Perencanaan Sistem Manajemen Keamanan Informasi pada Divisi Ekspor Impor CV Merpati Buana Lestari

Angga Eka Saputra [1] Ayuningtyas[2] Achmad Arrosyidi
Program Studi/Jurusan Sistem Informasi
Universitas Dinamika
Jl. Raya Kedung Baruk 98 Surabaya, 60298
Email : 1) 12410100102@dinamika.ac.id, 2) tyas@dinamika.ac.id, 3) achmad@dinamika.ac.id

Abstract: *CV. Merpati Buana Lestari Surabaya sebuah perusahaan yang bergerak dibidang jasa pengurusan perizinan ekspor impor, kepada perusahaan lain yang menginginkan proses administrasi pengiriman atau pengeluaran barang dari pelabuhan bongkar muat yang berhubungan dengan kepabeanan dan administrasi pemerintahan. Pada CV. Merpati Buana Lestari Surabaya memiliki proses bisnis diantaranya layanan kirim dan terima berkas dokumen perjanjian ekspor dan impor yang berperan untuk pemenuhan kebutuhan akan informasi dan data untuk pengolahan dokumen. Pentingnya informasi yang dimiliki membuat keamanan informasi itu perlu untuk dilakukan. Nilai sebuah informasi menyebabkan seringkali informasi hanya boleh diakses oleh orang-orang tertentu. Kondisi saat ini, masih terjadi kurangnya penanganan keamanan informasi sehingga masih menimbulkan Threat (Ancaman) dan Vulnerable (Kelemahan) yang mengakibatkan target tidak terpenuhi dan mempengaruhi Confidentiality (Kerahasiaan), Integrity (Keutuhan) dan Avaibility (Ketersediaan) yang akan berdampak pada Business Impact Analysis (BIA). Dengan demikian penelitian perencanaan sistem manajemen keamanan informasi ini akan menghasilkan dukungan dalam pengendalian kemanan informasi berdasarkan Confidentiality (Kerahasiaan), Integrity (Keutuhan) dan Avaibility (Ketersediaan) adalah menyusun dokumen pengelolaan risiko terkait dengan keamanan informasi dan pembuatan dokumen SOP (Standar Opertional Procedure) yang bertujuan sebagai landasan acuan kerja dan standarisasi dalam mengatur banyaknya karyawan yang menggunakan atau membuat proses bisnis yang berjalan pada lebih terstruktur dan juga diharapkan dapat meningkatkan kualitas keamanan informasi yang ada.*

Kata Kunci : Perencanaan, Sistem Manajemen Keamanan Informasi, Ekspor Impor.

CV. Merpati Buana Lestari Surabaya adalah sebuah perusahaan yang bergerak dibidang jasa pengurusan perizinan ekspor impor, kepada perusahaan lain yang menginginkan proses administrasi pengiriman atau pengeluaran barang dari pelabuhan bongkar muat yang berhubungan dengan kepabeanan dan administrasi pemerintahan.

Pada CV. Merpati Buana Lestari Surabaya memiliki proses bisnis diantaranya layanan kirim dan terima berkas dokumen perjanjian ekspor dan impor yang selanjutnya akan diolah kedalam aplikasi. Sistem informasi ETaxInvoice yang berperan untuk pemenuhan kebutuhan akan informasi dan data untuk pengolahan dokumen. Data dokumen ekspor impor yang wajib dibutuhkan dalam melakukan proses ekspor impor yaitu *Invoice, Packing List, Bill of Landing (B/L), Certificate of Origin* yang selanjutnya akan diolah oleh bagian EKSIM menggunakan ETaxInvoice yang selanjutnya akan menghasilkan dokumen-dokumen impor yaitu Pemberitahuan Impor Barang (PIB), Surat Setoran Pabean-Cukai-Pajak (SSPCP), dan Surat Persetujuan Pengeluaran Barang (SPPB). Sedangkan untuk ekspor akan menghasilkan dokumen-dokumen ekspor yaitu Pemberitahuan Ekspor Barang (PEB), dan Nota Pelayanan Ekspor (NPE).

