JTERA - Jurnal Teknologi Rekayasa, Vol. 3, No. 2, Desember 2018, Hal. 145-156 p-ISSN 2548-737X
DOI: 10.31544/jtera.v3.i2.2018.145-156 e-ISSN 2548-8678

Implementasi Awal Sistem Manajemen Keamanan Informasi pada UKM Menggunakan Kontrol ISO/IEC 27002

Rokhman Fauzi
Program Studi Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
Jalan Telekomunikasi No. 1 Bandung, Indonesia
rokhmanfauzi@telkomuniversity.ac.id

Abstrak

Informasi merupakan aset organisasi yang harus dilindungi keamanannya. Sistem manajemen keamanan informasi diimplementasikan untuk melindungi aset informasi dari berbagai ancaman untuk menjamin kelangsungan usaha, meminimalisasi kerusakan akibat terjadinya ancaman, mempercepat kembalinya investasi, dan peluang usaha. Pada penelitian ini, standar internasional ISO/IEC 27001 dan analisis risiko metode OCTAVE-S digunakan dalam perancangan sistem manajemen keamanan informasi di salah satu perusahaan yang merupakan sebuah Usaha Kecil Menengah (UKM) yang bergerak di bidang *engineering services*. Sesuai dengan kondisi perusahaan, analisis risiko dilakukan menggunakan metode OCTAVE-S. Implementasi awal sistem manajemen keamanan informasi dilakukan menggunakan kontrol-kontrol pada ISO/IEC 27002. Prioritas utama hasil implementasi adalah penyusunan kebijakan dan prosedur serta peningkatan kesadaran keamanan informasi.

Kata kunci: sistem manajemen keamanan informasi, ISO/IEC 27001, ISO/IEC 27002, analisis risiko metode OCTAVE-S

Abstract

Information is a part of organizational asset that must be secured. Information security management system is implemented to secure information assets from threats for ensuring business processes, minimizing loss, satisfying investment, and enlarging opportunities. In this research, international standard ISO/IEC 27001 and risk analysis OCTAVE-S method is used in design of information security management system in one company of engineering services small-medium enterprise. Based on organization specifications, OCTAVE-S method is chosen as risk analysis method. Initial implementation of the Information Security Management System is conducted using controls on ISO/IEC 27002. The main priorities of implementation are the formulation of policies and procedures, and also increased awareness of information security.

Keywords: *information security management system, ISO/IEC 27001, ISO/IEC 27002, risk analysis OCTAVE-S method*

I. PENDAHULUAN

Usaha kecil menengah (UKM) memiliki kontribusi yang sangat besar bagi perekonomian Indonesia. UKM mempunyai tingkat penyerapan tenaga kerja sekitar 97% dari seluruh tenaga kerja nasional dan mempunyai kontribusi terhadap produk domestik bruto (PDB) sekitar 57% [1]. Menurut Kementerian Koperasi dan Usaha Kecil Menengah (Kemenkop UKM), sejumlah 3,79 juta usaha mikro, kecil, dan menengah (UMKM) sudah memanfaatkan *platform online* dalam memasarkan produknya. Jumlah ini berkisar 8% dari total pelaku UMKM yang ada di Indonesia, yakni 59,2 juta [2]. Perkembangan tersebut menunjukkan bahwa penggunaan teknologi informasi telah meningkat berlipat ganda baik dalam pengolahan, penyimpanan, pertukaran, maupun distribusi informasi. Sebagai aset, informasi menjadi salah satu hal penting dalam menjamin kelangsungan dan pertumbuhan organisasi [3][4][5]. Hal ini mendorong meningkatnya kebutuhan akan keamanan informasi yang secara garis besar

Diterima: 20 Mei 2018; Direvisi: 21 Juli 2018; Disetujui: 11 Agustus 2018
JTERA, Vol. 3, No. 2, Desember 2018

memiliki tiga aspek utama yang disebut sebagai C.I.A triangle model (*confidentiality*, *integrity*, dan *availability*).

Manajemen keamanan informasi pada dasarnya ditujukan untuk menjamin pengamanan kerahasiaan data, integritas informasi, dan ketersediaan informasi. Selain itu, manajemen keamanan informasi juga ditujukan untuk memastikan kepatuhan organisasi terhadap peraturan, hukum, maupun standar yang berlaku. Tujuan manajemen keamanan informasi berbeda dengan manajemen teknologi informasi secara umum. Karakteristik khusus manajemen keamanan informasi dikenal sebagai 6P yaitu: *planning, policy, programs, protection, people,* dan *project management* [6]. Menurut laporan Symantec, pada tahun 2017 UKM mendapatkan rata-rata 45,2 *e-mail spam* per pengguna serta 12,8 *e-mail malware*. Indonesia berada pada peringkat ke-3 dunia dalam jumlah *email malware* dan peringkat ke-9 dunia dalam tingkat serangan *phising* [7]. Rata-rata kerugian akibat serangan *cyber* terhadap UKM di Asia Pasifik diperkirakan mencapai 96 ribu Dollar Amerika Serikat [8]. Dalam kondisi tersebut, masih banyak organisasi yang belum memahami pentingnya manajemen keamanan informasi. Di sisi lain, mayoritas organisasi yang sudah memahami pentingnya manajemen keamanan informasi ternyata hanya memperhatikan aspek teknologi yang mereka miliki. Manajemen keamanan informasi seharusnya memberikan solusi yang komprehensif mencakup faktor *people, process,* dan *technology* [9].

Pada penelitian ini dilakukan implementasi awal sistem manajemen keamanan informasi sebuah perusahaan yang merupakan sebuah UKM yang bergerak di bidang *engineering services*. Perancangan sistem manajemen keamanan informasi ini mengacu pada standar internasional ISO/IEC 27001 dan analisis risiko metode OCTAVE-S, sedangkan implementasi awalnya menggunakan kontrol-kontrol pada ISO/IEC 27002. Hasil penelitian ini diharapkan dapat menjadi salah satu langkah awal dalam perancangan dan implementasi sistem manajemen keamanan informasi, khususnya pada UKM di Indonesia.

