EVALUASI MANAJEMEN RISIKO KEAMANAN INFORMASI PADA PT HARDO SOLOPLAST MENGGUNAKAN FRAMEWORK NIST SP 800 30 DAN PENGHITUNGAN *MATURITY LEVEL* KEAMANAN INFORMASI MENGGUNAKAN ISO 27002:2005

Tugas Akhir

Diajukan untuk memenuhi persyaratan mencapai derajat Sarjana Sistem Informasi

RAFAEL LATU BAWONO

NPM: 171709335

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ATMA JAYA YOGYAKARTA

2020

HALAMAN PENGESAHAN

Tugas Akhir Berjudul

EVALUASI MANAJEMEN RISIKO KEAMANAN INFORMASI PADA PT HARDO SOLOPLAST MENGGUNAKAN FRAMEWORK NIST SP 800 30 DAN PENGHITUNGAN *MATURITY LEVEL* KEAMANAN INFORMASI MENGGUNAKAN ISO 27002:2005

Yang disusun oleh

Rafael Latu Bawonno

171709335

Dinyatakan telah memenuhi syarat pada tanggal 26 Januari 2021

		Keterangan
Dosen Pembimbing 1	: Yohanes Priadi Wibisono, S.T.,M.M.	Telah Menyetujui
Dosen Pembimbing 2	: Yohanes Priadi Wibisono, S.T.,M.M.	Telah Menyetujui

Tim Penguji

Penguji 1	: Yohanes Priadi Wibisono, S.T.,M.M.	Telah Menyetujui
Penguji 2	: Aloysius Bagas Pradipta Irianto, S.Kom., M.Eng.	Telah Menyetujui
Penguji 3	: Putri Nastiti, S.Kom., M.Eng	Telah Menyetujui

Yogyakarta, 26 Januari 2021

Universitas Atma Jaya Yogyakarta

Fakultas Teknologi Industri

Dekan

Ttd

Dr. A. Teguh Siswantoro, M.Sc.

LEMBAR PENYATAAN

Orisinalitas & Publikasi Ilmiah

Saya yang bertanda tangan di bawah ini:

Nama Lengkap	: Rafael Latu Bawono
NPM	: 171709335
Program Studi	: Sistem Informasi
Fakultas	: Teknik Industri
Judul Penelitian	: Evaluasi Manajemen Risiko Keamanan Informasi pada PT HARDO SOLOPLAST Menggunakan Framework NIST SP 800 30 dan Penghitungan *Maturity Level* Keamanan Informasi Menggunakan ISO 27002:2005

Menyatakan dengan ini:

1. Skripsi ini adalah benar merupakan hasil karya sendiri dan tidak merupakan salinan sebagian atau keseluruhan dari karya orang lain.
2. Memberikan kepada Universitas Atma Jaya Yogyakarta, berupa Hak Bebas Royalti non eksklusif (*Non-Exclusive-Royalty-Free Right*) atas Penelitian ini, dan berhak menyimpan, mengelola dalam pangkalan data, mendistribusikan, serta menampilkan untuk kepentingan akademis, tanpa perlu meminta izin selama tetap mencantumkan nama penulis.
3. Bersedia menanggung secara pribadi segala bentuk tuntutan hukum yang mengikuti atas pelanggaran Hak Cipta dalam pembuatan Skripsi ini.

Demikianlah pernyataan ini dibuat dan dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 26 Januari 2021
Yang menyatakan,

Rafael Latu Bawono
171709335

LEMBAR PENYATAAN

Persetujuan dari Instansi Asal Peneltian

(Jika penelitian membutuhkan akses data organisasi eksternal)

Saya yang bertanda tangan di bawah ini:

Nama Lengkap Pembimbing	: Yohanes Priadi Wibisono, S.T.,M.M.
Jabatan	: Kepala Program Studi
Departemen	: Sistem Informasi

Menyatakan dengan ini:

Nama Lengkap	: Rafael Latu Bawono
NPM	: 171709335
Program Studi	: Sistem Informasi
Fakultas	: Teknik Industri
Judul Penelitian	: Evaluasi Manajemen Risiko Keamanan Informasi pada PT HARDO SOLOPLAST Menggunakan Framework NIST SP 800 30 dan Penghitungan *Maturity Level* Keamanan Informasi Menggunakan ISO 27002:2005

1. Penelitian telah selesai dilaksanakan pada perusahaan, dan telah diaplikasikan pada sistem terkait.
2. Perusahaan telah melakukan sidang internal berupa kelayakan penelitian ini dan akan mencantumkan lembar penilaian secara tertutup kepada pihak universitas sebagai bagian dari nilai akhir mahasiswa.
3. Memberikan kepada perusahaan berupa Hak Bebas Royalti non eksklusif (*Non-Exclusive-Royalty-Free Right*) atas Penelitian ini, dan berhak menyimpan, mengelola dalam pangkalan data, tanpa perlu meminta izin selama tetap mencantumkan nama penulis.

Demikianlah pernyataan ini dibuat dan dapat dipergunakan sebagaimana mestinya.

Surakarta, 26 Januari 2021
Yang menyatakan,

Yudy Patrianto
Kepala Departemen IT

PRAKATA

Segala syukur dan puji hanya bagi Tuhan Yesus Kristus, oleh karena anugerah-Nya yang melimpah, dan kasih setia yang besar akhirnya peneliti dapat menyelesaikan penulisan tugas akhir dengan judul "**Evaluasi Manajemen Risiko Kemanan Informasi PT HARDO SOLOPLAST Menggunakan NIST SP 800 30 dan Penghitungan *Maturity Level* Keamanan Informasi Menggunakan ISO 27002:2005**" guna memenuhi persyaratan dalam mencapai Gelar Sarjana Komputer di Fakultas Teknologi Industri Universitas Atma Jaya Yogyakarta.

Dengan tersusunnya skripsi ini penulis ingin menyampaikan ucapan terimakasih yang sedalam-dalamnya kepada semua pihak yang telah membantu dan memberikan dukungan dalam menyelesaikan Tugas Akhir ini. Maka peneliti mengucapkan banyak terima kasih kepada:

1. Yang Maha Kuasa yang telah membimbing dan menyertai peneliti dalam proses penyusunan Tugas Akhir ini.
2. Kedua orang tua dan keluarga yang telah mendukung dan mendoakan penliti.
3. Bapak Yohanes Priadi Wibisono, S.T.,M.M. selaku Ketua Program Studi Sistem Informasi dan dosen pembimbing Tugas Akhir yang mendukung dan bembimbing selama proses penyusunan Tugas Akhir ini.
4. Ibu Putri Nastiti, S.Kom.,M.Eng selaku dosen Program Studi Sistem Informasi atas bimbingan dan bantuan dalam penyusunan Tugas Akhir ini.
5. Ibu Clara Hetty Primasari, S.T.,M.Cs selaku dosen Program Studi Sistem Informasi atas bimbingan dan bantuan dalam penyusunan Tugas Akhir ini.
6. Aloysius Bagas Pradipta Irianto, S.Kom., M.Eng. Selaku dosen Program Studi Sistem Informasi atas bimbingan dan bantuan dalam penyusunan Tugas Akhir ini.
7. Mas Aji selaku pembimbing lapangan yang membantu dalam proses pengumpulan data dan membimbing dalam proses penyusunan Tugas Akhir ini.
8. Mas Andika, Pak Nur, Pak Yudy, dan responden kuesioner yang membantu dalam proses pengumpulan data dalam proses penyusunan Tugas Akhir ini.
9. Seluruh teman-teman yang telah mendukung dan membantu dalam proses penyusunan Tugas Akhir ini.

