# PENGEMBANGAN PROSEDUR PELAPORAN INSIDEN KEAMANAN INFORMASI MENGGUNAKAN STANDARISASI ISO/IEC 27001 DAN 27002

**Iwan Santosa**
Program Studi Teknik Informatika, Universitas Trunojoyo Madura
Jl. Raya Telang, PO BOX 2, Kamal, Bangkalan - 69162
*iansantosa@gmail.com*

**ABSTRAK**

Pada tahun 1996, U.S. Federal Computer Incident Response Capability (FedCIRC) melaporkan telah terjadi sekitar 2500 "insiden" dalam sistem komputer[1]. Laporan penelitian yang dilakukan oleh NPO Japan Network Security Association, "Security Incident Investigation Working Group" pada 31 Maret 2010, insiden yang terjadi selama tahun 2008 meningkat signifikan jika dibandingkan dengan tahun sebelumnya, 509 insiden lebih banyak menjadi 1.373 insiden. [2]. Di Indonesia, berdasarkan laporan penelitian oleh ID-CERT (Indonesia Computer Emergency Response Team) memberikan informasi pada bulan juni 2010 mendapatkan serangan spam sebanyak 300.000 kali [3].Dari sebagian data yang telah disampaikan tersebut diperlukan upaya yang serius untuk menanggulangi insiden keamanan informasi yang terjadi. Institusi pemerintah maupun swasta harus memiliki sistem keamanan yang baik untuk menanggulangi segala bentuk serangan yang menyebabkan insiden terjadi seperti hilangnya layanan, sistem tidak berfungsi atau overload, kesalahan manusia, ketidakpatuhan dengan kebijakan, pelanggaran pengaturan fisik, perubahan sistem yang tidak terkendali, perangkat keras atau perangkat lunak yang tidak berfungsi dan pelanggaran akses[4].Dalam penelitian ini akan dilakukan pengembangan prosedur pelaporan insiden yang terjadi pada perusahaan mengacu pada standarisasi ISO/IEC 27001 dan 27002 sehingga terbentuklah Standard Operation Procedure (SOP) yang efektif untuk melakukan pelaporan terjadinya insiden tersebut.

Kata kunci : insiden, keamanan informasi, standart ISO/IEC 27001/27002

***ABSTRACT***

*In 1996, the U.S. Federal Computer Incident Response Capability (FedCIRC) reported have occurred around 2500 "incident" in computer systems [1]. Report of research conducted by NPO Japan Network Security Association, "Security Incident Investigation Working Group" on March 31, 2010, incident that occurred during 2008 increased significantly when compared with the previous year, 509 incidents to 1373 incidents more. [2]. In Indonesia, according to research reported by the PH-CERT (Computer Emergency Response Team Indonesia) provide information on the June 2010 attack getting spam as much as 300,000 times a month and June 2011 had as many as 80,000 times the incident network, in [3]. From some of the data that has been delivered a serious effort is needed to cope with information security incidents occurring. Government and private institutions should have a good security system to combat all forms of attack that led to incidents such as loss of service occurs, the system does not function or overload, human error, non-compliance with policies, violations of physical settings, uncontrollable system changes, hardware or software software is not functioning and an access violation [4]. In this paper the analysis will be done about the incident that occurred at the company refers to the standardization of ISO / IEC 27001 and 27002 then create a Standard Operation Procedure (SOP) Effective with reporting to be followed up immediately.*

