Kajian dan Pelaksanaan Manajemen Insiden di Kantor Pelayanan Perbendaharaan Negara di Lingkungan Kantor Wilayah Perbendaharaan Jawa Timur

Eko Supristiowadi, Bambang Setiawan, Yudhistira Kesuma
Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS)
Jl. Arief Rahman Hakim, Surabaya 60111
E-mail: yudhistira.k@gmail.com

***Abstrak*—Kantor Pelayanan Perbendaharaan Negara (KPPN) adalah kantor perwakilan Departemen Keuangan di daerah yang berada di bawah Direktorat Jenderal Perbendaharaan, yang fungsi utamanya adalah pengelolaan Anggaran Pendapatan dan Belanja Negara (APBN) khususnya dalam hal pengeluaran dana APBN. Untuk menunjang kegiatan operasional KPPN terkait pencairan dana APBN, KPPN menggunakan perangkat teknologi informasi baik yang bersifat perangkat keras maupun aplikasi. Semakin tinggi peranan teknologi informasi dalam menunjang kegiatan operasional KPPN, sudah seharusnya KPPN memiliki sebuah perangkat Manajemen Layanan Teknologi Informasi (MLTI) yang dapat menjaga kualitas layanan teknologi informasi yang ada di KPPN. Penerapan MLTI bisa didasarkan pada sebuah standart yang sudah berlaku internasional seperti salah satunya adalah ITIL (Information Technology Infrastructur Library). Sebagai langkah awal pelaksanaan MLTI di KPPN, maka KPPN dapat melaksanakan manajemen insiden. Dengan adanya manajemen insiden diharapkan insiden yang terjadi pada perangkat layanan teknologi informasi di KPPN dapat tertangani secara cepat dan tidak sampai menganggu proses bisnis yang ada.**

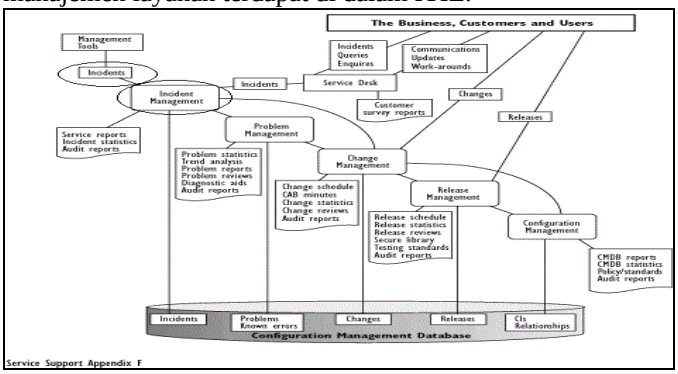
***Kata Kunci*—KPPN. APBN, MLTI, manajemen insiden.**

I. PENDAHULUAN

SEMAKIN penting peran teknologi informasi dalam menunjang kegiatan operasional organisasi, maka adanya sebuah manajemen yang dapat menjaga kualitas layanan teknologi informasi yang ada adalah sebuah keharusan. Manajemen layanan teknologi informasi memiliki banyak cabang manajemen, dimana kesemua cabang manajemen yang ada bertujuan untuk memastikan kualitas layanan teknologi informasi terus terjaga. Salah satu cabang manajemen layanan teknologi informasi adalah manajemen insiden. Manajemen insiden adalah manajemen yang bertindak sebagai "perisai" awal ketika sebuah kejadian atau insiden terjadi.

Kegiatan operasional KPPN sebagian besar atau bahkan seluruhnya menggunakan perangkat teknologi informasi sebagai pendukung kinerja. Dengan peranan teknologi informasi yang begitu besar di KPPN, maka proses bisnis yang ada di KPPN akan sangat rentan terganggu jika teknologi informasi yang berindak sebagai sarana pendukung operasional mengalami gangguan. Melihat dari tergantungnya proses bisnis pada layanan teknologi informasi yang ada, maka sudah seharusnya sebuah manajemen layanan yang dapat menjaga kualitas layanan teknologi informasi di KPPN itu ada dan berjalan sesuai dengan fungsinya. Semakin baik dan berjalannya fungsi manajemen layanan teknologi informasi maka proses bisnis KPPN dapat dipastikan tidak akan mengalami gangguan dan hambatan, walaupun nantinya akan terjadi sebuah kejadian yang dapat mengganggu proses bisnis KPPN maka gangguan tersebut tidak akan berlangsung lama dan secepatnya proses bisnis yang terganggu kembali berjalan normal.

