TRANSFORMATIKA, Vol.18, No.1, July 2020, pp. 25 - 35
ISSN: 1693-3656,
journals.usm.ac.id/index.php/transformatika

SOP of Information System Security on Koperasi Simpan Pinjam Using ISO/IEC 27002:2013

Myra Andriana[1], Irwan Sembiring[2], Kristoko Dwi Hartomo[3]
[1]Magister Sistem Informasi, Universitas Kristen Satya Wacana Salatiga, Indonesia, e-mail: my_andriana@yahoo.com
[2]Magister Sistem Informasi, Universitas Kristen Satya Wacana Salatiga, Indonesia, e-mail: irwan@uksw.edu
[3]Magister Sistem Informasi, Universitas Kristen Satya Wacana Salatiga, Indonesia, e-mail: kristoko@gmail.com

ARTICLE INFO

Article history:

Received 27 February 2020
Received in revised form 14 April 2020
Accepted 30 April 2020
Available online 30 July 2020

ABSTRACT

Information security problems always increase every year. One way to minimize problems related to information system security is to establish an SOP. This study was conducted in koperasi simpan pinjam for several reasons that there has never been an assessment related to the level of security of the information system used, there are threatshave occured, and there do not have documented information system security procedures. The method used is OCTAVE to process the information obtained and FMEA to assess each risk that arises. Using the FMEA method, it was found that 22% of the risks invloved in koperasi simpan pinjam studied had a low categories, 59% medium categories and 19% high categories. The final result of this study is the preparation of an SOP with 8 policies and 12 information system security procedures based on the framework of ISO/IEC 27002:2013.

Keyword: SOP (Standard Operational Procedure), Information System Security, ISO/IEC 27002:2013, OCTAVE, FMEA

1. Pendahuluan

Menurut survei *Information Security Breaches Survey* (ISBS) terjadi peningkatan pelanggaran terhadap keamanan informasi setiap tahunnya, dimana pada organisasi skala kecil pelanggaran keamanan naik dari 60% pada tahun 2014 menjadi 74% pada tahun 2015 (1). Menurut laporan Symantec, tahun 2017 perusahaan skala menengah dan kecil rata-rata mendapatkan 45,2% *e-mail spam* dan 12,8% *e-mail malware* (2). Kondisi tersebut masih belum menyadarkan organisasi tentang pentingnya manajemen keamanan informasi. Kesadaran akan keamanan informasi menjadikan organisasi fokus pada ancaman atau risiko yang mungkin terjadi (3). Organisasi yang sudah menyadari pentingnya manajemen keamanan informasi mayoritas saat ini hanya memperhatikan aspek teknologinya saja, tanpa memberikan solusi komperhensif yang mencakup faktor manusia, proses, dan teknologi. Pengelola sistem informasi cenderung mengabaikan masalah pengelolaan keamanan sistem informasi (4). Organisasi seringkali mereduksi bahkan menghilangkan keamanan sistem informasi jika mengganggu *performance* dari suatu sistem informasi. Keamanan sistem informasi akan menjadi perhatian organisasi ketika ancaman sudah terjadi (5). Survei yang dilakukan oleh IBM menunjukan 92% bisnis tidak memiliki persiapan apapun jika teknologi informasi mereka mengalami kegagalan atau serangan (6).

Received February 27, 2020; Revised April 14, 2020 ; Accepted April 30, 2020

Penelitian terdahulu menunjukkan tingkat kematangan keamanan informasi organisasi baru berada pada level 2 yaitu *repeatable but intuititive* yang berarti sistem keamanan masih harus dikembangkan lagi kedalam tahapan yang lebih baik (7)(8)(9)(10). Kondisi yang sama juga terjadi pada koperasi simpan pinjam. Hasil penelitian yang dilakukan Daisihara menunjukkan tingkat kematangan keamanan informasi pada KSP berada pada level *repeatable but intuititive* (11). Supriadi mengungkapkan bahwa pada koperasi kredit masih terdapat kelemahan pengelolaan aspek keamanan sistem informasi. Kelemahan tersebut tampak pada minimnya dokumentasi prosedur keamanan sistem informasi, adanya *double job* yang tidak relevan, serta fungsi setiap bagian yang kurang optimal dalam mengelola keamanan sistem informasi (12).

