56. *CSRID Journal, Vol. 10 No. 1 Februari 201, Hal. 56-67* *ISSN: 2085-1367*
https://www.doi.org/10.22303/csrid.10.1.2018.56-67 *eISSN :2460-870X*

Perancangan SMKI Berdasarkan SNI ISO/IEC27001:2013 dan SNI ISO/IEC27005:2013 (Studi Kasus DPTSI-ITS)

Designing ISMS Based on SNI ISO/IEC27001:2013 and SNI ISO/IEC27005:2013 (DPTSI-ITS)

Furqon Mauladani *[1], Daniel Oranova Siahaan [2]
[1,2] Institut Teknologi Sepuluh Nopember (ITS); Jl. Raya ITS, Sukolilo, Surabaya
[1]Departemen Manajemen Teknologi, MMT-ITS, Surabaya
[2]Departemen Sistem Informasi, FTIK-ITS, Surabaya
e-mail: *[1] furqonmauladani[at]gmail.com, [2] daniel[at]if.its.ac.id

Abstrak

Institut Teknologi Sepuluh Nopember (ITS) adalah salah satu universitas di Surabaya. ITS telah menggunakan TIK untuk keperluan operasional bisnisnya (contohnya isi kartu program studi, proses absensi, pembaharuan informasi, dan lainnya). Penggunaan TIK tidak dapat dipisahkan dari ancaman yang dapat mengganggu operasional TIK. Ancaman terdiri dari ancaman yang berasal dari luar (penyebaran malware, aktifitas social engineering), orang dalam (sengaja, tidak sengaja), kegagalan teknis (kesalahan penggunaan, kegagalan perangkat keras/lunak) ataupun bencana alam (kebakaran, gempa, banjir). Metode yang digunakan pada penelitian ini adalah melakukan manajemen resiko keamanan informasi berdasarkan SNI ISO/IEC 27005 dan perancangan dokumen SMKI berdasarkan SNI ISO/IEC 27001. Hasil penelitian ini adalah 60 resiko yang tidak diterima dari total 228 resiko yang telah teridentifikasi. Dari 60 resiko tersebut, terdapat 58 risk modification, 1 risk avoidance, dan 1 risk sharing. Tata kelola keamanan informasi yang dirancang berdasarkan SNI ISO/IEC 27001 adalah ruang lingkup SMKI, kebijakan SMKI, proses penilaian resiko, proses penanganan resiko, statement of applicability, dan sasaran keamanan informasi.

Kata kunci—Keamanan Informasi, Manajemen Resiko, SNI ISO/IEC 27001:2013, SNI ISO/IEC 27005:2013, Tata Kelola IT

Abstract

Institut Teknologi Sepuluh Nopember (ITS) is one of the university in Surabaya. ITS have already used ICT for their business operational (e.g. filling study program card activities, absence process, information update, etc.). The use of ICT can't be separated with threats that could disturb operational of ICT. The threats include external threats (e.g. malware deployment, social engineering activities), insiders (i.e. intentionally and unintentionally), technical failure (e.g. misuse, hardware/software failure) or disaster nature (e.g. fire, earthquake, flood). The used methods for this research are performed information security risk management based on SNI ISO/IEC 27005 and designed SMKI document based on SNI ISO/IEC 27001. This research found 60 unacceptable risks from total of 228 risk after identified. Out of 66 risk, there are 58 risk modification, 1 risk avoidance, 1 risk sharing. Information security governance designed based on SNI ISO/IEC 27001 are ISMS scope, ISMS policy, risk assessment process, risk treatment process, statement of applicability, and information security objective.

Keywords— *Information Security, IT Governance, Risk Management, SNI ISO/IEC 27001:2013, SNI ISO/IEC 27005:2013*

1. PENDAHULUAN

Perkembangan Teknologi Informasi dan Komunikasi (TIK) yang semakin pesat yang salah satunya disebabkan karena banyaknya manfaat yang bisa didapat dalam penggunaannya. Namun pada penggunaan TIK, terdapat ancaman yang mengganggu keamanan informasi yang bersifat merusak dan merugikan selain manfaat yang didapat. Kerusakan yang terjadi tidak hanya merubah konfigurasi sistem komputer ataupun informasi yang disimpan seperti yang biasanya dialami saat terkena *virus*, akan tetapi lebih mengarah ke pelanggaran privasi dan pencurian informasi yang berorientasi profit. Berdasarkan laporan Symantec ditahun 2015, dilaporkan bahwa terdapat 312 pelanggaran keamanan informasi yang mengakibatkan 348 juta informasi terbongkar, seperti kartu kredit, riwayat medis, data pribadi, *ID login*, dan lainnya [1]. Berdasarkan laporan Tempo ditahun 2015, Indonesia juga pernah mengalami kerugian akibat ancaman melalui internet dengan total kerugian yang bisa dihitung sekitar Rp.33,29 miliar [2].

Beberapa ancaman tersebut merupakan resiko yang memiliki efek domino yang bisa mengancam keberlangsungan aktifitas bisnis organisasi, tak terkecuali Institut Teknologi Sepuluh Nopember (ITS). Seperti organisasi lainnya, ITS juga memanfaatkan berbagai fasilitas TIK dalam menjalankan aktifitas bisnisnya. ITS memiliki instansi khusus yaitu Direktorat Pengembangan Teknologi Sistem Infromasi (DPTSI-ITS) untuk mengelola, mengordinasikan, mengendalikan, dan mengembangkan berbagai fasilitas TIK tersebut, terutama yang berhubungan dengan teknologi dan sistem informasi terpadu. Berdasarkan masalah keamanan informasi yang sudah dijelaskan, pihak DPTSI-ITS sudah seharusnya menggunakan Sistem Manajemen Keamanan Informasi (SMKI). SMKI merupakan bagian dari keseluruhan sistem manajemen organisasi untuk menetapkan, mengoperasikan, memantau, meninjau, memelihara dan meningkatkan keamanan informasi yang dibangun dengan pendekatan resiko [3]. Dalam membangun SMKI, standar SNI ISO/IEC 27001:2013 berisikan spesifikasi dan persyaratan yang harus dipenuhi [4]. Selain itu dikarenakan SMKI memerlukan pendekatan resiko, maka standar SNI ISO/IEC 27005:2013 diperlukan sebagai acuan untuk manajemen resiko keamanan informasi. SNI ISO/IEC 27005 merupakan standar yang menyediakan pedoman manajemen resiko keamanan informasi, termasuk saran penilaian resiko, penanganan resiko, penerimaan resiko, pengkomunikasian resiko, pengawasan dan peninjauan resiko [5].