ABSTRAK

PT Hardo Soloplast merupakan pabrik yang memproduksi karung plastik di Surakarta yang memiliki visi memimpin di persaingan pasar dan menjaga eksitensi di antar mitra kerja. Pencapai visi tersebut tentu sangat diperlukan peran TIK (Teknologi Informasi dan Komunikasi). Perkembangannya TIK dapat lebih mempermudah pekerjaan karyawan perusahaan, seperti SAP (*System Application and Production and Product in Data Processing*) yang digunakan untuk memperlancar jalan proses bisnis suatu perusahaan. SAP juga dapat meningkatkan produktivitas kegiatan perusahaan secara efisien dan efektif. PT Hardo Soloplast telah menerapkan SAP namun belum melakukan manajemen risiko keamanan informasi. PT Hardo Soloplast ingin mengetahui potensi risiko keamanan informasi SAP yang sudah diterapkan di PT Hardo Soloplast. Salah satu cara untuk melakukan manajemen risiko keamanan informasi menggunakan NIST SP 800 30. Dilakukannya evaluasi risiko keamanan informasi ini bertujuan untuk mengetahui potensi risiko keamanan informasi dan mengantisipasi risiko tersebut. Kegiatan evaluasi risiko keamanan informasi ini dapat mengurangi tingkat dampak risiko tersebut dari *level* tinggi ke *level* terendah. Keamanan informasi sendiri juga dilakukan penghitungan agar dapat mengetahui tingkat kematangan (*maturity level*) keamanan informasi SAP. Penghitungan *maturity level* berdasarkan kerangka kerja ISO 27005:2011. Penghitungan *maturity level* ini dilakukan agar dapat mengetahui tingkat kematangan keamanan informasi dan kontrol yang diterapkan, sehingga rekomendasi yang diberikan dapat tepat. Pengeluaran rekomendasi diharapkan dapat mengurangi dampak risiko dan meminimalisir potensi risiko yang dapat menyebabkan kerugian pada PT Hardo Soloplast.

Kata Kunci : [Manajemen risiko; NIST SP 800-30; ISO 27005:2011; SAP]

ABSTRACT

PT Hardo Soloplast is a factory that produces plastic bags in Surakarta which has a vision to lead in market competition and maintain existence among partners. To achieve this vision, of course, the role of ICT (Information and Communication Technology) is needed. The development of ICT can make the work of company employees easier, such as SAP (System Application and Production and Product in Data Processing) which is used to streamline a company's business processes. SAP can also increase the productivity of company activities efficiently and effectively. PT Hardo Soloplast has implemented SAP but has not performed information security risk management. PT Hardo Soloplast wants to know the potential risk of SAP information security that has been implemented at PT Hardo Soloplast. One of the ways to perform information security risk management is using NIST SP 800 30. This information security risk evaluation is carried out to determine potential information security risks and anticipate these risks. This information security risk evaluation activity can reduce the level of the impact of these risks from high to lowest levels. Information security itself is also calculated in order to determine the maturity level of SAP information security. Calculation of maturity levels based on the ISO 27005: 2011 framework. The calculation of the maturity level is carried out in order to determine the maturity level of information security and controls applied, so that the recommendations given can be precise. The issuance of recommendations is expected to reduce the impact of risks and minimize potential risks that can cause losses to PT Hardo Soloplast.

Keywords: [Risk management; NIST SP 800-30; ISO 27005: 2011; SAP]

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1. Latar Belakang

Penggunaan TIK (Teknologi Informasi dan Komunikasi) dalam perusahaan sangat memberikan kemudahan, terutama dalam hal pengaksesan suatu informasi dengan sangat cepat dan murah yang dikemas dalam sebuah Sistem Informasi digital [1]. Kemudahan dalam mengakses informasi membuat sekelompok orang memiliki keinginan untuk mendapatkan akses ke informasi dan mendapatkan kendali. Hal tersebut memicu munculnya individu atau kelompok orang baik dari pihak internal maupun external untuk mengerahkan segala upaya dalam mengakses dan mengendalikan informasi secara *illegal* [1]. Kegiatan mengakses dan mengendalikan informasi secara *illegal* tentu sangat mempengaruhi terhadap kerentanan keamanan informasi [2].

Keamanan Informasi merupakan suatu hal yang perannya sangat penting untuk menjaga informasi perusahaan atau organisasi [3]. Keamanan informasi setiap perusahaan dapat diukur tingkat kematangan (*maturity level*) keamanannya. *Maturity Level* keamanan informasi dirancang untuk mengukur kemampuan kontrol keamanan informasi dalam mengatasi risiko keamanan informasi [4]. Keamanan informasi perusahaan yang tidak diolah dengan baik, maka dapat menimbulkan risiko pada keberlangsungan proses bisnis perusahaan [5]. Suatu kejadian risiko yang dapat terjadi di suatu perusahaan disebut juga dengan kejadian potensial. Terdapat dua jenis yaitu kejadian yang *anticipated* (dapat diperkirakan) dan kejadian yang *unanticipated* (tidak dapat diperkirakan) [6]. Salah satu cara untuk menangani risiko keamanan informasi adalah dengan menerapkan manajemen risiko.

Manajemen risiko merupakan serangkaian kegiatan yang dilakukan dengan tujuan dapat meminimalkan bahkan dapat mencegah dampak dari terjadinya potensi risiko pada suatu perusahaan. Manajemen risiko juga

merupakan salah satu metode untuk mencegah perusahaan mengalami kerugian besar yang dapat menyebabkan gulung tikar [6]. Penyebab kerugian yang terjadi pada perusahaan dapat bermacam-macam, seperti pencurian data informasi, virus, *hacker*, *social engineering*, kebakaran atau bencana alam, dan *Human Error*. Manajemen risiko memiliki manfaat menyediakan informasi yang berhubungan dengan risiko [6], menemukan dan mengevaluasi potensi risiko, dan memiliki cara atau teknik yang tepat untuk menanggulangi kerugian [7]. Kegiatan manajemen risiko lebih berfokus terhadap beberapa hal yaitu, mengidentifikasi risiko, mengelola risiko dan mengendalikan risiko dengan baik [8].

Manajemen risiko perlu melakukan evaluasi risiko keamanan informasi untuk menghindari berbagai macam potensi risiko, mengurangi dampak risiko dan meminimalisir kerugian perusahaan [9]. Perusahaan yang menerapkan sistem informasi namun belum melakukan evaluasi manajemen risiko, khususnya dalam penilaian risiko keamanan informasi, membuat perusahaan tersebut dapat dikatakan belum mengetahui risiko pada keamanan informasi yang akan dihadapi. Salah satu perusahaan yang telah menerapkan sistem informasi namun belum melakukan evaluasi risiko keamanan informasi adalah PT Hardo Soloplast dan berdasarkan wawancara yang dilakukan kepada kepala *General Affair* selaku pengurus standar ISO, PT Hardo Soloplast ingin mengetahui potensi dan tingkat risiko pada keamanan informasi SAP mereka.

PT Hardo Soloplast telah menerapkan SAP untuk memperlancar jalannya proses bisnis mereka. SAP yang diterapkan merupakan SAP *All in One* versi 10. SAP terdapat 3 jenis *level license* yaitu *SuperAdmin*, *Operational*, dan *Financial*. Setiap *license* berisi beberapa *id user* SAP. 1 *id user* SAP hanya dapat *log in* di satu perangkat. PT Hardo memiliki sejumlah 29 *id user* SAP. *User name* dan *password id user user* yang ber-*license SuperAdmin* tidak boleh diketahui oleh orang lain. Sedangkan untuk setiap *user name* dan *password id user* yang ber-*license Operational* dan *Financial* dapat digunakan untuk lebih 1 orang secara bergantian, namun diwajibkan masih dalam departemen yang sama. Hal ini dikarenakan

terbatasnya jumlah *id user* SAP. Perbedaan setiap *license* adalah pada hak aksesnya. SuperAdmin bisa mengakses ke semua bagian. Operational untuk pembelian, produksi, *HRD*, penjualan. *Financial* untuk mengakses yang berhubungan dengan keuangan, kecuali Laba Rugi. Laba Rugi hanya dapat diakses oleh SuperAdmin. Selain SAP, PT Hardo Soloplast juga menggunakan rancangan sistem sendiri yang disebut *ADD ON*. *ADD ON* merupakan wadah berbagai aplikasi untuk mempermudah pekerjaan beberapa departemen (Produksi, *HRD*, *sales*) dan melengkapi kekurangan fungsi SAP. *ADD ON* ini menyediakan fungsi yang tidak terdapat pada SAP (Seperti fungsi filter untuk mencari *WO* (*Work Order*) pada proses produksi), sehingga karyawan dapat bekerja lebih cepat. PT Hardo Solopast menggunakan *SDK* (*Software Development Kit*) untuk mengkoneksikan *ADD ON* dengan SAP dan Database. Database yang digunakan PT Hardo Soloplast adalah HANA dan MySql. PT Hardo Soloplast sudah mengimplementasikan sistem informasi SAP dan memiliki manajemen resiko pada beberapa bagian dalam perusahaan, namun saat ini PT Hardo Soloplast belum melakukan evaluasi manajemen resiko untuk keamanan informasi. Hal ini membuat secara keseluruhan keamanan informasi pada SAP tidak terlindungi dengan baik. Evaluasi manajemen risiko keamanan informasi ini menjadi salah satu alat untuk mengetahui potensi risiko dan kontrol untuk menangani risiko pada keamanan informasi.