II. TINJAUAN PUSTAKA

Pemanfaatan teknologi dalam pengelolaan informasi selain meningkatkan peluang manfaat sekaligus juga memunculkan berbagai risiko. Risiko Teknologi Informasi/TI merupakan bagian dari risiko bisnis dalam kaitannya dengan penggunaan, kepemilikan, pengoperasian, pelibatan, pengaruh, dan penerapan TI [10][11]. Risiko TI terdiri atas 4 kategori, yakni risiko keamanan, risiko ketersediaan, risiko kinerja, dan risiko kepatuhan [12]. Klasifikasi umum dari beragam model klasifikasi risiko TI adalah kerahasiaan, keutuhan, dan ketersediaan yang juga merupakan pilar keamanan informasi [13][14][15]. Dengan kata lain, risiko TI memiliki korelasi yang sangat erat dengan keamanan informasi.

Manajemen risiko TI menjadi fondasi dari implementasi sistem manajemen keamanan informasi (ISO/IEC 27001, 2005) [16]. Sistem manajemen keamanan informasi merupakan bagian dari keseluruhan sistem manajemen organisasi, berdasarkan pada pendekatan risiko bisnis, untuk menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan keamanan informasi. Sistem manajemen yang dimaksud termasuk struktur organisasi, kebijakan, kegiatan perencanaan, tanggung jawab, praktik, prosedur, proses, dan sumber daya [17][18]. Satu cara untuk mengukur kinerja proses terhadap kebijakan sistem manajemen keamanan informasi adalah dengan suatu metrik penilaian tingkat kematangan proses (*maturity level*). Acuan penilaian *maturity level* dalam penelitian ini adalah Information Security Management Maturity Model (ISM3) [19].

ISO/IEC 27001 berisi persyaratan yang bersifat wajib (*mandatory*), sedangkan ISO/IEC 27002 berisi sekumpulan kontrol detail yang dapat dipilih (*optional*) dalam implementasi sistem manajemen keamanan informasi. Pemilihan kontrol tersebut harus berbasis risiko [20].

Dalam ISO/IEC Guide 73: 2002, analisis risiko didefinisikan sebagai penggunaan informasi secara sistematis untuk mengidentifikasi sumber dan memperkirakan risikonya. Analisis risiko memegang peranan penting dalam penerapan sistem manajemen keamanan informasi. Salah satu di antara banyak metode analisis risiko keamanan informasi adalah metode The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) yang dikembangkan oleh Carnegie Mellon Software Engineering Institute. Metode OCTAVE adalah sebuah kerangka penilaian dan perencanaan untuk keamanan yang memungkinkan organisasi untuk mengidentifikasi dan menganalisis risiko dan mengembangkan rencana untuk memitigasi risiko tersebut. [21] Metode OCTAVE dapat diimplementasikan menggunakan dua metode penilaian, yakni untuk organisasi/perusahaan besar (Metode OCTAVE) dan untuk organisasi/ perusahaan kecil (OCTAVE -S) [22].

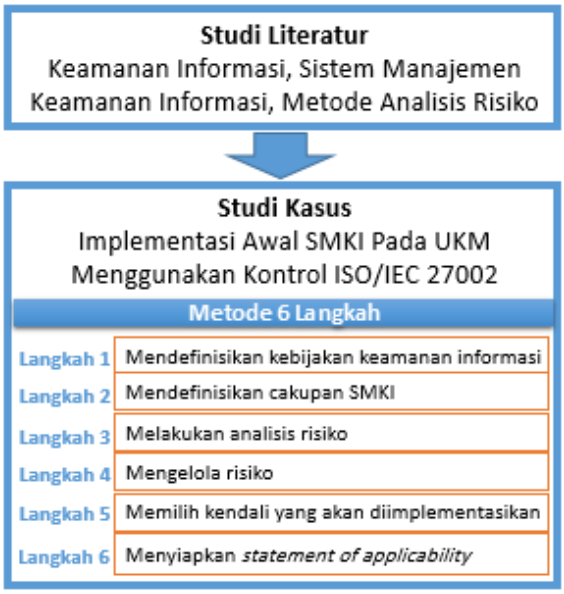
Penelitian mengenai perencanaan, perancangan, implementasi, serta evaluasi manajemen keamanan informasi di Indonesia sudah banyak dilakukan

dengan fokus pada institusi pemerintahan, BUMN, dan perbankan yang masuk dalam kategori organisasi besar. Sebagai contoh penyusunan tata kelola keamanan informasi Kantor Pelayanan Perbendaharaan Surabaya I [23], analisis risiko keamanan informasi Dishubkominfo Tulungagung [24], penilaian risiko keamanan informasi Bank XYZ Surabaya [25], serta audit keamanan sistem informasi Pemerintah Kota Yogyakarta [26]. Pada organisasi/perusahaan kecil dan menengah, telah dilakukan antara lain kajian awal praktek manajemen keamanan komputer [27], studi keamanan sistem informasi pada usaha kecil menengah menggunakan 10 domain CISSP [28], serta penyusunan Pedoman Praktis Keamanan Informasi Organisasi Skala Kecil dan Menengah yang dikeluarkan oleh Pemerintah [29]. Penelitian ini dilakukan sebagai langkah pengembangan kerangka manajemen keamanan informasi pada lingkup UKM di Indonesia dalam menghadapi persaingan global.

III. METODOLOGI

Penelitian ini dimulai dengan melakukan studi literatur. Tahap berikutnya adalah melakukan studi kasus implementasi awal sistem manajemen keamanan informasi dengan pendekatan model metode 6 langkah sebagaimana ditunjukkan pada Gambar 1.

Selanjutnya, Tabel 1 merupakan penjelasan singkat mengenai langkah, aktivitas, dan referensi dalam studi kasus penelitian ini. Analisis risiko metode OCTAVE-S dilakukan dengan langkah-langkah seperti pada Gambar 2.