Dalam hal penerapan manajemen layanan teknologi informasi, hendaknya didasarkan pada penggunaan standart internasional seperti salah satunya ITIL. ITIL digunakan karena ITIL berisi *best practises* di bidang manajemen layanan, sehingga jika KPPN akan menerapkan manajemen layanan menggunakan standart ITIL maka KPPN tidak perlu lagi memikirkan bagaimana pelaksanaan manajemen layanan yang baik karena semua hal yang terbaik dalam hal manajemen layanan terdapat di dalam ITIL.



Gambar. 1. Manajemen Insiden.

Salah satu cabang manajemen yang terdapat di dalam manajemen layanan teknologi informasi yang penting dan pertama kali yang sebaiknya diterapkan adalah manajemen insiden. Hal ini seperti yang terdapat pada alur kegiatan manajemen layanan di ITIL versi 5. Di dalam ITIL versi 5 digambarkan bahwa cabang manajemen di dalam manajemen layanan yang pertama kali menangani sebuah kejadian adalah manajemen insiden. Adapun gambaran lengkapnya seperti

yang terdapat pada Gambar 1.

II. TINJAUAN PUSTAKA

A. Sekilas tentang KPPN dan unit-unit kerjanya

Kantor Pelayanan Perbendaharaan Negara adalah kantor vertikal yang berada di bawah salah satu Unit Eselon I Departemen Keuangan yaitu Direktorat Jenderal Perbendaharaan. Tugas utama dari KPPN adalah menyelenggarakan proses pencairan dana Anggaran dan Pendapatan Belanja Negara dari masing-masing satuan kerja yang merupakan unit kerja dari seluruh Departemen yang ada di daerah di seluruh Indonesia. Dalam pelaksanaan tugasnya, KPPN banyak melibatkan hal yang terkait dengan teknologi informasi seperti aplikasi, jaringan LAN, komputer server, dan lainnya yang memiliki hubungan dengan kegiatan operasional KPPN. Layanan-layanan teknologi informasi yang ada di KPPN saat ini belum di-*cover* dengan manajemen yang baik terkait apabila suatu saat terjadi insiden yang dapat mengganggu kualitas layanan TI yang ada di KPPN.

Terdapat bagian-bagian atau unit kerja yang ada di KPPN antara lain :

1. Bagian Bendahara Umum
2. Bagian Perbendaharaan
3. Bagian Verifikasi dan Akuntansi
4. Bagian Umum

B. Sejarah *Information Technology Infrastructure Library* (ITIL)

ITIL dimulai pada tahun 1980. ITIL pertama kali diperkenalkan pada pertengahan sampai akhir tahun 1980. Kemudian pada tahun 1990 banyak perusahaan besar dan pemerintah di Inggris dan Eropa khususnya di Belanda mulai menerapkan kerangka kerja ITIL sebagai dasar kegiatan operasi Teknologi Informasi yang selanjutnya disebut TI. Pada milenium baru, itu adalah saat di mana ITIL berkembang pesat, banyak perusahaan lain yang mulai menerapkan ITIL pada proses bisnisnya khususnya di bidang operasional TI. Salah satu perusahaan yang menggunakan ITIL versi 1 adalah Microsoft. Microsoft menggunakan ITIL versi 1 sebagai pondasi mereka dalam mengembangkan Microsft Operations Framework (MOF) [1].

Pada tahun 2001, ITIL versi 2 diluncurkan, update yang diluncurkan antara lain teks yang lebih modern, terminologi, dan contoh-contoh di bidang *service support* dan *service delivery*. Tahun 2002, standart manajemen layanan BS1500 secara signifikan direvisi dan diluncurkan. Tahun 2005, BS1500 berganti menjadi standart ISO: ISO 20000. Pada tahun 2006, para anggota yang tergabung dalam tim perumus ITIL diseleksi untuk bagaimana nantinya dapat merumuskan set dokumen ITIL. Publikasi tentang isi dokumen ITIL yang baru dijadwalkan diluncurkan pada semester pertama tahun 2007 [1].