Evaluasi manajemen risiko keamanan informasi pada penelitian ini dilakukan dengan menggunakan acuan standar NIST SP 800 30. NIST SP 800 30 merupakan standar yang mengacu pada manajemen risiko keamanan informasi dan berfokus pada mengelola risiko agar dapat meminimalisir kerugian yang terjadi terhadap suatu perusahaan [1]. Risiko yang telah diidentifikasi, akan dilakukan penilaian risiko, kemudian dimitigasi risiko tersebut agar tingkat risiko dapat berkurang dari *level* tinggi ke *level* terendah [10]. NIST SP 800 30 sama dengan ISO 27005: 2011. Peneliti menggunakan NIST SP 800 30 karena NIST SP 800 30 memiliki langkah metode yang lebih rinci, sehingga dapat mengumpulkan data yang lebih detail dan NIST SP 800 30 lebih fokus membahas terhadap aset sistem

informasi perusahaan [11] [12]. Langkah selanjutnya setelah dilakukannya evaluasi manajemen risiko keamanan informasi menggunakan metode NIST SP 800 30, adalah peneliti melakukan penghitungan *maturity level* keamanan informasi.

Penghitungan *maturity level* keamanan informasi dilakukan berdasarkan kerangka kerja ISO 27002: 2005. Penghitungan *maturity level* dilakukan dengan tujuan untuk mengetahui tingkat kematangan keamanan informasi PT Hardo Soloplast. *Maturity Level* juga dapat digunakan untuk menganalisis kontrol yang sudah diimplementasikan dengan baik untuk menangani risiko keamanan informasi [1]. Hasil analisis kontrol dapat membantu peneliti dalam memberikan rekomendasi dengan tepat.

1.2. Perumusan Masalah

Dari latar belakang diatas dapat ditarik perumusan masalah bahwa PT Hardo Soloplast ingin mengetahui potensi risiko dan tingkat risiko pada keamanan informasi SAP, serta rekomendasi untuk menangani risiko pada keamanan informasi SAP. Rekomendasi ditarik berdasarkan hasil pengitungan *maturity level* keamanan informasi SAP.

1.3. Pertanyaan Penelitian

Dari perumusan masalah diatas, dapat dirumuskan pertanyaan penelitian sebagai berikut :

1. Bagaimana cara melakukan evaluasi manajemen risiko keamanan informasi SAP pada PT Hardo Soloplast?
2. Bagaimana cara penghitungan tingkat *maturity level* keamanan informasi SAP pada PT Hardo Soloplast?
3. Bagaimana rekomendasi yang tepat untuk menangani risiko keamanan informasi SAP pada PT Hardo Soloplast?

1.4. Tujuan

Penelitian ini memiliki tujuan yang ingin dicapai adalah :

1. Mengevaluasi manajemen risiko keamanan informasi SAP pada PT Hardo Soloplast, sehingga dapat mengetahui tingkat risiko yang dapat terjadi pada keamanan informasi SAP PT Hardo Soloplast.
2. Mengetahui tingkat *maturity level* pada keamanan informasi SAP PT Hardo Soloplast.
3. Memberikan rekomendasi-rekomendasi yang dapat meminimalisir risiko ke *level* terendah yang bisa diterima.
4. Dapat menjadi referensi untuk peneliti selanjutnya yang berhubungan dengan manajemen risiko keamanan informasi.

1.5. Batasan Masalah

Penelitian ini terbatas pada :

1. Studi kasus yang digunakan adalah PT Hardo Soloplast
2. Aset yang diteliti adalah sistem informasi mereka yaitu SAP dan lingkungan pendukung SAP yang telah diterapkan di PT Hardo Soloplast.
3. Kerangka kerja yang digunakan untuk melakukan evaluasi manajemen risiko keamanan informasi adalah NIST SP 800 30.
4. Kerangka kerja yang digunakan untuk melakukan *control maturity level* keamanan informasi menggunakan ISO 27002 : 2005.
5. Responden kuisioner yaitu sebatas staf yang memegang dan mengelola standar ISO yaitu 14 staf *non*-IT dan staf IT yang berjumlah 4 orang, dengan total 18 responden kuisioner.
6. Narasumber wawancara yaitu 2 orang terdiri dari Kepala *General Affair* selaku pengurus standar ISO, dan staf IT selaku pengelola sistem SAP.

1.6. Manfaat Penelitian

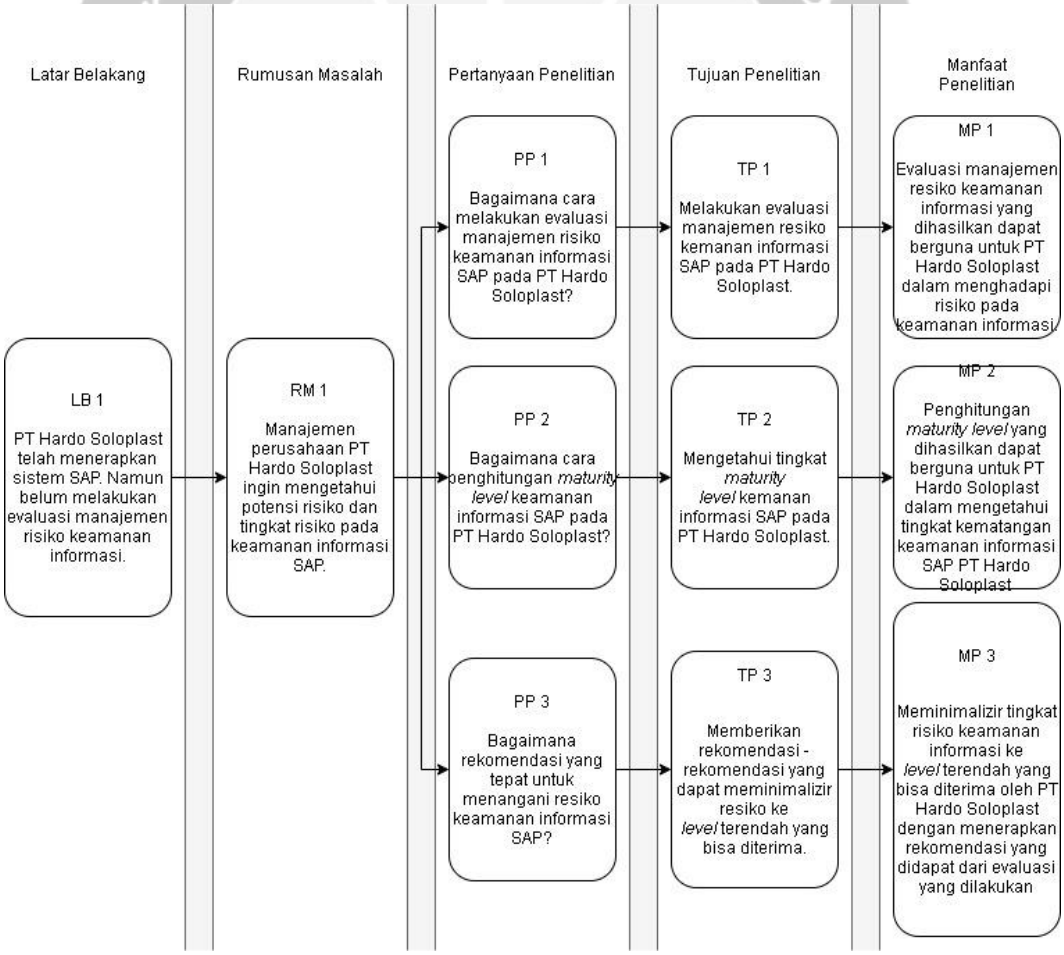
Diharapkan penelitian ini dapat memberikan manfaat :

1. Evaluasi manajemen resiko keamanan informasi yang dihasilkan dapat berguna untuk PT Hardo Soloplast dalam menghadapi risiko pada keamanan informasi.

2. Penghitungan *maturity level* yang dihasilkan dapat berguna untuk PT Hardo Soloplast dalam mengetahui tingkat kematangan keamanan informasi SAP PT Hardo Soloplast dan kontrol yang kurang diimplementasikan.
3. Meminimalisir tingkat risiko pada keamanan informasi ke *level* terendah yang bisa diterima oleh PT Hardo Soloplast dengan menerapkan rekomendasi yang didapat dari evaluasi yang dilakukan.