*Key words: incidents, information security, standard ISO / IEC 27001/27002*

## 1. PENDAHULUAN

Pada tahun 1996, U.S. Federal Computer Incident Response Capability (FedCIRC) melaporkan bahwa telah terjadi sekitar 2500 "insiden" dalam sistem komputer yang disebabkan oleh gagalnya sistem keamanan dan adanya upaya untuk membobol sistem keamanan[1]. Laporan penelitian yang dilakukan oleh NPO Japan Network Security Association, "Security Incident Investigation Working Group" pada 31 Maret 2010, memberikan informasi insiden yang terjadi selama kurun waktu tahun 2008 meningkat signifikan jika dibandingkan dengan tahun sebelumnya, 509 insiden lebih banyak menjadi 1.373 insiden. Padahal dari jumlah insiden tersebut, serangan yang terjadi sejumlah 7.232.763 serangan[2]. Begitu juga di Indonesia berdasarkan laporan penelitian oleh ID-CERT (Indonesia Computer Emergency Response Team) dengan 13 responden diantaranya PANDI, ID-CERT, 3 Operator Telekomunikasi, 2 NAP dan 6 ISP memberikan informasi bahwa pada bulan juni 2011 mengalami insiden jaringan sebanyak 80.000 kali, pada bulan juni 2010 mendapatkan serangan spam sebanyak 300.000 kali[3].

Dari sebagian data yang telah disampaikan diperlukan upaya yang sungguh-sungguh untuk menanggulangi insiden keamanan informasi yang terjadi. Institusi pemerintah maupun swasta harus memiliki sistem keamanan yang baik untuk menanggulangi segala bentuk serangan yang menyebabkan insiden terjadi seperti hilangnya layanan, peristiwa atau fasilitas, sistem tidak berfungsi atau overload, kesalahan manusia, ketidakpatuhan dengan kebijakan, pelanggaran pengaturan fisik, perubahan sistem yang tidak terkendali, perangkat keras atau perangkat lunak yang tidak berfungsi sesuai dengan yang diinginkan dan pelanggaran akses[4].

Untuk dapat membangun dan menerapkan sistem keamanan informasi yang baik, sebaiknya organisasi memulainya dari upaya melakukan kajian atau telaah terhadap resiko-resiko keamanan yang mungkin timbul. Kajian yang dimaksud dapat diterapkan dalam tingkatan organisasi, maupun pada tataran sub bagian atau fungsi organisasi tertentu, seperti sistem informasi, komponen, layanan, dan lain sebagainya sesuai dengan skala prioritas yang ada. Kajian resiko yang dimaksud merupakan suatu pendekatan sistematis dari proses:

1. Identifikasi terhadap kejadian-kejadian apa saja yang dapat mengancam keamanan informasi perusahaan dan potensi dampak kerugian yang ditimbulkan jika tidak terdapat kontrol yang memadai.
2. Analisa tingkat kemungkinan (probabilitas) terjadinya hal-hal yang tidak diinginkan tersebut akibat adanya sejumlah kelemahan pada sistem yang tidak dilindungi dengan kontrol tertentu.

Hasil dari kajian tersebut akan menghasilkan arahan yang jelas bagi manajemen dalam menentukan prioritas dan mengambil sejumlah tindakan terkait dengan resiko keamanan informasi yang dihadapi. Dengan adanya prioritas yang jelas maka akan dapat didefinisikan kontrol-kontrol mana saja yang perlu diterapkan. Perlu diperhatikan bahwa langkah-langkah tersebut harus dilakukan secara kontinyu dan periodik, mengingat dinamika perubahan organisasi dan lingkungan eksternal yang sedemikian cepat. Langkah-langkah interaktif yang dimaksud meliputi:

1. Menganalisa perubahan kebutuhan dan prioritas organisasi yang baru sesuai dengan pertumbuhannya.
2. Mempelajari ancaman-ancaman atau kelamahan-kelemahan baru apa yang terjadi akibat perubahan yang ada tersebut.
3. Memastikan bahwa kendali-kendali yang dimiliki tetap efektif dalam

