AUDIT KEAMANAN INFORMASI: STUDI KASUS PT XYZ

INFORMATION SECURITY AUDIT: CASE STUDY PT. XYZ

Reza Zulfikar Ruslam[1] , Budi Yuwono[2], Ivano Aviandi[3] , dan Nur Indrawati [4]

[1]PT XYZ, Universitas Indonesia, Jl. Salemba Raya No. 4, Jakarta Pusat, [2]Kementerian Komunikasi dan Informatika R.I., Jl. Medan Merdeka Barat No. 17, Jakarta Pusat 10110
e-mail : rezazulfikarruslam@yahoo.com[1], e-mail: byuwono@gmail.com[2], iaviandi@gmail.com[3], dan e-mail: nurindrawati@gmail.com[4]

Naskah diterima tanggal 26 September 2013, direvisi tanggal 22 Oktober 2013, disetujui tanggal 5 November 2013

Abstract

PT XYZ is a provider of document management services, in cooperation with local/foreign banks. Documents containing customer information, so that information security should be set to provide services that meet information security criteria. Information security audit results showed weak information security, less monitored and evaluated. This research focuses on information security audit in accordance with ISO 27001 to provide comprehensive information security policies and procedures. The methodology used are assessment, risk analysis and impact, controls selection and recommendation of policies and procedures. Audit results showed a gap between policies and procedures that apply in PT XYZ with ISO 27001.

Keywords: *information SecurityAaudit, ISO 27001, PT XYZ Chase.*

Abstrak

PT XYZ merupakan penyedia layanan pengelolaan dokumen tagihan, bekerja sama dengan bank-bank lokal/asing. Dokumen tagihan berkaitan dengan informasi pelanggan bank, sehingga keamanan informasi perlu diatur untuk memberikan layanan yang memenuhi kriteria keamanan informasi. Hasil audit keamanan informasi menunjukkan keamanan informasi PT XYZ lemah, kurang terpantau dan dievaluasi. Penelitian ini berfokus pada audit keamanan informasi sesuai ISO 27001 untuk memberikan rekomendasi kebijakan dan prosedur keamanan informasi yang komprehensif. Metodologi yang digunakan adalah penilaian, analisis risiko dan dampak, pemilihan kontrol-kontrol serta rekomendasi kebijakan dan prosedur. Hasil audit menunjukkan adanya kesenjangan antara kebijakan dan prosedur yang berlaku di PT XYZ dengan ISO 27001.

Kata kunci: Audit Keamanan Informasi, ISO 27001, Kasus PT XYZ.

PENDAHULUAN

Latar Belakang

PT XYZ merupakan perusahaan yang bergerak di bidang layanan pengelolaan dokumen. Proses bisnis utamanya yaitu percetakan *billing statement* atau rekening koran dan penyediaan jasa kurir. Dalam menjalankan bisnisnya, PT XYZ bekerja sama dengan beberapa bank di Indonesia (lokal) dan bank asing, salah satunya adalah Bank ABC. Bank ABC, sebagai salah satu pelanggan PT XYZ merupakan bank yang sudah melakukan sertifikasi ISO 27001. Bank ABC melakukan audit keamanan informasi pada PT XYZ selama kurang lebih 2 (dua) bulan, yaitu dari bulan Februari 2012 sampai dengan bulan Maret 2012. Di mana Bank ABC melakukan audit keamanan informasi di PT XYZ, yang meliputi audit terhadap informasi yang diterima, informasi yang diproses, serta informasi yang dicetak dan didistribusikan kepada pelanggan sesuai alamat pelanggan.

Hasil audit Bank ABC berbeda dengan ekspektasi Divisi Teknologi Informasi (TI) PT XYZ selama ini. Sesuai hasil audit keamanan informasi tersebut, keamanan informasi PT XYZ dinilai masih lemah. Selain itu, monitoring dan evaluasi dari pihak yang berwenang dinilai masih kurang, sehingga kriteria keamanan informasi belum terpenuhi. Kurangnya monitoring dan evaluasi ini menjadi salah satu penyebab masalah belum terpenuhinya kriteria keamanan informasi di PT XYZ. Belum tercapainya kriteria keamanan informasi salah satunya disebabkan karena belum adanya kebijakan dan prosedur keamanan informasi komprehensif, baik yang berlaku pada tingkat operasional (teknis) maupun manajerial.

Ekspektasi divisi TI selama ini adalah keamanan informasi perusahaan sudah baik (aman), begitu pula dengan keamanan informasi pelanggan. Hal ini ditunjang dari adanya kebijakan dan prosedur keamanan informasi yang berlaku di PT XYZ. Ditinjau dari hasil audit bank tersebut, divisi TI memutuskan melakukan audit kepatuhan keamanan informasi untuk menguji apakah tingkat kepatuhan keamanan informasi perusahaan terhadap visi dan misi *best services* terhadap pelanggan yang sudah memenuhi aspek keamanan informasi dan menguji penga- ruhnya terhadap keamanan informasi perusahaan dan pelanggan. Dari hasil audit kepatuhan keamanan informasi ini, nantinya didapatkan kebijakan dan prosedur yang lemah sehingga dapat diberikan rekomendasi kebijakan dan prosedur yang lebih komprehensif sesuai standar internasional ISO 27001.

Permasalahan yang dihadapi dalam penelitian ini yaitu divisi TI PT. XYZ mengalami kesulitan untuk mengetahui batasan-batasan atau ruang lingkup audit yang digunakan oleh bank ABC, sehingga divisi TI hanya terbatas pada audit kepatuhan keamanan informasi terhadap visi dan misi *best services* perusahaan. Jika di tengah jalan didapatkan kebijakan dan prosedur yang lemah maka akan direkomendasikan kebijakan dan prosedur baru. Untuk itu penelitian ini ditujukan untuk menjawab pertanyaan penelitian sebagai berikut:

a. Apakah kepatuhan perusahaan terhadap visi dan misi *best services* terhadap pelanggan sudah memenuhi aspek keamanan informasi?
b. Apakah Kebijakan dan prosedur yang ada sudah dapat dikatakan *best services* terhadap aspek keamanan informasi?
c. Apakah rekomendasi kebijakan dan prosedur yang akan dibuat dapat meningkatkan keamanan informasi?

Penelitian ini dilakukan untuk menyelesaikan permasalahan keamanan informasi melalui audit keamanan informasi dengan memberikan rekomendasi perbaikan kebijakan dan prosedur keamanan informasi sehingga lebih komprehensif sesuai praktik terbaik dan standar internasional keamanan informasi, ISO/IEC 27001: 2005, serta

terpenuhinya kriteria keamanan informasi di lingkungan PT XYZ dan pada akhirnya dapat mendukung PT XYZ dalam memberikan *best services* pengelolaan dokumen kepada pelanggan sesuai dengan visi dan misi PT XYZ. Sedangkan ruang lingkup dan batasan dalam penelitian ini yaitu hanya terbatas pada audit kepatuhan keamanan informasi untuk memberikan rekomendasi kebijakan dan prosedur guna meningkatkan keamanan informasi di lingkungan PT XYZ sesuai dengan hasil audit yang dilakukan oleh peneliti. Penelitian ini tidak mencakup implementasi, monitoring, dan evaluasi dari rekomendasi perbaikan kebijakan dan prosedur. Data dan informasi yang dimaksud dalam penelitian ini adalah data dan informasi yang dikelola oleh PT XYZ. Kerangka kerja dan standar yang menjadi dasar dalam penyusunan kebijakan dan prosedur adalah ISO/IEC 27001: 2005. Dalam penelitian ini tidak dibahas mengenai pemasalahan *outsourcing* SI/TI di lingkungan PT XYZ dan keamanan informasi dalam pengiriman dokumen yang dilakukan oleh kurir. Sedangkan *best services* atau layanan terbaik yang dimaksud dalam penelitian ini adalah pelayanan terhadap keamanan informasi.

Tujuan Penelitian

Berdasarkan pada permasalahan penelitian yang telah dikemukakan sebelumnya, maka tujuan dari penelitian ini adalah :

a. Mengetahui apakah kepatuhan perusahaan terhadap visi dan misi *best services* terhadap pelanggan sudah memenuhi aspek keamanan informasi.
b. Mengetahui apakah kebijakan dan prosedur yang ada sudah dapat dikatakan *best services* terhadap aspek keamanan informasi.
c. Mengetahui Apakah rekomendasi kebijakan dan prosedur yang akan dibuat dapat meningkatkan aspek keamanan informasi.

Tujuan yang ingin dicapai dalam penelitian ini yaitu:

a. Mengetahui apakah kepatuhan perusahaan terhadap visi dan misi *best services* terhadap pelanggan sudah memenuhi aspek keamanan informasi.
b. Mengetahui apakah kebijakan dan prosedur yang ada sudah dapat dikatakan *best services* terhadap aspek keamanan informasi.
c. Mengetahui Apakah rekomendasi kebijakan dan prosedur yang akan dibuat dapat meningkatkan aspek keamanan informasi.

Tinjauan Pustaka

Keamanan Informasi

Keamanan informasi merupakan salah satu hal penting yang perlu diperhatikan oleh perusahaan. Kebocoran informasi dan kegagalan sistem dapat menyebabkan kerugian baik dari sisi finansial maupun produktivitas perusahaan. Keamanan informasi meliputi suatu mekanisme untuk mengontrol akses dan penggunaan basis data pada level objek, keamanan informasi pada pengguna, di mana pengguna tersebut memiliki akses informasi tertentu. Pengaturan mengenai keamanan informasi terutama akan ditentukan berdasarkan seberapa jauh tingkat keamanan yang akan dibangun untuk informasi dalam basis data. Tingkat keamanan informasi juga bergantung pada tingkat sensitivitas informasi dalam *database*, biasanya informasi yang tidak terlalu sensitif sistem keamanannya tidak ketat sedangkan informasi yang sangat sensitif perlu pengaturan keamanan yang ketat untuk akses ke informasi tersebut (Mufadhol, 2009). Sebagai sebuah sistem, keamanan informasi harus didukung oleh keberadaan dari hal-hal berikut (Syafrizal, 2007):

a. Struktur organisasi

   Struktur organisasi biasanya berupa keberadaan fungsi-fungsi atau jabatan

organisasi yang terkait dengan keamanan informasi. Misalnya; *Chief Security Officer*, teknisi keamanan informasi, dan beberapa posisi lainnya.

b. Kebijakan keamanan

Kebijakan keamanan atau dalam bahasa Inggris disebut sebagai *Security Policy*. Contoh kebijakan keamanan ini misalnya adalah sebagai berikut: Semua kejadian pelanggaran keamanan dan setiap kelemahan sistem informasi harus segera dilaporkan dan administrator harus segera mengambil langkah-langkah keamanan yang dianggap perlu. Akses terhadap sumber daya pada jaringan harus dikendalikan secara ketat untuk mencegah akses dari yang tidak berhak. Akses terhadap sistem komputasi dan informasi serta periferalnya harus dibatasi dan koneksi ke jaringan, termasuk log-on pengguna, harus dikelola secara benar untuk menjamin bahwa hanya orang/ peralatan yang diotorisasi yang dapat terhubung ke jaringan.

c. Prosedur dan proses

Prosedur dan proses yaitu semua prosedur serta proses-proses yang terkait pada usaha-usaha pengimplementasian keamanan informasi di suatu perusahaan atau organisasi. Misalnya prosedur permohonan izin akses aplikasi, prosedur permohonan domain akun untuk staf atau karyawan baru, prosedur akses data atau file tertentu, dan lain sebagainya.

d. Tanggung jawab

Yang dimaksud dengan tanggung jawab atau *responsibility* terkait keamanan informasi adalah tercerminnya konsep dan aspek-aspek keamanan informasi perusahaan di dalam *job description* setiap jabatan dalam perusahaan. Begitu pula dengan adanya program-program pelatihan serta pembinaan tanggung jawab keamanan informasi untuk staf dan pimpinan perusahaan.

e. Sumber Daya Manusia

SDM merupakan pelaksana serta objek pengembangan keamanan informasi di perusahaan. Manusia yang bisa memperbaiki serta merusak semua usaha-usaha tersebut.