1.7. Bagan Keterkaitan

Latar Belakang, Rumusan Masalah, Pertanyaan Penelitian, Tujuan Penelitian, dan Manfaat Penelitian dirangkum menjadi Bagan Keterkaitan. Rangkuman tersebut dapat dilihat dan dipahami seperti pada Gambar 1.1



Gambar 1.1 Bagan Keterkaitan

BAB V
KESIMPULAN DAN REKOMENDASI

5.1. Kesimpulan

Berdasarkan hasil dari pembahasan dalam penelitian ini, penjelasan kesimpulan yang didapat adalah sebagai berikut :

1. Berdasarkan dilakukannya evaluasi risiko keamanan informasi SAP pada PT Hardo Soloplast menggunakan NIST SP 800 30 dapat disimpulkan rata-rata tingkat risiko keamanan informasi SAP pada PT Hardo Soloplast yaitu tinggi. Hal ini dikarenakan tingkat risiko keamanan informasi berupa 8 risiko tingkat tinggi dan 3 risiko tingkat sedang. Rata-rata dampak (*impact*) potensi risiko keamanan informasi SAP PT Hardo Soloplast yaitu sedang (berpengaruh besar namun perusahaan tidak terancam) dan rata-rata kemungkinan (*likelihood*) pada tingkat sering (11 sampai 15 kali dalam 5 tahun).
2. Berdasarkan hasil penghitungan *maturity level* menggunakan ISO 27002:2005 dapat disimpulkan bahwa *maturity level* keamanan informasi PT Hardo Soloplast sudah cukup matang dalam mengelola risiko karena *maturity level* keamanan informasi PT Hardo Soloplast sudah memenuhi target. Yaitu dengan maturity *level* pada tingkat 3.5 (Managed) yang berarti prosedur telah dikelola, dipantau, serta pengambilan tindakan proses tidak berjalan secara efektif namun dapat dilakukan dan Implementasi prosedur berjalan dengan baik. Sedangkan target *maturity level* pada tingkat 3 (Defined) yaitu prosedur telah terdokumentasi, terdefinisi, distandardisasikan, dan dikomunikasikan dengan baik namun proses implementasi diserahkan kepada pihak setiap individu.
3. Berdasarkan potensi risiko yang ada, peneliti menawarkan 7 rekomendasi untuk meminimalisir tingkat risiko dari tingkat tinggi ke tingkat terendah. Rekomendasi yang dikeluarkan berdasarkan kesepakatan dan wawancara

dengan salah satu staf IT yang bertanggung jawab untuk mengelola penggunaan sistem SAP di PT Hardo Soloplast.

a) Diadakannya edukasi karyawan atau staf agar tidak sembarang mengkoneksikan perangkatnya ke perangkat atau *network* umum. Hal ini untuk meminimalisir penyebaran *malware* ke perangkat keras server, komputer, laptop maupun *sharing* server PT Hardo Soloplast. Sehingga tingkat risiko penyebaran *malware* dapat dikurangi dari tingkat tinggi ke tingkat sedang, karena tingkat *likelihood* dari sedang (0.5) dapat berkurang menjadi jarang (0.1).
b) Dilakukannya edukasi karyawan atau staf untuk selalu melakukan *log out* SAP sebelum meninggalkan ruangan. Hal ini agar dapat meminimalisir risiko *social engineering* dan akses yang tidak sah dari pihak internal. Sehingga tingkat risiko dari tinggi dapat berkurang menjadi sedang, karena tingkat *likelihood* dari sering (1) dapat berkurang menjadi jarang (0.1).
c) Dilakukannya prosedur untuk memantau kapasitas memori RAM HANA *database* setidaknya 1 kali dalam 1 bulan. Hal ini agar meminimalisir risiko gagal koneksi ke HANA *database* . Sehingga tingkat risiko dapat dikurangi dari tinggi menjadi sedang, karena tingkat *likelihood* dari sering (1) dapat berkurang menjadi jarang (0.1).
d) Segera diadakannya *back up* server SAP. Hal ini agar proses bisnis PT Hardo Soloplast dapat tetap berjalan jika server SAP *down*. Sehingga tingkat risiko dapat dikurangi dari tinggi menjadi rendah, karena tingkat *impact* dapat dikurangi dari tinggi (100) menjadi rendah (10).
e) Diadakan kebijakan persyaratan untuk pihak ke 3 sebelum diberi hak akses ke aset informasi. Hal ini untuk meminimalisir risiko pencurian data informasi penting. Sehingga tingkat risiko dari tinggi dapat dikurangi menjadi sedang, karena tingkat *likelihood* dari sering (1) dapat dikurangi menjadi jarang (0.5).
f) Dilakukannya pelatihan berbasis peran khusus. Hal ini untuk mengurangi risiko data *corrupt* dan sistem SAP *crash*. Sehingga

tingkat risiko tinggi menjadi sedang, karena tingkat *likelihood* dari sering (1) dapat berkurang menjadi jarang (0.1).

g) Pemberian panduan undang-undang terhadap karyawan maupun masyarakat setempat. Hal ini untuk mengurangi risiko pencurian data informasi, karena masyarakat dan karyawan dapat mengetahui bahwa pencurian informasi sangat dilarang. Sehingga tingkat risiko dari tinggi dapat dikurangi menjadi sedang, karena tingkat *likelihood* dari sering (1) dapat berkurang menjadi jarang (0.1).

5.2. Saran

Untuk Penelitian selanjutnya, sebaiknya ditambahkan analisa manfaat dan biaya dengan melakukan penghitungan terhadap dampak dari kontrol yang diimplementasikan atau tidak diimplementasikan. Sehingga dapat diketahui kontrol yang paling efektif dan efisien dengan biaya terendah dan tidak lupa mengabaikan tingkat risiko.

DAFTAR PUSTAKA

[1] F. Mahardika, "Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1," *Jurnal Informatika:Jurnal Pengembangan IT,* vol. 2(2), pp. 1-8, 2017.

[2] P. W. D. G. Suherman, "Efektivitas Keamanan Informasi dalam Menghadapi Ancaman Sosial Engineering," *Jurnal Prodi Peperangan Asimetris,* vol. 3(1), pp. 73-90, 2017.

[3] E. S. A. A. Riszullah Putra, "Analisis Manajemen Resiko TI Pada Keamanan E-Learning dan Aset TI Menggunakan NIST SP 800 30 Revisi 1," *Jurnal Teknik Informatika dan Sistem Informasi,* vol. 6(1), pp. 96-105, 2019.

[4] I. K. A. P. I. P. A. E. P. Altry David Purba, "Audit Keamanan TI Menggunakan Standar ISO/IEC," *MERPATI,* vol. 6(3), pp. 148-158, 2018.

[5] R. P. A. R. I. A. Danis Sela Valena, "Analisis Manajemen Risiko Sistem Informasi Perpustakaan Universitas Lampung Menggunakan Metode NIST SP 800-30," *Jurnal Komputasi,* vol. 7(1), pp. 1-79, 2019.

[6] M. I. Fasa, "MANAJEMEN RESIKO PERBANKAN SYARIAH DI INDONESIA," *Jurnal Studi Ekonomi dan Bisnis Islam,* vol. 1(2), pp. 36-53, 2016.

[7] F. Fauzi, "MANAJEMEN RESIKO DI TENGAH PERUBAHAN MODEL BISNIS TELEKOMUNIKASI," *Jurnal Teknik Mesin,* vol. 5, pp. 33-36, 2016.

[8] Z. Prasetyo, "Penerapan Manajemen Resiko Operasional pada PT. Bank Pembangunan Daerah Sumatra Barat Cabang Painan Kabupaten Pesisir Selatan.," OSF, 2018. [Online]. Available: https://osf.io/83ea4. [Accessed 13 August 2020].

[9] A. Bank, "The Impact of Information System Risk Management on the Frequency and Intensity of Security Incidents," *International Journal of Electrical and Computer Engineering Systems*, vol. 8(2), pp. 41-46, 2017.

[10] W. Syafitri, "Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST SP 800-30 (Studi Khasus: Sistem Informasi Akademik Universitas XYZ)," *Jurnal CoreIT*, vol. 2(2), pp. 8-13, 2016.