Dokumen-dokumen tersebut berfungsi sebagai data yang akan dilaporkan kepada situs portal Indonesia *National Single Window* (INSW). INSW adalah Sistem Nasional Indonesia yang memungkinkan dilakukannya suatu penyampaian data dan informasi secara tunggal, pemrosesan data dan informasi secara tunggal dan sinkron, dan pembuatan keputusan secara tunggal untuk pemberian izin kepabeanan dan pengeluaran barang. Aset informasi yang diperlukan dalam mendukung proses bisnis pada CV.Merpati Buana Lestari yaitu meliputi aset informasi , aset perangkat lunak dan layanan teknologi informasi komunikasi. Informasi saat ini sudah menjadi sebuah nilai yang sangat penting.

Pentingnya informasi yang dimiliki CV.Merpati Buana Lestari membuat keamanan informasi itu perlu untuk dilakukan. Nilai sebuah informasi menyebabkan seringkali informasi hanya boleh diakses oleh orang-orang tertentu. Kondisi saat ini, masih terjadi kurangnya penanganan keamanan informasi sehingga masih menimbulkan *Threat* (Ancaman) dan *Vulnerable* (Kelemahan) yang mengakibatkan target tidak terpenuhi dan mempengaruhi *Confidentiality* (Kerahasiaan), *Integrity* (Keutuhan) dan *Avaibility* (Ketersediaan) yang akan berdampak pada *Business Impact Analysis* (BIA).

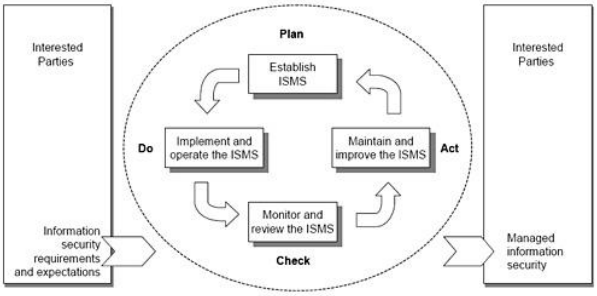
Pada kondisi saat ini CV. Merpati Buana Lestari mengalami masalah atau kendala adanya *Threat* (Ancaman) dan *Vulnerable* (Kelemahan). Permasalahan yang berkaitan dengan *Threat* (Ancaman) yaitu terjadi ancaman penyusupan ke dalam sistem dan akses ilegal (*Hack and Computer Criminal*). Dari ancaman tersebut dimungkinkan dapat menimbulkan pencurian data dan adanya data yang hilang. Dari sisi *Vulnerable* (Kelemahan) adanya akses ilegal yang terjadi karena pegawai memberi tahu sandi pribadi pada aplikasi yang yang telah ditetapkan dan seharusnya tidak dilakukan dengan tujuan untuk melihat data yang dibutuhkan, saat proses pelaporan perpajakan pegawai tidak dapat

membedakan penambahan data baru dan perubahan data yang sudah ada.

Dengan demikian penelitian perencanaan sistem manajemen keamanan informasi ini akan menghasilkan dukungan dalam pengendalian kemanan informasi berdasarkan *Confidentiality* (Kerahasiaan), *Integrity* (Keutuhan) dan *Availability* (Ketersediaan) adalah menyusun dokumen pengelolaan risiko terkait dengan keamanan informasi dan pembuatan dokumen SOP (*Standar Opertional Procedure*) yang bertujuan sebagai landasan acuan kerja dan standarisasi dalam mengatur banyaknya karyawan yang menggunakan atau membuat proses bisnis yang berjalan pada CV.Merpati Buana Lestari lebih terstruktur dan juga diharapkan dapat meningkatkan kualitas keamanan informasi yang ada. Dalam hal penyusunan SOP, Instruksi Kerja, dan Rekam Kerja yang terkait dengan tahap perencanaan sistem keamanan informasi pada CV. Merpati Buana Lestari Surabaya dengan menggunakan ISO/IEC 27001:2005 dan ISO/IEC 27002:2005 yang disesuaikan dengan kebutuhan keamanan informasi dan mempertimbangkan hasil pengelolaan risiko keamanan informasi.

