JURNAL ILMIAH
REKAYASA
http://journal.trunojoyo.ac.id/rekayasa

Volume 9 Nomor 2, Oktober 2016 Hlm. 108-115
ISSN 0216-9495 (Print)
ISSN 2502-5325 (Online)

Analisa Manajemen Resiko Keamanan Informasi pada Kantor Pelayanan Pajak Pratama XYZ

Iwan Santosa[1], Dwi Kuswanto[2]
[1,2]Program Studi Teknik Informatika, Universitas Trunojoyo Madura
[1]iwan@trunojoyo.ac.id,[2]dwikuswanto@if.trunojoyo.ac.id

ABSTRAK

Penggunaan Teknologi Informasi di lembaga-lembaga pemerintahan saat ini sangat dibutuhkan untuk mempermudah melakukan pendataan dan pengambilan keputusan yang strategis. Kantor Pelayanan Pajak Pratama XYZ yang merupakan salah satu lembaga pemerintahan yang bergerak dibidang keuangan memiliki data yang cukup banyak. Penggunaan Teknologi informasi bukan sekedar penting tapi sudah menjadi keharusan, melihat Pajak merupakan salah satu pendapatan negara yang utama. Data dan informasi yang terdapat pada Lembaga ini tidak hanya perlu penyimpanan secara digital akan tetapi juga memerlukan pengamanan yang serius. Kebocoran akan data yang ada dapat berakibat fatal bagi kepentingan negara. Untuk itu Sistem Manajemen Keamanan Informasi(SMKI) diperlukan dalam pengelolaan keamanannya. Dalam mengimplementasikan ISO 27001 sebelumnya diperlukan manajemen resiko keamanan informasi. Kegiatan manajemen resiko ini diperlukan untuk menentukan Control Objectives yang akan diambil untuk melakukan penanganan resiko yang kemungkinan terjadi. Dalam mengimplementasikan manajemen resiko didapatkan hasil hanya pada aset username dan password level yang resikonya High (6,67%) dari 15 aset yang sudah terdaftar, sehingga diperlukan kontrol keamanan yang berhubungan dengan username dan password untuk meminimalisir atau mengurangi terjadinya resiko.

Kata Kunci: Manajemen resiko,SMKI, iso 27001.

ANALYSIS OF INFORMATION SECURITY RISK MANAGEMENT IN TAX SERVICE OFFICE PRATAMA XYZ

ABSTRACT

Use of Information Technology in government institutions at this time is needed to make it easier to collect data and strategic decision making. KPP Pratama XYZ which is one of the government agencies engaged in finance have enough data. The use of information technology is not just important but has become imperative, see Tax is one of the main income of the country. The data and information contained in this Organization not only need a digital storage but also require security seriously. Leakage will be the existing data can be fatal to the interests of the state. For the Information Security Management System (ISMS) is required in the management of safety. In previously required to implement ISO 27001 information security risk management. Risk management activities is necessary to determine the Control Objectives that will be taken to have addressed the risk probabilities. In implementing risk management on assets showed only a username and password High risk level (6,67%) of 15 assets that are registered, so that the necessary security controls associated with a username and password to minimize or reduce the risk.

Keywords: Risk Management,SMKI, ISO 27001.

PENDAHULUAN

Keamanan data elektronik menjadi hal yang sangat penting di perusahaan penyedia jasa teknologi informasi (TI) maupun industri lainnya, seperti: perusahaan export-import, tranportasi, lembaga keuangan, pendidikan, pemberitaan, hingga perbankan yang menggunakan fasilitas TI dan menempatkannya sebagai infrastruktur kritikal (penting).

Informasi atau data adalah aset bagi perusahaan. Keamanan data secara tidak langsung dapat memastikan kontinuitas bisnis, mengurangi resiko, mengoptimalkan return on investment dan mencari kesempatan bisnis. Semakin banyak informasi perusahaan yang disimpan, dikelola dan disharing maka semakin besar pula resiko terjadinya kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan.