[11] U. Arfan, "Perbandingan Kerangka Kerja ISO/IEC 27005 : 2011, NIST SP 800-30, dan OCTAVE-S," Academia, 2020. [Online]. Available: https://www.academia.edu/42190846/Contoh_Resume_Jurnal_Perbandingan_ISO_IEC_27005_2011_NIST_SP_800_30_OCTAVE_S. [Accessed 12 November 2020].

[12] Y. R. Eryanto, *Perencanaan Manajemen Keamanan Resiko Teknologi Informasi Berdasarkan Kerangka Kerja ISO/IEC 27005 di PT.Z*, Jakarta: Program Studi Magister Teknologi Informasi Fakultas Ilmu Komputer Universitas Indonesia, 2015.

[13] S. Priharto, "Pengertian Lengkap Manajemen Resiko, Komponen, Jenis dan Tujuannya dalam Bisnis," Accurate, 2020. [Online]. Available: https://accurate.id/marketing-manajemen/pengertian-lengkap-manajemen-risiko/. [Accessed 13 August 2020].

[14] G. S. D. Ni Ketut Dewi, "Strategi Investasi & Manajemen Resiko Rumah Sakit Swasta di Bali," *Jurnal Manajemen dan Bisnis*, vol. 16(2), pp. 110-127, 20119.

[15] F. F. Hilda Siregar, "Pengaruh Penerapan Manajemen Resiko Terhadap Fleksibilitas Pada Bank Umum Yang Terdaftar di Bursa Efek Indonesia 2013-2017," *Jurnal EBBANK*, vol. 9(2), pp. 51-62, 2018.

[16] R. P. Nishani Vincent, "IT risk management: interrelationships based on strategy implementation," *International Journal of Accounting & Information Management*, vol. 28(3), pp. 553-575, 2020.

[17] P. M, "Pengertian Informasi: Definisi, Fungsi, dan Contohnya.," Maxmanroe, 2018. [Online]. Available:

https://www.maxmanroe.com/vid/umum/pengertian-informasi.html. [Accessed 6 October 2020].

[18] E. L. Sukma, *Evaluasi Manajemen Risiko Keamanan Informasi Sistem Provisioning Gateway Telkom Flexi,* Jakarta: Program Studi Magister Teknologi Informasi Fakultas Ilmu Komputer Universitas Indonesia, 2013.

[19] I. M. I. S. S. F. C. H. Maryuliana, "Sistem Informasi Angket Pengukuran Skala Kebutuhan Materi Pembelajaran Tambahan Sebagai Pendukung Pengambilan Keputusan Di Sekolah Menengah Atas Menggunakan Skala Likert," *Jurnal Transistor Elektro dan Informatika,* vol. 1(2), pp. 1-12, 2016.

[20] D. Erdianto, *Audit Sistem Informasi System Application and Product in Data Processing (SAP) Pengadaan Material dengan Menggunakan Kerangka Kerja Cobit 4.1 pada Kantor Pusat di PT. Pindad (Persero).*, Bandung: Digital Library Fakultas Teknik dan Ilmu Komputer UNIKOM, 2014.

[21] I. R. Y. P. Rosmiati, "A Maturity Level Framework for Measurement of," *International Journal of Computer Applications,* vol. 141(8), pp. 1-6, 2016.

[22] M. Riadi, "KajianPustaka.com," 2020. [Online]. Available: https://www.kajianpustaka.com/2020/07/sistem-pengertian-karakteristik-dan-klasifikasi.html.. [Accessed 8 December 2020].

[23] B. M. Susanto, "Mengukur Keamanan Informasi: Studi Komparasi ISO 27002 dan NIST SP 800-55," *Seminar Nasional Teknologi Informasi dan Komunikasi,* pp. 175-180, 2013.

[24] M. S. K. S. N. B. A. B. W. R. Elizabeth Chew, "NIST Special Publication 800-55 Revision 1," in *I N F O R M A T I O N S E C U R I T Y*, Gaithersburg, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, 2008, p. 80.

[25] E. Supristiowadi, "Manajemen RisikoKeamanan Informasi pada Sistem Aplikasi Keuangan Tingkat Instansi (Sakti) Kementrian Keuangan," *Jurnal Perbendaharaan, Keuangan Negara dan Kebijakan Publik*, vol. 3(1), pp. 23-33, 2018.

[26] Author's Guide, "slideshare," 2015. [Online]. Available: https://www.slideshare.net/kenzou99/iso-27002-46466537. [Accessed 2020 November 26].

[27] Author's Guide, "Pengertian Wawancara," Talde Brooklyn, 5 August 2020. [Online]. Available: https://taldebrooklyn.com/pengertian-data/. [Accessed 5 February 2021].

[28] G. M. A. S. A. A. K. A. C. Yulius C. N. Bless, "Audit Keamanan SIMAK Berdasarkan ISO 27002," *MERPATI*, vol. 2(2), pp. 157-166, 2014.

[29] Author's Guide, "Pengertian Kuisioner Menurut para Ahli," Kumpulan Pengertian, 2018. [Online]. Available: http://www.kumpulanpengertian.com/2018/07/pengertian-kuesioner-menurut-para-ahli.html. [Accessed 5 February 2021].

[30] Author's Guide, "Pengertian Observasi," Talde Brooklyn, 27 August 2020. [Online]. Available: https://taldebrooklyn.com/pengertian-akuntansi/. [Accessed 5 February 2021].

[31] Author's Guide, "Idcloudhost.com," 2016. [Online]. Available: https://idcloudhost.com/mengenal-apa-itu-malware-penyebab-dan-mengatasinya/.. [Accessed 5 January 2021].

[32] R. E. G. Fajar Ilham Satria Yudha, "RISK ASSESSMENT PADA MANAJEMEN RESIKO KEAMANAN INFORMASI MENGACU PADA BRITISH STANDARD ISO/IEC 27005 RISK MANAGEMENT," *Jurnal Algoritma*, vol. 13(1), pp. 333-340, 2016.

[33] S. A. P. Hana Driantami, "Analisis Resiko Teknologi Informasi Menggunakan ISO 31000," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer* , vol. 2(11), pp. 4991-4998, 2018.

[34] D. Rani, "ANALISIS MANAJEMEN RESIKO TEKNOLOGI INFORMASI DAN PEMETAAN MATURITY LEVEL PADAPT. XYZ MENGGUNAKAN FRAMEWORK COBIT 4.1," *Jurnal Manajemen Informatika*, vol. 7(2), pp. 43-54, 2017.

Lampiran

Transkrip Wawancara

Narasumber 1 : Prasetyo Aji Wibowo

Jabatan : Staff IT

Narasumber 2 : Nur Cholis

Jabatan : Kepala General Affair

Waktu : 1 November 2020 - 26 Januari 2021

1. **Pewawancara** : Siapa pengguna sistem SAP yang valid?

   Narasumber :Semua departemen menggunakan SAP, untuk yg tidak kontak langsung dengan SAP hanya departemen Produksi bagian pelaksana (Operator).

2. **Pewawancara** :Apa tujuan dari sistem dalam kaitannya dengan misi organisasi?

   Narasumber :

   1. Mempermudah analisa manajemen untuk mengambil keputusan yang terbaik. Contoh mencari harga jual sing pas (harga karung per kantong realnya berapa).
   2. Untuk bidang produksi tidak terlalu berpengaruh.
   3. Mempermudah kegiatan administratif (Contoh : Kalau tanpa sisem maka akan menjadi sangat rumit, untuk mengirim Work Order harus mengirim surat atau ngetik dan cetak, dst)

3. **Pewawancara** :Apa persyaratan requirement sistem SAP yang tersedia?

   Narasumber :

   1. Sisi Server : Spesifikasi server e harus high end. SO harus Linux (Krna menggunakan SAP HANA).
   2. Sisi User / karyawan : Laptop Spesifikasi standar yang bisa word dan exel.

4. **Pewawancara** :Informasi (input & output) yang diperlukan oleh organisasi?

   Narasumber :

   1. Semua yang diinputkan di SAP menjadi input = SO
   2. Output = laporan, neraca.

5. **Pewawancara** :Seberapa penting informasi terhadap misi penggunaan perusahaan?

Narasumber :Sangat penting. Segala bentuk informasi berujung ke pihak akuntansi untuk mengethaui laba rugi dll.

6. **Pewawancara** :Bagaimana jalur arus informasi dan bagaimana infrastruktur jaringan di PT Hardo Soloplast?