Menurut pendapat (Syafrizal, 2007) Keamanan Informasi terdiri dari 3 (tiga) prinsip atau kriteria, yaitu: *Confidentiality, Integrity* dan *Availability* (CIA). Pada awalnya prinsip keamanan informasi hanya CIA, namun seiring pertambahan waktu dan kebutuhan keamanan informasi, prinsip keamanan informasi diperluas menjadi CIA+ yaitu sebagai berikut:

Confidentiality

a. *Confidentiality a*dalah prinsip yang menjamin, memastikan dan menjaga kerahasiaan informasi, bahwa informasi hanya dapat diakses dan digunakan oleh orang yang mempunyai wewenang sekaligus menjamin informasi yang dikirim, diterima dan disimpan terjamin kerahasiaannya (Whitman & Mattord, 2010, p. 8). "*Confidentiality is the characteristic of information whereby only those with sufficient privilages and a demonstrated need may access certain information,"* (Whitman & Mattord, 2010, p. 6).

b. *Integrity*

*Integrity a*dalah prinsip yang menjamin informasi tidak dirubah, dimanipulasi, dimodifikasi maupun dihilangkan tanpa ijin dari pihak yang berwenang, serta menjaga keakuratan dan kesempurnaan informasi dan prosesnya (Whitman & Mattord, 2010, p. 8). "*Integrity is the quality or state of being whole, complete, and uncorrupted,"* (Whitman & Mattord, 2010, p. 6).

c. *Availability*

Availability adalah prinsip yang menjamin bahwa informasi akan tersedia ketika dibutuhkan, serta memastikan pihak yang berwenang dapat menggu-

nakan informasi yang dibutuhkan tanpa ada gangguan dari pihak lain (Whitman & Mattord, 2010, p. 8). "*Availability is the characteristic of information that enables user access to information in a usable format without interference or obstruction,"* (Whitman & Mattord, 2010, p. 7).

d. Privacy

Privacy adalah prinsip yang menjamin bahwa informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi digunakan hanya untuk tujuan tertentu oleh pemilik informasi pada saat informasi dikumpulkan (Whitman & Mattord, 2010, p. 8). "*Information that is collected, used, and stored by an organization is intended only for the purposes stated by the data owner at the time it was collected,"* (Whitman & Mattord, 2010, p. 7).

e. Identification

Identification adalah prinsip yang menjamin bahwa informasi memiliki karakteristik identifikasi ketika informasi dapat mengenali penggunanya. Identifikasi adalah langkah pertama dalam memperoleh akses ke informasi yang diamankan, dan berfungsi sebagai dasar untuk otentifikasi dan otorisasi (Whitman & Mattord, 2010, p. 8). "*An information system possesses the characteristic of identification when it is able to recognize individual users. Identification is the first step in gaining access to secured material, and it serves as the foundation for subsequent authentication and authorization,"* (Whitman & Mattord, 2010, p. 7).

f. Authentification

Authentification adalah prinsip yang menjamin bahwa saat otentifikasi terjadi ketika sistem dapat membuktikan bahwa pengguna memiliki hak klaim (Whitman & Mattord, 2010, p. 8). "*Authentication occurs when a control proves that a user possesses the identify that he or she claims,"* (Whitman & Mattord, 2010, p. 7).

g. Authorization

Authorization adalah prinsip yang menjamin bahwa pengguna telah mendapatkan otorisasi sehingga dapat mengakses, meng-*update* atau menghapus informasi (Whitman & Mattord, 2010, p. 8). "*After the identify of a user is authenticated, a process called authorization assures that the user has been specifically and axplicitly authorized by the proper authority to access, update, or delete the contents of information,"* (Whitman & Mattord, 2010, p. 8).

h. Accountability

Akuntabilitas dari informasi dikatakan eksis ketika sistem dapat menyajikan semua aktifitas terhadap informasi, dan siapa yang melakukan aktivitas itu (Whitman & Mattord, 2010, p. 8). "*Accountability of information exist when a control provides assurance that every activity undertaken can be attribute to a named person,"* (Whitman & Mattord, 2010, p. 8).

Audit Kepatuhan Keamanan Informasi

Audit kepatuhan adalah audit yang bertujuan untuk menilai kepatuhan terhadap hukum, aturan, regulasi, praktek yang sehat, kebijakan dan prosedur intern, atau standar yang berlaku. Manfaat audit kepatuhan adalah untuk mengetahui tingkat ketaatan suatu program atau kegiatan terhadap peraturan yang berlaku, juga untuk memberikan penghargaan bagi pengelola yang taat, dan member sanksi bagi yang melakukan pelanggaran, guna mendorong terselenggaranya tata kelola yang baik *(Good Corporate Governance)* di lingkungan perusahaan yang diaudit (Tim penyusun modul program pendidikan non

gelar auditor sektor publik, 2007). Audit kepatuhan yang dinilai adalah ketaatan semua aktivitas sesuai dengan kebijakan, aturan dan ketentuan yang berlaku. Audit kepatuhan juga berkaitan dengan kegiatan guna memperoleh dan memeriksa bukti-bukti untuk menetapkan apakah kegiatan operasional suatu entitas sudah memenuhi prosedur, standart dan aturan yang berlaku.

Prosedur audit merupakan alat bantu yang digunakan untuk mengidentifikasi sebuah peristiwa. Dalam proses audit ada 4 prosedur audit yang harus dilakukan yaitu inspeksi, observasi, penyelidikan, dan konfirmasi (Bastian, 2007). Beberapa prosedur audit yang dapat kita jumpai saat ini yaitu (Boynton, Johnson, & Kell, 2004) :

a. Inspeksi

   Merupakan pemeriksaan secara rinci dan spesifik terhadap dokumen atau kondisi fisik suatu dokumen. Prossedur ini banyak dilakukan oleh auditor.

b. Pengamatan

   Merupakan prosedur audit yang digunakan oleh auditor untuk melihat, memantau atau menyaksikan pelaksanaan suatu kegiatan.

c. Konfirmasi

   Merupakan bentuk penyelidikan yang memungkinkan auditor memperoleh informasi secara langsung dari pihak ketiga yang bebas, dalam hal ini auditor mendapatkan informasi langsung dari pihak luar atau disebut pihak ketiga yang bebas.

d. Permintaan keterangan

   Merupakan prosedur audit yag dilakukan dengan meminta keterangan secara lisan. Bukti audit yang dihasilkan oleh prosedur ini adalah bukti lisan dan dokumenter.

e. Penelusuran

   Dalam pelaksanaan prosedur auditing dan melakukan penelusuran informasi sejak mula-mula informasi tersebut direkam pertama kali dalam dokumen, dilanjutkan dengan pelacakan pengolahan informasi tersebut.

f. Pemeriksaan dokumen pendukung *(Vouching)*

   Merupakan prosedur audit yang meliputi:

   1. Inspeksi terhadap dokumen-dokumen yang mendukung suatu transaksi atau informasi keuangan untuk menentukan kewajaran dan kebenarannya.
   2. Pembandingan dokumen tersebut dengan catatan yang berkaitan.

g. Perhitungan *(Counting)*

   Prosedur ini meliputi:

   1. Penghitungan fisik terhadap sumber daya berwujud seperti persediaan di tangan.
   2. Pertanggungjawaban semua formulir bernomor urut cetak.

h. *Scanning*

   Merupakan review secara cepat terhadap dokumen, catatan, dan daftar untuk mendeteksi unsur-unsur yang tampak tidak biasa yang memerlukan penyelidikan lebih mendalam.

i. Pelaksanaan ulang *(Reperforming)*

   Merupakan pelaksanaan ulang *(reperforming)* perhitungan dan rekonsiliasi yang dibuat oleh pelanggan.

j. Teknik audit dengan bantuan komputer

   Apabila catatan pelanggan diselenggarakan dalam media elektronik, auditor perlu menggunakan teknik audit bantuan komputer *(computer-assisted audit techniques)* dalam menggunakan prosedur audit.

ISO/IEC 27001:2005

Standar internasional ISO/IEC 27001:2005 mengadopsi pendekatan proses untuk penetapan, penerapan, pengoperasian, pemantauan, pengkajian, pemeliharaan, dan perbaikan SMKI di suatu organisasi

(BSN, 2009). ISO 27001 mencakup semua jenis organisasi (seperti perusahaan swasta, lembaga pemerintahan, dan lembaga nirlaba). ISO 27001 menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memantau, menganalisa dan memelihara serta mendokumentasikan *Information Security Management System* (ISMS) dalam konteks risiko bisnis organisasi keseluruhan (Justanieah, 2009). ISO 27001 mendefenisikan keperluan-keperluan untuk Sistem Manajemen Keamanan Informasi (SMKI). ISMS atau SMKI yang baik akan membantu memberikan perlindungan terhadap gangguan pada aktivitas-aktivitas bisnis dan melindungi proses bisnis yang penting agar terhindar dari risiko kerugian atau bencana dan kegagalan serius pada pengamanan sistem informasi, implementasi ISMS ini akan memberikan jaminan pemulihan operasi bisnis akibat kerugian yang ditimbulkan dalam masa waktu yang relatif tidak lama.

Manajemen keamanan informasi pada ISO/IEC 27001:2005 (BSN, 2009) mengadopsi proses PDCA; plan (perencanaan Sistem Manajemen Keamanan Informasi (SMKI)), *do* (penerapan dan pengoperasian SMKI), *check* (pemantauan dan pengkajian SMKI), dan *act* (peningkatan dan pemeliharaan SMKI). SMKI mengatur masalah keamanan informasi untuk mencapai *Confidentially, Integrity, Availability* (CIA) (BSN, 2009). Pendekatan proses dalam membangun *Information Security Management System* (ISMS) atau Sistem Manajemen Keamanan Informasi (SMKI) dalam ISO/IEC 27001:2005 mengikuti proses PDCA (BSN, 2009). Proses perencanaan dan perancangan (*plan*) SMKI meliputi aktivitas membangun komitmen manajemen terkait keamanan informasi, menyusun kebijakan dan prosedur keamanan informasi, pemilihan kontrol dan penyusunan instruksi serta rencana kerja terkait keamanan informasi. Proses pengimplementasian *(do)* meliputi kebijakan, kontrol, dan rencana kerja manajemen keamanan informasi sesuai dengan rencana yang disusun pada tahap plan. Proses *check* memantauan pelaksanaan SMKI, mengevaluasi dan audit secara berkala terhadap rencana dan pelaksanaan SMKI. Proses *act* merupakan proses pengembangan dan *improvement* terhadap SMKI yang sudah disusun. Tahapan manajemen risiko keamanan informasi terdiri atas 6 (enam) proses, yaitu: identifikasi metode penilaian risiko, penentuan kriteria risiko, identifikasi risiko, analisis dan evaluasi risiko, identifikasi dan evaluasi pilihan mitigasi risiko, pemilihan kontrol, evaluasi serta monitoring (BSN, 2009).