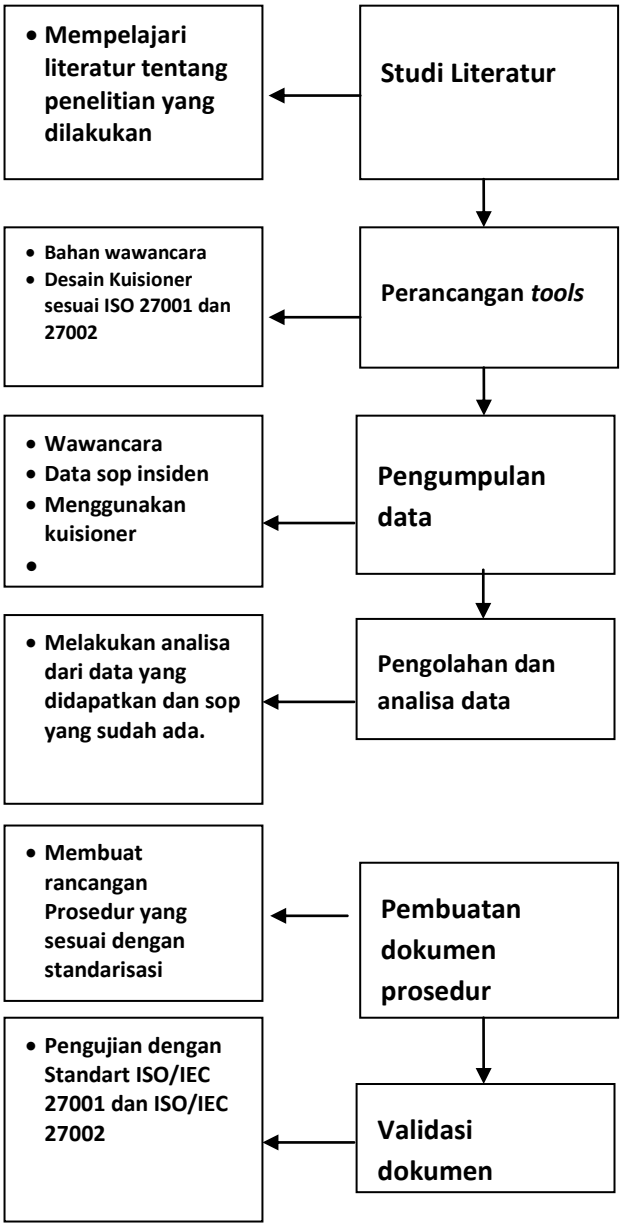
menghadapi ancaman-ancaman kejadian terkait

Perlu dicatat bahwa peninjauan berkala tersebut harus dilakukan pada bagian organisasi dengan tingkat kedalaman tertentu sesuai dengan hasil analisa resiko yang telah dilakukan sebelumnya. Karena keberadaan kontrol ini akan sangat berpengaruh terhadap kinerja sebuah organisasi, maka proses telaah resiko harus dimulai dari tingkat, agar mereka yang berwenang dapat menilainya berdasarkan tingkat kepentingan tertinggi (pendekatan top down)[5].

Keberadaan dan kepatuhan terhadap standar merupakan hal mutlak yang harus dimiliki oleh pihak manapun yang ingin menerapkan sistem keamanan informasi secara efektif. Sejumlah alasan utama mengapa standar diperlukan adalah untuk menjamin agar:

1. Seluruh pihak yang terlibat dalam proses keamanan informasi memiliki kesamaan pengertian, istilah, dan metodologi dalam melakukan upaya-upaya yang berkaitan dengan keamanan data.
2. Tidak terdapat aspek-aspek keamanan informasi yang terlupakan karena standar yang baik telah mencakup keseluruhan spektrum keamanan informasi yang disusun melalui pendekatan komprehensif dan holistik (utuh dan menyeluruh)
3. Upaya-upaya untuk membangun sistem keamanan informasi dilakukan secara efektif dan efisien dengan tingkat optimalisasi yang tinggi, karena telah memperhatikan faktor-faktor perkembangan teknologi serta situasi kondisi yang berpengaruh terhadap organisasi.
4. Tingkat keberhasilan dalam menghasilkan sistem keamanan informasi yang berkualitas menjadi tinggi, karena dipergunakan standar yang sudah teruji kehandalannya.

Dalam penelitian ini akan dilakukan pengembangan prosedur pelaporan insiden yang terjadi pada perusahaan mengacu pada standarisasi ISO/IEC 27001 dan 27002 sehingga terbentuklah Standard Operation Procedure (SOP) yang efektif untuk melakukan pelaporan insiden tersebut.