C. Manajemen Insiden menurut ITIL versi 3

Adapun isi dari manajemen insiden menurut ITIL versi 3 adalah sebagai berikut.

1. Tujuan manajemen insiden
   Tujuan dari manajemen insiden adalah layanan-layanan TI yang ada dapat di-*restore* ke kondisi operasi normal secepat mungkin dan meminimalisir dampak yang kurang baik terhadap kegiatan bisnis organisasi.
2. Ruang lingkup manajemen insiden
   Ruang lingkup manajemen insiden adalah semua insiden yang terjadi terkait dengan teknologi informasi yang ada di sebuah organisasi yang menghambat atau yang dapat menghambat kinerja layanan-layanan yang terdapat di dalam katalog layanan atau *service catalog*.
3. *Value to business*
   Ada beberapa *value to business* dari manajemen insiden, yaitu:
   a. Kemampuan untuk mendeteksi dan me-*resolve* insiden yang terjadi secapat mungkin.
   b. Kemampuan untuk mengalokasikan kemampuan teknologi infomasi organisasi sesuai prioritas bisnis yang ada.
   c. Kemampuan untuk mengidentifikasi pengembangan yang potensial terhadap layanan-layanan yang ada.
4. Konsep Dasar manajemen insiden
   Ada beberapa konsep dasar yang ada di manajemen insiden, yaitu:
   a. Skala waktu
      Skala waktu berhubungan dengan waktu penyelesaian insiden, alokasi waktu disesuaikan dengan prioritas dari insiden berdasarkan *Service Level Agreement* yang ada.
   b. Pemodelan insiden
      Pemodelan insiden dibuat berdasarkan hal-hal yang dilakukan pada penanganan insiden yang sebelumnya pernah terjadi
   c. Insiden besar
      Insiden besar harus mendapat prioritas, dan *urgency* yang tinggi serta waktu penyelesaian yang singkat.
5. Proses/alur kerja manajemen insiden
   Ada beberapa proses kerja yang terdapat dalam pelaksanaan manajemen insiden, yaitu:
   a. Identifikasi insiden
   b. Log/rekam insiden
   c. Kategorisasi insiden
   d. Prioritisasi insiden
   e. Diagnosa awal
   f. Eskalasi insiden
   g. Investigasi dan diagnosa lanjutan
   h. Proses resolusi dan recovery
   i. *Incident closure*

III. URAIAN PENELITIAN

A. Kajian Awal di KPPN

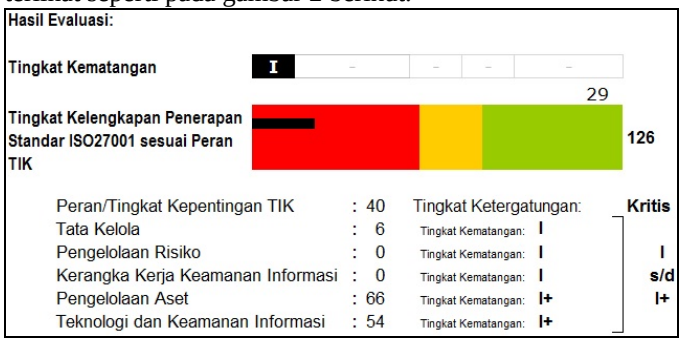
Kajian awal dilakukan agar diperoleh informasi terkait dengan peran teknologi informasi dalam menunjang kegiatan operasional organisasi. Dalam hal ini, kajian awal yang dilakukan di KPPN menggunakan indeks KAMI (Keamanan Informasi) yang dikeluarkan oleh Kementerian Komunikasi dan Informatika (KemenKomInfo). Menurut KemenKomInfo, indeks KAMI adalah alat evaluasi untuk menganalisis tingkat

