BAB I

PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

Pada sub bab ini akan dijelaskan mengenai gambaran umum objek penelitian seperti profil, logo, visi dan misi instansi

1.1.1 Profil Instansi

Pusat Penelitian Jalan dan Jembatan Kementerian Pekerjaan Umum dan Perumahan Rakyat adalah instansi Pemerintahan yang bergerak di bawah koordinasi Balitbang Kementerian Pekerjaan Umum dan Perumahan Rakyat. Untuk selanjutnya Pusat Penelitian Jalan dan Jembatan Kementerian Pekerjaan Umum dan Perumahan Rakyat ini disingkat dengan Pusjatan.

Pusjatan adalah pusat riset teknologi dan pengembangan di bidang jalan dan jembatan yang berskala nasional dan satu satunya di indonesia. Pusjatan melakukan aktifitas riset dan penyelidikan sebagai pengembangan dari teknologi yang digunakan untuk membuat struktur dan material yang digunakan untuk membuat jalan dan jembatan. Beberapa mitra dalam negeri yang bekerjasama dengan Pusjatan adalah Direktorat Jendral Bina Marga, PT. Jasa Marga, PT. Marga Mandala Sakti, PT. Citra Marga Nusaphala Persada, Pemerintah Pusat dan Daerah dan beberapa mitra perusahaan lainnya. Selain menjalin kemitraan dengan instansi dan perusahaan dalam negeri, beberapa negara lain menjadi mitra dengan Pusjatan seperti Jepang, Korea, Australia, Singapur, Jerman dan Afganistan.

Pusjatan menggunakan sumber dana APBN murni pemerintah pusat. Latar belakang pendidikan pegawai Pusjatan mulai tingkatan SMA/SMK hingga S3. Pegawai Pusjatan adalah pegawai negeri sipil yang memiliki batas pensiun umur 58 Tahun. Pusjatan memiliki tugas utama dalam pelaksanaan penelitian, pengembangan dan penerapan Iptek di bidang jalan dan jembatan seperti yang tertuang dalam Peraturan Menteri Pekerjaan Umum No. 08/PRT/M/2010 Pasal 856, sebagai Pusat Penelitian dan Pengembangan Jalan dan Jembatan yang mempunyai tugas penelitian dan pengembangan serta penerapan ilmu pengetahuan dan

teknologi di bidang jalan dan jembatan. Kantor Pusjatan berlokasi di JL. A. H. Nasution No.264, Ujung Berung, Bandung.

Berikut ini adalah logo Kementerian Pekerjaan Umum dan Perumahan Rakyat, seperti pada gambar 1.1.

Gambar 1.1 Logo Kementerian Pekerjaan Umum dan Perumahan Rakyat

(sumber: https://www.pu.go.id)

Berikut adalah visi dan misi Pusjatan:

- **Visi :** rumusan visi PUSJATAN menginduk pada visi jangka panjang Badan Balitbang Kementerian Pekerjaan umum dan Perumahan rakyat, yaitu; *'Tersedianya IPTEK untuk mendukung penyelenggaraan infrastruktur Bidang Pekerjaan Umum dan Permukiman yang Andal'*.
- **Misi :**Meneliti dan mengembangkan teknologi bidang jalan dan jembatan yang inovatif, aplikatif, dan berdaya saing.
    1. Memberikan pelayanan teknologi dalam rangka mewujudkan jalan dan jembatan yang handal.
    2. Menyebarluaskan dan mendorong pernerapan hasil Litbang Jalan dan Jembatan.

1.1.2 Lingkup Kegiatan

Pusjatan adalah Badan Riset Nasional berbentuk instansi pemerintah maka dalam proses kegiatan nya pusjatan bukanlah institusi yang berbasis *profitable*, berikut ini adalah lingkup kegiatan dari Pusjatan:

- Penelitian dan Pengembangan
  1. Teknis dan manajemen pembangunan infrastruktur.
  2. Peralatan dan instrumen untuk keperluan manufaktur mendukung pembangunan infrastruktur.
  3. Sistem informasi infrastruktur.
  4. Analisis laboratorium dan pengujian.
  5. Standarisasi.
- Pelayanan Jasa Konsultasi
  1. Advis Teknik.
  2. Pengujian.
  3. Perencanaan dan Perancangan.
  4. Survei dan Investigasi.
- Alih Teknologi
  1. Pelatihan dan Diseminasi.
  2. Peningkatan mutu teknisi dan laboratorium di daerah.
  3. Pengembangan kerjasama penelitian dan pengembangan dengan berbagai pihak.