   Narasumber :

   1. sesuai dengan bisnis proses yg dipelajari
   2. Infrastrukur : topologi tree.

Mempunyai ruang server sendiri, ada server baru, add on, server email, dll.

7. **Pewawancara** :Apa jenis informasi yang diproses oleh dan disimpan pada sistem?

   Narasumber :Keuangan, penjualan, pembelian, produksi, harga penjualan, harga pembelian, konsumen, tender, vendor.

8. **Pewawancara** :Apa sensitivitas/klasifikasi tingkat informasi? **Narasumber** :

   1. Financial : dipegang orang akunting. Bisa mengakses semuanya mirip dengan Super User.
   2. Logistik : Produksi, purchasing, marketing hanya bisa mengakses yang berhubungan dengan barnag - barang.

9. **Pewawancara** :Informasi ditangani oleh atau tentang sistem yang tidak harus diungkapkan dan kepada siapa?

   Narasumber :Keuangan laba rugi yang boleh diketahui oleh IT, head akunting, manajer dan general manajer. tidak boleh diketauhi semua orang

10. **Pewawancara** :Dimana secara khusus informasi diproses dan disimpan?

    Narasumber :Server. Sharing server. Laptop

11. **Pewawancara** :Apa saja jenis penyimpanan informasi?

    Narasumber :HDD external (backup), server, laptop

12. **Pewawancara** :Apa dampak potensial pada perusahaan jika data/ informasi yang diungkapkan kepada pihak yang tidak berwenang?

    Narasumber :

    1. kerugian.
    2. Kalau data tentang produksi bocor, bisa memperuntung kompetitor. (contoh : Kompetitor mengetahui jumlah kapasitas produksi PT Hardo Soloplast. Maka

kompetitor bisa mengetahui kelemahan itu dan menggunakan kelemahan itu untuk memperkuat perusahaan mereka).

13. **Pewawancara** :Apa persyaratan untuk ketersediaan informasi dan integritas?

    Narasumber :Tidak ada persyaratan khusus. Tiap bagian harus bertanggung jawab terhadap data/informasi yang dikelolannya baik itu dokumen elektronik atau dokumen fisik. Untuk penggunaan hardware, software, network setiap user wajib menjaga dan memelihara setiap penggunaannya.

14. **Pewawancara** :Apa efek pada misi perusahaan jika sistem atau informasi tidak dapat diandalkan?

    Narasumber :Pekerjaan tidak dapat maksimal.

15. **Pewawancara** :Pernahkan sistem SAP mengalami down? Berapa kali? Berapa lama waktu yang dibutuhkan untuk recovery?

    Narasumber :

    1. Pernah. Jarang. Tergantung keeroran. Pernah recory nya membuthkan 12 jam. Pernah 1 minggu. Selama down karyawan kerja data disimpan di exel.
    2. Listrik mati, solar generator habis
    3. Malware, server OS linux tidak ada anti virus

16. **Pewawancara** :Apakah PT Hardo Soloplast memiliki program manajemen risiko?

    Narasumber :Ada

17. **Pewawancara** :Sumber ancaman yang ada dalam penggunaan TI di PT Hardo Solopalst

    Narasumber :Malware

18. **Pewawancara** :Kejadian vulnerability yang pernah terjadi pada sistem informasi yang ada PT Hardo Soloplast?

    Narasumber :

    1. Ransomware

19. **Pewawancara** :Bagaimana prosedur penanganan bila semua ancaman terjadi?

Narasumber :Prosedur khusus tidak ada, namun untuk perawatan ada. Untuk penanganan bila terjadi tergantung situasi. Bila perlu diinstal ulang maka diinstal ulang. Bila cuma bisa dibersihkan virusnya maka dibersihkan saja.

20. **Pewawancara** :Seberapa penting penggunaan TI di PT Hardo Soloplast, apakah TI menjadi suatu kebutuhan yang harus dijaga dan dikelola dengan baik?

    Narasumber :Sangat penting untuk membantu keputusan manajemen. Maka dari itu sangat menjadi suatu kebutuhan yang harus dijaga dan dikelola dengan baik.

21. **Pewawancara** :Perlukah standar kebijakan dibuat, Standar kebijakan apa yang sudah diterapkan untuk mengatur dan mengelola keamanan informasi di PT Hardo Soloplast?

    Narasumber :Perlu. Kemanan ketat. Tidak boleh menyimpan data ke device lain. Tidak boleh instal downoad jaaln e program lain. Tidak boleh asal colok flashdisk sembarangan. Akses wifi asing.

Kuesioner

Level	Pertanyaan	Kriteria	Nilai						Komentar
			0	1	2	3	4	5	
Risk Management	P1	Apakah perusahaan anda memiliki program manajemen risiko?			1	6	6	2	
	P2	Apakah perusahaan anda memiliki proses untuk mengidentifikasi dan menilai risiko internal dan eksternal secara layak dapat diduga terhadap keamanan, kerahasiaan, dan atau integritas dari setiap data elektronik, dokumen, atau catatan lain yang mengandung informasi penting?		1	1	8	3	2	
	P3	Apakah perusahaan anda melakukan penilaian risiko secara rutin untuk mengidentifikasi tujuan utama yang perlu didukung oleh		1	1	8	1	3	

		program keamanan informasi anda?							
Kebijakan Keamanan	P4	Apakah perusahaan anda memiliki kebijakan keamanan informasi yang telah disetujui oleh manajemen?		1	3	6	2	2	
	P5	Apakah kebijakan tersebut telah dipublikasikan dan dikomunikasikan kesemua pihak terkait?		1	3	6	2	2	
	P6	Apakah perusahaan anda meninjau kebijakan pada jangka waktu tertentu untuk mencakup perubahan signifikan dan memantau kepatuhan?		2	1	1	8	2	
Organisasi Keamanan Informasi	P7	Apakah fungsi keamanan informasi anda memiliki kewenangan yang dibutuhkan untuk		2	2	5	4		

		mengelola dan memastikan kepatuhan dengan pemograman keamanan informasi?							
	P8	Apakah perusahaan anda memiliki individu dengan kemampuan informasi tanggung jawab keamanan perusahaan dan otoritas tertulis dalam deskripsi pekerjaan mereka, atau setara mungkin CEH, CIO, CISO atau lainnya?	1	1	1	8	2		
	P9	Apakah tanggung jawab secara jelas ditetapkan untuk semua bidang arsitektur keamanan informasi, kepatuhan, proses, dan audit?	1		3	6	3		

P10	Apakah ada proses formal terhadap individu dengan tanggung jawab untuk menilai keamanan informasi dan perangkat keras yang tepat, perangkat lunak, dan layanan, yang memastikan mereka mengikuti persyaratan kebijakan keamanan?		1	2	2	8		
P11	Apakah perusahaan anda memerlukan penggunaan perjanjian kerahasiaan atau menjaga rahasia bagi karyawan dan pihak ketiga?		1	6	4	2		
P12	Apakah perusahaan anda menjaga hubungan dengan pemerintah setempat?				3	7	5	

P13	Apakah perusahaan anda berpatisipasi dengan kelompok - kelompok lokal atau nasional keamanan (seperti DEPHAN, REN-ISAC, EDUCAUSE, InfraGard, Asosiasi Keamanan Informasi, dll) ?	1	3	6	1	1	1	
P14	Apakah perusahaan anda memiliki review keamanan secara independen yang lengkap pada interval yang direncanakan atau ketika terjadi perubahan yang signifikan terhadap lingkungan?		1	7	3	1	1	
P15	Apakah perusahaan anda menentukan persyaratan keamanan dalam kontrak dengan entitas eksternal (pihak ketiga) sebelum memberikan akses		3	5	2	1	2	

		ke aset informasi kelembagaan yang sensitif?							
	P16	Apakah persyaratan dialamatkan dan remediated sebelum memberikan akses ke data, aset, dan sistem informasi?	2	2	5	2	1	1	
Manajemen Aset	P17	Sudahkah perusahaan anda mengidentifikasi aset informasi penting dan fungsi yang bergantung padanya?		1		8	3	2	
	P18	Apakah perusahaan anda mengelompokkan informasi untuk menunjukkan tingkat yang sesuai dari keamanan informasi?		1		8	3	2	
Keamanan Sumber Daya Manusia	P19	Apakah semua individu yang berinteraksi dengan sistem PT Hardo Soloplast menerima pelatihan kesadaran	1		1	5	5	2	

		keamanan informasi?							
	P20	Apakah perusahaan anda melakukan pelatihan berbasis peran khusus?	1		9	3		1	
	P21	Apakah program keamanan informasi ini dengan jelas menyatakan tanggung jawab, kewajiban, dan konsekuensi?		1	2	8	2	1	
	P22	Apakah perusahaan anda memiliki sebuah proses untuk mengambil sistem dan membangun akses kembali asset yang digunakan?	1	1	1	8	2	1	
	P23	Apakah perusahaan anda memiliki sebuah proses untuk mengambil akses sistem ketika ada perubahan posisi atau mengubah tanggung jawab?		1	1	6	4	2	