**Gambar 1. Diagram Alir Penelitian**

Pada studi literatur penulis melakukan pendalaman materi yang terkait dengan insiden keamanan informasi. Pendalaman materi yang dilakukan yaitu terkait tentang definisi dari istilah insiden keamanan informasi dan perkembangan pengertian terkait dengan insiden yang ternyata dari berbagai macam sumber dapat disimpulkan bahwa pengertian insiden keamanan informasi itu berdasarkan [referensi taksonomi], memiliki pengertian yang relatif.Studi literatur selanjutnya adalah terkait dengan standarisasi ISO/IEC 27001:2005 tentang ISMS (Information Security Management System), yang terkait dengan insiden yaitu pada klausul ke 13 tentang Information Security Management System,pada sub klausulnya ada Reporting Information Security Event And Weakness dan Management Informationsecurity Incident And Inprovement yang nantinya dijadikan dasar untuk membuat prosedur pelaporan. Standarisasi ISO/IEC 27002:2005 code of practise for information security management, yang merupakan penjelasan lebih terperinci dari implementasi ISMS pada ISO/IEC 27001:2005, karena secara ringkas berdasarkan riset yang dilakukan oleh Praxiom Recearch Group di dalamnya berisi empat penjelasan yaitu Control (Kontrol), Goal (tujuan), Guidance (Pedoman) dan Note (catatan). Standarisasi selanjutnya adalah ISO/IEC TR 18044 yang telah mengalami pembaruan menjadi ISO/IEC 27035:2005 dan telah diadopsi sebagai dasar untuk membuat standarisasi SNI 7512:2008 oleh Badan Standarisasi Nasional (BSN) indonesia. Standarisasi ini berisi tentang Teknologi informasi – teknik keamanan – pengelolaan insiden keamanan informasi.

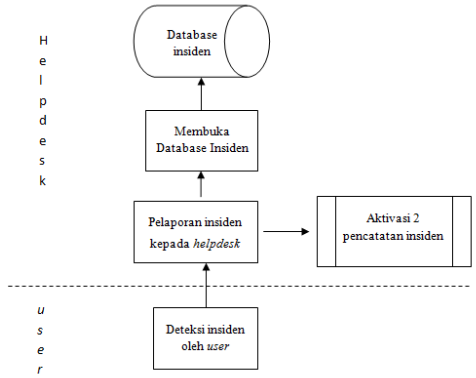
Untuk menjamin agar pengambilan data pada penelitian yang dilakukan memiliki kualitas dan korelasi yang benar maka dibutuhkan perancangan pertanyaan-pertanyaan tentang prosedur pelaporan yang sesuai dengan standarisasi ISO/IEC yang digunakan, yaitu ISO/IEC 27001/27002. Disamping membuat pertanyaan-pertanyaan untuk mengetahui kondisi sebenarnya dari obyek penelitian juga merancang kuisioner yang melalui uji validitas dan uji korelasi untuk memberikan jaminan memang tools ini layak dijadikan sebagai alat mengambil data yang akurat. Pengujian tools yang dilakukan, jika memang hasilnya adalah sesuai dengan aturan yang berlaku akan dapat mempermudah dalam mengambil data dan melakukan analisa untuk kemudian melakukan interprestasi dari data tersebut.