1.2 Latar Belakang Penelitian

Keamanan informasi saat ini adalah hal yang sangat penting. Organisasi saat ini sudah banyak yang menerapkan sistem TI sebagai pendukung proses kegiatan bisnisnya. Salah satu elemen penting dalam tata kelola perusahaan yang baik adalah tata kelola Teknologi Informasi, termasuk didalamnya adalah tata kelola kemanan informasi. "Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (business continuity), meminimalisasi resiko bisnis (reduce business risk) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis" ISO 27001 dalam Sarno dan Iffano (2009:27). Ancaman yang dimaksud adalah dampak yang ditimbulkan atas terjadinya sesuatu yang mengancam 3 aspek keamanan informasi yaitu *Confidentiality, Integrity, Availability* (CIA).

Saat ini kemajuan teknologi informasi di Indonesia terus berkembang, hal ini diperkuat dengan yang dikemukakan oleh Sarno dan Iffano (2012:4), pengguna internet di indonesia berkisar 20 juta an, dan terus mengalami peningkatan 2% - 3% pertahunnya. Dibalik sebuah kemajuan teknologi terdapat pula sisi negatif seiring dengan perkembangannya. Dalam sebuah kutipan di halaman interpol.go.id menyebutkan bahwa *"crime is a product of society its self",* masyarakat sendirilah yang melahirkan sebuah kejahatan, semakin tinggi tingkat intelektualitas masyarakat maka semakin canggih pula tindak kejahatan yang terjadi. Semakin tinggi penguasaan TI maka semakin canggih pula jenis tindak kejahatan di bidang TI. Beberapa bentuk kejahatan *cyber* yang sering terjadi adalah *unaothorized* akses kedalam sistem dan layanan komputer, *data forgery, data espionage* dll. Bentuk kejahatan yang menjadi ancaman keamanan informasi dapat berupa fisik maupun *logic*, maka diperlukan sebuah *win win solution* yang melindungi fasilitas dan konten sistem informasi.

Menurut hasil sosialisasi dan survey keamanan informasi yang dilakukan oleh Kominfo menemukan bahwa mayoritas instansi pemerintah belum memiliki standar kerja keamanan informasi atau sedang menyusun standar keamanan informasi yang sesuai dengan standar SNI ISO/IEC 27001. Bahkan, beberapa

instansi yang sudah memiliki manajemen keamanan informasi pun masih belum mengetahui apakah kerangka kerja yang mereka miliki sudah sesuai dengan SNI ISO/IEC 27001 karena belum melakukan auditing secara independent (Kominfo,2011;7). Walaupun sudah memiliki kebijakan terkait keamanan informasi, saat ini Pusjatan sedang menyusun standar keamanan informasi yang sesuai dengan standar ISO/IEC 27001 hal ini dilakukan dengan maksud meningkatkan pelayanan terhadap publik dan sistem manajerial di Pusjatan.

Sistem manajemen keamanan infromasi pada sebuah organisasi adalah hal yang fundamental. Terdapat beberapa referensi standar keamanan informasi yang sudah diakui secara internasional yaitu ISO 27001, PCIDSS, dan COBIT yang dikeluarkan oleh ISACA. Kominfo sudah mengeluarkan standar yang diadaptasi dari ISO/IEC 27001 yaitu SNI ISO/IEC27001. Beberapa hal penting yang patut dijadikan pertimbangan mengapa standar ISO 27001 dipilih karena dengan standar ini sangat fleksibel dikembangkan karena sangat tergantung dari kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis dan jumlah pegawai dan ukuran struktur organisasi serta ISO 27001 menyediakan sertifikat implementasi Sistem Manajemen Keamanan Informasi yang diakui secara internasional yang disebut Information Security Management System (ISMS) certification Sarno dan Iffano(2009: 59).