Penelitian tentang perancangan SMKI berdasarkan SNI ISO/IEC 27001 telah banyak dilakukan, seperti perancangan SMKI pada Bank Nagari [4], Hashemite University [6], dan Fakultas Teknik Universitas Ibn Khaldun (UIKA) [7]. Dengan adanya rancangan SMKI, diharapkan resiko yang ada di ITS dapat dikurangi dampak yang diakibatkan maupun kemungkinan kehadirannya.

2. METODE PENELITIAN

2.1 Pengumpulan Data

1. Peninjauan Dokumen

   Peninjauan dokumen dilakukan untuk memahami kondisi keamanan informasi di organisasi melalui peninjauan dokumen pendukung berupa kebijakan, prosedur, instruksi kerja, hukum/peraturan yang berlaku, *website* organisasi, topologi jaringan, dan lainnya.
2. Wawancara

   Wawancara dilakukan untuk mengetahui kondisi dan kebutuhan keamanan informasi di organisasi melalui tanya jawab kepada narasumber yang terpercaya. Wawancara dilakukan saat aktifitas penetapan konteks sampai penilaian resiko didalam metode penelitian.
3. Observasi

   Observasi dilakukan untuk memperoleh gambaran kondisi saat ini melalui pengamatan secara langsung terhadap aktifitas bisnis, aset dan kontrol keamanan dilingkungan organisasi yang berada pada ruang lingkup SMKI.

2.2 Penetapan Konteks

1. Pengaturan Kriteria Resiko, Dampak dan Kemungkinan

   Aktifitas ini dilakukan untuk menetapkan beberapa kriteria dari resiko, dampak dan kemungkinan untuk acuan dalam proses penilaian resiko dan evaluasi resiko nantinya. Kriteria resiko merupakan definisi skala nilai level resiko yang tidak dapat diterima dan yang dapat diterima. Kriteria dampak dan kemungkinan merupakan definisi skala nilai dampak dan kemungkinan untuk setiap resiko yang akan diidentifikasi.
2. Pendefinisian Ruang Lingkup dan Batasan SMKI

   Aktifitas ini dilakukan untuk menggambarkan secara jelas ruang lingkup SMKI. Pembatasan ini dilakukan karena mengurangi kekompleksan pelaksanaan analisis kesenjangan dengan SNI ISO/IEC 27001:2013. Contohnya kontrol keamanan A.9.4.2. Prosedur *login* yang aman yang menjabarkan poin-poin keamanan informasi dalam proses *login* yang harus ada disetiap sistem dan aplikasi. Jika pembatasan tidak dilakukan, maka semua sistem dan aplikasi yang dikelola oleh DPTSI-ITS harus dianalisis kesenjangannya.
3. Penetapan Peran dan Tanggung Jawab

   Aktifitas ini dilakukan untuk menentukan siapa yang berperan dan bertanggung jawab untuk mengelola SMKI melalui penetapan tim pengelola SMKI. Susunan tim pengelola SMKI ditetapkan melalui wawancara dengan pihak manajemen serta pemetaan struktur tim pengelola SMKI yang dibutuhkan SNI ISO/IEC 27001:2013 dengan struktur organisasi yang berlaku di organisasi.

2.3 Pengusulan Kebijakan SMKI

Aktifitas ini dilakukan untuk mengusulkan kebijakan SMKI yang terdiri dari kebijakan SMKI adalah hasil wawancara dengan pihak manajemen (seperti sasaran SMKI serta hasil yang diharapkan), kriteria resiko yang sudah diatur, ruang lingkup SMKI yang sudah didefinisikan, serta peran dan tanggung jawab yang sudah ditetapkan.

2.4 Pelaksanaan Analisis Kesenjangan

Aktifitas ini dilakukan untuk mengetahui seberapa jauh tingkat kesenjangan keamananan informasi (baik sebelum maupun sesudah) pada organisasi terhadap SNI ISO/IEC 27001. Aktifitas yang dilakukan saat analisis kesenjangan adalah menentukan kesesuaian/kepatuhan organisasi terhadap setiap kontrol keamanan yang ada pada Annex A didalam SNI ISO/IEC 27001:2013 melalui aktifitas pengumpulan data. Contoh topik pertanyaan yang dapat digunakan saat analisis kesenjangan yang berasal dari kontrol keamanan pada Annex A dapat dilihat pada Tabel 1.

Tabel 1. Contoh Topik Pertanyaan Analisis Kesenjangan dari Annex A [8]

Kontrol Keamanan	Ekstraksi Pertanyaan
A.8.1.2 Kepemilikan aset	Apakah setiap aset yang dikelola pada inventaris terdapat pemiliknya?
A.13.1.1 Kontrol jaringan	Apakah jaringan dimanajemen dan dikontrol untuk melindungi informasi pada sistem dan aplikasi?

Jawaban dari setiap topik pertanyaan pada Tabel 1 bisa didapat melalui hasil wawancara, peninjauan dokumen dan/atau hasil temuan dari aktifitas observasi. Setelah itu menentukan kondisi organisasi menggunakan klasifikasi tingkat kepatuhan pada Tabel 2 terhadap setiap jawaban dari setiap topik yang didapat. Analisis kesenjangan dilakukan sebelum penilaian resiko dan setelah perencanaan penanganan resiko.

Tabel 2. Klasifikasi Tingkat Kepatuhan terhadap SNI ISO/IEC 27001 [9]

Klasifikasi	Keterangan
Compliant	Organisasi patuh secara keseluruhan dengan area tertentu pada SNI ISO/IEC 27001.
Partially compliant	Organisasi telah melakukan berbagai cara untuk patuh, namun masih memerlukan pekerjaan tambahan yang harus dijalankan.
Non-compliant	Organisasi tidak memiliki beberapa kontrol keamanan ditempat untuk memenuhi beberapa persyaratan dari SNI ISO/IEC 27001.
Not applicable	Organisasi telah ditinjau dan diidentifikasi bahwa kontrol keamanan tidak dapat diterapkan.