Berdasarkan pada kondisi yang sudah disampaikan sebelumnya, penelitian ini dilakukan pada koperasi simpan pinjam yang ada di Kota Semarang. Koperasi yang menjadi objek penelitian memiliki kondisi dan klasifikasi usaha yang serupa. Koperasi yang digunakan termasuk kedalam klasifikasi usaha menengah, dengan jumlah karyawan antara 20 – 30 orang (13). Penelitian ini menggunakan lima koperasi simpan pinjam sebagai respondennya. Beberapa alasan menjadi dasar mengapa penelitian ini dilakukan pada kelima koperasi tersebut. Pertama, selama memanfaatkan sistem informasi belum pernah dilakukan audit atau penilaian terkait tingkat keamanan sistem informasi yang digunakan. Kedua, adanya ancaman-ancaman yang terjadi seperti virus, hilang data, *sharing password*, dan matinya koneksi internet. Ketiga belum adanya prosedur keamanan sistem informasi yang terdokumentasi. Meskipun tindakan preventif untuk mereduksi risiko keamanan sistem informasi sudah dilakukan seperti pemasangan antivirus, *maintenance hardware* secara berkala, *backup* data, dan penggunaan utilitas pendukung, tetapi belum didokumentasikan dengan baik.

Dalam membantu pengelolaan keamanan sistem informasi, alternatif yang gunakan dalam penelitian ini adalah dengan menyusun suatu SOP (Standar Operasional Prosedur) keamanan sistem informasi. SOP mampu mengurangi atau menghindari ancaman keamanan sistem informasi. R Stup mengungkapkan bahwa SOP berguna untuk menginterpretasikan seluruh konsep, teknik, dan persyaratan dalam melakukan proses bisnis yang terdokumentasi sehingga mudah digunakan oleh pegawai dalam melaksanakan proses bisnis suatu organisasi (5). Sebelumnya sudah ada beberapa penelitian yang mendesain dan mengimplementasikan SOP terkait kemanan sistem informasi, diantaranya penelitian yang dilakukan oleh Rachmawan dkk yang menyusun sebuah SOP keamanan aset informasi pada CV. Cempaka Tulung Agung yang mengacu pada kontrol kerangka kerja ISO 27002:2013 (5). Selanjutnya penelitian yang dilakukan oleh Penji Prasetya dkk yang mendesain SOP keamanan sistem informasi Fakultas Teknik Universitas Diponegoro menggunakan standar ISO 27001 (14). Penelitian yang dilakukan oleh Wicaksana dkk juga menyusun SOP manajemen akses untuk aplikasi e-performance Bina Program Kota Surabaya dengan menggunakan tiga kerangka kerja yaitu ITIL, V3, dan ISO 27002 (15). Fauzi Rokhman meneliti implementasi awal sistem manajemen keamanan informasi pada UKM dengan menggunakan kontrol ISO/IEC 27002 (16).

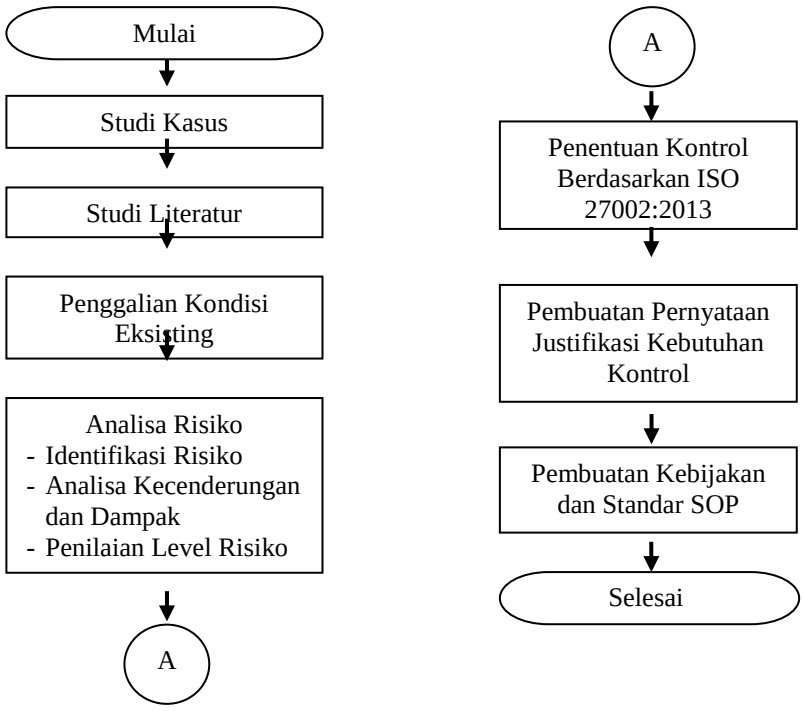
Dalam mendesain suatu SOP keamanan sistem informasi yang sesuai dengan kebutuhan organisasi, tahap awal yang perlu dilakukan adalah dengan mengidentifikasi aset yang dimiliki organisasi serta ancaman yang telah atau mungkin muncul dari setiap aset. Penelitian ini menggunakan metode OCTAVE untuk membantu mengidentifikasi risiko yang dimiliki masing-masing aset. Metode OCTAVE adalah suatu pendekatan yang dapat digunakan untuk mengidentifikasi ancaman keamanan sistem informasi secara komperhensif, terstruktur, terarah, serta dapat dilaksanakan secara independen (6). Luaran dari proses identifikasi risiko menggunakan metode OCTAVE berupa *risk register*. Seluruh risiko yang terdapat pada r*isk register* kemudian dianalisis dan dinilai untuk mengetahui tingkat prioritasnya menggunakan metode FMEA. FMEA merupakan metode yang mampu mengidentifikasi, memprioritaskan, dan mereduksi masalah kegagalan sistem (17). Hasil penilaian risiko akan menjadi dasar dalam memetakan kontrol yang mengacu pada ISO 27002:2013. Risiko dengan klasifikasi tinggi yang muncul pada aset informasi

