



TESIS  
PEMBUATAN TATA LAKSANA MANAJEMEN INSIDEN  
PADA PROGRAM MANAJEMEN HELPDESK DAN  
DUKUNGAN TI BERDASARKAN *FRAMEWORK* ITIL V3  
(STUDI KASUS PADA BIRO TI BPK-RI)

TUMPAL PARADONGAN SILITONGA  
NRP 9108.205.803

DOSEN PEMBIMBING  
Ir. A. Holil Noor Ali, M. Kom

PROGRAM STUDI MAGISTER MANAJEMEN TEKNOLOGI  
BIDANG KEAHLIAN MANAJEMEN TEKNOLOGI INFORMASI  
PROGRAM PASCASARJANA  
INSTITUT TEKNOLOGI SEPULUH NOPEMBER  
SURABAYA  
2010



THESIS - MM2402

**DESIGNING THE STANDARD OPERATION  
PROCEDURE OF INCIDENT MANAGEMENT PROCESS  
ON HELPDESK MANAGEMENT AND INFORMATION  
TECHNOLOGY SUPPORTING PROGRAM  
BASED ON ITIL V3 FRAMEWORK  
(CASE STUDY ON INFORMATION TECHNOLOGY  
DEPARTMENT OF BPK-RI)**

TUMPAL PARADONGAN SILITONGA  
Student Identity Number 9108.205.803

SUPERVISOR  
Ir. A. Holil Noor Ali, M. Kom

POSTGRADUATE PROGRAM  
DEPARTMENT OF TECHNOLOGY MANAGEMENT  
FACULTY OF INFORMATION TECHNOLOGY MANAGEMENT  
SEPULUH NOPEMBER INSTITUTE OF TECHNOLOGY  
SURABAYA  
2010

**PEMBUATAN TATA LAKSANA MANAJEMEN INSIDEN  
PADA PROGRAM MANAJEMEN HELPDESK DAN DUKUNGAN TI  
BERDASARKAN *FRAMEWORK* ITIL V3  
(STUDI KASUS PADA BIRO TI BPK-RI)**

Nama Mahasiswa : Tumpal Paradongan Silitonga  
NRP : 9108205803  
Pembimbing : Ir. Achmad Holil Noor Ali, M.Kom

**Abstrak**

Dalam pengelolaan layanan TI di lingkungan BPK-RI, salah satu proses TI yang paling sering dilakukan adalah proses manajemen insiden yang dituangkan dalam bentuk program manajemen helpdesk dan dukungan TI. Hal ini disebabkan semakin banyak perangkat keras komputer dan jaringan yang ditangani berikut aplikasi sistem informasi yang digunakan. Adanya harapan dari pimpinan dan pegawai BPK-RI agar waktu penanganan insiden dapat diminimalkan dan tingginya ketergantungan kepada staf teknis tertentu, membuat dokumentasi tata laksana manajemen insiden yang terstandar sangat diperlukan.

Pembuatan tata laksana manajemen insiden program manajemen helpdesk dan dukungan TI diawali dengan pengumpulan informasi dan analisa melalui penelaahan dokumen tata kelola TI BPK-RI, dan studi literatur *framework* ITIL. Analisa dilakukan untuk menyempurnakan proses manajemen insiden yang sudah ada, dan kemudian mengembangkan dokumen prosedur terstandar yang berisi fungsi dan tanggungjawab dalam diagram RACI, dan formulir yang digunakan. Setelah dokumen selesai dibuat, maka langkah selanjutnya adalah verifikasi masing-masing bagian dari dokumen. Setelah verifikasi, dilakukan validasi dokumen untuk mengetahui tujuan dari proses manajemen insiden sudah terpenuhi.

Dokumentasi tata laksana manajemen insiden diperlukan untuk menjadi standar acuan dalam penanganan insiden, mengurangi miskomunikasi antar pihak yang menangani insiden, dan meminimalkan waktu penanganan insiden. Dokumen tata laksana ini akan digunakan oleh pihak manajemen untuk menjadi standar dalam penanganan insiden. Selain itu dokumen ini memberikan kemudahan bagi pihak manajemen untuk mengukur capaian setiap aktifitas dalam program manajemen insiden dengan menggunakan matrik tata laksana.

Kata kunci: Tata Laksana, ITIL, Manajemen Insiden, BPK-RI

--- Halaman ini dikosongkan ---

**DESIGNING THE STANDARD OPERATION PROCEDURE OF  
INCIDENT MANAGEMENT PROCESS ON  
HELPDESK MANAGEMENT AND IT SUPPORT PROGRAM  
BASED ON ITIL V3 FRAMEWORK  
(IN INFORMATION TECHNOLOGY DEPARTMENT OF BPK-RI)**

Student Name : Tumpal Paradongan Silitonga  
Student Identity Number : 9108205803  
Supervisor : Ir. Achmad Holil Noor Ali, M.Kom

**Abstract**

One of IT services within the BPK-RI that most often done is incident management process. This is due to more computer hardware, networking tools, and information systems used by BPK-RI. The hope of management and employee of BPK-RI that the process can be handled in a minimized time and not depended on certain technical staff, made the documentation of incident management process is needed.

The making of documentation of incident management process in helpdesk management and IT support program begins with information gathering and analysis through a review of IT governance document of BPK-RI, and literature study of ITIL framework. Analysis was carried out to improve incident management process which already exists, and then develop a standardized procedure document that contains the functions and responsibilities in the RACI chart, and forms. After the document was completed, then the next step is to verify each part of the document. After verification, validation documents conducted to determine the purpose of incident management processes have been fulfilled.

Documentation of incident management process is required to set standards in the handling of incidents, reduce miscommunication between the parties which handles incidents, and minimized incident handling time. The document will be used by management to become standard in the handling of the incident. In addition, this document provides convenience for the management to measure the achievement of each activity within the incident management program by using a matrix.

Keyword: Governance, ITIL, Incident Management, BPK-RI

--- Halaman ini dikosongkan ---

## **BAB 2**

### **Kajian Pustaka dan Dasar Teori**

#### **2.1 Tata Kelola**

Tata kelola adalah prinsip keterbukaan, integritas dan akuntabilitas yang diterapkan oleh organisasi untuk meningkatkan kualitas serta kontrol atas proses bisnis yang dijalankan [CAD92]. Dalam pengertian ini, organisasi bertanggungjawab membentuk rencana strategis, meningkatkan kemampuan kepemimpinan, mengelola manajemen dengan baik, dan secara berkala melaporkan pelaksanaan organisasi kepada *stakeholder*.

Menurut pengertian lain, tata kelola adalah penggunaan struktur lembaga, otoritas dan kolaborasi dalam mengalokasikan sumber daya dan koordinasi kontrol aktifitas pada sebuah entitas organisasi [BEL02].

Dari kedua pengertian ini dapat disimpulkan bahwa implementasi tata kelola dalam suatu organisasi memiliki tujuan agar visi, misi dan rencana strategis organisasi dapat tercapai. Dalam mencapai visi, misi dan rencana strategis tersebut, perlu diperhatikan tata kelola juga menyinggung mengenai proses alokasi sumber daya agar penggunaannya efektif.

##### **2.1.1 Tata Kelola TI**

Tata kelola TI adalah sebuah sistem dimana penggunaan TI pada saat sekarang dan masa yang akan datang diarahkan dan dikontrol [ISO08]. Lebih lanjut dikatakan dalam standar ini, sebuah badan tata kelola TI harus dibentuk dan bertugas untuk mengevaluasi dan mengarahkan TI dalam mendukung proses bisnis organisasi dan memonitor penggunaannya agar sesuai dengan rencana strategis TI organisasi.

Defenisi tata kelola TI yang lain yang bisa kita cermati, tata kelola TI adalah tanggung jawab bersama dewan direksi dan manajer serta sebagai bagian integral dalam tata kelola organisasi keseluruhan [ITG03]. Lebih lanjut dikatakan juga bahwa tata kelola TI harus memiliki struktur organisasi sendiri untuk mendukung

strategi dan tujuan bisnis utama. Defenisi yang ketiga mengenai tata kelola TI adalah tindakan spesifik menurut hak yang diberikan dan dalam koridor sebuah framework tertentu dengan pengambilan keputusan terkait penggunaan TI [WEI02].

Dari semua defenisi diatas, dapat ditarik persamaan defenisi mengenai tata kelola TI [ANT09], yaitu:

1. Tata kelola TI adalah tanggung jawab dari pimpinan organisasi
2. Tujuan utama tata kelola TI adalah untuk mensukseskan strategi bisnis dan strategi TI
3. Tata kelola TI harus terdiri dari strategi, *policy*, tanggung jawab, struktur, dan proses TI
4. Ada perbedaan mendasar antara tata kelola TI dan manajemen TI
5. Tata kelola TI adalah bagian yang tak terpisahkan dari tata kelola organisasi

Dalam membangun sebuah tata kelola TI, setiap organisasi dibebaskan untuk membentuknya menurut kebutuhan masing-masing. Dalam proses implementasi tersebut, sebuah tata kelola TI dapat terdiri dari beragam struktur (misalnya menurut besar organisasi dan banyaknya fungsi IT yang digunakan), proses (misalnya menurut rencana strategis organisasi dan model tata kelola TI), dan mekanisme relasional (misalnya menurut bentuk partisipasi antara manajemen TI dengan bisnis). Jika ketiga hal ini dikombinasikan maka hasil kombinasi tersebut adalah berupa *framework* tata kelola TI.

Ada beberapa *framework* tata kelola TI yang menjadi acuan dalam pengembangan tata kelola TI di berbagai organisasi. *Framework* tata kelola TI tersebut antara lain yang sudah dikenal (berikut versi terakhirnya) adalah COBIT v4.1 (*Control Objectives for Information and related Technology*), MOF v4.0 (*Microsoft Operations Framework*), ITIL v3 (*Information Technology Infrastructure Library*), TOGAF v9 (*The Open Group Architecture Framework*), CMMI v1.2 (*Capability Maturity Model Integration*), ISO/IEC 27001:2005 mengenai *Information Technology Security Techniques*, ISO/IEC 38500:2008 mengenai *Corporate Governance of Information Technology*, dan lain sebagainya.



### 2.1.2 Tata laksana

Tata laksana adalah bagian dari keseluruhan tata kelola. Menurut standar ISO 9001:2008 mengenai *Quality Management Systems*, tata laksana adalah implementasi prosedur dan formulir sebagai langkah untuk mencapai pedoman, tujuan dan kebijakan organisasi yang telah ditetapkan sebelumnya. Dokumentasi tata laksana harus memperhatikan pedoman, tujuan, dan kebijakan organisasi.

Standar ISO 9001:2008 mengenai *Quality Management Systems* [ISO90], menyebutkan 5 level dokumen dalam pembuatan tata kelola, yaitu:

1. Dokumen *quality policy* dan *quality objective*

Dokumen *quality policy* dan *quality objective* dibuat untuk setiap strategi bisnis yang telah ditetapkan organisasi. Dokumen *quality policy* adalah dokumen yang berisi pedoman/kebijakan mengenai proses bisnis dalam organisasi. Pada dokumen ini terdapat maksud dan tujuan organisasi, komitmen bersama serta kerangka kerja untuk mencapai tujuan tersebut. Sedangkan dokumen *quality objective* adalah dokumen yang berisi sasaran yang akan diraih oleh proses bisnis.

2. Dokumen *quality manual*

Dokumen *quality manual* adalah dokumen yang berisi kebijakan organisasi untuk mencapai sasaran yang sudah dibuat dalam dokumen *quality objective*. Pada dokumen ini terdapat indikator kualitas maupun kuantitas dari aktifitas-aktifitas yang dibuat untuk mencapai sasaran yang telah ditetapkan.

3. Dokumen prosedur

Dokumen prosedur dikenal juga sebagai *Standard Operating Procedures* (SOP). Dalam dokumen ini ditetapkan bagaimana aktifitas dilakukan, siapa yang melakukannya, kapan dan dimana dilakukan, serta merujuk dari/kepada aktifitas mana.

4. Dokumen *Plan/Operate/Control*

Standar manajemen mutu ISO 9001:2008 mengenalkan level baru dalam dokumentasi tata kelola yaitu dokumen-dokumen yang dibuat untuk memastikan proses perencanaan (*Plan*), pengoperasian (*Operate*), dan kontrol (*Control*) sudah dijalankan dengan baik. Dokumen-dokumen

dalam level ini berhubungan erat dengan dokumen *quality policy* dan *quality objectives* pada level 1, dokumen *quality manual* pada level 2, dan dokumen SOP pada level 3. Menurut standar ISO 9001:2008, setiap dokumen dalam level-level tersebut wajib memiliki dokumen ini sebagai pendukung. Hal ini ditujukan agar dokumen yang dihasilkan dapat dipertanggungjawabkan, dan prosesnya terkontrol sejak awal proses pembentukan hingga pelaksanaan.

#### 5. Dokumen *record*

Dokumen *record* berisi formulir maupun menu aplikasi yang digunakan untuk dokumentasi pelaksanaan prosedur.

Menurut standar ISO 9001:2008 mengenai *Quality Management Systems*, keseluruhan dokumen tata kelola memiliki 5 (lima) level dokumen seperti yang telah disebutkan sebelumnya. Sementara itu dokumen tata laksana yang merupakan bagian dari tata kelola, pembuatannya dimulai dari level dokumen prosedur hingga dokumen record.

### **2.1.3 Contoh Penerapan Tata Kelola dan Tata Laksana**

Berikut ini adalah beberapa contoh penelitian mengenai penerapan tata kelola dan tata laksana dalam lingkungan organisasi. Penelitian pertama dilakukan menggunakan model tata kelola TI berskala luas yaitu ISO/IEC 38500:2008 mengenai *Corporate Governance of Information Technology Standard*. Penelitian kedua dilakukan menggunakan model tata kelola TI ITIL v2 dan COBIT.

#### **2.1.3.1 Pembuatan Model Tata kelola TI menggunakan framework ISO/IEC 38500:2008**

Antonio Fernández dan Faraón Llorens (2009) menulis sebuah paper berjudul “*An IT Governance Framework for Universities in Spain*”. Paper ini merupakan penelitian mengenai penerapan *framework* tata kelola TI ISO/IEC 38500:2008 menjadi sebuah tata kelola TI bagi organisasi [ANT09]. Dalam penelitian ini, mereka membangun model tata kelola IT

bagi forum rektor di Spanyol atau yang lebih dikenal sebagai ITG4U (*IT Governance for University*).

Model tata kelola TI yang dihasilkan mereka adalah sebuah model tata kelola TI yang terdiri dari 3 level yaitu level pertama berisi 6 (enam) prinsip TI ISO/IEC 38500:2008, level kedua terdiri atas *IT Goal* beserta pemetaannya kepada prinsip TI di level pertama, dan level ketiga berupa matrik pengukuran kinerja pencapaian *IT Goal*.

Prinsip TI yang menjadi dasar model tata kelola TI yang dikembangkan kedua peneliti itu adalah 6 (enam) prinsip TI dalam ISO/IEC 38500:2008, yaitu *Responsibility, Strategy, Acquisition, Conformance, Performance, dan Human Behaviour*. Berangkat dari 6 (enam) prinsip TI ini, kemudian mereka mendefinisikan masing-masing *IT Goal* untuk model tata kelola TI yang dikembangkan. Referensi yang digunakan dalam menentukan *IT Goal* bersumber dari penelitian-penelitian mengenai *IT Governance* seperti JISC (*Joint Information System Comitee*), Weill Ross, Calder-Moir, dan Wim Van Grembergen.

Langkah selanjutnya yang dilakukan adalah memvalidasi masing-masing *IT Goal* tersebut. Ada 2 (dua) jenis validasi yang dilakukan yaitu validasi *IT Goal*, dan validasi relasi antara *IT Goal* dengan prinsip TI. Validasi *IT Goal* bertujuan untuk menentukan apakah *IT Goal* yang didefinisikan adalah penting buat organisasi dan apakah ada tujuan lain yang belum tercakup dalam *IT Goal*. Sedangkan validasi relasi *IT Goal* dengan prinsip TI bertujuan untuk menentukan *IT Goal* mana yang terpenting untuk masing-masing prinsip TI dan apakah masih ada relasi lain yang bisa dibangun antara *IT Goal* dan prinsip TI.

Setelah *IT Goal* didefinisikan dan divalidasi, langkah penelitian selanjutnya adalah membangun indikator untuk masing-masing *IT Goal* tersebut. Indikator yang dikembangkan adalah *maturity model* untuk model kematangan, *self-assessment toolkit* untuk pengukuran kinerja, *benchmark analysis* untuk menganalisa hasil pengukuran kinerja, dan *good practice guidance* untuk mengembangkan tata kelola hingga ke level tata laksana.

### **2.1.3.2 Pembuatan Model Tata Laksana menggunakan framework COBIT dan ITIL**

Christopher Laurence (2007) melakukan sebuah penelitian dengan judul “Pembuatan Tata Kelola TI untuk Sera SMS Service (dengan IT Service Management sesuai ITIL)”. Dalam penelitian ini dilakukan penerapan *framework* ITIL pada sebuah layanan TI yaitu Sera SMS Service dari sebuah organisasi bisnis [CLI07]. Hasil dari penelitian ini adalah sebuah *guideline* atau panduan pengoperasian Sera SMS Service berdasarkan *framework* ITIL.

Langkah pertama yang dilakukan dalam penelitian ini adalah menganalisa kondisi operasional saat ini. Kondisi operasional layanan Sera SMS Service dianalisa menggunakan sudut pandang *Service Level Management, Capacity Management, IT Service Continuity Management, dan Availability Management*. Kondisi operasional saat ini dianalisa untuk mengetahui permasalahan yang sedang dihadapi menurut sudut pandang organisasi, staf pelaksana dan customer.

Selanjutnya adalah menentukan proses-proses utama dalam keseluruhan layanan. Proses-proses utama layanan Sera SMS Service didefinisikan berdasarkan hasil analisa pelaksanaan layanan saat ini. Setelah penentuan proses-proses utama layanan, kemudian peneliti mengembangkan sebuah tata kelola yang berisi kebijakan (*policy*), standar dan aturan (*guideline and rule*), prosedur (*procedure*), dan kriteria (*standard*). Keseluruhan tata kelola dibangun berdasarkan *framework* ITIL v2.

Dalam membangun tata kelola layanan Sera SMS Service, peneliti juga membuat kriteria-kriteria untuk mengukur keberhasilan pelaksanaan masing-masing kebijakan (*policy*). Selain itu peneliti juga melakukan validasi atas tata kelola yang dihasilkan tersebut menggunakan model penilaian kematangan COBIT.

## **2.2 Framework ITIL**

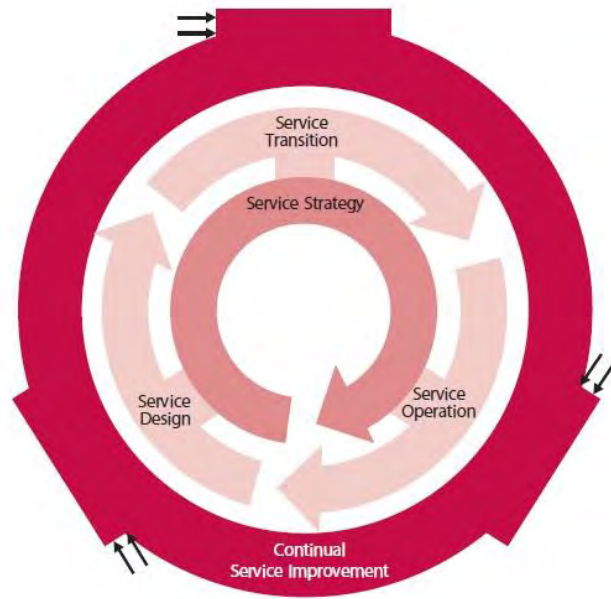
Dalam penelitian ini *framework* ITIL v3 (*Information Technology Infrastructure Library*) dipilih sebagai panduan mengembangkan tata laksana manajemen insiden pada

biro TI BPK-RI. *Framework* ini telah digunakan dalam berbagai organisasi di dunia oleh karena sifatnya *best practice* dan memiliki *library* yang siap pakai dalam mengembangkan suatu tata laksana. *Library* dalam *framework* ITIL dikembangkan berdasarkan prinsip-prinsip umum layanan TI dan telah diterima sebagai suatu konsep bersama.

ITIL adalah sebuah *framework* tata kelola TI yang berisi *best practice* secara khusus dalam manajemen *service* TI [ITL07]. Pada saat ini ITIL sudah dikembangkan hingga versi 3. Pada versi ini, *framework* ITIL dijelaskan tahapan-tahapan pengelolaan manajemen layanan TI yaitu sebagai *service lifecycle*. Gambar 2.1 menjelaskan rupa *framework* ITIL v3 sebagai *service lifecycle*.

Ada 5 proses *service lifecycle* dalam ITIL [ITL07], yaitu:

1. *Service Strategy*: Pada tahap ini dilakukan pengembangan strategi untuk mengubah manajemen *service* TI menjadi sebuah aset strategis dari organisasi.
2. *Service Design*: Pada tahap ini dilakukan pembangunan panduan manajemen layanan TI berdasarkan strategi yang sudah dikembangkan sebelumnya pada tahap *Service Strategy*. Selain itu panduan dibangun berdasarkan *policy* yang berlaku dalam organisasi dan untuk pemenuhan kepuasan pelanggan.
3. *Service Transition*: Pada tahap ini dilakukan proses transisi dari tata kelola yang lama kepada tata kelola yang baru yang sudah dikembangkan dalam tahap *Service Design*.
4. *Service Operation*: Pada bagian ini berisi langkah-langkah *best practice* untuk melakukan manajemen *service* TI.
5. *Continual Service Improvement*: Pada bagian ini dilakukan pengelolaan masukan dari pelanggan yang kemudian dikolaborasikan kedalam empat tahap diatas. Hal ini bertujuan untuk meningkatkan hasil keluaran dari kegiatan *Service Strategy*, *Service Design*, *Service Transition*, dan *Service Operation*.



Gambar 2.1 *Framework* ITIL v3

## 2.2.1 *Service Strategy*

### 2.2.1.1 Konsep utama *Service Strategy*

*Lifecycle Service Strategy* adalah langkah pertama untuk membuat keseluruhan proses ITIL. Proses inti yang dilakukan *lifecycle Service Strategy* adalah merencanakan *service* TI yang akan dibangun.

Hasil dari *lifecycle Service Strategy* adalah dokumen rencana strategis organisasi TI berupa *Service Portofolio*, yang menjadi dasar kerja bagi *lifecycle Service Design*. Selain itu *lifecycle Service Strategy* juga bertujuan mengubah manajemen *service* TI menjadi sebuah aset strategis organisasi, dengan menggunakan *framework* ITIL.

Dalam *lifecycle Service Strategy*, *framework* ITIL membutuhkan 4 faktor P, yaitu:

1. *Perspective*, yaitu pendefinisian visi dan misi dalam membangun manajemen *service* TI.
2. *Position*, yaitu pemahaman mengenai kondisi manajemen *service* TI saat ini.
3. *Plan*, yaitu perencanaan dalam membangun manajemen *service* TI.

4. *Pattern*, yaitu pemilihan cara membangun manajemen *service* TI.

#### 2.2.1.2 Proses utama *Service Strategy*

Berikut adalah proses-proses utama yang dilakukan dalam *lifecycle Service Strategy* :

1. *Financial Management*, yaitu manajemen biaya yang digunakan dalam *service* TI. Dalam *lifecycle* ini yang dilakukan adalah perencanaan sumber biaya dan besar biaya yang digunakan.
2. *Service Portfolio Management* (SPM), yaitu pengelolaan portofolio *service* TI yang digunakan organisasi.
3. *Demand Management*, yaitu manajemen kebutuhan *service* TI organisasi. Proses ini dilakukan agar setiap *service* TI yang direncanakan tidak mengalami kelebihan penggunaan oleh *user*.

#### 2.2.1.3 Fungsi dan Tanggungjawab dalam *Service Strategy*

Berikut adalah fungsi dalam *lifecycle Service Strategy* berikut tanggungjawabnya:

1. *Business Relationship Manager* (BRM), yaitu yang berfungsi untuk membangun hubungan bisnis yang baik dengan *customer*.
2. *Product Manager* (PM), yaitu yang bertanggungjawab dengan membangun manajemen *service* TI, berdasarkan hasil identifikasi *Business Relationship Manager* (BRM).
3. *Chief Sourcing Officer* (CSO), yaitu yang berfungsi untuk mengelola proses *sourcing service* TI dalam organisasi.

### 2.2.2 *Service Design*

#### 2.2.2.1 Konsep utama *Service Design*

*Lifecycle Service Design* bertujuan mendesain kebutuhan seluruh *service* TI berdasarkan dokumen *Service Portofolio* yang dihasilkan dalam *lifecycle Service Strategy*.

*Lifecycle Service Design* akan menghasilkan beberapa dokumen seperti *Service Design Package (SDP)*, *Service Level Agreements (SLA)*, *Operational Level Agreements (OLA)*, *Capacity Management Information System (CMIS)*, dan *Supplier and Contract Database (SCD)* yang akan digunakan dalam *lifecyle Service Transition*.

Dalam *lifecyle Service Design*, *framework* ITIL membutuhkan 4 faktor P, yaitu:

1. *People*, yaitu sumber daya manusia berupa tenaga, ketrampilan dan kompetensi dalam manajemen *service* TI.
2. *Products*, yaitu teknologi dan sistem manajemen yang digunakan dalam manajemen *service* TI.
3. *Processes*, yaitu proses, fungsi dan aktifitas yang terdefenisi dalam manajemen *service* TI.
4. *Partners*, yaitu pihak ketiga yang membantu organisasi dalam mengadakan manajemen *service* TI.

#### 2.2.2.2 Proses utama *Service Design*

Berikut adalah proses-proses utama yang dilakukan dalam *lifecyle Service Design*:

1. *Service Catalogue Management (SCM)*, yaitu katalog *service* TI yang berikut keterangan dan statusnya.
2. *Service Level Management (SLM)*, yaitu pengelolaan ekspektasi stakeholder (*agreement*) yang ditetapkan kepada masing-masing *service* TI.
3. *Capacity Management*, yaitu pengelolaan kapasitas sumber daya organisasi yang dapat diberikan kepada *service* TI, dan kapasitas informasi yang diharapkan dari *service* TI tersebut.
4. *Availability Management*, yaitu manajemen ketersediaan *service* TI. Hal ini ditujukan agar *service* TI dapat tersedia setiap saat sesuai target yang ditentukan.
5. *IT Service Continuity Management (ITSCM)*, yaitu manajemen kelangsungan *service* TI pada saat kritis. Proses ini sangat



terkait dengan proses manajemen resiko dan proses *Business Continuity Plan*.

6. *Information Security Management (ISM)*, yaitu pengelolaan keamanan informasi dalam manajemen *service TI*.
7. *Supplier Management*, yaitu pengelolaan kontrak pengadaan dan rekanan yang terkait dengan *service TI*.

### 2.2.2.3 Fungsi dan Tanggungjawab dalam *Service Design*

Berikut adalah fungsi dalam *lifecycle Service Design* berikut tanggungjawabnya:

1. *Service Design Manager*, yaitu yang bertanggungjawab dalam koordinasi dan seluruh proses pengembangan desain *service TI*.
2. *IT Designer/Architect*, yaitu yang bertanggungjawab dalam mendefinisikan teknologi, arsitektur, dan rancang bangun *service TI*.
3. *Service Catalogue Manager*, yaitu yang bertanggungjawab dalam membangun katalog *service TI*.
4. *Service Level Manager*, yaitu yang bertanggungjawab memastikan tercapainya ekspektasi stakeholder (*agreement*) dari *service TI*. Selain itu fungsi ini juga bertanggungjawab dalam menentukan ekspektasi stakeholder (*agreement*) bagi setiap *service TI*.
5. *Availability Manager*, yaitu yang bertanggungjawab dalam ketersediaan *service TI*.
6. *IT Service Continuity Manager*, yaitu yang bertanggungjawab dalam kelangsungan *service TI*.
7. *Capacity Manager*, yaitu yang bertanggungjawab memastikan terpenuhinya kapasitas *service TI*.
8. *Security Manager*, yaitu yang bertanggungjawab dalam hal penyediaan keamanan informasi *service TI*.
9. *Supplier Manager*, yaitu yang bertanggungjawab dalam pengelolaan kontrak pengadaan *service TI*.

### 2.2.3 *Service Transition*

#### 2.2.3.1 Konsep utama *Service Transition*

*Lifecycle Service Transition* bertujuan untuk memastikan seluruh *service* TI yang dibangun pada *lifecycle Service Design* sudah sesuai dengan kebutuhan *customer* organisasi. Dalam *lifecylce* ini banyak dilakukan proses evaluasi sehingga dari proses evaluasi tersebut dihasilkan dokumen *Request For Change* atas *service* TI.

Jika dalam proses evaluasi terdapat perubahan terhadap *service* TI, maka akan dilakukan desain ulang terhadap *service* TI tersebut pada *lifecycle Service Design*. Sedangkan jika tidak ada perubahan lagi terhadap *service* TI tersebut, maka *service* TI tersebut sudah boleh dijalankan sepenuhnya dalam *lifecycle Service Operation*.

#### 2.2.3.2 Proses utama *Service Transition*

Berikut adalah proses-proses utama yang dilakukan dalam *lifecycle Service Transition*:

1. *Change Management*, yaitu pengelolaan perubahan masing-masing *service* TI. Pada manajemen ini setiap perubahan pada *service* TI, akan direkam, dievaluasi, diotorisasi, didokumentasikan, dan direviu dalam tindakan yang terukur.
2. *Service Asset and Configuration Management*, yaitu pengelolaan aset yang digunakan berikut konfigurasi *service* TI.
3. *Knowledge Management*, yaitu manajemen pengetahuan dimana orang yang tepat harus mendapat informasi yang benar pada waktu yang tepat sehingga dapat mendukung proses bisnis utama.
4. *Transition Planning and Support*, yaitu proses perencanaan dan koordinasi penggunaan sumber daya organisasi, serta proses identifikasi dan pengelolaan resiko agar *service* TI dapat digunakan secara efektif pada *lifecycle Service Operation*.
5. *Release and Deployment Management*, yaitu proses pengelolaan keputusan penerbitan *service* TI yang baru. Setiap *service* TI

yang baru selesai dikembangkan, akan masuk ke dalam tahap ini untuk diketahui apakah service TI tersebut sudah layak untuk diluncurkan. Hal ini dilakukan untuk mengurangi resiko pasca produksi yang dapat muncul.

6. *Service Validation and Testing*, yaitu proses validasi service TI agar sesuai dengan kebutuhan bisnis dan SLA yang telah ditetapkan.
7. *Evaluation*, yaitu proses evaluasi untuk memastikan service TI apakah benar-benar berguna bagi bisnis utama organisasi.
8. *Service Transition Stage Operational Activities*, yaitu beberapa kegiatan operasional *lifecycle Service Transition* seperti pengelolaan komunikasi seluruh bagian manajemen service TI, pengelolaan organisasi manajemen, pengelolaan stakeholder, dan pengelolaan keseluruhan proses utama dalam *lifecycle Service Transition*.

#### 2.2.3.3 Fungsi dan Tanggungjawab dalam *Service Transition*

Berikut adalah fungsi dalam *lifecycle Service Transition* berikut tanggungjawabnya:

##### 1. Staf

*Lifecycle Service Transition* tidak memiliki fungsi struktur yang khusus sehingga dalam pelaksanaannya hanya difokuskan kepada staf yang disertai tanggungjawab. Fokus diberikan dalam bentuk pengorganisasian staf serta pemilihan staf dengan kemampuan dan pengalaman yang khusus.

#### 2.2.4 *Service Operation*

##### 2.2.4.1 Konsep utama *Service Operation*

*Lifecycle Service Operation* bertujuan untuk membuat seluruh service TI sesuai SLA yang disepakati dengan *customer*. Dalam prakteknya, *lifecycle Service Operation* harus dapat menyeimbangkan konflik antar hal-hal seperti sudut pandangan internal bagian TI dengan sudut pandang

eksternal bisnis, stabilitas dengan responsif, kualitas dengan biaya, hingga sifat reaktif dengan proaktif.