METODE

Metode dalam penelitian ini menggunakan model proses ISO 27001:2005. ISO/IEC 27001:2005 merupakan model tahapan yang dibutuhkan dalam mengimplementasikan pemenuhan manajemen keamanan informasi dengan tujuan organisasi dan kebutuhan bisnis. Tahapan tersebut dapat dilihat pada gambar 1.



Gambar 1. Model PDCA
(Sumber : ISO/IEC, 2005 a)

Panduan Sistem Manajemen Keamanan Informasi

Panduan penyusunan langkah-langkah sistem manajemen keamanan informasi (SMKI) pada tahap *Plan-Do-Check-Act* akan dijelaskan sebagai berikut.

Mengidentifikasi risiko

Identifikasi risiko bertujuan memahami seberapa besar dan identifikasi risiko yang akan diterima oleh oraganisasi jika informasi organisasi mendapat ancaman atau gangguan keamanan yang menyebabkan gagalnya penjagaan aspek keamanan informasi. (ISO/IEC, 2005 c). Langkah-langkah untuk mengidentifikasi risiko yaitu :

1) Identifikasi Aset

Mengidentifikasi aset dalam SMKI dapat dilakukan dengan menggunakan tabel aset yang telah dikategorikan menurut jenis atau kebutuhan organisasi (Sarno & Iffano, 2009).

2) Menghitung Nilai Aset

Cara menghitung nilai aset berdasarkan keamanan informasi yaitu *Confidentiality, Integrity dan Avaibility* dapat menggunakan tabel penilian aset berdasarkan kriteria *Confidentiality* yang di tunjukkan pada Tabel 1, kriteria *Integrity* yang di tunjukkan pada Tabel 2, kriteria *avaibility* yang di tunjukkan pada Tabel 3.

Tabel 1 Kriteria *Confidentiality*

Kriteria *Confidentiality*	Nilai *Confidentiality* (NC)
Public	0
Internal use Only	1
Private	2
Confidential	3
Secret	4

(Sumber : Sarno & Iffano, 2009)

Tabel 2 Kriteria *Integrity*

Kriteria *Integrity*	Nilai *Integrity* (NI)
No Impact	0
Minor incident	1
General distubance	2
Mayor disturbance	3
Uncceptable	4

(Sumber : Sarno & Iffano, 2009)

Tabel 3 Kriteria *Avaibility*

Kriteria *Avaibility*	Nilai *Avaibility* (NA)
No Avaibility	0
Office hours Avaibility	1
Strong Avaibility	2
High Avaibility	3
Very High Avaibility	4

(Sumber : Sarno & Iffano, 2009)

Perhitungan nilai aset dapat dihitung dengan menggunakan persamaan matematis berikut :

Nilai aset (NS) = NC + NI + NA

Keterangan :

NC = Nilai *Confidentiality*

NI = Nilai *Integrity*

NA = Nilai *Avaibility*

Mengidentifikasi Ancaman dan Kelemahan Terhadap Aset

Mengidentifikasi ancaman dan kelemahan terhadap aset dapat menggunakan tabel *Probabilitas of Occurance* seperti pada Tabel 4 dengan menentukan rentang nilai probability dari level Low, Medium, dan High (Sarno & Iffano, 2009)

Tabel 4 Contoh Kemungkinan Gangguan Keamanan

No	Ancaman	Jenis	Proba bilitas	Rerata Probabilitas
1	Gangguan Perangkat Keras	Ancaman	Low	0,3

2	Akses Ilegal	Ancaman	Medium	0,6
3	Gangguan sumber daya	Kelemahan	Low	0,3
4	Bencana Alam	Ancaman	High	0,8
	Σancaman			ΣPO

(Sumber : Sarno & Iffano, 2009)

Keterangan :
Low : Nilai Rerata Probabilitas 0,1 - 0,3
Medium : Nilai Rerata Probabilitas 0,4 - 0,6
High : Nilai Rerata Probabilitas 0,7 - 0,9

Nilai ancaman dapat langsung dihitug menggunakan persamaan matematis berikut:

NT = ΣPO/ Σancaman
Keterangan :
NT : Nilai Ancaman
ΣPO : Jumlah Rerata Probabilitas
ΣAncaman : Jumlah ancaman

Menentukan risiko yang timbul diterima atau tidak

Pengelolahan risiko dengan menggunakan kriteria penerimaan risiko untuk menentukan level risiko diperlukan nilai risiko untuk menentukan letak level dari masing-masing aset yaitu dengan menggunakan perhitungan persamaan matematis berikut (Sarno & Iffano, 2009).