ISO/IEC 27001 adalah standar yang populer secara global, dalam survey yang dilakukan oleh Gartner (2011:4) pada tahun 2011 lebih dari 7500 organisasi sudah disertifikasi (terdapat lebih dari 3.900 organisasi di jepang), dalam survey nya tersebut 29% dari responden mengatakan mereka mendukung dan akan mempertimbangkan pengembangan dari penggunaan standar keluarga ISO/IEC 2700X, 20% dari responden memilih *Statement on Auditing Standards* (SAS), 19% responden memilih standar COBIT dan 17% responden memilih PCIDSS. Negara yang memiliki presentase tertinggi penggunaan ISO 27001/27002 adalah United Kingdom dan India dengan presentase organisasi pengguna mencapai 42%, 40% organisasi di Jepang menggunakan standar ISO 27001/27002, di tempat ketiga dengan presentase 37% adalah Jerman, Australia dengan presentase 27%, United

states dengan presentase 22%, dan Canada dengan presentase organisasi pengguna 14%.

Kebijakan dan komitmen adalah hal yang mendasar dalam sebuah organisasi, terkait dengan upaya peningkatan keamanan informasi dan meningkatkan kepercayaan pelanggan, pihak ke 3 dan seluruh stakeholder yang terkait dengan organisasi, maka setiap kebijakan harus dilakukan *review* dan di dokumentasikan dengan baik. Setiap proses kegiatan yang dilakukan haruslah mengacu pada kebijakan keamanan informasi.

Merujuk pada panduan tata kelola KIPPP yang diterbitkan oleh Kominfo, pengertian aset informasi adalah pengetahuan atau data yang memiliki nilai bagi organisasi (Kominfo,2011:24). Aset pun menjadi hal penting dalam upaya peningkatan kualitas keamanan informasi. Pengelolaan aset infromasi ,dokumentasi aset, dan pemetaan otoritas user harus sesuai dengan tanggung jawab dan batasan pengguna. Salah satu klausul keamanan informasi adalah keamanan fisik dan lingkungan, ada beberapa hal terkait di Pusjatan yang belum di implementasi dengan baik seperti pengawasan terhadap tamu atau orang asing di sekitar lingkungan Pusjatan.

Berikut ini adalah beberapa temuan hasil observasi yang terkait dengan sistem manajemen keamanan informasi di kantor Pusjatan:

1. Kebijakan penguncian komputer pengguna menggunakan password belum/tidak ada. Kebijakan penguncian komputer adalah salah satu upaya dalam menjaga keamanan informasi yang di implementasikan dalam tingkat user. Selain kebijakan, sosialisasi pun diperlukan terkait dengan kebijakan penguncian komputer karyawan Pusjatan, hal ini dilakukan agar kebijakan tersebut dapat diimplementasikan secara optimal dan timbul nya *awareness* dari pegawai Pusjatan terkait dengan keamanan informasi.
2. Komputer pengguna dapat mengakses semua situs tanpa ada situs yang diblokir. Akses kontrol di kantor Pusjatan masih lemah, hal ini terbukti dengan tidak adanya pembatasan situs yang dapat diakses oleh pegawai.

Pembatasan akses sangat diperlukan untuk mencegah penyalahgunaan otoritas serta tanggung jawab terhadap informasi dan mencegah bocornya rahasia negara yang bersifat sensitif dan strategis ke publik.

3. Pengawasan pihak keamanan terhadap pihak ketiga kurang ketat mulai gerbang masuk hingga lokasi gedung dimana ruang server berada. Pengawalan dan rintangan yang dilakukan oleh tenaga keamanan dinilai kurang maksimal.
4. Pemetaan lokasi server yang rentan terhadap ancaman lingkungan external kantor. Menurut hasil observasi yang dilakukan, penempatan ruang server dirasa kurang tepat, karena ruang server berada dalam satu gedung yang digunakan oleh divisi tata usaha, dimana banyaknya kepentingan orang pihak ke 3 dengan divisi tersebut. Selain itu, penempatan lokasi ruang server sangat dekat dengan pintu utama gedung yang mudah dijangkau oleh orang yang tidak memiliki kepentingan, serta pengamanan fisik disekitar gedung kurang maksimal.
5. Ditemukannya APAR yang sudah masuk masa kadaluwarsa di gedung server berada. Menurut hasil observasi yang dilakukan pada masa magang, ditemukannya beberapa APAR yang sudah melewati masa kadaluwarsa, hal ini tidak sesuai dengan syarat keamanan informasi klausul keamanan fisik dan lingkungan.