#### 2.2.4.2 Proses utama *Service Operation*

Berikut adalah proses-proses utama yang dilakukan dalam *lifecycle Service Operation*:

1. *Event Management Process*, yaitu proses pengelolaan setiap kejadian yang terkait dengan *service TI*.
2. *Incident Management Process*, yaitu proses manajemen insiden agar *service TI* dapat segera bekerja normal kembali.
3. *Request Fulfillment Process*, yaitu proses yang memungkinkan customer dapat meminta/menerima *service TI* terstandar, dan memberikan customer informasi lengkap mengenai *service TI* yang tersedia.
4. *Access Management Process*, yaitu proses manajemen akses *service TI* yang bertujuan untuk melindungi informasi dalam organisasi.
5. *Problem Management Process*, yaitu proses manajemen masalah *service TI*. Hal ini dilakukan dengan mendiagnosa masalah, menentukan resolusi atas masalah tersebut, dan memastikan resolusi tersebut telah diimplementasikan. Proses ini bertujuan untuk mengurangi efek yang terjadi dari masalah *service TI* tersebut.
6. *Common Service Operation Activities*, yaitu beberapa kegiatan operasional *lifecycle Service Operation* seperti pengawasan/pengendalian masalah, koordinasi penyelesaian masalah, manajemen sumber daya infrastruktur, dan kegiatan operasional dari *lifecyle service* lainnya.

#### 2.2.4.3 Fungsi dan Tanggungjawab dalam *Service Operation*

Berikut adalah fungsi dalam *lifecycle Service Operation* berikut tanggungjawabnya:

1. *Service Desk Function*, yaitu yang bertanggungjawab sebagai kontak utama untuk seluruh pengguna *service* TI. Selain itu juga bertanggungjawab dalam pencatatan dan penanganan seluruh insiden, pengelolaan kebutuhan *service* dan akses, serta penyediaan antar muka proses dan aktifitas lainnya dari *lifecycle Service Operation*.
2. *Technical Management Function*, yaitu yang terdiri dari banyak sumber daya manusia yang handal dalam perencanaan, implementasi, dan penanganan teknis masalah perangkat keras dalam organisasi.
3. *Application Management Function*, yaitu yang terdiri dari banyak sumber daya manusia yang handal dalam perencanaan, implementasi, dan penanganan teknis masalah perangkat lunak dalam organisasi.
4. *IT Operations Management Function*, yaitu yang terdiri dari banyak sumber daya manusia yang handal dalam perencanaan, implementasi, dan penanganan teknis masalah infrastruktur dalam organisasi. Fungsi ini terbagi menjadi dua bagian yaitu *IT Operation Control* yang bertanggungjawab dalam kegiatan operasional rutin, dan *Facilities Management* yang bertanggungjawab dalam manajemen *data centre*, ruangan komputer dan ruang *recovery*, serta koordinasi proyek konsolidasi *server/data centre*.

## 2.2.5 *Continual Service Improvement*

### 2.2.5.1 Konsep utama *Continual Service Improvement*

*Lifecycle Continual Service Improvement* adalah *lifecyle* yang bertujuan meningkatkan kualitas *service* TI dengan cara melakukan evaluasi dan menilai kematangan secara berkala.

### 2.2.5.2 Proses utama *Continual Service Improvement*

Berikut adalah proses-proses utama yang dilakukan dalam *lifecycle Continual Service Improvement*:

1. *7-Step Improvement Process*, yaitu langkah-langkah yang dilakukan dalam meningkatkan kualitas suatu *service* TI. Langkah-langkah ini meliputi pengumpulan data, analisa data untuk mengetahui isu dan trend, memberikan informasi kepada pihak manajemen, dan kemudian implementasi peningkatan kualitas.

Berikut adalah ketujuh langkah tersebut:

- *Step 1 – Define what you should measure*, yaitu mendefinisikan faktor-faktor yang akan diukur.
  - *Step 2 – Define what you can measure*, yaitu mendefinisikan faktor-faktor yang dapat kita ukur.
  - *Step 3 – Gather the data*, yaitu pengumpulan data.
  - *Step 4 – Process the data*, yaitu pemrosesan data.
  - *Step 5 – Analyze the data*, yaitu analisa data.
  - *Step 6 – Present and use the Information*, yaitu presentasi hasil analisa data berupa informasi.
  - *Step 7 – Implement corrective action*, yaitu implementasi tindakan koreksi.
2. *Service Measurement*, yaitu proses pengukuran pencapaian *service* TI. Proses ini meliputi pengukuran *technology metrics* (berupa penilaian performa dan ketersediaan), *process metrics* (berupa *Critical Success Factors* dan *Key Performance Indicators*), dan *service metrics* (penilaian keseluruhan pelaksanaan *service* TI)
  3. *Service Reporting*, yaitu proses pelaporan kondisi *service* TI berikut tindakan historis yang dilakukan terhadapnya.

### 2.2.5.3 Fungsi dan Tanggungjawab dalam *Continual Service Improvement*

Berikut adalah fungsi dalam *lifecycle Continual Service Improvement* berikut tanggungjawabnya:

1. *CSI Manager*, yaitu yang bertanggungjawab atas pelaksanaan *lifecycle Continual Service Improvement*.

## 2.3 Proses Manajemen Insiden (*Incident Management*)

Menurut *framework* ITIL, pengertian insiden adalah sebuah interupsi atau pengurangan kualitas dari layanan TI. Selain itu sebuah kesalahan konfigurasi pada sistem dapat dikatakan sebagai insiden walaupun belum menimbulkan masalah yang berarti pada sistem tersebut. Manajemen insiden (*incident management*) adalah proses yang dilakukan untuk menyelesaikan suatu insiden. Proses manajemen insiden (*incident management*) dilakukan berdasarkan input dari user melalui service desk, laporan teknisi, dan juga deteksi otomatis dari sebuah tool *event management*. Manajemen insiden (*incident management*) pada *framework* ITIL v3 berada pada *cycle Service Operation* [TSO07].

Tujuan utama dari manajemen insiden (*incident management*) adalah untuk mengembalikan kondisi layanan TI ke keadaan normal secepat mungkin, dan meminimalkan dampak negatif yang ditimbulkan terhadap kegiatan bisnis utama organisasi. Keadaan normal layanan TI adalah keadaan yang telah didefinisikan sebelumnya dalam sebuah SLA (*Service Level Agreement*).

Manajemen insiden (*incident management*) memiliki beberapa nilai utama bagi proses bisnis organisasi, yaitu:

1. Mengurangi waktu downtime proses bisnis, karena kemampuannya untuk mendeteksi dan menyelesaikan suatu insiden.
2. Menggunakan sumber daya yang ada secara dinamis.
3. Mengidentifikasi potensi peningkatan kualitas layanan TI.
4. Dalam menangani insiden, *Service Desk* dapat juga mengidentifikasi kebutuhan layanan atau pelatihan yang dibutuhkan.

Sebelum membangun manajemen insiden (*incident management*), dibutuhkan kesepakatan bersama mengenai jumlah waktu penanganan insiden dan hal ini wajib

dituangkan dalam SLA. Kesepakatan ini dapat dibuat berdasarkan laporan penanganan insiden selama ini ataupun target yang ditetapkan bersama.

Selain penetapan waktu maksimal penanganan insiden, perlu juga dibangun sebuah model insiden (*incident model*) yang berisi ringkasan proses manajemen insiden. Model insiden dibangun berdasarkan proses penanganan insiden yang umum terjadi dan sering dilakukan selama ini. Dari model insiden ini kemudian akan dibangun perangkat penanganan insiden yang dibutuhkan. Model insiden wajib memiliki hal-hal berikut ini: langkah-langkah penanganan insiden, kronologis beserta langkah-langkah tambahan yang diperlukan, para penanggungjawab, jangka waktu penyelesaian insiden, prosedur jika terjadi eskalasi insiden, dan kegiatan tambahan untuk kasus insiden terkait *security* (keamanan sistem) dan *capacity* (kapasitas sistem).

Berikut adalah aktifitas-aktifitas dalam manajemen insiden (*incident management*) menurut *framework* ITIL v3 seperti yang juga ditampilkan pada gambar 2.2 [TSO07]:

1. Identifikasi insiden (*incident identification*)

Proses manajemen insiden (*incident management*) dimulai dengan identifikasi. Identifikasi yang paling umum dilakukan adalah melalui layanan *service desk* dan laporan dari staf teknis. Selain itu identifikasi insiden dapat dilakukan secara otomatis oleh tool *event management* yang dipasang pada perangkat-perangkat utama. Kondisi ideal dari langkah identifikasi adalah insiden dapat teridentifikasi sebelum terjadi implikasi terhadap *user*.

2. Pencatatan insiden (*incident logging*)

Langkah ini wajib dilakukan untuk setiap jenis insiden baik yang berskala besar maupun kecil. Beberapa informasi yang harus dicatat terkait suatu insiden adalah ID, kategori insiden, waktu terjadi, deskripsi insiden, nama orang/grup yang bertanggungjawab atas penanganan, implikasi insiden, dan waktu penutupan kasus.

3. Pengkategorisasian insiden (*incident categorization*)

Dalam membuat kategori insiden dibutuhkan sebuah proses khusus antara pengelola TI dan pihak manajemen organisasi. Hal ini bertujuan untuk menghasilkan kategori insiden dan prioritas penanganannya sejalan dengan proses bisnis organisasi. Kategori insiden dapat dibuat berdasarkan jenis



insiden, perkiraan lamanya penanganan, implikasi terhadap proses bisnis organisasi, atau jumlah staf teknis terkait.

4. Prioritas insiden (*incident prioritization*)

Langkah prioritas insiden dilakukan berdasarkan kategorisasi yang telah dibuat sebelumnya. Prioritas penanganan insiden dapat dilakukan berdasarkan besarnya implikasi insiden terhadap kegiatan bisnis utama organisasi, ataupun berdasarkan lamanya penanganan insiden.

5. Diagnosa awal (*initial diagnosis*)

Diagnosa awal terhadap insiden wajib dilakukan oleh setiap pihak yang pertama kali berhubungan dengan insiden baik itu *service desk*, staf teknis, maupun perangkat otomatis seperti *event management*. Jika insiden ditemukan oleh *service desk* melalui telepon dari *user*, maka diusahakan *service desk* tersebut yang menyelesaikan insiden selama *user* masih berhubungan telepon.

6. Eskalasi insiden (*incident escalation*)

Eskalasi insiden adalah tindakan menaikkan level penanganan insiden. Hal ini berkaitan erat dengan hasil diagnosa awal terhadap insiden. Jika dari diagnosa ditemukan insiden yang tidak dapat ditangani, maka wajib dilakukan eskalasi insiden. Eskalasi insiden ada 2 macam, yaitu eskalasi fungsi dan eskalasi hierarki. Eskalasi fungsi adalah tindakan menaikkan level penanganan kepada satu level di atasnya. Sedangkan eskalasi hierarki adalah tindakan menaikkan level penanganan melintasi hirarki organisasi misalnya kepada manajer IT atau manajer bisnis yang terkait.

7. Investigasi (*investigation and diagnosis*)

Tindakan investigasi dilakukan untuk menemukan sumber masalah dari insiden. Dalam melakukan investigasi, setiap tindakan wajib dilaporkan juga ke dalam formulir insiden. Hal ini berguna sebagai data historis tindakan penanganan suatu insiden.

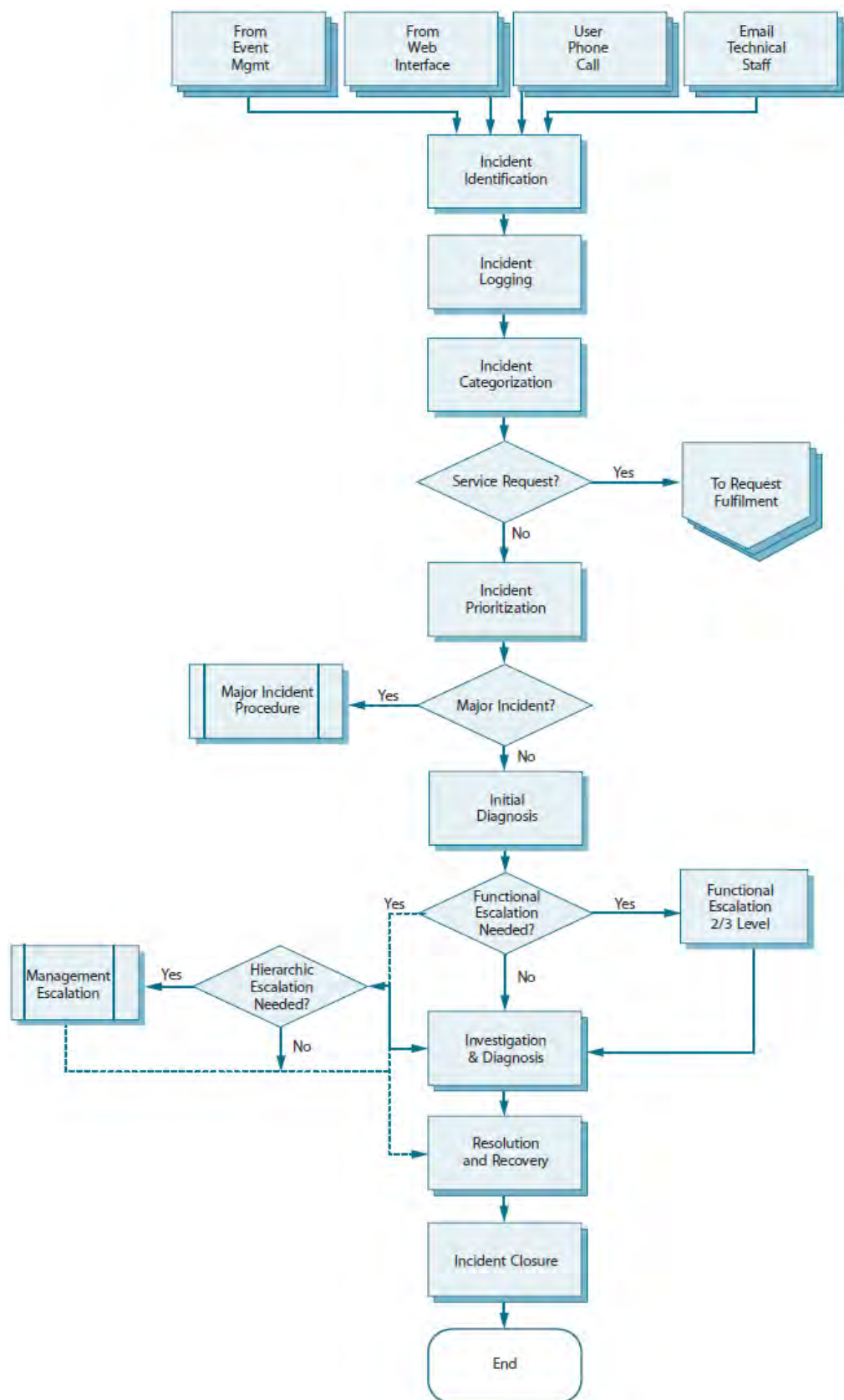
8. Resolusi (*resolution and recovery*)

Langkah ini merupakan tindakan yang diambil untuk menyelesaikan suatu insiden. Langkah resolusi dapat dilakukan oleh *service desk* sebagai pihak yang pertama menemukan insiden dari *user*, staf teknis yang sedang

mengerjakan kegiatan konfigurasi, maupun oleh supplier terhadap perangkat yang masih dalam garansi.

9. Penutupan (*incident closure*)

Langkah penutupan adalah langkah yang dilakukan oleh *service desk* maupun staf teknisi terkait untuk memastikan apakah insiden telah benar selesai ditangani. Yang harus diperhatikan dalam langkah penutupan ini adalah dokumentasi proses penanganan insiden, perkiraan terhadap perulangan insiden, dan survei kepuasan *user* atas penanganan insiden.



Gambar 2.2 ITIL *Incident Management*

Proses manajemen insiden (*incident management*) terkait erat dengan beberapa proses lain *framework* ITIL v3, antara lain *Problem Management*, *Configuration Management*, *Change Management*, *Capacity Management*, *Availability Management*, dan *Service Level Management*.

Kaitan dengan proses-proses tersebut adalah sebagai berikut:

1. *Problem Management*

Manajemen insiden (*incident management*) melakukan tugas penanganan insiden dan memastikan insiden yang terjadi tidak akan terulang lagi. Jika diketahui insidennya memiliki lingkup yang luas, maka informasi dalam manajemen insiden (*incident management*) akan menaikkan menjadi titik tolak proses *problem management* untuk menyelesaikan masalah tersebut.

2. *Configuration Management*

Manajemen insiden melakukan tugas penanganan insiden berdasarkan konfigurasi yang tersimpan dalam *configuration management*. Data-data mengenai sistem yang dibutuhkan dalam penanganan insiden diambil dari sistem *configuration management*.

3. *Change Management*

Ketika dalam penanganan insiden ditemukan suatu kebutuhan perubahan atas sistem, maka manajemen insiden akan meneruskan informasi kebutuhan perubahan tersebut dalam format RFC (*Request For Change*) kepada *change management* untuk diproses.

4. *Capacity Management*

Manajemen insiden (*incident management*) menyediakan *trigger* atau penanda jika terjadi penurunan kinerja sistem pada suatu insiden yang ditemukan. Kemudian *capacity management* akan melakukan proses penanganan masalah kinerja ini.

5. *Availability Management*

Manajemen insiden (*incident management*) akan menyediakan data kepada *availability management* sebagai dasar analisa ketersediaan layanan.

6. *Service Level Management*

Manajemen insiden (*incident management*) menggunakan *service level management* dalam menetapkan SLA (*Service Level Agreement*) bagi proses penanganan insiden.

Pelaksanaan manajemen insiden (*incident management*) memerlukan kegiatan pengukuran. Pengukuran manajemen insiden menurut *framework* ITIL berupa jumlah insiden yang berhasil ditangani sesuai jangka waktu pada SLA (*service level agreement*), biaya rata-rata yang dikeluarkan untuk penanganan suatu insiden, jumlah insiden yang tidak benar ditangani, dan lain sebagainya. Pengukuran ini bertujuan untuk mengetahui sejauh mana pelaksanaan manajemen insiden dan apakah sudah sesuai dengan harapan manajemen organisasi, dalam hal ini sesuai dengan kesepakatan bersama pada SLA (*service level agreement*).

#### 2.4 Responsibility Assignment Matrix (RAM)

*Responsibility Assignment Matrix* (RAM) merupakan suatu bentuk pemetaan sumber daya kepada aktifitas dalam tiap prosedur. Dalam hal ini sumber daya tersebut adalah masing-masing pelaksana aktifitas.

Model RAM yang akan digunakan dalam dokumen tata laksana adalah diagram RACI (*Responsible, Accountable, Consult, Inform*). *Responsible* mengacu kepada pihak pelaksana yang harus bertanggungjawab melaksanakan dan menyelesaikan aktifitas yang menjadi tanggungjawabnya. *Accountable* mengacu kepada pihak pelaksana yang harus mengarahkan jalannya pelaksanaan aktifitas. *Consult* mengacu kepada pihak pelaksana yang akan menjadi tempat konsultasi selama pelaksanaan aktifitas. *Inform* mengacu kepada pihak pelaksana yang akan menjadi pihak yang diberikan informasi mengenai pelaksanaan aktifitas. Tabel 2.1 adalah contoh penerapan diagram RACI pada dokumen tata laksana.

Tabel 2.1 Contoh penerapan diagram RACI

No.	Langkah	U	HO	HS	IM	SM	NM	MM
1.	Deteksi insiden	AR						
2.	Pelaporan insiden	AR	R					
3.	Membuka kartu insiden		AR	I		I	I	I

--- Halaman ini dikosongkan ---

## **BAB 3**

### **Metodologi Penelitian**

Pada bab ini akan diterangkan mengenai tahapan-tahapan penelitian yang akan dilakukan dalam membuat tata laksana manajemen insiden pada biro Teknologi Informasi BPK-RI. Secara garis besar tahapan-tahapan tersebut adalah:

1. Pengumpulan Informasi dan Analisa
2. Pembuatan Dokumen Tata Laksana
3. Verifikasi Dokumen Tata Laksana
4. Validasi Dokumen Tata Laksana
5. Kesimpulan

#### **3.1 Tahap Pengumpulan Informasi dan Analisa**

Sesuai dengan paparan pada latar belakang penelitian, kondisi existing pelaksanaan manajemen insiden di BPK-RI saat ini belum sesuai sepenuhnya dengan standar yang ada. Aktifitas-aktifitas yang dilakukan belum sesuai dengan tahapan yang disebutkan dalam *framework* ITIL. Oleh karena itu pada tahap pengumpulan informasi ini akan difokuskan kepada studi literatur. Pada tahap ini dilakukan studi literatur pada 2 (dua) macam dokumen, yaitu:

1. Penelaahan dokumen BPK-RI

Pada sub tahap ini dilakukan pemahaman dokumen terkait dengan layanan TI oleh biro TI BPK-RI. Dokumen yang dipelajari mencakup dokumen Rencana Strategis TI BPK-RI, dokumen kebijakan dan panduan dukungan TI, dan dokumen struktur organisasi biro TI BPK-RI.

Telaah dokumen rencana strategis TI dilakukan untuk mengetahui model tata kelola yang digunakan oleh biro TI dan program apa saja yang ditentukan untuk menjalankan rencana strategis TI tersebut. Sementara telaah dokumen kebijakan dan panduan dukungan TI dilakukan untuk mengetahui kondisi mengenai proses penanganan insiden yang sedang dilakukan pada saat ini.

Selain itu telaah dokumen struktur organisasi dilakukan dalam rangka perancangan diagram RACI (*Responsible Accountable Consulted Informed*) sebagai bagian dari dokumen tata laksana yang akan dibuat. Diagram RACI yang dibuat akan memperhatikan jumlah staf yang terlibat dalam proses manajemen insiden dan masing-masing penanggungjawab dari aktifitas manajemen insiden.

## 2. Studi literatur *framework* ITIL

Pada sub tahap studi literatur *framework* ITIL, dilakukan pemahaman mengenai *framework* ITIL dan contoh-contoh implementasinya pada organisasi yang lain. Sumber literatur utama adalah dokumen *Service Operation* dari *framework* ITIL.

Beberapa analisa yang dilakukan dalam tahap ini adalah:

- a. Menentukan aktifitas yang akan dikembangkan menjadi prosedur dalam dokumen manajemen insiden.
- b. Menghubungkan kebijakan dukungan TI dengan prosedur yang akan dibuat.
- c. Menentukan proses TI yang akan terkait dengan manajemen insiden sebagai proses input dan output-nya. Dasar penentuan proses TI tersebut diambil dari dokumen *framework* ITIL mengenai proses manajemen insiden.
- d. Menentukan tujuan dari masing-masing prosedur dan kemudian menentukan indikator kinerja pelaksanaan tujuan tersebut. Penentuan tujuan dilakukan dengan memperhatikan deskripsi masing-masing aktifitas yang ditentukan *framework* ITIL mengenai proses manajemen insiden.
- e. Menetapkan sumber daya dan batasan dalam melaksanakan prosedur. Pada tahap ini yang ditetapkan adalah pihak-pihak yang akan terlibat dalam aktifitas, waktu pelaksanaan aktifitas, dan batasan pelaksanaan/ruang lingkup aktifitas.
- f. Merinci pelaksanaan masing-masing aktifitas. Proses perincian masing-masing aktifitas dilakukan dengan mengembangkan rincian masing-masing aktifitas dalam *framework* ITIL mengenai proses manajemen insiden.



- g. Menentukan format dokumen pendukung dan formulir yang akan digunakan dalam pelaksanaan prosedur.

Hasil dari studi literatur *framework* ITIL ini kemudian dikombinasikan dengan hasil telaah dokumen BPK-RI, akan digunakan dalam pembuatan dokumen tata laksana pada tahap berikutnya.

### **3.2 Tahap Pembuatan Dokumen Tata Laksana**

Pada tahap ini dilakukan pembuatan draft dokumen tata laksana manajemen insiden menurut hasil analisa sebelumnya. Draft dokumen tata laksana yang dibuat akan terdiri atas prosedur, dan formulir. Selain itu draft dokumen tata laksana ini juga berisi matriks tata laksana sebagai kesimpulan dari keseluruhan prosedur, dan formulir yang telah dibuat sebelumnya.

Prosedur yang dibuat, secara khusus akan dihubungkan dengan kebijakan dukungan TI yang mengatur mengenai kategori insiden, prioritas insiden, pengukuran kinerja atau CSF (*Critical Success Factor*), dan target waktu penanganan insiden yang dituangkan dalam sebuah SLA (*Service Level Agreement*). Selain dokumen diatas, akan dibuat juga diagram flow chart yang menggambarkan tiap aktifitas yang dilakukan, dan diagram RACI yang menggambarkan fungsi pelaksana dalam masing-masing prosedur.

### **3.3 Tahap Verifikasi Dokumen Tata Laksana**

Tahap verifikasi dilakukan pada masing-masing bagian dari dokumen tata laksana. Verifikasi diperlukan untuk menentukan apakah draft dokumen yang dihasilkan sudah sesuai dengan yang diinginkan. Bagian-bagian yang diverifikasi adalah masing-masing aktifitas manajemen insiden, dan lampiran-lampiran dokumen seperti kategori insiden, prioritas insiden, metrik dan CSF (*Critical Success Factor*), SLA (*Service Level Agreement*) serta diagram RACI

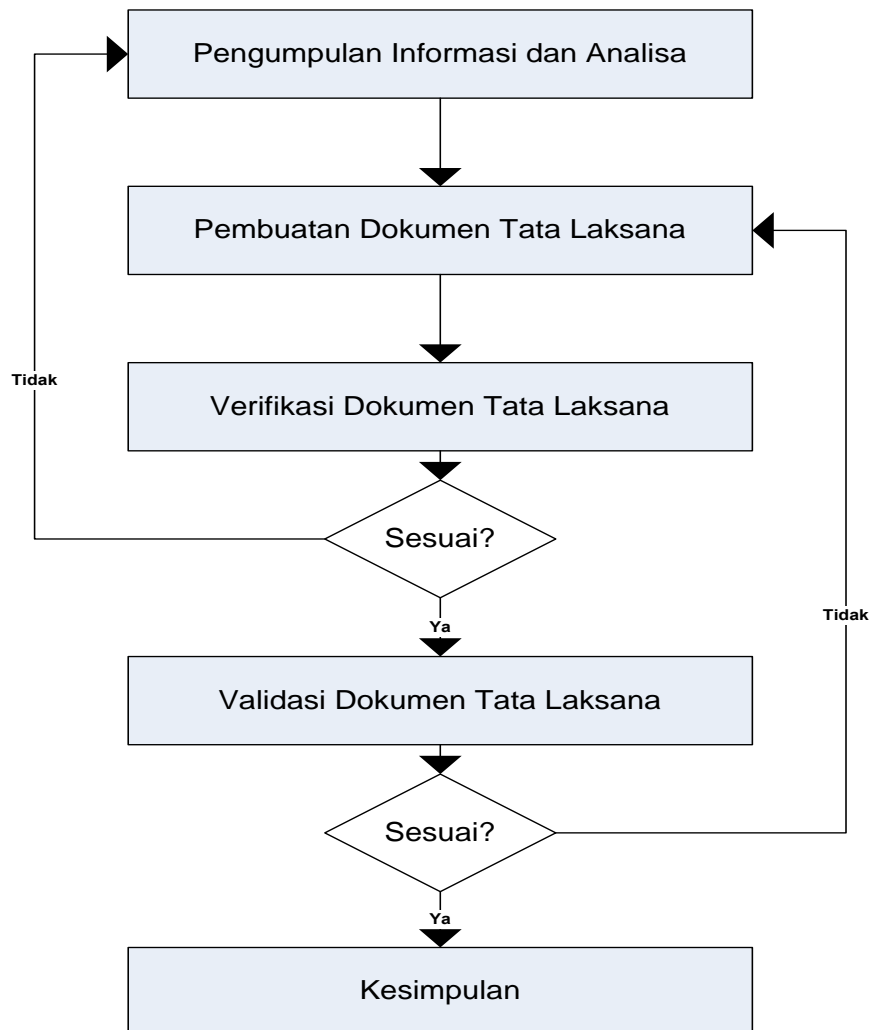
### **3.4 Tahap Validasi Dokumen Tata Laksana**

Pada tahap ini dilakukan validasi dokumen tata laksana dengan menguji apakah tujuan dari proses manajemen insiden sudah terpenuhi dengan dokumen ini. Validasi dilakukan dengan meminta *acceptance letter* dari manajemen biro TI.

### 3.5 Tahap Kesimpulan

Pada tahap ini dilakukan perumusan kesimpulan dan saran mengenai pembuatan tata laksana manajemen insiden pada biro Teknologi Informasi BPK-RI.

Gambar 3.1 menjelaskan mengenai tahap-tahap yang akan dilakukan dalam penelitian ini.



Gambar 3.1 Metodologi Penelitian

## **BAB 4**

### **Hasil Penelitian dan Pembahasan**

#### **4.1 Profil BPK-RI**

BPK-RI adalah lembaga tinggi negara berdasarkan UUD 1945 Perubahan Ketiga Bab VIII A, yang memiliki kewajiban dalam hal pemeriksaan pengelolaan dan tanggung jawab keuangan negara. Kewenangan BPK-RI dalam memeriksa pengelolaan dan tanggung jawab keuangan negara lebih lanjut diperjelas dengan UU No. 15 Tahun 2006 mengenai Badan Pemeriksa Keuangan [BPK06].

BPK-RI memiliki visi dan misi untuk mencapai tujuan utamanya dalam pemeriksaan pengelolaan dan tanggung jawab keuangan negara. Visi BPK-RI adalah “Menjadi lembaga pemeriksa keuangan negara yang bebas, mandiri dan profesional serta berperan aktif dalam mewujudkan tata kelola keuangan negara yang akuntabel dan transparan”. Sedangkan misi BPK-RI adalah “Memeriksa pengelolaan dan tanggung jawab keuangan negara dalam rangka mendorong terwujudnya akuntabilitas dan transparansi keuangan negara, serta berperan aktif dalam mewujudkan pemerintahan yang baik, bersih dan transparan”.

Biro TI BPK-RI didirikan untuk mendukung visi dan misi tersebut. Tujuan didirikannya biro TI ini disesuaikan dengan konteks visi dan misi yang telah dipaparkan diatas. Konteks pertama adalah BPK-RI sebagai lembaga pemeriksa keuangan negara, yang berarti TI harus menjadi tulang punggung utama seluruh proses bisnis di BPK-RI. Konteks kedua adalah BPK-RI harus berperan aktif, yang berarti TI harus memberi sumbangan sebagai media komunikasi dan informasi yang tidak mengenal batas waktu, dan wilayah. Konteks ketiga adalah BPK-RI mewujudkan akuntabilitas dan transparansi, yang berarti TI harus menjamin terciptanya tata kelola informasi yang baik.

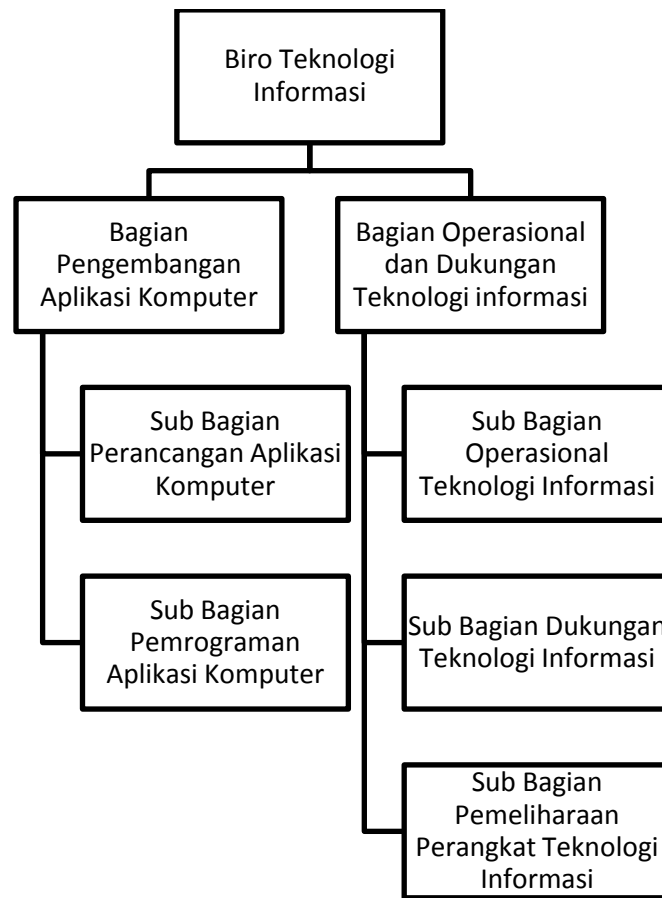
Biro TI BPK-RI, seperti yang terlihat pada gambar 4.1, terdiri dari 2 (dua) bagian yaitu bagian Pengembangan Aplikasi Komputer, dan bagian Operasional dan Dukungan TI. Bagian Pengembangan Aplikasi Komputer bertugas dalam perancangan dan pemrograman aplikasi komputer yang dibutuhkan oleh manajemen. Sedangkan bagian Operasional dan Dukungan TI bertugas melayani kebutuhan pegawai dalam hal *trouble*

*shooting* jaringan dan perangkat lunak/keras, serta pemeliharaan seluruh perangkat TI di BPK-RI [BPK07].