akan mengadopsi lebih banyak kontrol dalam penyusunan SOP keamanan sistem informasi, dibandingkan risiko dengan klasifikasi rendah. Hal tersebut sesuai dengan prinsip *framework* ISO 27002:2013 yang memberikan opsi kepada pengguna untuk memilih dan mengimplementasikan kontrol-kontrol yang sesuai dengan kebutuhan organisasinya (18).

Standar Operasional Prosedur keamanan sistem informasi yang dihasilkan selain digunakan oleh koperasi simpan pinjam yang menjadi objek dalam penelitian ini, diharapkan dapat juga digunakan sebagai acuan oleh koperasi simpan pinjam lainnya yang memiliki klasifikasi dan kondisi serupa dalam mengimplementasikan prosedur keamanan sistem informasi.

2. Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah kualitatif dengan pendekatan deskriptif. Penelitian kualitatif dideskripsikan sebagai prosedur penelitian yang memiliki *output* berupa data deskriptif dalam bentuk kalimat tertulis, hasil wawancara, serta perilaku responden selama proses pengamatan. Tahapan dalam penelitian ini ditunjukan pada gambar 1 berikut:



Gambar 1. Tahapan Penelitian

Tahap pertama pada penelitian ini yaitu membahas masalah atau kasus yang akan diteliti pada koperasi simpan pinjam. Tahapan yang kedua adalah studi literatur, dimana pada tahapan ini dipelajari berbagai refrensi yang digunakan melalui buku, jurnal, dan lainnya. Tahap ketiga adalah penggalian kondisi eksisting pada koperasi simpan pinjam. Hasil pada tahapan ini digunakan sebagai dasar dilakukannya penelitian, dengan cara menghimpun berbagai data dan informasi terkait kondisi yang ada. Aktivitas yang dilakukan adalah wawancara dan observasi. Wawancara dilakukan kepada bagian yang membawahi operasional perusahaan. Sedangkan aktivitas observasi dilakukan melalui studi lapangan terhadap teknologi informai yang digunakan, aset informasi dan *resources* yang berkenaan dengan risiko dalam suatu proses bisnis.

Tahap keempat adalah analisa risiko yang terdiri dari identifikasi risiko, analisis kecenderungan dan dampak, serta penialain risiko. Pendekatan dengan metode OCTAVE digunakan untuk mengidentifikasi risiko melalui beberapa fase diantaranya menentukan aset informasi penting, kebutuhan keamanan organisasi, tindakan pengamanan yang telah dilakukan, mengklasifikasikan aset kritis, dan mengidentifikasi kelemahan infrastruktur TI yang ada. *Output* pada tahap identifikasi risiko adalah sebuah *risk register*. Setelah diperoleh *risk register*, selanjutnya dilakukan penilaian terhadap setiap risiko menggunakan metode FMEA (*Failure Modes an Effect Analysis*). Metode FMEA menilai risiko melalui tiga aspek, yaitu berdasarkan dampak yang ditimbulkan jika risiko tersebut terjadi (*severity*), kecenderungan terjadinya (*occurence*), dan deteksi yang diberikan terhadap setiap risiko (*detection*). Nilai dari ketiga aspek tersebut kemudian dikalikan yang kemudian menghasilkan nilai *Risk Priority Number* (RPN)

Tahap kelima adalah memetakan kontrol-kontrol berdasarkan *framework* ISO 27002:2013 yang akan digunakan pada koperasi simpan pinjam, dengan mengacu pada hasil penilaian risiko yang telah dilakukan di tahap sebelumnya. Tahap keenam yaitu pembuatan justifikasi kebutuhan kontrol. Pada proses justifikasi, disesuaikan dengan aktivitas praktik keamanan yang terdapat pada koperasi simpan pinjam agar dapat diterapkan dan rekomendasi pengendalian risiko yang diusulkan sesuai dengan kondisi koperasi. Selanjutnya tahap ketujuh atau tahap terakhir dari penelitian ini adalah disusunnya SOP keamanan sistem informasi. Sebelum menyusun SOP, terlebih dulu dilakukan *adjustment* antara pengendalian risiko yang direkomendasikan dengan tindakan pengamanan yang telah dilakukan oleh koperasi simpan pinjan sebagai dasar dibentuknya SOP keamanan sistem informasi pada koperasi simpan pinjam.

