Journal of Information and Information Security (JIFORTY)
Vol. 2, No. 1, Juni 2021, 89-98
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Penanganan Risiko Keamanan Informasi Aplikasi Webmarket Berdasarkan ISO 27001:2013 (Study Kasus pada PT Sanjaya Citra Anugrah)

M. Hadi Prayitno[1,*]

[1]Informatika; Universitas Bhayangkaya Jakarta Raya; Kampus II, Jalan Perjuangan, Bekasi; e-mail: hadi.prayitno@dsn.ubharajaya.ac.id

* Korespondensi: e-mail: hadi.prayitno@dsn.ubharajaya.ac.id

Diterima: 6 Juni 2021; Review: 26 Juni 2021; Disetujui: 29 Juni 2021; Diterbitkan: 3 Juli 2021

Abstract

PT. Sanjaya Citra Anugerah (SCA) is a company engaged in the rental and sale of heavy equipment, committed to ensuring the security of organizational information to maintain the confidentiality, integrity and availability of information from the threat of information security failure. This is realized by implementing an information security management system based on the international standard ISO 27001:2013.

This study aims to describe the scope of the information security management system, the internal and external factors that influence it and to identify broadly the potential failures of information security and their impact. The potential failure is a risk that must be identified based on current conditions, which will then be determined to cause a risk management plan to be prepared, so that information security can be maintained and ultimately increase the level of trust from stakeholders.

***Keywords**: Information Security, ISO 27001:2013, risk*

Abstrak

PT. Sanjaya Citra Anugerah (SCA) adalah perusahaan yang bergerak dibidang sewa menyewa dan penjualan alat berat, memiliki komitmen untuk memastikan keamanan informasi organisasi untuk menjaga aspek kerahasiaan, integritas dan ketersediaan informasi dari ancaman kegagalan keamanan informasi. Hal tersebut diwujudkan dengan mengimplementasikan sistem manajemen keamanan informasi yang berdasarkan pada standar internasional ISO 27001:2013.

Penelitian ini bertujuan untuk mendeskripsikan ruang lingkup sistem manajemen keamanan informasi, faktor internal dan eksternal yang mempengaruhinya dan untuk mengidentifikasi secara garis besar potensi kegagalan keamanan informasi dan dampaknya. Potensi kegagalan tersebut, merupakan risiko yang harus di idetifikasikan berdasarkan kondisi saat ini, yang selanjutnya ditentukan penyebabnya hingga disusun rencana penanganan risiko dimaksud, sehingga keamanan informasi dapat terjaga dan pada akhirnya meningkatkan tingkat kepercayaan dari *stakeholder*.

Kata kunci : Keamanan Informasi, ISO 27001:2013, risiko

1. Pendahuluan

Perkembangan proses bisnis pada organisasi dan atau institusi menuntut sebuat alat yang dapat menunjuang berjalannya proses bisnis dimaksud. Alat tersebut adalah penerapan teknologi informasi di segala lini, penerapan teknologi ini harus tepat dan sesuai dengan kebutuhan bisnis, yang pada kahirnya penerapan teknologi informasi tersebut akan memberikan *added value* bagi bisnis.

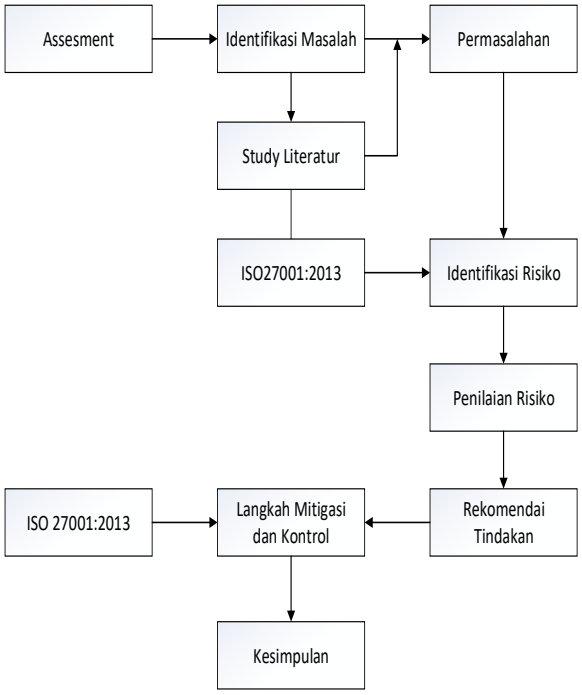
Disamping itu, penerapan teknologi informasi akan merubah data menjadi informasi. Informasi ini yang harus dijaga kerahasiaannya, kelengkapannya, dan keberadaannya, sehingga informasi menjadi salah satu asset yang paling penting. Keamanan informasi sering kali kurang mendapatkan perhatian dari para pengelola teknologi informasi yang hanya berkonsentrasi dengan performasi sistem.