Gambar 1. Metodologi penelitian

Tabel 1. Deskripsi metodologi

Langkah	Aktivitas	Referensi
1	Mendefinisikan kebijakan keamanan informasi (*define the policy*)	ISO/IEC 27001:2005
2	Mendefinisikan cakupan Sistem Manajemen Keamanan Informasi (*define scope of ISMS*)	ISO/IEC 27001:2005
3	Melakukan analisis risiko menggunakan OCTAVE – S (*undertake risk analysis*)	OCTAVE-S Method ISM3
4	Mengelola risiko (*manage risks*)	OCTAVE-S Method
5	Memilih kendali-kendali yang akan diimplementasikan (*select controls*)	ISO/IEC 27002:2005
6	Menyiapkan statement of applicability (*statement of applicability*)	ISO/IEC 27001:2005

Gambar 2. Analisis risiko OCTAVE-S

Pelaksanaan analisis risiko adalah sebagai berikut:

1) Fase 1: membuat profil ancaman berbasis aset. Fase ini merupakan evaluasi pada aspek keorganisasian. Pada fase ini, dilakukan pendefinisian Impact Evaluation Criteria yang akan digunakan untuk mengevaluasi tingkat risiko. Pada fase ini juga dilakukan proses identifikasi aset-aset kritikal organisasi dan evaluasi tingkat keamanan yang saat ini diterapkan. Aset kritikal yang dipilih sejumlah 2 (dua) sampai 5 (lima) aset. Hasil fase ini adalah pendefinisian kebutuhan keamanan informasi dan profil ancaman untuk aset-aset kritikal tersebut.

2) Fase 2: mengidentifikasi kerentanan infrastruktur. Pada fase ini dilakukan evaluasi terhadap infrastruktur TI organisasi dengan berfokus pada hal-hal yang menjadi perhatian utama para pengelola infrastruktur TI dan terkait langsung dengan aset-aset kritikal.

3) Fase 3: membuat perencanaan dan strategi keamanan. Pada fase ini dilakukan identifikasi risiko terhadap aset-aset kritikal dan diputuskan langkah-langkah yang harus dilakukan oleh organisasi.

IV. ANALISIS RISIKO DAN *MATURITY LEVEL*

Objek perusahaan berbentuk Perseroan Terbatas (PT) yang didirikan pada tahun 2003. Sasaran bisnis perusahaan ini memberikan solusi terhadap masalah terkait dengan pembangkitan listrik. Ruang lingkup bisnisnya meliputi: desain, manufaktur, *trial run*, *trouble shooting*, perbaikan, dan pelatihan operasional. Visi perusahaan adalah menjadi perusahaan yang sehat dan tangguh. Visi tersebut dicapai dengan dua strategi utama. Strategi pertama adalah menerapkan teknologi terbaru di dalam rekayasa engineering praktis. Strategi kedua adalah menyatukan kelebihan-kelebihan dari ide-ide berbagai sumber terutama ide yang orisinil. Perusahaan mempunyai 20 orang karyawan yang terdiri dari *engineer*, teknisi, bagian keuangan, personalia dan umum, administrasi, *research and development*. Selain karyawan tetap, di beberapa kesempatan ada pelajar/mahasiswa yang melakukan kerja praktik di sana.

Kebutuhan utama dari perusahaan saat ini adalah inisiasi sebuah sistem manajemen keamanan informasi yang memenuhi kebutuhan aktual serta mudah dan tepat untuk dikembangkan sesuai dengan target perusahaan di masa mendatang.

Tahap awal evaluasi menggunakan metode OCTAVE-S adalah pembentukan sebuah tim kerja. Pada studi kasus ini yang terlibat langsung dalam proses evaluasi adalah pemimpin perusahaan, staf TI, dan staf *engineering*.

A. Analisis Risiko

Pelaksanaan analisis resiko dilakukan melalui tiga fase, yaitu fase 1 membuat profil ancaman berbasis aset, fase 2 mengidentifikasi kerentanan infrastruktur, dan fase 3 membuat perencanaan dan strategi keamanan.

Pada fase 1, terdapat proses S1 mengidentifikasi informasi keorganisasian dan proses S2 membuat profil ancaman.

Pada proses S1 terlebih dahulu perlu ditentukan kriteria evaluasi dampak ancaman. Kriteria kualitatif untuk melakukan evaluasi dampak ancaman ditunjukkan pada Tabel 2. Selanjutnya mengidentifikasi aset organisasi yang dilakukan bersama dengan tim evaluasi OCTAVE-S. Tabel 3 menunjukkan aset utama perusahaan berdasarkan kategori: Informasi, Sistem Aplikasi, Perangkat Lunak, dan Layanan Pendukung, serta Sumber Daya Manusia. Langkah selanjutnya adalah mengevaluasi keberjalanan keamanan organisasi. Hasil evaluasi kualitatif atas praktek keamanan informasi dirangkum dalam Tabel 4.

Tabel 2. Kriteria evaluasi dampak

Tipe Dampak	Rendah (Low)	Sedang (Medium)	Tinggi (High)
Reputasi atau kepercayaan pelanggan	Dampak terhadap reputasi sangat rendah; hanya sedikit atau bahkan tidak ada upaya yang diperlukan untuk mengatasinya	Reputasi perusahaan terganggu; diperlukan upaya dan biaya untuk memperbaiki reputasi perusahaan	Reputasi perusahaan rusak dan tidak bisa diperbaiki
Keuangan	Terjadi penambahan biaya operasi tahunan setidaknya 2%	Terjadi penambahan biaya operasi tahunan 2-15 %	Terjadi penambahan biaya operasi tahunan lebih besar dari 15%
Produktivitas	Terjadi penambahan waktu operasi tahunan setidaknya 2%	Terjadi penambahan waktu operasi tahunan 2-15 %	Terjadi penambahan waktu operasi tahunan lebih besar dari 15%