Bagian Pengembangan Aplikasi Komputer terdiri dari 2 sub bagian yaitu, sub bagian Perancangan Aplikasi dan sub bagian Pemrograman Aplikasi. Sub bagian Perancangan Aplikasi bertugas dalam menerima masukan dari pimpinan, dan pengguna aplikasi sistem informasi BPK-RI mengenai aplikasi yang ingin dikembangkan selanjutnya. Sedangkan sub bagian Pemrograman Aplikasi bertugas dalam pengembangan dan pemeliharaan aplikasi sistem informasi BPK-RI.

Bagian Operasional dan Dukungan TI terdiri dari 3 sub bagian yaitu, sub bagian Operasional TI, sub bagian Dukungan TI, dan sub bagian Pemeliharaan Perangkat TI. Sub bagian Operasional TI bertugas dalam pengembangan sumber daya *network* BPK-RI yang meliputi kegiatan perencanaan, implementasi dan pemeliharaan. Sub bagian Dukungan TI bertugas dalam penyediaan dukungan TI bagi seluruh pegawai BPK-RI dalam hal TI. Dukungan TI yang disediakan sub bagian Dukungan TI (sub bagian Dukungan TI) terdiri dari 3 (tiga) proses TI utama yaitu *helpdesk*, manajemen aset TI, dan manajemen insiden yang akan dijelaskan selanjutnya di paragraf bawah. Sedangkan sub bagian Pemeliharaan Perangkat TI bertugas dalam pemeliharaan berkala perangkat TI maupun *maintenance* perangkat TI yang tidak dapat diselesaikan oleh sub bagian Dukungan TI.

Layanan TI yang dilakukan oleh sub bagian Dukungan TI BPK-RI antara lain mengelola keluhan pegawai mengenai perangkat PC/Laptop dan aplikasi sistem informasi, peminjaman perangkat keras komputer (seperti in-focus, laptop dan printer), mengelola perbaikan perangkat keras komputer, dan mendukung setiap kegiatan rapat/pertemuan seluruh unit kerja di kantor pusat.



Gambar 4.1 Struktur organisasi Biro TI BPK-RI

Biro TI BPK-RI memiliki dokumen Rencana Strategis TI yang menjabarkan arah pengembangan TI agar selaras menurut Rencana Strategis BPK-RI. Dokumen Rencana Strategis TI BPK-RI 2006-2010 menyebutkan 3 (tiga) fokus utama pengembangan TI di BPK, yaitu TI sebagai alat bantu pengelolaan data, informasi dan pengetahuan yang dimiliki BPK-RI, TI sebagai alat bantu dalam proses pengambilan keputusan, dan TI sebagai alat bantu pendukung kegiatan proses bisnis sehari-hari. [BTI06]

Ketiga fokus ini kemudian dijabarkan dalam 10 (sepuluh) inisiatif strategis pengembangan TI BPK-RI, dan 5 (lima) kelompok inisiatif strategis pendukung. 10 (sepuluh) inisiatif strategis ini adalah sebagai berikut:

1. Memperbaiki infrastruktur TI dan komunikasi karena terlihat masih rendahnya kinerja infrastruktur komunikasi antara kantor pusat dengan kantor perwakilan, terutama terkait dengan besarnya *bandwidth* yang tersedia.

2. Mengembangkan sebuah *data warehouse* di level organisasi pusat dan daerah, dengan cara menerapkan sistem manajemen dokumen berbasis elektronik yang disimpan dalam gudang data tersebut.
3. Memperbaiki dan merevisi berbagai aplikasi yang sebenarnya sudah dibangun oleh BPK-RI selama ini, dan melengkapinya dengan beragam aplikasi lain, untuk kemudian diintegrasikan dengan sebuah tool sistem manajemen workflow yang harus diadakan.
4. Mengimplimentasikan konsep manajemen pengetahuan (*knowledge management*) dan konsep *business intelligent* untuk para auditor dan pengambil keputusan.
5. Mengembangkan *cockpit management system* untuk memantau kinerja organisasi secara keseluruhan yang bisa dimanfaatkan oleh internal maupun eksternal stakeholder.
6. Mengimplimentasikan konsep kantor maya (*virtual office*), untuk meningkatkan efisiensi dan optimalisasi penggunaan sumber daya yang terbatas.
7. Melakukan pemantapan struktur organisasi yang terkait dengan divisi TI agar dapat lebih responsif menjawab kepentingan pengguna dan organisasi.
8. Membentuk divisi manajemen proyek (*Project Management Office*) untuk mengelola berbagai proyek pengembangan TI terutama yang bersifat inovatif sebagai hasil dari program riset dan pengembangan.
9. Meningkatkan keberdayaan para sumber daya manusia dari BPK-RI agar mereka dapat memperoleh manfaat maksimal dari aplikasi TI yang tersedia (*e-literacy*).
10. Menjalankan konsep tata kelola TI (*IT Governance*) secara efektif dengan mengikuti standar internasional yang ada.

Sedangkan 5 (lima) kelompok inisiatif strategis pendukung meliputi kelompok proses (*process*), sumber daya manusia (*people*), perangkat keras (*hardware*), perangkat lunak (*software*), dan database.

Inisiatif strategis pendukung pada kelompok proses (*process*) memiliki 7 (tujuh) program kerja dalam Rencana Strategis TI BPK-RI 2006-2010, yaitu:

1. Mempersingkat proses audit melalui kapabilitas teknologi (*streamline the audit chain through technology capabilities*).
2. Memberdayakan dan mengoptimasi sumber daya organisasi (*leverage and optimize organization limited resources*).
3. Mengimplementasi standar best practice manajemen TI (*implement best-practice standard for IT management*).
4. Merancang mekanisme kerjasama antar bagian dengan TI (*promote inter-departmental IT relationship mechanism*).
5. Melembagakan penggunaan TI dalam organisasi (*institutionalise IT usage within the organization*).
6. Membangun panduan TI dan prosedur (*develop IT policies and procedures*).
7. Membangun manajemen *helpdesk* dan dukungan TI (*form helpdesk and supporting system*).

Dalam pelaksanaannya, program ketujuh dari inisiatif strategis pendukung pada kelompok proses (*process*) dilaksanakan sepenuhnya oleh sub bagian Dukungan TI. Pelaksanaan kegiatan dukungan TI sehari-hari sebagian besar berupa kegiatan penanganan insiden yang dialami oleh segenap pimpinan dan pegawai BPK-RI. Hal ini menjadi dasar kaitan antara program manajemen *helpdesk* dan dukungan TI dengan proses TI manajemen insiden dari *framework* ITIL.

Dari hasil telaah dokumen Rencana Strategis BPK-RI beserta dokumen pendukungnya, diketahui bahwa belum semua program yang tercantum dalam inisiatif strategis dikembangkan menjadi sebuah dokumen standar tata kelola TI BPK-RI. Dalam pelaksanaan kegiatan layanan sehari-hari, biro TI menyerahkan tiap-tiap bagian dan sub bagian untuk mengembangkan sendiri dokumen tata laksana menurut kebutuhannya masing-masing.

Hasil telaah juga menunjukkan dokumen kebijakan dan panduan untuk program manajemen *helpdesk* dan dukungan TI dikembangkan oleh sub bagian Dukungan TI. Dokumen ini dikembangkan sendiri oleh sub bagian Dukungan TI dan belum mendapat pengesahan dari biro TI. Hal ini juga terjadi pada sub bagian lain yang mengembangkan kebijakan dan panduan serta prosedur sendiri untuk masing-masing layanan yang dilaksanakannya.

Dari hasil konfirmasi dengan Kepala sub bagian Dukungan TI, diketahui untuk pelaksanaan layanan dukungan TI belum memiliki dokumen tata laksana yang terstandar. Dokumen tata laksana yang ada pada sub bagian Dukungan TI adalah dokumen tata laksana untuk berbagai layanan TI yang dilakukan oleh sub bagian Dukungan TI. Layanan tersebut antara lain adalah *helpdesk*, dukungan TI, pengelolaan arsip, dan administrasi hak akses terkait intranet/internet.

## **4.2 Kebijakan**

Biro TI memiliki kebijakan terkait program manajemen help desk dan dukungan TI, yaitu kebijakan dukungan TI [BKI07].

### **4.2.1 Kebijakan mengenai fungsi sub bagian dan penanggungjawab penanganan insiden**

Kebijakan ini berkaitan dengan fungsi masing-masing pihak pelaksana dalam proses manajemen insiden. Selain itu kebijakan ini menjadi dasar bagi biro TI BPK-RI untuk menunjuk sub bagian Dukungan TI sebagai penanggungjawab keseluruhan penanganan proses manajemen insiden.

Berikut ini adalah rincian dari kebijakan mengenai fungsi sub bagian dan penanggungjawab penanganan insiden:

1. Sub bagian Dukungan TI bertanggungjawab atas penanganan setiap insiden. Insiden yang ditangani antara lain insiden yang terkait dengan perangkat keras komputer, sistem operasi dan perangkat lunak seperti aplikasi *office*, insiden yang terkait dengan perangkat jaringan komputer beserta layanan jaringan lokal maupun internet, dan insiden yang terkait dengan aplikasi Sistem Informasi yang dibangun oleh biro TI.
2. Jika terjadi eskalasi insiden maka, tanggungjawab penanganan insiden ada pada sub bagian Pemrograman Aplikasi Komputer untuk insiden terkait aplikasi sistem informasi, dan pada sub bagian Operasional TI untuk insiden terkait jaringan (*network*).
3. Jika hasil dari diagnosa insiden menyebutkan adanya tindakan *maintenance* perangkat TI, maka tanggungjawab selanjutnya diserahkan kepada sub bagian Pemeliharaan Perangkat TI.



4. Untuk insiden yang saling terkait diantara ketiga jenis insiden diatas, akan dibentuk sebuah tim penanganan insiden terpadu.
5. Lebih lanjut kebijakan ini dituangkan dalam tabel 4.1

Tabel 4.1 Fungsi dan tanggungjawab dalam manajemen insiden

<b>Fungsi</b>	<b>Tanggungjawab</b>
Pelapor insiden (U)	<ol style="list-style-type: none"> <li>1. Bertanggungjawab melaporkan setiap insiden yang dialaminya kepada <i>Helpdesk Operator</i> (HO).</li> <li>2. Memberikan informasi yang jelas mengenai insiden tersebut.</li> <li>3. Memberikan informasi jika telah mendapatkan solusi atas insiden.</li> </ol>
<i>Helpdesk Operator</i> (HO) – Dukungan TI Level 1	<ol style="list-style-type: none"> <li>1. Bertanggungjawab menerima informasi insiden dari pelapor insiden (U).</li> <li>2. Bertanggungjawab melakukan pencatatan, kategorisasi, tindakan prioritas, diagnosa awal, dan memberi solusi awal.</li> <li>3. Melakukan eskalasi jika ditemukan proses penanganan tidak akan memenuhi standar waktu penanganan.</li> <li>4. Menerima konfirmasi status penanganan insiden dari <i>helpdesk specialist</i> (HS), <i>Software Manager</i> (SM) dan <i>Network Manager</i> (NM).</li> <li>5. Melakukan konfirmasi kepada pelapor insiden (U) jika insiden telah selesai ditangani.</li> </ol>
<i>Helpdesk Specialist</i> (HS) – Dukungan TI Level 2	<ol style="list-style-type: none"> <li>1. Menerima eskalasi insiden dari <i>Helpdesk Operator</i> (HO).</li> <li>2. Melakukan proses penanganan insiden.</li> <li>3. Melakukan pencatatan status penanganan insiden.</li> <li>4. Melakukan eskalasi insiden kepada <i>Software Manager</i> (SM) atau <i>Network Manager</i> (NM) jika penanganan belum bisa dilakukan.</li> <li>5. Melaporkan status penanganan insiden kepada <i>Helpdesk Operator</i> (HO).</li> </ol>
<i>Incident Manager</i> (IM)	<ol style="list-style-type: none"> <li>1. Mengawasi proses penanganan insiden agar sesuai dengan SLA yang ditetapkan.</li> <li>2. Menerima laporan penanganan insiden dari masing-masing level.</li> <li>3. Membuat laporan kinerja pelaksanaan manajemen insiden.</li> </ol>
<i>Software Manager</i> (SM)	<ol style="list-style-type: none"> <li>1. Menerima eskalasi insiden dari <i>helpdesk specialist</i> (HS) terkait dengan aplikasi sistem informasi.</li> <li>2. Melakukan proses penanganan insiden.</li> <li>3. Melakukan pencatatan status penanganan insiden.</li> </ol>

<b>Fungsi</b>	<b>Tanggungjawab</b>
	4. Melaporkan status penanganan insiden kepada <i>Helpdesk Operator</i> (HO).
<i>Network Manager</i> (NM)	<ol style="list-style-type: none"> <li>1. Menerima eskalasi insiden dari <i>helpdesk specialist</i> (HS) terkait dengan persoalan jaringan komputer.</li> <li>2. Melakukan proses penanganan insiden.</li> <li>3. Melakukan pencatatan status penanganan insiden.</li> <li>4. Melaporkan status penanganan insiden kepada <i>Helpdesk Operator</i> (HO).</li> </ol>
<i>Maintenance Manager</i> (MM)	<ol style="list-style-type: none"> <li>1. Menerima eskalasi insiden dari <i>helpdesk specialist</i> (HS), terkait dengan persoalan perangkat TI.</li> <li>2. Memeriksa status garansi perangkat TI dan menyerahkan tindakan <i>maintenance</i> kepada pihak <i>supplier</i> jika perangkat TI masih dalam masa garansi.</li> <li>3. Melakukan tindakan <i>maintenance</i> perangkat TI.</li> <li>4. Melaporkan status penanganan insiden kepada <i>Helpdesk Operator</i> (HO).</li> </ol>

#### **4.2.2 Kebijakan mengenai hubungan antara jabatan struktural dengan fungsi dalam manajemen insiden**

Kebijakan ini bertujuan untuk menghubungkan jabatan struktural dalam biro TI BPK-RI dengan masing-masing fungsi pelaksana tugas manajemen insiden.

Berikut ini adalah rincian dari kebijakan mengenai hubungan antara jabatan struktural dengan fungsi dalam manajemen insiden:

1. Fungsi *Incident Manager* (IM) dilaksanakan oleh struktural Kasub bagian Dukungan TI
2. Fungsi *Software Manager* (SM) dilaksanakan oleh struktural Kasub bagian Perancangan Aplikasi Komputer
3. Fungsi *Network Manager* (NM) dilaksanakan oleh struktural Kasub bagian Operasional TI
4. Fungsi *Maintenance Manager* (MM) dilaksanakan oleh struktural Kasub bagian Pemeliharaan Perangkat TI
5. Fungsi *Helpdesk Operator* (HO) dilaksanakan oleh perwakilan staf sub bagian Dukungan TI
6. Fungsi *Helpdesk Operator* (HS) dilaksanakan oleh perwakilan staf sub bagian Dukungan TI

### 4.2.3 Kebijakan mengenai kategori insiden

Kebijakan ini digunakan dalam prosedur kategorisasi insiden.

Berikut ini adalah rincian dari kebijakan mengenai kategori insiden:

1. Kategori utama insiden adalah sebagai berikut:
  - a) Pimpinan, untuk insiden yang dialami pimpinan atau pejabat BPK-RI.
  - b) *Hardware*, untuk insiden terkait perangkat keras komputer.
  - c) *Software*, untuk insiden terkait perangkat lunak komputer.
  - d) Aplikasi SI, untuk insiden terkait aplikasi SI yang dibangun biro TI.
  - e) *Network*, untuk insiden terkait perangkat jaringan (*network*).
2. Pemilihan kategori insiden harus dilakukan hingga ke level terbawah.
3. Lebih lanjut kebijakan ini dituangkan dalam tabel 4.2

Tabel 4.2 Kategori insiden

<b>Kategori insiden</b>	<b>Keterangan</b>
Pimpinan/pejabat	Insiden yang terjadi pada pimpinan/pejabat BPK-RI
➤ Pimpinan	Insiden yang termasuk dalam sub kategori pimpinan adalah insiden yang menimpa seluruh perangkat TI yang terkait dengan Ketua, Wakil Ketua dan para Anggota BPK-RI
➤ Pejabat	Insiden yang termasuk dalam sub kategori pejabat adalah insiden yang menimpa seluruh perangkat TI yang terkait dengan para pimpinan satuan kerja setingkat Eselon I dan II.
<i>Hardware</i>	Insiden mencakup perangkat keras komputer seperti PC, laptop, printer, dsb.
➤ PC	Insiden yang termasuk dalam sub kategori PC adalah insiden yang terjadi pada perangkat PC seperti <i>harddisk</i> , <i>memory</i> , <i>graphic card</i> , monitor, <i>mainboard</i> , <i>network card</i> , <i>usb card</i> , <i>mouse</i> , <i>keyboard</i> , dsb.
➤ Laptop	Insiden yang termasuk dalam sub kategori laptop adalah insiden yang terjadi pada perangkat laptop seperti <i>harddisk</i> , <i>memory</i> , <i>monitor</i> , <i>mainboard</i> , <i>network card</i> , <i>usb card</i> , dsb.
➤ Office tools	Insiden yang termasuk dalam sub kategori <i>office tools</i> adalah insiden yang terjadi pada perangkat non PC/laptop seperti printer, <i>scanner</i> , <i>mobile harddisk</i> , <i>digital camera</i> , <i>in-focus</i> , <i>card reader</i> , dsb.
<i>Software</i>	Insiden mencakup perangkat lunak komputer seperti sistem operasi, aplikasi <i>office</i> , antivirus, dsb.

<b>Kategori insiden</b>	<b>Keterangan</b>
➤ Office	Insiden yang termasuk dalam sub kategori <i>office</i> adalah insiden yang terjadi pada aplikasi <i>office</i> dalam hal ini Microsoft Office dan OpenOffice.org untuk semua versinya, dan aplikasi audit seperti ACL.
➤ Non Office	Insiden yang termasuk dalam sub kategori non <i>office</i> adalah insiden yang terjadi pada aplikasi non <i>office</i> seperti <i>PDF Reader, internet browser</i> , aplikasi zip, OS Windows untuk semua versi, <i>AntiVirus, Firewall, multimedia player</i> , dsb.
SI	Insiden mencakup aplikasi sistem informasi yang dikembangkan biro TI.
➤ Database	Insiden yang termasuk dalam sub kategori database adalah insiden yang menimpa database aplikasi yang digunakan baik itu kejadian fisik ataupun non fisik.
➤ Aplikasi Audit	Insiden yang termasuk dalam sub kategori aplikasi audit adalah insiden yang menimpa aplikasi seperti aplikasi SMP dan SI Database Entitas.
➤ Aplikasi Umum	Insiden yang termasuk dalam sub kategori aplikasi umum adalah insiden yang menimpa aplikasi seperti aplikasi SAK, SABMN, persuratan, SIMA, <i>helpdesk</i> , SI-SDM, SIMBAKUM, SI-Gaji, e-library, RKPP, dan SI-Diklat.
<i>Network</i>	Insiden mencakup perangkat keras dan lunak yang berkaitan dengan jaringan ( <i>network</i> ) misalnya <i>router</i> , kabel jaringan, <i>wifi</i> , dsb.
➤ <i>Network OS</i>	Insiden yang termasuk dalam sub kategori <i>network OS</i> adalah insiden yang menimpa software, driver, dan sistem operasi perangkat <i>network</i> yang digunakan seperti <i>Router OS, firewall</i> , dsb.
➤ <i>Network Hardware</i>	Insiden yang termasuk dalam sub kategori <i>network hardware</i> adalah insiden yang menimpa perangkat keras <i>network</i> seperti SAN, mesin server, dsb.

#### 4.2.4 Kebijakan mengenai prioritas insiden

Kebijakan ini digunakan dalam prosedur prioritas insiden.

Berikut ini adalah rincian dari kebijakan mengenai prioritas insiden:

1. Prioritas penanganan insiden harus dilakukan oleh *Helpdesk Operator* pada saat menerima laporan insiden.
2. Prioritas dibuat dengan memperhatikan tabel implikasi insiden, dan tabel kepentingan insiden.

3. Prioritas penanganan insiden dapat diubah pada saat eskalasi dengan memperhatikan SLA target penanganan insiden.
4. Lebih lanjut kebijakan ini dituangkan dalam tabel 4.3, 4.4, dan 4.5

Tabel 4.3 Implikasi insiden

<b>Implikasi insiden</b>	<b>Keterangan</b>
Sangat luas	Mencakup seluruh bagian kerja BPK-RI.
Luas	Implikasinya terhadap lebih dari 200 orang.
Sedang	Implikasinya terhadap 21-199 orang.
Kecil	Implikasinya terhadap kurang dari 20 orang.

Tabel 4.4 Kepentingan insiden

<b>Kepentingan insiden</b>	<b>Keterangan</b>
Pimpinan	Insiden yang dialami pimpinan dan/atau pejabat (dalam hal ini pejabat eselon II dan I).
Kritis	Insiden berakibat langsung pada beberapa proses bisnis utama atau beberapa bagian struktur organisasi dalam BPK-RI. Misalnya virus menghilangkan data-data penting.
Tinggi	Insiden yang mengakibatkan sebuah proses bisnis berhenti. Misalnya virus menyerang sistem informasi yang digunakan.
Sedang	Insiden mengakibatkan sistem terganggu tetapi proses bisnis tidak berhenti. Misalnya jaringan down.
Rendah	Insiden mengakibatkan kenyamanan user terganggu. Misalnya aplikasi „hang“.

Tabel 4.5 Prioritas penanganan insiden

<b>Prioritas Insiden</b>		<b>Implikasi</b>			
		<b>Sangat Luas</b>	<b>Luas</b>	<b>Sedang</b>	<b>Kecil</b>
<b>Kepentingan</b>	<b>Pimpinan</b>	Utama	Utama	Utama	Utama
	<b>Kritis</b>	Utama	Utama	Tinggi	Tinggi
	<b>Tinggi</b>	Utama	Tinggi	Tinggi	Sedang
	<b>Sedang</b>	Tinggi	Sedang	Sedang	Sedang
	<b>Rendah</b>	Sedang	Rendah	Rendah	Rendah

#### 4.2.5 Kebijakan mengenai penanganan insiden

Kebijakan ini mengatur bagaimana proses penanganan insiden dilakukan. Selain itu kebijakan ini juga dipakai sebagai acuan waktu penanganan insiden.

Berikut ini adalah rincian dari kebijakan mengenai penanganan insiden:

1. Waktu penanganan insiden harus dibuat seminimal mungkin untuk memenuhi kepuasan pimpinan dan pegawai.
2. Penanganan insiden wajib dilaksanakan menggunakan standar dan *best practice* TI.
3. Sumber informasi yang utama mengenai insiden adalah *service desk*. Selain itu, sumber informasi insiden diketahui juga melalui inspeksi berkala oleh staf teknis kepada sumber daya TI yang sangat penting bagi proses bisnis.
4. Lebih lanjut kebijakan ini dituangkan dalam tabel 4.6

Tabel 4.6 SLA target waktu penanganan insiden

Prioritas	Keterangan	SLA	
		Respon	Resolusi
Utama	Insiden dialami oleh pimpinan dan pejabat atau berimplikasi pada beberapa proses bisnis berhenti.	<ol style="list-style-type: none"> <li>1. Respon harus diambil dalam waktu 1 jam sejak laporan insiden masuk.</li> <li>2. Untuk kepentingan pimpinan dan pejabat, respon harus diambil pada laporan insiden masuk.</li> </ol>	<ol style="list-style-type: none"> <li>1. Resolusi atas insiden harus ada dalam waktu &lt; 3 jam.</li> <li>2. Untuk kepentingan pimpinan dan pejabat, resolusi atas insiden harus ada dalam waktu &lt; 1 jam.</li> </ol>
Tinggi	Insiden mengakibatkan salah satu proses bisnis berhenti.	Respon harus diambil dalam waktu 2 jam sejak laporan insiden masuk.	Resolusi atas insiden harus ada dalam waktu < 1 hari kerja.
Sedang	Insiden mengakibatkan sistem terganggu tetapi proses bisnis masih dapat berjalan.	Respon harus diambil dalam waktu 24 jam sejak laporan insiden masuk.	Resolusi atas insiden harus ada dalam waktu < 3 hari kerja.
Rendah	Insiden mengakibatkan kenyamanan user terganggu	Respon harus diambil dalam waktu 48 jam sejak laporan insiden masuk.	Respon atas insiden sesuai rencana.

#### 4.2.6 Kebijakan mengenai eskalasi insiden

Kebijakan ini digunakan dalam prosedur eskalasi insiden.

Berikut ini adalah rincian dari kebijakan mengenai eskalasi insiden:

1. Eskalasi insiden wajib dilakukan jika penanganan insiden belum memenuhi SLA yang ditetapkan.

#### **4.2.7 Kebijakan mengenai evaluasi berkala atas manajemen insiden**

Kebijakan ini digunakan dalam prosedur evaluasi penanganan insiden.

Berikut ini adalah rincian dari kebijakan mengenai evaluasi berkala atas manajemen insiden:

1. Evaluasi atas manajemen insiden dibuat oleh masing-masing penanggungjawab, secara berkala setiap bulan sekali, untuk semua insiden yang selesai ditutup.
2. Hasil evaluasi dilaporkan oleh masing-masing penanggungjawab kepada Kepala Biro TI melalui Kepala Sub Bagian Dukungan TI.

#### **4.2.8 Kebijakan mengenai pengukuran kinerja penanganan insiden**

Kebijakan ini digunakan dalam prosedur evaluasi insiden.

Berikut ini adalah rincian dari kebijakan mengenai pengukuran kinerja penanganan insiden:

1. Rincian pengukuran kinerja penanganan insiden dibuat berdasarkan target SLA waktu penanganan insiden dan disepakati bersama oleh seluruh pejabat di lingkungan Biro TI.
2. Rincian pengukuran kinerja dapat diubah menurut kondisi yang ada.
3. Lebih lanjut kebijakan ini dituangkan dalam tabel 4.7

Tabel 4.7 Pengukuran kinerja penanganan insiden

<b>Kategori</b>	<b>Keterangan</b>	<b>Pengukuran</b>	<b>Target</b>
Repon	Waktu yang dibutuhkan dalam menerima masukan insiden maupun eskalasi yang dilakukan.	Pengukuran yang ditetapkan: Utama: 1 jam (khusus pimpinan dan pejabat harus lebih cepat) Tinggi: 2 jam Sedang: 24 jam Rendah: 48 jam	SLA terpenuhi sebanyak 95% dari insiden yang masuk.
Resolusi	Waktu yang dibutuhkan hingga	Pengukuran yang ditetapkan: Utama: 3 jam	SLA terpenuhi sebanyak 95% dari

<b>Kategori</b>	<b>Keterangan</b>	<b>Pengukuran</b>	<b>Target</b>
	insiden selesai ditangani.	(khusus pimpinan dan pejabat harus < 1 jam) Tinggi: < 1 hari kerja Sedang: < 3 hari kerja Rendah: sesuai rencana	insiden yang masuk.
Keberadaan manajemen insiden	Tingkat keberadaan manajemen insiden selalu ada saat dibutuhkan.	Waktu dimana layanan manajemen insiden saat sedang down.	99% dari seluruh periode layanan manajemen insiden.

### **4.3 Panduan Penanganan Insiden**

Dalam melaksanakan program manajemen help desk dan dukungan TI, selain kebijakan diatas, Biro TI juga mengembangkan sebuah panduan layanan dukungan TI untuk pelaksanaan program. Panduan dukungan TI [BPI07] ditetapkan oleh Biro TI dengan kerangka kerja sebagai berikut.

#### **4.3.1 Tujuan**

Tujuan dari layanan dukungan TI pada program manajemen *helpdesk* dan dukungan TI adalah sebagai berikut:

1. Memberikan dukungan TI yang dibutuhkan oleh pegawai dan pimpinan BPK-RI.
2. Mengembalikan proses kepada kondisi normal dengan cepat dan tepat segera setelah terjadi insiden.
3. Memastikan layanan TI selalu berjalan sesuai dengan SLA yang telah ditetapkan.

#### **4.3.2 Fokus**

Fokus dari layanan dukungan TI pada program manajemen *helpdesk* dan dukungan TI adalah sebagai berikut:

1. Memastikan dukungan TI dan penanganan insiden berjalan sesuai pedoman yang ditetapkan.
2. Memastikan *helpdesk* bekerja sesuai dengan pedoman yang ditetapkan.



### **4.3.3 Cakupan**

Cakupan pelaksanaan layanan dukungan TI pada program manajemen *helpdesk* dan dukungan TI adalah sebagai berikut:

1. Insiden yang terkait dengan perangkat keras komputer, sistem operasi dan perangkat lunak.
2. Insiden yang terkait dengan perangkat jaringan komputer beserta layanan jaringan lokal maupun internet.
3. Insiden yang terkait dengan aplikasi Sistem Informasi yang dibangun oleh biro TI.

### **4.3.4 Kriteria Keberhasilan**

Kriteria keberhasilan pelaksanaan layanan dukungan TI pada program manajemen *helpdesk* dan dukungan TI adalah sebagai berikut:

1. Semua insiden dapat diidentifikasi dan ditangani dalam SLA yang sudah ditetapkan.
2. Tidak ada komplain dari pimpinan dan pegawai mengenai penanganan insiden.

### **4.3.5 Indikator Keberhasilan**

Indikator keberhasilan pelaksanaan layanan dukungan TI pada program manajemen *helpdesk* dan dukungan TI adalah sebagai berikut:

1. Prosentase insiden berhasil ditangani menurut standar waktu yang ditetapkan.
2. Prosentase insiden yang berhasil diselesaikan langsung oleh *helpdesk*.

### **4.3.6 Masukan**

Masukan bagi pelaksanaan layanan dukungan TI pada program manajemen *helpdesk* dan dukungan TI adalah sebagai berikut:

1. Laporan kepada *helpdesk*.
2. Inspeksi oleh staf teknis.

#### 4.3.7 Keluaran

Keluaran dari pelaksanaan layanan dukungan TI pada program manajemen *helpdesk* dan dukungan TI adalah sebagai berikut:

1. Usulan perubahan SLA kepada proses manajemen SLA (*service level management*).
2. Usulan perubahan konfigurasi sistem kepada proses manajemen konfigurasi (*configuration management*).
3. Usulan perubahan kapasitas sistem kepada proses manajemen kapasitas (*Capacity Management*).
4. Laporan ketersediaan layanan kepada proses manajemen ketersediaan (*Availability Management*).
5. Eskalasi insiden kepada proses manajemen masalah (*Problem Management*).

#### 4.3.8 Aktifitas

Tabel 4.8 berisi rincian aktifitas dan produk yang dihasilkan dalam program manajemen help desk dan dukungan TI.

Tabel 4.8 Aktifitas dalam program manajemen help desk dan dukungan TI

Aktifitas	Produk Pokok
1. Menyelenggarakan pusat layanan dan bantuan teknis untuk seluruh pengguna TI	Layanan dan bantuan teknis TI
2. Mengkoordinasikan pelaksanaan layanan dan bantuan teknis operasional TI dengan solver <i>helpdesk</i> BPK-RI	Pelaksanaan layanan dan bantuan teknis
3. Mengevaluasi permasalahan operasional sistem, aplikasi, jaringan serta sistem komunikasi yang diterima	Laporan evaluasi operasional sistem , aplikasi, jaringan serta sistem komunikasi
4. Menyampaikan informasi layanan TI kepada pihak yang memerlukan atas permasalahan yang telah disampaikan kepada <i>helpdesk</i> BPK-RI	Informasi layanan TI
5. Menyusun, mengkompilasi dan mengelola database penanggulangan/solusi permasalahan operasional TI	Database penanggulangan masalah
6. Memberikan dan mengadministrasikan hak akses dan kewenangan terkait dengan domain (intra/xnet) , internet, email dan desktop (administrator)	Pelaksanaan Administrator Sistem TI yang terkait dengan domain, email dan desktop

Aktifitas	Produk Pokok
7. Mengelola arsip dan dokumen kelompok	Pengelolaan arsip dan dokumen.