Bagaimana data atau informasi tersebut dikelola, dipelihara dan diekspose, melatarbelakangi disusunnya ISO 17799, standar untuk sistem manajemen keamanan informasi. Penyusunan standar ini berawal pada tahun 1995, dimana sekelompok perusahaan besar seperti BOC, BT, Marks & Spencer, Midland Bank, Nationwide Building Society, Shell dan Unilever bekerja sama untuk membuat suatu standar yang dinamakan BS (British Standard) 7799. BS 7799 Part 1: the Code of Practice for Information Security Management. Februari 1998 BS 7799 Part 2: The Specification for Information Security Management Systems (ISMS) menyusul diterbitkan. Desember 2000 ISO (International Organization of Standardization) dan IEC (International Electro-Technical Commission) mengadopsi BS 7799 Part 1 dan menerbitkannya sebagai standar ISO/IEC 17799:2000 yang diakui secara internasional.

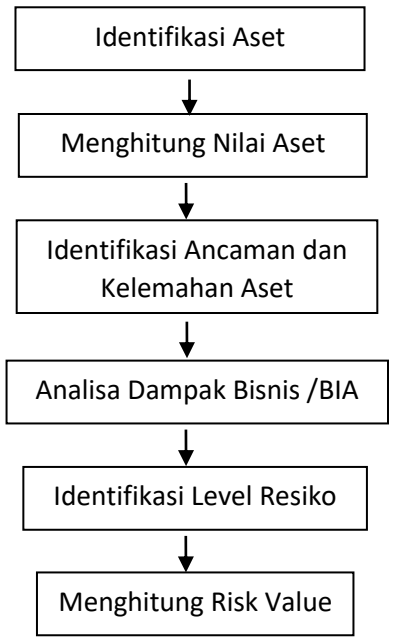
Keamanan informasi terdiri dari perlindungan terhadap aspek-aspek berikut:

1. *Confidentiality* (kerahasiaan) aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
2. *Integrity* (integritas) aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin fihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.
3. *Availability* (ketersediaan) aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).

Keamanan informasi diperoleh dengan mengimple-mentasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur-prosedur, struktur-struktur organisasi dan piranti lunak (Syafrizal,2007).

Sebelum menerapkan kontrol keamanan, perlu dilakukan manajemen resiko supaya dapat memaksimalkan pemilihan kontrol keamanan. Dalam penelitian ini telah dilakukan analisa resiko terhadap aset yang ada.

Gambar 1. Keamana informasi (CIA)



Gambar 2. Diagram Alir Penelitian

METODE PENELITIAN

Pada pembahasan ini akan dijelaskan metodologi dalam penelitian ini mulai dari pengumpulan data untuk melakukan identifikasi aset, melakukan perhitungan Nilai aset yang telah dikumpuklan, melakukan identifikasi ancaman dan kelemahan aset, melakukan analisa dampak bisnis atau yang sering disebut *Business Impact Analysis (BIA)*, melakukan identifikasi level resiko dan yang terakhir menghitung risk value untuk mengetahui level resiko dari aset.

Tabel 1. Kriteria *Convidentiality*

Kriteria *Cinvidentiality*	Nilai *Convidentiality (NC)*
Public	0
Internal use only	1
Private	2
Convidential	3
Secret	4

Tabel 2. Kriteria *Integrity*

Kriteria *Integrity*	Nilai *Integrity (NI)*
No Impact	0
Minor Incident	1
General Disturbance	2
Mayor Disturbance	3
Unacceptable damage	4

Tabel 3. Kriteria Availability

Kriteria *Availability*	Nilai *Availability (NV)*
No Availability	0
Office Hour Availability	1
Strong Availability	2
High availability	3
Very High Availability	4

Tahap awal penelitian ini adalah mengumpulkan data aset yaitu aset yang mengandung data dan atau informasi. Identifikasi Aset dilakukan untuk menentukan aset yang berhubungan dengan kontrol akses di KPP Pratama XYZ.

