:2013 DENGAN MENGGUNAKAN MODEL SSE-CMM (*SYSTEM SECURITY ENGINEERING CAPABILITY MATURITY MODEL*) PADA PERUSAHAAN DAERAH AIR MINUM SURYA SEMBADA KOTA SURABAYA

Menerangkan bahwa rekomendasi yang diberikan oleh penulis untuk memperbaiki gap yang ditemukan pada evaluasi tata kelola keamanan informasi berdasarkan ISO/IEC 27001:2013 pada PDAM Surya Sembada Kota Surabaya telah diketahui dan sesuai dengan kondisi maupun kebutuhan perusahaan. Mahasiswa / penulis hanya diijinkan untuk melihat bukti pendukung tersebut secara fisik / terbatas dan tidak diijinkan untuk di foto atau di publikasi dalam bentuk apapun untuk kepentingan umum.

Demikian surat keterangan ini dibuat, untuk digunakan sebagaimana mestinya.

Surabaya, Juli 2022

Menyetujui,

Supervisor Pengembangan Teknologi Informasi	Supervisor Infrastruktur	Supervisor Sistem Informasi
(Eko Yudha Prasetya)	(Dedy Purwanto)	(Ira Nuraini)
NIP. 1.09.01552	NIP. 1.06.01414	NIP. 1.06.01390

Mengetahui,

Manajer Teknologi Sistem Informasi

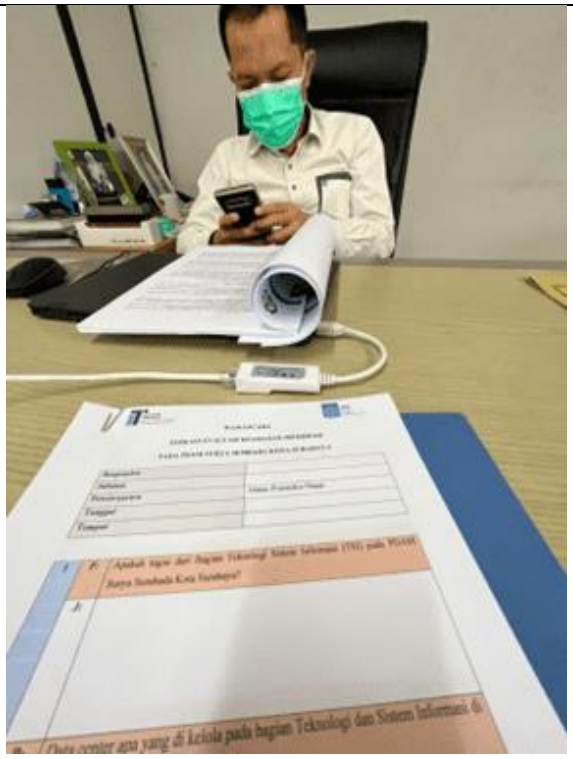
PDAM Surya Sembada Kota Surabaya

(Nasrul Amir, S. Kom)

NIP. 1.08.01498

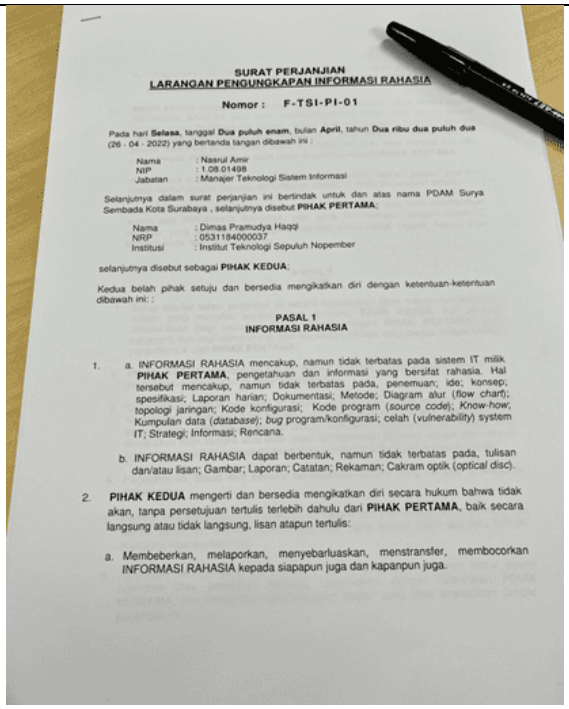
Kantor :
Jl. Mayjen. Prof. Dr. Moestopo No. 2, Telp. 031-5039373, 5039676, Fax 031-5030100, Surabaya 60131
Website : www.pdam-sby.go.id Call Center : 0800 192 6666 (bebas pulsa) Layanan WA : 08123316666

LAMPIRAN G
DOKUMENTASI PENELITIAN



Dokumentasi pada saat wawancara

Dokumentasi pada saat pemberian kuesioner



SURAT PERJANJIAN
LARANGAN PENGUNGKAPAN INFORMASI RAHASIA

Nomor : F-TSI-PI-01

Pada hari **Selasa**, tanggal **Dua puluh enam**, bulan **April**, tahun **Dua ribu dua puluh dua** (26 - 04 - 2022) yang bertanda tangan dibawah ini :