#### 4.4 Aktifitas Dalam Program Manajemen Help Desk dan Dukungan TI

Aktifitas-aktifitas yang disebutkan dalam tabel 4.8 kemudian dirinci dalam dokumen program manajemen *helpdesk* dan dukungan TI [BDI07]. Rincian aktifitas-aktifitas tersebut adalah sebagai berikut:

##### 4.4.1 Menyelenggarakan pusat layanan dan bantuan teknis untuk seluruh pengguna TI.

Aktifitas ini adalah aktifitas yang paling utama yang dilaksanakan oleh sub bagian Dukungan TI. Dalam pelaksanaannya aktifitas ini sangat terkait dengan *framework* ITIL untuk proses TI manajemen insiden, karena dukungan TI yang diberikan oleh sub bagian Dukungan TI selalu terkait dengan penanganan insiden yang terjadi diantara para pengguna TI.

Berikut adalah langkah-langkah kerja yang dilakukan dalam mengimplementasikan aktifitas ini.

1. Menerima pengaduan permasalahan TI sesuai dengan jam kerja dan daftar aplikasi yang ditangani *helpdesk* BPK-RI
2. Melakukan administrasi pengaduan permasalahan dalam Sistem Informasi Pelayanan TI (SIMPLI) BPK-RI.
3. Melakukan assignment pengaduan ke solver sesuai dengan kategori permasalahan.
4. Problem Solving (solver) untuk permasalahan TI yang ada di Kelompok *Helpdesk*.
5. Eskalasi permasalahan
6. Monitoring problem solving yang berada diluar kelompok *Helpdesk*
7. Melakukan administrasi penyelesaian penanganan permasalahan dalam SIMPLI BPK-RI
8. Memberikan dan menyampaikan solusi permasalahan ke user

#### **4.4.2 Mengkoordinasikan pelaksanaan layanan dan bantuan teknis operasional TI dengan solver unit kerja terkait.**

Aktifitas ini berfokus pada koordinasi pelayanan dukungan TI di sub bagian Dukungan TI.

Berikut adalah langkah-langkah kerja yang dilakukan dalam mengimplementasikan aktifitas ini.

1. Menjalankan mekanisme penerimaan pengaduan permasalahan TI
2. Menjalankan mekanisme penanganan pengaduan permasalahan TI
3. Melakukan evaluasi koordinasi tim/satker terkait
4. Melakukan koordinasi tim/satker terkait

#### **4.4.3 Mengevaluasi permasalahan operasional sistem, aplikasi, jaringan serta sistem komunikasi yang diterima.**

Aktifitas laporan dan evaluasi diperlukan untuk kebutuhan manajemen Biro TI menilai pelaksanaan program manajemen *helpdesk* dan dukungan TI yang dilaksanakan sub bagian Dukungan TI. Aktifitas ini dilakukan dalam 2 tahap yaitu pembuatan laporan dan evaluasi melalui kuisisioner. Terkait dengan pembuatan tata laksana manajemen insiden, aktifitas ini akan menjadi pelengkap bagi prosedur proses TI manajemen insiden yang akan dibuat.

Berikut ini rincian langkah-langkah yang dilakukan dalam aktifitas ini.

##### **A. Pembuatan Laporan Evaluasi Bulanan *helpdesk* BPK-RI**

1. Melakukan rekapitulasi database permasalahan antara lain: perkembangan permasalahan, status, klasifikasi masalah, SLA, eskalasi permasalahan
2. Membuat Laporan Evaluasi Bulanan *helpdesk* terhadap rekapitulasi database permasalahan
3. Verifikasi Laporan Evaluasi Bulanan *helpdesk*
4. Persetujuan atas Laporan Evaluasi Bulanan *helpdesk*
5. Melakukan penyebaran Laporan Evaluasi Bulanan *helpdesk* ke satker terkait dan website *Helpdesk*

##### **B. Menyusun dan menyebarkan kuisisioner terhadap tingkat kepuasan layanan *helpdesk* BPK-RI**

1. Melakukan pembuatan konsep dan materi kuisisioner
2. Persetujuan atas materi kuisisioner
3. Distribusi kuisisioner
4. Rekapitulasi
5. Follow up terhadap hasil kuisisioner

#### **4.4.4 Menyampaikan informasi layanan TI kepada pihak yang memerlukan atas permasalahan yang telah disampaikan kepada *helpdesk* BPK-RI.**

Aktifitas ini bertujuan untuk memberikan informasi kepada seluruh pengguna TI di BPK-RI mengenai sub bagian Dukungan TI yang menjadi penanggungjawab seluruh kegiatan dukungan TI. Selain itu dalam aktifitas ini juga dilakukan pengumpulan kritik dan saran dari pengguna TI di BPK-RI mengenai layanan dukungan TI yang dilaksanakan.

Berikut adalah langkah-langkah yang dilakukan untuk melaksanakan aktifitas ini.

##### A. Melakukan Sosialisasi *Helpdesk*

1. Merencanakan konsep materi sosialisasi
2. Merencanakan rincian acara kegiatan
3. Pembuatan catatan persetujuan sosialisasi
4. Koordinasi pelaksanaan kegiatan
5. Pembuatan pertanggung-jawaban acara

##### B. Penyebaran Tips & Trik *Helpdesk*

1. Penyusunan Tips & Trik *Helpdesk*
2. Persetujuan atas materi Tips & Trik
3. Proses pengadaan Tips & Trik
4. Proses distribusi Tips & Trik

##### C. Mengelola komunikasi dengan LO TI

1. Pengelolaan forum komunikasi

##### D. Pengelolaan Berita Terkini di Website *Helpdesk*

1. Menerima informasi satker/solver mengenai kejadian pada layanan TI
2. Melakukan verifikasi atas kejadian pada layanan teknologi dan informasi yang diinformasikan

3. Melakukan penyusunan redaksional
  4. Melakukan persetujuan atas usulan informasi layanan / kejadian TI
  5. Melakukan upload berita terkini di website *helpdesk*
- E. Pengelolaan Kritik dan Saran di Website *Helpdesk*
1. Menerima kritik dan saran dari user melalui web site *Helpdesk*
  2. Melakukan verifikasi atas kritik dan saran yang diadukan
  3. Melakukan penyusunan redaksional
  4. Melakukan persetujuan jawaban kritik dan saran
  5. Menjawab kritik dan saran sesuai dengan persetujuan di website *helpdesk*

#### **4.4.5 Menyusun, mengkompilasi dan mengelola database penanggulangan / solusi permasalahan operasional TI.**

Aktifitas ini dilakukan untuk mengumpulkan setiap solusi yang ditemukan dalam tindakan penanganan insiden. Solusi-solusi tersebut dikumpulkan dalam sebuah database dengan tujuan agar dapat digunakan sebagai referensi dalam tindakan penanganan insiden selanjutnya.

Berikut adalah langkah-langkah yang dilakukan dalam melaksanakan aktifitas ini.

- A. Pengelolaan database Solusi
1. Menerima masukan dari solver/tim terkait mengenai database solusi
  2. Melakukan rekapitulasi solusi dari database permasalahan dan masukan dari solver/tim terkait
  3. Melakukan (redaksional) usulan baru/update/hapus database solusi
  4. Melakukan persetujuan atas usulan database solusi
  5. Melakukan upload database solusi ke SIMPLI
- B. Pengelolaan FAQ
1. Menerima masukan dari solver/tim terkait mengenai FAQ
  2. Melakukan rekapitulasi solusi dari FAQ dan masukan dari solver/tim terkait
  3. Melakukan (redaksional) usulan baru/update/hapus FAQ
  4. Melakukan persetujuan atas usulan FAQ

5. Melakukan upload FAQ ke Website *Helpdesk*

C. Pengelolaan Tips & Trik

1. Menerima masukan dari solver/tim terkait mengenai Tips & Trik
2. Melakukan rekapitulasi solusi dari Tips & Trik dan masukan dari solver/tim terkait
3. Melakukan (redaksional) usulan baru/update/hapus Tips & Trik
4. Melakukan persetujuan atas usulan Tips & Trik
5. Melakukan upload Tips & Trik Website *Helpdesk*

D. Pengelolaan Dokumentasi *Helpdesk*

1. Menerima masukan dari solver/tim terkait mengenai Dokumentasi *Helpdesk*
2. Melakukan rekapitulasi solusi dari Dokumentasi *Helpdesk* dan masukan dari solver/tim terkait
3. Melakukan (redaksional) usulan baru/update/hapus Dokumentasi *Helpdesk*
4. Melakukan persetujuan atas usulan Dokumentasi *Helpdesk*
5. Melakukan upload Dokumentasi *Helpdesk* Website *Helpdesk*

**4.4.6 Memberikan dan mengadministrasikan hak akses dan kewenangan terkait dengan domain, email dan desktop (administrator).**

Aktifitas ini merupakan pelimpahan wewenang dari sub bagian Operasional TI kepada sub bagian Dukungan TI. Hal ini dikarenakan banyaknya laporan dari pengguna sumber daya *network* kepada sub bagian Operasional TI sementara sumber daya manusia yang dimiliki tidak sebanding jumlahnya.

Berikut adalah langkah-langkah yang dilakukan dalam melaksanakan aktifitas ini.

A. Pendaftaran Hak Akses Jaringan

1. Penerimaan nota dinas / faksimili permintaan hak akses user jaringan
2. Persetujuan pemberian hak akses user jaringan
3. Pengecekan user-id pegawai di dalam Active Directory untuk menghindari duplikasi
4. Pemberian user-id dan pemberian password serta akses jaringan

5. Pemberian nota dinas balasan

B. Pendaftaran Hak Akses Internet

1. Penerimaan nota dinas / faksimili permintaan hak akses Internet
2. Persetujuan pemberian hak akses Internet
3. Pengecekan user-id pegawai di dalam Active Directory untuk menghindari duplikasi
4. Apabila user-id telah terdaftar, lakukan pengecekan hak akses Internet untuk user-id tersebut
5. Apabila user-id belum terdaftar, daftarkan user-id dan password serta hak akses Internet
6. Apabila user-id telah terdaftar, tetapi belum memiliki hak akses internet, tambahkan hak akses Internet untuk userid tersebut
7. Pemberian nota dinas balasan

C. Pendaftaran Hak Akses E-mail

1. Penerimaan nota dinas /Faksimili permintaan hak akses E-mail
2. Persetujuan pemberian hak akses E-mail
3. Pengecekan user-id pegawai di dalam Active Directory untuk menghindari duplikasi berdasarkan melihat NIP pegawai tersebut
4. Apabila user-id telah terdaftar, lakukan pengecekan alamat e-mail untuk user-id tersebut
5. Apabila user-id belum terdaftar, daftarkan user-id dan password serta alamat e-mail untuk user-id tersebut
6. Apabila user-id telah terdaftar, tetapi belum memiliki alamat e-mail internet, tambahkan alamat e-mail sesuai dengan lokasi mailbox untuk user-id tersebut
7. Tambahkan user-id tersebut ke dalam groupnya masing-masing
8. Pemberian nota dinas balasan

D. Mailing List

1. Penerimaan nota dinas / Faksimili permintaan Mailing List
2. Persetujuan pemberian Distribution List
3. Pengecekan Distribution List di dalam Active Directory untuk menghindari duplikasi Distribution List



4. Apabila Distribution List belum terdaftar, lakukan pengecekan nama owner atau penanggung-jawab Distribution List pada nota dinas / Faksimili
5. Apabila terdapat nama owner atau penanggung-jawab Distribution List, lakukan pendaftaran Distribution List dimaksud
6. Pemberian nota dinas balasan

#### **4.4.7 Mengelola arsip dan dokumen kelompok.**

Aktifitas ini mencakup pengelolaan seluruh dokumen dalam biro TI. Dokumen-dokumen yang dihasilkan dari tiap-tiap bagian dan sub bagian dalam biro TI disimpan oleh sub bagian Dukungan TI. Jika ada dokumen yang dibutuhkan, maka sub bagian Dukungan TI wajib menyediakan dokumen yang diminta.

Berikut adalah langkah-langkah yang dilakukan dalam melaksanakan aktifitas ini.

##### **A. Mengelola Dokumen Kelompok**

1. Menghimpun dan Mengelompokkan dokumen sesuai dengan proyek masing-masing
2. Menyusun dokumen berdasarkan waktu atau tanggal pelaksanaan
3. Mengklasifikasi dokumen menjadi dokumen aktif/pasif

##### **B. Mengelola Arsip Kelompok**

1. Menghimpun dokumen yang telah selesai ditindaklanjuti menjadi suatu berkas arsip
2. Mengelompokkan arsip sesuai dengan proyek masing-masing
3. Menyetujui penyimpanan berkas arsip dan pengiriman arsip > 6 tahun ke Sub Bagian Arsip

#### **4.5 Penyempurnaan Program Manajemen *Helpdesk* dan Dukungan TI dengan Fokus pada Proses TI Manajemen Insiden**

Program manajemen help desk dan dukungan TI dilaksanakan sepenuhnya oleh sub bagian Dukungan TI. Program ini melakukan 2 kegiatan TI utama yaitu manajemen *helpdesk* dan dukungan TI. *Helpdesk* adalah layanan TI yang diberikan sub bagian

Dukungan TI BPK-RI untuk menerima pengaduan dan laporan dari para pengguna TI. Sedangkan dukungan TI adalah layanan TI yang diberikan sub bagian Dukungan TI BPK-RI berupa proses TI manajemen insiden dan layanan TI lainnya yang diminta oleh pengguna.

Dalam pelaksanaan program ini, diketahui sub bagian Dukungan TI melakukan 7 (tujuh) aktifitas yang telah disebutkan pada tabel 4.8. Akan tetapi tidak semua aktifitas tersebut seturut dengan tujuan utama program yaitu pengembangan manajemen *helpdesk* dan dukungan TI. Beberapa aktifitas memiliki tugas yang sama sekali berbeda dengan tujuan utama program. Aktifitas-aktifitas tersebut antara lain adalah:

1. Memberikan dan mengadministrasikan hak akses dan kewenangan terkait dengan domain (intra/extra) internet, email, dan desktop (administrator).
2. Mengelola arsip dan dokumen kelompok.

Aktifitas yang pertama diketahui lebih banyak berfokus pada tugas layanan operasional atau manajemen *network*. Aktifitas ini merupakan pelimpahan tugas dari sub bagian operasional TI. Hal ini didasarkan pada pertimbangan dari biro TI BPK-RI agar sub bagian operasional TI dapat lebih berfokus pada permasalahan manajemen *network* yang lebih besar dibandingkan mengerjakan tugas-tugas administrasi hak akses. Sementara aktifitas yang kedua diketahui lebih banyak berfokus pada tugas pengelolaan arsip dan dokumen dari seluruh bagian/sub bagian biro TI.

Aktifitas yang berbeda tujuannya dengan tujuan utama program mengakibatkan pelaksanaan program tidak maksimal. Untuk menghindari hal tersebut, yang harus dilakukan adalah membuat lebih dari 1 (satu) dokumen tata laksana untuk program tersebut dimana masing-masing dokumen tata laksana mendukung tujuan utama program. Terkait dengan program manajemen *helpdesk* dan dukungan TI yang menjadi wewenang sub bagian Dukungan TI, dokumen tata laksana yang dapat dibuat adalah dokumen tata laksana mengenai manajemen *helpdesk*, dan dokumen tata laksana mengenai dukungan TI dalam hal ini proses TI manajemen insiden, manajemen masalah, dan perangkat *event management*. Pelaksanaan program dalam hal ini layanan dukungan TI, juga diketahui tidak maksimal. Hal ini dikarenakan dalam penyusunan prosedur, dokumen program belum menyesuaikan dengan standar tata kelola TI yang ada seperti best practice dari *framework* ITIL.

Dari aktifitas-aktifitas dalam prosedur program manajemen *helpdesk* dan dukungan TI, yang akan tetap digunakan dalam penyempurnaan ini ada 5 (lima) aktifitas yaitu:

1. Menyelenggarakan pusat layanan dan bantuan teknis untuk seluruh pengguna TI.
2. Mengkoordinasikan pelaksanaan layanan dan bantuan teknis operasional TI dengan solver *helpdesk* TI BPK-RI.
3. Mengevaluasi permasalahan operasional sistem, aplikasi, jaringan serta sistem komunikasi yang diterima.
4. Menyampaikan informasi layanan TI kepada pihak yang memerlukan atas permasalahan yang telah disampaikan kepada *helpdesk* TI BPK-RI.
5. Menyusun, mengkompilasi dan mengelola database penanggulangan/solusi permasalahan operasional TI.

Kelima aktifitas ini diketahui memiliki keterkaitan dengan proses TI manajemen insiden. Oleh karena itu, langkah-langkah dalam kelima aktifitas ini akan dirangkum untuk kemudian dilakukan penggabungan kepada dokumen program yang akan disempurnakan.

Bagian berikut ini adalah penyempurnaan prosedur program manajemen help desk dan dukungan TI, secara khusus berfokus pada proses TI manajemen insiden. Penyempurnaan dilakukan dengan membagi proses manajemen insiden ke dalam 11 (sebelas) aktifitas yaitu 9 (sembilan) aktifitas yang berdasarkan *framework* ITIL, serta 2 (dua) aktifitas tambahan untuk memenuhi kebutuhan pelaporan dan evaluasi. Selanjutnya rincian proses penyempurnaan dokumen program dapat dilihat pada Lampiran 1 mengenai brainstorming pembuatan dokumen tata laksana.

#### **4.5.1 Identifikasi insiden (*incident identification*)**

Aktifitas identifikasi insiden (*incident identification*) bertujuan untuk memastikan setiap insiden dapat diidentifikasi sebelum menimbulkan implikasi negatif pada proses bisnis yang sedang berlangsung. Selain itu aktifitas ini juga bertujuan untuk memastikan kartu insiden dengan status “Belum selesai” dibuka dan didistribusikan.

Indikator kinerja untuk tujuan pertama adalah % insiden yang menimbulkan implikasi negatif sebelum bisa dilaporkan. Sedangkan indikator kinerja untuk tujuan kedua adalah jumlah kartu insiden yang dibuka kembali setiap harinya.

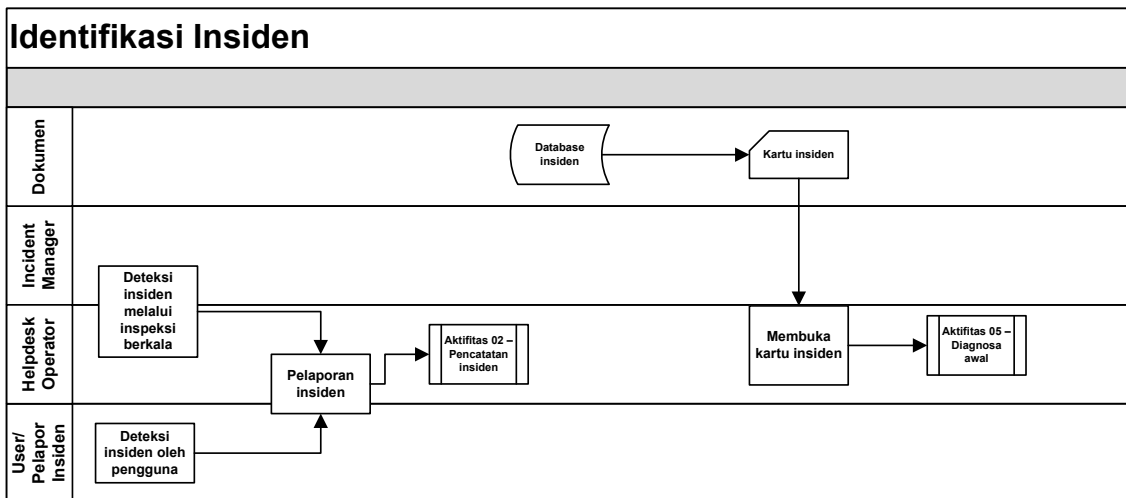
Langkah pertama aktifitas identifikasi insiden (*incident identification*) adalah deteksi insiden. Deteksi insiden dibagi menjadi 2 (dua) kegiatan yaitu deteksi insiden melalui inspeksi berkala dan deteksi insiden oleh pegawai/pimpinan pengguna TI.

Pelapor Insiden/*User* (U) dalam hal ini adalah para pegawai dan pimpinan di lingkungan BPK-RI mendeteksi insiden yang terjadi melalui kejadian yang dialaminya pada perangkat komputer yang digunakannya. Selain itu deteksi insiden juga dilakukan melalui inspeksi berkala oleh staf teknis kepada perangkat TI yang penting. Hasil inspeksi oleh staf teknis adalah laporan inspeksi staf teknis yang berisi kondisi perangkat saat ini dan potensi terjadinya insiden.

Selanjutnya setelah insiden terdeteksi, Pelapor Insiden/*User* (U) wajib melaporkan insiden yang ditemuinya kepada *Helpdesk Operator* (HO). Ada 3 (tiga) cara untuk melaporkan insiden, yaitu melalui telepon, email dan pelaporan langsung ke meja *Helpdesk Operator* (HO). Laporan oleh Pelapor Insiden/*User* (U) akan diterima oleh *Helpdesk Operator* (HO) yang kemudian akan melakukan aktifitas Pencatatan Insiden (*incident logging*).

Selain laporan deteksi insiden oleh Pelapor Insiden/*User* (U), deteksi insiden juga dilakukan melalui tindakan membuka kartu insiden yang belum selesai ditangani. Kartu insiden tersebut diambil dari database insiden setiap pagi hari oleh *Helpdesk Operator* (HO).

Diagram alir aktifitas identifikasi insiden dapat dilihat pada Gambar 4.1.



Gambar 4.2 Diagram alir prosedur identifikasi insiden

#### 4.5.2 Pencatatan insiden (*incident logging*)

Aktifitas pencatatan insiden (*incident logging*) bertujuan untuk memastikan dilakukannya pencatatan informasi dari laporan insiden yang masuk sebagai dasar pelaksanaan proses penanganan insiden. Selain itu aktifitas ini juga bertujuan untuk memastikan informasi dicatat secara lengkap dan diverifikasi. Dan tujuan terakhir adalah untuk memastikan dibuatnya ringkasan insiden dan kata kunci pencarian kartu insiden.

Indikator kinerja untuk tujuan pertama adalah jumlah waktu yang dibutuhkan dalam mencatat informasi insiden, jumlah komplain dari Pelapor Insiden/*User* (U) dikarenakan *Helpdesk Operator* (HO) tidak berada ditempat pada saat pelaporan, jumlah laporan yang masuk melalui telepon, jumlah laporan yang masuk melalui email, dan jumlah laporan yang masuk melalui meja *helpdesk*. Indikator kinerja untuk tujuan kedua adalah % kartu insiden tercatat lengkap, dan % kartu insiden yang sumbernya terverifikasi. Sedangkan indikator kinerja untuk tujuan ketiga adalah jumlah kartu insiden yang memiliki kata kunci yang tepat.

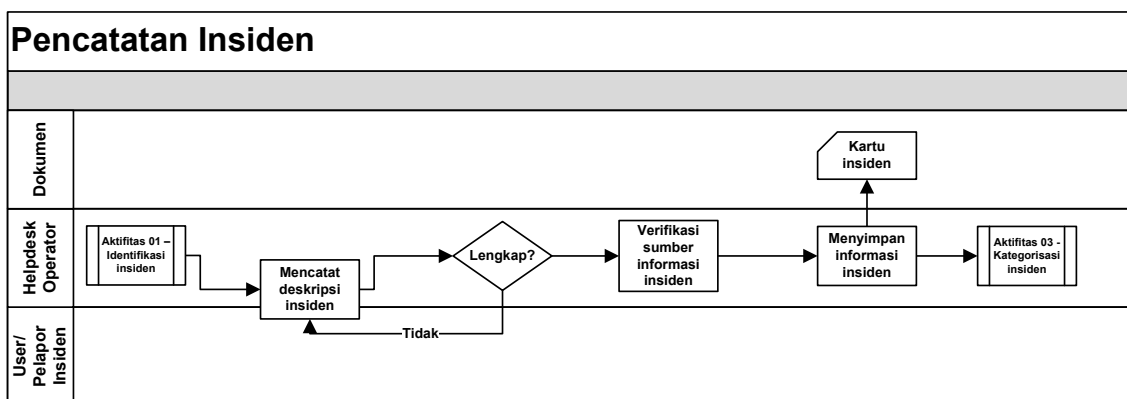
Langkah pertama aktifitas pencatatan insiden (*incident logging*) adalah pencatatan informasi insiden. *Helpdesk Operator* (HO) yang menerima laporan insiden dari Pelapor Insiden/*User* (U) kemudian mencatat informasi yang disampaikan. Informasi yang dicatat adalah waktu insiden terjadi, deskripsi insiden secara lengkap, sumber informasi insiden, dan waktu pelaporan insiden.

*Helpdesk Operator* (HO) juga mencatat media penghubung dengan Pelapor Insiden/*User* (U) untuk keperluan notifikasi kembali, berupa nomor telepon, email atau posisi Pelapor Insiden/*User* (U) di kantor. Laporan insiden dicatat dalam kartu insiden dan dilengkapi dengan waktu laporan dibuat, dan kemudian diverifikasi kelengkapannya.

Verifikasi sumber informasi insiden dilakukan dengan mengkonfirmasi jabatan Pelapor Insiden/*User* (U) dan ruangan Pelapor Insiden/*User* (U) berada. *Helpdesk Operator* (HO) akan mencocokkan data sumber informasi dengan database SISDM. Sedangkan verifikasi kelengkapan dilakukan dengan menilai kelengkapan deskripsi laporan insiden oleh Pelapor Insiden/*User* (U). Jika hasil verifikasi menunjukkan ketidaklengkapan, *Helpdesk Operator* (HO) wajib bertanya ulang kepada Pelapor Insiden/*User* (U) agar deskripsi informasi insiden yang disampaikan benar-benar jelas.

Selanjutnya *Helpdesk Operator* (HO) menyimpan informasi insiden yang disampaikan kedalam kartu insiden.

Diagram alir aktifitas pencatatan insiden dapat dilihat pada Gambar 4.3.



Gambar 4.3 Diagram alir prosedur pencatatan insiden

#### 4.5.3 Kategorisasi insiden (*incident categorization*)

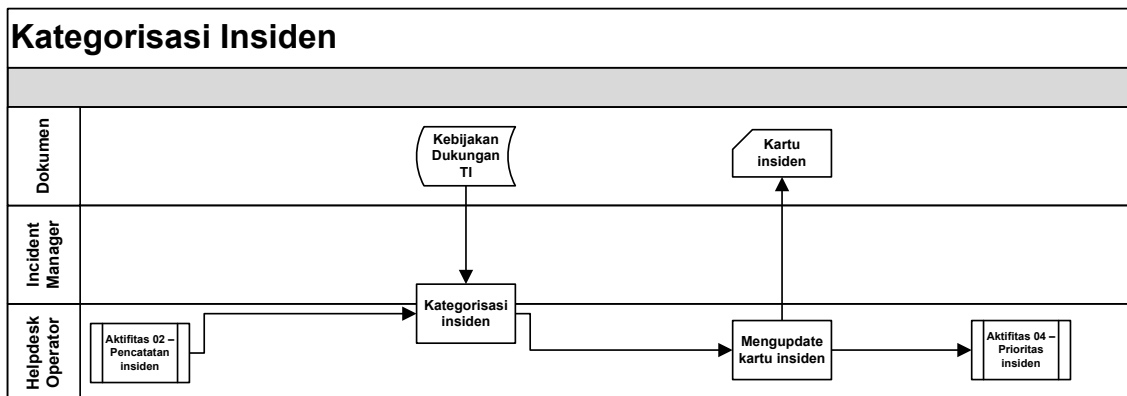
Aktifitas kategorisasi insiden (*incident categorization*) bertujuan untuk memastikan dilakukannya kategorisasi laporan insiden.

Indikator kinerja untuk tujuan ini adalah % laporan insiden yang masuk dalam kategori yang benar, dan jumlah waktu yang dibutuhkan dalam mengkategorikan laporan insiden.

Langkah pertama aktifitas kategorisasi insiden (*incident categorization*) adalah kategorisasi insiden. Dalam langkah ini *Helpdesk Operator* (HO) mengkategorisasikan informasi insiden yang masuk menurut tabel kebijakan kategori insiden. Jika ditemukan suatu insiden memiliki kategori kombinasi atau dapat dimasukkan kedalam 2 kategori utama, maka *Helpdesk Operator* (HO) dapat berkonsultasi dengan *Incident Manager* (IM) mengenai kategori insiden yang akan dipilih.

Selanjutnya *Helpdesk Operator* (HO) mengupdate kartu insiden dengan kategorisasi yang telah dibuat.

Diagram alir aktifitas kategorisasi insiden dapat dilihat pada Gambar 4.4.



Gambar 4.4 Diagram alir prosedur kategorisasi insiden

#### 4.5.4 Prioritas insiden (*incident prioritization*)

Aktifitas prioritas insiden (*incident prioritization*) bertujuan untuk memastikan laporan insiden yang masuk mendapat prioritas penanganan yang tepat dan dilakukan dalam waktu singkat. Selain itu aktifitas ini juga bertujuan untuk memastikan pendelegasian penanganan insiden mendapat staf yang tepat untuk menanganinya.

Indikator kinerja untuk tujuan pertama adalah % laporan insiden yang diberikan prioritas yang sesuai, dan jumlah waktu yang dibutuhkan dalam membuat prioritas laporan insiden. Sedangkan indikator kinerja untuk tujuan kedua adalah % kejadian dimana staf pada level *Helpdesk Operator* (HO) tidak tersedia, dan jumlah eskalasi dari *Helpdesk Operator* (HO) kepada *Helpdesk Specialist* (HS) yang dikarenakan ketidakmampuan staf.

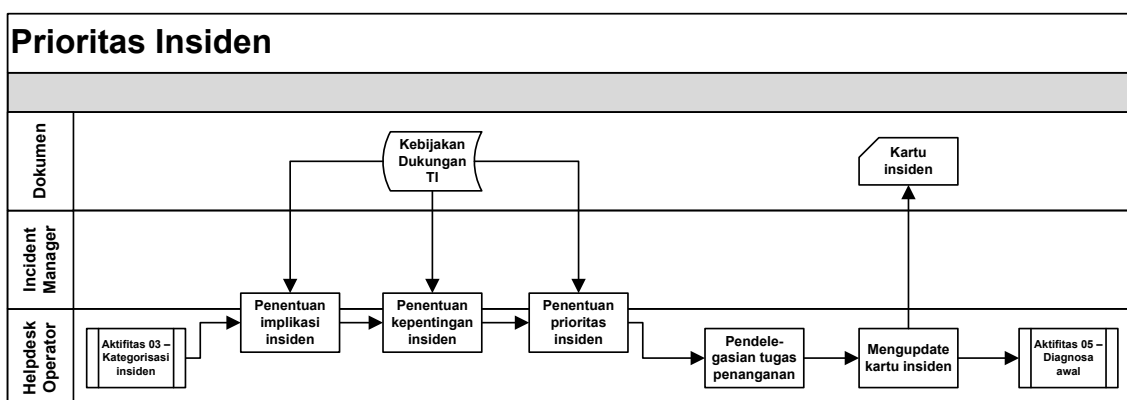
Langkah pertama aktifitas prioritas insiden (*incident prioritization*) adalah menentukan implikasi insiden. *Helpdesk Operator* (HO) membuat penilaian atas informasi insiden yang masuk, mengenai implikasi yang diakibatkan oleh insiden tersebut. Selanjutnya *Helpdesk Operator* (HO) membuat penilaian mengenai kepentingan insiden. Hasil dari 2 (dua) langkah penilaian ini menjadi dasar penentuan prioritas penanganan insiden.

Dalam membuat penilaian, *Helpdesk Operator* (HO) dapat berkonsultasi dengan *Incident Manager* (IM) mengenai asumsi yang akan digunakan. Tabel kebijakan yang menjadi acuan adalah tabel kebijakan implikasi insiden dan tabel kebijakan kepentingan insiden. Sedangkan tabel kebijakan yang digunakan dalam penentuan prioritas insiden adalah tabel kebijakan prioritas insiden.