ISO/IEC 27001:2005 memberikan model yang kokoh dalam menerapkan prinsip-prinsip keamanan informasi, yang meliputi: penilaian risiko, perencanaan keamanan, penerapan rencana keamanan, manajemen keamanan informasi, dan peninjauan ulang *(review)*. ISO/IEC 27001:2005 memberikan panduan proses manajemen risiko yang cukup fleksibel dikembangkan sesuai dengan kebutuhan organisasi, tujuan yang akan dicapai oleh organisasi, persyaratan keamanan yang diperlukan, proses bisnis organisasi, jumlah pegawai, ukuran, dan struktur organisasi (Sarno dan Iffano). Pengendalian dalam standar ISO/IEC 27001:2005 meliputi: kebijakan keamanan; organisasi keamanan informasi; pengelolaan aset; keamanan SDM; keamanan fisik lingkungan; manajemen komunikasi dan operasi; pengendalian akses; akusisi, pengembangan, dan pemeliharaan sistem informasi; manajemen insiden keamanan informasi; manajemen keberlanjutan bisnis; dan kesesuaian (BSN, 2009). Standar internasional ini memberikan panduan teknis dalam manajemen keamanan informasi untuk mencapai kerahasiaan, integritas, dan ketersediaan informasi. Domain dan kontrol dari ISO/IEC 27001:2005 dapat dilihat pada Tabel 1 (BSN, 2009).

Tabel 1. Domain dan Kontrol Objektif ISO 27001

No	Domain	Kontrol Objektif
1.	Security Policy	1.Information Security Policy
2.	Organization of Information Security	2.Internal Organization
		3.External Parties
3.	Asset Management	4. Responsibilies for Assets
		5. Information Classification
4.	Human Resources Security	6. Prior to Employment
		7. During Employment
		8. Termination or Change of Employment
5.	Physical and Environmental security	9. Secure Areas
		10. Equipment Security
6.	Communication and Operations Management	11. Operational Procedures and Responsibilities
		12. Third Party Service Delivery Management
		13. System Planning and Acceptance
		14. Protection Against Malicious and Mobile Code
		15. Backup
		16. Network Security Management
		17. Media Handling
		18. Exchange of Information
		19. Electronic Commerce Services
		20. Monitoring
7.	Access Control	21. Business Control for Access Control
		22. User Access Management
		23. User Responsibilities
		24. Network Access Control
		25. Operating System Access Control
		26. Application and Information Access Control
		27. Mobile Computing and Teleworking
8.	Information system Acquision, Development and Maintenance	28. Security Requirements of Information Systems
		29. Correct Processing in Applications
		30. Cryptographic Controls
		31. Security of System Files
		32. Security Indevelopment and Support Services
		33. Technical Vulnerability Management
9.	Information Security Incident Management	34. Reporting Information Security Events and Weakness
		35. Management of Information Security Incidents And Improvements
10.	Business Continuity Management	36. Information Security Aspects of Business Continuity Management
11.	Compliance	37. Compliance With Legal Requirements
		38. Compliance With Technical Policies and Standard and Technical Compliance
		39. Information System Audit Considerations

Pada Tabel 1 dapat dilihat bahwa ISO/IEC 27001: 2005 terdiri atas 11 (sebelas) domain dan 39 (tiga puluh sembilan) kontrol objektif. Domain dan kontrol tersebut memberikan standar terkait keamanan informasi secara komprehensif. Identifikasi kelemahan kontrol dilakukan berdasarkan domain dan kontrol objektif tersebut.

Selain ISO 27001, terdapat beberapa kerangka kerja yang cukup banyak diaplikasikan oleh organisasi seperti ITIL, dan COBIT. Setiap *framework* memiliki latar belakang pembentukan dan area kontrol masing-masing seperti COBIT yang berfokus pada *Business Orientation and IT Governance* dan ITIL yang berfokus pada *Service Delivery and Service Support* (Arora, 2010) (Aygun, 2010). Kerangka kerja- kerangka kerja yang berfokus pada keamanan informasi yang sudah diterapkan di berbagai negara, antara lain sebagai berikut (Syafrizal, 2007):

1. NIST (*National Institute of standard and technology*). NIST merupakan sebuah standar yang dijadikan sebuah acuan dalam melakukan manajemen keamanan teknologi informasi yang dibuat oleh FISMA (*Federal Information Security Management Act*) yang digunakan di Negara Amerika Serikat.
2. GMITS (*Guidelines for the Management of Information Technology Security*). GMITS adalah sebuah kerangka kerja untuk melakukan manajemen keamanan teknologi informasi.
3. BS (*British standard*).

Dari beberapa *framework* keamanan informasi tersebut, yang paling spesifik terhadap keamanan informasi adalah ISO 27001. ISO 27001 dilengkapi dengan 8 (delapan) struktur, *Annex* A (ISO27002), *Annex* B dan *Annex* C.

ISO 27001 mencakup semua jenis organisasi (seperti perusahaan swasta, lembaga pemerintahan, dan lembaga nirlaba). ISO 27001menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memantau, menganalisis dan memelihara seta mendokumentasikan *Information security management system* dalam konteks risiko bisnis organisasi secara keseluruhan.

Final Draft International Standards (FDIS) ISO/IEC 27001: 2005

Final Draft Internastional Standards (FDIS) ISO 27001 berisi persyaratan untuk penetapan, penerapan, pemeliharaan, peningkatan secara terus-menerus sistem manajemen keamanan informasi suatu organisasi. Standar ini juga mencakup persyaratan untuk penilaian dan penanganan risiko keamanan informasi sesuai dengan kebutuhan organisasi. Persyaratan yang ditetapkan dalam FDIS ISO 27001 bersifat generik dan dimaksudkan agar dapat diterapkan pada semua organisasi, terlepas dari jenis, ukuran atau *nature* dari suatu organisasi. (*International Organization for Standardization,* 2013).

FDIS ISO 27001 lebih menekankan pada bagaimana organisasi menjalankan Sistem Manajemen Keamanan Informasi (*International Organization for Standardization,* 2013). Perubahan kontrol pada FDIS ISO 27001 dibandingkan dengan ISO/IEC 27001:2005 dapat dilihat pada Tabel 2. Terdapat bagian baru yang mengatur tentang *outsource*, sesuai dengan kondisi perusahaan atau organisasi yang saat ini relatif banyak memanfaatkan jasa pihak ketiga atau *outsourcing* dalam menjalankan bisnisnya, termasuk dalam lingkup TI (*Gama Secure Systems Limited, 2013).*

Tabel 2. Perubahan Kontrol dan Perubahan Kontrol Objektif ISO/IEC 27001:2005 (*Gama Secure Systems Limited,* 2013)

FDIS ISO 27001	*ISO/IEC 27001:2005*
A.5 Information Security Policy	
A.5.1 Management Directions for Information Security	
A.5.1.1 Policies for information security	*A.5.1.1 Information security policy document*
A.5.1.2 Review of the policies for information security	*A.5.1.2 Review of the information security policy*
A.6 Organisation of Information Security	
A.6.1 Internal Organisation	
A.6.1.1 Information security roles and responsibilities	*A.6.1.3 Allocation of information security responsibilities* *A.8.1.1 Roles and responsibilities*
A.6.1.2 Contact with authorities	*A.6.1.6 Contact with authorities*
A.6.1.3 Contact with special interest groups	*A.6.1.7 Contact with special interest groups*
A.6.1.4 Information security in project management	
A.6.1.5 Segregation of duties	*A.10.1.3 Segregation of duties*
A.6.2 Mobile devices and teleworking	
A.6.2.1 Mobile device policy	*A.11.7.1 Mobile computing and communications*
A.6.2.2 Teleworking	*A.11.7.2 Teleworking*
A.7 Human Resource Security	
A.7.1 Prior to employment	
A.7.1.1 Screening	*A.8.1.2 Screening*
A.7.1.2 Terms and conditions of employment	*A.8.1.3 Terms and conditions of employment*
A.7.2 During Employment	
A.7.2.1 Management responsibilities	*A.8.2.1 Management responsibilities*
A.7.2.2 Information security awareness, education and training	*A.8.2.2 Information security awareness, education and training*
A.7.2.3 Disciplinary process	*A.8.2.3 Disciplinary process*
A.7.3 Termination and change of employment	
A.7.3.1 Termination or change of employment responsibilities	*A.8.3.1 Termination responsibilities*
A.8 Asset Management	
A.8.1 Responsibility for Assets	
A.8.1.1 Inventory of assets	*A.7.1.1 Inventory of assets*
A.8.1.2 Ownership of assets	*A.7.1.2 Ownership of assets*
A.8.1.3 Acceptable use of assets	*A.7.1.3 Acceptable use of assets*
A.8.2 Information classification	
A.8.2.1 Classification of information	*A.7.2.1 Classification guidelines*
A.8.2.2 Labeling of information	*A.7.2.2 Information labeling and handling*
A.8.2.3 Handling of assets	*A.10.7.3 Information Handling procedures*
A.8.2.4 Return of assets	*A.8.3.2 Return of assets*
A.8.3 Media Handling	
A.8.3.1 Management of removable media	*A.10.7.1 Management of removable media*
A.8.3.2 Disposal of media	*A.10.7.2 Disposal of Media*
A.8.3.3 Physical media transfer	*A.10.8.3 Physical media in transit*
A.9 Logical Security/Access Control	
A.9.1.2 Policy on the use of network services	*A.11.4.1 Policy on use of network services*