2.5 Penilaian Resiko

1. Identifikasi Resiko

   Identifikasi resiko dilakukan untuk mengidentifikasi semua resiko yang dihadapi oleh organisasi didalam ruang lingkup SMKI. Identifikasi resiko terdiri dari identifikasi aset, ancaman, kontrol keamanan yang ada, dan kerentanan yang saling terkait.
2. Analisis Resiko

   Analisis resiko dilakukan untuk menganalisis resiko yang telah teridentifikasi dengan memberikan nilai dampak dan kemungkinan, lalu menghitung nilai level resiko pada setiap resiko yang teridentifikasi. Penentuan nilai level resiko dapat dihitung dengan rumus sebagai berikut [6].

   Resiko = Kemungkinan x Dampak (1)
3. Evaluasi Resiko

   Evaluasi resiko dilakukan untuk membuat keputusan tindakan kedepan, seperti resiko mana yang perlu ditangani serta prioritas dari keputusan tersebut. Dalam aktifitas ini, dilakukan perbandingan level resiko pada setiap resiko dengan kriteria resiko yang sudah ditetapkan, lalu dibuat keputusan apakah resiko diterima atau tidak diterima.

2.6 Perencanaan Penanganan Resiko

Aktifitas ini dilakukan untuk memilih penanganan keseluruhan resiko berdasarkan hasil evaluasi resiko. Penanganan dapat dilakukan melalui pemilihan kontrol keamanan yang mengacu pada Annex A didalam SNI ISO/IEC 27001:2013 (*risk modification*), menghindari resiko dengan cara menghindari aktifitas atau kondisi yang dapat menimbulkan resiko (*risk avoidance*), membagi resiko dengan cara mengkontrak pihak ketiga (*risk sharing*), atau menerima resiko tanpa melakukan tindakan lebih lanjut (*risk retention*).

2.7 Perancangan Dokumen SMKI

Aktifitas ini dilakukan untuk merancang dokumen SMKI yang diperlukan berdasarkan SNI ISO/IEC 27001:2013. Dokumen SMKI yang dibuat bersumber dari beberapa aktifitas yang sudah dilakukan sebelumnya.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Penetapan Konteks

1. Pengaturan Kriteria Resiko, Dampak dan Kemungkinan

   Hasil dari pengaturan kriteria resiko yang disesuaikan dengan kebutuhan DPTSI-ITS adalah menerima resiko jika nilai level resiko 1 sampai 3 dan tidak menerima resiko jika nilai level resiko 4 sampai 9. Sedangkan hasil dari pengaturan kriteria dampak dan kemungkinan dapat dilihat pada Tabel 3 dan Tabel 4.

Tabel 3. Skala Nilai Dampak

Nilai	Kriteria Dampak
1	Gangguan layanan < = 2 hari.
2	Gangguan layanan 3 - 6 hari.
3	Gangguan layanan > = 1 minggu.

Tabel 4. Skala Nilai Kemungkinan

Nilai	Kriteria Kemungkinan
1	Kejadian dapat terjadi pada suatu waktu.
2	Telah terjadi di masa lalu, dan/atau kejadian mungkin kerap terjadi (berulang) pada suatu waktu.
3	Kejadian akan terjadi (berulang) pada sebagian besar keadaan.

2. Pendefinisian Ruang Lingkup dan Batasan SMKI

   Ruang lingkup SMKI pada penelitian ini hanya mencakup layanan *email* yang dikelola oleh DPTSI-ITS. Hal yang tidak termasuk dalam ruang lingkup seperti *server* yang dikelola oleh DPTSI-ITS yang tidak berkaitan dengan *email* ITS, misalnya *website* ITS (https://its.ac.id), Integra ITS (https://integra.its.ac.id), dan lainnya.
3. Penetapan Peran dan Tanggung Jawab

   Tim pengelola SMKI yang dibutuhkan DPTSI-ITS seperti *top management* (Rektor ITS) yang memastikan pengembangan dan kekompabilitasan kebijakan sesuai dengan sasaran strategis organisasi, *ISMS steering committee* (Direktur DPTSI-ITS) yang berperan memimpin SMKI dan menangani aset informasi di organisasi, *ISMS lead team* (setiap Kasubdit dan beberapa karyawan IT yang dipilih) yang merencanakan, menjalankan, mengkoordinasikan dan mengontrol aktifitas pada SMKI, dan *ISMS implementation team* (contohnya Direktorat SDM dan Organisasi, Subdit Infrastruktur dan Keamanan Informasi) untuk melakukan dan menerapkan semua aktifitas SMKI yang direncanakan oleh *ISMS lead team*.

3.2 Hasil Pengusulan Kebijakan SMKI

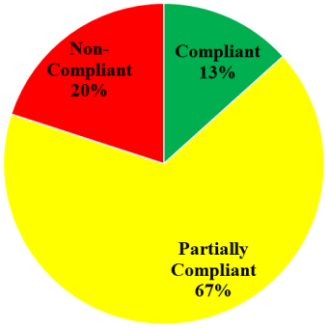
Sasaran SMKI yang ditetapkan adalah melindungi aset informasi yang dikelola oleh DPTSI-ITS dari segala resiko terkait keamanan informasi yang ada dan mendukung proses bisnis di ITS.serta hasil yang diharapkan). Sedangkan hasil yang diharapkan adalah sebagai berikut:

- Terlindunginya aspek *confidentiality*, *integrity* dan *availability* dari keseluruhan aset informasi yang dikelola oleh DPTSI-ITS.
- Meningkatkan keamanan, kepercayaan dan kenyamanan pemangku kepentingan di DPTSI-ITS.

Sedangkan untuk kriteria resiko yang sudah diatur, ruang lingkup SMKI yang sudah didefinisikan, serta peran dan tanggung jawab sudah dibahas dibagian sebelumnya.

3.3 Hasil Pelaksanaan Analisis Kesenjangan (Sebelum)

Hasil dari pelaksanaan analisis kesenjangan sebelum adalah 14 kontrol keamanan yang *compliant*, 70 kontrol keamanan yang *partially compliant*, 21 kontrol keamanan yang *non-compliant*) dan 9 kontrol keamanan yang tidak dapat diterapkan (*not applicable*). Persentasi jumlah tingkat kesenjangan sebelum dapat dilihat pada Gambar 1



Gambar 1. Persentasi Jumlah Tingkat Kesenjangan (Sebelum)

3.4 Hasil Penilaian Resiko

1. Identifikasi Resiko

   Jumlah resiko yang telah diidentifikasi didalam ruang lingkup SMKI adalah 228 resiko. Sebagian dari hasil identifikasi resiko pada penelitian ini dapat dilihat pada Tabel 5.