Risk value = NA x BIA x NT
Keterangan :
Risk Value : Nilai Risiko
NA : Nilai Aset
BIA : Nilai BIA
NT : Nilai Ancaman

HASIL DAN PEMBAHASAN

Tahap Awal

Tahap awal dilakukan untuk pengumpulan data dan penggalian informasi agar memperoleh data yang dibutuhkan dalam menyelesaikan penelitian ini. Pengumpulan data dan penggalian informasi dilakukan dengan wawancara, studi literatur dan observasi.

Identifikasi Aset

Identifikasi aset pada CV.Merpati Buana Lestari bertujuan untuk menentukan aset-aset yang ada pada CV.Merpati Buana Lestari. Berdasarkan hasil dari observasi yang dilakukan dapat digolongkan menjadi beberapa jenis aset yaitu aset *hardware*, *software*, jaringan, data dan Sumber Daya Manusia.

Tabel 5 Identifikasi Aset

No	Kategori Aset	Aset
1.	*Hardware*	*Server* PC *Router* *Wifi hotspot* *Switch* Kabel Scanner Paper Shredder Kamera CCTV Printer IP Telepon
2.	*Software*	Sistem Informasi Presensi Pegawai Sistem Informasi Ekspor Impor Sistem Informasi Perpajakan Sistem Informasi Keuangan
3.	Data	Data Pegawai Data Keuangan Data Ekspor Impor Data Perpajakan Data Aset Perusahaan
4.	Sumber Daya Manusia	Pegawai

Tahap Pengembangan

Tahap pengembangan dilakukan dengan menggunakan langkah-langkah pada sistem manajemen keamanan informasi yang ada pada standar ISO/IEC 27001:2005 dan ISO 27002:2005 mengenai tahap perancanaan sistem manajemen keamanan informasi yang akan diperjelas sebagai berikut :

Menghitung Nilai Aset

Setelah melakukan identifikasi aset langkah selanjutnya adalah melakukan perhitungan nilai aset yang dimiliki perusahaan dengan melakukan perhitungan nilai aset berdasarkan pada pendekatan aspek keamanan informasi yaitu kerahasiaan (*Confidentiality*), keutuhan (*Integrity*), dan ketersediaan (*Avaibility*).

Setelah mendefinisikan kriteria sesuai dengan aspek keamanan informasi langkah selanjutnya adalah melakukan perhitungan nilai aset dengan menggunakan persamaan matematis.
Keterangan persamaan matematis :
Nilai aset = NC+NI+NA
NC = Nilai *Confidentiality*
NI = Nilai *Integrity*
NA = Nilai *Availability*

Tabel 6 Menghitung Nilai Aset

No	Kategori Aset	Daftar Aset	Kriteria			Nilai Aset (NC+ NI+NA)
			NC	NI	NA	
1.	*Hardware*	Server	4	4	3	11
		PC	3	3	3	9
		Kamera CCTV	2	1	1	4
		Printer	1	1	1	3
		IP Telepon	1	1	1	3
		Scanner	1	1	1	3
		Mesin sheredder	1	1	1	3

No	Kategori Aset	Daftar Aset	Kriteria			Nilai Aset (NC+ NI+NA)
			NC	NI	NA	
		Router	2	2	2	6
		Wifi	1	1	2	4
		Switch	2	2	2	6
		Kabel	1	1	1	3
2.	*Software*	Sistem Informasi Presensi Pegawai	3	2	2	7
		Sistem Informasi Ekspor Impor	3	3	3	9
		Sistem Informasi Perpajakan	4	2	2	8
		Sistem Informasi Keuangan	4	3	3	10
3.	Data	Data Pegawai	2	2	2	6
		Data Keuangan	4	3	2	9
		Data Ekspor Impor	3	3	2	8
		Data Perpajakan	3	3	2	8
		Data Aset Perusahaan	3	2	2	7
4.	SDM	Pegawai	2	2	1	5