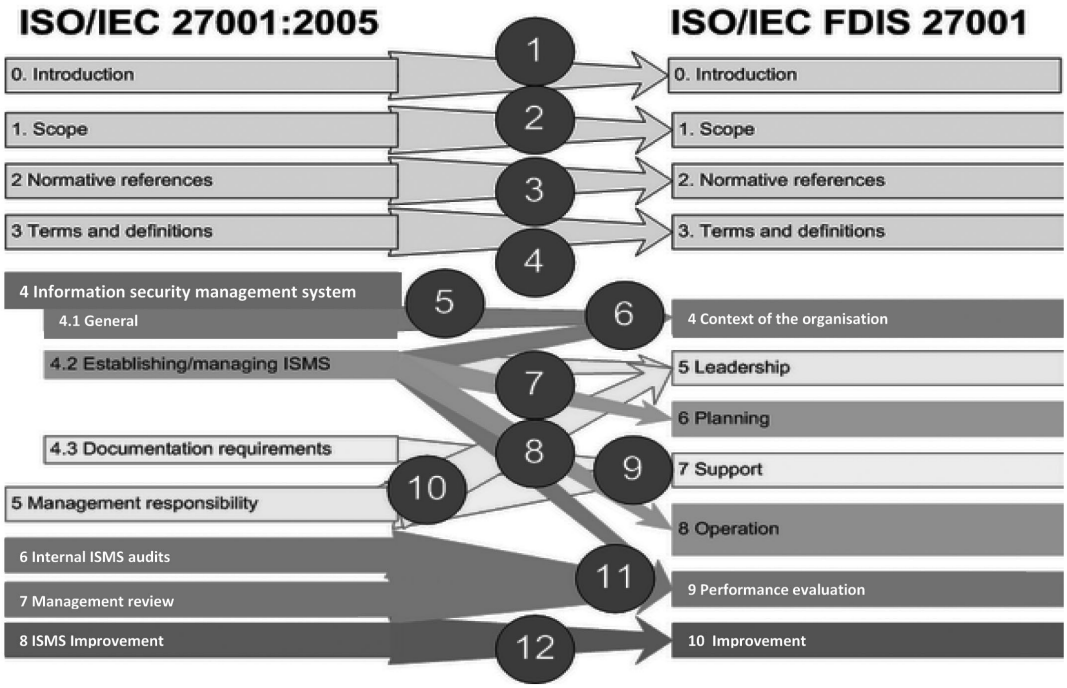
FDIS ISO 27001	*ISO/IEC 27001:2005*
A.9.2 User access management	
A.9.2.1 User registration and de-registration	*A.11.2.1 User registration*
	A.11.5.2 User identification and authentication
A.9.2.2 Privilege management	*A.11.2.2 Privilege management*
A.9.2.3 Management of secret authentication information of users	*A.11.2.3 User password management*
A.9.2.4 Review of user access rights	*A.11.2.4 Review of user access rights*
A.9.2.5 Removal or adjustment of access rights	*A.8.3.3 Removal of access rights*
A.9.3 User responsibilities	
A.9.3.1 Use of secret authentication information	*A.11.3.1 Password use*
A.9.4 System and application access control	
A.9.4.1 Information access restriction	*A.11.6.1 Information access restriction*
A.9.4.2 Secure log-on procedures	*A.11.5.1 Secure log-on procedures*
	A.11.5.5 Session time-out
	A.11.5.6 Limitation of connection time
A.9.4.3 Password management system	*A.11.5.3 Password management system*
A.9.4.4 Use of privileged utility programs	*A.11.5.4 Use of system utilities*
A.9.4.5 Access control to program source code	*A.12.4.3 Access control to program source code*
A.10 Cryptography	
A.10.1 Cryptographic controls	
A.10.1.1 Policy on the use of cryptographic controls	*A.12.3.1 Policy on the use of cryptographic controls*
A.10.1.2 Key management	*A.12.3.2 Key management*
A.11 Physical and environmental Security	
A.11.1 Secure areas	
A.11.1.1 Physical security perimeter	*A.9.1.1 Physical security perimeter*
A.11.1.2 Physical entry controls	*A.9.1.2 Physical entry controls*
A.11.1.3 Securing office, room and facilities	*A.9.1.3 Securing offices, rooms and facilities*
A.11.1.4 Protecting against external end environmental threats	*A.9.1.4 Protecting against external and environmental threats*
A.11.1.5 Working in secure areas	*A.9.1.5 Working in secure areas*
A.11.1.6 Delivery and loading areas	*A.9.1.6 Public access, delivery and loading areas*
A.11.2 Equipment	
A.11.2.1 Equipment siting and protection	*A.9.2.1 Equipment sitting and protection*
A.11.2.2 Supporting utilities	*A.9.2.2 Supporting utilities*
A.11.2.3 Cabling security	*A.9.2.3 Cabling security*
A.11.2.4 Equipment maintenance	*A.9.2.4 Equipment maintenance*
A.11.2.5 Removal of assets	*A.9.2.7 Removal of property*
A.11.2.6 Security of equipment and assets off- premises	*A.11.2.6 Security of equipment and assets off- premises*
A.11.2.7 Security disposal or re-use of equipment	*A.9.2.6 Secure disposal or re-use of equipment*
A.11.2.8 Unattended user equipment	*A.11.3.2 Unattended user equipment*
A.11.2.9 Clear desk and clear screen policy	*A.11.3.3 Clear desk and clear screen policy*
A.12 Operations Security	
A.12.1 Operational Procedures and Responsibilities	
A.12.1.1 Documented operating procedures	*A.10.1.1 Documented operating procedures*
A.12.1.2 Change management	*A.10.1.2 Change management*
A.12.1.3 Capacity management	*A.10.3.1 Capacity management*
A.12.1.4 Separation of development, test and operational environments	*A.10.1.4 Separation of development, test and operational facilities*
A.12.2 Protection from Malware	
A.12.2.1 Controls against malware	*A.10.4.1 Controls against malicious code*
A.12.3 Back-Up	
A.12.3.1 Information backup	*A.10.5.1 Information back-up*

FDIS ISO 27001	*ISO/IEC 27001:2005*
A.12.4 Logging and Monitoring To record events and generate evidence.	
A.12.4.1 Event logging	*A.10.10.1 Audit logging*
A.12.4.2 Protection of log information	*A.10.10.3 Protection of log information*
A.12.4.3 Administrator and operator logs	*A.10.10.3 Protection of log information* *A.10.10.4 Administrator and operator logs*
A.12.4.4 Clock Synchronisaton	*A.10.10.6 Clock synchronization*
A.12.5 Control of operational software	
A.12.5.1 Installation of software on operational systems	*A.12.4.1 Control of operational software*
A.12.6 Technical Vulnerability Management	
A.12.6.1 Management of technical vulnerabilities	*A.12.6.1 Control of technical vulnerabilities*
A.12.6.2 Restrictions on software installation	
A.12.7 Information Systems Audit Considerations	
A.12.7.1 Information systems audit controls	*A.15.3.1 Information system audit controls*
A.13 Communications Security	
A.13.1 Network Security Management	
A.13.1.1 Network controls	*A.10.6.1 Network controls*
A.13.1.2 Security of network services	*A.10.6.2 Security of network services*
A.13.1.3 Segregation in networks	*A.11.4.5 Segregation in Networks*
A.13.2 Information transfer	
A.13.2.1 Information transfer policies and procedures	*A.10.8.1 Information exchange policies and procedures*
A.13.2.2 Agreements on information transfer	*A.10.8.2 Exchange agreements*
A.13.2.3 Electronic messaging	*A.10.8.4 Electronic messaging*
A.13.2.4 Confidentiality or non-disclosure agreements	*A.6.1.5 Confidentiality agreements*
A.14 System acquisition, development and maintenance	
A.14.1 Security requirements of information systems	
A.14.1.1 Security requirements analysis and specification	*A.12.1.1 Security requirements analysis and specification*
A.14.1.2 Securing applications services on public networks	*A.10.9.1 Electronic commerce* *A.10.9.3 Publicly available information*
A.14.1.3 Protecting application services transactions	*A.10.9.2 Online-transactions*
A.14.2 Security in development and support processes	
A.14.2.1 Secure development policy	
A.14.2.2 Change control procedures	*A.12.5.1 Change control procedures*
A.14.2.3 Technical review of applications after operating platform changes	*A.12.5.2 Technical review of applications after operating system changes*
A.14.2.4 Restrictions on changes to software packages	*A.12.5.3 Restrictions on changes to software packages*
A.14.2.5 System development procedures	
A.14.2.6 Secure development environment	
A.14.2.7 Outsourced development	*A.12.5.5 Outsourced software development*
A.14.2.9 System acceptance testing	*A.10.3.2 System Acceptance*
A.14.3 Test data	
A.14.3.1 Protection of test data	*A.12.4.2 Protection of system test data*
A.15 Supplier relationships	
A.15.1 Security in supplier relationship	
A.15.1.1 Information security policy for supplier relationships	*A.6.2.3 Addressing security in third party agreements*
A.15.1.2 Addressing security within supplier agreements	*A.6.2.3 Addressing security in third party agreements*
A.15.1.3 ICT Supply chain	
A.15.2 Supplier service delivery management	
A.15.2.1 Monitoring and review of supplier services	*A.10.2.2 Monitoring and review of third party services*
A.15.2.2 Managing changes to supplier services	*A.10.2.3 Managing changes to third party services*

FDIS ISO 27001	***ISO/IEC 27001:2005***
A.16 Information Security Incident Management	
A.16.1 Management of information security incidents and improvements	
A.16.1.1 Responsibilities and procedures	*A.13.2.1 Responsibilities and Procedures*
A.16.1.2 Reporting information security events	*A.13.1.1 Reporting information security events*
A.16.1.3 Reporting information security weaknesses	*A.13.1.2 Reporting security weakness*
A.16.1.4 Assessment and decision of information security events	
A.16.1.5 Response to information security incidents	
A.16.1.6 Learning from information security incidents	*A.13.2.2 Learning from information security incidents*
A.16.1.7 Collection of evidence	*A.13.2.3 Collection of evidence*
A.17 Business Continuity	
A.17.1 Information security aspects of business continuity management	
A.17.1.1 Planning information security continuity	*A.14.1.2 Business continuity and risk assessment*
A.17.1.2 Implementing information security continuity	
A.17.1.3 Verify, review and evaluate information security continuity	*A.14.1.5 Testing, maintaining and re-assessing business continuity plans*
A.17.2 Redundancies	
A.17.2.1 Availability of information processing facilities	
A.18 Compliance	
A.18.1 Information security reviews	
A.18.1.1 Independent review of information security	*A.6.1.8 Independent review of information security*
A.18.1.2 Compliance with security policies and standards	*A.15.2.1 Compliance with security policies and standards*
A.18.1.3 Technical compliance inspection	*A.15.2.2 Technical compliance checking*
A.18.2 Compliance with legal and contractual requirements	
A.18.2.1 Identification of applicable legislation and contractual requirements	*A.15.1.1 Identification of applicable legislation*
A.18.2.2 Intellectual property rights (IPR)	*A.15.1.2 Intellectual property rights (IPR)*
A.18.2.3 Protection of documented information	*A.15.1.3 Protection of organisational records*
A.18.2.4 Privacy and protection of personal information	*A.15.1.4 Data protection and privacy of personal information*
A.18.2.5 Regulation of cryptographic controls	*A.15.1.6 Regulation of cryptographic controls*

Dari Tabel 2 dapat dilihat detail perbedaan dari tiap domain dan kontrol objektif antara ISO 27001 dengan FDIS ISO 27001. Perubahan termasuk perubahan dalam *outsourcing*. Sedangkan perubahan struktur dari standar ISO 27001 dapat dilihat pada Gambar 1 (*Gama Secure Systems Limited,* 2013). Terdapat 12 (dua belas) poin perubahan struktur dari standar ISO/IEC 27001:2005, seperti yang dapat dilihat pada Gambar 1.

Pada Gambar 1 dapat dilihat pemetaan struktur dokumen dan isi dari ISO 27001 ke FDIS ISO 27001 (*Gama Secure Systems Limited*, 2013). Bagian audit internal dan peninjauan ulang oleh manajemen pada ISO 27001 dipetakan menjadi evaluasi performansi pada FDIS ISO 27001 (*Gama Secure Systems Limited*, 2013). Tanggung jawab manajemen dan manajemen ISMS atau SMKI pada ISO 27001 dipetakan ke bagian *leadership* (kepemimpinan) pada FDIS ISO 27001 (*Gama Secure Systems* Limited, 2013). *Support* pada FDIS ISO 27001 merupakan pemetaan dari persyaratan dokumentasi dan tanggung jawab manajemen pada ISO 27001 (*Gama Secure Systems Limited,* 2013). Sedangkan perencanaan dan operasi pada FDIS ISO 27001 merupakan pemetaan dari manajemen ISMS atau SMKI pada ISO 27001 (Gama Secure Systems Limited, 2013).



Gambar 1. Rancangan Akhir Perubahan Struktur Dokumen dan Isi dari Standar ISO/IEC 27001:2005

(Sumber: Gama Secure Systems Limited, 2013)

Terdapat beberapa penelitian terkait audit keamanan informasi, serta kebijakan dan prosedur keamanan informasi. Penelitian "Perancangan Kebijakan dan Standar Manajemen Layanan Teknologi Informasi Mengacu Kepada ISO 20000, ISO 27001, dan COBIT: Studi Kasus PT. Bhanda Ghara Reksa (Persero)" (Akmal, 2011) memberikan solusi berupa rancangan kebijakan dan standar dalam Manajemen Layanan TI. Permasalahan layanan TI dikelompokkan dan dipetakan berdasarkan COBIT, ISO 20000, dan ISO 27001, kemudian diprioritaskan berdasar hasil analisis risiko. Penelitian tersebut tidak membahas metode validasi kebijakan dan standar manajemen layanan Teknologi Informasi.