Perencanaan keamanan informasi ini bertujuan untuk mengurangi kerentanan dan penurunan risiko yang akan terjadi, sehingga dapat segera mengetahui ancaman yang dapat timbul berikut dengan dampak terhadai informasi.

Dalam penelitian ini, penulis mencoba mengimplementasikan keamanan informasi berdasarkan ISO 27001:2013 dalam mengidenntifikasikan risiko yang akan terjadi, guna memberikan batasan dan syarat yang harus terpenuhi dalam keamanan informasi pada PT SCA.

2. Metode Penelitian

Pada penelitian ini, penulis menggunakan metodologi denganstandar ISO 27001:2013. Standar ini digunakan untuk membantu PT SCA dalam melindungi keamanan informasi perusahaan dengan memberikan rekomendasi pengelolaan sistem manajemen keamanan informasi. Pada ISO 27001:2013 terdapat annex (klausul) yang digunakan untuk proses mitigasi dan kontrol terhadap risiko yang teridentifikasi. Berikut bagan metode yang digunakan penulis dalam penelitian :



Sumber : Hasil Penelitian (2021)

Gambar 1 : Metode Penelitian

3. Hasil dan Pembahasan

3.1. Kondisi saat ini

Saat ini pandangan nilai TI terhadap nilai bisnis organisasi, bukan lagi sebagai suatu hal yang berdiri sendiri, tapi sudah menjadi salah satu sumber daya yang harus dikelola. Sumber daya IT yang harus dikelola diantaranya Aplikasi, Informasi, Infrastruktur dan Sumber daya Manusia.

Disamping hal diatas, terdapat pula isu yang terdapat pada perusahaan. Isu tersebut meliputi isu internal dan isu eksternal

a. Isu Internal

Faktor dan permasalahan internal yang utama terkait dengan SMKI yang dihadapi oleh PT SCA saat ini pada saat ini meliputi:

1) Dokumentasi operasional sistem belum dilengkapi sesuai dengan persyaratan standard keamanan.
2) Dokumen terkait keamanan informasi belum disesuaikan dengan persyaratan kontrol keamanan informasi.
3) Fitur keamanan terhadap aplikasi belum memadai.
4) Implementasi kontrol keamanan pada infrastruktur belum menyeluruh.
5) Kontrol aset belum diterapkan terkait kebutuhan keamanan.
6) Kurangnya pengendalian dan validitas pada sistem dan informasi.

7) Proses review terhadap kontrol sistem dan infrastruktur belum diterapkan.
8) Proses siklus pengembangan sistem tidak memadai.

b. Isu Eksternal

Faktor dan permasalahan eksternal yang utama terkait dengan SMKI yang dihadapi oleh PT SCA pada saat ini meliputi:

1) Ketidaksinambungan layanan pihak ketiga dengan kebutuhan sistem.
2) Kewajiban terhdap Ketidakpatuhan terhadap peraturan yang berlaku.

3.2. Konsep Manajemen Risiko Keamanan Informasi di PT SCA

Pengelolaan risiko Keamanan Informasi di PT SCA didefinisikan sesuai dengan definisi dari standard ISO 27000:2012 yaitu pelaksanakan secara sistematis dari kebijakan, prosedur dan kegiatan manajemen untuk mengkomunikasikan, mengkonsultasikan serta menetapkan konteks risiko organisasi dan juga untuk mengidentifikasi, menganalisa, mengevaluasi, menangani, memantau dan meninjau risiko.

Pengelola risiko keamanan informasi di PT SCA berdasarkan risiko terhadap asset yang terkait kepada informasi dan fasilitas pengolahan informasi. Aset-aset tersebut dikelompokkan kedalam kelompok aset berikut:

a. Aset fisik;
b. Aset layanan;
c. Aset jaringan;
d. Aset informasi;
e. Aset perangkat lunak;
f. Aset personil; dan
g. Aset sarana pendukung.

