Sistem Manajemen Keamanan Informasi Berbasis ISO/IEC 27001:2013 Pada PT Angkasa Pura 1 (Persero) Surabaya

Yusuf Bahrudin Nizar [1] **Pantjawati Sudarmaningtyas** [2] **Slamet** [3]
Program Studi/Jurusan Sistem Informasi
Universitas Dinamika
Jl. Raya Kedung Baruk 98 Surabaya, 60298
Email : 1)yusufbahrudin97@gmail.com, 2)pantja@dinamika.ac.id , 3)slamet@dinamika.ac.id

Abstract: *Information security related to information assets is a critical aspect that must maintain by PT Angkasa Pura 1 (Persero) Surabaya, which handles the airport business sector includes services such as baggage control, aerodrome, and airport facilities. Information security systems that unwell manage can pose problems related to confidentiality, integrity, and availability. This study aims to improve security information systems thru risk assessment using the OCTAVE method to find the highest impact when the risk occurs and prioritization those risks. The objective and security controls build based on using ISO/IEC 27001:2013.*
The results of this study are the document of objective and security control, risk management documents, standard operational procedure (SOP) documents. The risk management documents related to information security, including risk assessment, risk identification, risk analysis, and evaluation at PT Angkasa Pura 1 (Persero) Surabaya. Standard Operational Procedure (SOP) documents include policy documents, work instructions, and work records that align with the selection of objective controls and security controls from risk management.

Keywords: *ISO27001, OCTAVE, Standard Operational Procedure*

PT Angkasa Pura I (Persero) Surabaya merupakan badan usaha milik negara dalam bidang usaha kebandarudaraan yang meliputi layanan pengendalian bagasi, layanan garbarata dan layanan fasilitas pengguna bandara. Salah satu misi PT Angkasa Pura 1 (Persero) Surabaya Yaitu mengusahakan jasa kebandaraudaraan melalui pelayanan prima yang memenuhi standar keamanan, kesalamatan, dan kenyamanan (PT Angkasa Pura 1, 2017). Untuk mengetahui proses yang ada pada layanan bisnis utama PT Angkasa Pura 1 (Persero) Surabaya dapat diperoleh dengan analisis *value chain*.

Kondisi saat ini banyak ditemukan ancaman (*Threat*) dan kelemahan (*Vurnerable*) dari segi manajerial maupun teknis antara lain: Ancaman (*Threat*) yang terjadi dari luar organisasi meliputi *virus*, *worm*, dan *malware* yang menyebabkan kerusakan, kehilangan, dan lambatnya akses data penerbangan pada aplikasi *Flight Information Display System* (FIDS) yang dibutuhkan untuk menjalankan salah satu layanan utama yaitu *baggage handling*. belum adanya kebijakan *recovery server* Ketika mengalami sebuah kegagalan sistem (*down*) yang menyebabkan informasi penerbangan tidak tersedia untuk pengunjung sehingga proses bisnis perusahaan terganggu. Berdasarkan *Service Level Agreement* (SLA) down time pada permasalahan tersebut paling lama terjadi selama 24 jam.

Belum adanya kebijakan manajemen asset terkait keamanan informasi sehingga tidak ada yang bertanggung jawab dalam mengelola asset informasi. Selain itu belum adanya kebijakan autentikasi dan otorisasi terkait keamanan informasi untuk pengguna yang memiliki hak akses terhadap informasi terkait penentuan kualitas, perencanaan, pengendalian dan evaluasi proses bisnis utama, sehingga ketika terjadi kehilangan atau kesalahan informasi proses bisnis dapat terganggu dan pihak manajer tidak dapat menelusuri terkait kesalahan yang terjadi.

Dengan demikian bentuk dukungan dalam pengendalian sistem manajemen keamanan informasi dari sisi *CIA* adalah dengan penyusunan dokumen Sistem Manajemen Keamanan Informasi dan pembuatan SOP (*Standard Operational Procedure*) dengan tujuan sebagai acuan kerja dan standarisasi untuk mengatur banyaknya orang yang menggunakan dan membuat proses bisnis yang ada pada PT Angkasa Pura 1 (Persero) Surabaya agar lebih terstruktur, juga meningkatkan kualitas keamanan informasi yang ada. Pembuatan Dokumen SOP (*Standard Operational Procedure*) dipilih melalui pengendalian kontrol

objektif dan kontrol keamanan menggunakan ISO/IEC 27001:2013 yang sesuai dengan kebutuhan keamanan informasi dengan mempertimbangkan hasil pengelolaan risiko keamanan informasi yang dilakukan.