Penelitian "Perancangan Model Tata Kelola Teknologi Informasi Berbasis COBIT pada Proses Pengelolaan Data Studi Kasus: PT PLN (Persero) Distribusi Jawa Timur" (Maulidevi, 2007) menilai kematangan penerapan tata kelola pada proses pengelolaan data (DS11) berdasarkan kerangka kerja COBIT, kemudian dirancang solusi atas perma- salahan-permasalahan yang meng-hambat organisasi dalam penerapan tata kelola pengelolaan data. Penelitian tersebut memberikan solusi berupa kebijakan dan prosedur dalam pengelolaan data berdasar pada COBIT 4.1 (DS11), namun kurang memperhatikan aspek keamanan sistem (DS5).

Theoretical Framework

Permasalahan keamanan informasi, visi, misi, tujuan, dan strategi bisnis organisasi, serta kebijakan dan prosedur yang berlaku di lingkungan PT XYZ menjadi salah satu faktor pendorong dilakukannya audit keamanan informasi. Rekomendasi kebijakan dan prosedur keamanan informasi disusun berdasarkan ISO 27001. Kebutuhan bisnis PT XYZ terhadap keamanan informasi diharapkan dapat dicapai melalui kontrol yang dituangkan dalam rekomendasi perbaikan kebijakan dan prosedur keamanan informasi. Proses-proses

tersebut dituangkan dalam prosedur-prosedur dan kebijakan yang direkomendasikan untuk diterapkan di lingkungan PT XYZ, sebagai solusi untuk memenuhi kriteria keamanan informasi.

Metode Penelitian

Perumusan masalah dan pengambilan data dilakukan dengan observasi, studi literatur, dan wawancara yang disesuaikan dengan hasil observasi. Penilaian risiko dilakukan sesuai standar ISO/IEC 27001: 2005. Dari hasil observasi dan wawancara diperoleh dokumen *Statement of Applicability* (SOA). Analisis data meliputi analisis kesenjangan kebijakan, analisis identifikasi risiko; identifikasi aset, ancaman, dampak, dan kelemahan kontrol. Hasil analisis ini mendasari penyusunan rekomendasi perbaikan kebijakan dan prosedur keamanan informasi. Berdasar hasil analisis risiko, diberikan rekomendasi kontrol dan proses. Rekomendasi kebijakan dan prosedur disusun sesuai visi, misi, tujuan, strategi organisasi, dan kebijakan serta prosedur yang sudah berlaku di PT XYZ, dan ISO 27001.

Pada studi kasus ini, langkah-langkah yang dilakukan sesuai dengan tahapan plan (perencanaan) yang ada pada standar ISO/IEC 27001:2005. Langkah-langkah yang dilakukan yaitu sebagai berikut:

a. Menentukan ruang lingkup;
b. Melakukan analisis kesenjangan;
c. Melakukan penilaian risiko (identifikasi aset, identifikasi ancaman/ kerawanan/ dampak, prioritasi risiko, memilih kontrol yang sesuai untuk meningkatkan keamanan informasi);
d. Menyusun rekomendasi perbaikan kebijakan dan prosedur keamanan informasi.

HASIL DAN PEMBAHASAN

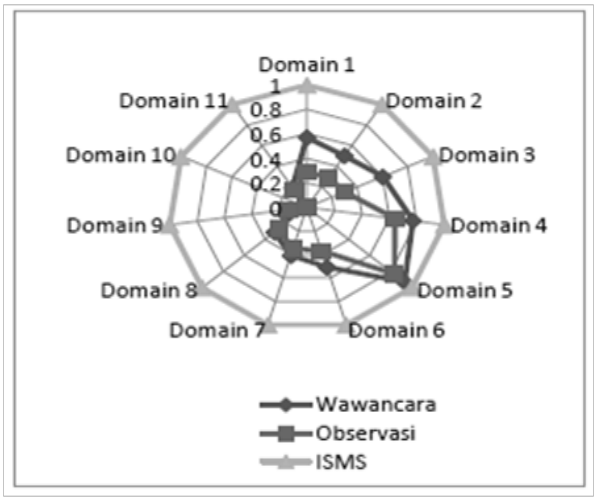
Pada penelitian ini, ruang lingkup sistem manajemen keamanan informasi, yaitu:

a. Audit kepatuhan terhadap visi dan misi perusahaan;
b. Mencakup seluruh aset dalam bentuk teknologi, proses, sistem, layanan, aplikasi, jaringan dan *software* yang dimiliki perusahaan; dan
c. *Risk assessment* keamanan informasi meliputi identifikasi Aset, identifikasi kerawanan *(vulnerability)* dan ancaman *(threats)*, mengkategorikan risiko atau menentukan risiko prioritas (*Risk Prioritization*), mementukan kontrol (*Develop control*) dan monitoring.

Sebelum melakukan analisis kesenjangan, terlebih dahulu dilakukan penilaian kesenjangan untuk mengetahui dan membandingkan sejauh apa kontrol-kontrol ISO 27001 yang sudah dilakukan, baik dalam kebijakan, prosedur, instruksi maupun dokumentasinya. Hasil penilaian kesenjangan keamanan informasi yang dilakukan melalui wawancara dan observasi sesuai dengan panduan *checklist* ISO/IEC 27001:2005 dapat dilihat pada Gambar 2 dan Gambar 3.

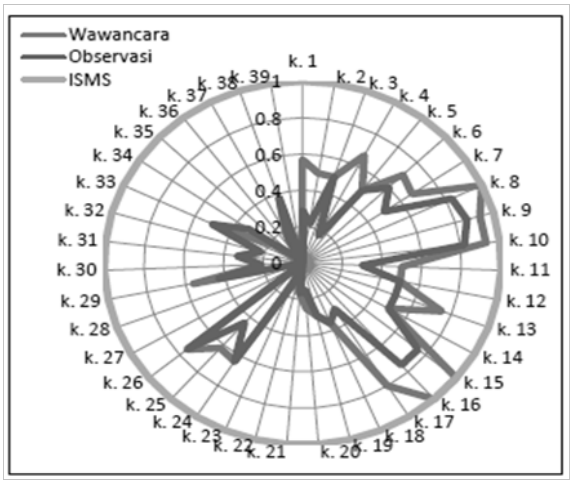
Gambar 2 menyajikan hasil penilaian kesenjangan keamanan informasi untuk masing-masing domain sesuai standar ISO/ IEC 27001: 2005. Pada Gambar 2 dapat dilihat bahwa tingkat penerapan keamanan informasi pada PT XYZ masih belum memenuhi standar ISO/IEC 27001: 2005. Hanya 2 (dua) domain yang mencapai angka 80% (delapan puluh persen) dalam penerapan atau praktiknya, baik berdasarkan hasil wawancara maupun observasi, yaitu domain 5. Domain 5 merupakan domain yang terkait *Physical and Environmental security.* Artinya, penerapan kebijakan dan prosedur keamanan

informasi keamanan fisik dan lingkungan sudah dilaksanakan dengan baik di lingkungan PT XYZ. Namun jika dilihat dari 11 (sebelas) domain, kepatuhan PT XYZ terhadap visi dan misi *best services* kepada pelanggan belum memenuhi kriteria keamanan informasi.



Gambar 2. Hasil Penilaian Kesenjangan Keamanan Informasi Sesuai Standar ISO/IEC 27001:2005 pada PT XYZ

Gambar 3 menyajikan hasil penilaian kesenjangan keamanan informasi untuk masing-masing kontrol onjektif sesuai standar ISO/IEC 27001:2005 pada PT XYZ. Pada Gambar 3 dapat dilihat tingkat kepatuhan terhadap ISO/IEC 27001:2005 pada masing-masing kontrol objektif. Dapat dilihat bahwa sebagian besar kontrol objektif masih di bawah 80% (delapan puluh persen) dalam pemenuhan atau penerapannya. Hasil penilaian kesenjangan tersebut dapat menjadi salah satu bahan pertimbangan dalam menyusun rekomendasi perbaikan kebijakan dan prosedur keamanan informasi.



Gambar 3. Hasil Penilaian Kesenjangan Keamanan Informasi untuk Setiap Kontrol Objektif Sesuai Standar ISO/IEC 27001:2005 pada PT XYZ

Penilaian Risiko Berdasarkan Standar ISO/IEC 27001:2005

Tahapan-tahapan dalam penilaian risiko, yaitu sebagai berikut:

a. Melakukan identifikasi aset;
b. Melakukan identifikasi kerawanan (*vulnerability*) dan ancaman (*threats*);
c. Menentukan prioritas risiko;
d. Memilih kontrol yang sesuai;
e. Monitoring.

Hasil identifikasi aset SI/TI pada PT XYZ dapat dilihat pada Tabel 3.

Tabel 3. Aset SI/TI PT. XYZ

No	Aset	Pemilik	Alokasi
1	Server	IT dan non-IT (keuangan, developer, dll).	Internal
2.	Router	IT	Internal dan Eksternal
2.	DVR	IT	Internal
3.	Kamera CCTV	Non-IT	Internal
4.	Access point	IT	Internal dan eksternal
5.	Firewall	IT	Internal dan eksternal
6.	Switch	IT	Internal
7.	Modem Dial up	IT dan non-IT	Internal dan eksternal
8.	Pintu	IT dan non-IT	Internal
9.	PC, Laptop	IT	Internal
10.	Sistem operasi	IT	Internal
11.	Email internal	IT	Internal
12	Email eksternal	IT	Internal dan eksternal
13.	Website pemasaran	Non-IT (pemasaran)	Internal dan eksternal
14.	MRTG (Multi Router Traffic Grapher)	IT	Internal
15.	Sistem informasi pengelolaan pegawai	Non-IT (kepegawaian)	Internal
16.	Sistem ERP	IT	Internal
17.	UPS	IT	Internal
18.	Antivirus	IT	Internal
19.	Document Management (Integrator)	Bag. Produksi	Internal
20.	Koneksi PT. XYZ - Bank ABC	Non-IT	Internal dan eksternal
21.	Koneksi PT. XYZ - Bank DEF	Non-IT	Internal dan eksternal
22.	Karyawan	IT dan non-IT	Internal

Tabel 3 menyajikan daftar aset SI/TI yang dimiliki dan digunakan oleh PT XYZ dalam menjalankan kegiatan bisnisnya. Pada Tabel 3 dapat dilihat bahwa sebagian aset dialokasikan untuk internal, sebagian lainnya dialokasikan untuk eksternal. Namun terdapat juga beberapa aset yang dialokasikan untuk keduanya, baik internal maupun eksternal. Hasil identifikasi kerawanan pada PT XYZ dapat dilihat pada Tabel 4.