Tabel 3. Kategori aset

Kategori	Nama Aset
Informasi	Desain produk (*soft* dan *hard*), informasi proyek, *data sheet*, data pegawai (kehadiran, kinerja, gaji)
Sistem Aplikasi	SIS (sistem informasi utama perusahaan), Sistem Informasi Absensi, *email server*
Software dan Layanan Pendukung	Linux, Windows, Microsoft Office, Open Office
SDM	• Pengguna 1: pengguna SIS, Sistem Informasi Absen, *email server* • Pengguna 2: kemampuan jaringan TI, pemrograman, setting sarana informasi yang telah ada (SIS, Sistem Informasi Absen, *email server*) • Pengguna 3: pengguna SIS, Microsoft Visio, *email server*. Sistem yang terkait yaitu SIS karena terkait pendisribusian informasi proyek • Pengguna 4: kemampuan Microsoft Excel. Sistem yang digunakan yaitu SIS, Sistem Informasi Absen, *email server*

Tabel 4. Evaluasi praktek keamanan

No	Area Praktek Keamanan	Penilaian
1	*Security Awareness and Training*	*Fair*
2	*Security Strategy*	*Fair*
3	*Security Management*	*Fair*
4	*Security Policies and Regulations*	*Poor*
5	*Collaborative Security Management*	*Poor*
6	*Contingency Planning/Disaster Recovery*	*Poor*
7	*Physical Access Control*	*Poor*
8	*Monitoring and Auditing Physical Security*	*Poor*
9	*System and Network Management*	*Fair*
10	*Monitoring and Auditing IT Security*	*Fair*
11	*Authentication and Authorization*	*Fair*
12	*Vulnerability Management*	*Poor*
13	*Encryption*	*Poor*
14	*Security Architecture and Design*	*Fair*
15	*Incident Management*	*Poor*

Keterangan:
- *Good*: Telah diimplementasikan dengan sangat baik sehingga belum memerlukan peningkatan
- *Fair*: Telah diimplementasikan tetapi masih banyak yang harus ditingkatkan
- *Poor*: Belum diimplementasikan

Tabel 5. Aset kritikal

Kategori Aset	Nama Aset Kritikal
Sistem (*system*)	SIS (sistem informasi utama perusahaan)
Informasi (*information*)	Desain produk (*soft* dan *hard*)

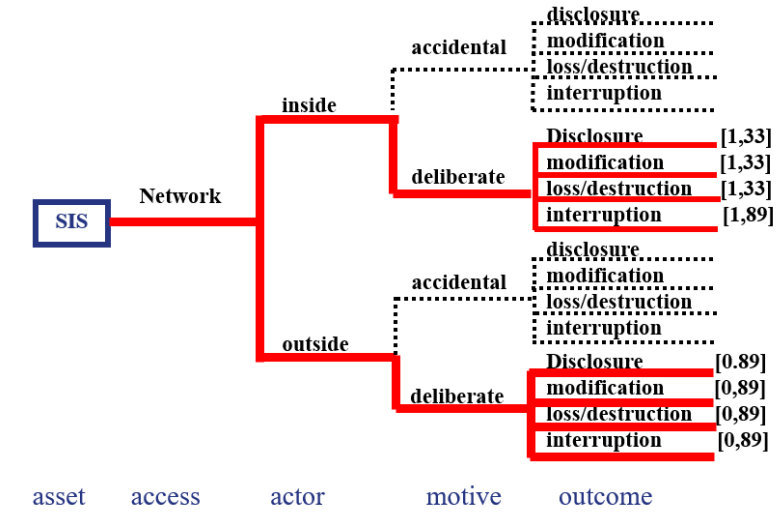
Tabel 6. Aspek keamanan terpenting pada aset kritikal

Aset Kritikal	Aspek Keamanan Terpenting
SIS	*Availability*
Desain produk (*soft* dan *hard*)	*Confidentiality*

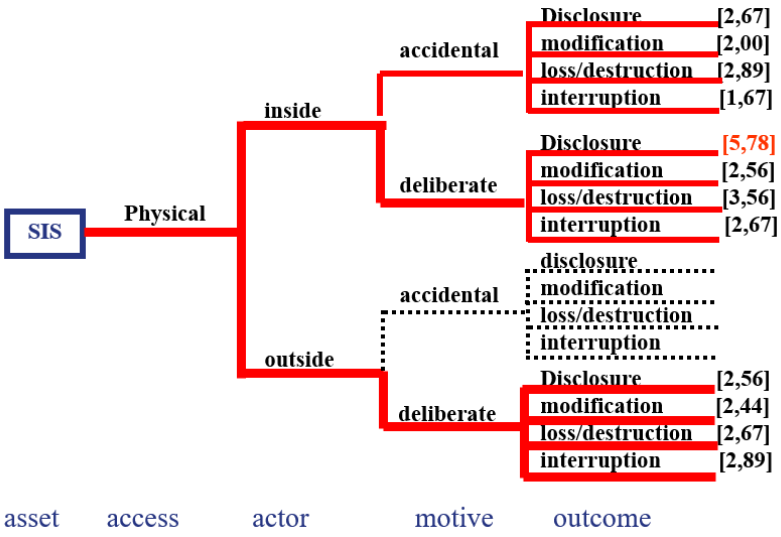
Tabel 7. Identifikasi ancaman

No	Kejadian/Potensi Ancaman	Tipe Ancaman Terkait
1	Desain produk (bersifat rahasia) diketemukan ada di perusahaan lain. Ada karyawan yang terindikasi melakukan *disclosure*.	• *Human actors using network access* • *Human actors using Physical access* • *System Problems*
2	Terjadi kerusakan perangkat LAN dan UPS akibat petir.	• *Other Problems*