Pada tahap selanjutnya penulis memperbanyak data yang akan digunakan untuk pengolahan. Data yang akan diambil adalah data primer, yaitu data yang kita dapat langsung dari obyek penelitian. Pengumpulan informasi data primer ini berfungsi untuk menemukan prosedur pelaporan insiden informasi yang sudah berjalan pada instansi tersebut. Prosedur existing, yaitu prosedur yang sudah berjalan, apakan sudah sesuai dengan standarisasi dari ISO atau masih diperlukan penyesuaian tertentu atau bahkan tidak sesuai dengan standarisasi. Kondisi inilah yang digunakan untuk melakukan pemetaan dengan standarisasi yang ada. Pemetaan dilakukan untuk mempermudah menemukan kesesuaian prosedur dengan standarisasi yang ada. Kegiatan yang dilakukan adalah dengan metode riset lapangan, terjun langsung ke obyek penelitian dengan melakukan observasi, pengumpulan dokumen terkait, wawancara dan kuisioner.Pada pengolahan dan analisa data dari data yang didapatkan melalui studi literatur, riset lapangan dan metode survey yang telah dilakukan terdapat beberapa tahap analisa. Tahap pertama adalah melakukan identifikasi kontrol obyektif, pada tahap kedua melakukan pemetaan terhadap data yang telah didapatkan dengan kontrol obyektif dari standarisasi yang sesuai dengan insiden keamanan informasi. Dari hasil pemetaan tersebut akan ditemukan permasalahan yang akan muncul. Untuk dicarikan solusi nyata dengan membuat prosedur pelaporan yang sesuai dengan standarisasi yang digunakan. Pada tahap terakhir adalah pembuatan dokumen prosedur. Untuk membuat dokumen prosedur terlebih dahulu pada bab ini akan diidentifikasikan komponen penyusun prosedur pelaporan insiden keamanan informasi. Aktifitas yang dilakukan adalah dengan menyusun rekomendasi kebijakan (policy) yang digunakan untuk mengidentifikasikan semua stakeholder yang terkait dengan prosedur pelaporan insiden keamanan informasi tersebut.

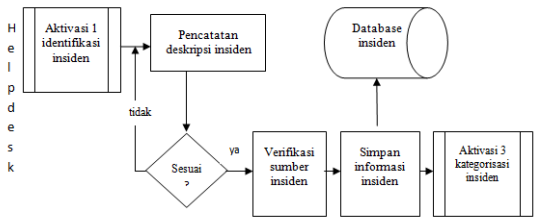
## 3. PEMBAHASAN

Perancangan prosedur yang dilakukan mengikuti beberapa referensi yang digunakan dalam pembuatan SOP. Berdasarkan pada EPA – Envioronmental Protection Agency (April 2007) di dalam SOP mengandung Purpose (Tujuan), Scope (Ruang Lingkup), Definition (Definisi), Reference (Referensi), General Information (Informasi umum) , Guidelines (Pedoman) dan SOP Process. Dalam pedoman implementasi seperti yang tertera dibawah ini akan dijelaskan proses SOP dengan memberikan diagram dan flow chart untuk memudahkan dalam memahaminya. Tahapan SOP yang dibuat adalah sebagai berikut :

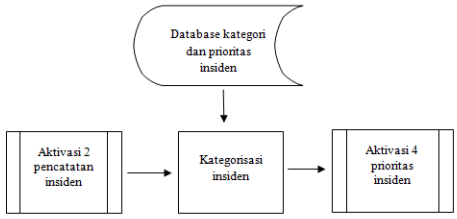
1. Tujuan
2. Ruang lingkup
3. Definisi
4. Referensi
5. Informasi umum
6. Pedoman implementasi