Menentukan Risiko diterima atau Perlunya Penanganan Risiko

Menentukan risiko diterima atau tidak adalah dengan cara menghitung nilai risiko dari masing-masing aset yang telah diidentifikasi sebelumnya. Dari hasil perhitungan yang telah dilakukan maka ditentukan nilai risiko dari masing-masing aset pada Tabel 7

Tabel 7 Perhitungan Nilai Risiko pada masing-masing Aset

No	Katagori Aset	Daftar Aset	Nilai Aset	Nilai BIA	Nilai Ancaman	Nilai Risiko
1.	*Hardware*	Server	11	3	0,375	12,375
		PC	9	3	0,37	9,99
		Kamera CCTV	4	2	0,35	2,8
		Printer	3	2	0,2	1,2
		IP Telepon	3	2	0,23	1,38
		Scanner	3	2	0,2	1,2
		Mesin sheredder	3	2	0,15	0,9
		Router	6	2	0,36	4,32
		Wifi	4	2	0,32	2,56
		Switch	6	2	0,3	3,6
		Kabel	3	2	0,34	2,04
2.	*Software*	Sistem Informasi Presensi Pegawai	7	2	0,42	5,88
		Sistem Informasi Ekspor Impor	9	4	0,52	18,72
		Sistem Informasi Perpajakan	8	4	0,55	17,6
		Sistem Informasi Keuangan	10	4	0,65	26
3.	Data	Data Pegawai	6	2	0,425	5,1
		Data Keuangan	9	4	0,6	21,6
		Data Ekspor Impor	8	4	0,6125	19,6
		Data Perpajakan	8	4	0,65	20,8
		Data Aset Perusahaan	7	3	0,525	11,025
4.	Sumber Daya Manusia	Pegawai	5	2	0,2	2

Setelah diketahui nilai risiko pada masing-masing aset selanjutnya adalah menentukan level risiko pada masing-masing aset. Hasil dari level risiko dari masing-masing aset dapat dilihat pada Tabel 8

Tabel 8 Level Risiko pada masing-masing Aset

No	Katagori Aset	Daftar Aset	Nilai Risiko	Level Risiko
1.	*Hardware*	Server	12,375	*Medium*
		PC	9,99	*Low*
		Kamera CCTV	2,8	*Low*
		Printer	1,2	*Low*
		IP Telepon	1,38	*Low*
		Scanner	1,2	*Low*
		Mesin sheredder	0,9	*Low*
		Router	4,32	*Low*
		Wifi	2,56	*Low*
		Switch	3,6	*Low*
		Kabel	2,04	*Low*
2.	*Software*	Sistem Informasi Presensi Pegawai	5,88	*Low*
		Sistem Informasi Ekspor Impor	18,72	*Medium*
		Sistem Informasi Perpajakan	17,6	*Medium*
		Sistem Informasi Keuangan	26	*High*
3.	Data	Data Pegawai	5,1	*Low*
		Data Keuangan	21,6	*High*
		Data Ekspor Impor	19,6	*Medium*
		Data Perpajakan	20,8	*High*
		Data Aset Perusahaan	11,025	*Medium*
4.	Sumber Daya Manusia	Pegawai	2	*Low*

Identifikasi dan Evaluasi Penanganan Risiko

Identifikasi dan evaluasi risiko bertujuan untuk meentukan pemilihan penanganan risiko jika risiko yang timbul tidak dapat diterima langsung akan tetapi diterima

tetapi perlu dikelola lebih lanjut dengan menggunakan kriteria penerimaan risiko yang telah ditetapkan sebelumnya.

Setelah menentukan pemilihan penanganan langkah selanjutnya adalah melakukan pemilihan penanganan risiko setiap aset yang bernilai *high* yaitu sistem informasi keuangan, data keuangan dan data perpajakan. Pilihan penanganan risiko pasa masing-masing aset akan dijelaskan pada Tabel 9

Tabel 9 Pilihan Penanganan Risiko

No	Aset	Pilihan Penanganan Risiko
1.	Sistem Informasi Keuangan	Status risiko *Risk Reduction* yaitu dengan menetapkan kontrol keamanan yang sesuai berdasarkan ISO 27002.
2.	Data Keuangan	Status risiko *Risk Reduction* yaitu dengan menetapkan kontrol keamanan yang sesuai berdasarkan ISO 27002.
3.	Data Perpajakan	Status risiko *Risk Reduction* yaitu dengan menetapkan kontrol keamanan yang sesuai berdasarkan ISO 27002.