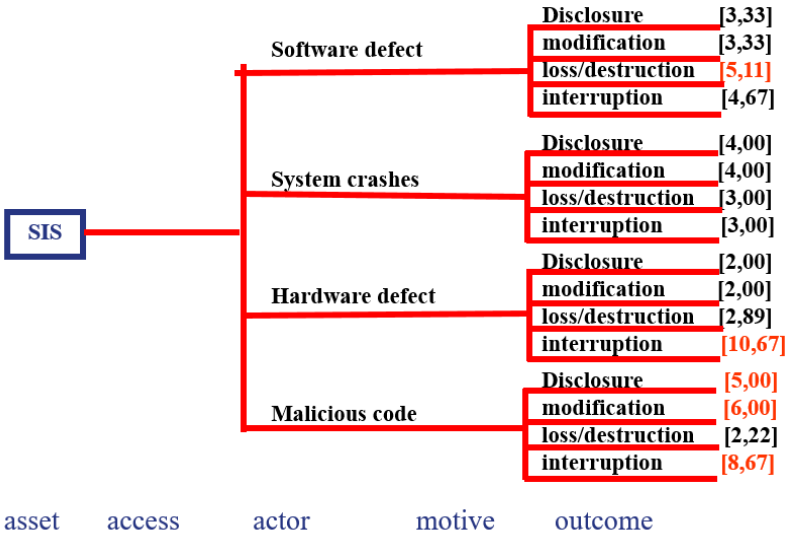
Pada proses S2, dilakukan pemilihan terhadap aset-aset terpenting. Dari analisis diperoleh bahwa perusahaan memiliki aset kritikal (*critical assets*) sebagaimana ditunjukkan pada Tabel 5. Selanjutnya mengidentifikasi kebutuhan keamanan untuk aset-aset terpenting. Tentu saja semua aset kritikal memerlukan perlindungan secara menyeluruh. Akan tetapi, ada kebutuhan keamanan yang paling menonjol pada tiap aset kritikal tersebut sebagaimana ditunjukkan pada Tabel 6. SIS sebagai sistem informasi (khususnya untuk penggunaan internal) paling memerlukan *availability*, sedangkan desain produk paling memerlukan terpenuhinya aspek *confidentiality*. Langkah berikutnya dilakukan identifikasi ancaman bagi kritikal aset dengan menggunakan empat tipe ancaman, yaitu *human actors using network access, human actors using physical access, system problems,* dan *other problems*. Hasil identifikasi ancaman dirangkum pada Tabel 7. Gambar 3, Gambar 4, Gambar 5, dan Gambar 6 berturut-turut merupakan pemetaan ancaman *human actors* melalui akses jaringan, pemetaan ancaman *human actors* melalui akses fisik, pemetaan ancaman *system problems*, dan pemetaan ancaman *other problems*, yang masing-masing disertai hasil penilaian risiko-risiko yang terkait.



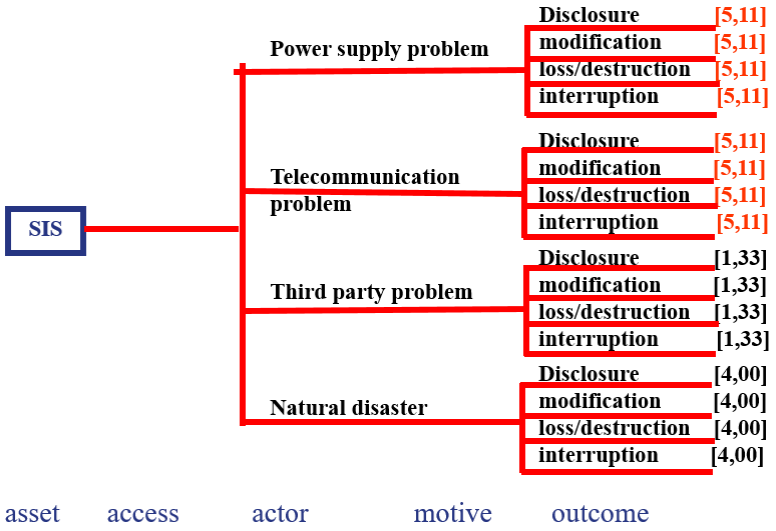
Gambar 3. ***Human actors using network access***



Gambar 4. ***Human actors using physical access***



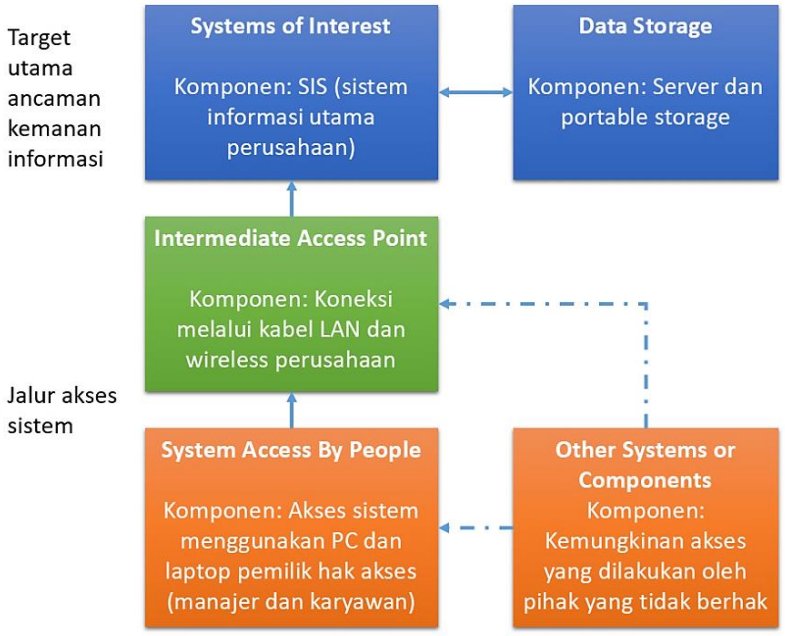
Gambar 5. ***System problems***



Gambar 6. *Other problems*

Pada fase 2, terdapat proses S3 memeriksa infrastruktur komputer yang berhubungan dengan aset-aset terpenting.

Pada proses S3, dilakukan pemeriksaan terhadap jalur akses. Hasil pemeriksaan jalur akses ke target utama ancaman keamanan informasi ditunjukkan pada Gambar 7. Langkah selanjutnya adalah menganalisis proses-proses yang terkait dengan teknologi. Proses dan aktivitas yang terkait dengan teknologi informasi dianalisis sehingga teridentifikasi perangkat yang sangat terkait dengan aset kritikal. Hasil analisis ini dirangkum pada Tabel 8.