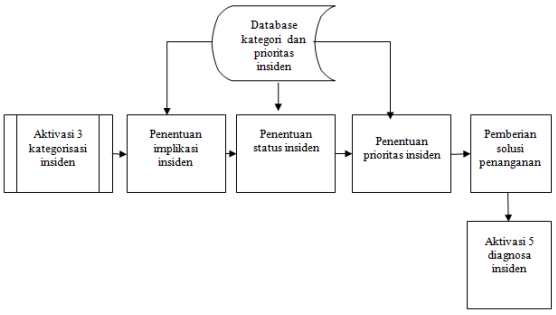

1. Identifikasi Insiden



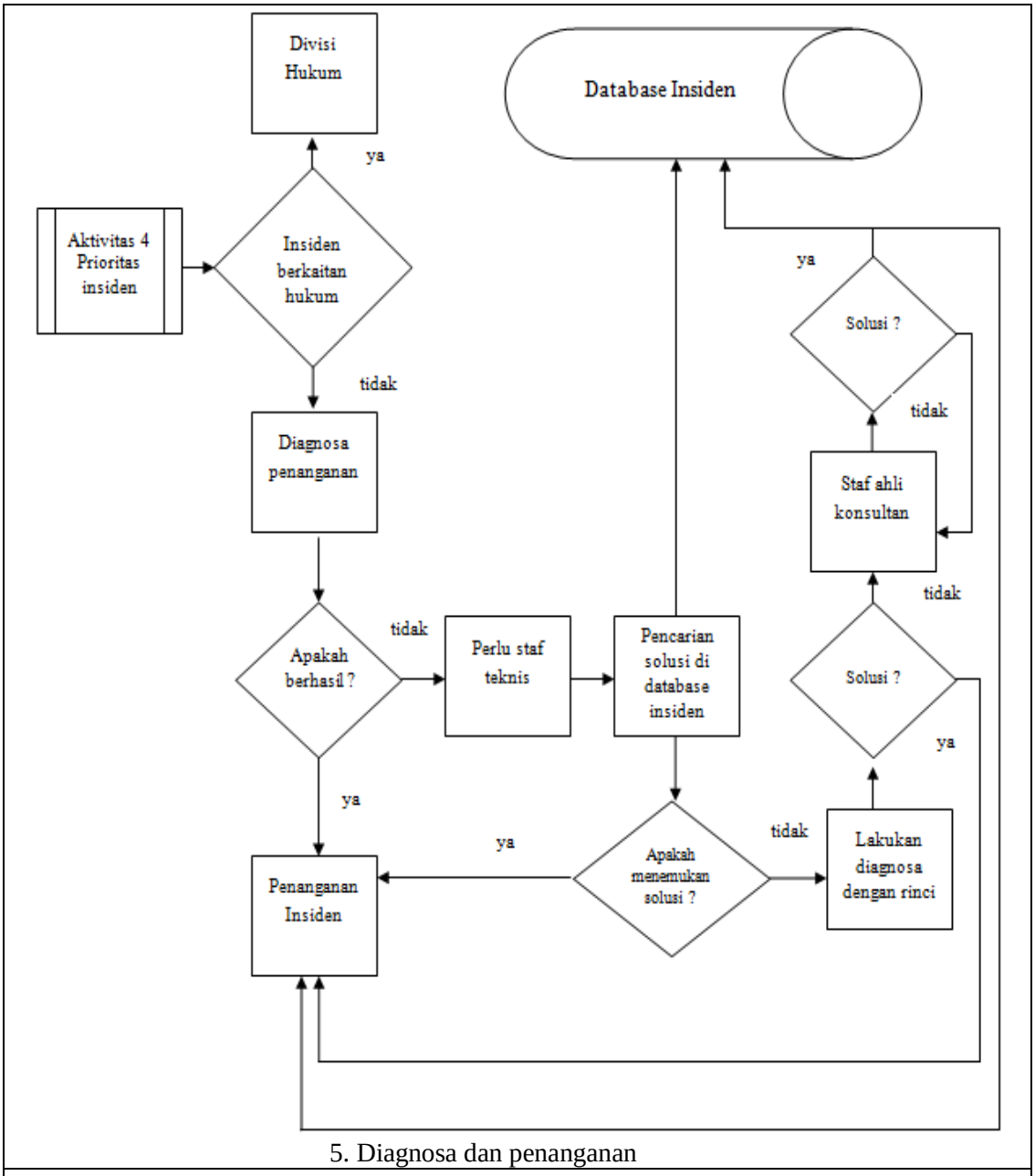

2. Pencatatan informasi insiden



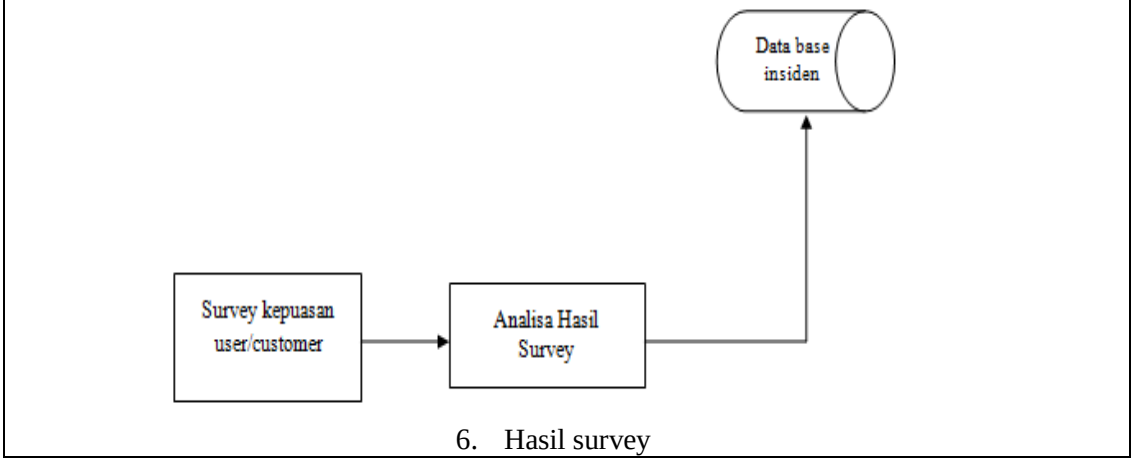

3. Pengkategorian insiden




4. Penentuan Status insiden




5. Diagnosa dan penanganan




6. Hasil survey

Untuk analisa kelengkapan sesuai dengan standarisasi ISO/IEC 27002 dapat dilihat pada table dibawah ini :

**Tabel V.1 Analisa kelengkapan dengan ISO/IEC 27002**

| No | Kriteria | ISO/IEC 27002 | Kelengkapan |
|---|---|---|---|
| 1 | Pengguna (karyawan, kontraktor dan pihak ketiga) | 13.1 | √ |
| 2 | Adanya saluran manajemen pelaporan | 13.1.1 (C) | √ |
| 3 | Adanya titik kontak yang dikenal | 13.1.1 (IG) | √ |
| 4 | Adanya umpan balik penanganan insiden | 13.1.1 (IG - a) | √ |
| 5 | Adanya media untuk mengingat kejadian keamanan informasi yang terjadi | 13.1.1 (IG - b) | √ |
| 6 | Melakukan perincian pelaporan | 13.1.1 (IG - c(a)) | √ |
| 7 | Insiden dilaporkan ke titik kontak | 13.1.1 (IG - c(b)) | √ |
| 8 | Adanya sistem alarm (insiden yang berat) | 13.1.1 (IG ) | √ |