Setelah aset teridentifikasi, langkah selanjutnya yaitu melakukan perhitungan nilai aset. Pendekatan yang dilakukan dengan menggunakan tiga aspek keamanan, yaitu kerahasiaan (*confidentiality*), keutuhan (*Integrity*) dan ketersediaan (*availiability*).

Perhitungannya dilakukan dengan menggunakan rumus :

NA = NC + NI + NV

*NA : **N**ilai **A**set*
*NC : **N**ilai **C**onvidentiality*
*NI : **N**ilai **I**ntegrity*
*NA : **N**ilai A**v**aliability*

Perhitungan selanjutnya adalah melakukan identifikasi ancaman dan kelemahan terhadap masing-masing aset, kemudian menentukan nilai rerata probabilitas kemunculan ancaman dan kelemahan dengan menggunakan rentang nilai sebagai berikut :

1. *Low* : 0,0 - 0,3
2. *Medium* : 0,4 – 0,6
3. *High* : 0,7 – 1,0

Langkah selanjutnya adalah menentukan analisa dampak bisnis atau yang sering disebut *Business Impact Analysis* (BIA). Kriteria penilaian untuk BIA dapat dilihat pada tabel 4 dibawah ini :

Penilaian level resiko menggunakan matriks resiko seperti Tabel 5. Nilai yang didapatkan berasal dari perkalian antara *Probability of threat* (probabilitas ancaman) dengan dampak bisnis BIA.

Tabel 4. Kriteria Nilai BIA

Batas Toleransi gangguan	Keterangan	Nilai BIA
< 1 minggu	Not critical (NC)	0
1 – 2 hari	Minor critical (MiC)	1
< 1 hari	Mayor critical (MaC)	2
< 12 jam	High critical (HC)	3
< 1 jam	Very high critical(VHC)	4

Tabel 5. Matrik Level Resiko

Prob. Threat	Dampak Bisnis				
	NC 0	MiC 1	MaC 2	HC 3	VHC 4
Low (0,1)	LOW 0	LOW 0,1	LOW 0,2	LOW 0,3	LOW 0,4
Med (0,5)	LOW 0	MED 0,5	MED 1,0	MED 1,5	MED 2,0
High (1,0)	LOW 0	MED 1,0	MED 2,0	HIGH 3,0	HIGH 4,0

Untuk menentukan apakah resiko diterima atau diperlukan pengelolaan resiko maka perlu menghitung nilai dari resiko yang ada. Nilai Resiko dapat dihitung dengan menggunakan rumus :

Risk Value = NA X BIA X NT

Keterangan :
NA : Nilai Aset
BIA : *Business Impact Analysis*
NT : Nilai *Threat*

Setelah mendapatkan nilai resiko, level resiko didapatkan dengan menyesuaikan nilai resiko dengan Tabel 5 Matrik Level Resiko.

Hasil yang didapatkan setiap aset akan teridentifikasi tingkat level resikonya. Level resiko berdasarkan Tabel tersebut menunjukkan *Low, Medium* atau *High*. Dari hasil tersebut aset yang akan dilakukan pengelolaan resiko adalah aset yang beresiko *High*.

HASIL DAN PEMBAHASAN

Berdasarkan pengambilan data dengan wawancara dan observasi di KPP Pratama XYZ didapatkan data aset seperti terlihat pada Tabel 6. Daftar Aset dibagi menjadi jenis Aset yang terdiri dari perangkat keras, perangkat lunak dan Data.

Tabel 6. Aset

No	Jenis Aset	Aset
1	Perangkat Keras	PC, Server, Jaringan fisik Kabel , Kamera CCTV,DVR CCTV Cisco Router
2	Perangkat Lunak	ESPT,EFAKTUT,EFILING,EBILING, SIM-Kepegawaian, SIM-WP, SIM-Pajak,WEB-Server
3	Data	Username dan Password

Dari data aset yang telah didapatkan selanjutnya menghitung nilai aset, dan dari hasil observasi dan wawancara didapatkan nilai aset yang teridentifikasi seperti tabel 7 dibawah ini.