Gambar 7. Pemeriksaan jalur akses

Tabel 8. Analisis proses yang terkait TI

No	Proses dan Aktivitas	Aset Kritikal	Perangkat Teknologi Yang Terkait
1	Proses dan aktivitas non TI (keuangan, manajemen SDM, dokumentasi proyek)	• SIS • Desain produk	• PC, Laptop
2	Proses dan aktivitas TI (operasional dan pemeliharaan: sistem aplikasi, *software*, dan layanan pendukung)	• SIS	• PC, Laptop • *Server*, perangkat jaringan

Pada fase 3, terdapat proses S4 mengidentifikasi dan menganalisis risiko, serta proses S5 membuat strategi proteksi dan rencana mitigasi.

Pada proses S4, berdasarkan analisis terhadap data-data yang diperoleh pada fase-fase sebelumnya, pada tahap ini dilakukan kuantifikasi risiko menggunakaan persamaan (1).

Risk Exposure = Probability x Impact (1)

Probability: peluang munculnya ancaman
- LOW – frekuensi ancaman kurang 1 kali dalam 5 tahun (skor 0,33)
- MEDIUM – frekuensi ancaman 1-5 kali dalam setahun (skor 0,67)
- HIGH – frekuensi ancaman lebih dari 5 kali dalam setahun (skor 1,00)

Impact: dampak ancaman
- LOW – tingkat ancaman terendah (skor 1)
- MEDIUM – tingkat ancaman sedang (skor 2)
- HIGH – tingkat ancaman tinggi (skor 3)

Tabel 9 menunjukkan risiko-risiko dengan skor terbesar pada analisis ini. Berdasarkan analisis pada kondisi aktual, diperoleh 2 (dua) macam ancaman yang memiliki tingkat dampak terbesar pada perusahaan, yakni *hardware defect* dan *malicious code*.

Tabel 9. Risiko-risiko terbesar (Skor > 4)

Tipe Ancaman	Skor Risiko	Keterangan
Human Actors Using Physical access	5,78	*Deliberate*: bocornya desain produk ke luar perusahaan.
System Problems	5,11	*Software defect*: kebanyakan merupakan konsekuensi dari *malicious code*.
System Problems	10,67	*Hardware defect*: kerusakan hardware ini membawa dampak kerugian terbesar, dari aspek: finansial, efektivitas waktu, maupun kredibilitas perusahaan.
System Problems	8,67	*Malicious code*: frekuensi gangguan *worm*, trojan, maupun virus cukup tinggi. pernah mengakibatkan sistem *down*.
Other Problems	5,11	*Power supply*: sangat berpengaruh pada efektivitas waktu.
Other Problems	5,11	*Telecommunication*: sangat berpengaruh pada efektivitas waktu.

Pada proses S5, setelah melakukan kuantifikasi risiko, perusahaan memilih salah satu dari 4 (empat) strategi utama untuk pengendalian risiko sebagai berikut:
- *Avoidance*: mengaplikasikan perangkat pengamanan untuk menghilangkan risiko yang tidak terkendali.
- *Transference*: memindahkan risiko ke area lain atau keluar dari sistem.
- *Mitigation*: mengurangi dampak yang mungkin timbul dari ancaman yang ada dengan cara mengendalikan risiko.
- *Acceptance*: memahami konsekuensi risiko dan menerima risiko tanpa adanya kendali atau mitigasi.

Dengan *risk exposure* tingkat sedang (*medium*) pada contoh kasus tersebut, perusahaan mengambil pilihan mitigasi.

B. Penilaian Maturity Level

Penilaian dilakukan menggunakan *Information Security Management Maturity Model* (ISM3). Setiap level diidentifikasi dengan beberapa kriteria yang didasarkan pada keberjalanan proses. Pada lingkup studi ini, penilaian difokuskan pada kriteria *maturity level* 1, 2, dan 3 dengan aspek penilaian mencakup: aspek umum, aspek manajemen strategis, aspek manajemen taktis, dan aspek manajemen operasional. Masing-masing aspek penilaian terdiri atas sub-sub kriteria sebagaimana dirangkum pada Tabel 10.

Dari penilaian tersebut terlihat masih terdapat kesenjangan yang cukup besar untuk mencapai *maturity level* yang diharapkan. Prioritas agenda pada tahap implementasi awal ini adalah menutup kesenjangan sehingga terpenuhi 100% kriteria pada *maturity level* 3. Kesenjangan pada aspek Taktikal dan Operasional dapat diatasi dengan penyusunan dan penerapan Kebijakan dan Prosedur Keamanan Informasi.

V. PERANCANGAN DAN IMPLEMENTASI AWAL SISTEM MANAJEMEN KEAMANAN INFORMASI

A. Penentuan Standar Acuan (Define the Policy)

Sistem manajemen keamanan informasi dirancang dan diimplementasikan dengan menggunakan ISO/IEC 27001 sebagai acuan. Implementasi awal menggunakan kontrol-kontrol dalam standar ISO/IEC 27002 sesuai dengan hasil analisis risiko yang dilakukan.

Tabel 10. Penilaian *maturity level*

Aspek Penilaian	Proses yang terpenuhi saat ini pada tiap level (%)		
	Level 1	Level 2	Level 3
Umum (*General*)			
GP-1 Document Management	50	50	50
GP-2 ISM System Audit			
Manajemen Strategis (*Strategic Management*)			
SSP-1 Report to Stakeholders	75	75	75
SSP-2 Coordination			
SSP-3 Strategic Vision			
SSP-4 Define TPSRSR Rules			
SSP-5 Check Compliance With TPSRSR			
SSP-6 Allocate Resources For Information Security			
Manajemen Taktis (*Tactical Management*)			
TSP-1 Report To Strategic Management	75	75	30
TSP-2 Manage Allocated Resources			
TSP-3 Define Security Targets			
TSP-4 Service Level Management			
TSP-5 Define Properties Groups			
TSP-6 Define Environments and Lifecycles			
TSP-7 Background Checks			
TSP-8 Security Personnel Selection			
TSP-9 Security Personnel Training			
TSP-10 Disciplinary Process			
TSP-11 Security Awareness			
TSP-12 Select Specific Processes			
Manajemen Operasional (*Operational Management*)			
OSP-1 Report to Tactical Management	80	80	40
OSP-2 Select Tools For Implementing Security Measures			
OSP-3 Inventory Management			
OSP-4 Information Systems Environment Change Control			
OSP-5 Environment Patching			
OSP-6 Environment Clearing			
OSP-7 Environment Hardening			
OSP-8 Software Development Lifecycle Control			
OSP-9 Security Measures Change Control			
OSP-10 Backup & Redundancy Management			
OSP-11 Access Control			
OSP-12 User Registration			
OSP-14 Physical Environment Protection Management			
OSP-15 Operations Continuity Management			
OSP-16 Segmentation and Filtering Management			
OSP-17 Malware Protection Management			
OSP-18 Insurance Management			
OSP-19 Attacks, Errors and Accidents Emulation (Internal Audit)			
OSP-20 Incident Emulation			
OSP-21 Information Quality Probing			
OSP-22 Alerts Monitoring			
OSP-23 Events Detection and Analysis			
OSP-24 Handling of Incidents and Near Incidents			
OSP-25 Forensics			