Kontrol objektif dan kontrol keamanan pengelolaan risiko

Setelah menetapkan pemilihan penanganan risiko langkah selanjutnya adalah menentukan kontrol keamanan yang sesuai pada aset yang memiliki level risiko tinggi. Penetapan kontrol objektif dan kontrol keamanan disesuaikan dengan ancaman dan kelemahan dari masing-masing aset yang dipilih pada subbab 4.2.3.

Dalam tujuan penentuan kontrol keamanan ini dijadikan dasar untuk membuat prosedur kontrol dalam pengelolaan risiko. Berikut adalah kontrol objektif dan kontrol keamanan berdasarkan ISO 27001:2005 yang digunakan untuk masing-masing aset yang memerlukan penanganan risiko setiap aset yang bernilai *high* pada subbab 4.2.4, Pemetaan kontrol objektif dan kontrol keamanan terdapat 3 klausul, 6 kontrol objektif dan 7 kontrol keamanan.

Tabel 10 Pemetaan Kontrol Objektif dan Kontrol Keamanan

No	Klausul	Kontrol Objektif	Kontrol Keamanan
1	5 - Kebijakan Keamanan	5.1 - Kebijakan Kemanan Informasi	5.1.1 - Dokumen Kebijakan Keamanan Informasi
			5.1.2 - Tinjauan Ulang Kebijakan Keamanan Informasi
2	6 - Organisasi Keamanan Informasi	6.1 - Organisasi Internal Keamanan Informasi	6.1.3 - Pembagian Peran dan Tanggung Jawab
3	10 - Manajemen Komnukasi dan Operasi	10.5 - Back Up	10.5.1 - Back Up Informasi
4	11 - Kontrol Akses	11.1 - Persyaratan Bisnis untuk Kontrol Akses	11.1.1 - Kebijakan Kontrol Akses
		11.6 - Kontrol Aksses Informasi dan Aplikasi	11.6.1 - Pembatasan Akses Informasi

Hasil Perencanaan

Pembuatan perancangan dilakukan berdasarkan kontrol objektif dan kontrol yang telah ditentukan sebelumnya pada klausul-klausul berikut :

1. Kebijakan pengendalian hak akses (Klausul 11.1)
2. Kebijakan keamanan informasi (Klausul 5.1)
3. Prosedur pengelolaan hak akses (Klausul 11.1.1)
4. Prosedur backup dan restore (Klausul 10.5.1)
5. Prosedur keamanan informasi (Klausul 6.1.3)

Dalam pembuatan kebijakan dihasilkan dari klausul yang telah ditentukan, prosedur dihasilkan dari salah satu point yang telah dibuat, instruksi kerja dihasilkan dari prosedur yang membutuhkan langkah yang lebih terinci dalam proses pengerjaannya, sedangkan rekam kerja atau formulir dihasilkan dari proses akhir yang terdapat pada instruksi kerja. Pada Tabel 11 merupakan rincian dari kebutuhan kebijakan, prosedur, instruksi kerja dan rekam kerja atau formulir berdasarkan tahap perencanaan sistem manajemen keamanan informasi CV Merpati Buana Lestari.

Tabel 11 Pemetaan Risiko dengan Dokumen Kebijakan

No	Nama	Referensi
1.	Kebijakan pengendalian hak akses (**KBJK-MBL-PHA.01**)	(Klausul 11.1,11.2)
2.	Kebijakan keamanan informasi (**KBJK-MBL-KI.02**)	(Klausul 5.1, 6.1)
3.	Prosedur pengelolaan hak akses (**PROS-MBL-PHA.01**)	(Klausul 11.1.1)