| 9 | Mekanisme pelaporan mudah diakses | 13.1.2 (IG) | √ |
| 10 | Kejelasan tanggungjawab setiap prosedur | 13.2.1 (C) | √ |
| 11 | Prosedur harus menangani berbagai macam insiden | 13.2.1(IG - a) | √ |
| 12 | Prosedur mencakup analisa dan identifikasi insiden | 13.2.1(IG - b) | √ |
| 13 | Prosedur mencakup penahanan (hukum) | 13.2.1(IG - b) | √ |
| 14 | Prosedur mencakup perencanaan tindakan korektif | 13.2.1(IG - b) | √ |
| 15 | Pelaporan kepada pihak yang tepat | 13.2.1(IG - b) | √ |
| 16 | Prosedur mencakup pengumpulan bukti | 13.2.1(IG - c) | √ |
| 17 | Prosedur mencakup boleh tidaknya akses terhadap data | 13.2.1(IG - d) | √ |
| 18 | Prosedur mencakup laporan pihak ketiga jika insiden berasal dari luar | 13.2.1(OI) | √ |
| 19 | Prosedur mencakup identifikasi jenis, volume dan biaya insiden | 13.2.2(C) | × |
| 20 | Prosedur mencakup pencatatan insiden dan penanggulangan | 13.2.2(IG) | √ |
| 21 | Prosedur harus mencakup pengumpulan bukti (hukum) | 13.2.3(C) | √ |
| 22 | Prosedur meliputi identifikasi bukti (hukum) | 13.2.3(IG) | √ |