Tabel 11. Implementasi kontrol sistem manajemen keamanan informasi

No	Area kontrol	Implementasi kontrol
1	Kebijakan keamanan informasi (*Information Security Policy*)	Mengacu pada nomor klausul dalam ISO/IEC 27002: • *Clause 5.1.1 Information security policy document* • *Clause 5.1.2 Review of the information security policy*
2	Organisasi keamanan informasi (*Organization of Information Security*)	Belum prioritas
3	Manajemen aset (*Asset Management*)	Belum prioritas
4	Keamanan terkait Sumber Daya Manusia (*Human Resources Security*)	Mengacu pada nomor klausul dalam ISO/IEC 27002: • *Clause 8.2.2 Information security awareness, education and training* • *Clause 8.2.3 Disciplinary process*
5	Keamanan fisik dan lingkungan (*Physical and Environmental Security*)	Mengacu pada nomor klausul dalam ISO/IEC 27002: • *Clause 9.1.1 Physical security perimeter* • *Clause 9.1.2 Physical entry controls* • *Clause 9.2.2 Supporting utilities* • *Clause 9.2.3 Cabling security* • *Clause 9.2.4 Equipment maintenance*
6	Komunikasi dan manajemen operasi (*Communication and Operation Management*)	Mengacu pada nomor klausul dalam ISO/IEC 27002: • *Clause 10.4.1 Controls againts malicious code* • *Clause 10.4.2 Controls againts mobile code* • *Clause 10.5.1 Information back-up* • *Clause 10.6.1 Network controls* • *Clause 10.6.2 Security of network services* • *Clause 10.7.1 Management of removable media* • *Clause 10.7.2 Disposal of media* • *Clause 10.7.3 Information handling procedures* • *Clause 10.7.4 Security of system documentation* • *Clause 10.8.1 Information exchange policies and procedures* • *Clause 10.8.4 Electronic messaging*
7	Kontrol akses (*Access Control*)	Mengacu pada nomor klausul dalam ISO/IEC 27002: • *Clause 11.2.2 Privilege management* • *Clause 11.3.1 Password use* • *Clause 11.3.2 Unattended user equipment*
8	Akuisisi, pengembangan, dan pemeliharaan sistem informasi (*Information Systems Acquisiton, Development and Maintenance*)	Belum prioritas
9	Manajemen insiden keamanan informasi (*Information Security Incident Management*)	Mengacu pada nomor klausul dalam ISO/IEC 27002: • Clause 13.1.1 Reporting information security events
10	Manajemen keberlanjutan organisasi (*Business Continuity Management*)	Belum prioritas
11	Kepatuhan (*Compliance*)	Belum prioritas

B. Penentuan Lingkup Perancangan dan Implementasi (*Define the Scope*)

Lingkup utama penelitian ini adalah Unit Teknologi Informasi yang meliputi: kebijakan dan prosedur, topologi jaringan komputer yang diterapkan, dan lingkungan fisiknya.

1. Kebijakan dan Prosedur
   Kebijakan dan prosedur keamanan informasi belum memadai.
2. Topologi Jaringan Komputer
   Unit Teknologi Informasi menerapkan topologi jaringan komputer yang merupakan kombinasi antara jaringan kabel dan nirkabel (*wired and wireless* LAN).
3. Lingkungan Fisik
   Lingkungan fisik sangat rentan terhadap ancaman, khususnya dalam kontrol akses. Kontrol akses akan dibahas lebih lanjut pada bagian kebijakan dan prosedur.

C. Analisis Risiko

Pada penelitian ini analisis risiko metode OCTAVE-S dipilih sebagai acuan. Hasil dari analisis ini adalah perencanaan proteksi aset informasi dan rencana mitigasinya. Perencanaan proteksi dan rencana mitigasi tercakup dalam standar ISO/IEC 27001 dan kontrol-kontrol pada ISO/IEC 27002. Hasil penilaian *maturity level*

menggunakan *tools Information Security Management Maturity Models* dapat menjadi penguat hasil analisis risiko.

D. Manajemen Risiko

Proses manajemen risiko yang berkelanjutan menggunakan hasil analisis risiko Metode OCTAVE-S dan Siklus PDCA pada ISO/IEC 27001.

E. Pemilihan Kontrol

Implementasi standar ISO/IEC 27001 tergantung pada proses bisnis utama organisasi, target utama organisasi yang terkait dengan keamanan informasi, serta hasil analisis risiko. Target utama implementasi awal Sistem Manajemen Keamanan Informasi pada organisasi dengan jumlah karyawan kurang dari 200 orang adalah peningkatan kesadaran keamanan informasi pada area kontrol Keamanan Terkait Sumber Daya Manusia (*Human Resources Security*) [30]. Selain itu, beberapa area kontrol lain juga diimplementasikan dengan mengacu pada hasil analisis risiko yang telah dilakukan.

Berdasarkan hasil analisis risiko dan penilaian *maturity level*, kontrol-kontrol dari ISO/IEC 27002 yang dipilih untuk diimplementasikan dirangkum dalam Tabel 11.