kesiapan pengamanan informasi di instansi pemerintah. Sedangkan tujuan dari adanya indeks KAMI adalah untuk memperoleh gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi. Lalu apa hubungan antara penggunaan indeks KAMI sebagai alat pengkaji awal dengan pelaksanaan manajemen insiden? Hubungan antara penggunaan indeks KAMI dan pelaksanaan manajemen insiden adalah terletak pada kesamaaan standart yang mendasari kedua hal tersebut. Indeks KAMI dibuat berdasarkan standart ISO 27001, sedangkan pelaksanaan manajemen insiden didasarkan pada ITIL. Kedua standart yaitu ISO 27001 dan ITIL sama-sama memiliki model PDCA (Plan Do Check Action) [2][3]. Berdasarkan kesamaan inilah mengapa indeks KAMI dapat digunakan untuk menilai apakah sebuah organisasi perlu melaksanakan manajemen insiden atau tidak.

Ada beberapa area evaluasi yang terdapat di dalam indeks KAMI menurut KemenKomInfo, yaitu :

1. Peran/Tingkat Kepentingan teknologi informasi
   Dari area evaluas ini akan didapatkan informasi seberapa penting peranan teknologi informasi dalam menunjang kegiatan operasional organisasi pemerintah.
2. Tata Kelola Keamanan Informasi – Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.
3. Pengelolaan Risiko Keamanan Informasi – Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.
4. Kerangka Kerja Keamanan Informasi – Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.
5. Pengelolaan Aset Informasi – Bagian ini mengevaluasi kelengkapan pengamanan terhadap aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut; dan
6. Teknologi dan Keamanan Informasi – Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.

Contoh hasil dari kajian menggunakan indeks KAMI dapat terlihat seperti pada gambar 2 berikut.



Gambar. 2.Hasil Evaluasi Indeks KAMI.

Pada contoh hasil evaluasi indeks KAMI di atas, terlihat bahwa peran teknologi informasi kritis dalam mendukung kegiatan operasional yang ada, namun tidak dibarengi dengan adanya tata kelola maupun pengelolaan risiko teknologi informasi yang memadai. Melihat hal ini tentu saja kondisi yang ada sangat mengkhawatirkan, ketika layanan teknologi informasi yang ada mengalami gangguan, sudah dapat dipastikan proses bisnis yang ada juga akan mengalami gangguan. Sebagai langkah awal dalam menjaga kualitas layanan teknologi informasi terhadap sebuah kejadian atau insiden, maka pelaksanaan manajemen insiden sangatlah tepat.

Mengapa harus manajemen insiden yang terlebih dahulu dialaksanakan? Seperti yang telah dijelaskan sebelumnya menurut ITIL versi 5 bahwa manajemen insiden adalah cabang manajemen di dalam manajemen layanan teknologi informasi yang menempati posisi pertama ketika sebuah kejadian atau insiden terjadi.

B. Pembuatan Aplikasi pembantu perekaman insiden

Dikarenakan KPPN baru mengenal manajemen insiden maka adanya aplikasi pembantu untuk melakukan perekaman insiden maka akan sangat mempermudah KPPN dalam memahami manajemen insiden. Aplikasi perekaman insiden nantinya dapat dijadikan sebagai alat untuk menyimpan *log* insiden atau dijadikan *library* bagi KPPN ketika insiden yang sama terjadi di KPPN.

Proses pembuatan aplikasi terbagi ke dalam proses-proses berikut:

a. Analisis kebutuhan:
   1. Kebutuhan pengguna
   2. Kebutuhan teknologi
   3. Kebutuhan layanan-layanan SI/TI KPPN
   4. Kebutuhan fungsi
b. Design database
   1. Conseptual Data Model
   2. Physical Data Model
c. Design aplikasi:
   1. Domain model
   2. Use Case Diagram
   3. Robustness Diagram
   4. Sequence Diagram
   5. Class Diagram
d. Design Antarmuka
e. Test Case dan Unit Test