No	Nama	Referensi
4.	Prosedur backup dan restore (**PROS-MBL-BR.02**)	(Klausul 10.5.1)
5.	Prosedur keamanan informasi (**PROS-MBL-PKI.03**)	(Klausul 6.1.3)
6.	Instruksi Kerja pengelolaan hak akses (**INSKER-MBL-PHA.01**)	Prosedur pengelolaan hak akses
7.	Instruksi Kerja backup data dan file (**INSKER-MBL-BDA.02**)	Prosedur backup dan restore
8.	Instruksi Kerja restore data (**INSKER-MBL-RD.03**)	Prosedur backup dan restore
9.	Instruksi Kerja klasifikasi keamanan (**INSKER-MBL-KK.04**)	Prosedur keamanan informasi
10.	Rekam kerja / formulir pengelolaan hak akses (**RKF-MBL-PHA.01**)	Instruksi Kerja pengelolaan hak akses
11.	Rekam kerja / formulir kontrak perjanjian hak akses (**RKF-MBL-KPHA.02**)	Instruksi Kerja pengelolaan hak akses
12.	Rekam kerja / formulir klasifikasi data (**RKF-MBL-KD.03**)	Instruksi Kerja klasifikasi keamanan
13.	Rekam kerja / formulir backup data (**RKF-MBL-BD.04**)	Instruksi Kerja backup data dan file
14.	Rekam kerja / formulir restore data (**RKF-MBL-RD.05**)	Instruksi Kerja restore data
15.	Rekam kerja / formulir klasifikasi informasi (**RKF-MBL-KI.06**)	Instruksi Kerja klasifikasi keamanan

Tahap Akhir

Tahap terakhir yang dilakukan adalah menentukan hasil dari proses-proses yang telah dilaksanakan pada tahap pengembangan yang telah dilakukan sebelumnya dan akan menghasilkan keluaran sebagai berikut:

1. Hasil Perencanaan Kebijakan

Hasil perencanaan Kebijakan yang telah disetujui oleh pimpinan perusahaan kemudian disosialisasikan kepada seluruh personel/pegawai yang terkait sesuai dengan ruang lingkup yang telah ditetapkan. Kegiatan ini untuk menjamin bahwa kebijakan terkait telah dipahami sehingga penerapannya dilakukan secara tepat.

2. Hasil Perencanaan Prosedur

Hasil perencanaan Prosedur bertujuan mendukung kegiatan pelaksanaan Kebijakan yang telah ditetapkan perusahaan dan dibutuhkan beberapa pedoman atau acuan dalam melaksanakan tugas dan tanggun jawab masing masing unit kerja yang bersangkutan didalam perusahaan.

3. Hasil Perencanaan Instruksi Kerja

Hasil perencanaan Instruksi Kerja bertujuan mendukung kegiatan pelaksanaan Prosedur yang telah ditetapkan perusahaan dan dibutuhkan beberapa langkah dengan tujuan memastikan setiap proses

4. Hasil Perencanaan Rekam Kerja atau Formulir

Hasil perencanaan Rekam Kerja atau Formulir bertujuan untuk mendukung pelaksanaan Instruksi Kerja dan dibutuhkan beberapa formulir dengan tujuan pendokumentasian dengan baik setiap aktivitas.

SIMPULAN

Dari hasil perencanaan sistem manajemen keamanan sistem informasi yang dilakukan pada CV Merpati Buana Lestari dapat diperoleh kesimpulan sebagai berikut :

1. Perencanaan sistem manajemen keamanan informasi telah berhasil dilakukan dan menghasilkan dokumen perencanaan yang meliputi laporan risiko, kebijakan, *standart operasional prosedur*, instruksi kerja dan rekam kerja/formulir.
2. Dari hasil perencanaan sistem manajemen keamanan informasi telah dihasilkan 2 (dua) kebijakan, 3 (tiga) SOP, 4 (empat) instruksi kerja, 6 (enam) rekam kerja

RUJUKAN

ISO/IEC. (2005 a). *ISO/IEC 27001 Information Technology-Security Techniques-information Security Management System-Requirement.* ISO/IEC.

ISO/IEC. (2005 b). *ISO/IEC 27001 Security Techniques Information Security Management Systems Requirements.* ISO/IEC.

ISO/IEC. (2005 c). *ISO/IEC 27002 Security Techniques Information Security Management Systems Requirements.* ISO/IEC.

Sarno, R., & Iffano, I. (2009). *Sistem Manajemen Keamanan Informasi berbasis ISO 27001*. Surabaya: ITSPress.