Tabel 5. Lembar Kerja Identifikasi Resiko

No	Aset	Ancaman	Kontrol Keamanan	Kerentanan
R1	Pusat Data	Kebakaran	• Menghubungi pihak pemadam kebakaran. • Instruksi kerja penggunaan APAR. • Prosedur pemeliharaan perlengkapan. • Prosedur pengujian kabel. • Pintu darurat kebakaran. • *Hydrant*. • Perangkat pendeteksi asap. • Perangkat pemadam otomatis. • Perangkat APAR. • *Circuit breaker*. • *Data recovery center*.	• Tidak adanya pengelolaan dan peninjauan akses ke pusat data. • Tidak adanya pemeriksan kiriman berbahaya. • Tidak ada pengecekan barang bawaan karyawan atau pengunjung.
R2	Cisco ASA Firewall	Kegagalan Perangkat jaringan	• Menghubungi vendor untuk perbaikan perangkat selama masa garansi. • Menghubungi unit pengadaan (ULP-ITS). • Menghubungi forum. • Prosedur pengawasan jaringan. • *Air conditioner*.	• Kurangnya penjadwalan dan pencatatan perawatan perangkat secara berkala. • Kurangnya cadangan komponen dan perangkat keras atau jaringan. • Temperatur perangkat saat beroperasi.

			• Perangkat lunak pengawas jaringan (Cacti). • Prosedur penanganan insiden. • *Circuit breaker*.	• Kurangnya manajemen kerentanan teknis untuk untuk menambal kerentanan yang ada baik secara prosedural maupun kebijakan.
R3	*Server*	*Denial of Service*	• Layanan keamanan *ISP* yang menyediakan *anti-DDoS*. • Menghubungi vendor *ISP* untuk memblokir *IP address* yang melakukan *DDoS*. • Menghubungi forum (misalnya pembaharuan konfigurasi dan pencarian *patch* yang benar). • Pemasangan *patch*. • Prosedur pengawasan jaringan. • Perangkat lunak pengawas jaringan (Cacti, SIEM AlienVault, ITS Web Monitoring System). • Cisco ASA Firewall. • *Data recovery center*.	• Kurangnya aturan dan prosedur manajemen perubahan. • Kurangnya rencana manajemen kapasitas yang memproyeksikan kebutuhan kapasitas kedepan. • Kurangnya manajemen kerentanan teknis. • Kurangnya aktifitas audit keamanan informasi untuk melihat kontrol apa saja yang kurang dalam penerapannya. • Kurangnya peninjauan kepatuhan teknis pada sistem untuk melihat kerentanan dan kehandalan sistem.

2. Hasil Analisis dan Evaluasi Resiko

   Berdasarkan hasil analisis dan evaluasi resiko, terhitung sejumlah 60 resiko merupakan resiko yang tidak diterima dan 168 resiko merupakan resiko yang diterima. Hasil dari analisis dan evaluasi resiko pada Tabel 5 dapat dilihat pada Tabel 6.

Tabel 6. Lembar Kerja Analisis dan Evaluasi Resiko

No	Prioritas	Resiko	Nilai Dampak	Nilai Kemungkinan	Level Resiko	Keputusan Resiko
R2	1	Kegagalan Perangkat jaringan	3	3	9	Tidak diterima
R3	2	*Denial of Service*	3	2	6	Tidak diterima
R1	3	Kebakaran	3	1	3	Diterima

3.5 Perencanaan Penanganan Resiko

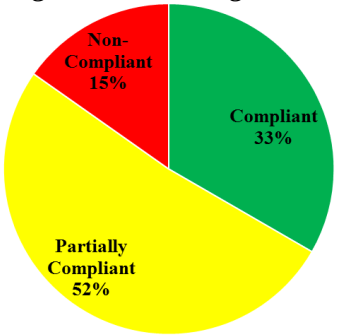
Dari 60 resiko yang tidak diterima, terdapat 58 resiko yang dilakukan *risk modification*, 1 resiko yang dilakukan *risk avoidance* dan 1 resiko yang dilakukan *risk sharing*. Hasil dari perencanaan penanganan resiko pada Tabel 6 dapat dilihat pada Tabel 7.

Tabel 7. Lembar Kerja Perencanaan Penanganan Resiko

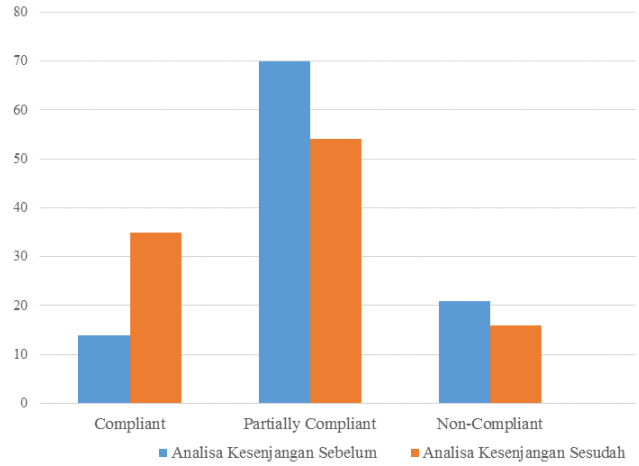
No	Penanganan	Kontrol Keamanan	Tindakan
R2	*Risk Modification*	A.8.1.1. Inventaris aset	• Pencatatan perangkat keras didalam Daftar Inventaris Aset harus menyertakan informasi yang tepat terutama jumlah perangkat cadangan, dan yang sedang digunakan berikut tanggal garansi habis untuk masing- masing perangkat agar memudahkan dalam penyiapan perangkat cadangannya.
		A.11.2.4. Pemeliharaan perlengkapan	• Melakukan perekaman setiap riwayat pemeriksaan dan perawatan yang dilakukan menggunakan *checklist* waktu, nama perangkat dan tanggal pemeriksaan/perawatan. • Merekam semua riwayat perbaikan pada perangkat yang berisikan semua kesalahan sebenarnya atau yang diperkirakan, dan semua tindakan pencegahan atau perbaikannya.
		A.17.2.1. Ketersediaan dari fasilitas pemrosesan informasi	• Mendefiniskan beberapa perangkat keras/jaringan atau komponennya yang dirasakan kritis untuk segera disediakan cadangannya dengan mempertimbangkan proses bisnis yang terlibat. • Menyiapkan cadangan perangkat ataupun komponennya jika suatu perangkat atau komponen perangkat didefinisikan kritis, sedang digunakan/beroperasional dan sudah melewati umur garansi.
R3	*Risk Sharing*	-	• Menyewa jasa pihak ketiga yang ahli dalam penanganan *denial of service*.
R1	*Risk Retention*	-	-