3. Hasil dan Pembahasan

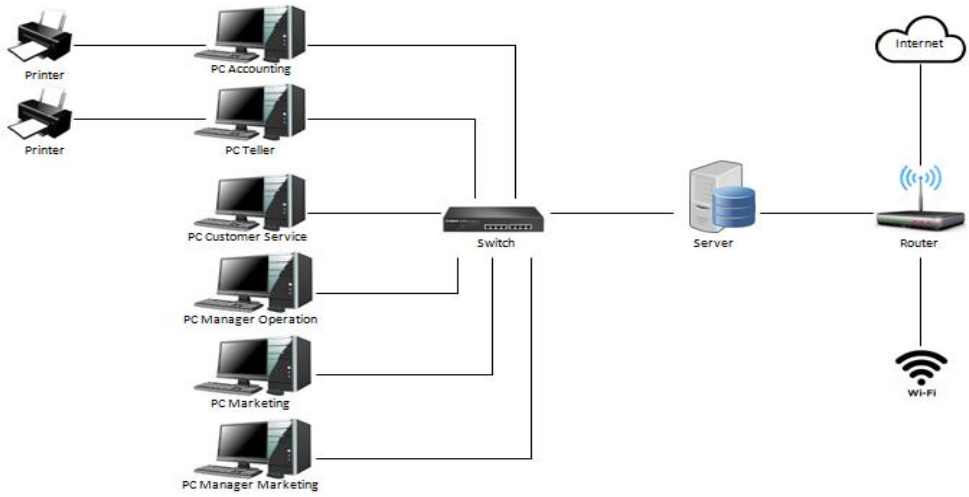
3.1. Penggalian Kondisi Eksisting

Proses penggalian kondisi yang ada saat ini dilakukan untuk mengetahui kondisi dan kebutuhan pada KSP. Tahap ini dilakukan melalui kegiatan wawancara dan observasi. Dari hasil identifikasi aset informasi yang dimiliki koperasi simpan pinjam, diperoleh lima kategori aset dengan delapan belas daftar aset. Kategori aset tersebut yaitu *hardware*, *software*, jaringan, data, dan sumber daya manusia. Sedangkan untuk daftar aset yang berhasil diidentiifikasi ditunjukan pada tabel 1.

Tabel 1. Data Aset Informasi pada Koperasi Simpan Pinjam

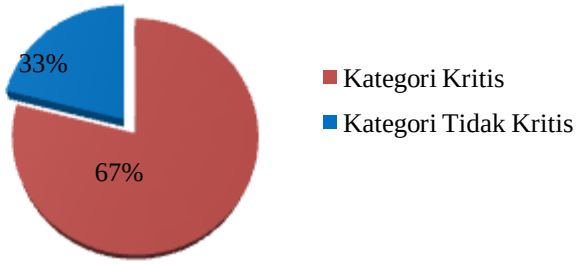
Kategori Aset	Daftar Aset
Hardware	Server, PC, Printer, Scanner, Laptop, IP telepon, LCD proyektor, dan CCTV
Software	Sistem Informasi Koperasi
Jaringan	Wifi, Router, Switch, dan Kabel
Data	Data Keuangan, Data Anggota, Data Karyawan, Data Simpanan, Data Simpanan Berjangka, Data pinjaman, Data Inventaris, dan Data Utility
Sumber Daya Manusia	Karyawan

Jika aset-aset pada koperasi simpan pinjam tersebut divisualkan dalam bentuk arsitektur jaringan, maka akan disajikan pada gambar 2 berikut.



Gambar 2. Arsitektur Jaringan pada Koperasi Simpan Pinjam

Setelah diketahui aset apa saja yang dimiliki oleh koperasi simpan pinjam, fase selanjutnya adalah melakukan identifikasi untuk menentukan aset yang sangat berperan dalam proses bisnis yang kemudian disebut sebagai aset kritis. Aset kritis merupakan aset yang bilamana terjadi kegagalan atau gangguan akan memberikan dampak yang cukup signifikan, misalnya koperasi akan mengalami kendala operasional yang mengakibatkan kerugian. Dari hasil klasifikasi aset pada koperasi simpan pinjam, 12 aset atau 67% masuk ke dalam kategori aset kritis. Sedangkan 6 aset lainnya atau 33% masuk kedalam kategori aset tidak kritis, yang ditunjukkan pada gambar 3.