METODOLOGI PENELITIAN

Penelitian ini dilakukan dalam 3 tahap yaitu tahap awal, tahap pengembangan, dan tahap akhir. Metodologi penelitian secara detil terdapat pada Gambar 1.

A. Studi Literatur

Studi literatur dilakukan dengan cara mempelajari dan mencari referensi, yang menjadi dasar keterkaitan topik penelitian yang berkaitan dengan keamanan informasi. Mengingat pentingnya keamanan informai bagi suatu organisasi, maka keamanan informasi sangat dibutuhkan untuk menjaga informasi dari seluruh ancaman yang mungkin terjadi, dalam upaya untuk memastikan atau menjamin kelangsungan bisnis, meminimalisasi risiko bisnis (Sarno & Iffano, 2009).

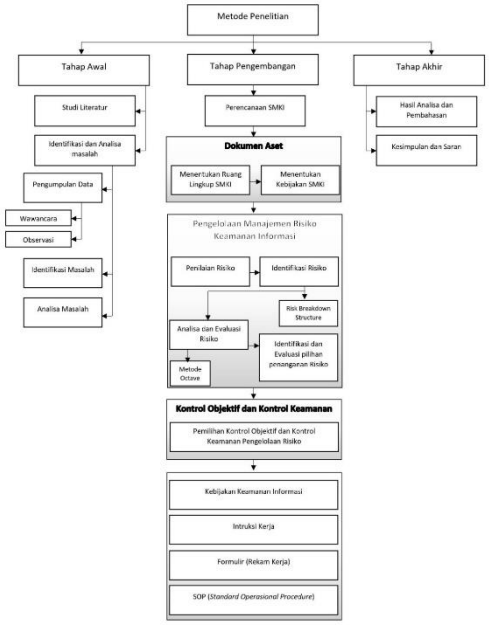
B. Identifikasi Masalah

Identifikasi masalah dilakukan dengan mengidentifikasi aset penting yang dimiliki organisasi, kebutuhan keamanan organisasi, permasalahan objek terkait dalam penelitian yakni pada PT Angkasa Pura 1 (Persero) Surabaya khususnya pada divisi ICT. Identifikasi dilakukan sesuai dengan hasil wawancara dan observasi terkait kondisi saat ini pada instansi.

C. Identifikasi Aset dan Risiko

Identifikasi risiko bertujuan untuk memahami seberapa besar dan identifikasi risiko apa yang akan diterima oleh organisasi jika informasi organisasi mendapat ancaman atau gangguan keamanan yang menyebabkan gagalnya penjagaan aspek keamanan informasi (ISO, 2013). Proses ini memeliki empat langkah, yaitu:

1) Identifikasi aset dan klasifikasi aset dengan menggunakan tabel aset
2) Menghitung nilai aset berdasarkan aspek keamanan informasi (CIA) dengan memberikan nilai masing-masing, setelah ini dihitung nilai asetnya.
3) Menghitung nilai ancaman dan kelemahan aset
4) Identifikasi dampak kegagalan terhadap aspek keamanam informasi (CIA) yaitu dengan membuat tabel identifikasi dampak bisnis disertai level dampak yang terjadi.



Gambar 1. Metodologi Penelitian

D. Penilaian risiko

Peniliaian terhadap risiko yang telah teridentifikasi dengan melakukan penerapan metode OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) dengan hitungan matematis dalam analisa penilaian risikonya. OCTAVE adalah sebuah pendekatan terhadap evaluasi risiko dari tiga aspek keamanan informasi yaitu *confidentiality, integrity,* dan *availability* yang komprehensif, sistematik, terarah, dan dilakukan sendiri. (Suprandono, 2009)

E. Identifikasi dan evaluasi penanganan risiko

Melakukan penanganan risiko langkah yang harus dilakukan yaitu mengidentifikasi atau menentukan pilihan pengelolaan risikonya. Pilihan pengelolaan risiko: menerina risiko dengan menerapakan kontrol keamanan yang sesuai, menerima risiko dengan menggunakan kriteria risiko yang telah diterapkan, dan menerima risiko dengan men-transfer risiko kepada pihak ketiga (asuransi, vendor, atau pihak tertentu) (Sarno & Iffano, 2009).