3.6 Hasil Pelaksanaan Analisis Kesenjangan (Sesudah)

Hasil dari pelaksanaan analisis kesenjangan sesudah adalah 35 kontrol keamanan yang *compliant*, 54 kontrol keamanan yang *partially compliant*, 16 kontrol keamanan yang *non-compliant*. Persentasi jumlah tingkat kesenjangan sesudah dapat dilihat pada Gambar 2. Selain itu perbandingan jumlah tingkat kesenjangan sebelum dengan sesudah dapat dilihat pada Gambar 3.



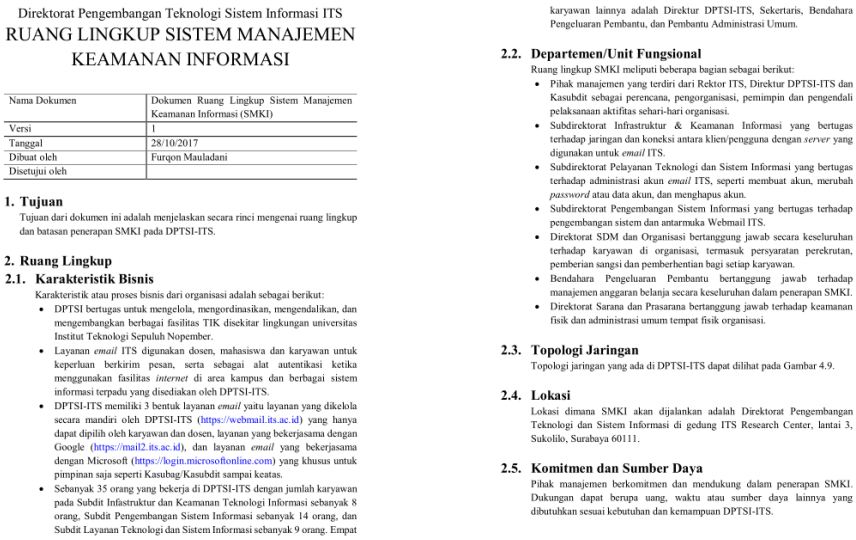
Gambar 2. Persentasi Jumlah Tingkat Kesenjangan (Sesudah)



Gambar 3. Perbandingan Persentasi Jumlah Tingkat Kesenjangan Sebelum dan Sesudah

3.7 Perancangan Dokumen SMKI

Rancangan tata kelola keamanan informasi berdasarkan SNI ISO/IEC 27001:2013 yang dibuat adalah dokumen ruang lingkup SMKI pada Gambar 4, dokumen kebijakan SMKI pada Gambar 5, dokumen proses penilaian resiko pada Gambar 6, dokumen proses penanganan resiko pada Gambar 7, dokumen *statement of applicability* pada Gambar 8, dan dokumen sasaran keamanan informasi pada Gambar 9.



Direktorat Pengembangan Teknologi Sistem Informasi ITS

RUANG LINGKUP SISTEM MANAJEMEN KEAMANAN INFORMASI

Nama Dokumen	Dokumen Ruang Lingkup Sistem Manajemen Keamanan Informasi (SMKI)
Versi	1
Tanggal	28/10/2017
Dibuat oleh	Furqon Mauladani
Disetujui oleh	

1. Tujuan

Tujuan dari dokumen ini adalah menjelaskan secara rinci mengenai ruang lingkup dan batasan penerapan SMKI pada DPTSI-ITS.

2. Ruang Lingkup

2.1. Karakteristik Bisnis

Karakteristik atau proses bisnis dari organisasi adalah sebagai berikut:

- DPTSI bertugas untuk mengelola, mengordinasikan, mengendalikan, dan mengembangkan berbagai fasilitas TIK disekitar lingkungan universitas Institut Teknologi Sepuluh Nopember.
- Layanan *email* ITS digunakan dosen, mahasiswa dan karyawan untuk keperluan berkirim pesan, serta sebagai alat autentikasi ketika menggunakan fasilitas *internet* di area kampus dan berbagai sistem informasi terpadu yang disediakan oleh DPTSI-ITS.
- DPTSI-ITS memiliki 3 bentuk layanan *email* yaitu layanan yang dikelola secara mandiri oleh DPTSI-ITS (https://webmail.its.ac.id) yang hanya dapat dipilih oleh karyawan dan dosen, layanan yang bekerjasama dengan Google (https://mail2.its.ac.id), dan layanan *email* yang bekerjasama dengan Microsoft (https://login.microsoftonline.com) yang khusus untuk pimpinan saja seperti Kasubag/Kasubdit sampai keatas.
- Sebanyak 35 orang yang bekerja di DPTSI-ITS dengan jumlah karyawan pada Subdit Infastruktur dan Keamanan Teknologi Informasi sebanyak 8 orang, Subdit Pengembangan Sistem Informasi sebanyak 14 orang, dan Subdit Layanan Teknologi dan Sistem Informasi sebanyak 9 orang. Empat karyawan lainnya adalah Direktur DPTSI-ITS, Sekertaris, Bendahara Pengeluaran Pembantu, dan Pembantu Administrasi Umum.