Setelah menentukan prioritas insiden, *Helpdesk Operator* (HO) mendelegasikan tugas penanganan kepada solver. Dalam pendelegasian tugas, *Helpdesk Operator* (HO) wajib memperhatikan jumlah solver yang tersedia dan beban kerja yang sedang ditanganinya. Selain itu *Helpdesk Operator* (HO) juga dapat berkonsultasi kepada *Incident Manager* (IM) mengenai pemilihan solver.

Selanjutnya *Helpdesk Operator* (HO) mengupdate kartu insiden dengan prioritas yang telah dibuat.

Diagram alir aktifitas prioritas insiden dapat dilihat pada Gambar 4.5.



Gambar 4.5 Diagram alir prosedur prioritas insiden

#### 4.5.5 Diagnosa awal (*initial diagnosis*)

Aktifitas diagnosa awal (*initial diagnosis*) bertujuan untuk memastikan tindakan diagnosa awal dilakukan pada level *Helpdesk Operator* (HO) dalam



waktu singkat. Tujuan kedua aktifitas ini adalah memastikan pimpinan/pejabat mendapat prioritas penanganan on-site. Tujuan ketiga aktifitas ini adalah untuk memastikan tindakan diagnosa awal dapat memberi masukan bagi penanganan insiden keseluruhan dan kalau dimungkinkan dapat memberi solusi atas insiden.

Indikator kinerja tujuan pertama adalah jumlah waktu yang dibutuhkan dalam tindakan diagnosa awal, dan % kesalahan *Helpdesk Operator* (HO) dalam diagnosa awal. Indikator kinerja tujuan kedua adalah % ketersediaan staf *Helpdesk Operator* (HO) untuk penanganan on-site. Indikator kinerja tujuan ketiga adalah % laporan insiden yang ditemukan solusinya dalam diagnosa awal.

Langkah pertama aktifitas diagnosa awal (*initial diagnosis*) adalah diagnosa SLA target waktu penanganan insiden. Diagnosa ini dibutuhkan untuk memenuhi target waktu penanganan setiap insiden. Dalam diagnosa SLA target waktu penanganan insiden, *Helpdesk Operator* (HO) memprediksi waktu yang dibutuhkan untuk penanganan insiden. Hasil prediksi digunakan untuk memilih tindakan penanganan selanjutnya. Jika diketahui insiden termasuk sulit ditangani dan diprediksi waktu penanganan akan lama ditangan *Helpdesk Operator* (HO) maka insiden akan dieskalasi ke level *Helpdesk Specialist* (HS). Jika diprediksi penanganan masih bisa dilakukan dalam target waktu SLA, maka *Helpdesk Operator* (HO) melanjutkan tindakan penanganan ke langkah selanjutnya. Dalam diagnosa SLA, *Helpdesk Operator* (HO) menggunakan tabel kebijakan SLA target waktu penanganan insiden.

Setelah diagnosa tersebut, *Helpdesk Operator* (HO) melihat informasi insiden apakah terjadi pada pimpinan atau pejabat. Jika diketahui insiden tersebut menimpa pimpinan atau pejabat, maka *Helpdesk Operator* (HO) melapor kepada *Incident Manager* (IM) untuk melakukan tindakan penanganan insiden secara langsung atau on-site. Jika insiden terjadi bukan pada pimpinan atau pejabat, *Helpdesk Operator* (HO) melanjutkan ke langkah selanjutnya.

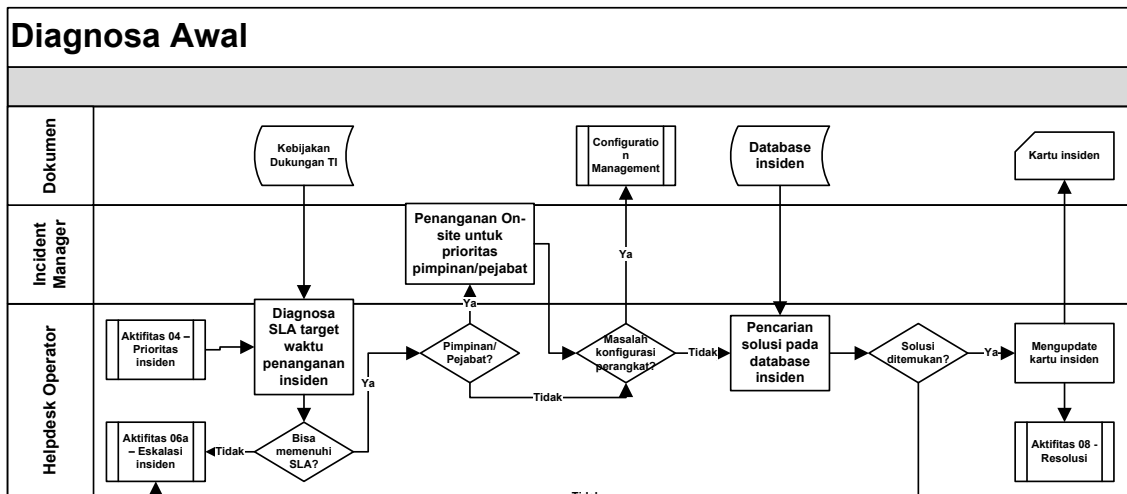
Langkah selanjutnya adalah pemeriksaan konfigurasi perangkat. *Helpdesk Operator* (HO) memeriksa seluruh konfigurasi perangkat yang terkena insiden. Sumber informasi pemeriksaan konfigurasi adalah dari database konfigurasi. Jika ditemukan insiden disebabkan kesalahan konfigurasi, *Helpdesk Operator* (HO)

melakukan usulan perubahan konfigurasi sistem kepada proses manajemen konfigurasi (*configuration management*).

Jika diketahui bukan masalah konfigurasi, *Helpdesk Operator* (HO) mencari solusi pada database insiden untuk mengetahui insiden yang mirip yang pernah terjadi dan solusi yang diambil. Database insiden berisikan kumpulan insiden yang dilaporkan dan ditangani serta solusi yang diambil untuk insiden yang dimaksud. *Helpdesk Operator* (HO) akan membandingkan solusi dalam database insiden dengan insiden yang sedang ditanganinya saat ini. Jika solusi ditemukan dan sesuai dengan kondisi insiden, langkah selanjutnya *Helpdesk Operator* (HO) melakukan aktifitas Resolusi (*resolution and recovery*). Tetapi jika solusi tidak ditemukan dari dalam database insiden, *Helpdesk Operator* (HO) akan melakukan aktifitas Eskalasi (*incident escalation*) kepada level *Helpdesk Specialist* (HS).

Selanjutnya *Helpdesk Operator* (HO) menyimpan informasi penanganan insiden yang sudah dilakukannya berikut segala hasil yang diperolehnya kedalam kartu insiden.

Diagram alir aktifitas diagnosa awal dapat dilihat pada Gambar 4.6.



Gambar 4.6 Diagram alir prosedur diagnosa awal

#### 4.5.6 Eskalasi insiden (*incident escalation*)

Aktifitas eskalasi insiden (*incident escalation*) bertujuan untuk memastikan proses eskalasi dilakukan dalam waktu singkat untuk memenuhi SLA

target waktu penanganan insiden. Tujuan kedua aktifitas ini adalah memastikan eskalasi dilakukan dengan pertimbangan mendalam atas tindakan penanganan yang sudah dilakukan. Tujuan ketiga aktifitas ini adalah untuk memastikan didapatkannya penanggungjawab penanganan insiden pasca eskalasi.

Indikator kinerja untuk tujuan pertama adalah jumlah waktu yang dibutuhkan dalam menetapkan eskalasi insiden, dan % laporan insiden yang terlambat dieskalasi. Indikator kinerja untuk tujuan kedua adalah % eskalasi melalui pertimbangan dari *Incident Manager* (IM). Indikator kinerja untuk tujuan ketiga adalah % ketersediaan staf untuk menangani insiden kombinasi.

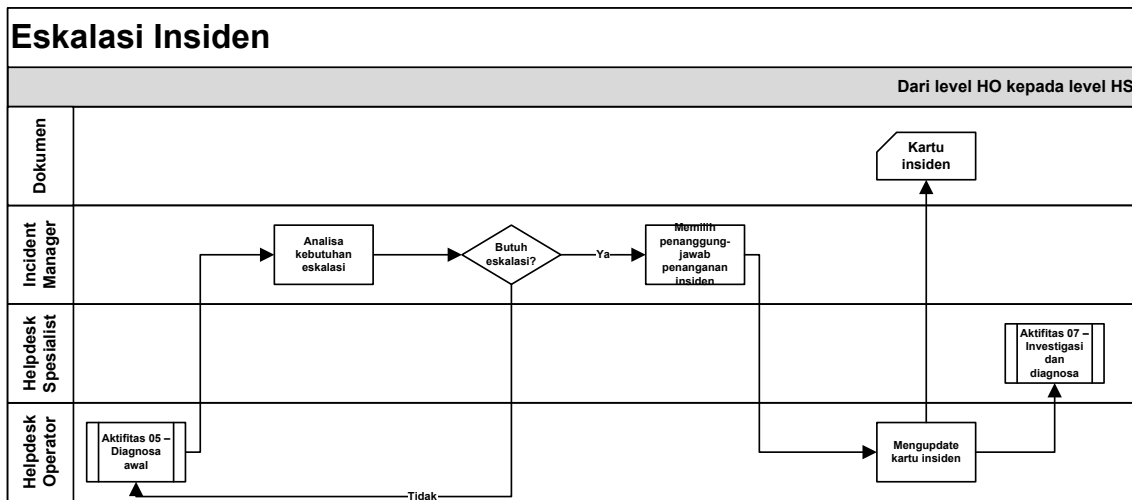
Langkah pertama aktifitas eskalasi insiden (*incident escalation*) adalah analisa kebutuhan eskalasi. Analisa dilakukan untuk menilai apakah eskalasi akan diteruskan ke level penanganan selanjutnya atau kembali ke level penanganan sebelumnya. Dasar analisa adalah tingkat kesulitan penanganan insiden dan SLA target waktu penanganan insiden. Yang terutama diperhatikan oleh *Incident Manager* (IM) adalah SLA target waktu penanganan insiden. Jika diketahui waktu penanganan insiden sudah memakan waktu hingga lebih dari 50% target waktu penanganan, *Incident Manager* (IM) wajib menyetujui usulan eskalasi. Tetapi jika diketahui waktu penanganan insiden masih dibawah 50% target waktu penanganan, *Incident Manager* (IM) akan mempertimbangkan hal lain seperti tingkat kesulitan penanganan insiden.

Setelah analisa dilakukan, kemudian *Incident Manager* (IM) membuat surat tugas baru dan memilih penanggungjawab penanganan insiden khusus untuk proses eskalasi dari *Helpdesk Specialist* (HS) kepada *Software Manager* (SM) / *Network Manager* (NM) / *Maintenance Manager* (MM). Jika kategori insiden adalah pimpinan/pejabat atau software, maka eskalasi tidak perlu dilakukan. Untuk insiden dengan kategori ini, maka penanganan insiden wajib untuk dapat menemukan solusi pada level *Helpdesk Specialist* (HS). Jika kategori insiden adalah SI, maka eskalasi dilakukan kepada level *Software Manager* (SM). Jika kategori insiden adalah *network*, maka eskalasi dilakukan kepada level *Network Manager* (NM). Jika kategori insiden adalah hardware, maka eskalasi dilakukan kepada level *Maintenance Manager* (MM). Khusus untuk penanganan insiden kombinasi atau insiden yang memiliki kategori lebih dari 1 (satu), IM akan

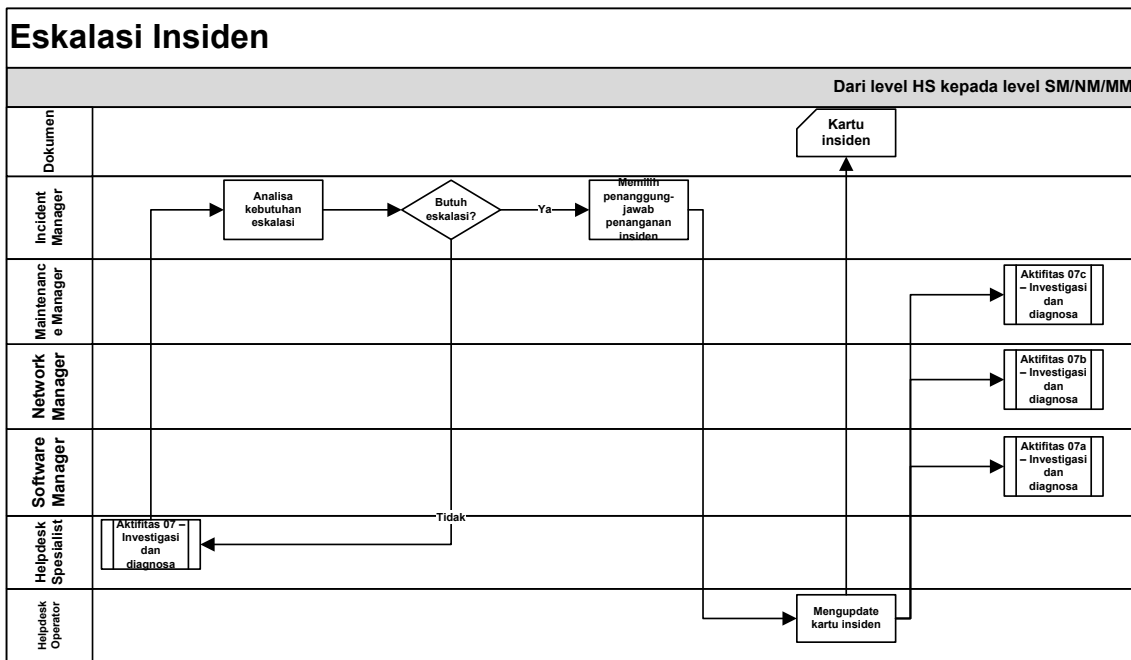
menunjuk langsung penanggungjawab pada level *Software Manager* (SM) / *Network Manager* (NM) / *Maintenance Manager* (MM).

Selanjutnya *Helpdesk Operator* (HO) menerima kembali kartu insiden dari *Incident Manager* (IM) dan kemudian mengupdate kartu insiden dengan informasi eskalasi yang dilakukan.

Diagram alir aktifitas eskalasi insiden dari level *Helpdesk Operator* (HO) kepada *Helpdesk Spesialist* (HS) dapat dilihat pada Gambar 4.7. Sedangkan diagram alir aktifitas eskalasi insiden dari level *Helpdesk Spesialist* (HS) kepada *Software Maneger* (SM) / *Network Manager* (NM) / *Maintenance Manager* (MM) dapat dilihat pada Gambar 4.8.



Gambar 4.7 Diagram alir prosedur eskalasi insiden dari level HO kepada level HS



Gambar 4.8 Diagram alir prosedur eskalasi insiden dari level HS kepada level SM/NM/MM

#### 4.5.7 Investigasi dan diagnosa (*investigation and diagnosis*)

Aktifitas investigasi dan diagnosa (*investigation and diagnosis*) bertujuan untuk memastikan investigasi dilakukan menyeluruh dan mendalam untuk menemukan sumber permasalahan insiden. Tujuan kedua dari aktifitas ini adalah untuk memastikan aktifitas investigasi dan diagnosa dilakukan berdasarkan standar dan memenuhi SLA target waktu penanganan. Tujuan ketiga dari aktifitas ini adalah untuk memastikan solusi yang ditemukan adalah tepat untuk insiden yang dimaksud.

Indikator kinerja untuk tujuan pertama adalah jumlah waktu yang dibutuhkan dalam investigasi laporan insiden, % deskripsi insiden yang sudah lengkap sebelum investigasi dilakukan, dan jumlah tindakan investigasi yang dilakukan hingga menemui Pelapor Insiden/*User* (U) lagi untuk melengkapi deskripsi insiden. Indikator kinerja untuk tujuan kedua adalah % waktu yang dibutuhkan untuk melakukan aktifitas investigasi dan diagnosa. Indikator kinerja untuk tujuan ketiga adalah % solusi yang ditemukan setelah aktifitas investigasi dan diagnosa oleh *Helpdesk Specialist* (HS), % solusi yang ditemukan setelah aktifitas investigasi dan diagnosa oleh *Software Manager* (SM), % solusi yang

ditemukan setelah aktifitas investigasi dan diagnosa oleh *Network Manager* (NM), % solusi yang ditemukan setelah aktifitas investigasi dan diagnosa oleh *Maintenance Manager* (MM), dan % penanganan diberikan kepada pihak *supplier*.

Langkah pertama aktifitas investigasi dan diagnosa (*investigation and diagnosis*) adalah rievew kartu insiden. Rievew diberikan atas deskripsi insiden dan semua tindakan penanganan yang telah dilakukan sebelumnya. Jika *Helpdesk Spesialist* (HS) merasa belum jelas dengan deskripsi yang terdapat pada kartu insiden, maka *Helpdesk Operator* (HO) wajib memberikan seluruh keterangan mengenai deskripsi yang didapatkannya dari Pelapor Insiden/*User* (U) dan tindakan diagnosa yang sudah dilakukannya. *Helpdesk Spesialist* (HS) dapat menemui langsung Pelapor Insiden/*User* (U) jika dirasakan deskripsi insiden masih belum jelas juga. Pada langkah review ini, *Helpdesk Spesialist* (HS) harus dapat menemukan akar permasalahan insiden.

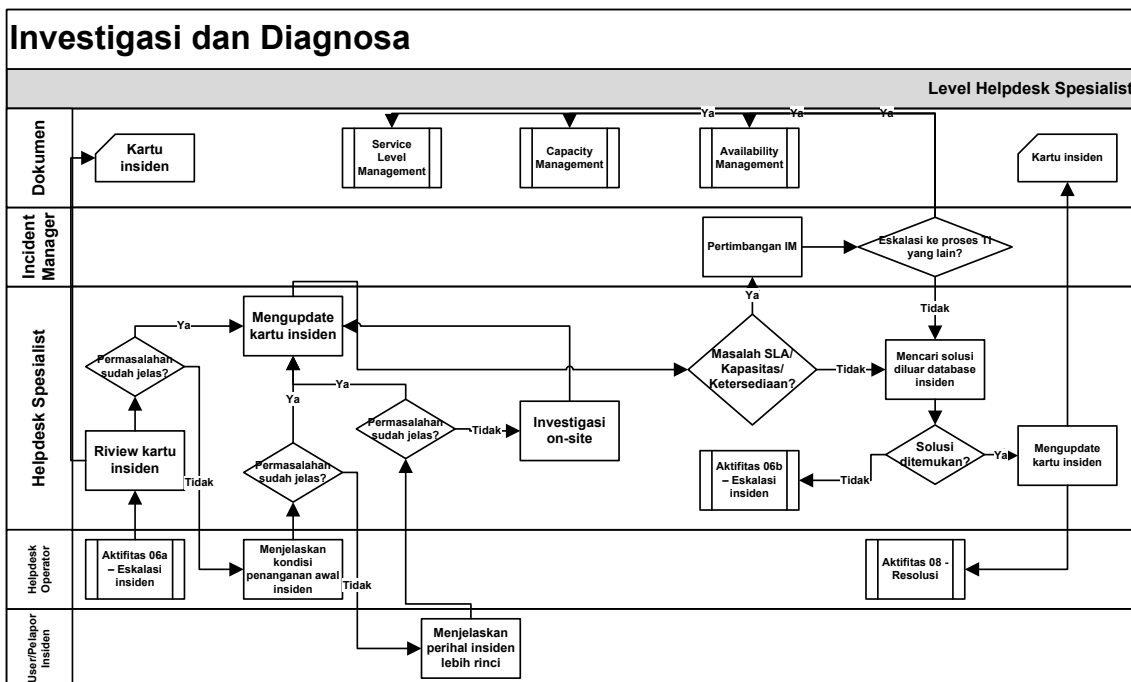
Setelah melakukan rievew kartu insiden, langkah selanjutnya adalah *Helpdesk Spesialist* (HS) memeriksa apakah insiden terkait dengan proses manajemen SLA, proses manajemen kapasitas, dan proses manajemen ketersediaan. Jika insiden diketahui terkait dengan proses manajemen SLA, *Helpdesk Spesialist* (HS) melakukan usulan perubahan SLA kepada proses manajemen SLA (*SLA Management*). Jika insiden diketahui terkait dengan proses manajemen kapasitas, *Helpdesk Spesialist* (HS) melakukan usulan perubahan kapasitas kepada proses manajemen kapasitas (*Capacity Management*). Jika insiden diketahui terkait dengan proses manajemen ketersediaan, *Helpdesk Spesialist* (HS) melakukan usulan perubahan ketersediaan kepada proses manajemen ketersediaan (*Availability Management*).

Untuk insiden yang diketahui tidak terkait dengan proses manajemen SLA, proses manajemen kapasitas, dan proses manajemen ketersediaan, selanjutnya *Helpdesk Spesialist* (HS) melakukan investigasi menyeluruh menggunakan informasi insiden yang dimiliki untuk mencari solusi atas insiden. Investigasi yang dilakukan wajib menggunakan panduan maupun standar yang sudah ditetapkan. Selain itu dimungkinkan *Helpdesk Spesialist* (HS) mencari solusi pada forum-forum internal/eksternal atau pada ahli yang terpercaya. Aktifitas eskalasi

insiden (*incident escalation*) akan dilakukan jika solusi atas insiden belum juga ditemukan.

Selanjutnya *Helpdesk Specialist* (HS) mengkonfirmasi *Helpdesk Operator* (HO) untuk mengupdate kartu insiden dengan informasi tindakan penanganan insiden yang telah dilakukannya.

Diagram alir aktifitas investigasi dan diagnosa pada level *Helpdesk Specialist* (HS) dapat dilihat pada Gambar 4.9.



Gambar 4.9 Diagram alir prosedur investigasi dan diagnosa oleh level *Helpdesk Specialist*

Langkah pertama aktifitas investigasi dan diagnosa (*investigation and diagnosis*) oleh *Software Manager* (SM) adalah memastikan deskripsi insiden sudah lengkap dan menyentuh akar permasalahan insiden.

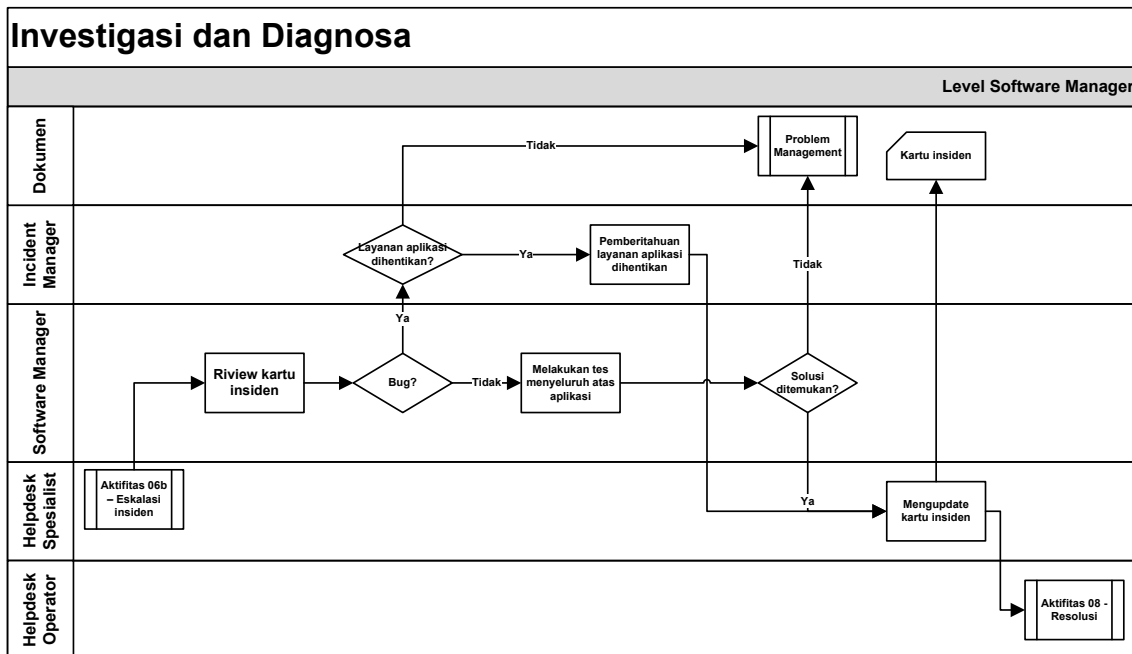
Kemudian *Software Manager* (SM) melakukan uji atas aplikasi SI yang dilaporkan mengalami insiden. Uji aplikasi dilakukan untuk mengetahui adanya bug atau tidak. Jika ditemukan adanya bug, langkah selanjutnya *Software Manager* (SM) akan melapor kepada *Incident Manager* (IM) mengenai penghentian layanan aplikasi SI untuk sementara.

*Incident Manager* (IM) akan memutuskan mengenai penghentian layanan dengan mempertimbangkan kepentingan penggunaan aplikasi saat itu. Jika diputuskan layanan aplikasi akan dihentikan, *Software Manager* (SM) akan mengupdate kartu insiden mengenai solusi yang diambil tersebut. Jika diputuskan layanan aplikasi tidak bisa dihentikan sementara bug didalamnya menyebabkan insiden, *Incident Manager* (IM) melakukan usulan penanganan insiden kepada proses manajemen masalah (*Problem Management*).

Untuk insiden yang diketahui bukan karena bug aplikasi, *Software Manager* (SM) memperluas cakupan pemeriksaan dengan memeriksa keterkaitan aplikasi yang terkena insiden tersebut dengan aplikasi lainnya untuk mencari penyebab insiden sebenarnya. Dalam melakukan tes, *Software Manager* (SM) menggunakan panduan pengembangan aplikasi SI.

Selanjutnya *Software Manager* (SM) mengkonfirmasi *Helpdesk Operator* (HO) untuk mengupdate kartu insiden dengan informasi tindakan penanganan insiden yang telah dilakukannya.

Diagram alir aktifitas investigasi dan diagnosa pada level *Software Manager* (SM) dapat dilihat pada Gambar 4.10.



Gambar 4.10 Diagram alir prosedur investigasi dan diagnosa oleh level *Software Manager*



Langkah pertama aktifitas investigasi dan diagnosa (*investigation and diagnosis*) oleh *Network Manager* (NM) adalah memastikan deskripsi insiden sudah lengkap dan menyentuh akar permasalahan insiden.

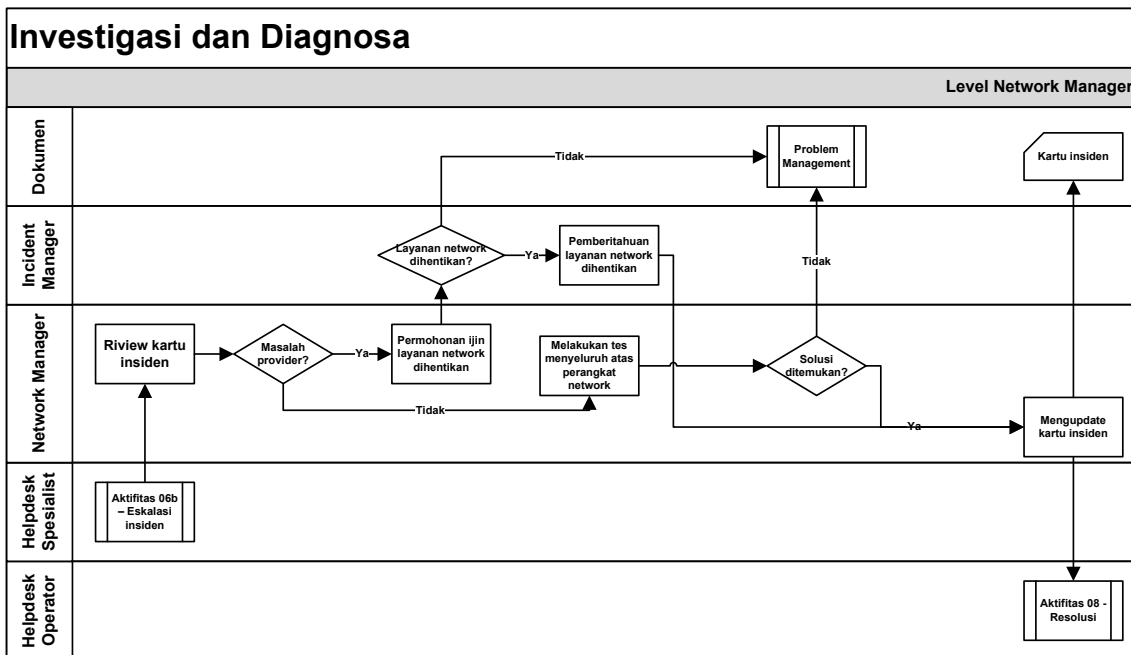
Kemudian *Network Manager* (NM) memeriksa apakah insiden terkait dengan operator provider *network*. Jika ditemukan insiden terkait dengan provider, *Network Manager* (NM) membuat permohonan kepada *Incident Manager* (IM) untuk menghentikan sementara layanan *network*. Hal ini untuk menghindari insiden yang sama terulang kembali.

*Incident Manager* (IM) akan mempertimbangkan segala aspek dalam membuat keputusan penghentian sementara layanan *network*. Jika diputuskan untuk menghentikan sementara layanan *network*, *Incident Manager* (IM) akan membuat pengumuman penghentian sementara layanan *network* dan *Network Operator* kemudian mengupdate solusi tersebut pada kartu insiden. Jika diputuskan layanan *network* tidak perlu dihentikan, selanjutnya *Incident Manager* (IM) melakukan usulan penanganan insiden kepada proses manajemen masalah (*Problem Management*).

Jika tidak ditemukan masalah dengan provider, *Network Manager* (NM) akan melakukan inspeksi menyeluruh atas perangkat *network* yang dilaporkan terkena insiden. Inspeksi dilakukan untuk mencari sumber permasalahan insiden. Jika solusi ditemukan, kemudian *Network Manager* (NM) mengupdate kartu insiden. Dan jika solusi juga belum ditemukan, *Network Manager* melakukan usulan penanganan insiden kepada proses manajemen masalah (*Problem Management*).

Selanjutnya *Network Manager* (NM) mengkonfirmasi *Helpdesk Operator* (HO) untuk mengupdate kartu insiden dengan informasi tindakan penanganan insiden yang telah dilakukannya.

Diagram alir aktifitas investigasi dan diagnosa pada level *Network Manager* (NM) dapat dilihat pada Gambar 4.11.



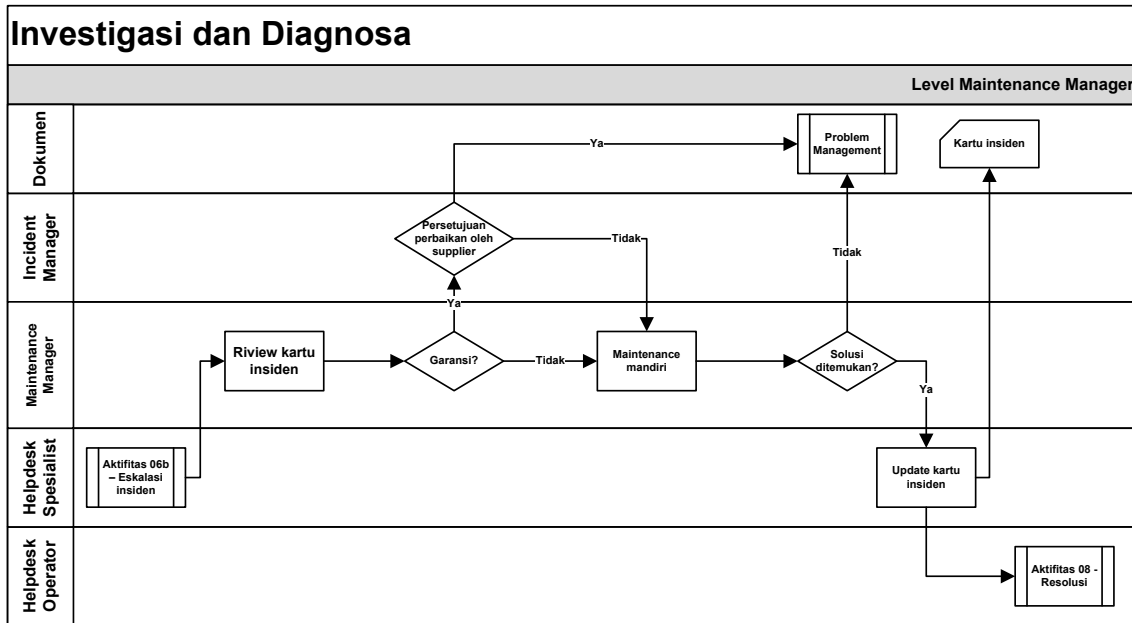
Gambar 4.11 Diagram alir prosedur investigasi dan diagnosa oleh level *Network Manager*

Langkah pertama aktifitas investigasi dan diagnosa (*investigation and diagnosis*) oleh *Maintenance Manager* (MM) adalah memastikan deskripsi insiden sudah lengkap dan menyentuh akar permasalahan insiden.