F. Penentuan ruang lingkup SMKI

Penentuan ruang lingkup ini sangat dibutuhkan dengan tujuan dokumen yang dihasilkan sesuai dengan kebutuhan permasalahan keamanan informasi pada divisi ICT. Dalam menentukan ruang lingkup Sistem Manajemen Keamanan Informasi (SMKI)

dibutuhkan identifikasi masalah dari sisi eksternal dan internal di bagian ICT.

HASIL DAN PEMBAHASAN

A. Identifikasi Aset Kritis

Daftar Aset kritis yang dimiliki divisi *Information Communication and Technology Department Head* (ICT) terdapat pada Tabel 1, dan secara lengkap disajikan pada lanjutan tabel 1 pada lampiran.

B. Identifikasi Ancaman dan kelamahan

Identifikasi ancaman dan kelemahan pada aset kritis dikategorikan ke dalam hardware, software, jaringan, data atau informasi dan SDM pada divisi *Information Communication and Department Head* (ICT). Daftar ancaman dan kelemahan terdapat pada Tabel 2 secara lengkap disajikan pada lanjutan tabel 2 pada lampiran.

Tabel 1. Daftar Aset Kritis

No	Ketegori	Aset
1.	Hardware	PC Server
2.	Software	FIDS Counter *check-in*
3.	Jaringan	Wifi Router Switch Kabel
4.	Data	Data Center Data Jadwal penerbangan Data Shift Kerja Pegawai Data Maskapai

Tabel 2. Identifikasi Ancaman dan Kelemahan

No	Kategori aset	Daftar aset	Ancaman dan kelemahan
1.	Hardware	Server	Bencana alam Kehilangan data Pencurian komponen Kerusakan server Server down
		PC	Server mati Bencana alam PC rusak Kerusakan komponen PC Pencurian komponen PC
	Software	FIDS	Serangan *virus,worm, mallware.* Kesalahan konfigurasi Akses ilegal Pembobolan sistem Aplikasi tidak dapat diakses
	Jaringan	Wifi	Monopoly bandwitch
		Router	Kerusakan hardware
		Switch	Hilangnya komponen hardware Gangguan router

C. Penilaian Risiko

Penilaian Risiko sendiri adalah sebagai suatu keadaan yang dihadapi oleh manusia dalam setiap kegiatannya dan risiko adalah suatu ketidakpastian dimasa yang datang tentang kerugian (Siahaan 2007).

Metode yang digunakan dalam penilaian risiko yaitu metode OCTAVE. Dengan menggunakan pendekatan terhadap evaluasi risiko dari tiga aspek keamanan informasi yaitu *confidentiality*, *integrity*, *availability* yang komprehensif, sistematik, terarah dan dilakukan sendiri dengan hitungan kuantitatif.

D. Menentukan Kemungkinan (*Probability*)

Tujuan menentukan kemungkinan ancaman yang timbul sesuai dengan identifikasi dan kelemahan. Penentuan kemungkinan (*probability*) berdasarkan histori kejadian ancaman sebelumnya, atau ditentukan berdasarkan pengamatan kondisi yang dinilai. Dijabarkan pada tebel 3.

E. Identifikasi dan evaluasi penanganan risiko

Identifikasi dan evaluasi risiko bertujuan untuk menentukan pemilihan penanganan risiko yang timbul tidak dapat diterima langsung akan tetapi perlu dikelola lebih lanjut dengan menggunakan kriteria penerimaan risiko. Pilihan penanganan risiko pada ICT ditentukan sebagai berikut:

1) Menerima risiko dengan menetapkan kontrol keamanan yang sesuai
2) Menerima risiko dengan menggunakan kriteria penerimaan risiko yang ada

F. Memilih Kontrol Objektif dan Kontrol Keamanan Pengelolaan Risiko

Tujuan penentuan pemetaan kontrol obejektif ini disesuaikan dengan ancaman dan kelemahan dari masing-masing aset. Berikut tabel pemetaan hasil rekomendasi pengendalian risiko dengan kebutuhan pada ISO 27001:2013. Pemetaan risiko dengan kebutuhan terdapat pada tabel 4 dan secara lengkap disajikan pada lanjutan tabel 4 pada lampiran.