2.2. Departemen/Unit Fungsional

Ruang lingkup SMKI meliputi beberapa bagian sebagai berikut:

- Pihak manajemen yang terdiri dari Rektor ITS, Direktur DPTSI-ITS dan Kasubdit sebagai perencana, pengorganisasi, pemimpin dan pengendali pelaksanaan aktifitas sehari-hari organisasi.
- Subdirektorat Infrastruktur & Keamanan Informasi yang bertugas terhadap jaringan dan koneksi antara klien/pengguna dengan *server* yang digunakan untuk *email* ITS.
- Subdirektorat Pelayanan Teknologi dan Sistem Informasi yang bertugas terhadap administrasi akun *email* ITS, seperti membuat akun, merubah *password* atau data akun, dan menghapus akun.
- Subdirektorat Pengembangan Sistem Informasi yang bertugas terhadap pengembangan sistem dan antarmuka Webmail ITS.
- Direktorat SDM dan Organisasi bertanggung jawab secara keseluruhan terhadap karyawan di organisasi, termasuk persyaratan perekrutan, pemberian sangsi dan pemberhentian bagi setiap karyawan.
- Bendahara Pengeluaran Pembantu bertanggung jawab terhadap manajemen anggaran belanja secara keseluruhan dalam penerapan SMKI.
- Direktorat Sarana dan Prasarana bertanggung jawab terhadap keamanan fisik dan administrasi umum tempat fisik organisasi.

2.3. Topologi Jaringan

Topologi jaringan yang ada di DPTSI-ITS dapat dilihat pada Gambar 4.9.

2.4. Lokasi

Lokasi dimana SMKI akan dijalankan adalah Direktorat Pengembangan Teknologi dan Sistem Informasi di gedung ITS Research Center, lantai 3, Sukolilo, Surabaya 60111.

2.5. Komitmen dan Sumber Daya

Pihak manajemen berkomitmen dan mendukung dalam penerapan SMKI. Dukungan dapat berupa uang, waktu atau sumber daya lainnya yang dibutuhkan sesuai kebutuhan dan kemampuan DPTSI-ITS.

Gambar 4. Ruang Lingkup SMKI

Direktorat Pengembangan Teknologi Sistem Informasi ITS

KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI

Nama Dokumen:	Dokumen Kebijakan Sistem Manajemen Keamanan Informasi (SMKI)
Versi	1
Tanggal	28/10/2017
Dibuat oleh	Furqon Mauladani
Disetujui oleh	

1. Pendahuluan

Tujuan dari dokumen ini adalah menunjang tujuan bisnis dengan memastikan *confidentiality*, *integrity*, dan *availability* dari setiap aset informasi yang penting bagi DPTSI-ITS.

2. Ruang Lingkup

Kebijakan SMKI melingkupi layanan TIK yang terkait, termasuk (dan tidak terbatas pada) beberapa departemen/unit dan layanan sebagai berikut:

- Subdirektorat Infrastruktur & Keamanan Informasi.
- Subdirektorat Pelayanan Teknologi dan Sistem Informasi.
- Subdirektorat Pengembangan Sistem Informasi.
- Ruang pusat data.
- Webmail ITS.
- Perangkat keras/lunak/jaringan, data, karyawan dan vendor yang berkaitan dengan Webmail ITS.

3. Sasaran

Sasaran yang harus dicapai dalam SMKI adalah sebagai berikut:

1. Sasaran dari penerapan SMKI adalah melindungi aset informasi yang dikelola oleh DPTSI-ITS dari segala resiko terkait keamanan informasi yang ada dan mendukung proses bisnis di ITS.
2. Menyediakan pelatihan yang diperlukan kepada karyawan, dosen dan mahasiswa untuk memastikan keamanan informasi.
3. Melakukan penilaian dan penanganan resiko untuk menunjang proses SMKI.
4. Melakukan audit internal dan tinjauan pihak manajemen untuk memastikan penerapan dan kesesuaian SMKI.

4. Hasil yang Diharapkan

Hasil yang diharapkan dari penerapan SMKI adalah sebagai berikut:

- Terlindunginya aspek *confidentiality*, *integrity* dan *availability* dari keseluruhan aset informasi yang dikelola oleh DPTSI-ITS
- Meningkatkan keamanan, kepercayaan dan kenyamanan pemangku kepentingan di DPTSI-ITS.

5. Peran dan Tanggung Jawab

Peran dan tanggung jawab pada SMKI adalah sebagai berikut:

1. Pimpinan bertanggung jawab dalam memastikan tersedianya sumber daya yang dibutuhkan SMKI, serta kesesuaian kebijakan dan sasaran keamanan informasi dengan arah strategis organisasi. Selain itu bertugas mengkomunikasikan pentingnya kepatuhan dan mendukung kontribusi setiap pemangku kepentingan terhadap SMKI.
2. Komite pengendali SMKI bertanggung jawab untuk memastikan dan meninjau kesesuaian penerapan dan peningkatan SMKI. Selain itu bertugas menyediakan arahan yang jelas pada strategi SMKI organisasi dalam mengelola keamanan informasi dan mendukung pimpinan untuk mencapai sasaran strategis organisasi.
3. Tim pemimpin SMKI bertanggung jawab dalam merencanakan, mengerakkan, dan mengatur aktifitas yang berkaitan dengan SMKI. Selain itu bertugas mengelola resiko dan beberapa dokumen terkait SMKI.
4. Tim penerapan SMKI bertanggung jawab untuk melakukan dan menerapkan semua aktifitas SMKI yang direncanakan oleh tim pemimpin SMKI.
5. Perlindungan terhadap *confidentiality*, *integrity* dan *availability* dari setiap aset informasi merupakan tanggung jawab dari pemilik ataupun pengguna pada masing-masing aset.

6. Kebijakan/Dokumen Terkait

Kebijakan atau dokumen yang terkait dengan dokumen ini adalah sebagai berikut:

1. Dokumen [Ruang Lingkup SMKI] dapat dilihat pada Lampiran G.
2. Susunan tim pengelola SMKI dapat dilihat pada Gambar 4.10.
3. Kriteria resiko dapat dilihat pada Tabel 4.1.

Gambar 5. Kebijakan SMKI

Direktorat Pengembangan Teknologi Sistem Informasi ITS

PROSES PENILAIAN RESIKO

Nama Dokumen:	Laporan Proses Penilaian Risiko
Versi	1
Tanggal	28/10/2017
Dibuat oleh	Furqon Mauladani
Disetujui oleh	

1. Pendahuluan

Tujuan dari dokumen ini adalah mendefinisikan metodologi untuk penilaian resiko keamanan informasi, seperti identifikasi resiko, analisis resiko dan evaluasi resiko berdasarkan dokumen standar SNI ISO/IEC 27005:2013 dan SNI ISO/IEC 27001:2013. Dokumen ini juga melaporkan hasil dari proses penilaian resiko.