Langkah selanjutnya adalah mengidentifikasi kelemahan dan ancaman untuk mendapatkan Nilai Threat (NT). Hasil identifikasinya terlihat pada tabel 8.

Tabel 7. Nilai Aset

No	Aset	Kriteria			Nilai Aset
		NC	NI	NV	
1	PC	2	1	2	5
2	Server	4	4	4	12
3	Jaringan Fisik Kabel	3	2	3	8
4	Kamera CCTV	2	2	2	6
5	DVDR CCTV	2	2	2	6
6	Cisco Router	3	2	4	9
7	ESPT	3	3	3	9
8	EFAKTUT	3	3	3	9
9	EFILLING	3	2	3	8
10	EBILLING	3	2	2	7
11	SIM-Kepegawaian	2	2	2	6
12	SIM-WP	2	2	3	7
13	SIM-Pajak	3	3	3	9
14	Web Server	4	3	3	10
15	Data User dan Password	4	3	3	10

Tabel 8. Probabilitas dan Nilai Ancaman (NT)

Aset	Kejadian	Jenis ancaman/ kelemahan	Prob. (low/ med/ high)	Event	Nilai Prob.	∑ PO	NT
PC	Pencurian PC	ancaman	low	0	0	0	-
Server	Pencurian PC	ancaman	low	0	0	0	-
	Illegal Akses	ancaman	low	0	0		
Jaringan	Illegal Akses	ancaman	low	0	0	0	-
	Pencurian PC	ancaman	low	0	0		
Kamera CCTV	Pencurian PC	ancaman	low	0	0	0	-
	Perusakan	ancaman	low	0	0		
DVDR CCTV	Pencurian Perangkat	ancaman	low	0	0	0	-
	Perusakan	ancaman	low	0	0		
	Pencurian Rekaman	ancaman	low	0	0		
Cisco Router	Illegal Akses	ancaman	low	0	0	0	-
	Pencurian	ancaman	low	0	0		
ESPT	Aplikasi tidak terupdate	kelemahan	low	0	0	0.4	0.13
	serangan Virus	ancaman	low	3	0.15		
	Kegagalan Operasional	kelemahan	low	5	0.25		

Aset	Kejadian	Jenis ancaman/ kelemahan	Prob. (low/ med/ high)	Event	Nilai Prob.	∑ PO	NT
EFAKTUT	Aplikasi tidak terupdate	kelemahan	low	0	0	0.4	0.13
	serangan Virus	ancaman	low	6	0.3		
	Kegagalan Operasional	kelemahan	low	2	0.1		
EFILLING	Aplikasi tidak terupdate	kelemahan	low	0	0	0.3	0.10
	serangan Virus	ancaman	low	2	0.1		
	Kegagalan Operasional	kelemahan	low	4	0.2		
EBILLING	Aplikasi tidak terupdate	kelemahan	low	0	0	0.25	0.08
	serangan Virus	ancaman	low	4	0.2		
	Kegagalan Operasional	kelemahan	low	1	0.05		
SIM-Kep.	Aplikasi tidak terupdate	kelemahan	low	0	0	0.1	0.03
	serangan Virus	ancaman	low	1	0.05		
	Kegagalan Operasional	kelemahan	low	1	0.05		
SIM-WP	Aplikasi tidak terupdate	kelemahan	low	0	0	0.4	0.13
	serangan Virus	ancaman	low	6	0.3		
	Kegagalan Operasional	kelemahan	low	2	0.1		
SIM-Pajak	Aplikasi tidak terupdate	kelemahan	low	0	0	0.3	0.10
	serangan Virus	ancaman	low	5	0.25		
	Kegagalan Operasional	kelemahan	low	1	0.05		
Web Server	Aplikasi tidak terupdate	kelemahan	low	0	0	0.05	0.02
	serangan Virus	ancaman	low	0	0		
	Kegagalan Operasional	kelemahan	low	1	0.05		
Data User dan Password	Data pegawai yang pindah dan belum dihapus	kelemahan	low	5	0.25	0.5	0.13
	password yang panjang kharakternya kurang dari 6	kelemahan	low	0	0		
	penggunaan user dan password oleh pengguna lain	ancaman	high	1	0.05		
	penggunaan password yang tidak diubah-ubah	kelemahan	low	4	0.2		

Setelah melakukan identifikasi ancaman dan kelemahan sehingga mendapatkan hasil Nilai ancaman (NT), langkah selanjutnya adalah dengan menentukan nilai BIA dari masing-masing aset. Dari hasil wawancara dan observasi didapatkan nilai BIA seperti terlihat pada Tabel 9.