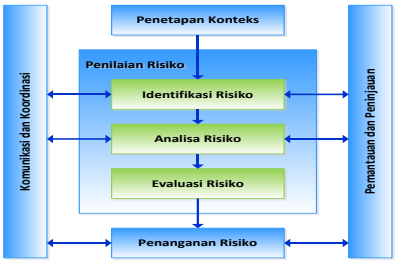
Pengelolaan risiko keamanan informasi di PT SCA mencakup aktifitas yang bersifat iteratif berikut:

a. Menetapkan konteks risiko. Dalam aktifitas ini, akan ditentukan dan ditetapkan juga kriteria risiko yang dibutuhkan untuk mengevaluasi risiko keamanan informasi.
b. Penilaian risiko yang mencakup:
   1) Identifikasi risiko, adalah proses untuk mengidentifikasi dan menjabarkan risiko yang dapat mengurangi aspek kerahasiaan, integritas dan ketersediaan dari informasi, fasilitas pengolahan informasi dan fasilitas pendukungnya;
   2) Analisa risiko, adalah proses untuk menganalisa risiko dan dampaknya serta menentukan tingkat dari risiko;

3) Evaluasi risiko, adalah proses dimana risiko yang telah dianalisa akan dibandingkan dengan kriteria risiko untuk menentukan apakah risiko tersebut dapat diterima.

c. Penanganan risiko. Hal ini adalah aktifitas untuk memodifikasi risiko untuk menurunkan tingkat risiko sampai ke tingkat yang dapat diterima.
d. Pemantauan dan peninjauan risiko. Dalam aktifitas ini risiko dan penanganannya akan secara berkelanjutan dipantauan dan ditinjau.
e. Komunikasi dan konsultasi risiko. Risiko keamanan informasi yang dihadapi suatu organisasi harus dikomunikasikan dan dikonsultasikan kepada pihak perwakilan manajemen dan manajemen puncak dari PT SCA.

Deskripsi secara grafis dari konsep manajemen risiko SMKI yang diadopsi oleh Bagian yang mengelola keamanan informasi PT SCA diberikan pada **Gambar 2. Konsep Pengelolaan Risiko**.



Sumber : Safaat H, Nazruddin. (2011)

Gambar 2. Konsep Pengelolaan Risiko

3.3. Penetapan konteks

Dalam proses ini, kondisi dan prasyarat organisasi – baik internal maupun eksternal – yang terkait dengan keamanan informasi harus diidentifikasikan dan ditetapkan. Hal ini harus mencakup:

a. Kegiatan utama yang dilakukan oleh organisasi.
b. Kebijakan internal organisasi.
c. Proses bisnis organisasi.
d. Kewajiban hukum, perundangan dan kewajiban kontrak yang dimiliki oleh organisasi.
e. Kondisi teknologi informasi dan keamanan informasi, baik internal maupun eksternal, yang relevan dengan organisasi.

3.4. Penilaian risiko

3.4.1. Identifikasi risiko

Identifikasi risiko mencakup aktifitas berikut:

a. Identifikasi ancaman, merupakan aktifitas untuk mengidentifikasi potensi penyebab insiden yang tidak diinginkan yang dapat menyebabkan kerusakan / kerugian bagi organisasi dan sistemnya. Sebuah ancaman dapat mengurangi aspek kerahasiaan, integritas dan ketersediaan dari informasi;
b. Identifikasi dampak merupakan aktifitas yang dilakukan untuk mengidentifikasi potensi dampak jika ancaman yang teridentifikasi, mengeksploitasi kelemahan yang telah ada;
c. Alokasi pemilik risiko untuk setiap risiko yang teridentifikasi. Pemilik risiko bertanggung jawab untuk mengelola risiko yang telah teridentifikasi.

Identifikasi risiko ini didapatkan dengan melakukan wawancara tatap muka secara langsung dengan kepala bidang IT PT SCA serta melakukan observasi bahwa aset tersebut benar-benar dimiliki. Berikut merupakan tabel dari hasl identifikasi risiko

Tabel 1 : Identifikasi Risiko

Area / Proses	Ancaman (Kejadian Risiko)
Pengelolaan Fasilitas Pemroses Informasi	Penyalahgunaan perangkat kerja saat dimusnahkan
	Akses data dan sistem pada perangkat kerja yang tidak terotorisasi
	Kerusakan perangkat infrastruktur
	Perangkat notebook terinfeksi malicious code / virus.
Pengelolaan Infrastruktur	Serangan DoS/DDoS pada sistem yang terhubung ke database
	Serangan Spoofing pada jaringan
	Lisensi aplikasi/OS digunakan oleh pihak yang tidak berwenang
Pengelolaan Pihak Ketiga	layanan pihak ketiga tidak terkendali
	Kebocoran informasi terkait dengan sistem yang dikelola
	Sistem mengalami serangan siber
Pengelolaan SDM	Human Error
Pengelolaan Sistem Informasi	Terjadinya perubahan terhadap informasi tanpa izin (corrupted information) pada aplikasi
	Akses ke aplikasi oleh pihak yang tidak berwenang/ serangan hacking.
	Kelemahan (bugs) dan kesalahan (error) dalam aplikasi
	terdapat backdoor pada sistem/aplikasi
	Sistem mengalami kesalahan operasional