Tabel 3. Penilaian kemungkinan probalitas

Nama aset	Jenis aset	Risiko	Jenis kejadian	*Probability*	Rata-rata probability
server	Hardware	Bencana alam	Threat	Low	0,2
		Kehilangan data	Vulnerable	Low	0,2
		Kerusakan server	Threat	Medium	0,4
		Pencurian komponen	Threat	Medium	0,6
		Kesalahan konfigurasi	Vulnerable	Medium	0,4
		akses ilegal	Threat	Medium	0,4
		Server Down	Threat	Low	0,2
		Serangan Virus	Vulnerable	High	0,8
		Jumlah ancaman	Jumlah rata-rata probabilitas		3,2
		Nilai Threat	Jumlah rata-rata probabilitas/ jumlah ancaman		
			3,2 / 8 = 0,4		

Tabel 4. Memilih kontrol objektif dan kontrol keamanan pengelolaan risiko

Kategori aset	Aset potensi kegagalan	Potensi Penyebab kegagalan	Kontrol keamanan
Hardware	Kerusakan server	Kesalahan konfigurasi server	A.11.2.4 kontrol pemeliharaan peralatan
	Kerusakan PC	Kesalahan konfigurasi PC	
Data	Data hilang	Kelalaian teknisi	A.9.1.1 Kebijakan pengendalian kontrol akses A.9.3.1 penggunaan informasi otentikasi rahasia A.12.4.3 Log administrasi dan operator
		Aset tidak dipelihara	A.8.1.1 inventarisasi terhadap aset A.10.1.1 kebijakan dalam penggunaan kontrol kriptografi
	Manipulasi data	Rusaknya media penyimpanan	A.12.3.1 backup informasi A.11.2.4 kontrol keamanan pemeliharaan peralatan
		Username password diketahui orang lain	A.9.1.1 kebijakan pengendalian kontrol akses A.9.2.3 manajemen hak akses khusus A.9.4.3. prosedur *log-on* yang aman A.9.4.3 sistem manajemen *password*
Informasi	Kesalahan penyampaian informasi	Adanya kesalahan penyampaian informasi akibat kelalaian pegawai	A.5.1.1 kebijakan untuk keamanan informasi A.5.1.2 tinjauan kebijakan untuk keamanan informasi
		Manajemen kelangsungan bisnis	A.17.1 aspek keamanan informasi dalam manajemen kelangsungan bisnis
		Adanya kesalahan tanggung jawab peran dalam penyampaian informasi	A.6.1.1 peran dan tanggung jawab keamanan informasi
Software	Aplikasi diakses oleh pihak yang tidak berwenang	User dan password diketahui oleh pengguna lain	A.9.1.1 kebijakan pengendalian kontol akses A.9.4.1 pembatasan akses informasi A.9.4.2 prosedure *log-on* yang aman A.9.4.3 sistem manajemen *password*

Tabel 5. Perancangan dan struktur isi SOP

Struktur	Sub-Bab	Konten
Pendahuluan	Tujuan	Deskripsi umum dokumen Prosedur keamanan aset informasi
	Ruang lingkup	
	Overview keamanan data	Aspek keamanan aset informasi
	Evaluasi penilaian risiko keamaman aset informasi pada ICT	Tabel daftar prioritas risiko keamanan aset informasi
Kebijakan pengendalian hak akses	Rincian kebijakan	- Pengelolaan hak akses - Hak akses pihak ketiga
	Dokumen terkait	- Prosedur pengelolaan hak akses
Kebijakan keamanan informasi	Tujuan	Deskripsi umum pengendalian hak akses dan keamanan data
	Ruang lingkup	
	referensi	Acuan yang digunakan dalam pembuatan kebijakan - Pengelolaan sistem informasi - Pengelolaan sistem *log-on* - Password pegguna - Pengelolaan *back-up* dan *restore* informasi
	Dokumen terkait	- Prosedur pengelolaan password - Prosedur *back-up* dan *restore*
Kebijakan pengelolaan *hardware* dan jaringan	Tujuan	Deskripsi umu kebijakan pengelolaan *hardware* dan jaringan