Keamanan Fisik dan Lingkungan	P24	Apakah data center di perusahaan anda termasuk control untuk memastikan bahwa hanya pihak berwenang yang dapat mengakses fisiknya?						2	
	P25	Apakah perusahaan anda memiliki langkah - langkah preventif di tempat untuk melindungi hardware kritis dan kabel - kabel dari alam dan ancaman manusia?					1	1	
	P26	Apakah perusahaan anda memiliki proses atau prosedur untuk mengeluarkan kunci, kode, dan kartu yang memerlukan otorisasi yang tepat dan cek background untuk akses ke fasilitas - fasilitas yang sensitif?				2			
	P27	Apakah perusahaan anda mengikuti					1	1	

		panduan rekomendasi vendor dalam menjaga peralatan?							
	P28	Apakah ada proses untuk mendeteksi penghapusan yang tidak sah terhadap peralatan, informasi atau perangkat lunak?					1	1	
Komunikasi dan Manjemen Operasi	P29	Apakah perusahaan anda mempertahankan standar konfigurasi keamanan untuk sistem informasi dan aplikasi?						2	
	P30	Apakah perubahan sistem informasi diuji, disahkan, dan dilaporkan?					1	1	
	P31	Apakah tugas yang dipisahkan bisa memastikan modifikasi informasi terdeteksi secara disengaja atau tidak sah?			1		1		
	P32	Apakah kesepakatan untuk layanan eksternal				1	1		

	sistem informasi menentukan persyaratan keamanan?							
P33	Apakah perusahaan anda memiliki proses di tempat untuk menilai penyedia sistem informai eksternal sesuai dengan persyaratan keamanan yang sesuai?				1	1		
P35	Apakah perjanjian layanan sistem informasi eksternal dilaksanakan dan ditinjau secara rutin untuk memastikan persyaratan keamanan saat ini?					2		
P36	Apakah perusahaan anda memiliki proses untuk memantau penggunaan kunci sumber daya sistem dan memitimigasi risiko terjadinya sistem downtime?					2		

P37	Adakah metode yang digunakan untuk mendeteksi dan membasmi malicious code yang diketahui melalui transfer email, web atau removable media?		1	1				
P38	Apakah frekuensi proses back up data anda konsisten dengan persyaratan ketersediaan organisasi anda?					1	1	
P39	Apakah perusahaan anda secara rutin menguji pemulihan prosedur?		1			1		
P40	Apakah perusahaan anda memantau jaringan kabel dan nirkabel untuk akses yang tidak sah?					1	1	
P41	Apakah perusahaan anda saat ini memiliki proses untuk memeriksa, seperti antivirus, firewall diaktifkan, update patch OS, dll		1			1		

	ketika perangkat mereka (karyawan maupun non karyawan) terhubung dengan jaringan anda?							
P42	Apakah perusahaan anda memiliki arsitektur jaringan tersegmentasi untuk menyediakan tingkat keamanan yang berbeda berdasarkan klasifikasi informasi?			1			1	
P43	Apakah akses sever internet dilindungi oleh lebih dari satu lapisan / layer keamanan (firewall, IDS Jaringan, IDS Host, aplikasi IDS)?				1	1		
P44	Apakah perusahaan anda menggunakan / metode enkripsi yang sesuai untuk melindungi data sensitif dalam perjalanan / pengiriman data?				2			

P45	Apakah perusahaan Anda memiliki kebijakan dan prosedur untuk melindungi informasi yang sudah ditukarkan (dalam organisasi Anda dan dalam Perjanjian pihak ketiga) dari pencegatan, penyalinan, modifikasi, misrouting dan kehancuran?				1	1		
P46	Apakah perusahaan Anda memiliki proses untuk memastikan data yang terkait dengan perdagangan elektronik (ecommerce) melintasi jaringan publik dilindungi dari aktivitas penipuan, pengungkapan yang tidak sah, atau modifikasi?				2			

P47	Apakah perusahaan anda memiliki otomatisasi privilege untuk kegiatan keamanan terkait dengan perubahan konfigurasi hardware, perubahan konfigurasi perangkat lunak, upaya akses, dan otorisasi dan login?				1	1		
P48	Apakah perusahaan Anda memiliki proses secara rutin memantau log akitivitas untuk mendeteksi kegiatan tidak sah dan aktivitas anomali?				1	1		
P49	Apakah perusahaan Anda merekam log review (resertifikasi / atestasi)?				1		1	
P50	Adakah langkah yang diambil untuk mengamankan data log untuk mencegah					1	1	

		akses yang tidak sah dan sabotase?							
	P51	Apakah lembaga Anda secara teratur meninjau akses administratif dan operatif untuk log audit?					1	1	
	P52	Adakah tool pemantauan file integritas yang digunakan untuk mengingatkan personil dari modifikasi yang tidak sah terhadap file system yang kritis, file konfigurasi, atau file konten dan mengkonfigurasi perangkat lunak untuk menangani file yang penting setidaknya seminggu sekali?					1	1	
	P53	Apakah perusahaan Anda memiliki proses untuk memastikan sinkronisasi system jam dengan sumber					1	1	Direct Server

		otoritatif (misalnya, melalui NTP) secara periodik sepadan dengan potensi risiko?							
Access Control	P54	Apakah perusahaan anda memiliki kebijakan akses control untuk otorisasi dan mengambil hak akses ke sistem informasi?					1	1	
	P55	Apakah perusahaan anda memiliki proses di tempat untuk memberikan atau mengambil hak akses pengguna yang tepat?					1	1	
	P56	Apakah perusahaan anda memiliki program manajemen password yang mengikuti standar keamanan sekarang?					1	1	
	P57	Apakah perusahaan anda memiliki prosedur untuk meninjau akses					1	1	

	pengguna untuk memastikan pengguna memiliki previliges yang sesuai?							
P58	Apakah perusahaan anda menggunakan langkah - langkah khusus untuk mengamankan akses layanan?				1		1	
P59	Apakah perusahaan anda memastikan bahwa akses pengguna terhadap diagnostic port dan aplikasi, dan konfigurasinya dibatasi hanya untuk individu yang berwenang?					1	1	
P60	Apakah perusahaan anda menggunakan langkah - langkah tertentu untuk mencegah dan mendeteksi akses aneh untuk semua wireless LAN?					1	1	

P61	Apakah perusahaan anda menggunakan teknologi untuk memblokir atau membatasi informasi sensitif yang tidak terenkripsi terhadap penerimaan data dari untrusted network?				1	1		
P62	Apakah perusahaan anda memiliki mekanisme di tempat untuk mengelola identitas digital (rekening, kunci, token) sepanjang siklus hidup mereka, dari pendaftaran sampai pemutusan?				1	1		
P63	Apakah ada kebijakan di tempat untuk membatasi sharing password?				2			
P64	Apakah perusahaan Anda melarang penggunaan akun/rekening generik (umum) dengan akses	1				1		

	istimewa terhadap sistem?							
P65	Apakah perusahaan anda menerapkan sistem otentikasi untuk melindungi sumber daya dengan tingkat sensitivitas yang lebih tinggi?					2		
P66	Apakah perusahaan anda memiliki otorisasi yang memaksa batas waktu lockout terhadap login yang gagal dan default untuk minimun previliges?					1	1	
P67	Apakah perusahaan anda memiliki standar untuk mengisolasi data sensitif dan prosedur dan teknologi ditempat untuk melindunginya dari akses yang tidak sah dan merusak?					1	1	

P68	Apakah perusahaan anda memiliki prosedur untuk penggunaan perangkat komputasi mobile (terlepas dari kepemilikan) yang menyimpan, mengolah, atau mengirimkan data yang berhubungan dengan perusahaan?	1				1		
P69	Apakah perusahaan anda melakukan enkripsi pada ponsel (laptop, tablet, dll) perangkat komputer?	1				1		
P70	Apakah perusahaan anda memiliki kebijakan telework yang membahas akses dan persyaratan keamanan multi faktor untuk tiitk akhir yang digunakan?	1				1		