Kemudian *Maintenance Manager* (MM) memeriksa masa garansi perangkat yang terkena insiden. Jika diketahui perangkat masih dalam masa garansi, selanjutnya *Maintenance Manager* (MM) membuat usulan kepada *Incident Manager* (IM) mengenai perbaikan perangkat oleh *supplier*. Jika diputuskan perbaikan perangkat oleh *supplier*, *Incident Manager* (IM) akan melakukan usulan penanganan insiden kepada proses manajemen masalah (*Problem Management*) oleh karena solusi perbaikan perangkat kepada *supplier*, adalah bagian dari proses manajemen masalah (*Problem Management*). Jika diputuskan untuk tidak melakukan perbaikan perangkat oleh *supplier*, maka *Maintenance Manager* (MM) akan menyelesaikan permasalahan insiden secara mandiri.

Selanjutnya *Maintenance Manager* (MM) mengkonfirmasi *Helpdesk Operator* (HO) untuk mengupdate kartu insiden dengan informasi tindakan penanganan insiden yang telah dilakukannya.

Diagram alir aktifitas investigasi dan diagnosa pada level *Maintenance Manager* (MM) dapat dilihat pada Gambar 4.12.



Gambar 4.12 Diagram alir prosedur investigasi dan diagnosa oleh level *Maintenance Manager*

#### 4.5.8 Resolusi (*resolution and recovery*)

Aktifitas resolusi (*resolution and recovery*) bertujuan untuk memastikan solusi atas insiden sudah teruji dan dapat diimplementasikan.

Indikator untuk tujuan ini adalah % solusi yang diimplementasikan adalah benar solusi atas insiden tersebut, dan % solusi yang tidak dapat diimplementasikan.

Langkah pertama aktifitas resolusi (*resolution and recovery*) adalah *Helpdesk Operator* (HO) menerima solusi atas insiden dari aktifitas diagnosa awal (*initial diagnosis*) yang dilakukannya, maupun aktifitas investigasi dan diagnosa (*investigation and diagnosis*) yang dilakukan oleh *Helpdesk Specialist* (HS) / *Software Manager* (SM) / *Network Manager* (NM) / *Maintenance Manager* (MM). *Helpdesk Operator* (HO) akan memastikan solusi yang diterima adalah solusi untuk insiden yang dimaksud dan solusi tersebut sudah teruji benar.

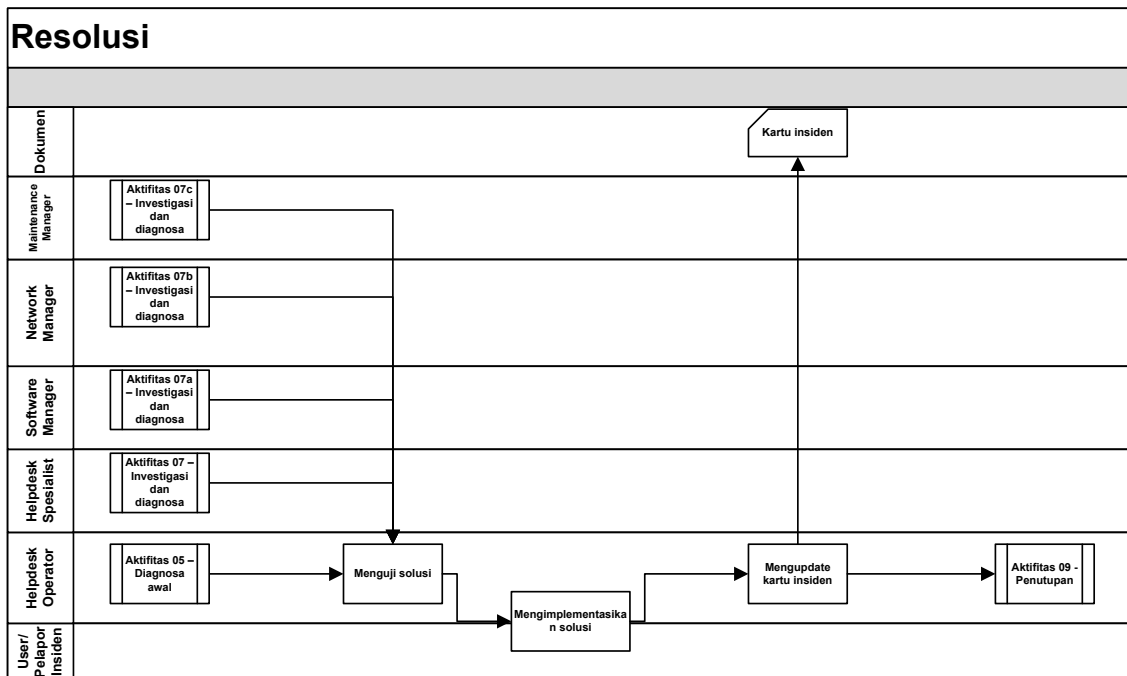
Kemudian *Helpdesk Operator* (HO) akan menguji solusi yang ditemukan sebelum implementasi. Pengujian dilakukan dengan mereview langkah-langkah

penanganan insiden yang tertulis dalam kartu insiden. Tujuannya adalah untuk memastikan solusi diperoleh melalui langkah-langkah terstandar. Proses ujicoba solusi insiden tersebut dilakukan oleh *Helpdesk Operator* (HO) dengan supervisi dari *Helpdesk Specialist* (HS) atau *Software Manager* (SM) / *Network Manager* (NM) / *Maintenance Manager* (MM) yang menemukan solusi insiden tersebut.

Setelah ujicoba dinyatakan berhasil, *Helpdesk Operator* (HO) mengkonfirmasi Pelapor Insiden/*User* (U) mengenai implementasi solusi tersebut. *Helpdesk Operator* (HO) meminta ijin kepada Pelapor Insiden/*User* (U) mengenai proses implementasi solusi. Ijin dibutuhkan untuk implementasi solusi dalam ruangan kerja Pelapor Insiden/*User* (U). Hal ini dilakukan untuk menghindari terganggunya proses kerja yang sedang dilakukan Pelapor Insiden/*User* (U) maupun staf lainnya yang seruangan dengan Pelapor Insiden/*User* (U).

Selanjutnya *Helpdesk Operator* (HO) mengupdate kartu insiden dengan informasi tindakan implementasi solusi yang telah dilakukannya.

Diagram alir aktifitas resolusi dapat dilihat pada Gambar 4.13.



Gambar 4.13 Diagram alir prosedur resolusi

#### 4.5.9 Penutupan (*incident closure*)

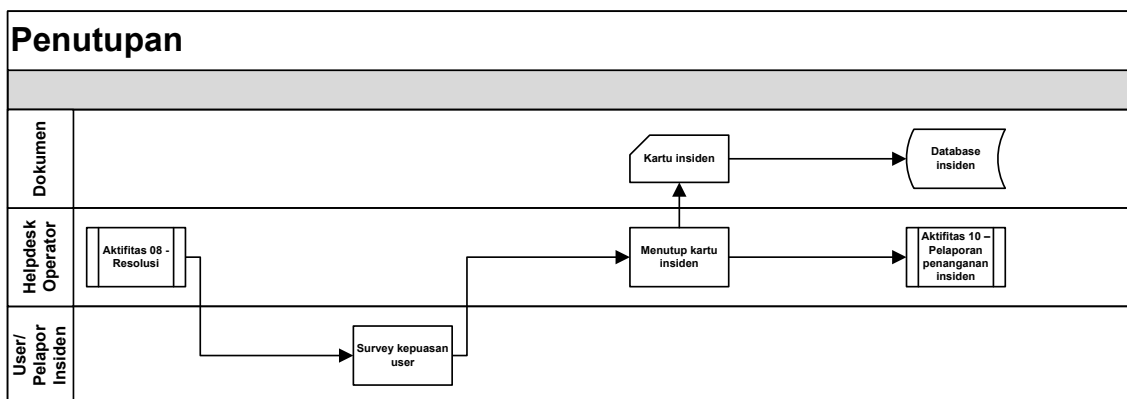
Aktifitas penutupan (*incident closure*) bertujuan untuk memastikan Memastikan aktifitas penutupan dilakukan. Selain itu aktifitas ini juga bertujuan untuk memastikan komplain dari Pelapor Insiden/*User* (U) diterima.

Indikator kinerja untuk aktifitas pertama adalah % kartu insiden dengan status “Belum selesai” tetapi sebenarnya sudah ditemukan dan sudah diimplementasikan solusinya, dan % penanganan insiden yang sesuai SLA target waktu penanganan. Indikator kinerja untuk aktifitas kedua adalah % komplain dari Pelapor Insiden/*User* (U) atas solusi yang diberikan.

Langkah pertama aktifitas penutupan (*incident closure*) adalah survey kepuasan Pelapor Insiden/*User* (U). *Helpdesk Operator* (HO) bertanya kepada Pelapor Insiden/*User* (U) mengenai tindakan penanganan insiden yang sudah dilakukan. Selain itu *Helpdesk Operator* (HO) juga bertanya kepada Pelapor Insiden/*User* (U) mengenai kepuasan atas waktu dan metode penanganan insiden.

*Helpdesk Operator* (HO) kemudian mencatat jawaban Pelapor Insiden/*User* (U) ke dalam kartu insiden. Setelah dicatat dalam kartu insiden, *Helpdesk Operator* (HO) menutup proses penanganan insiden dengan menyimpan kartu insiden dalam database insiden.

Diagram alir aktifitas penutupan dapat dilihat pada Gambar 4.14.



Gambar 4.14 Diagram alir prosedur penutupan

#### 4.5.10 Pelaporan penanganan insiden (*incident management report*)

Aktifitas pelaporan penanganan insiden (*incident management report*) bertujuan untuk memastikan dilakukannya rekapitulasi harian. Tujuan kedua

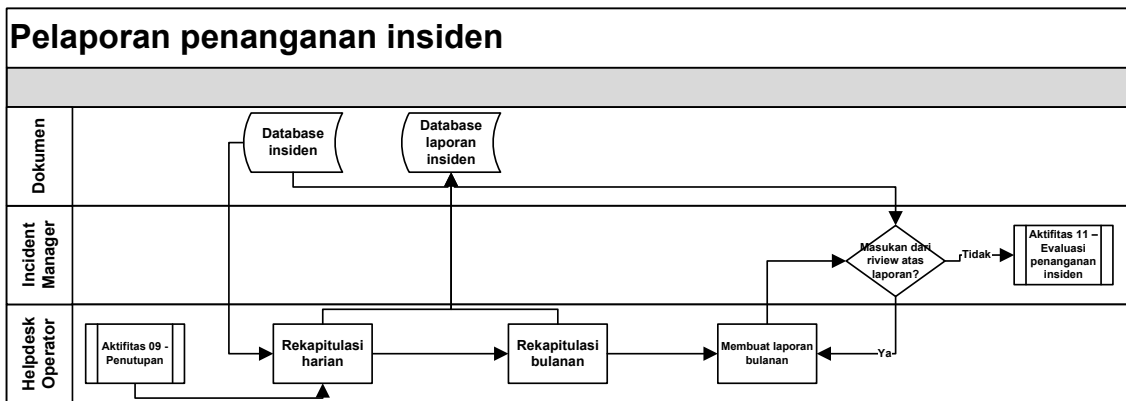
aktifitas ini adalah memastikan dilakukannya rekapitulasi bulanan. Tujuan ketiga aktifitas ini adalah memastikan laporan penanganan insiden dibuat sebagai bahan evaluasi tindakan penanganan di masa datang.

Indikator tujuan pertama dan kedua aktifitas ini adalah % kelengkapan rekapitulasi. Sedangkan indikator tujuan ketiga aktifitas ini adalah % kelengkapan laporan, dan jumlah ketepatan waktu penyampaian laporan.

Langkah pertama aktifitas pelaporan penanganan insiden (*incident management report*) adalah rekapitulasi harian. Setiap akhir hari kerja *Helpdesk Operator* (HO) merekapitulasi seluruh penanganan insiden yang dilakukan pada hari tersebut. Sumber kompilasi berasal dari database insiden. Data yang dicatat dalam formulir formulir rekapitulasi harian adalah ID kartu insiden, status masing-masing kartu insiden, deskripsi singkat insiden, langkah penanganan insiden yang sudah dilakukan, hasil survey lisan, serta nama staf yang menanganinya dan level penanganan dimana dia berada

Setiap awal bulan, *Helpdesk Operator* (HO) melakukan rekapitulasi bulanan penanganan insiden bulan sebelumnya. Hasil rekapitulasi akan digunakan dalam membuat laporan bulanan penanganan insiden. Laporan ini kemudian akan diriview oleh *Incident Manager* (IM) dengan menggunakan data pembanding langsung dari database insiden. Jika ada masukan dari *Incident Manager* (IM), *Helpdesk Operator* (HO) akan memperbaiki laporan tersebut. Jika laporan sudah disetujui, selanjutnya laporan akan dibawa ke dalam aktifitas evaluasi penanganan insiden (*incident management evaluation*).

Diagram alir aktifitas pelaporan penanganan insiden dapat dilihat pada Gambar 4.15.



Gambar 4.15 Diagram alir prosedur pelaporan penanganan insiden

#### 4.5.11 Evaluasi penanganan insiden (*incident management evaluation*)

Aktifitas evaluasi penanganan insiden (*incident management evaluation*) bertujuan untuk memastikan evaluasi dilakukan secara setiap bulan untuk meningkatkan kualitas penanganan insiden. Tujuan kedua aktifitas ini adalah untuk memastikan hasil evaluasi ditindaklanjuti oleh masing-masing pihak pada level penanganan insiden

Indikator aktifitas pertama adalah jumlah rapat evaluasi yang dilakukan selama tahun kerja, dan jumlah survey yang dilakukan selama tahun kerja. Indikator kinerja untuk aktifitas kedua adalah % hasil evaluasi yang tidak ditindaklanjuti.

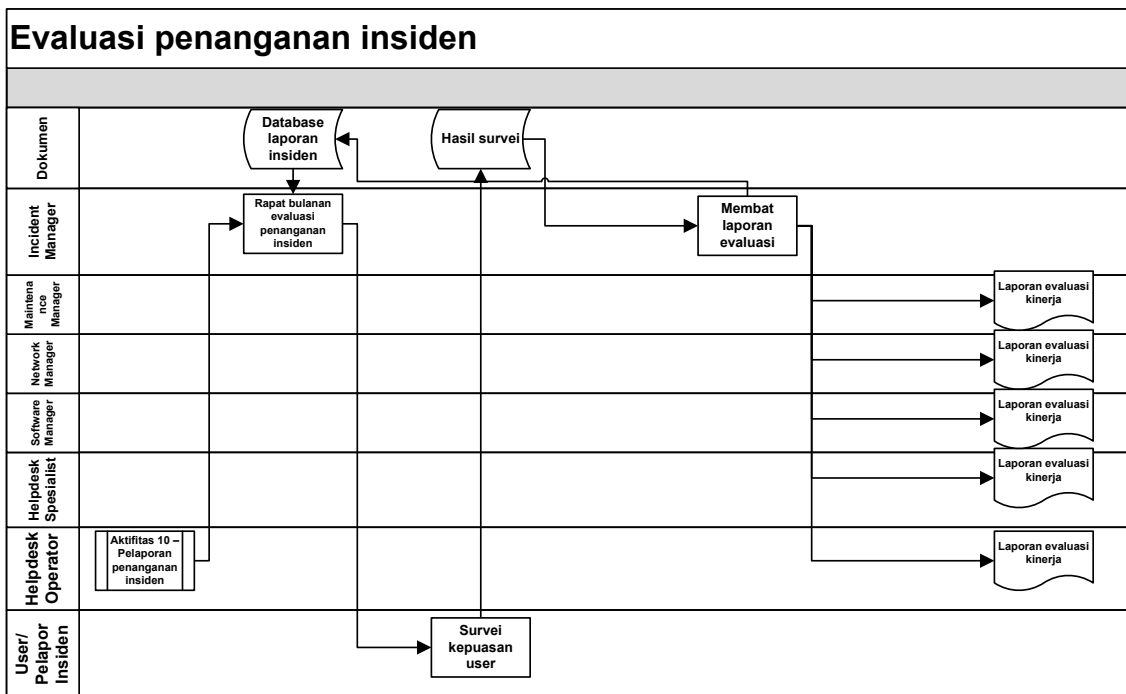
Langkah pertama aktifitas evaluasi penanganan insiden (*incident management evaluation*) adalah rapat bulanan evaluasi penanganan insiden. Setiap awal bulan setelah laporan bulanan penanganan insiden selesai dibuat dan diriview oleh *Incident Manager* (IM), diadakan rapat bulanan evaluasi penanganan insiden yang diikuti oleh penanggungjawab *Helpdesk Operator* (HO), penanggungjawab *Helpdesk Specialist* (HS), *Software Manager* (SM), *Network Manager* (NM), dan *Maintenance Manager* (MM), dengan *Incident Manager* (IM) sebagai pemimpin rapat.

Kemudian pada setiap akhir semester atau setiap 6 (enam) bulan sekali, dilakukan survei kepuasan Pelapor Insiden/*User* (U) atas penanganan insiden. Hasil survei kemudian disimpan dalam database hasil survei. Dalam survei juga

diminta masukan mengenai pelaksanaan penanganan insiden dan keluhan dari Pelapor Insiden/*User* (U).

Hasil survei akan diolah menjadi laporan evaluasi dan usulan peningkatan kinerja. Laporan ini akan menjadi masukan bagi masing-masing pihak pelaksana penanganan insiden. Laporan evaluasi dan usulan peningkatan kinerja kemudian disimpan dalam database laporan dan evaluasi. Selain itu usulan peningkatan kinerja juga disampaikan kepada masing-masing pelaksana penanganan insiden.

Diagram alir aktifitas evaluasi penanganan insiden dapat dilihat pada Gambar 4.16.



Gambar 4.16 Diagram alir prosedur evaluasi penanganan insiden

#### 4.6 Pembuatan Formulir dan Dokumen Pelaksanaan Manajemen Insiden

Formulir pelaksanaan diperlukan untuk penyelenggaraan manajemen insiden. Tabel 4.9 menampilkan formulir dan dokumen yang dibutuhkan dalam penyempurnaan program manajemen help desk dan dukungan TI dengan fokus pada manajemen insiden, sesuai dengan paparan aktifitas-aktifitas di atas.



Tabel 4.9 Dokumen dan Formulir

No.	Aktifitas	Nama Dokumen dan Formulir
1.	Identifikasi insiden ( <i>incident identification</i> )	<ul style="list-style-type: none"> <li>• Jadwal inspeksi berkala</li> <li>• Surat tugas inspeksi berkala</li> <li>• Database konfigurasi</li> <li>• Database SLA kinerja perangkat TI</li> <li>• Database laporan inspeksi</li> <li>• Formulir laporan inspeksi staf teknis</li> </ul>
2.	Pencatatan insiden ( <i>incident logging</i> )	<ul style="list-style-type: none"> <li>• Formulir laporan pengaduan email</li> <li>• Formulir laporan pengaduan meja <i>helpdesk</i></li> <li>• Formulir laporan pengaduan telepon</li> <li>• Formulir laporan inspeksi staf teknis</li> <li>• Kartu insiden</li> <li>• Database SISDM</li> </ul>
3.	Kategorisasi insiden ( <i>incident categorization</i> )	<ul style="list-style-type: none"> <li>• Kebijakan mengenai kategori insiden</li> <li>• Kartu insiden</li> </ul>
4.	Prioritas insiden ( <i>incident prioritization</i> )	<ul style="list-style-type: none"> <li>• Kebijakan mengenai prioritas insiden</li> <li>• Kartu insiden</li> <li>• Surat permohonan bantuan staf penanganan insiden</li> <li>• Surat tugas penanganan insiden</li> <li>• Rekapitan daftar tugas penanganan insiden</li> <li>• Database insiden</li> </ul>
5.	Diagnosa awal ( <i>initial diagnosis</i> )	<ul style="list-style-type: none"> <li>• Kartu insiden</li> <li>• Kebijakan SLA target waktu penanganan insiden</li> <li>• Database insiden</li> <li>• Database konfigurasi</li> <li>• Formulir eskalasi</li> <li>• Formulir penanganan on-site</li> <li>• Surat tugas penanganan insiden</li> <li>• Proses manajemen konfigurasi</li> </ul>
6.	Eskalasi insiden ( <i>incident escalation</i> )	<ul style="list-style-type: none"> <li>• Formulir eskalasi</li> <li>• Surat tugas penanganan insiden</li> <li>• Surat pemberitahuan eskalasi</li> </ul>

No.	Aktifitas	Nama Dokumen dan Formulir
		<ul style="list-style-type: none"> <li>• Kebijakan SLA target waktu penanganan insiden</li> <li>• Kebijakan mengenai kategori insiden</li> </ul>
7.	Investigasi ( <i>investigation and diagnosis</i> )	<ul style="list-style-type: none"> <li>• Kartu insiden</li> <li>• Formulir eskalasi</li> <li>• Formulir penghentian layanan aplikasi SI</li> <li>• Formulir penghentian layanan <i>network</i></li> <li>• Formulir pengajuan perbaikan perangkat oleh <i>supplier</i></li> <li>• Surat tugas penanganan insiden</li> <li>• Surat pemberitahuan perubahan SLA</li> <li>• Surat pemberitahuan perubahan kapasitas</li> <li>• Surat pemberitahuan perubahan ketersediaan</li> <li>• Proses manajemen SLA</li> <li>• Proses manajemen kapasitas</li> <li>• Proses manajemen ketersediaan</li> <li>• Proses manajemen masalah</li> <li>• Kebijakan SLA target waktu penanganan insiden</li> </ul>
8.	Resolusi ( <i>resolution and recovery</i> )	<ul style="list-style-type: none"> <li>• Kartu insiden</li> <li>• Database insiden</li> <li>• Surat pemberitahuan gagalnya ujicoba solusi</li> <li>• Surat ijin implementasi solusi</li> </ul>
9.	Penutupan ( <i>incident closure</i> )	<ul style="list-style-type: none"> <li>• Kartu insiden</li> <li>• Database insiden</li> </ul>
10.	Pelaporan penanganan insiden ( <i>incident management report</i> )	<ul style="list-style-type: none"> <li>• Database insiden</li> <li>• Database laporan insiden</li> <li>• Rekapian harian penanganan insiden</li> <li>• Rekapian bulanan penanganan insiden</li> <li>• Laporan bulanan penanganan insiden</li> </ul>
11.	Evaluasi penanganan insiden ( <i>incident management evaluation</i> )	<ul style="list-style-type: none"> <li>• Laporan bulanan penanganan insiden</li> <li>• Database SISDM</li> <li>• Laporan evaluasi kinerja</li> </ul>

#### **4.7 Pembuatan Matriks Tata Laksana**

Pada tahap ini dibuat matriks tata laksana program manajemen *helpdesk* dan dukungan TI dengan fokus pada manajemen insiden sebagai kesimpulan dari keseluruhan proses manajemen insiden. Selain itu matriks tata laksana tersebut juga bertujuan untuk membantu pelaksana membaca keseluruhan proses, memahami dan mengontrol aktifitas yang dijalankannya.

Matriks tata laksana ini memiliki rincian prosedur berikut indikator kinerja, RACI Chart, dokumen yang digunakan dan waktu pelaksanaan masing-masing aktifitas. Diagram RACI disertakan dalam matriks untuk menunjukkan pelaksana dan peran dalam setiap langkah aktifitas.

Waktu pelaksanaan masing-masing aktifitas ditetapkan dalam format minggu. Hal ini dikarenakan menurut dokumen *framework* ITIL, pelaksanaan aktifitas-aktifitas tersebut saling terkait satu sama lain. Keseluruhan proses manajemen insiden diawali oleh aktifitas identifikasi insiden dan aktifitas selanjutnya dilaksanakan menurut urutan yang ditetapkan. Khusus untuk aktifitas pelaporan ditetapkan dilaksanakan pada akhir bulan, sementara untuk aktifitas evaluasi ditetapkan dilaksanakan pada awal bulan.

Alasan penetapan waktu pelaksanaan aktifitas pelaporan pada akhir bulan adalah untuk merangkum keseluruhan pelaksanaan proses manajemen insiden pada bulan tersebut. Sementara alasan penetapan waktu pelaksanaan aktifitas evaluasi pada awal bulan adalah untuk mengevaluasi pelaksanaan proses manajemen insiden pada bulan sebelumnya sebagai acuan pelaksanaan pada bulan selanjutnya.

#### **4.8 Pembuatan Dokumen Tata Laksana**

Dokumen tata laksana disusun terdiri dari bagian I yaitu sampul dokumen, halaman daftar isi, dan dokumen kontrol, bagian II yang berisi dokumen prosedur, bagian III yang berisi diagram RACI dan diagram alir, bagian IV yang berisi dokumen dan formulir pendukung prosedur, dan bagian V yang berisi matriks tata laksana.

Keseluruhan dokumen tata laksana dapat dilihat pada buku kedua dari tesis ini.

#### **4.8.1 Lembar Kontrol**

Bagian ini berisi kontrol terhadap pengembangan dokumen. Dokumen ini berisi 2 (dua) tabel yaitu tabel kontrol dan tabel pengesahan. Pada tabel pertama berisi nomor versi dokumen terkini berikut keterangan masukan yang didapat pada versi dokumen terdahulu. Sedangkan tabel kedua berisi tanggal, pihak yang mengesahkan dan nomor resmi dokumen setelah disahkan oleh organisasi. Tabel kontrol akan selalu diisi selama dokumen dipergunakan dan jika ditemukan suatu masukan perubahan besar ataupun kecil.

Dokumen kontrol dapat dilihat pada buku kedua dari tesis ini, bagian Dokumen Kontrol.

#### **4.8.2 Pendahuluan**

Bagian pendahuluan terdiri atas 3 poin yaitu fokus, defenisi dan ruang lingkup. Poin-poin ini menjadi dasar pelaksanaan dokumen tata laksana. Pernyataan fokus pelaksanaan dokumen tata laksana dapat dilihat pada buku kedua dari tesis ini, bagian Pendahuluan poin A.

Selanjutnya adalah poin yang berisi defenisi dasar dari insiden dan manajemen insiden yang digunakan dalam dokumen tata laksana. Pernyataan defenisi insiden dan manajemen insiden tersebut dapat dilihat pada buku kedua dari tesis ini, bagian Pendahuluan poin B.

Kemudian poin terakhir berisi batasan proses penanganan insiden yang akan diterapkan. Pernyataan batasan tersebut dapat dilihat pada buku kedua dari tesis ini, bagian Pendahuluan poin C.

#### **4.8.3 Dokumen Prosedur**

Bagian ini berisi rincian prosedur manajemen insiden pada program manajemen *helpdesk* dan dukungan TI. Dokumen prosedur terkait erat dengan dokumen kebijakan dukungan TI dan dokumen panduan dukungan TI yang dibangun oleh biro TI. Rincian prosedur diterjemahkan ke dalam 11 (sebelas) aktifitas beserta langkah-langkah kerja dilakukannya. Aktifitas utama berjumlah 9 (sembilan) dikembangkan berdasarkan *framework* ITIL, sementara 2 (dua)

aktifitas tambahan dikembangkan berdasarkan kebutuhan organisasi untuk evaluasi. Berikut adalah rincian prosedur-prosedur tersebut:

1. Identifikasi insiden (*incident identification*)
2. Pencatatan insiden (*incident logging*)
3. Kategorisasi insiden (*incident categorization*)
4. Prioritas insiden (*incident prioritization*)
5. Diagnosa awal (*initial diagnosis*)
6. Eskalasi insiden (*incident escalation*)
7. Investigasi dan diagnosa (*investigation and diagnosis*)
8. Resolusi (*resolution and recovery*)
9. Penutupan (*incident closure*)
10. Pelaporan penanganan insiden (*incident management report*)
11. Evaluasi penanganan insiden (*incident management evaluation*)

Masing-masing dokumen prosedur disusun dengan urutan lembar pengesahan, tujuan, indikator kinerja, ruang lingkup, rincian prosedur, formulir dan dokumen, diagram RACI, istilah dan singkatan, dan catatan perubahan.

#### **4.8.3.1 Lembar pengesahan**

Lembar pengesahan merupakan halaman awal dari tiap prosedur. Lembar ini digunakan untuk menjelaskan secara ringkas isi dokumen prosedur. Pada lembar ini ditulis judul dokumen prosedur, nomor dokumen, nomor revisi, pihak yang membuat dokumen, dan pihak yang memberi pengesahan dokumen. Contoh lembar pengesahan dapat dilihat di Lampiran 3, bagian Prosedur Identifikasi Insiden pada halaman awal.

#### **4.8.3.2 Tujuan**

Bagian ini berisikan tujuan yang akan dicapai oleh aktifitas. Rangkuman tujuan dari tiap aktifitas dapat dilihat pada tabel 5.1. Pernyataan tujuan berikut diambil dari Lampiran 3, bagian Prosedur Identifikasi Insiden pada sub bab A:

1. Kepastian bahwa setiap insiden dapat diidentifikasi sebelum menimbulkan implikasi negatif pada proses bisnis yang sedang berlangsung.
2. Kepastian bahwa kartu insiden dengan status “Belum selesai” dibuka dan didistribusikan kembali.

#### 4.8.3.3 Indikator kinerja

Bagian ini berisikan indikator kinerja untuk melaksanakan tujuan yang telah didefinisikan pada bagian sebelumnya. Rangkuman indikator kinerja dari tiap tujuan aktifitas dapat dilihat pada tabel 5.1. Pernyataan indikator kinerja berikut diambil dari Lampiran 3, bagian Prosedur Identifikasi Insiden pada sub bab B:

1. Persentase insiden yang menimbulkan implikasi negatif sebelum bisa dilaporkan.
2. Jumlah kartu insiden yang dibuka kembali setiap hari.