Gambar 3. Klasifikasi Aset Informasi Koperasi Simpan Pinjam

Dari ke 12 aset kritis kemudian dianalisis untuk mengetahui gangguan yang pernah dan mungkin terjadi pada aset kritis sehingga berakibat pada terganggunya proses bisnis koperasi simpan pinjam. Hasil analisis menunjukan terdapat 25 ancaman yang pernah atau mungkin akan terjadi ditinjau dari aspek lingkungan, aspek manusia, dan aspek infrastruktur (*hardware*, *software*, dan jaringan).

Koperasi simpan pinjam sebenarnya telah melakukan beberapa tindakan pengamanan terhadap sistem informasinya agar terhindar dari ancaman dan kegagalan. Namun, berbagai tindakan pengamanan tersebut belum didokumentasikan. Praktek tersebut dilakukan untuk menjamin bahwa proses bisnis yang terdapat pada koperasi simpan pinjam tidak akan terganggu. Dari hasil identifikasi terdapat 22 prektek keamanan yang telah dilakukan, ditampilkan pada tabel 2.

Tabel 2. Daftar praktek Keamanan yang Telah Dilakukan

No	Praktek Keamanan Koperasi
1	Terdapat antivirus dan diupdate secara rutin
2	Patch dan firewall diupdate secara berkala

3	Tidak dapat memasang USB pada PC
4	Selain admin tidak dapat menginstal aplikasi lain
5	Terdapat CCTV yang aktif 24 jam
6	Terdapat pendingin pada ruang server untuk mengantisipasi overheat
7	Terdapat UPS dan genset untuk mengantisipasi saat aliran listrik padam
8	Backup server dilakukan setiap hari
9	Laporan di printout dandidokumentasikan
10	Input, edit, dan hapus data hanya bisa dilakaukan oleh data administrator

Berdasarkan hasil analisis kondisi yang ada saat ini pada koperasi simpan pinjam selanjutnya dilakukan pemetaan keterkaitan antara aset, kebutuhan keamanan aset, ancaman yang pernah dan mungkin terjadi, serta tindakan pengamanan yang telah dilakukan. Hal tersebut dilakukan untuk mengetahui secara mendalam bagaimana koperasi simpan pinjam selama ini mengatasi atau mengantisipasi ancaman yang pernah atau mungkin terjadi.

3.2. Identifikasi Risiko

Framework OCTAVE digunakan untuk menidentifikasi risiko yang ada pada koperasi simpan pinjam. Terdapat beberapa tahapan untuk menganalisis risiko menggunakan *framework* OCTAVE. Pertama, mengidentifikasi aset-aset informasi yang dimiliki oleh koperasi simpan pinjam. Kedua, menganalisis praktek keamanan apa saja yang diperlukan untuk setiap aset yang dimiliki oleh koperasi simpan pinjam. Ketiga, menginventarisir tindakan pengamanan apa saja yang telah dilakukan koperasi simpan pinjam untuk mengatasi ancaman dan mengantisipasi ancaman yang mungkin terjadi. Keempat adalah menganalisis risiko apa saja yang pernah dan mungkin terjadi pada koperasi simpan pinjam. Setelah melakukan berbagai tahapan dalam menganalisis risiko dengan menggunakan *framework* OCTAVE, maka diperoleh *output* dari aktivitas tersebut berupa *risk register* yang ditampilkan pada tabel 3.

Tabel 3. *Risk Register* Aset Informasi Koperasi Simpan Pinjam

Kategori Aset	Aset	Potensi Risiko	Dampak dari Risiko	Potensi Penyebab Risko
Hardware	Server	Kerusakan pada server	Kerugian secara finansial dan terhambatnya proses bisnis	Kebakaran
				Overheat
				Kerusakan bangunan
				Kesalahan konfigurasi
		Server mati	Terhambatnya proses bisnis	Tidak adanya aliran listrik
				Kerusakan pada UPS dan genset
Software	Sistem informasi koperasi	Aplikasi dapat diakses oleh pihak yang tidak berwenang	Kerugian secara finansial dan terhambatnya proses bisnis	Berbagi *username* dan *password*