Tabel 4. Hasil Identifikasi Kerawanan pada PT XYZ

No	Kerawanan (*Vulnerability*)	Kode
1.	Persyaratan *sharing password*, pengamanan identitas dan hak akses pengguna yang tidak tepat. Misal: *password default*, ditulis pada kertas yang ditempel di tempat yang mudah diakses oleh yang tidak berhak, *sharing* akun dan *password*.	V1
2.	Informasi cetak (*hardcopy*) maupun non-cetak (*softcopy*) yang diletakkan atau disimpan di tempat yang tidak tepat. Misalnya: informasi berupa softcopy disimpan pada media yang dapat dipindahkan dengan mudah seperti hard disk atau flash disk, dan tidak disimpan di file server.	V2
3.	Patching atau *update* yang terlambat atau versi yang sudah lama dan ketinggalan.	V3
4.	Proses pemeliharaan (*maintenance*) dan pengawasan (*monitoring)* tidak berjalan dan tidak terpantau.	V4
5.	Perangkat lunak dan perangkat keras sudah habis *lifetime*-nya serta sparepart yang sudah tidak didukung leh vendor.	V5
6.	Ada IP *publilc* yang bisa diakses oleh karyawan atau pengguna dari jarak jauh. Misalnya: ada beberapa server yang dapat diakses melalui web.	V6
7.	Konfigurasi sistem yang masih mengikuti bawaan pabrik, sehingga *password* mudah ditebak.	V7
8.	Beberapa komputer PC belum dikonfigurasi dengan benar. Misal: port USB yang masih terbuka, pengguna dapat mengganti IP.	V8
9.	*Password* yang tidak dirubah secara berkala.	V9

Tabel 4 menyajikan hasil identifikasi kerawanan pada PT XYZ. Masing-masing kerawanan diberikan kode untuk memudahkan dalam penilaian risiko. Hasil identifikasi ancaman dan kerawanan menunjukkan bahwa ancaman dan kerawanan tidak hanya berasal dari internal PT XYZ saja tetapi juga berasal dari eksternal organisasi (misalnya: *vendor*). Kerawanan yang teridentifikasi termasuk aspek *people, process,* dan *technology*. Hasil identifikasi ancaman pada PT XYZ dapat dilihat pada Tabel 5.

Tabel 5. Hasil Identifikasi Ancaman pada PT XYZ

No	Ancaman (*Threats*)	Kode
1.	Serangan virus, worm dan malware	T1
2.	Spam pada email yang menyebabkan email-email penting tertunda baik pengiriman maupun penerimaannya	T2
3.	Penerobosan sistem oleh pihak eksternal	T3
4.	Penerobosan sistem oleh pihak internal	T4
5.	Kegagalan sistem akibat kerusakan perangkat keras dan perangkat lunak	T5
6.	Pengrusakan aset secara fisik	T6
7.	Kartu akses yang terdaftar bisa digunakan oleh siapa saja, tidak adanya pembatasan hak akses.	T7

Tabel 5 menyajikan hasil identifikasi ancaman pada PT XYZ. Masing-masing ancaman yang teridentifikasi diberikan kode untuk memudahkan dalam penilaian risiko. Dampak jika terjadi kegagalan penjagaan aspek keamanan informasi disajikan pada Tabel 6.

Tabel 6. Identifikasi Dampak
(jika terjadi kegagalan penjagaan aspek Keamanan Informasi)

Dampak		
Low	**Medium**	***High***
Dapat menyebabkan dampak, kerusakan, atau kerugian secara terbatas, kecil, atau tidak penting kepada organisasi atau individu pemilik informasi. Downtime kurang dari 8 (delapan) jam atau kejadian downtime tidak memberi dampak pada organisasi.	Dapat menyebabkan kerugian operasional, mengganggu kelancaran proses bisnis, atau mengganggu citra/reputasi organisasi, atau kerusakan yang bersifat biasa bagi organisasi. Nilai kerusakan bersifat biasa bagi organisasi. Dampak kejadian akan berpengaruh pada operasional organisasi. *Downtime* cukup lama (8 s.d. 36 jam).	Dapat menyebabkan kerugian operasional cukup besar, terhentinya proses bisnis, atau kerugian menjadi perhatian para pemangku kepentingan, atau nilai kerusakan bersifat penting bagi organisasi. Downtime lama (lebih dari 36 jam) atau terjadi kegagalan sistem.

Pada Tabel 6 dapat dilihat hasil identifikasi dampak jika terdapat kegagalan penjagaan aspek keamanan informasi. Dampak dikategorikan menjadi 3 (tiga) kategori, yaitu: *low*, *medium*, *high,* dan *critical*. Untuk mengidentifikasi tingkat risiko digunakan matriks tingkat risiko pada Tabel 7.

Tabel 7. Matriks Tingkat Resiko

Dampak (Impact)	Probabilitas		
	Low (0.1)	Medium (0.5)	High (1.0)
Low critical (10)	Low (1.0)	Medium (5)	Medium (10)
Medium (50)	Medium (5)	Medium (25)	High (50)
High critical (100)	High (10)	High (50)	Critical (100)

Setelah mendefinisikan matriks tingkat risiko, selanjutnya dilakukam pengukuran tingkat risiko saat ini (*inherent risk*). Setelah melakukan mitigasi pada sebuah risiko, selanjutnya diukur *residual risk*. Setelah semua terpetakan, selanjutnya dipetakan ancaman dan kerawanan pada aset, menilai dampak yang ditimbulkan, dengan kontrol yang ada didapatkan nilai risiko saat ini (*inherent risk*). Berdasarkan nilai *inherent risk* dan nilai risiko harapan dipilih rekomendasi kontrol-kontrol yang sesuai untuk meningkatkan keamanan informasi, dengan mengacu pada ISO 27001. Nilai risiko yang tinggi disebabkan karena dampak yang terjadi dikategorikan tinggi *(high)* meskipun probabilitasnya rendah.

Identifikasi dan evaluasi pilihan penanganan risiko ditujukan untuk mengidentifikasi dan menentukan pilihan penanganan risiko yang timbul namun tidak dapat langsung diterima olehPT XYZ. Risiko yangtidakdapatlangsungditerimaperludikelola sesuai dengan kriteria penerimaan risiko yang telah disepakati dengan pimpinan PT XYZ. Pemilihan dan rekomendasi penerapan kontrol yang sesuai dan dapat diterapkan di lingkungan PT XYZ dilakukan untuk mengurangi risiko sampai pada tingkat yang dapat diterima oleh perusahaan, disesuaikan dengan target kinerja perusahaan. Daftar kontrol dan kontrol objektif pada PT XYZ berikut keterangannya yang tidak dapat diaplikasikan serta dicantumkan dalam *Statement of Applicability* atau SOA (Regalado, 2007). Daftar aset, *vulnerability, threats*, nilai *inherent risk*, residual risk, dan nilai risiko harapan pada PT XYZ disajikan dalam Tabel 8.

Tabel 8. Daftar aset, Vulnerability, *Threats*, Nilai Inherent Risk, Residual Risk, dan Nilai Risiko Harapan pada PT XYZ

Aset	Vulnerability	*Threats*	Nilai Inherent Risk	Nilai Residual Risk
Server	V4, V5, V8	T5, T6, T7	High	Medium
Router	V5	T6, T7	Low	Low
DVR	V5	T6, T7	Critical	High
Kamera CCTV	V5	T6	High	Medium
Access point	V5	T6	Low	Low
Firewall	V5	T6, T7	Low	Low
Switch	V5	T6, T7	Medium	Low
Modem	V5	T6, T7	High	Medium
Pintu	V5	T6, T7	High	Medium
PC, Laptop	V5, V8	T5, T6	High	Medium
Sistem operasi	V1, V3, V5, V8, V9	T1, T4, T5, T7	High	Medium
Email internal	V1, V4, V9	T1, T2, T3, T4, T5, T7	High	Medium
Email eksternal	V1, V4, V9	T1, T2, T3, T4, T5, T7	Critical	High
Website pemasaran	V4, V9	T1, T3, T4, T5,	Low	Low
MRTG	V4, V9	T1, T4, T5, T6, T7	Low	Low
Sistem informasi pengelolaan pegawai	V1, V4, V9	T1, T4, T5, T7	Low	Low
Sistem ERP	V4, V9	T1, T4, T5, T7	Low	Low
UPS	V1, V3, V4, V5, V9	T1, T4, T5, T7	Critical	High
Antivirus	V1, V3, V4, V9	T1, T4, T5, T7	Medium	Low
Document Management (Integrator)	V1, V4, V9	T1, T4, T5, T7	Medium	Low
Koneksi PT. XYZ - Bank ABC	V1, V2, V3, V4, V5, V8, V9	T4, T5, T7	High	Medium
Koneksi PT. XYZ - Bank DEF	V1, V2, V3, V4, V5, V8, V9	T4, T5, T7	Critical	High
Karyawan	V1, V2, V4, V6, V9	T3, T4, T6, T7	High	Medium

Pemilihan Kontrol dan Rencana Kerja

Setelah diidentifikasi risiko-risiko yang harus diperbaiki, selanjutnya dipilih kontrol yang akan digunakan untuk mengurangi nilai risiko. Pemilihan kontrol didasarkan hasil identifikasi kerawanan, ancaman dan dampak. Daftar kontrol dan rencana kerja untuk mengelola risiko keamanan informasi (*vulnerability* atau kerawanan) sesuai dengan harapan perusahaan disajikan pada Tabel 9.

Tabel 9. Kontrol ISO 27001 untuk Kerawanan

Kerawanan	Kontrol	Rencana kerja
Persyaratan *sharing password,* pengamanan identitas dan hak akses pengguna yang tidak tepat.	*User responsibilities*	Melakukan sosialisasi terhadap pengguna untuk mengikuti pedoman pengamanan yang baik dalam pemilihan dan penggunaan password.
Informasi cetak maupun non-cetak yang diletakkan atau disimpan di tempat yang tidak tepat.	*Media Handling*	Melindungi penangan dan penyimpanan informasi dari pengungkapan yang tidak sah/penyalahgunaan.
Patching terlambat atau versi ketinggalan	*System planning and acceptance*	Menguji sistem informasi yang sesuai untuk menyesuaikan kriteria acceptance yang baru, upgrade, dan versi baru.
Proses *maintenance* dan monitoring tidak berjalan dan tidak terpantau.	*Monitoring*	Menetapkan dan menjalankan prosedur untuk pemantauan panggunaan fasilitas informasi penggunaan sistem

Kerawanan	Kontrol	Rencana kerja
Perangkat lunak dan perangkat keras sudah habis *lifetime*-nya, *sparepart* sudah tidak didukung vendor	*Security of system files*	Membuat prosedur pengendalian instalasi perangkat yang terkait sistem operasional
	Equipment security	Membuat prosedur pemeliharaan barang untuk memastikan ketersediaan dan integritas layanan
Ada IP public yang bisa diakses oleh pengguna dari jarak jauh.	*Network Access control*	Melakukan identifikasi peralatan dan otentikasi pengguna
	Mobile computing and teleworking	Membuat kebijakan *teleworking*
	Terminating or change employment	Menghapus seluruh hak akses pengguna yang telah berhenti, maksimal sehari setelah status user dilaporkan secara resmi
Konfigurasi sistem yang masih mengikuti bawaan pabrik, *password* mudah ditebak.	*Application and Information access control*	Membuat konfigurasi, pembatasan sistem aplikasi dan fungsinya sesuai dengan kebijakan yang ada.
Beberapa PC belum dikonfigurasi dengan benar.	*Network access control*	Mengendalikan akses secara fisik dan logical terhadap *diagnostic* dan *configuration port*
Password yang tidak dirubah secara berkala	*User Access Management*	Peninjauan hak akses pengguna secara regular dengan menggunakan proses formal.

Pada Tabel 9 dapat dilihat kontrol-kontrol sesuai standar ISO 27001 untuk mengelola risiko (kerawanan) sampai pada tingkat yang dapat diterima oleh PT XYZ. Kontrol-kontrol tersebut berasal dari 11 (domain) dalam ISO 27001. Sedangkan kontrol-kontrol ISO 27001 terhadap *threats* atau ancaman SI/TI di lingkungan PT XYZ disajikan dalam Tabel 10.