C. Kajian Lanjutan Pelaksanaan Manajemen Insiden KPPN

Kajian lanjutan dilaksanakan untuk mengetahui sejauh mana manajemen layanan yang telah diterapkan dapat berjalan baik dan dapat membantu mempercepat proses pemulihan dari adanya sebuah insiden. Kajian lanjutan dilaksanakan menggunakan sejumlah pertanyaan untuk menggali informasi mengenai pelaksanaan manajemen insiden di KPPN. Setelah kajian dilakukan, maka akan diperoleh nilai dari pelaksanaan manajemen insiden di KPPN. Semakin tinggi nilai yang diperoleh maka mengindikasikan bahwa pelaksanaan manajemen insiden berjalan baik dan dapat membantu mempercepat proses pemulihan akibat dari adanya insiden.

Adapun daftar pertanyaan yang dibuat berdasarkan alur dari manajemen insiden yang ada di dalam ITIL versi 3, dan proses

penilaian dari kajian lanjutan yang dilakukan adalah sebagai berikut:

1. Daftar Pertanyaan
   Daftar pertanyaan yang ada, terbagi ke dalam beberapa kategori pertanyaan, yaitu:
   a. Pertanyaan seputar ada atau tidaknya pengelolaan insiden dan bila terdapat pengelolaan insiden apakah disesuaikan dengan standart yang ada seperti ITIL.
   b. Pertanyaan seputar keterjadian insiden.
   c. Pertanyaan seputar peran dan tanggung jawab pihak-pihak yang terkait dengan terjadinya insiden.
   d. Pertanyaan seputar waktu penyelesaian insiden.
2. Penilaian pelaksanaan manajemen insiden
   Penilaian didasarkan pada pertanyaan yang disampaikan sebelumnya pada point 1 di atas. Dari sejumlah jawaban yang didapat, maka akan ter-*generate* secara otomatis nilai yang kemudian dapat dicetak. Dari nilai yang ter-*generate* ini nantinya dapat diketahui seberapa jauh KPPN telah menjalankan manajemen insiden, dan seberapa baik manajemen insiden dalam mempercepat proses pemulihan dari imbas akiibat terjadinya insiden.

   Dari penilaian ini diharapkan KPPN yang memiliki nilai kurang baik dalam hal pelaksanaan manajemen insiden, maka KPPN tersebut harus lebih berusaha untuk dapat melaksanakan manajemen insiden dengan baik sehingga insiden yang terjadi dapat cepat tertangani dan imbas yang terjadi tidak terlalu besar.

IV. KESIMPULAN/RINGKASAN

Berikut ini adalah beberapa kesimpulan yang dapat diambil dari tulisan ini, yaitu:

1. Penerapan awal manajemen layanan SI/TI dapat dimulai terlebih dahulu dengan manajemen insiden.
2. Adanya manajemen insiden dapat mempercepat proses pemulihan kegiatan operasional yang terkena insiden dan meminimalisir risiko dari insiden yang terjadi tersebut.
3. Proses percepatan penyelesaian insiden menggunakan aplikasi adalah dengan cara melihat *log* atau *library* dari rekaman penyelesaian insiden yang terjadi, hal ini bisa dilakukan terhadap insiden yang sama dengan insiden yang sebelumnya pernah terjadi. Jika ternyata belum terdapat *log* penyelesaian insiden, maka proses percepatan penyelesaian insiden adalah berupa penggunaan *list* atau daftar insiden yang berasal dari aplikasi. Dengan adanya daftar insiden yang dihasilkan dari aplikasi, maka user yang berwenang mengawasi keterjadian insiden dapat memantau insiden mana saja yang harus secepatnya ditangani dan masih belum terselesaikan.

DAFTAR PUSTAKA

[1] KV, Warre. 2010. *Security controls in service management.* SANS Institute reading room. http://www.sans.org/search/results.

[2] Sheikhpour, Razieh dan Nasser Modiri, 2012. *A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management*. Indian Journal of Science and Technology, Vol 5 No. 2.

[3] Office of Government Commerce (OGC), 2007. ITIL V3-Service Operation. APMG Service Desk, Buckinghamshire.

[4] Depkominfo, 2012. Indeks KAMI versi 2.2. Direktorat Keamanan Informasi, Jakarta.