G. Perancangan struktur dan isi SOP

Pada perancangan struktur dan isi SOP ini akan di sesuaikan dengan kebutuhan penelitian. *Standar Operational Procedure* (SOP) adalah pedoman yang berisi prosedur operasional standar yang berada di suatu organisasi yang digunakan untuk memastikan semua keputusan dan tindakan, serta penggunaan fasilitas-fasilitas proses yang dilakukan oleh orang-orang dalam organisasi dan merupakan anggota organisasi agar dapat berjalan dengan efektif,efisien, standar dan sistematis (Tambunan, 2013).

Adapun struktur atau konten yang akan dimasukkan ke dalam kerangka dokumen *Standar Operational Procedure* (SOP) keamanan aset informasi dapat dilihat pada tabel 5 dan secara lengkap disajikan pada lanjutan tabel 5 pada lampiran

H. Dokumen yang dihasilkan

membahas terkait dengan proses dan output dari penelitian ini, penjelasannya dapat dilihat pada tabel 6.

Tabel 6. Hasil Proses dan Output

Proses	Output
1. Pemetaan klausul dengan kontrol objektif	1. Kebijakan pengelolaan hardware
2. Pemetaan risiko dengan kontrol keamanan	2. Kebijakan human resource security
3. Pemetaan klausul dengan kebutuhan keamanan informasi	3. Intruksi kerja pengelolaan hak akses
4. Pemetaan risiko dengan dokumen kebijakan	4. Intruksi kerja reset password
5. Pemetaan	5. Intruksi kerja back-up data dan file
	6. Intruksi kerja restore data

Proses	Output
kebijakan, intruksi kerja, dan rekam kerja.	7. Intruksi kerja perawatan hardware 8. Intruksi kerja keamanaan informasi 9. Intruksi kerja perawatan kabel dan jaringan 10. prosedur pengelolaan hak akses 11. prosedur pengelolaan password 12. prosedur backup dan restore 13. prosedur pengelolaaan hardware 14. formulir pengelolaan hak akses

KESIMPULAN DAN SARAN

A. KESIMPULAN

Berdasarkan hasil pengerjaan penelitian yang telah dilakukan maka di dapat :

a) Dokumen kontrol objektif dan kontrol keamanan Dokumen pengelolaan risiko terkait keamanan informasi, meliputi: penilaian risiko, identifikasi risiko, analisa dan evaluasi risiko, identifikasi dan evaluasi risiko penanganan risiko pada PT Angkasa Pura 1(Persero) Surabaya.

b) Dokumen SOP (*Standar Operational Procedure*) meliputi: dokumen kebijakan, intruksi kerja, dan rekam kerja yang sesuai dengan pemilihan kontrol objektif dan kontrol keamanan dari hasil pengelolaan risiko terkait keamanan informasi

B. Saran

a) Pengembangan tugas akhir dapat dilakukan dengan menambahkan dampak biaya kerugian yang dialami oleh instansi

b) Penelitian ini hanya sebatas pembuatan dokumen SOP tanpa proses pengujian SOP, dan implementasi bagi proses bisnis organisasi

c) Dokumen SOP ini masih dapat terus dikembangkan dilihat dari perkembangan teknologi yang begitu pesat sehingga instansi dapat terus bersaing dan dapat terus menjalankan proses bisnisnya dengan baik

DAFTAR PUSTAKA

Iffano, Irsyad, Sarno, Riyanarto. (2009). *Sistem Manajemen Keamanan Informasi : Berbasis ISO 27001* . Surabaya: ITS Press.

ISO, (2013). ISO/IEC 27001 *Security Techniques Information Security Management Systems Requirements*: ISO/IEC

PT Angkasa Pura 1, (2017). *Laporan Tahunan*. Surabaya.

Siahaan, H. 2007. *Manajemen Risiko*. Jakarta: PT. Elex Media Computindo.