**Keterangan :**

**C = *Control***

**IG = *Information Guide***

**OI = *Other Information***

## 5. KESIMPULAN

Pada penelitian yang telah dilakukan oleh penulis dapat diambil kesimpulan sebagai berikut :

1. Faktor utama yang menyebabkan terjadinya insiden adalah tidak segeranya melaporkan setiap insiden yang terjadi berdasarkan hasil *survey* yaitu 73,3% .
2. Minimal formulir pelaporan terdapat informasi pelapor, waktu terjadi insiden, jenis serangan (insiden), deskripsi insiden, perangkat yang diserang dan *log file*.
3. SOP yang telah dibuat 95,5 % memenuhi standarisasi ISO/IEC 27001 dan 27002 dari sudut pandang kelengkapan proses pelaporan insiden yang terjadi.

## DAFTAR PUSTAKA


[1] John D. Howard, "An Analysis Of Security Incidents On The Internet 1989 - 1995," PhD thesis, Engineering and Public Policy, Carnegie Mellon University, 1997.

[2] NPO Japan Network Security Association," Information Security Incident Survey Report", Security Incident Investigation Working Group , Japan ,2010.

[3] Alkazimy, A.," Peran ID-CERT dan Tren Keamanan Informasi di Cyber Space", Rapat Kerja Nasional (Rakernas) APJI, Indonesia, 2011.

[4] ISO copyright office,"Information technology – Security techniques – Code for practice for information security management", ISO/IEC 1799:2005 International Standard, Switzerland, 2005.

[5] Indrajit, R.,E., "ISO 1799. Kerangka Standard Keamanan Informasi", ABFI Institut Perbanas.

[6] _____, "ISO 27000 Series",[online] http://www.itgovernanceonline.com/information-security/iso-27000-series/. diakses 29 Januari 2012.

[7] Notohadiprawiro, T., Seminar Nasional Plantagama, Fakultas Pertanian UGM. 27 Oktober 1990.

[8] Syafrizal, M., Seminar Nasional Teknologi 2007 (SNT 2007) , Yogyakarta, 24 November 2007.

[9] BSN (Badan Standarisasi Nasional), SNI 7512 – 2008, Teknologi informasi – Teknik keamanan – Pengelolaan insiden keamanan Informasi "Information technology – Security techniques – Information security incident management (ISO/IEC TR 18044:2004, MOD)" ICS 35.040.

[10] U.S. Environmental Protection (EPA), Guidance for Preparing Standard Operating Procedures (SOPs), EPA/600/B-07/001, April 2007.

[11] Reeuwijk, L., P., V., Guidelines for quality management in soll and plant laboratories ,Belanda. 2001.

[12] ICT Policy and Coordination Office,Departement of Publick Works,Queensland Government

[13] HPCT Information Security Event Reporting, Control and Management Procedures

[14] ____, "Mission Statement", [online], http://oit.wvu.edu/infosecurity/mission-statement/ , diakses 30 januari 2012

[15] MnSCU(Minnesota State Colleges and Universities), "Incident Handling Applied Risk Management", September 2002.

[16] ____, "Information Security Management", [online] "http://www.toshiba.co.jp/csr/en/fair_practices/security.htm, diakses 30 januari 2012.

[17] ____, "ISO 27001 Home", [online], http://iso27001security.com, diakses 30 januari 2012

[18] ____, "What are Policies,Standards,Guidelines and Procedures ?", [online], "http://mindfulsecurity.com/2009/02/03/policies-standards-and-guidelines/, diakses 1 pebruari 2012

[19] ____, "ISO IEC 27002 2005 Introduction", [online], http://www.praxiom.com/iso-17799-intro.htm , diakses 2 pebruari 2012

[20] ____, "information Security",[online], http://www.exin-security.com/en GB/ continual-protection.html, diakses 2 pebruari 2012.