F. Statement of Applicability

Berdasarkan analisis proses bisnis utama organisasi, target utama organisasi yang terkait dengan keamanan informasi, serta hasil analisis risiko, sebagian kontrol tidak dipilih untuk diimplementasikan pada tahap ini.

Implementasi awal mencakup sebagian kecil/besar area kontrol: kebijakan keamanan informasi, keamanan terkait Sumber Daya Manusia, keamanan fisik dan lingkungan, komunikasi dan manajemen operasi, kontrol akses, dan manajemen insiden keamanan informasi.

VI. KESIMPULAN

Implementasi Awal Sistem Manajemen Keamanan Informasi pada UKM Menggunakan Kontrol ISO/IEC 27002 telah dilakukan pada penelitian ini. Hasil penelitian ini adalah dalam analisis risiko menggunakan metode OCTAVE-S, ditunjukkan bahwa perusahaan memiliki risiko keamanan tingkat sedang (*medium*) dengan pilihan strategi mitigasi yang mengacu pada kontrol ISO/IEC 27002. Implementasi awal mencakup area kontrol: kebijakan keamanan informasi, keamanan terkait Sumber Daya Manusia, keamanan fisik dan lingkungan, komunikasi dan manajemen operasi, kontrol akses, dan manajemen insiden keamanan informasi. Program prioritas yang dilakukan adalah: (1) Area kontrol kebijakan keamanan informasi berupa penyusunan kebijakan dan prosedur, (2) Area kontrol keamanan terkait Sumber Daya Manusia berupa peningkatan kesadaran keamanan informasi (*security awareness*) di kalangan manajemen dan karyawan.

REFERENSI

[1] Lembaga Pengembangan Perbankan Indonesia, *Profil Bisnis Usaha Mikro, Kecil, dan Menengah (UMKM)*, Jakarta, Indonesia: Kerja Sama LPPI dan Bank Indonesia, 2015.

[2] (2017) Website Kementerian Komunikasi dan Informatika, Berita: 3,79 UMKM Sudah Go Online. Link: https://www.kominfo.go.id/content/detail/11526/kemenkop-ukm-379-juta-umkm-sudah-go-online/0/sorotan_media.

[3] *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, OECD (the Organisation for Economic Co-operation and Development), 2002.

[4] *ISO/IEC 13335-1: Information Technology - Security Techniques - Management of Information and Communications Technology Security, Part 1: Concepts and Models for Information and Communications Technology Security Management*, ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), 2004.

[5] *ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security management*, ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), 2005.

[6] M. E. Whitman and H. J. Mattord, *Management of Information Security*, 4th Ed, Boston, United States: Cengage Learning, 2004.

[7] *Internet Security Threat Report*, Vol 23, Symantec Corporation, March 2018.

[8] *Global Corporate IT Security Risks: 2013*, Karspersky Lab ZAO, May 2013.

[9] (2013) Website Kementerian Komunikasi dan Informatika, SIARAN PERS NO. 83/PIH/KOMINFO/11/2013 Ancaman Cyber Attack dan Urgensi Keamanan Informasi Nasional 2013.

[10] *COBIT 4.0/COBIT 4.1*, Information Technology Governance Institute, 2007.

[11] *Enterprise Risk: Identify, Govern and Manage IT Risk, The Risk IT Framework Exposure Draft*, Information Technology Governance Institute, 2009

[12] *IT Risk Management Report*, Vol 2, Symantec Corporation, 2008.

[13] Abram. T, "The Hidden Values of IT Risk Management", ISACA Journal Vol 2, 2009.

[14] *FIPS PUB 199*, Federal Information Processing Standards Publication—Standard for Federal

Information and Information Systems, February 2004.
[15] R. Harrison, "The 10 Most Important Things an IT Person Must Understand About Security Across the Enterprise", ISACA Journal, 2005.
[16] S. T. Arnason and K. D. Willet, *How To Achieve 27001 Certification*, Florida, United States: Auerbach Publication, 2007.
[17] *ISO/IEC 27001 Information technology — Security techniques — Information Security Management Systems*, ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), 2005.
[18] *SNI ISO/IEC 27001:2009 Teknologi Informasi - Teknik Keamanan - Sistem Manajemen Keamanan Informasi - Persyaratan*, Badan Standardisasi Nasional, 2009.
[19] *Information Security Management Maturity Model*, ISM3 Consortium, 2007.
[20] *ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO/IEC 27005:2008*, ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission).
[21] C. Alberts, et. al., "Introduction to the OCTAVE Approach", CERT Coordination Center, 2005.
[22] R. S. Germain, "Information Security Management Best Practice Based On ISO/IEC 17799", The Information Management Journal, 2005.
[23] M. Utomo, et al, "Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I", Jurnal Teknik ITS Vol 1 No 1, 2012.
[24] B. L Mahersmi, et al, "Analisis Risiko Keamanan Informasi Dengan Menggunakan Metode OCTAVE Dan Kontrol ISO 27001 Pada Dishubkominfo Kabupaten Tulungagung", Seminar Nasional Sistem Informasi Indonesia, 2016.
[25] I. Desy. et al, "Penilaian Risiko Keamanan Informasi Menggunakan Metode Failure Mode and Effects Analysis Di Divisi TI PT Bank XYZ Surabaya", Seminar Nasional Sistem Informasi Indonesia, 2014.
[26] D. Ciptaningrum, et al, "Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan COBIT 5", Seminar Nasional Teknologi Informasi dan Komunikasi, 2015.
[27] A. P. Tejoyuwono, et al. "Praktek Manajemen Keamanan Komputer", MTI Universitas Indonesia, 2005.
[28] Kahardityo, et al, "Keamanan Sistem Informasi Untuk Perusahaan Kecil dan Menengah", MTI Universitas Indonesia, 2005.
[29] *Pedoman Praktis Keamanan Informasi Organisasi Skala Kecil dan Menengah*, Departemen Komunikasi dan Informatika, 2007.
[30] R. S. Germain, "Information Security Management Best Practice Based On ISO/IEC 17799", The Information Management Journal, 2005.