Suprandono, B. (2009). *Manajemen Resiko Keamanan Informasi dengan Menggunakan Metode OCTAVE*. Semarang: Teknik Elektro Universitas Muhammadiyah Semarang

Tambunan, R.M. (2013). *Pedoman Penyusunan Standar Operating Procedures (SOP)*. Jakarta: Masitas Publishing.

LAMPIRAN

Lanjutan tabel 1. Daftar Aset Kritis

No	Kategori	Aset
4.	Data	Data perencanaan pengadaan fasilitas bandara Data pengendalian bagasi Data oeprator garbarata Data keuangan Data hasil evaluasi tiap layanan bisnis utama Data aset Data calon penumpang
5	Sumber Daya Manusia (SDM)	Pegawai Satuan pengamanan

Lanjutan tabel 2. Identifikasi ancaman dan Kelemahan

No	Kategori Aset	Daftar Aset	Ancaman dan kelemahan
4.	Data	Data center	Kesalahan input data
		Data jadwal penerbangan	Pencurian data
		Data shift kerja pegawai	Data corrupt/rusak
		Data hasil evaluasi tiap layanan bisnis utama	Data tidak dapat diakses
		Data aset	Data hilang
		Data maskapai	
		Data pengendalian bagasi	
		Data keuangan	
5.	Sumber Daya Manusia (SDM)	Pegawai	Password shared
		Satuan pengamanan	Penyalahgunaan data tidak sesuai Password shared

Lanjutan Tabel 4. Memilih kontrol objektif dan kontrol keamanan pengelolaan risiko

Ketegori Aset	Aset Potensi Kegagalan	Potensi penyebab Kegagalan	Kontrol keamanan
SDM	Sharing password	Kelalaian pegawai yang memiliki hak akses	A.7.2 syarat dan ketentuan kerja A.7.2.2 kepedulian pendidikan dan pelatihan keamanan informasi A.9.1.1 kebijakan pengendalian kontrol akses
	Data tidak sesuai (tidak valid)	Kesalahan input data	A.12.4.1 pencatatan kejadian A.12.4.2 perlindungan informasi *log-on*

Lanjutan Tabel 5 Perancangan Struktur dan isi SOP

Struktur	Sub-Bab	Konten
Kebijakan keamanan informasi	Ruang lingkup	
	Referensi	Acuan kerja yang digunakan dalam pembuatan kebijakan - pengelolaan sistem informasi -password pengguna -pengelolaan backup dan restore informasi
	Dokumen terkait	-prosedur pengelolaan password -prosedur backup dan restore
Kebijakan pengelolaan hardware	Tujuan	Deskripsi umum, kebijakan pengelolaan hardware dan jaringan
	Ruang lingkup	Acuan kerja yang digunakan dalam pembuatan kebijakan
	Rincian kerja	-pengelolaan hardware -pengelolaan jaringan
	Dokumen terkait	-prosedur perawatan hardware -prosedur pengamanan kabel
Kebijakan *human resource security*	Tujuan	Deskripsi umum kebijakan human resource security
	Ruang lingkup referensi	Acuan yang digunakan dalam pembuatan kebijakan
	Rincian kebijakan	-keamanan SDM -tanggung jawab penggunaan hak akses
	Dokumen terkait tujuan	-Prosedur pelatihan dan pengembangan SDM
Prosedure pengelolaan hak akses	tujuan	Deskripsi umum SOP
	Ruang lingkup	
	definisi rincian prosedure	Penjelasan istilah dalam prosedur -proses pengelolaan password -proses permintaan password Tabel bagan alur SOP
Prosedur backup dan restore	Tujuan	Deskripsi umum SOP
	Ruang lingkup	
	Referensi	Acuan yang digunakan dalam pembuatan prosedur
	Rincian umum prosedur	-proses umum sebelum melakukan backup -proses backup secara berkala -proses pengujian -backup secara berkala -proses restore data
	Bagan alur SOP	Tabel bagan alur SOP
Intruksi kerja	Intruksi kerja perubahan hak kases Intruksi kerja perubahan password	

ISSN 2338-137X

Struktur	Sub-bab	Konten
	Intruksi kerja reset password	
	Intruksi kerja backup file	
	Intruksi kerja restore data	
	Intruksi kerja perawatan hardware	
	Intruksi kerja perawatan kabel jaringan telekomunikasi	