Area / Proses	Ancaman (Kejadian Risiko)
	Database tidak dapat dipulihkan ketika Server mengalami kerusakan.
	Kegagalan operasional sistem aplikasi
Pengendalian Informasi	Kesalahan dalam perlindungan data
	Penyalahgunaan dalam pengelolaan informasi

Sumber : Hasil Penelitian (2021)

3.4.2. Penyebab risiko

Penyebab risiko ini dilakukan dnegan memperhatikan kondisi risiko yang terdapat pada PT SCA dan penyebab risiko dapat dijelaskan sebagai berikut

Tabel 2 : Tabel Penyebab Risiko

	Penyebab risiko
1	Tidak adanya aturan mengenai manajemen asset
2	Lemahnya pengendalian akses jaringan terkait pembatasan kewenangan akses
3	Proses manajemen perubahan terhadap data di aplikasi yang tidak terkontrol
4	Tidak terdapat pencatatan log Security Event pada sistem/aplikasi
5	Ketidaksempurnaan dalam proses pengujian sistem/aplikasi (software testing).
6	Belum tersedianya panduan mengenai manajemen keberlangsungan bisnis / *Business Continuity Management* (BCP).
7	Tidak adanya aturan dalam perlindungan data
8	Belum diaturnya mekanisme penanganan informasi pada perusahaan
9	Tidak adanya program peningkatan kompetensi pegawai
10	Tidak ada monitoring SLA
11	Tidak adanya "Perjanjian Tidak Membocorkan Informasi" bagi personil pihak ketiga yang mengakses langsung ke informasi
12	Belum diterapkannya standard keamanan pada perangkat
13	Routing Access Control Lists pada jaringan dikonfigurasi secara tidak tepat atau tidak dipelihara dengan baik untuk memastikan keamanan.
14	Lemahnya pengendalian terkait proses / metode verifikasi dan mekanisme pemberian otorisasi akses ke Data / Informasi / Sistem
15	Proses pelaksanaan backup belum dilaksanakan secara memadai
16	Kurangnya awareness terkait perlindungan keamanan pada sistem dan infrastruktur

Sumber : Hasil Penelitian (2021)

3.4.3. Akibat dari risiko

Setelah mempertimbangkan masalah, pihak yang berkepentingan, ruang lingkup dan aset informasi, organisasi dapat mengidentifikasi risiko, kemudian mengevaluasi dan mempertimbangkan perlakuan untuk risiko tersebut . Risiko seputar informasi berharga dan fasilitas pemrosesan, perangkat, orang yang terlibat, dll. Harus dievaluasi dengan mempertimbangkan Kerahasiaan, Integritas, dan Ketersediaan (CIA) informasi.

Tabel 3 : Tabel Akibat Yang MunginTimbul dan Gejala

Akibat Yang Mungkin Timbul	Gejala pada Faktor Keamanan Informasi
Berpotensi adanya malware pada aplikasi yang menyebabkan data tidak aman	Confidenciality
Kebocoran informasi yang dapat menimbulkan kerugian bagi organisasi	Confidenciality
Potensi kebocoran data dari sistem yang terbuka	Confidenciality
Kesalahan dalam pelaksanaan proses bisnis dan layanan pada sistem;	Integraty
Penyalahgunaan kewenangan akses yang menyebabkan terungkapnya data tanpa sepengetahuan organisasi	Integraty
Penyalahgunaan sistem / penggunaan sistem tidak tekontrol	Integraty
Reputasi perusahaan mengalami penurunan	Integraty
Kesulitan dalam mengevaluasi keamanan aplikasi	Integraty
Terjadinya data atau system corrupt akibat kesalahan prosedur keamanan	Integraty
Aplikasi tidak berfungsi sesuai dengan persyaratan spesifikasinya.	Availability
Kesulitan dalam melakukan pengembangan lebih lanjut.	Availability
Layanan proses bisnis terhenti ketika terjadi bencana / insiden	Availability
Terganggunya proses bisnis yang menggunakan aset tersebut	Availability

Sumber : Hasil Penelitian (2021)

3.5. Rekomendasi Pengendalian Risiko

PT SCA menentukan bahwa, risiko keamanan informasi yang dinyatakan langsung dapat diterima adalah risiko dengan nilai “Rendah” dan untuk risiko dengan nilai "Sedang / Tinggi / Ekstrim" harus diberikan rencana penanganan risiko.