3.3. Penilaian Risiko

Setelah mengidentifikasi risiko-risiko yang terdapat pada koperasi simpan pinjam dengan menggunakan *framework* OCTAVE, selanjutnya dilakukan *scoring* terhadap masing-masing risiko. Penilaian ini digunakan untuk mengklasifikasikan risiko-risiko yang ada kedalam level risiko yaitu *very low, low, medium, high, very high*. Medode FMEA digunakan dalam menilai risiko-risiko yang terdapat pada koperasi simpan pinjam. Terdapat tiga kriteria yang digunakan yaitu *severity*, *occurence*, dan *detection*. Dalam menilai risiko yang ada, ditentukan berapa nilai untuk masing-masing kriteria tersebut. Kemudian seluruh kriteria dikalkulasi untuk menentukan besarnya nilai RPN (*Risk Priority Number*) tiap risiko dengan menggunakan formula berikut:

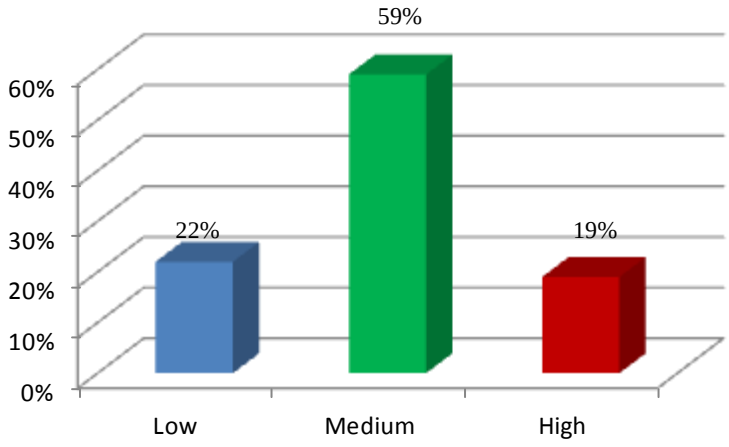
RPN (*Risk Priority Number*) = *Severity* x *Occurence* x *Detection*

Hasil perhitungan RPN (*risk priority number*) yang dihasilkan untuk masing-masing risiko yang terdapat pada *risk register* di tabel 3, kemudian dikategorikan berdasarkan skala penentuan nilai RPN yang ditunjukan pada tabel 4.

Tabel 4. Skala Penentuan Nilai RPN

Level Risiko	Skala Nilai RPN
Very High	> 200
High	< 200
Medium	< 120
Low	< 80
Very Low	< 20

Hasil *scoring* RPN menunjukan bahwa risiko yang terdapat pada koperasi simpan pinjam 22% masuk ke dalam kategori *low* dengan hasil penilaian risiko kurang dari 80. 59% risiko masuk kedalam kategori medium dengan hasil penilaian risiko kurang dari 120. 19% risiko masuk kedalam kategori *high* dengan hasil penilaian lebih dari kurang dari 200. Hasil penilaian risiko pada koperasi simpan pinjam ditunjukan pada gambar 4.



Gambar 4. Hasil Penilaian Risiko

3.4. Pemetaan Kontrol ISO 27002:2013

Pemetaan kontrol ISO 27002:2013 dilakukan terhadap setiap aset koperasi simpan pinjam yang telah diidentifikasi diawal. Penentuan kontrol tidak dibatasi pada risiko dengan klasifikasi tinggi saja, karena setiap risiko dengan klasifikasi *very low* sampai dengan *very high* berpotensi mengancam aset informasi yang dimiliki koperasi. Setiap aset memiliki fungsi dan peran yang saling berkontribusi dalam suatu proses bisnis, sehingga ketika terjadi ancaman akan menghambat proses bisnis yang terdapat pada koperasi. Diperlukan kontrol untuk mereduksi risiko-risiko yang mungkin terjadi terhadap seluruh aset informasi. Pemetaan kontrol dilakukan sesuai dengan kebutuhan, dimana semakin tinggi klasifikasi risiko maka kontrol yang dibutuhkan akan akan semakin banyak. Hasil pemetaan kontrol untuk setiap aset dituntukan pada tabel 5.

Tabel 5. Pemetan Kontrol ISO 27002:2013

Kategori Aset	Aset	Potensi Ancaman	Potensi Penyebab Ancaman	Kontrol ISO 27002:2013	Justifikasi
Hardware	*Server* PC	Kerusakan pada *hardware*	Kesalahan konfigurasi	11.2.4. *Equipment Maintenance*	Memastikan *maintenance* aset yang dimiliki. Manfaat kontrol ini adalah menjamin aset dapat digunakan selama proses bisnis.
Data	Keseluruhan data	Data hilang	Kelalaian administrator	9.3.1 *Use of Secret Aunthentication Information*	Memastikan administrator atau pengguna yang memiliki hak akses mengikuti praktek dalam menggunakan informasi penting.