Tabel 10. Kontrol ISO 27001 untuk Ancaman

Ancaman	**Kontrol ISO 27001**	Rencana kerja
Serangan virus, worm dan malware	*Reporting information security events and weakness*	Mengurangi dampak akibat serangan virus dengan cara mengimplementasikan dan menyusun laporan kejadian, respon insiden dan prosedur eskalasi
Spam pada email	*Exchange of information*	Melakukan perlindungan informasi yang tepat dalam bentuk pesan elektronik.
Penerobosan sistem oleh pihak eksternal	*Termination or change of employment*	Melakukan penyesuaian dengan perubahan hak akses semua pegawai yang masa kerjanya sudah berakhir.
	Network access control	Melakukan metode otentikasi yang tepat untuk mengendalikan akses pengguna.
Penerobosan sistem oleh pihak internal	*User access management*	Mengendalikan alokasi *password* dengan proses manajemen formal.
	Network access control	Otentikasi yang tepat untuk mengendalikan akses pengguna.
Kegagalan sistem akibat kerusakan perangkat keras dan perangkat lunak	*Equipment security*	Membuat prosedur pemeliharaan barang untuk memastikan ketersediaan dan integritas layanan
Pengrusakan aset secara fisik	*Equipment security*	Menempatkan dan melindungi peralatan dari ancaman/bahaya lingkungan serta akses oleh yang tidak berhak.
Kartu akses yang terdaftar bisa digunakan siapa saja	*Secure Area*	Membuat perimeter keamanan untuk melindungi area yang berisi informasi dan fasilitas pengolahan informasi.

Pada Tabel 10 dapat dilihat kontrol-kontrol sesuai standar ISO 27001 untuk mengelola risiko (ancaman) sampai pada tingkat yang dapat diterima oleh PT XYZ. Kontrol-kontrol tersebut berasal dari 11 (domain) dalam ISO 27001. Sedangkan kontrol-kontrol dampak atau ancaman SI/TI di lingkungan PT XYZ disajikan dalam Tabel 11.

Tabel 11. Kontrol ISO 27001 untuk Dampak

Dampak	Kontrol ISO 27001	Rencana Kerja
Kinerja karyawan dan kegiatan operasional terganggu	*During Employment*	Melakukan pendidikan dan pelatihan keamanan informasi untuk semua karyawan.
Hasil rekaman CCTV tidak tersimpan	*Monitoring*	Kegiatan pengguna dan kejadian keamanan informasi dijaga untuk membantu investigasi di masa yang akan datang
Pantauan terhadap situasi keamanan informasi perusahaan tidak ada	*Monitoring*	Pemantauan penggunaan fasilitas pengolahan informasi
Pengrusakan fisik *Access point*	*Equipment security*	Menempatkan atau melindungi peralatan untuk mengurangi risiko dari ancaman dan bahaya lingkungan dan akses oleh yang tidak berhak
Karyawan tidak dapat menggunakan *Access point*	*Responsibilities for asset*	Penggunaan informasi dan aset yang dapat diterima terkait dengan fasilitas pengolahan informasi.
Tidak ada penyaring informasi yang keluar dan masuk	*Network Access Control*	Segresi jaringan menggunakan mekanisme perimeter keamanan yang sesuai
Beberapa jaringan akan lumpuh dan mengganggu operasional perusahaan	*Network Access Control*	Menerapkan pengendalian routing dalam jaringan untuk memastikan koneksi jaringan dan aliran informasi tidak mengganggu jaringan yang vital.
Koneksi dengan bank yang masih menggunakan dial up akan terganggu	*Network Access Control*	Menetapkan pengendalian routing berdasarkan skema sumber dan tujuan yang dikenal.
Ruangan penting dapat dimasuki dengan mudah oleh pihak yang tidak berhak	*Secure Areas*	Membuat perimeter keamanan untuk melindungi area yang berisi informasi dan fasilitas pengolahan informasi.
Penyebaran virus memalui PC dan laptop yang terhubung ke jaringan.	*Network Access Control*	Membuat identifikasi peralatan secara otomatis guna mengotentikasi koneksi lokasi dan jenis peralatan secara spesifik.
User dapat mengambil informasi penting mengandalkan port USB yang terbuka	*Network access control*	Mengendalikan akses secara fisik dan logical terhadap *diagnostic* dan *configutaion port*
IP *conflict*	*Network Access Control*	Melakukan metode otentikasi yang tepat untuk mengendalikan akses pengguna.
PC *user* dapat diakses oleh pihak yang tidak berwenang	*User access management*	Mengendalikan alokasi password dengan proses manajemen formal.
File penting dalam server dapat dirubah oleh pihak yang tidak berwenang.	*User access management*	Peninjauan hak akses pengguna secara regular dengan menggunakan proses formal.
Bukan OS asli sehingga tidak bisa di-*update*.	*System planning and acceptance*	Melakukan pengujian sistem informasi yang sesuai guna menyesuaikan criteria acceptance sistem informasi yang baru, upgrade, dan versi baru
Komunikasi internal terganggu karena banyak *e-mail* yang berulang	*Exchange of information*	Melindungi informasi yang tepat dalam bentuk pesan elektronik.
Komunikasi eksternal terganggu akibat spam	*Exchange of Information*	Melindungi informasi yang tepat dalam bentuk pesan elektronik.
Pengrusakan *website* yang dapat mencemarkan nama baik	*Electronic commerce services*	Menjaga integritas informasi yang tersedia pada sistem yang digunakan untuk umum guna melindungi dan mencegah modifikasi yang tidak sah.
Hidup mati jaringan tidak terpantau	*Monitoring*	Menetapkan dan menjalankan prosedur untuk pemantauan panggunaan fasilitas informasi.
Karyawan tidak dapat mengisi form absen	*Responsibilities for asset*	Penggunaan informasi dan aset yang dapat diterima terkait dengan fasilitas pengolahan informasi.

Dampak	Kontrol ISO 27001	Rencana Kerja
Aplikasi rekaman CCTV akan terganggu	*Application and Information access control*	Mengisolasi lingkungan aplikasi sistem yang sensitif
Komputer akan diserang virus	*Reporting information security events and weakness*	Melakukan implementasi dan penyusunan terhadap pelaporan kejadian, respon insiden dan prosedur eskalasi
Proses pengiriman informasi dari bank akan terganggu sehingga terjadi penundaan dalam percetakan.	*Network Access Control*	Mengendalikan akses dan persyaratan dalam aplikasi bisnis untuk jaringan yang digunakan bersama.
	External Parties	Mengidentifikasi risiko informasi organisasi dari proses bisnis yang melibatkan pihak-pihak eksternal
Informasi dapat diambil dan dirubah oleh pihak yang tidak berwenang	*User access management*	Peninjauan hak akses pengguna secara regular dengan menggunakan proses formal.
Kebocoran informasi yang disengaja	*During employment*	Melakukan pendidikan dan pelatihan keamanan informasi untuk semua karyawan.
Karyawan yang sudah resign masih bisa masuk ke webmail	*Terminating or Change of employment.*	Mengatur perubahan hak akses karyawan yang masa kerjanya sudah berakhir.

Pada Tabel 11 dapat dilihat kontrol-kontrol sesuai standar ISO 27001 untuk mengelola risiko (dampak) sampai pada tingkat yang dapat diterima oleh PT XYZ. Kontrol-kontrol tersebut berasal dari 11 (domain) dalam ISO 27001. Berdasarkan hasil pemetaan kontrol ISO 27001 terhadap ancaman, kerawananan, dan dampak kemudian disusun rekomendasi kebijakan, prosedur dan instruksi untuk meningkatkan keamanan informasi.

Rekomendasi Kebijakan dan Prosedur Keamanan Informasi

Kebijakan, prosedur, instruksi, dan dokumentasi yang direkomendasikan sesuai dengan hasil audit keamanan informasi berdasarkan standar ISO/IEC 27001:2005, terdapat 67 (enam puluh delapan) kebijakan, prosedur, instruksi, dan dokumentasi yaitu sebagai berikut:

1. Kebijakan *clear desk* dan *clear screen*.
2. Kebijakan yang mengatur jaringan dan *service* yang disediakan atas jaringan.
3. Kebijakan pengelompokan layanan informasi, seperti memisahkan jaringan wireless terhadap jaringan internal dan umum.
4. Kebijakan pengendalian akses dan persyaratan dalam aplikasi bisnis.
5. Kebijakan pengamanan untuk melindungi risiko dari penggunaan fasilitas *mobile computing* dan *teleworking*.
6. Kebijakan pengendalian akses terhadap informasi dan fungsi sistem aplikasi
7. Kebijakan penggunaan hak akses
8 Kebijakan dalam menjaga kerahasiaan password
9. Kebijakan pendisiplinan untuk pegawai yang melakukan pelanggaran keamanan
10. Kebijakan kepemilikan aset.
11. Kebijakan dan prosedur pengendalian secara formal untuk melindungi pertukaran informasi.
12. Kebijakan dan prosedur untuk melindungi informasi yang berkaitan dengan interkoneksi sistem informasi bisnis
13. Prosedur untuk manajemen media yang dapat dipindahkan
14. Prosedur pemusnahan media yang tidak diperlukan
15. Prosedur penanganan dan penyim- panan informasi.
16. Prosedur pemantauan penggunaan fasilitas pengolahan informasi.

17. Prosedur pengamanan fasilitas log dan informasi log hasil pemantauan dan pengawasan dari gangguan dan akses yang tidak sah.
18. Prosedur untuk mengendalikan instalasi perangkat lunak pada sistem operasional.
19. Prosedur perlindungan informasi
20. Prosedur akses ke informasi
21. Prosedur tempat perlindungan peralatan keamanan untuk melindungi dari ancaman oleh pihak yang tidak berwenang
22. Prosedur sarana pendukung untuk melindungi peralatan dari kegagalan catu daya
23. Prosedur pengamanan kabel dan jaringan yang membawa data informasi.
24. Prosedur pemeliharaan peralatan untuk memastikan ketersediaan dan integritas layanan.
25. Prosedur keamanan untuk melindungi peralatan yang berada diluar lokasi.
26. Prosedur peralatan informasi penyimpanan yang memuat informasi sensitif dan perangkat lunak berlisensi telah dihapus sebelum dibuang.
27. Prosedur yang mengatur peralatan, informasi atau perangkat lunak dibawa keluar lokasi.
28. Prosedur otentikasi untuk mengendalikan akses pengguna remote.
29. Prosedur identifikasi peralatan secara otomatis mengotentikasi koneksi dan peralatan yang digunakan secara spesifik.
30. Prosedur pengendalian akses fisik dan logical terhadap diagnostic dan konfigurasi port.
31. Prosedur pengakhiran atau perubahan pekerjaan
32. Prosedur pengembalian aset organisasi ketika pekerjaan, kontrak dan perjanjian berakhir
33. Prosedur penghapusan hak akses untuk karyawan ketika pekerjaan, kontrak dan perjanjian berakhir
34. Prosedur keamanan lingkungan untuk aplikasi yang sensitif
35. Prosedur pendaftaran dan pembatalan dalam pemberian dan pencabutan akses terhadap seluruh layanan dan sistem informasi.
36. Prosedur penggantian password secara regular
37. Prosedur pelaporan insiden, respon insiden dan prosedur eskalasi untuk mengamankan informasi yang terkena serangan virus
38. Prosedur perlindungan informasi yang termasuk dalam layanan *electronic commerce* yang memalui jaringan publik.
39. Prosedur perimeter keamanan fisik untuk melindungi area yang berisi informasi dan fasilitas informasi
40. Prosedur pengamanan fisik untuk kantor, ruangan dan fasilitas
41. Prosedur perlindungan untuk media yang memuat informasi terhadap akses yang tidak sah, penyalahgunaan atau kerusakan selama diluar batas fisik organisasi.
42. Prosedur perlindungan informasi dalam bentuk pesan elektronik
43. Prosedur penanganan risiko terhadap informasi organisasi dan fasilitas pengolahan informasi dari proses bisnis yang melibatkan pihak-pihak eksternal
44. Instruksi untuk mengikuti pedoman pengamanan yang baik dalam pemilihan dan penggunaan password
45. Instruksi untuk memastikan peralatan yang ditinggal sudah terlindungi dengan tepat. Misalnya log off saat meninggalkan komputer.
46. Instruksi dokumentasi dan definisi terhadap media yang dapat dipindahkan.