Risiko dengan nilai "Sedang / Tinggi / Ekstrim" dapat dinyatakan diterima jika tidak lagi terdapat rencana penanganan risiko lain yang dapat dilakukan dan harus memperoleh persetujuan dari Manajemen Puncak PT SCA. Untuk risiko keamanan informasi yang dinyatakan perlu diberikan tindak lanjut, risiko dengan nilai risiko residual "Tinggi" merupakan prioritas untuk ditangani terlebih dahulu.

Tabel 4: Rencana Penangan Risiko

	Rencana Penanganan Risiko
1	Menyusun suatu prosedur manajemen aset, baik yang aktif atau pasif (tidak terpakai)
2	Melakukan pembatasan akses dengan mendokumentasikan kewenangan akses tersebut, serta mereview hak akses ke sistem
3	Menyusun mekanisme pengendalian perubahan pada input informasi pada system
4	Melaksanakan review dan analisa log system
5	Merencanakan dan melaksanakan kegiatan Vulnarebility Assesment pada jaringan dan sistem aplikasi
6	Mempersiapkan template skenario pengujian sistem
7	Menyusun dokumen BCP dan mengidentifikasi aktivitas pemulihan
8	Mempersiapkan dokumen kriteria penerimaan sistem
9	Membuat kebijakan mengenai standard enkripsi
10	Membuat standard versioning aplikasi
11	Membuat prosedur pengendalian informasi
12	Mendefinisikan matriks kompetensi dan melakukan evaluasi secara berkala
13	Mendata SLA yang disediakan vendor dan melakukan review berkala terhadap SLA tersebut
14	Melengkapi Perjanjian Kerahasiaan informasi bagi pihak ketiga yang secara langsung mengakses data

Sumber : Hasil Penelitian (2021)

4. Kesimpulan

Berdasarkan hasil penelitian yang telah telah dilakukan, maka dapat disimpulkan :

a. Terdapat 6 buah area/proses dengan 20 risiko yang di temukan, dan di temukan pula penyebab terjadinya risiko kegagalan keamanan informs serta dampak akan akan terjadi berdasarkan factor keamanan informasi
b. Guna menghindari terjadinya risiko Kembali, perlu disusun rencana penanganya risiko, dan didapatkan 14 butir rencana yang akan dilakukan perusahaan, berdasarkan pada ISO 27001:2013 yang terdiri dari beberapa dapat digunakan untuk mencegah atau meminimalisir potensi terjadinya risiko.

Daftar Pustaka

Andrianto Moeljono, M., (2016). Manajemen Risiko Teknologi Informasi. [Online] Available at: https://itgid.org/manajemen risiko-teknologi-informasi-part-i/

Bakri M, Nia I, (2017), Analisis dan Penerapanan Sistem Manajemen Keamanan Informasi SIMH BPKP Menggunakan Standar ISO 27001. Universitas Teknokrat Indonesia, Jurnal Teknokompak, 11 (2), 41-44

Hamid Tohidi, (2011). The Role of Risk Management in IT systems of organizations, Procedia Computer Science 3, 881–887.

Husda, N. E., & Wangdra, Y. (2016). Pengantar Teknologi Informasi. Jakarta: Baduose Media.

International Standard , (2009). ISO 31000: Risk management — Principles and guidelines.

ISACA. (2009). The Risk IT Framework

ISO/IEC 27001. (2013). Information Technology – Security Techniques – Information Security Management Systems – Requirements. [ebook]

Putra, A.N. (2016). Perencanaan dan Implementasi Information Security Management System Menggunakan Framework ISO/IEC 27001. Universitas Diponegoro. Jurnal Teknologi dan Sistem Komputer, 4(1). 60-66.

Rhodes, M., (2013). Information Security: The Complete Reference (2nd Edition). [Online] Tersedia di [diakses 14 Mei 2021].

Safaat H, Nazruddin. 2011. Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000. Jurnal Sains, Teknologi dan Industri. 9(1): 1- 15.