3.5. Perancangan Kebijakan dan Prosedur

Sebelum melakukan penyusunan kebijakan dan prosedur keamanan sistem informasi, terlebih dahulu dilakukan pemetaan petunjuk pelaksanan yang diusulkan sesuai ISO 27002:2013 dengan pelaksanaan praktek keamanan yang telah diimplementasikan oleh koperasi simpan pinjam saat ini. Hal tersebut bertujuan untuk mengetahui kesenjangan yang terjadi. Untuk mengurangi kesenjangan yang ada, dilakukanlah standarisasi dengan membuat rekomendasi pengendalian risiko yang akan mendasari penyusuanan kebijakan dan prosedur. Kebijakan dan prosedur merupakan standar yang dijadikan acuan oleh karyawan sehingga dapat mencapai kinerja yang diharapkan. Selain itu kebijakan dan standar dapat digunakan sebagai alat evaluasi atas usaha yang telah dilaksanakan. Dalam menentukan usulan kebijakan dan prosedur keamanan sistem informasi pada koperasi simpan pinjam, didasarkan pada output rekomendasi pengendalian risiko yang telah dilakukan sebelumnya. Penentuan usulan kebijakan dan prosedur ditunjukan pada tabel 6.

Tabel 6. Pemetaan Risiko dengan Kontrol ISO 27002:2013 dan Kebijakan Prosedur Diusulkan

Potensi Risiko	Penyebab Potensial Risiko	Kontrol ISO 27002:2013	Kebijakan Prosedur yang dihasilkan
Data Hilang	Kelalaian Administrator	9.1.1 *Access Control Policy*	Kebijakan Manajemen Hak Akses
		9.2.3 *Management of Privileged Access Rights*	Prosedur Manajemen Hak Akses
		9.3.1 *Use of Secret Authentication Information*	Kebijakan Keamanan Sumber Daya Manusia
		12.4.3 *Administrtaor & Operator Log*	Kebijakan Keamanan Informasi

Dari hasil pemetaan risiko dengan kontrol ISO 27002:2013 dan kebijakan prosedur, ditentukan 8 usulan kebijakan keamanan sistem informasi koperasi simpan pinjam. Kebijakan berperan sebagai arahan dalam melakukan proses kerja berdasarkan keamanan sistem informasi ISO 27002:2013. Kebijakan yang dibuat mengacu pada risiko yang teridentifikasi dan rekomendasi pengendalian risiko yang telah diusulkan. Adapun daftar dokumen kebijakan keamanan sistem informasi ditunjukan pada tabel 7.

Tabel 7. Kebijakan Keamanan Sistem Informasi KSP

No	Kebijakan Keamanan Informasi
1	Kebijakan Manajemen Hak Akses
2	Kebijakan Keamanan Informasi
3	Kebijakan Manajemen *Password*
4	Kebijakan *Back-up* Data
5	Kebijakan Operasional Fasilitas Manajemen Informasi
6	Kebijakan Manajemen Aset
7	Kebijakan Keamanan Lingkungan
8	Kebijakan Keamanan Sumber Daya Manusia

SOP (Standar Operasional Prosedur) keamanan sistem informasi koperasi simpan pinjam yang berisi instruksi kerja dalam manajemen keamanan informasi. Pada prosedur operasional berisi instruksi-instruksi kerja dalam sistem manajemen keamanan informasi. Terdapat 12 usulan prosedur terkait keamanan sistem informasi yang ditunjukan pada tabel 8.

Tabel 8. SOP Kemanan Sistem Informasi KSP

No	Standar Operasional Prosedur
1	Prosedur Manajemen Hak Akses
2	Prosedur Manajemen Keamanan Terhadap Virus atau *Malware*
3	Prosedur Manajemen *Password*
4	Prosedur *Back-up* dan *restore*
5	Prosedur Manajemen Insiden Keamanan Informasi pada Fasilitas Informasi
6	Prosedur Instalasi Perangkat Lunak
7	Prosedur Manajemen Jaringan
8	Prosedur Pengamanan Kabel
9	Prosedur Perawatan Aset
10	Prosedur Perbaikan Aset
11	Prosedur Keamanan Lingkungan

12 Prosedur Keamanan Sumber Daya Manusia

4. Kesimpulan

Penelitian terkait penyusunan SOP (Standar Operasional Prosedur) keamanan sistem informasi pada koperasi simpan pinjam, memperoleh beberapa kesimpulan yaitu pertama, hasil analisa kritikalitas yang didasarkan pada dampak yang signifikan ketika aset mengalami ancaman atau kegagalan maka, dari 18 aset informasi yang terdapat pada koperasi simpan pinjam 12 aset masuk kedalam kategori kritis. Kedua, hasil *scoring* risiko yang telah dan mungkin terjadi menunjukan 19% risiko yang ada pada koperasi simpan pinjam berada pada level *high*, 59% risiko yang terdapat pada koperasi simpan pinjam berada pada level medium, dan 22% risiko yang terdapat pada koperasi simpan pinjam berada pada level *low*.Ketiga, hasil pemetaan kontrol yang didasarkan pada hasil penlaian risiko, maka diperoleh usulan desain SOP (Standar Operasional Prosedur) dalam bentuk 8 kebijakan dan 12 prosedur.