Berikut ini adalah beberapa alasan mengapa kantor Pusjatan perlu mengimplementasikan standar Sistem Manajemen Keamanan Informasi ISO 27001:

1. Membantu organisasi terhadap kesesuaian kebutuhan standar keamanan informasi yang sudah teruji.
2. Membuat pengaruh positif dalam hal citra organisasi, nilai dan persepsi yang baik dari pihak lain.

3. Memastikan bahwa organisasi memiliki kontrol-kontrol keamanan informasi terhadap lingkungan dan proses bisnisnya yang mungkin menimbulkan resiko atau gangguan.
4. Meningkatkan kepercayaan pelanggan, pihak ketiga dan seluruh stakeholder yang terkait dengan kegiatan organisasi.
5. Meningkatkan efektivitas dan keandalan pengamanan informasi.

Terkait beberapa temuan tersebut dan merujuk pada rencana implementasi standar ISO/IEC 27001:2013 yang akan dilakukan pada kantor Pusjatan dan dalam upaya pengembangan keamanan informasi tersebut, maka diperlukan sebuah pengukuran nilai kematangan keamanan informasi yang dilakukan melalui audit keamanan informasi secara teliti dan independen, pada penelitian ini menggunakan referensi ISO/IEC 27001:2013 sebagai panduan auditing dengan objek divisi IT Pusjatan.

1.3 Perumusan Masalah

Berdasarkan latar belakang permasalahan tersebut, maka dapat dirumuskan permasalahan sebagai berikut:

1. Klausul *Information security policies* di Pusjatan masih menggunakan kebijakan IT Pusjatan.
2. Klausul *Asset management* di Pusjatan masih mengacu pada kebijakan IT Pusjatan.
3. Klausul *Physical and Environmental securities* di Pusjatan masih mengacu pada kebijakan IT Pusjatan.
4. Klausul *Access Control* di Pusjatan masih mengacu pada kebijakan IT Pusjatan.

1.4 Pertanyaan Penelitian

Berdasarkan rumusan masalah tersebut, maka pertanyaan penelitian ini adalah sebagai berikut:

1. Apakah kebijakan keamanan informasi pada kantor Pusjatan sudah sesuai dengan kebutuhan instansi dan sesuai dengan standar ISO?

2. Bagaimana tingkat kematangan dan *gap analysis* klausul Kebijakan Keamanan Informasi, Manajemen Asset, Akses Kontrol, dan Keamanan Fisik dan Lingkungan yang ada di Pusjatan dikaitkan dengan standar ISO/IEC 27001:2013?

1.5 Tujuan Penelitian

Sesuai dengan rumusan masalah yang telah diutarakan pada sub-bab sebelumnya maka dapat di ketahui bahwa tujuan analisis dari kegiatan auditing ini adalah sebagai berikut:

1. Membuat pengukuran dan analisa tingkat kematangan klausul *information security policies* dengan objek divisi IT Pusjatan berdasarkan ISO/IEC 27001:2013.
2. Membuat pengukuran dan analisa tingkat kematangan klausul *Asset management* dengan objek divisi IT Pusjatan berdasarkan ISO/IEC 27001:2013.
3. Membuat pengukuran dan analisa tingkat kematangan klausul *Physical and Environmental Security* dengan objek divisi IT Pusjatan berdasarkan ISO/IEC 27001:2013.
4. Membuat pengukuran dan analisa tingkat kematangan klausul *Access control* dengan objek divisi IT Pusjatan berdasarkan ISO/IEC 27001:2013.
5. Membuat rekomendasi berdasarkan hasil dari *work gap paper analysis.*

1.6 Manfaat Penelitian

Penelitian ini diharapkan dapat membawa *impact* yang positif bagi berbagai pihak terkait, baik dari segi toritis maupun segi praktis sebagai berikut:

- Segi Teoritis

  Hasil penelitian ini diharapkan dapat dijadikan rujukan untuk selanjutnya dapat dikembangkan kembali pada penelitian selanjutnya selain itu dapat:

  a) Menambah pengetahuan keilmuan terkait dengan kebijakan keamanan informasi pada sebuah organisasi khususnya instansi pemerintahan.

b) Menambah pengetahuan keilmuan terkait dengan manajemen aset dalam koridor keamanan informasi pada sebuah organisasi khususnya instansi pemerintahan.
c) Menambah pengetahuan keilmuan terkait dengan keamanan fisik dan lingkungan dalam aktivitas menjaga keamanan informasi pada sebuah organisasi khususnya instansi pemerintahan.
d) Menambah pengetahuan keilmuan terkait dengan akses kontrol terkait dengan implementasi keamanan informasi pada sebuah instansi pemerintahan.