Nama : Nasrul Amir
NIP : 1.08.01498
Jabatan : Manajer Teknologi Sistem Informasi

Selanjutnya dalam surat perjanjian ini bertindak untuk dan atas nama PDAM Surya Sembada Kota Surabaya , selanjutnya disebut **PIHAK PERTAMA**;

Nama : Dimas Pramudya Haqq
NRP : 0531184000037
Institusi : Institut Teknologi Sepuluh Nopember

selanjutnya disebut sebagai **PIHAK KEDUA**.

Kedua belah pihak setuju dan bersedia mengikatkan diri dengan ketentuan-ketentuan dibawah ini: :

PASAL 1
INFORMASI RAHASIA

1. a. INFORMASI RAHASIA mencakup, namun tidak terbatas pada sistem IT milik **PIHAK PERTAMA**, pengetahuan dan informasi yang bersifat rahasia. Hal tersebut mencakup, namun tidak terbatas pada, penemuan; ide; konsep; spesifikasi; Laporan harian; Dokumentasi; Metode; Diagram alur (flow chart); topologi jaringan; Kode konfigurasi; Kode program (source code); Know-how; Kumpulan data (*database*); *bug* program/konfigurasi; celah (vulnerability) system IT; Strategi; Informasi; Rencana.

b. INFORMASI RAHASIA dapat berbentuk, namun tidak terbatas pada, tulisan dan/atau lisan; Gambar; Laporan; Catatan; Rekaman; Cakram optik (optical disc).

2. **PIHAK KEDUA** mengerti dan bersedia mengikatkan diri secara hukum bahwa tidak akan, tanpa persetujuan tertulis terlebih dahulu dari **PIHAK PERTAMA**, baik secara langsung atau tidak langsung, lisan atapun tertulis:

a. Membeberkan, melaporkan, menyebarluaskan, menstransfer, membocorkan INFORMASI RAHASIA kepada siapapun juga dan kapanpun juga.

Dokumentasi pada saat penandatanganan NDA

BIODATA PENULIS

Penulis memiliki nama lengkap Dimas Pramudya Haqqi, lahir pada tanggal 14 Agustus 2000 dan merupakan anak kedua dari dua bersaudara. Pendidikan formal penulis ditempuh di TK Aisyah Surabaya, SDN Kandangan 3 Surabaya, SMPN 40 Surabaya, dan SMAN 12 Kota Surabaya yang kemudian dilanjutkan di Departemen Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS) Surabaya. Selama masa perkuliahannya, penulis aktif dalam kegiatan organisasi intra kampus. Pada lingkup departemen, penulis beberapa kali berpartisipasi dalam kepanitiaan acara himpunan, seperti OKKBK HMIT ITS, ARA ITS 2020, LKMW-TD, PKTI-TD dsb. Kemudian, pada lingkup ITS, penulis bergabung di Badan Eksekutif Mahasiswa (BEM) ITS sebagai Menteri Koordinator Inovasi dan Karya pada BEM ITS 2022, Menteri pada Kementrian Riset dan Teknologi BEM ITS Unjuk Asa 2021 dan *staff* direktorat jenderal (ditjen) ekslakasi keilmiahan untuk Kementrian Riset dan Teknologi BEM ITS Rectoverso 2020. Beberapa program kerja yang telah dilakukan penulis selama bergabung di BEM ITS, antara lain PKTI-TD ITS, Rencana Strategis (Renstra), PEKIL ITS, Forum Keilmiahan (RUMAH), Festival Karya ITS, Seminar Mawapres ITS, Bincang Ristek, dsb. Dan melakukan koordinasi dengan *stakeholder* keilmiahan seperti direktorat kemahasiswaan, tim-tim riset ITS, dan departemen riset dan teknologi himpunan mahasiswa di ITS serta mengkoordinir kementerian-kementerian yang ada di bawah kemenkoan inovasi dan karya agar selaras dan berkesinambungan. Selain itu, untuk kegiatan diluar kampus, penulis aktif dalam kegiatan perlombaan *business plan competition* dengan mengikuti beberapa kompetisi yang diadakan perguruan tinggi di Indonesia. Penulis berkesempatan untuk melakukan kerja praktik dan magang pada chapter IT *Integration* PT. Telkom Indonesia pada Merdeka Belajar Kampus Merdeka (MBKM) MSIB *batch* 1 dan melakukan *penetration tester* pada PDAM Surya Sembada Kota Surabaya Penulis memiliki kemampuan berbahasa Indonesia dan Bahasa Inggris yang baik. Penulis terbuka untuk berdiskusi mengenai berbagai hal dan dapat dihubungi melalui alamat *email*: dimas.pramudya20648@gmail.com.