Akuisisi Sistem Informasi, Pengembangan dan Pemeliharaan	P71	Apakah perusahaan anda melakukan proses untuk memvalidasi produk keamanan dan layanan perangkat lunak yang dibeli?					1	1	
	P72	Apakah perusahaan anda melakukan validasi sistem informasi baru atau perangkat tambahan untuk sistem informasi yang ada terhadap persyaratan keamanan yang ditetapkan?				1		1	
	P73	Apakah standar telah ditetapkan bahwa praktek pengalamatan coding yang aman (misalnya, validasi input, penanganan error yang tepat, manajemen sesi, dll), dan mempertimbangkan kerentanan					1	1	

	keamanan aplikasi umum (e.g., CSRF, XSS, code injection, etc.)?							
P74	Apakah pemeriksaan validasi dimasukkan kedalam aplikasi untuk untuk mendeteksi korupsi informasi melalui kesalahan proses atau tindakan yang disengaja?					1	1	
P75	Apakah perusahaan anda melakukan integritas pesan yang diperlukan?				1	1		
P76	Output yang salah mengakibatkan kerusakan, meskipun system teruji. Apakah perusahaan anda memiliki cek validasi untuk memastikan data output seperti yang diharapkan ?					1	1	

P77	Apakah kebijakan perusahaan anda menunjukkan keadaan bagaimana enkripsi harus digunakan (seperti saat istirahat, dalam keadaan transit, dengan data rahasia atau sensitif) ?				1	1		
P78	Apakah standar untuk manajemen kunci didokumentasikan dan dikerjakan?					1	1	
P79	Apakah Anda menetapkan prosedur untuk menjaga kode sumber selama siklus hidup pengembangan dan produksi sementara untuk mengurangi risiko corupt perangkat lunak?			1	1			
P80	Apakah perusahaan anda menerapkan standar keamanan yang sama untuk uji data sensitif yang anda terapkan pada				2			

	data produksi sensitif ?							
P81	Apakah perusahaan anda membatasi dan memonitor akses ke kode sumber untuk untuk mengurangi korupnya risiko?				2			
P82	Apakah perusahaan anda memiliki dan melakukan proses manajemen konfigurasi untuk memastikan bahwa perubahan kritis sistem untuk alasan bisnis telah menerima otorisasi yang tepat?				1		1	
P83	Apakah perusahaan anda melakukan ulasan dan test untuk memastikan bahwa perubahan yang dibuat untuk sistem (Console / SAP) tidak memiliki dampak negatif pada					1	1	

	keamanan atau operasi?							
P84	Apakah perusahaan anda menerapkan alat dan prosedur untuk memantau dan mencegah hilangnya data sensitif?					1	1	
P85	Apakah perjanjian kontrak anda termasuk persyaratan keamanan untuk outsourcing pengembangan perangkat lunak?				1	1		
P86	Apakah perusahaan anda memiliki strategi manajemen patch dan tanggung jawab yang ditugaskan untuk memantau dan menanggapi segera, merilis, buletin keamanan, dan laporan kerentanan ?				1	1		

Manajemen Insiden Keamanan Informasi	P87	Apakah prosedur penanganan insiden di tempat untuk melaporkan dan menanggapi peristiwa keamanan di seluruh siklus hidup insiden , termasuk definisi peran dan tanggung jawab ?			1		1		
	P88	Apakah staff respon insiden anda menyadari persyaratan hukum atau kepatuhan sekitarnya pengumpulan bukti?					2		
Manajemen Kelangsungan Bisnis	P89	Apakah perusahaan Anda memiliki rencana kesinambungan bisnis yang didokumentasikan teknologi informasi yang didasarkan pada analisis dampak bisnis, diuji secara berkala oleh staf senior atau dewan pengawas ?					1	1	

	P90	Apakah perusahaan Anda memiliki rencana kesinambungan bisnis yang didokumentasikan teknologi informasi dan telah ditinjau dan disetujui oleh staf senior atau dewan pengawas ?					1	1	
Compliance	P91	Apakah perusahaan anda memiliki catatan manajemen atau data tata kelola kebijakan yang membahas siklus hidup baik dokumen maupun catatan elektronik di perusahaan ?			6	3	3	2	
	P92	Apakah perusahaan anda memiliki kebijakan perlindungan data yang dilaksanakan mencakup informasi pribadi personaly identifiable information (PII)?					1	1	

P93	Apakah perusahaan anda memiliki kebijakan penggunaan yang diterima untuk mendefinisikan penyalahgunaan?		3		9	1	1	
P94	Apakah perusahaan anda memberikan panduan bagi masyarakat terhadap undang - undang / hukum?	2		7	1	2		
P95	Apakah standar operasional prosedur dievaluasi secara berkala untuk kepatuhan terhadap kebijakan keamanan organisasi, standar, dan prosedur?		1		9	1	3	
P96	Apakah perusahaan anda melakukan pengujian aplikasi secara periodik dan vulnerability jaringan atau pengujian penetrasi terhadap sistem informasi yang kritis?					1	1	

	P97	Apakah anda melakukan audit independen pada sistem informasi untuk mengidentifikasi kekuatan dan kelemahan?					1	1	
	P98	Apakah perusahaan anda melakukan pemisahan antara perangkat audit dengan pembangunan dan sistem operasional untuk menghindari penyalahgunaan atau kompromi?					1	1	

Tabel Revisi

No.	Tugas Revisi	Halaman Revisi
1.	Bagan Penelitian	Latar Belakang diganti menjadi " PT Hardo telah menerapkan SAP namun belum melakukan evaluasi manajemen risiko keamanan informasi" dan Rumusan Masalah diganti menjadi "Manajemen perusahaan PT Hardo Soloplast ingin mengetahui risiko keamanan informasi"
2.	Penataan Kalimat Bab 1 Pendahuluan, Latar Belakang	Menceritakan keadaan SAP sekarang. Membuang kalimat yang tidak digunakan. Pemberian titik dan koma yang tepat. Paragraf 1 dengan selanjutnya harus ada kata penyambung. Kalimat berbahasa teori dipindahkan ke Bab 2 Dasar Teori.
3.	Penataan Sub Bab 2	Sub Bab dengan judul "Perbandingan" tidak diperbolehkan.
4.	Sinkronisasi dari awal hingga akhir	Sinkronisasi dari latar belakang hingga kesimpulan.
5.	Penataan Bab 5 Kesimpulan	Kesimpulan berisi tentang jawaban dari tujuan dan pertanyaan penelitian.
6.	Pemanggilan nomor tabel dan gambar	Setiap nomor tabel dan gambar harus dipanggil.
7.	Merapikan font pada nama tabel	Penamaan tabel dengan font yang sesuai dengan template yang disediakan.
8.	Gambar Bab 4 diperjelas	Menampilkan gambar pada Bab 4 yang lebih jelas, tidak buram.
9.	Penomoran dalam tabel	Nomor tabel tidak urut. Dimulai pada nomor 2
10.	Rekomendasi	Menjelaskan dari mana peneliti mendapatkan rekomendasi yang diberikan pada Tabel 4.2 dan Tabel 4.11, serta memberi dasar rekomendasi.
11.	Pelengkapan Dokumen	Untuk tahap penelitian "Identifikasi Aset" dan "Identifikasi Proses alur kerja"

		dikerjakan pada Bab 4. Lampiran Interview dan Hasil Kuesioner diletakan pada halaman Lampiran
12.	Penjelasan Bab 2	Menegaskan perbedaan penggunaan NIST SP 800 30 dan ISO 27002:2005 pada penelitian ini
13.	Perbaikan Kesalahan Penulisan	Memperbaiki kesalahan penulisan (bersifat ambigu, typo)
14.	Perbaikan Penulisan Rumus	Memperbaiki tata cara penulisan rumus pada Bab 2.
15.	Perbaikan Tata Penulisan	Penggantian kalimat penghubung yang digunakan untuk kata pembuka. Penggunaan kata baku. Penggunaan kalimat yang berisi rujukan.
16.	Perbaikan Penulisan Sitas	Menulis sitasi berdasarkan IEEE
17.	Judul	Menyesuaikan judul penelitian dengan isi.