- Segi praktis

  Hasil penelitian ini diharapkan dapat memberikan laporan temuan dan referensi bagi Pusjatan terkait evaluasi keamanan informasi dengan :

  1. Kebijakan keamanan informasi yang akan atau sudah dibuat dan dikomentasikan.
  2. Akses kontrol.
  3. Pengelolaan aset manajemen.
  4. Keamanan fisik dan lingkungan sekitar.

  Rekomendasi yang disertakan dapat digunakan sebagai bahan pertimbangan instansi dalam merumuskan dan menentukan kebijakan yang akan diambil sesuai dengan prinsip-prinsip keamanan informasi khususnya kebijakan dalam upaya peningkatan kematangan keamanan infomasi yang beredar dalam instansi.

1.7 Batasan Penelitian

Dalam upaya pencapaian kesempurnaan penelitian, maka ditentukanlah batasan-batasan dalam penelitian sebagai berikut:

- Aktivitas audit keamanan informasi hanya dilakukan pada divisi IT Pusjatan, hal-hal terkait lainnya yang berada diluar koridor divisi IT akan disesuaikan dengan kondisi yang terjadi di lapangan.

- Aktivitas audit keamanan informasi ini mengacu pada standar ISO/IEC 27001:2013 dan ISO 27002.
- Aktivitas audit keamanan informasi hanya dilakukan pada klausul yang sudah ditentukan dengan kontrol objek sebagai berikut:

1. *Information Security Policies*:
    a. *Policies for information security.*
    b. *Review and improvement of the policies for information security.*
2. *Asset Management:*
    a. *Responsibility for asset.*
    b. *Information classification.*
    c. *Media handling.*
3. *Physical and Environmental Security:*
    a. *Secure area.*
    b. *Equipment.*
4. *Access Control*
    a. *Business requirements of access control.*
    b. *User access management.*
    c. *User responsibilities.*
    d. *System and application access control.*
5. Seluruh kegiatan audit disesuaikan dengan kondisi lapangan, dengan mematuhi aturan dan hukum yang berlaku. Terkait dengan hal-hal yang dibatasi oleh instansi semua dilakukan untuk menjaga beberapa rahasia negara sesuai dengan tingkat kewajaran dan tanggung jawab yang dapat dipublikasikan.

1.8 Sistematika Penulisan

Penulisan laporan penelitian dilakukan secara sistematis sesuai dengan pedoman penulisan yang diterbitkan di tahun 2015, sebagai berikut:

- **BAB 1 Pendahuluan**

  Pada bab ini berisi profil instansi, latar belakang dan rumusan masalah yang menjadi gambaran awal objek penelitian.

- **BAB 2 Tinjauan Pustaka**

  Pada bab ini berisi teori-teori yang relevan dengan penelitian yang dilakukan dan penelitian terdahulu yang digunakan sebagai referensi, selain itu, pada bab ini pun berisi kerangka pemikiran yang melandaskan penelitian.

- **BAB 3 Metode Penelitian**

  Pada bab ini berisi pendekatan, metode, dan teknik yang digunakan untuk mengumpulkan, mengolah dan menganalisis data yang digunakan dalam penelitian guna menemukan dan menjelaskan permasalahan penelitian.

- **BAB 4 Hasil Penelitian dan Pembahasan**

  Pada bab ini berisi hasil temuan audit dan penjelasan yang menjabarkan permasalahan yang ditemukan dilapangan secara jelas dan *independent* dengan batasan-batasan yang sudah ditentukan.

- **BAB 5 Kesimpulan dan Rekomendasi**

  Pada bab ini berisi simpulan kegiatan audit dengan disertakan rekomendasi yang berguna untuk instansi sesuai dengan ruang lingkup penelitian.