Tabel 4.10 Aktifitas berikut tujuan dan indikator kinerja

<b>Aktifitas</b>	<b>Tujuan</b>	<b>Indikator Kinerja</b>
1. Identifikasi insiden ( <i>incident identification</i> )	1.1 Kepastian bahwa setiap insiden dapat diidentifikasi sebelum menimbulkan implikasi negatif pada proses bisnis yang sedang berlangsung.	a) Persentase insiden yang menimbulkan implikasi negatif sebelum bisa dilaporkan.
	1.2 Kepastian bahwa kartu insiden dengan status “Belum selesai” dibuka dan didistribusikan.	a) Jumlah kartu insiden yang dibuka kembali setiap hari.
2. Pencatatan insiden ( <i>incident logging</i> )	2.1 Kepastian bahwa dilakukan pencatatan informasi dari laporan insiden yang masuk sebagai dasar pelaksanaan proses penanganan insiden.	a) Jumlah waktu yang dibutuhkan dalam mencatat informasi insiden. b) Jumlah komplain dari U dikarenakan HO tidak berada ditempat pada saat pelaporan c) Jumlah laporan yang masuk melalui telepon d) Jumlah laporan yang

<b>Aktifitas</b>	<b>Tujuan</b>	<b>Indikator Kinerja</b>
		masuk melalui email e) Jumlah laporan yang masuk di meja <i>helpdesk</i>
	2.2 Kepastian bahwa informasi dicatat secara lengkap dan sumbernya diverifikasi.	a) Persentase kartu insiden tercatat lengkap b) Persentase kartu insiden yang sumbernya terverifikasi
	2.3 Kepastian bahwa dibuatnya ringkasan insiden dan kata kunci pencarian kartu insiden.	a) Jumlah kartu insiden yang memiliki kata kunci yang tepat
3. Kategorisasi insiden ( <i>incident categorization</i> )	3.1 Kepastian ketepatan kategorisasi laporan insiden dan dilakukan dalam waktu singkat.	a) Persentase laporan insiden yang masuk dalam kategori yang benar. b) Jumlah waktu yang dibutuhkan dalam mengkategorikan laporan insiden.
4. Prioritas insiden ( <i>incident prioritization</i> )	4.1 Kepastian laporan insiden yang masuk mendapat prioritas penanganan yang tepat dan dilakukan dalam waktu singkat.	a) Persentase laporan insiden yang diberikan prioritas yang sesuai. b) Jumlah waktu yang dibutuhkan dalam membuat prioritas laporan insiden.
	4.2 Kepastian pen delegasian penanganan insiden mendapat staf yang tepat untuk menanganinya.	a) Persentase kejadian dimana staf pada level HO tidak tersedia. b) Jumlah eskalasi dari HO kepada HS yang dikarenakan ketidakmampuan staf.
5. Diagnosa awal ( <i>initial diagnosis</i> )	5.1 Kepastian mengenai tindakan diagnosa awal dilakukan pada level HO dalam waktu singkat.	a) Jumlah waktu yang dibutuhkan dalam tindakan diagnosa awal. b) Persentase kesalahan HO dalam diagnosa awal.
	5.2 Kepastian mengenai pimpinan/pejabat mendapat prioritas penanganan on-site.	a) Persentase ketersediaan staf HO untuk penanganan on-site.
	5.3 Kepastian mengenai tindakan diagnosa awal dapat memberi	a) Persentase laporan insiden yang

Aktifitas	Tujuan	Indikator Kinerja
	masukannya bagi penanganan insiden keseluruhan dan kalau dimungkinkan dapat memberi solusi atas insiden.	ditemukan solusinya dalam diagnosa awal.
6. Eskalasi insiden ( <i>incident escalation</i> )	6.1 Kepastian mengenai proses eskalasi dilakukan dalam waktu singkat untuk memenuhi SLA target waktu penanganan insiden.	a) Jumlah waktu yang dibutuhkan dalam menetapkan eskalasi insiden. b) Persentase laporan insiden yang terlambat dieskalasi.
	6.2 Kepastian mengenai eskalasi dilakukan dengan pertimbangan mendalam atas tindakan penanganan yang sudah dilakukan.	a) Persentase eskalasi melalui pertimbangan dari IM.
	6.3 Kepastian didapatkannya penanggungjawab penanganan insiden pasca eskalasi.	a) Persentase ketersediaan staf untuk menangani insiden kombinasi.
7. Investigasi dan diagnosa ( <i>investigation and diagnosis</i> )	7.1 Kepastian bahwa investigasi dilakukan menyeluruh dan mendalam untuk menemukan sumber permasalahan insiden.	a) Jumlah waktu yang dibutuhkan dalam investigasi laporan insiden. b) Persentase deskripsi insiden yang sudah lengkap sebelum investigasi dilakukan. c) Jumlah tindakan investigasi yang dilakukan hingga menemui U lagi untuk melengkapi deskripsi insiden.
	7.2 Kepastian bahwa aktifitas investigasi dan diagnosa dilakukan berdasarkan standar dan memenuhi SLA target waktu penanganan.	a) Persentase waktu yang dibutuhkan untuk melakukan aktifitas investigasi dan diagnosa.
	7.3 Kepastian bahwa solusi yang ditemukan adalah tepat untuk insiden yang dimaksud.	a) Persentase solusi yang ditemukan setelah aktifitas investigasi dan diagnosa oleh HS. b) Persentase solusi yang ditemukan setelah aktifitas investigasi



Aktifitas	Tujuan	Indikator Kinerja
		<p>dan diagnosa oleh SM.</p> <p>c) Persentase solusi yang ditemukan setelah aktifitas investigasi dan diagnosa oleh NM.</p> <p>d) Persentase solusi yang ditemukan setelah aktifitas investigasi dan diagnosa oleh MM.</p> <p>e) Persentase penanganan diberikan kepada pihak supplier.</p>
8. Resolusi ( <i>resolution and recovery</i> )	8.1 Kepastian bahwa solusi atas insiden sudah teruji dan dapat diimplementasikan.	<p>a) Persentase solusi yang diimplementasikan adalah benar solusi atas insiden tersebut.</p> <p>b) Persentase solusi yang tidak dapat diimplementasikan.</p>
9. Penutupan ( <i>incident closure</i> )	9.1 Kepastian bahwa aktifitas penutupan dilakukan.	<p>a) Persentase kartu insiden dengan status “Belum selesai” tetapi sebenarnya sudah ditemukan dan sudah diimplementasikan solusinya.</p> <p>b) Persentase penanganan insiden yang sesuai SLA target waktu penanganan.</p>
	9.2 Kepastian bahwa komplain dari U diterima.	a) Persentase komplain dari Pelapor Insiden/ <i>User</i> (U) atas solusi yang diberikan.
10. Pelaporan penanganan insiden ( <i>incident management report</i> )	<p>10.1 Kepastian sudah dilakukannya rekapitulasi harian.</p> <p>10.2 Kepastian sudah dilakukannya rekapitulasi bulanan.</p>	a) Persentase kelengkapan rekapitulasi.
	10.3 Kepastian bahwa laporan penanganan insiden dibuat sebagai bahan evaluasi tindakan penanganan di masa datang.	<p>a) Persentase kelengkapan laporan.</p> <p>b) Jumlah ketepatan waktu penyampaian laporan.</p>

<b>Aktifitas</b>	<b>Tujuan</b>	<b>Indikator Kinerja</b>
11. Evaluasi penanganan insiden ( <i>incident management evaluation</i> )	11.1 Kepastian bahwa evaluasi dilakukan secara setiap bulan untuk meningkatkan kualitas penanganan insiden.	a) Jumlah rapat evaluasi yang dilakukan selama tahun kerja. b) Jumlah survey yang dilakukan selama tahun kerja.
	11.2 Kepastian hasil evaluasi ditindaklanjuti oleh masing-masing pihak pada level penanganan insiden.	a) Persentase hasil evaluasi yang tidak ditindaklanjuti.

#### 4.8.3.4 Ruang lingkup

Bagian ini berisikan ruang lingkup atau batasan dari pelaksanaan aktifitas (*constraints*). Rangkuman ruang lingkup dari tiap aktifitas dapat dilihat pada tabel 5.2. Pernyataan ruang lingkup berikut diambil dari Lampiran 3, bagian Prosedur Identifikasi Insiden pada sub bab C:

1. Deteksi insiden melalui inspeksi berkala,
2. Deteksi insiden oleh pengguna,
3. Pelaporan insiden, dan
4. Membuka kartu insiden.

Tabel 4.11 Aktifitas dan ruang lingkup pelaksanaan

<b>Aktifitas</b>	<b>Ruang lingkup</b>
1. Identifikasi insiden ( <i>incident identification</i> )	1) Deteksi insiden melalui inspeksi berkala, 2) Deteksi insiden oleh pengguna, 3) Pelaporan insiden, dan 4) Membuka kartu insiden.
2. Pencatatan insiden ( <i>incident logging</i> )	1) Mencatat deskripsi insiden, 2) Verifikasi sumber informasi insiden, dan 3) Menyimpan informasi insiden.
3. Kategorisasi insiden ( <i>incident categorization</i> )	1) Kategorisasi insiden, dan 2) Mengupdate kartu insiden.
4. Prioritas insiden ( <i>incident prioritization</i> )	1) Penentuan implikasi insiden, 2) Penentuan kepentingan insiden, 3) Penentuan prioritas insiden, 4) Pendelegasian tugas penanganan, dan 5) Mengupdate kartu insiden.
5. Diagnosa awal ( <i>initial diagnosis</i> )	1) Diagnosa SLA target waktu penanganan insiden,

Aktifitas	Ruang lingkup
	2) Penanganan on-site untuk prioritas pimpinan/pejabat, 3) Pemeriksaan insiden terkait konfigurasi, 4) Pencarian solusi pada database insiden, dan 5) Mengupdate kartu insiden.
6. Eskalasi insiden ( <i>incident escalation</i> )	1) Analisa kebutuhan eskalasi, 2) Memilih penanggungjawab penanganan insiden, dan 3) Mengupdate kartu insiden.
7. Investigasi dan diagnosa ( <i>investigation and diagnosis</i> )	1) Riview kartu insiden, 2) Investigasi dan diagnosa oleh HS, 3) Investigasi dan diagnosa oleh SM, 4) Investigasi dan diagnosa oleh NM, 5) Investigasi dan diagnosa oleh MM, dan 6) Mengupdate kartu insiden.
8. Resolusi ( <i>resolution and recovery</i> )	1) Menguji solusi, 2) Mengimplementasikan solusi, dan 3) Mengupdate kartu insiden.
9. Penutupan ( <i>incident closure</i> )	1) Survey kepuasan U, dan 2) Mengupdate kartu insiden.
10. Pelaporan penanganan insiden ( <i>incident management report</i> )	1) Rekapitulasi harian, 2) Rekapitulasi bulanan, dan 3) Membuat laporan bulanan.
11. Evaluasi penanganan insiden ( <i>incident management evaluation</i> )	1) Rapat bulanan evaluasi penanganan insiden, 2) Survey kepuasan U, dan 3) Membuat laporan evaluasi.

#### 4.8.3.5 Rincian prosedur

Bagian ini berisikan detail langkah-langkah pelaksanaan prosedur. Jumlah rincian prosedur terkait erat dengan ruang lingkup yang didefinisikan sebelumnya. Rincian prosedur disusun sejelas-jelasnya dan menyebutkan semua pihak yang terlibat dalam pelaksanaan prosedur, dan bagaimana seharusnya prosedur dijalankan.

Contoh rincian prosedur dapat dilihat di Lampiran 3, bagian Prosedur Identifikasi Insiden pada sub bab D.

#### 4.8.3.6 Formulir dan dokumen

Bagian ini berisikan seluruh formulir dan dokumen yang dibutuhkan untuk pelaksanaan prosedur. Rangkuman ruang lingkup dari

tiap aktifitas dapat dilihat pada tabel 4.9. Pernyataan formulir dan dokumen berikut diambil dari Lampiran 3, bagian Prosedur Identifikasi Insiden pada sub bab E:

1. Jadwal inspeksi berkala [JD001]
2. Surat tugas inspeksi berkala [ST001]
3. Database konfigurasi [DB001]
4. Database SLA kinerja perangkat TI [DB002]
5. Database laporan inspeksi [DB003]
6. Formulir laporan inspeksi staf teknis [FL001]

#### 4.8.3.7 Diagram RACI

Bagian ini berisikan diagram RACI sebagai rangkuman dari masing-masing ruang lingkup pelaksanaan aktifitas berikut pelaksanaannya. Pernyataan diagram RACI berikut diambil dari Lampiran 3, bagian Prosedur Identifikasi Insiden pada sub bab F:

No.	Langkah	U	HO	HS	IM	SM	NM	MM
1.	Deteksi insiden melalui inspeksi berkala		R		A			
2.	Deteksi insiden oleh pengguna	AR						
3.	Pelaporan insiden	AR	R					
4.	Membuka kartu insiden		AR	I		I	I	I

#### 4.8.3.8 Istilah dan singkatan

Bagian ini berisikan istilah dan singkatan yang digunakan dalam prosedur. Contoh istilah dan singkatan dapat dilihat di Lampiran 3, bagian Prosedur Identifikasi Insiden pada sub bab G.

#### 4.8.3.9 Catatan perubahan

Bagian ini berisikan catatan-catatan perubahan yang dibuat terkait dengan dokumen prosedur. Contoh catatan perubahan dapat dilihat di Lampiran 3, bagian Prosedur Identifikasi Insiden pada sub bab H.

#### **4.8.4 Diagram**

Bagian ini berisi tabel diagram RACI yang terdiri dari langkah dalam aktifitas-aktifitas prosedur, dan masing-masing jenis status yang melekat pada pihak yang terlibat dalam pelaksanaan prosedur tersebut. Selain itu bagian ini juga berisi diagram alir masing-masing aktifitas sebagai panduan pelaksanaan aktifitas. Tabel diagram RACI dan diagram alir aktifitas dapat dilihat pada buku kedua dari tesis ini, bagian Diagram.

#### **4.8.5 Dokumen dan Formulir**

Bagian ini berisi dokumen formulir yang dikembangkan sebagai pendukung dari pelaksanaan aktifitas program. Pada bagian ini jenis dokumen dan formulir yang digunakan dalam pelaksanaan prosedur adalah formulir, database, dokumen kebijakan, dan dokumen pelaksanaan proses TI yang lain. Dokumen formulir dapat dilihat pada buku kedua dari tesis ini, bagian Dokumen dan Formulir.

#### **4.8.6 Matriks Tata Laksana**

Bagian ini berisi matriks tata laksana sebagai kesimpulan dari keseluruhan dokumen program. Matriks tata laksana disusun dalam bentuk tabel 7 (tujuh) kolom yang terdiri dari:

1. Kolom pertama berisi nomor prosedur aktifitas.
2. Kolom kedua berisi nama aktifitas dan tujuannya.
3. Kolom ketiga berisi indikator kinerja dari tujuan tiap aktifitas.
4. Kolom keempat berisi rincian prosedur yang dirangkum dalam ruang lingkup/batasan pelaksanaan aktifitas.
5. Kolom kelima berisi fungsi masing-masing pihak pelaksana aktifitas yang disusun menggunakan format diagram RACI.
6. Kolom keenam berisi waktu pelaksanaan rincian prosedur dalam format waktu minggu.
7. Kolom ketujuh berisi dokumen pendukung prosedur.

Matriks tata laksana dokumen program dapat dilihat pada buku kedua dari tesis ini, bagian Matriks Tata Laksana.

#### **4.9 Verifikasi Dokumen Tata Laksana**

Proses verifikasi dilakukan dengan memberikan draft dokumen program kepada pihak dalam manajemen biro TI untuk dilakukan review dan meminta masukan atas dokumen tersebut. Rangkaian proses review dilakukan sebanyak 5 (lima) kali hingga semua masukan dari pihak manajemen tercakup. Manajemen Biro TI BPK-RI dalam hal ini diwakili oleh Kasubag Dukungan TI BPK-RI.

Dalam melakukan review aktifitas-aktifitas dalam dokumen program, pihak manajemen menggunakan pembandingan *framework* ITIL dan dokumen pelaksanaan yang mereka gunakan selama ini.

#### **4.10 Validasi Dokumen Tata Laksana**

Validasi dokumen tata laksana dilakukan setelah proses verifikasi dirasa sudah cukup memenuhi semua kebutuhan dari *framework* ITIL dan masukan dari manajemen. Validasi diberikan dalam bentuk surat penerimaan (*acceptance letter*) oleh pihak manajemen. Surat penerimaan (*acceptance letter*) dapat dilihat pada Lampiran 2.

Untuk implementasi lebih lanjut pada lingkungan kantor, validasi dokumen akan dilakukan dengan mengesahkan dokumen program menjadi dokumen resmi oleh kantor. Proses validasi disini berarti melengkapi dokumen kontrol dengan SK Sekretaris Jenderal. Surat Keputusan ini akan berisi tanggal pengesahan, pihak yang mengesahkan yang dalam hal ini Sekretaris Jenderal, dan nomor dokumen yang resmi.

#### **4.11 Penomoran Dokumen Tata Laksana**

Dokumen tata laksana ini disusun untuk melaksanakan proses manajemen insiden dari program manajemen *helpdesk* dan dukungan TI dimana program ini merupakan bagian dari insiatif strategis pendukung pada kelompok proses.

Untuk itu penomoran umum dokumen diberikan sebagai **ISP-H7-MI**, dimana **ISP** merujuk pada kode inisiatif strategis yaitu Inisiatif Strategis Pendukung, **H7** merujuk pada kode urutan program yaitu program ke-7, dan **MI** merujuk pada kode proses TI yaitu proses Manajemen Insiden.

Sedangkan untuk penomoran tiap-tiap bagian dalam dokumen tata laksana dilakukan sebagai **MI-RXX-Y**, dimana **MI** merujuk pada kode proses TI Manajemen

Insiden, **R** adalah singkatan dari rilis, **XX** adalah 2 (dua) digit angka rilis, dan **Y** adalah kode yang merujuk tiap bagian dalam dokumen tata laksana (prosedur, diagram, dokumen/formulir atau matriks tata laksana).

Sebagai contoh **ISP-H7-MI-R06-P06** merujuk pada bagian prosedur keenam yaitu aktifitas Eskalasi Insiden.

--- Halaman ini dikosongkan ---



## **BAB 5**

### **Kesimpulan dan Saran**

#### **5.1 Kesimpulan**

Kesimpulan yang dihasilkan berdasarkan penelitian yang telah dikerjakan adalah sebagai berikut:

1. Dokumen tata laksana dikembangkan untuk sebagian proses TI yang dilaksanakan oleh program manajemen helpdesk dan dukungan TI, yaitu proses manajemen insiden. Dokumen tata laksana ini berisi 11 (sebelas) prosedur untuk 9 (sembilan) aktifitas yang dikembangkan berdasarkan proses manajemen insiden dari *framework* ITIL v3 dan 2 (dua) aktifitas tambahan sebagai kebutuhan dari organisasi yaitu aktifitas pelaporan dan evaluasi. Selain itu dokumen tata laksana juga memiliki formulir dan dokumen pendukung prosedur serta matriks tata laksana.
2. Pelaksana program dibagi menjadi 7 (tujuh) pihak yaitu Pelapor Insiden (U), *Helpdesk Operator* (HO), *Helpdesk Specialist* (HS), *Incident Manager* (IM), *Software Manager* (SM), *Network Manager* (NM), dan *Maintenance Manager* (MM). Masing-masing pihak pelaksana terhubung dengan jabatan struktural pada biro TI BPK-RI.
3. Diagram RACI disusun untuk menunjukkan tugas dan tanggungjawab masing-masing pihak tersebut diatas dalam tiap langkah aktifitas. Sementara diagram alir disusun untuk menunjukkan aliran aktifitas yang dilakukan dalam prosedur berikut masing-masing pelaksananya.
4. Aktifitas-aktifitas yang dikembangkan dari *framework* ITIL, pelaksanaannya dilakukan secara kontinu dan terus menerus. Sementara aktifitas pelaporan dan evaluasi dilaksanakan pada awal dan akhir bulan saja.
5. Matriks tata laksana dibangun untuk menjadi kesimpulan keseluruhan proses program. Matriks berisikan masing-masing aktifitas dalam program berikut dengan tujuan, indikator kinerja, formulir dan dokumen yang diperlukan untuk pelaksanaan aktifitas, dan diagram RACI.

## 5.2 Saran

Dokumen tata laksana yang dihasilkan belum mencakup keseluruhan program manajemen *helpdesk* dan dukungan TI. Dokumen tata laksana yang dibuat baru berisikan proses TI manajemen insiden. Agar tujuan dari program dapat tercapai seluruhnya, diharapkan agar manajemen juga mengembangkan sebuah dokumen tata laksana bagi proses TI manajemen *helpdesk*.

Untuk lebih mengoptimalkan pelaksanaan dokumen program, perlu dikembangkan sebuah aplikasi pendukung agar pelaksanaan program manajemen *helpdesk* dan dukungan TI bisa lebih otomatis.

Selain itu untuk mencapai tujuan program kerja yang lain yang menjadi tanggungjawab sub bagian Dukungan TI, diperlukan sebuah penelitian mendalam oleh biro TI BPK-RI untuk mengembangkan dokumen tata laksana masing-masing program.

## LAMPIRAN 1

### Brainstorming Pembuatan Dokumen Tata Laksana

Proses brainstorming dilakukan menggunakan metode dari Phil Barte, PhD. Metode tersebut dapat dilihat pada website <http://www.scn.org/cmp/modules/mnt-4.htm>. Proses brainstorming bertujuan untuk menjawab 4 (empat) pertanyaan, yaitu:

1. Apa yang kita inginkan?
2. Apa yang kita punya saat ini?
3. Bagaimana kita menggunakan yang dimiliki untuk menghasilkan mendapatkan yang kita inginkan?
4. Apa yang akan terjadi ketika kita mendapatkan yang kita inginkan?

Untuk menjawab pertanyaan-pertanyaan tersebut, dilakukan prosedur sebagai berikut:

1. Menetapkan masalah
2. Menetapkan goal
3. Menetapkan tujuan
4. Menetapkan sumber daya dan ruang lingkup
5. Menetapkan strategi
6. Meringkas kelima hal diatas

#### **Menetapkan masalah (*problem*)**

Pada langkah awal ditetapkan permasalahan yang akan dikerjakan dalam penelitian ini adalah pembuatan tata laksana manajemen insiden menggunakan *framework* ITIL v3. Pokok permasalahan ini kemudian dihubungkan dengan sebuah program yang sepenuhnya dilaksanakan oleh subag Dukungan TI, yaitu program Manajemen Helpdesk dan Dukungan TI.

Menurut Panduan Dukungan TI [BPI07] ada 3 (tiga) tujuan utama dari program ini, salah satunya adalah mengembalikan proses kepada kondisi normal dengan cepat

dan tepat segera setelah terjadi insiden. Pada tujuan inilah terdapat keterkaitan antara program manajemen helpdesk dan dukungan TI dengan proses TI Manajemen insiden.

Catatan pengerjaan:

Tahap ini dilakukan pada Februari 2010.

### Menetapkan goal (*purposes*)

IT Goal untuk permasalahan diatas ditetapkan diambil dari *framework* COBIT 4.1. Hal ini didasarkan pada pemetaan proses TI Manajemen Insiden dari *framework* ITIL v3 kepada *framework* COBIT 4.1 didapatkan bahwa proses TI Manajemen Insiden terkait erat dengan proses DS 8 yaitu *Manage Service Desk and Incidents*. Tabel berikut menampilkan pemetaan proses TI Manajemen Insiden dari *framework* ITIL v3 kepada proses DS 8 *framework* COBIT 4.1.

<b>Aktifitas dalam Manajemen Insiden ITIL</b>	<b>Proses COBIT</b>	<b>Control Objective COBIT</b>	<b>Keterangan</b>
Identifikasi insiden ( <i>Incident Identification</i> )	DS 8	DS 8.2	<i>Registration of customer service</i>
Pencatatan insiden ( <i>Incident Logging</i> )	DS 8	DS 8.2	<i>Registration of customer service</i>
Kategorisasi insiden ( <i>Incident Categorization</i> )	DS 8	DS 8.2	<i>Registration of customer service</i>
Prioritas insiden ( <i>Incident Priorization</i> )	DS 8	DS 8.2	<i>Registration of customer service</i>
Diagnosa awal ( <i>Initial Diagnosis</i> )	DS 8	DS 8.2	<i>Registration of customer service</i>
Eskalasi insiden ( <i>Incident Escalation</i> )	DS 8	DS 8.3	<i>Incident Escalation</i>
Investigasi dan Diagnosa ( <i>Investigation and Diagnosis</i> )	DS 8	DS 8.3	<i>Incident Escalation</i>
Resolusi ( <i>Resolution and Recovery</i> )	DS 8	DS 8.3	<i>Incident Escalation</i>
Penutupan ( <i>Incident Closure</i> )	DS 8	DS 8.4	<i>Incident Closure</i>

Kemudian dengan menggunakan dokumen *framework* COBIT 4.1 didapatkan IT Goal yang terkait dengan proses DS8 tersebut adalah:

1. *Ensure satisfaction of end users with service offerings and service levels.*
2. *Ensure proper use and performance of the applications and technology solutions.*
3. *Make sure that IT services are available as required.*

Catatan pengerjaan:

Tahap ini dilakukan pada Maret 2010.

### **Menetapkan tujuan (*objectives*)**

Sebelum menetapkan tujuan, terlebih dahulu dilakukan penetapan aktifitas yang akan dilakukan dalam proses manajemen insiden. Aktifitas-aktifitas ditetapkan sebanyak 11 (sebelas) aktifitas yang terdiri dari 9 (sembilan) aktifitas yang telah disebutkan diatas, ditambah 2 (dua) aktifitas baru untuk pelaporan dan evaluasi kinerja manajemen. Tambahan 2 (dua) aktifitas diluar proses manajemen insiden *framework* ITIL v3, dilakukan atas permintaan manajemen biro TI.

Rincian aktifitas tersebut adalah sebagai berikut:

1. Identifikasi insiden (*Incident Identification*)
2. Pencatatan insiden (*Incident Logging*)
3. Kategorisasi insiden (*Incident Categorization*)
4. Prioritas insiden (*Incident Priorization*)
5. Diagnosa awal (*Initial Diagnosis*)
6. Eskalasi insiden (*Incident Escalation*)
7. Investigasi dan Diagnosa (*Investigation and Diagnosis*)
8. Resolusi (*Resolution and Recovery*)
9. Penutupan (*Incident Closure*)
10. Pelaporan penanganan insiden (*Incident Management Report*)

## 11. Evaluasi penanganan insiden (*Incident Management Evaluation*)

Setelah menetapkan aktifitas, langkah selanjutnya adalah menetapkan tujuan dari masing-masing aktifitas tersebut. Penetapan tujuan dilakukan dengan memperhatikan penjabaran manajemen insiden (*incident management*) dalam dokumen *framework* ITIL v3, secara khusus dalam buku *Service Operation*. Untuk penetapan tujuan dari aktifitas pelaporan dan evaluasi, dilakukan dengan brainstorming bersama dengan manajemen biro TI BPK-RI khususnya dengan Kasubag Dukungan TI.

Berikut adalah tujuan masing-masing aktifitas tersebut.

<b>Aktifitas</b>	<b>Tujuan</b>
1. Identifikasi insiden ( <i>incident identification</i> )	a) Kepastian bahwa setiap insiden dapat diidentifikasi sebelum menimbulkan implikasi negatif pada proses bisnis yang sedang berlangsung.
	b) Kepastian bahwa kartu insiden dengan status “Belum selesai” dibuka dan didistribusikan.
2. Pencatatan insiden ( <i>incident logging</i> )	a) Kepastian bahwa dilakukan pencatatan informasi dari laporan insiden yang masuk sebagai dasar pelaksanaan proses penanganan insiden.
	b) Kepastian bahwa informasi dicatat secara lengkap dan sumbernya diverifikasi.
	c) Kepastian bahwa dibuatnya ringkasan insiden dan kata kunci pencarian kartu insiden.
3. Kategorisasi insiden ( <i>incident categorization</i> )	a) Kepastian ketepatan kategorisasi laporan insiden dan dilakukan dalam waktu singkat.
4. Prioritas insiden ( <i>incident prioritization</i> )	a) Kepastian laporan insiden yang masuk mendapat prioritas penanganan yang tepat dan dilakukan dalam waktu singkat.
	b) Kepastian pendelegasian penanganan insiden mendapat staf yang tepat untuk menanganinya.
5. Diagnosa awal ( <i>initial diagnosis</i> )	a) Kepastian mengenai tindakan diagnosa awal dilakukan pada level HO dalam waktu singkat.
	b) Kepastian mengenai pimpinan/pejabat mendapat prioritas penanganan on-site.

Aktifitas	Tujuan
	c) Kepastian mengenai tindakan diagnosa awal dapat memberi masukan bagi penanganan insiden keseluruhan dan kalau dimungkinkan dapat memberi solusi atas insiden.
6. Eskalasi insiden ( <i>incident escalation</i> )	a) Kepastian mengenai proses eskalasi dilakukan dalam waktu singkat untuk memenuhi SLA target waktu penanganan insiden.
	b) Kepastian mengenai eskalasi dilakukan dengan pertimbangan mendalam atas tindakan penanganan yang sudah dilakukan.
	c) Kepastian didapatkannya penanggungjawab penanganan insiden pasca eskalasi.
7. Investigasi dan diagnosa ( <i>investigation and diagnosis</i> )	a) Kepastian bahwa investigasi dilakukan menyeluruh dan mendalam untuk menemukan sumber permasalahan insiden.
	b) Kepastian bahwa aktifitas investigasi dan diagnosa dilakukan berdasarkan standar dan memenuhi SLA target waktu penanganan.
	c) Kepastian bahwa solusi yang ditemukan adalah tepat untuk insiden yang dimaksud.
8. Resolusi ( <i>resolution and recovery</i> )	a) Kepastian bahwa solusi atas insiden sudah teruji dan dapat diimplementasikan.
9. Penutupan ( <i>incident closure</i> )	a) Kepastian bahwa aktifitas penutupan dilakukan.
	b) Kepastian bahwa komplain dari U diterima.
10. Pelaporan penanganan insiden ( <i>incident management report</i> )	a) Kepastian sudah dilakukannya rekapitulasi harian. b) Kepastian sudah dilakukannya rekapitulasi bulanan.
	c) Kepastian bahwa laporan penanganan insiden dibuat sebagai bahan evaluasi tindakan penanganan di masa datang.
11. Evaluasi penanganan insiden ( <i>incident</i>	a) Kepastian bahwa evaluasi dilakukan secara setiap bulan untuk meningkatkan kualitas penanganan insiden.

<b>Aktifitas</b>	<b>Tujuan</b>
<i>management evaluation)</i>	
	b) Kepastian hasil evaluasi ditindaklanjuti oleh masing-masing pihak pada level penanganan insiden.

Catatan pengerjaan:

Tahap ini dilakukan pada Maret 2010.

### **Menetapkan sumber daya dan batasan (*resources and constraints*)**

Setelah menetapkan aktifitas dan tujuannya, langkah berikutnya adalah menetapkan sumber daya dan batasan pelaksanaan/ruang lingkup aktifitas. Pada tahap ini yang ditetapkan adalah pihak-pihak yang akan terlibat dalam aktifitas, waktu pelaksanaan aktifitas, dan batasan pelaksanaan/ruang lingkup aktifitas.

Penentuan pihak-pihak yang akan terlibat dalam aktifitas didasarkan pada dokumen Kebijakan Dukungan TI [BKI07] yang disusun oleh biro TI. Pihak-pihak tersebut adalah:

1. Pelapor Insiden/*User* yang diberi inisial U.
2. *Helpdesk Operator* yang diberi inisial HO.
3. *Helpdesk Specialist* yang diberi inisial HS.
4. *Incident Manager* yang diberi inisial IM.
5. *Software Manager* yang diberi inisial SM.
6. *Network Manager* yang diberi inisial NM.
7. *Maintenance Manager* yang diberi inisial MM.

Setelah menentukan semua pihak yang akan terlibat dalam pelaksanaan proses manajemen insiden, selanjutnya adalah menentukan keterlibatannya dalam masing-masing aktifitas. Tabel berikut berisi hubungan antara pelaksana dengan masing-masing aktifitas.

<b>Aktifitas</b>	<b>Pelaksana</b>
1. Identifikasi insiden ( <i>incident identification</i> )	<ul style="list-style-type: none"> <li>• Pelapor Insiden/<i>User</i> (U)</li> <li>• Helpdesk Operator (HO)</li> <li>• Incident Manager (IM)</li> </ul>



<b>Aktifitas</b>	<b>Pelaksana</b>
2. Pencatatan insiden ( <i>incident logging</i> )	<ul style="list-style-type: none"> <li>• Pelapor Insiden/User (U)</li> <li>• Helpdesk Operator (HO)</li> </ul>
3. Kategorisasi insiden ( <i>incident categorization</i> )	<ul style="list-style-type: none"> <li>• Helpdesk Operator (HO)</li> <li>• Incident Manager (IM)</li> </ul>
4. Prioritas insiden ( <i>incident prioritization</i> )	<ul style="list-style-type: none"> <li>• Helpdesk Operator (HO)</li> <li>• Incident Manager (IM)</li> </ul>
5. Diagnosa awal ( <i>initial diagnosis</i> )	<ul style="list-style-type: none"> <li>• Helpdesk Operator (HO)</li> <li>• Incident Manager (IM)</li> </ul>
6. Eskalasi insiden ( <i>incident escalation</i> )	<ul style="list-style-type: none"> <li>• Helpdesk Operator (HO)</li> <li>• Helpdesk Spesialist (HS)</li> <li>• Incident Manager (IM)</li> <li>• Software Manager (SM)</li> <li>• Network Manager (NM)</li> <li>• Maintenance Manager (MM)</li> </ul>
7. Investigasi dan diagnosa ( <i>investigation and diagnosis</i> )	<ul style="list-style-type: none"> <li>• Pelapor Insiden/User (U)</li> <li>• Helpdesk Operator (HO)</li> <li>• Helpdesk Spesialist (HS)</li> <li>• Software Manager (SM)</li> <li>• Network Manager (NM)</li> <li>• Maintenance Manager (MM)</li> </ul>
8. Resolusi ( <i>resolution and recovery</i> )	<ul style="list-style-type: none"> <li>• Pelapor Insiden/User (U)</li> <li>• Helpdesk Operator (HO)</li> <li>• Helpdesk Spesialist (HS)</li> <li>• Incident Manager (IM)</li> <li>• Software Manager (SM)</li> <li>• Network Manager (NM)</li> <li>• Maintenance Manager (MM)</li> </ul>
9. Penutupan ( <i>incident closure</i> )	<ul style="list-style-type: none"> <li>• Pelapor Insiden/User (U)</li> <li>• Helpdesk Operator (HO)</li> <li>• Incident Manager (IM)</li> </ul>
10. Pelaporan penanganan insiden ( <i>incident</i>	<ul style="list-style-type: none"> <li>• Helpdesk Operator (HO)</li> </ul>

Aktifitas	Pelaksana
<i>management report</i> )	<ul style="list-style-type: none"> <li>• Incident Manager (IM)</li> </ul>
11. Evaluasi penanganan insiden ( <i>incident management evaluation</i> )	<ul style="list-style-type: none"> <li>• Pelapor Insiden/User (U)</li> <li>• Helpdesk Operator (HO)</li> <li>• Helpdesk Specialist (HS)</li> <li>• Incident Manager (IM)</li> <li>• Software Manager (SM)</li> <li>• Network Manager (NM)</li> <li>• Maintenance Manager (MM)</li> </ul>

Waktu pelaksanaan masing-masing aktifitas ditetapkan dalam format minggu. Hal ini dikarenakan menurut dokumen *framework* ITIL, pelaksanaan aktifitas-aktifitas tersebut saling terkait satu sama lain. Keseluruhan proses manajemen insiden diawali oleh aktifitas identifikasi insiden dan aktifitas selanjutnya dilaksanakan menurut urutan yang ditetapkan. Khusus untuk aktifitas pelaporan ditetapkan dilaksanakan pada akhir bulan, sementara untuk aktifitas evaluasi ditetapkan dilaksanakan pada awal bulan.