Referensi

1. Government H. 2015 Information Security Breaches Survey. Infosecurity. 2015;
2. Version F, Yeboah-ofori A, Islam S, Kure HI, Johnson J, Xu JJ, et al. Internet Security Threat Report: Volume 23. Procedia Comput Sci. 2018;
3. Islami DC, I.H KB, Candiwan C. Kesadaran Keamanan Informasi pada Pegawai Bank x di Bandung Indonesia. J INKOM. 2016;
4. Chazar C. Standar Manajemen Keamanan Sistem Informasi Berbasi ISO/IEC 27001:2005. J Inf. 2015;
5. Rachmawan D, Pribadi A, Tyas D. E. Pembuatan Dokumen Sop Keamanan Aset Informasi Yang Mengacu Pada Kontrol Kerangka Kerja Iso 27002:2013 (Studi Kasus : Cv Cempaka Tulungagung). J Tek ITS. 2017;
6. Chazar C, Ramdhani MA. Model Perencanaan Keamanan Sistem Informasi Menggunakan Pendekatan Metode Octave dan ISO 27001:2005. 2016;(Selisik).
7. Rosmiati, Riadi I. Analisis Keamanan Informasi Berdasarkan Kebutuhan Teknikal dan Operasional Mengkombinasikan Standar ISO 27001:2005 dengan Maturity Level (Studi Kasus Kantor Biro Teknologi Informasi PT . XYZ). 2016;6–7.
8. Kurniawan E, Riadi I. Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standard ISO/IEC 27002:2013 Menggunakan SSE-CMM. INTENSIF J Ilm Penelit dan Penerapan Teknol Sist Inf. 2018;
9. Afandi H, Darmawan A. Audit Keamanan Informasi Menggunakan ISO 27002 Pada Data Center PT. Gigipatra Multimedia. J Teknol Inf Magister Darmajaya. 2015;
10. Putra AA, Nurhayati OD, Windasari IP, Studi P, Komputer S, Teknik F, et al. Perencanaan dan Implementasi Information Security Management System Menggunakan Framework ISO / IEC. 2016;4(1):60–6.
11. Daisihara M. Evaluasi Kinerja Sistem Informasi pada KSP "Kopdit Mekar Sai" Bandarlampung Menggunakan Framework COBIT 4.1 [Internet]. Universitas Kristen Satya Wacana; 2014. Available from: http://repository.uksw.edu/handle/123456789/8808
12. Supriadi C, Darmansyah. Penerapan Audit Sistem Informasi untuk Mengevaluasi Pengendalian Umum Pengelolaan Keamanan pada Sistem Informasi Koperasi Kredit Sehati [Internet]. Universitas Esa Unggul; 2012. Available from: https://digilib.esaunggul.ac.id/penerapan-audit-sistem-informasi-untuk-mengevaluasi-pengendalian-umum-pengelolaan-keamanan-pada-sistem-informasi-koperasi-kredit-sehati-10.html
13. Undang-Undang No. 20 Tahun 2008. Tentang: Usaha,Mikro,Kecil dan Menengah. Sekr

Negara Jakarta. 2008;
14. Prasetya P, Rochim AF, Windasari IP. Desain dan Implementasi Standar Operasional Prosedur (SOP) Keamanan Sistem Informasi Fakultas Teknik Universitas Diponegoro Menggunakan Standar ISO 27001. J Teknol dan Sist Komput. 2015;
15. Wicaksana WR, Susanto TD, Herdiyanti A. Pembuatan Standar Operasional Prosedur (SOP) Manajemen Akses Untuk Aplikasi E-Performance Bina Program Kota Surabaya Berdasarkan Kerangka Kerja ITIL V3 Dan ISO 27002. Sisfo. 2016;
16. Fauzi R. Implementasi Awal Sistem Manajemen Keamanan Informasi pada UKM Menggunakan Kontrol ISO / IEC 27002. 2018;3(2):145–56.
17. Budiarto R. Manajemen Risiko Keamanan Sistem Informasi Menggunakan Metode Fmea Dan Iso 27001 Pada Organisasi Xyz. CESS (Journal Comput Eng Syst Sci. 2017;
18. ISO/IEC 27002. International Standard ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls. Iec. 2013;