47. Membuat instruksi guna menerapkan keamanan sesuai kebijakan dan prosedur yang sudah ditetapkan
48. Dokumentasi sistem yang sudah terlindungi atas akses yang tidak sah.
49. Dokumentasi yang disesuaikan dan diproyeksikan untuk pemenuhan kapasitas mendatang, guna memastikan kinerja sistem.
50. Dokumentasi sistem informasi yang baru, yang sudah diupgrade dan versi baru yang sdah diuji.
51. Dokumentasi log audit untuk membantu investigasi di masa mendatang.
52. Dokumentasi hasil pemantauan dan pengawasan yang diperlukan berdasarkan tingkat risiko.
53. Dokumentasi kegiatan sistem administrator dan operator dan dianalisa secara regular.
54. Dokumentasi kesalahan dalam melakukan log audit dan dokumentasi log ditentukan berdasarkan tingkat risiko.
55. Dokumentasi waktu yang sudah disingkronisasikan dengan sumber penunjuk waktu akurat yang sudah disepakati.
56. Dokumentasi user akses terhadap layanan yang diberikan dan kewenangan penggunaannya.
57. Dokumentasi dan melaporkan setiap kelemahan atas sistem atau layanan
58. Dokumentasi karyawan yang diperbolehkan masuk ke daerah secure untuk memastikan hanya karyawan yang berwenang yang mempuinyai akses masuk
59. Dokumentasi perlindungan fisik terhadap kerusakan akibat dari bencana alam dan buatan manusia yang mungkin akan terjadi
60. Dokumentasi pedoman kerja dalam area yang aman
61. Dokumentasi titik akses publik, seperti area bongkar muat dan titik lainnya di mana orang yang tidak berwenang dapat masuk kedalam lokasi.
62. Dokumentasi perjanjian untuk pertukaran informasi pertukaran informasi
63. Dokumentasi pelatihan kepeduliaan dan kebijakan serta prosedur yang mutakhir secara regular.
64. Dokumentasi persyaratan keamanan sebelum memberikan akses kepada pihak ketiga.
65. Dokumentasi perjanjian dengan pihak ketiga yang meliputi pemberian hak akses, pengolahan, pengelolaan komunikasi dan informasi atau penambahan produk atau jasa.
66. Dokumentasi semua aset dengan jelas dan inventaris semua aset penting.
67. Dokumentasi penggunaan aset.

Sedangkan kebijakan, prosedur, instruksi, dan dokumentasi yang sudah ada, perlu ditinjau ulang pada proses audit keamanan informasi, yaitu sebagai berikut:

1. Kebijakan pemakaian fasilitas perangkat keras dan perangkat lunak komputer
2. Kebijakan penggunaan *password*
3. Kebijakan penggunaan internet
4. Kebijakan penggunaan e-mail perusahaan
5. Prosedur standar keadaan darurat untuk penanganan server
6. Prosedur penanganan komplain
7. Prosedur *copy* data/program dan *restore* data/program
8. Prosedur peminjaman dan pengembalian barang TI milik perusahaan
9. Prosedur pengadaan barang TI
10. Prosedur *back-up* data
11. Prosedur pengamanan data dan pelaporan insiden.

PENUTUP

Simpulan

Kesimpulan yang dapat diambil dari penelitian ini yaitu Kebijakan, prosedur, instruksi, dan dokumentasi keamanan informasi yang ada dan berlaku di PT XYZ belum dikaji ulang dan cakupannya belum komprehensif mengatur aspek keamanan informasi dari ISO 27001/ISMS. Salah satu domain dan kontrol objektif yang belum diterapkan atau belum diatur dalam kebijakan, prosedur, instruksi, maupun dokumentasi adalah manajemen keberlangsungan bisnis. Dalam tahap ini perusahaan belum memiliki langkah-langkah yang harus dilakukan jika terjadi kebocoran informasi, padahal kebocoran informasi sekecil apapun dapat menghilangkan kepercayaan pelanggan dan menyebabkan terhentinya keberlangsungan bisnis perusahaan.

Kebijakan dan prosedur yang ada, yaitu sebanyak 11 (sebelas) kebijakan dan prosedur, belum dapat dikatakan *best services* terhadap keamanan informasi. Kebijakan dan prosedur yang ada belum pernah dikaji lebih lanjut dan cakupan dari 11 (sebelas) kebijakan dan prosedur yang ada belum mencerminkan aspek keamanan informasi dari ISO 27001/ISMS. Hal inilah yang menjadi salah satu penyebab lemahnya keamanan informasi PT. XYZ.

Rekomendasi kebijakan, prosedur, instruksi, dan dokumentasi keamanan informasi disusun berdasarkan hasil audit keamanan informasi sesuai domain, kontrol, dan kontrol objektif standar ISO/IEC 27001:2005. Terdapat 67 (enam puluh tujuh) kebijakan, prosedur, instruksi, dan dokumentasi yang direkomendasikan untuk meningkatkan keamanan informasi melalui penerapan kontrol-kontrol. Untuk menentukan skala prioritas dalam perbaikan kebijakan, prosedur, instruksi, dan dokumentasi keamanan informasi, dapat dilakukan dengan memperhatikan 3 (tiga) prinsip utama keamanan informasi, yaitu *confidentiality, integrity dan availability*. Lima prinsip berikutnya bisa dilakukan secara bertahap setelah 3 (tiga) prinsip utama terpenuhi. Adapun tahapan dalam perbaikan yang merupakan sebuah siklus perbaikan berkelanjutan, aktivitas mendasar yang perlu dilakukan yaitu: kaji ulang kebijakan, prosedur, dan instruksi, dan dokumentasi yang berlaku; kemudian menyusun dan menetapkan kebijakan, prosedur, instruksi, dan dokumentasi sesuai dengan standar ISO/IEC 27001:2005; melakukan sosialisasi terhadap kebijakan, prosedur, instruksi, dan dokumentasi baru yang sudah disusun dan ditetapkan; serta melakukan evaluasi terhadap kebijakan, prosedur, instruksi, dan dokumentasi baru yang sudah ditetapkan dan diberlakukan.

Saran

Rekomendasi bagi PT XYZ sebaiknya dilakukan sosialisasi dan program kepedulian keamanan diren- canakan dan dilakukan pelatihan dan *sharing knowledge* khususnya terkait keamanan informasi untuk mendukung pelaksanaan aturan.

PT XYZ juga dapat menyusun kebijakan keamanan informasi yang komprehensif berdasarkan praktik terbaik lainnya sesuai kebutuhan organisasi. Kemudian sebaiknya meminta dan mempertimbangkan masukan-masukan tidak hanya dari pihak internal organisasi dalam penyusunan rancangan kebijakan dan prosedur.

PT XYZ dapat menerapkan kebijakan, prosedur, instruksi, dan dokumentasi keamanan informasi sesuai dengan praktik terbaik ISO 27001. Selain itu juga perlu melakukan evaluasi terhadap penerapan kebijakan, prosedur, instruksi, dan dokumentasi keamanan informasi sehingga dapat dilakukan perbaikan berkelanjutan guna meningkatkan keamanan informasi.

PT XYZ juga perlu membentuk struktur dan penugasan khusus terkait keamanan informasi, misalnya pegawai atau karyawan PT. XYZ yang ditugaskan sebagai *Chief of Information Security Officer* (CISO), konsultan

keamanan informasi, manajer keamanan informasi, analis keamanan informasi, dan teknisi keamanan informasi.

Rekomendasi untuk penelitian selanjutnya, diharapkan dapat dilakukan penelitian audit operasional keamanan informasi dan audit kelayakan kebijakan, prosedur, instruksi, dan dokumentasi keamanan informasi. Audit berdasarkan standar ISO 27001 versi terbaru, sehingga hasil audit dan rekomendasi yang diberikanlebih *update* dan sesuai dengan perkembangan permasalahan keamanan informasi. Perlunya melibatkan pihak ketiga dalam ruang lingkup audit keamanan informasi.

DAFTAR PUSTAKA

Akmal, M. (2011). *Perancangan kebijakan dan standar manajemen layanan teknologi informasi mengacu Kepada ISO 20000, ISO 27001, dan COBIT: Studi kasus PT. Bhanda Ghara Reksa (Persero)*. Karya Akhir Program Magister Teknologi Informasi Universitas Indonesia. Jakarta: Universitas Indonesia.

Arora, V. (2010). *Comparing different information security standards : COBIT vs ISO 27001*. Qatar: Carnegia Mellon University.

Aygun, B. (2010). *Unification of IT process Models into asimple framework supplemented by turkish web based application.* Turki: Department of Information Systems.

Bastian, I. (2007). *Akuntansi yayasan dan lembaga publik.* Jakarta: Erlangga.

Boynton, W. c., Johnson, R. N., & Kell, W. G. (2004). *Modern auditing* (7 ed.). John Wiley & Sons Incorporated.

BSN. (2009). *SNI ISO/IEC 27001:2009: Teknologi Informasi-Teknik Keamanan-Sistem Manajemen Keamanan Informasi-Persyaratan.* Jakarta: Badan Standardisasi Nasional.

Gama Secure Systems Limited . The new versions of ISO/IEC 27001 and 27002 are now Final Draft International Standards. (http://www.gammassl.co.uk/27001/revision.php, diperoleh pada 23 September 2013).

International Standard Organization. (http://www.iso.org/iso/catalogue_detail?csnumber=54534, diperoleh tanggal 23 September 2013).

Justanieah, M. (2009). *Information Security management systems an ISO 27001 introduction.* Jeddah: ISACA.

Maulidevi, N.U. (2007) *"Perancangan Model Tata Kelola Teknologi Informasi Berbasis COBIT pada proses pengelolaan pata studi kasus : PT PLN (Persero) Distribusi Jawa Timur"*. Master Thesis pada Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung. Bandung: Institut Teknologi Bandung.

Mufadhol. (2009). Kerahasiaan dan keutuhan keamanan data dalam menjaga integritas dan keberadaan informasi data. *Jurnal Transfor- matika, volume 6, No 2* , 80.

Regalado, R.O., (2007), *Statement of Applicability Template*. (http://www.ISO27001security.com, diperoleh tanggal 15 Desember 2011).

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

Syafrizal, M. (2007). ISO 17799 : Standar Sistem Manajemen Keamanan Informasi. *Seminar Nasional Teknologi 2007 (SNT 2007)* , 10.

Tim penyusun modul program pendidikan non gelar auditor sektor publik. 2007. *Dasar-dasar audit internal sektor publik.* Jakarta: Sekolah Tinggi Akuntansi Negara.

Whitman, M. E., & Mattord, H. J. (2010). *Management of information security, Third Edition.* Boston: Course Technology.