Alasan penetapan waktu pelaksanaan aktifitas pelaporan pada akhir bulan adalah untuk merangkum keseluruhan pelaksanaan proses manajemen insiden pada bulan tersebut. Sementara alasan penetapan waktu pelaksanaan aktifitas evaluasi pada awal bulan adalah untuk mengevaluasi pelaksanaan proses manajemen insiden pada bulan sebelumnya sebagai acuan pelaksanaan pada bulan selanjutnya. Rincian waktu pelaksanaan masing-masing aktifitas dapat dilihat pada bagian matriks tata laksana dari dokumen.

Batasan pelaksanaan/ruang lingkup aktifitas ditetapkan dengan melihat tujuan masing-masing aktifitas yang telah ditetapkan sebelumnya. Penentuan batasan pelaksanaan/ruang lingkup dilakukan terhadap masing-masing tujuan dalam aktifitas. Beberapa tujuan memiliki lebih dari 1 (satu) batasan pelaksanaan/ruang lingkup, sementara yang lain hanya memiliki 1 (satu) batasan pelaksanaan/ruang lingkup. Tetapi dimungkinkan juga 2 (dua) buah tujuan memiliki batasan pelaksanaan/ruang lingkup yang sama.

Tabel berikut berisi tujuan aktifitas berikut batasan pelaksanaan/ruang lingkungannya.

<b>Aktifitas</b>	<b>Tujuan</b>	<b>Ruang Lingkup</b>
1. Identifikasi insiden ( <i>incident identification</i> )	a) Kepastian bahwa setiap insiden dapat diidentifikasi sebelum menimbulkan implikasi negatif pada proses bisnis yang sedang berlangsung.	1) Deteksi insiden melalui inspeksi berkala, 2) Deteksi insiden oleh pengguna, 3) Pelaporan insiden, dan
	b) Kepastian bahwa kartu insiden dengan status “Belum selesai” dibuka dan didistribusikan.	4) Membuka kartu insiden.
2. Pencatatan insiden ( <i>incident logging</i> )	a) Kepastian bahwa dilakukan pencatatan informasi dari laporan insiden yang masuk sebagai dasar pelaksanaan proses penanganan insiden.	1) Mencatat deskripsi insiden,
	b) Kepastian bahwa informasi dicatat secara lengkap dan sumbernya diverifikasi.	2) Verifikasi sumber informasi insiden, dan
	c) Kepastian bahwa dibuatnya ringkasan insiden dan kata kunci pencarian kartu insiden.	3) Menyimpan informasi insiden.
3. Kategorisasi insiden ( <i>incident categorization</i> )	a) Kepastian ketepatan kategorisasi laporan insiden dan dilakukan dalam waktu singkat.	1) Kategorisasi insiden, dan 2) Mengupdate kartu insiden.
4. Prioritas insiden ( <i>incident prioritization</i> )	a) Kepastian laporan insiden yang masuk mendapat prioritas penanganan yang tepat dan dilakukan dalam waktu singkat.	1) Penentuan implikasi insiden, 2) Penentuan kepentingan insiden,

Aktifitas	Tujuan	Ruang Lingkup
		3) Penentuan prioritas insiden,
	b) Kepastian pendelegasian penanganan insiden mendapat staf yang tepat untuk menanganinya.	4) Pendelegasian tugas penanganan, dan 5) Mengupdate kartu insiden.
5. Diagnosa awal ( <i>initial diagnosis</i> )	a) Kepastian mengenai tindakan diagnosa awal dilakukan pada level HO dalam waktu singkat.	1) Diagnosa SLA target waktu penanganan insiden,
	b) Kepastian mengenai pimpinan/pejabat mendapat prioritas penanganan on-site.	2) Penanganan on-site untuk prioritas pimpinan/pejabat,
	c) Kepastian mengenai tindakan diagnosa awal dapat memberi masukan bagi penanganan insiden keseluruhan dan kalau dimungkinkan dapat memberi solusi atas insiden.	3) Pemeriksaan insiden terkait konfigurasi, 4) Pencarian solusi pada database insiden, dan 5) Mengupdate kartu insiden.
6. Eskalasi insiden ( <i>incident escalation</i> )	a) Kepastian mengenai proses eskalasi dilakukan dalam waktu singkat untuk memenuhi SLA target waktu penanganan insiden.	1) Analisa kebutuhan eskalasi,
	b) Kepastian mengenai eskalasi dilakukan dengan pertimbangan mendalam atas tindakan penanganan yang sudah dilakukan.	
	c) Kepastian didapatkannya penanggungjawab penanganan	2) Memilih penanggungjawab

Aktifitas	Tujuan	Ruang Lingkup
	insiden pasca eskalasi.	penanganan insiden, dan 3) Mengupdate kartu insiden.
7. Investigasi dan diagnosa ( <i>investigation and diagnosis</i> )	a) Kepastian bahwa investigasi dilakukan menyeluruh dan mendalam untuk menemukan sumber permasalahan insiden.	1) Riview kartu insiden,
	b) Kepastian bahwa aktifitas investigasi dan diagnosa dilakukan berdasarkan standar dan memenuhi SLA target waktu penanganan.	
	c) Kepastian bahwa solusi yang ditemukan adalah tepat untuk insiden yang dimaksud.	
8. Resolusi ( <i>resolution and recovery</i> )	a) Kepastian bahwa solusi atas insiden sudah teruji dan dapat diimplementasikan.	1) Menguji solusi, 2) Mengimplementasikan solusi, dan 3) Mengupdate kartu insiden.
9. Penutupan ( <i>incident closure</i> )	a) Kepastian bahwa aktifitas penutupan dilakukan.	1) Survey kepuasan U, dan

<b>Aktifitas</b>	<b>Tujuan</b>	<b>Ruang Lingkup</b>
	b) Kepastian bahwa komplain dari U diterima.	2) Mengupdate kartu insiden.
10. Pelaporan penanganan insiden ( <i>incident management report</i> )	a) Kepastian sudah dilakukannya rekapitulasi harian.	1) Rekapitulasi harian,
	b) Kepastian sudah dilakukannya rekapitulasi bulanan.	2) Rekapitulasi bulanan, dan
	c) Kepastian bahwa laporan penanganan insiden dibuat sebagai bahan evaluasi tindakan penanganan di masa datang.	3) Membuat laporan bulanan.
11. Evaluasi penanganan insiden ( <i>incident management evaluation</i> )	a) Kepastian bahwa evaluasi dilakukan secara setiap bulan untuk meningkatkan kualitas penanganan insiden.	1) Rapat bulanan evaluasi penanganan insiden, 2) Survey kepuasan U, dan
	b) Kepastian hasil evaluasi ditindaklanjuti oleh masing-masing pihak pada level penanganan insiden.	3) Membuat laporan evaluasi.

Catatan pengerjaan:

Tahap ini dilakukan pada April 2010.

### **Menetapkan strategi (*strategy*)**

Langkah penetapan strategi dilakukan dengan cara merinci pelaksanaan masing-masing aktifitas. Dalam rincian pelaksanaan digabungkan juga hasil brainstorming mengenai sumber daya dan batasan pelaksanaan/ruang lingkup yang telah disebutkan diatas. Selain itu dalam langkah ini juga ditetapkan indikator kinerja pelaksanaan dari

masing-masing tujuan. Dalam merinci pelaksanaan masing-masing aktifitas, ditentukan juga dokumen dan formulir yang dibutuhkan dalam pelaksanaan aktifitas.

Berikut adalah rincian prosedur-prosedur tersebut:

- Identifikasi insiden (*incident identification*)
- Pencatatan insiden (*incident logging*)
- Kategorisasi insiden (*incident categorization*)
- Prioritas insiden (*incident prioritization*)
- Diagnosa awal (*initial diagnosis*)
- Eskalasi insiden (*incident escalation*)
- Investigasi dan diagnosa (*investigation and diagnosis*)
- Resolusi (*resolution and recovery*)
- Penutupan (*incident closure*)
- Pelaporan penanganan insiden (*incident management report*)
- Evaluasi penanganan insiden (*incident management evaluation*)

Masing-masing dokumen prosedur disusun dengan urutan lembar pengesahan, tujuan, indikator kinerja, ruang lingkup, rincian prosedur, formulir dan dokumen, diagram RACI, istilah dan singkatan, dan catatan perubahan.

Perancangan dokumen prosedur dalam tahap ini diawali dengan proses brainstorming oleh penulis. Kemudian dalam langkah selanjutnya dilakukan review oleh manajemen biro TI dalam hal ini kasubag Dukungan TI. Proses review oleh manajemen biro TI dilakukan sebanyak 5 (lima) kali dan dalam masing-masing proses pihak manajemen memberikan masukan mengenai dokumen tata laksana yang disusun. Pada akhir proses review, manajemen biro TI memberikan *acceptance letter* sebagai langkah validasi dokumen tata laksana.

Penjabaran prosedur dapat dilihat pada Lampiran 3, bagian Prosedur Identifikasi Insiden hingga Prosedur Evaluasi Penanganan Insiden, bagian Formulir dan Dokumen, dan bagian Diagram yang berisi diagram RACI dan diagram alir prosedur.

Catatan pengerjaan:

Tahap ini dilakukan pada April – Mei 2010.

### **Meringkas kelima hal diatas (*summarize*)**

Langkah terakhir dalam proses brainstorming adalah meringkas semua kegiatan diatas dalam bentuk matriks tata laksana. Matriks tata laksana disusun menggunakan 7 (tujuh) kolom yaitu kolom nomor, kolom aktifitas dan masing-masing tujuannya, kolom indikator kinerja untuk masing-masing tujuan aktifitas, kolom batasan pelaksanaan/ruang lingkup pelaksanaan aktifitas, kolom diagram RACI, kolom waktu pelaksanaan aktifitas, dan kolom dokumen dan formulir.

Penjabaran matriks tata laksana dapat dilihat pada Lampiran 3, bagian Matriks Tata Laksana.

Catatan pengerjaan:

Tahap ini dilakukan pada Mei 2010.



## LAMPIRAN 2

### Dokumen Kontrol Pembuatan Dokumen Tata Laksana

Dokumen prosedur manajemen insiden pada program manajemen helpdesk dan dukungan TI disusun dan diverifikasi sebanyak 5 (lima) kali dengan rincian sebagai berikut:

1. R01, adalah dokumen rilis awal ketika pertama kali disusun. Dokumen ini dikeluarkan pada tanggal 1 April 2010.
2. R02, adalah dokumen rilis kedua yang telah diberi masukan oleh manajemen biro TI, dalam hal ini Kasubag Dukungan TI BPK-RI. Masukan yang diberikan adalah pada aktifitas penutupan dan aktifitas evaluasi. Dokumen ini dikeluarkan pada tanggal 12 April 2010.
3. R03, adalah dokumen rilis ketiga yang telah diberi masukan oleh manajemen biro TI, dalam hal ini Kasubag Dukungan TI BPK-RI. Masukan yang diberikan adalah pada aktifitas pencatatan insiden. Dokumen ini dikeluarkan pada tanggal 14 Mei 2010.
4. R04, adalah dokumen rilis keempat yang telah diberi masukan oleh manajemen biro TI, dalam hal ini Kasubag Dukungan TI BPK-RI. Masukan yang diberikan adalah pada kebijakan kategorisasi insiden. Dokumen ini dikeluarkan pada tanggal 21 Mei 2010.
5. R05, adalah dokumen rilis kelima yang telah mendapat *acceptance letter* dari manajemen Biro TI BPK-RI dalam hal ini diwakili oleh Kasubag Dukungan TI BPK-RI.
6. R06, adalah dokumen rilis keenam yang telah mendapat perubahan total dalam format penulisan dokumen.

Proses verifikasi dilakukan sebanyak 5 (lima) kali oleh pihak manajemen Biro TI BPK-RI yang dalam hal ini diwakili oleh Kasubag Dukungan TI BPK-RI. Selanjutnya pada rilis dokumen yang terakhir telah divalidasi oleh manajemen dengan memberikan *acceptance letter* pada tanggal 25 Mei 2010

--- Halaman ini dikosongkan ---

### **LAMPIRAN 3**

#### **Dokumen Tata Laksana Manajemen Insiden pada Program Manajemen Helpdesk dan Dukungan TI**

--- Halaman ini dikosongkan ---



# Badan Pemeriksa Keuangan Republik Indonesia

## LEMBAR PENGESAHAN

# PROSEDUR

Judul : Identifikasi Insiden

No. Dokumen : MI-R06-P01

Revisi : 06

Jumlah Salinan :

1	2	3	4	5	6	7	8	9	10
---	---	---	---	---	---	---	---	---	----

DISUSUN OLEH	DISAHKAN OLEH
Biro Teknologi Informasi BPK-RI	Sekretaris Jenderal BPK-RI
Tanggal: 01 Juni 2010	Tanggal:



# Badan Pemeriksa Keuangan Republik Indonesia

Diterbitkan:  
1 Juni 2010

No. Revisi: 06

Halaman 2 dari 6

MI-R06-P01

Identifikasi Insiden

## PROSEDUR

### A. TUJUAN

1. Kepastian bahwa setiap insiden dapat diidentifikasi sebelum menimbulkan implikasi negatif pada proses bisnis yang sedang berlangsung.
2. Kepastian bahwa kartu insiden dengan status “Belum selesai” dibuka dan didistribusikan kembali.

### B. INDIKATOR KINERJA

1. Persentase insiden yang menimbulkan implikasi negatif sebelum bisa dilaporkan.
2. Jumlah kartu insiden yang dibuka kembali setiap hari.

### C. RUANG LINGKUP

Prosedur aktifitas I yaitu Identifikasi Insiden, meliputi:

1. Deteksi insiden melalui inspeksi berkala,
2. Deteksi insiden oleh pengguna,
3. Pelaporan insiden, dan
4. Membuka kartu insiden.

### D. RINCIAN PROSEDUR

1. Deteksi insiden melalui inspeksi berkala
  - a. IM memberikan tugas kepada HO untuk melakukan inspeksi berkala atas perangkat TI yang menjadi wewenangnya.
  - b. IM bertanggungjawab membuat jadwal inspeksi berkala [JD001] dan membuat surat tugas [ST001] untuk masing-masing staf HO yang ditugaskan untuk inspeksi berkala. Inspeksi berkala dilakukan oleh minimal 1 (satu) orang dan maksimal 3 (tiga) orang staf sub bagian Dukungan TI dalam hal ini HO.
  - c. U (staf inspeksi berkala), mendeteksi insiden dengan cara:

PROSEDUR  
Identifikasi Insiden

**SIFAT RAHASIA**

Hanya didistribusikan kepada yang berhak mengetahui



# Badan Pemeriksa Keuangan Republik Indonesia

Diterbitkan:  
1 Juni 2010

No. Revisi: 06

Halaman 3 dari 6

MI-R06-P01

Identifikasi Insiden

## PROSEDUR

- a) Memeriksa konfigurasi perangkat TI yang diinspeksi, apakah konfigurasi perangkat masih sesuai dengan database konfigurasi [DB001].
- b) Memeriksa kinerja perangkat TI yang diinspeksi, apakah kinerja perangkat TI masih sesuai dengan SLA yang disepakati dalam database SLA kinerja perangkat TI [DB002].
- c) Mengidentifikasi potensi insiden pada perangkat TI yang diinspeksi.
- d) Potensi insiden pada perangkat yang diinspeksi diketahui pada saat konfigurasi perangkat TI sudah berubah dan/atau kinerja perangkat TI berada dibawah SLA yang disepakati.
- d. U (staf inspeksi berkala) membuat laporan berisi hasil inspeksi yang ditulis dalam laporan inspeksi staf teknis [FL001] dan diserahkan kepada HO dengan tembusan kepada IM sebagai laporan pelaksanaan.
- e. HO menerima laporan inspeksi staf teknis [FL001] dan menyimpannya ke dalam database laporan inspeksi [DB003] setelah melakukan prosedur Pencatatan Insiden.

### 2. Deteksi insiden oleh pengguna

- a. U (pegawai atau pimpinan/pejabat pengguna TI), mendeteksi insiden jika diketahui:
  - a) U tiba-tiba mendapat pesan error pada perangkat komputer yang digunakannya.
  - b) U tiba-tiba tidak dapat mengakses jaringan lokal dan/atau internet.
  - c) U tiba-tiba tidak dapat menggunakan fitur dalam aplikasi SI yang sedang dipakai.

**SIFAT RAHASIA**

Hanya didistribusikan kepada yang berhak mengetahui



# Badan Pemeriksa Keuangan Republik Indonesia

Diterbitkan:  
1 Juni 2010

No. Revisi: 06

Halaman 4 dari 6

MI-R06-P01

Identifikasi Insiden

## PROSEDUR

b. U mencatat deskripsi insiden yang dialaminya dan tidak mengutak-atik lagi perangkat TI yang terkena insiden tersebut.

### 3. Pelaporan insiden

- a. HO menerima laporan insiden melalui telepon dengan nomor telepon 021-5704395 pswt.999 (kode pesawat telepon dapat diubah dan ditambah sesuai kondisi yang ada).
- b. HO menerima laporan insiden melalui email dengan alamat email [helpdesk@bpk.go.id](mailto:helpdesk@bpk.go.id) (alamat email dapat diubah dan ditambah sesuai kondisi yang ada).
- c. HO menerima laporan insiden di meja helpdesk yang berada di lantai II Gedung Sekretariat Jenderal BPK-RI.
- d. HO menerima laporan insiden dan menyimpannya ke dalam database laporan inspeksi

### 4. Membuka kartu insiden

- a. HO membuka kartu insiden dengan status "Belum selesai" dari dalam database insiden.
- b. HO kemudian mendistribusikan masing-masing kartu insiden tersebut kepada staf yang bertanggungjawab menanganinya di level HO, HS, dan SM/NM/MM.

## E. FORMULIR DAN DOKUMEN

1. Jadwal inspeksi berkala [JD001]
2. Surat tugas inspeksi berkala [ST001]
3. Database konfigurasi [DB001]
4. Database SLA kinerja perangkat TI [DB002]
5. Database laporan inspeksi [DB003]
6. Formulir laporan inspeksi staf teknis [FL001]

## SIFAT RAHASIA

Hanya didistribusikan kepada yang berhak mengetahui





# Badan Pemeriksa Keuangan Republik Indonesia

Diterbitkan:  
1 Juni 2010

No. Revisi: 06

Halaman 5 dari 6

MI-R06-P01

Identifikasi Insiden

## PROSEDUR

### F. DIAGRAM RACI

No.	Langkah	U	HO	HS	IM	SM	NM	MM
1.	Deteksi insiden melalui inspeksi berkala		R		A			
2.	Deteksi insiden oleh pengguna	AR						
3.	Pelaporan insiden	AR	R					
4.	Membuka kartu insiden		AR	I		I	I	I

### G. ISTILAH DAN SINGKATAN

U ,singkatan dari User atau Pelapor Insiden. U adalah sebutan bagi pihak-pihak yang melaporkan insiden. Dalam prosedur ini, U terdiri atas 2 (dua) macam pelapor yaitu staf inspeksi dan pengguna perangkat TI (pegawai dan pimpinan).

HO ,singkatan dari Helpdesk Operator. HO adalah level pertama penanganan insiden. HO juga memiliki tugas untuk menerima setiap laporan insiden dari U.

HS ,singkatan dari Helpdesk Spesialist. HS adalah level kedua penanganan insiden. HS menerima tugas penanganan insiden setelah dilakukan tindakan eskalasi insiden dari HO.

IM ,singkatan dari Incident Manager. IM adalah penanggungjawab keseluruhan proses TI penanganan insiden. Dalam keseharian IM adalah bagian dari manajemen biro TI yaitu Kasubag Dukungan TI.

SM ,singkatan dari Software Manager. SM adalah level ketiga penanganan insiden. SM menerima tugas penanganan insiden setelah dilakukan tindakan eskalasi insiden dari HS. Dalam

**SIFAT RAHASIA**

Hanya didistribusikan kepada yang berhak mengetahui



# Badan Pemeriksa Keuangan Republik Indonesia

Diterbitkan:  
1 Juni 2010

No. Revisi: 06

Halaman 6 dari 6

MI-R06-P01

Identifikasi Insiden

## PROSEDUR

keseharian SM adalah bagian dari manajemen biro TI yaitu Kasubag Perancangan Aplikasi Komputer.

NM ,singkatan dari Network Manager. NM adalah level ketiga penanganan insiden. NM menerima tugas penanganan insiden setelah dilakukan tindakan eskalasi insiden dari HS. Dalam keseharian NM adalah bagian dari manajemen biro TI yaitu Kasubag Operasional TI.

MM ,singkatan dari Maintenance Manager. MM adalah level ketiga penanganan insiden. MM menerima tugas penanganan insiden setelah dilakukan tindakan eskalasi insiden dari HS. Dalam keseharian MM adalah bagian dari manajemen biro TI yaitu Kasubag Pemeliharaan Perangkat TI.

R ,singkatan dari Responsible. R adalah fungsi dalam diagram RACI yang merujuk pada pihak pelaksana yang harus bertanggungjawab melaksanakan dan menyelesaikan aktifitas yang menjadi tanggungjawabnya.

A ,singkatan dari Accountable. A adalah fungsi dalam diagram RACI yang merujuk pada pihak pelaksana yang harus mengarahkan jalannya pelaksanaan aktifitas.

C ,singkatan dari Consult. C adalah fungsi dalam diagram RACI yang merujuk pada pihak pelaksana yang akan menjadi tempat konsultasi selama pelaksanaan aktifitas.

I ,singkatan dari Inform. I adalah fungsi dalam diagram RACI yang merujuk pada pihak pelaksana yang akan menjadi pihak yang diberikan informasi mengenai pelaksanaan aktifitas.

### H. CATATAN PERUBAHAN

Tidak ada

**SIFAT RAHASIA**

Hanya didistribusikan kepada yang berhak mengetahui



# Badan Pemeriksa Keuangan Republik Indonesia

Diterbitkan:  
1 Juni 2010

No. Revisi: 06

Halaman 1 dari 3

MI-R06-JD001

Jadwal Inspeksi Berkala

DOKUMEN DAN FORMULIR

## Jadwal mingguan

Minggu ke-	Nama staf	Nama perangkat TI yang akan diinspeksi	Keterangan
I	[nama staf HO yang ditunjuk]		
II	[nama staf HO yang ditunjuk]		
III	[nama staf HO yang ditunjuk]		
IV	[nama staf HO yang ditunjuk]		
V	[nama staf HO yang ditunjuk]		

Disusun oleh:

[paraf]

[nama kasubag Dukti]

[NIP. ]

DOKUMEN  
Dan FORMULIR

**SIFAT RAHASIA**

Hanya didistribusikan kepada yang berhak mengetahui



# Badan Pemeriksa Keuangan Republik Indonesia

Diterbitkan:  
1 Juni 2010

No. Revisi: 06

Halaman 2 dari 3

MI-R06-JD001

Jadwal Inspeksi Berkala

DOKUMEN DAN FORMULIR

## Jadwal bulanan

Bulan ke-	Nama staf	Nama perangkat TI yang akan diinspeksi	Lokasi perangkat TI	Keterangan
I	[nama staf HO yang ditunjuk]			
II	[nama staf HO yang ditunjuk]			
III	[nama staf HO yang ditunjuk]			
IV	[nama staf HO yang ditunjuk]			
V	[nama staf HO yang ditunjuk]			
VI	[nama staf HO yang ditunjuk]			
VII	[nama staf HO yang ditunjuk]			
VIII	[nama staf HO yang ditunjuk]			
IX	[nama staf HO yang ditunjuk]			
X	[nama staf HO yang ditunjuk]			
XI	[nama staf HO yang ditunjuk]			

**SIFAT RAHASIA**

Hanya didistribusikan kepada yang berhak mengetahui



# Badan Pemeriksa Keuangan Republik Indonesia

Diterbitkan:  
1 Juni 2010

No. Revisi: 06

Halaman 3 dari 3

MI-R06-JD001

Jadwal Inspeksi Berkala

## DOKUMEN DAN FORMULIR

Bulan ke-	Nama staf	Nama perangkat TI yang akan diinspeksi	Lokasi perangkat TI	Keterangan
XII	[nama staf HO yang ditunjuk]			

Disusun oleh:

[paraf]

[nama kasubag Dukti]

[NIP. ]

**SIFAT RAHASIA**

Hanya didistribusikan kepada yang berhak mengetahui

	<b>Badan Pemeriksa Keuangan Republik Indonesia</b>	
Diterbitkan: 1 Juni 2010	No. Revisi: 06	Halaman 1 dari 2
<b>MI-R06-ST001</b>		<b>Surat Tugas Inspeksi Berkala</b>
<b>DOKUMEN DAN FORMULIR</b>		

**SURAT TUGAS**

No. [mengacu pada SK Sekjen]

Dengan ini, Sub Bagian Dukungan TI menugaskan kepada:

Nama :

NIP :

Untuk melakukan tugas inspeksi berkala atas perangkat TI:

Nama perangkat :

Lokasi :

Lama penugasan : ... hari

Demikian surat tugas ini dibuat untuk dilaksanakan sebagaimana mestinya.

Jakarta, [tanggal surat tugas]

[TTD dan cap kantor]

[nama kasubag Dukti]

[NIP. ]

**DOKUMEN  
Dan FORMULIR**

**SIFAT RAHASIA**

Hanya didistribusikan kepada yang berhak mengetahui

	<h2 style="text-align: center;">Badan Pemeriksa Keuangan Republik Indonesia</h2>	
Diterbitkan: 1 Juni 2010	No. Revisi: 06	Halaman 2 dari 2
MI-R06-ST001		Surat Tugas Inspeksi Berkala
<b>DOKUMEN DAN FORMULIR</b>		

### SURAT TUGAS

No. [mengacu pada SK Sekjen]

Dengan ini, Sub Bagian Dukungan TI menugaskan kepada:

- Ketua Tim : [nama/NIP.]  
Anggota : 1. [nama/NIP.]  
2. [nama/NIP.]

Untuk melakukan tugas inspeksi berkala atas perangkat TI:

- Nama perangkat :  
Lokasi :  
Lama penugasan : ... hari

Demikian surat tugas ini dibuat untuk dilaksanakan sebagaimana mestinya.

Jakarta, [tanggal surat tugas]

[TTD dan cap kantor]

[nama kasubag Dukti]  
[NIP.                                ]

### SIFAT RAHASIA

Hanya didistribusikan kepada yang berhak mengetahui



# Badan Pemeriksa Keuangan Republik Indonesia

Diterbitkan:  
1 Juni 2010

No. Revisi: 06

Halaman 1 dari 2

MI-R06-FL001

Formulir Laporan  
Inspeksi Staf Teknis

DOKUMEN DAN FORMULIR

## Formulir Inspeksi

### No. Formulir

[nomor formulir]

### *Surat Tugas*

No. Surat Tugas

[nomor surat tugas]

Nama staf inspeksi

[nama-nama staf inspeksi]

### *Pelaksanaan inspeksi*

Tanggal pelaksanaan inspeksi

[format YYYYMMDD]

Lokasi inspeksi

[lokasi inspeksi]

Perangkat TI yang diinspeksi

[nama perangkat TI]

### *Hasil inspeksi*

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

DOKUMEN  
Dan FORMULIR

**SIFAT RAHASIA**

Hanya didistribusikan kepada yang berhak mengetahui





# Badan Pemeriksa Keuangan Republik Indonesia

Diterbitkan:  
1 Juni 2010

No. Revisi: 06

Halaman 2 dari 2

MI-R06-FL001

Formulir Laporan  
Inspeksi Staf Teknis

DOKUMEN DAN FORMULIR

*Laporan kepada Helpdesk Operator*

Tanggal penyerahan laporan [format YYYYMMDD]

Staf HO yang menerima [nama staf HO]

Paraf [paraf staf HO]

**SIFAT RAHASIA**

Hanya didistribusikan kepada yang berhak mengetahui

	<h1 style="text-align: center;">Badan Pemeriksa Keuangan Republik Indonesia</h1>	
Diterbitkan: 1 Juni 2010	No. Revisi: 06	Halaman 1 dari 1
<b>MI-R06-DB001</b>		<b>Database Konfigurasi</b>
<b>DOKUMEN DAN FORMULIR</b>		

Dokumen database konfigurasi berisikan daftar konfigurasi perangkat TI yang digunakan dalam lingkungan BPK-RI. Daftar konfigurasi ini mencakup perangkat TI baik perangkat jaringan (network), perangkat keras (hardware), maupun perangkat lunak (software) yang dikembangkan sendiri atau dibeli melalui proses pengadaan. Daftar konfigurasi yang dicatat adalah konfigurasi perangkat agar dapat berjalan normal. Pada saat ini dokumen database konfigurasi belum bisa digunakan karena masih sedang dikembangkan.

Status: *To Be Defined.*

**DOKUMEN  
Dan FORMULIR**

**SIFAT RAHASIA**

Hanya didistribusikan kepada yang berhak mengetahui

	<h1 style="text-align: center;">Badan Pemeriksa Keuangan Republik Indonesia</h1>	
Diterbitkan: 1 Juni 2010	No. Revisi: 06	Halaman 1 dari 1
<b>MI-R06-DB002</b>		<b>Database SLA Kinerja Perangkat TI</b>
<b>DOKUMEN DAN FORMULIR</b>		

Dokumen database SLA kinerja perangkat TI berisikan daftar standar kinerja perangkat TI yang digunakan dalam lingkungan BPK-RI. Standar kinerja yang dimaksud adalah target kinerja yang diharapkan dari masing-masing perangkat pada saat melaksanakan fungsinya. Daftar standar kinerja ini mencakup perangkat TI baik perangkat jaringan (network), perangkat keras (hardware), maupun perangkat lunak (software) yang dikembangkan sendiri atau dibeli melalui proses pengadaan.

Pada saat ini dokumen SLA kinerja perangkat TI belum bisa digunakan karena masih sedang dikembangkan.

Status: *To Be Defined.*

**DOKUMEN  
Dan FORMULIR**

**SIFAT RAHASIA**

Hanya didistribusikan kepada yang berhak mengetahui

	<h1 style="text-align: center;">Badan Pemeriksa Keuangan Republik Indonesia</h1>	
Diterbitkan: 1 Juni 2010	No. Revisi: 06	Halaman 1 dari 1
<b>MI-R06-DB003</b>		<b>Database Laporan Inspeksi</b>
<b>DOKUMEN DAN FORMULIR</b>		

Dokumen database laporan inspeksi berisikan kumpulan laporan inspeksi yang dilakukan secara berkala oleh staf HO (*Helpdesk Operator*). Database ini akan digunakan staf inspeksi untuk membandingkan kondisi perangkat pada saat inspeksi saat ini dengan inspeksi sebelumnya.

Pada saat ini dokumen database laporan inspeksi belum bisa digunakan karena belum ada laporan inspeksi berkala yang dilakukan.

Status: *To Be Defined.*

**DOKUMEN  
Dan FORMULIR**

**SIFAT RAHASIA**

Hanya didistribusikan kepada yang berhak mengetahui