Langkah selanjutnya yaitu menghitung Nilai Resiko dari NA, BIA dan NT yang sudah didapatkan.

Tabel 9. BIA

Aset	Nilai BIA
PC	1
Server	4
Jaringan Fisik Kabel	2
Kamera CCTV	1
DVDR CCTV	1
Cisco Router	3
ESPT	2
EFAKTUT	2
EFILLING	2
EBILLING	2
SIM-Kepegawaian	3
SIM-WP	3
SIM-Pajak	3
Web Server	4
Data User dan Password	3

Dengan menggunakan Tabel 5 tentang matrik resiko akan didapatkan hasil level resiko. Hasil perhitungan dan level resiko terlihat pada tabel 10.

Dari tabel 10 didapatkan aset yang memiliki resiko tinggi dan diperlukan kontrol keamanan untuk mengurangi resiko yang terjadi adalah Data User dan Password dengan prosentase 6,67% dari data Aset yang terdaftar, 26,67% memiliki level Medium serta 66,67 memiliki level High.

KESIMPULAN

Dari hasil penelitian yang telah dilakukan dapat disimpulkan bahwa dari aset yang terdaftar hanya satu aset yang memiliki resiko *High* yaitu Data Username dan Password dengan prosentase 6,67%.

Untuk meningkatkan kualitas penelitian diperlukan analisa yang lebih banyak dari jenis kejadian, sehingga hasil analisanya lebih mendalam. Rekomendasi lainya yaitu penelitian dapat dilanjutkan kepada pemilihan kontrol keamanan dalam rangka menyusun portofolio SMKI.

Tabel 10. Nilai Resiko dan Level Resiko

No	Aset	Nilai Aset	Nilai Ancaman	BIA	Nilai Resiko	Level Resiko
1	PC	5	0	1	0	low
2	Server	12	0	4	0	low
3	Jaringan Fisik Kabel	8	0	2	0	low
4	Kamera CCTV	6	0	1	0	low
5	DVDR CCTV	6	0	1	0	low
6	Cisco Router	9	0	3	0	low
7	ESPT	9	0.13	2	2.34	med
8	EFAKTUT	9	0.13	2	2.34	med
9	EFILLING	8	0.1	2	1.6	low
10	EBILLING	7	0.08	2	1.12	low
11	SIM-Kepegawaian	6	0.03	3	0.54	low
12	SIM-WP	7	0.13	3	2.73	med
13	SIM-Pajak	9	0.1	3	2.7	med
14	Web Server	10	0.02	4	0.8	low
15	Data User dan Password	10	0.13	3	3.9	high

DAFTAR PUSTAKA

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

Sarno, R. 2009. Audit Sistem & Teknologi Informasi.Surabaya: ITS Press 2 ISO/IEC 27001:2005, Information Technology – Security Techniques – Information Security Management System – Requirements, 15 Oktober 2005

Sarno, R., Iffano, Irsyat 2009. Sistem Manajemen Keamanan Informasi berbasis ISO 27001. Surabaya: ITS Press.

Utomo, M.,Ali, A. H. N.,Affandi, I. (2012). Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya 1.Jurnal Teknik ITS. Vol. 1 No. 1

Rozas, I. S., Sarno, R. (2010). Bayesian Probabilistik Sebagai Pendekatan Heuristik untuk Manajemen Resiko Teknologi Informasi. Prosiding Seminar Nasional Manajemen Teknologi XII.

Aprian, R.,Rizal, S., Sobri, M.(2015).Perencanaan Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO 27001:2013. Jurnal Informatika