2. Tahapan Penilaian Risiko

Beberapa tahapan dalam penilaian resiko adalah sebagai berikut:

1. Identifikasi aset yang kritis yang berfungsi sebagai pengolah, pengirim maupun media/penyimpanan informasi, ancaman yang mengganggu aspek keamanan informasi seperti *confidentiality*, *integrity* dan *availability* terhadap aset tersebut, kontrol keamanan pada ketiga area seperti *administrative*, *physical*, dan *technical* yang melindungi aset dari ancaman, dan kerentanan pada keamanan informasi yang dapat diekploitasi oleh ancaman.
2. Pemilik resiko harus memberikan penilaian dampak dari ancaman yang ada berdasarkan Tabel I.1.

Tabel I.1 Skala Nilai Dampak

Nilai		Kriteria Dampak
1	*Low*	Gangguan layanan < = 2 hari.
2	*Medium*	Gangguan layanan 3 - 6 hari.
3	*High*	Gangguan layanan > = 1 minggu.

3. Pemilik resiko harus memberikan penilaian kemungkinan dari ancaman yang ada berdasarkan Tabel I.2.

Tabel I.2 Skala Nilai Kemungkinan

Nilai		Kriteria Kemungkinan
1	*Unlikely*	Kejadian bisa terjadi (berulang) pada suatu waktu.
2	*Possible*	• Telah terjadi di masa lalu. • Kejadian mungkin kerap terjadi (berulang) pada suatu waktu.
3	*Likely*	Kejadian akan terjadi (berulang) pada sebagian besar keadaan.

4. Hitung level resiko dengan menggunakan metode perkalian antara nilai dampak dan kemungkinan.
5. Petakan keseluruhan hasil sebelumnya yang saling berhubungan kedalam lembar kerja penilaian resiko.
6. Evaluasi resiko dengan membandingkan level resiko pada lembar kerja penilaian resiko dengan kriteria resiko dari dokumen [Kebijakan SMKI].
7. Untuk resiko yang memiliki level resiko yang berada diatas skala nilai resiko yang bisa diterima artinya resiko akan ditangani nantinya dan untuk resiko yang level resikonya sama dengan atau dibawah skala nilai resiko yang bisa diterima artinya resiko dapat dibiarkan dan diterima.
8. Urutkan setiap resiko berdasarkan level resikonya.

3. Komunikasi dan Konsultasi

Laporan [Proses Penilaian Resiko] harus didokumentasikan dan dilaporkan ke pemangku kepentingan yang tepat, serta dijaga oleh tim pemimpin SMKI selaku yang bertanggung jawab dalam pengelolaan dokumen terkait SMKI.

4. Pengawasan dan Peninjauan

Pimpinan bersama dengan komite pengendali SMKI harus melakukan peninjauan terhadap resiko yang ada saat ini dan memperbarui dokumen [Proses Penilaian Resiko] dengan cara penambahan resiko baru, ataupun pembaharuan nilai resiko yang ada pada aspek nilai dampak dan kemungkinannya. Hal ini dikarenakan resiko yang bisa muncul baru dan berubah-ubah sepanjang waktu. Peninjauan dapat dilakukan setahun sekali, atau bisa saja lebih bila terjadi perubahan signifikan pada organisasi, teknologi, tujuan bisnis atau lingkungan bisnis.

5. Laporan Proses Penilaian Resiko

Hasil dari proses penilaian resiko dapat dilihat pada halaman dibawah ini.

Gambar 6. Proses Penilaian Resiko

Direktorat Pengembangan Teknologi Sistem Informasi ITS

PROSES PENANGANAN RESIKO

Nama Dokumen:	Laporan Proses Penanganan Risiko
Versi	1
Tanggal	28/10/2017
Dibuat oleh	Furqon Mauladani
Disetujui oleh	

1. Pendahuluan

Tujuan dari dokumen ini adalah mendefinisikan metodologi untuk penanganan resiko keamanan informasi dan menetapkan kontrol keamanan berdasarkan dokumen standar SNI ISO/IEC 27001:2013. Dokumen ini juga melaporkan hasil dari proses penanganan resiko.

2. Tahapan Penanganan Resiko

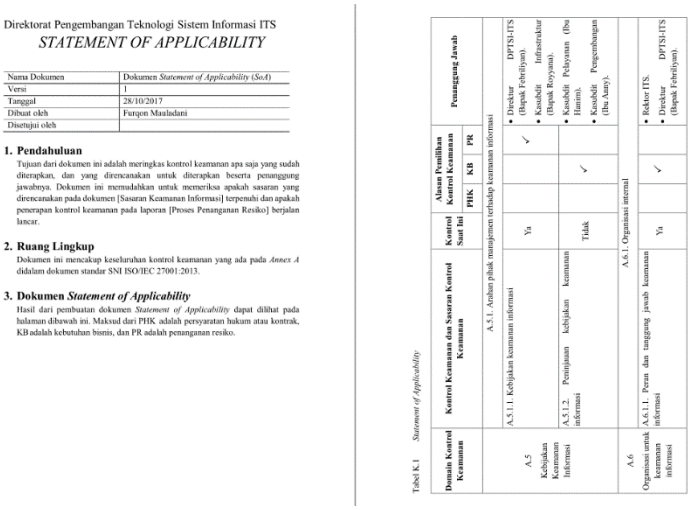
Beberapa tahapan dalam penanganan resiko adalah sebagai berikut:

1. Dapatkan hasil dari laporan [Proses Penilaian Resiko].
2. Pilih resiko yang tidak diterima oleh DPTSI-ITS.
3. Pemilihan penanganan resiko dengan kontrol-kontrol keamanan pada *Annex A* didalam dokumen standar SNI ISO/IEC 27001:2013 yang sesuai dengan sasaran kontrol keamanan dan deskripsi kontrol keamanan tersebut, atau merencanakan aktifitas menghindari resiko, membagi resiko atau menerima resiko.
4. Berdasarkan kontrol keamanan yang dipilih, selanjutnya dilakukan pemilihan apakah beberapa kontrol keamanan yang ada dapat diterapkan atau tidak. Contoh rincian dari penerapan kontrol keamanan terkait dapat dilihat pada dokumen standar SNI ISO/IEC 27002:2013 pada nomor atau kontrol keamanan yang sama. Rincian penerapan kontrol keamanan tidak diharuskan dari dokumen standar SNI ISO/IEC 27002:2013, namun bisa menggunakan standar lain atau praktek terbaik lainnya asal penanganan resiko sesuai dengan sasaran kontrol keamanan dan deskripsi kontrol keamanan tersebut.
5. Bila kontrol keamanan tersebut dapat diterapkan dan disetujui, maka pilih siapa yang akan bertanggung jawab dalam pelaksanaan kontrol keamanan tersebut.
6. Bila pemilihan kontrol keamanan pada sasaran kontrol keamanan sudah selesai, selanjutnya rancang [*Statement of Applicability*] yang berisi keseluruhan kontrol keamanan pada dokumen standar SNI ISO/IEC 27001:2013 dengan informasi tambahan seperti:

Tabel I.1 Pemilihan Penanganan Resiko

No Resiko	Resiko	Pemilihan Penanganan
IK39, IK45, IK51, IK57, IK76	Kegagalan perangkat jaringan	*Risk Modification*
	• A.5.1.1. Kebijakan keamanan informasi.	
	• A.8.1.1. Inventaris aset.	
	• A.8.1.2. Kepemilikan aset.	
	• A.11.2.4. Pemeliharaan perlengkapan.	
	• A.12.1.1. Mendokumentasikan prosedur operasional.	
	• A.12.1.2. Manajemen perubahan.	
	• A.17.2.1. Ketersediaan dari fasilitas pemrosesan informasi.	
IK46, IK52, IK58, IK77	Kesalahan konfigurasi	*Risk Modification*
	• A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi.	
	• A.8.1.4. Pengembalian aset.	
D10, PT33	Terkena aktifitas *social engineering*	*Risk Modification*
	• A.5.1.1. Kebijakan keamanan informasi.	

Gambar 7. Proses Penanganan Resiko



Direktorat Pengembangan Teknologi Sistem Informasi ITS
STATEMENT OF APPLICABILITY

Nama Dokumen	Dokumen *Statement of Applicability (SoA)*
Versi	1
Tanggal	28/10/2017
Dibuat oleh	Furqon Mauladani
Disetujui oleh	

1. Pendahuluan

Tujuan dari dokumen ini adalah meringkas kontrol keamanan apa saja yang sudah diterapkan, dan yang direncanakan untuk diterapkan beserta penanggung jawabnya. Dokumen ini memudahkan untuk memeriksa apakah sasaran yang direncanakan pada dokumen [Sasaran Keamanan Informasi] terpenuhi dan apakah penerapan kontrol keamanan pada laporan [Proses Penanganan Resiko] berjalan lancar.

2. Ruang Lingkup

Dokumen ini mencakup keseluruhan kontrol keamanan yang ada pada *Annex A* didalam dokumen standar SNI ISO/IEC 27001:2013.

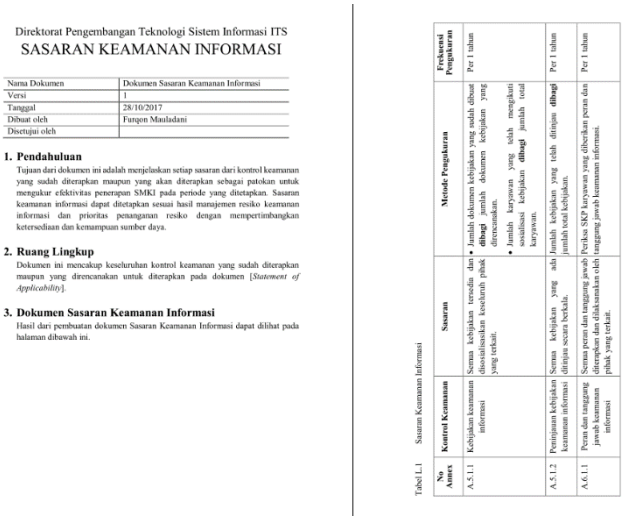
3. Dokumen *Statement of Applicability*

Hasil dari pembuatan dokumen *Statement of Applicability* dapat dilihat pada halaman dibawah ini. Maksud dari PHK adalah persyaratan hukum atau kontrak, KB adalah kebutuhan bisnis, dan PR adalah penanganan resiko.

Tabel K.1 *Statement of Applicability*

Domain Kontrol Keamanan		Kontrol Keamanan dan Sasaran Kontrol Keamanan	Kontrol Saat Ini	Alasan Pemilihan Kontrol Keamanan			Penanggung Jawab
				PHK	KB	PR	
		A.5.1. Arahan pihak manajemen terhadap keamanan informasi					
A.5 Kebijakan Keamanan Informasi	A.5.1.1	Kebijakan keamanan informasi	Ya			✓	• Direktur DPTSI-ITS (Dapat Fehriyani). • Kasubdit Infrastruktur (Dapat Royyana).
	A.5.1.2	Peninjauan kebijakan keamanan informasi	Tidak		✓		• Kasubdit Pelayanan (Ibu Hanim). • Kasubdit Pengembangan (Ibu Amy).
		A.6.1. Organisasi internal					
A.6 Organisasi untuk keamanan informasi	A.6.1.1	Peran dan tanggung jawab keamanan informasi	Ya		✓		• Rektor ITS • Direktur DPTSI-ITS (Dapat Fehriyani).

Gambar 8. *Statement of Applicability*



Direktorat Pengembangan Teknologi Sistem Informasi ITS
SASARAN KEAMANAN INFORMASI

Nama Dokumen	Dokumen Sasaran Keamanan Informasi
Versi	1
Tanggal	28/10/2017
Dibuat oleh	Furqon Mauladani
Disetujui oleh	

1. Pendahuluan

Tujuan dari dokumen ini adalah menjelaskan setiap sasaran dari kontrol keamanan yang sudah diterapkan maupun yang akan diterapkan sebagai patokan untuk mengukur efektivitas penerapan SMKI pada periode yang ditetapkan. Sasaran keamanan informasi dapat ditetapkan sesuai hasil manajemen resiko keamanan informasi dan prioritas penanganan resiko dengan mempertimbangkan ketersediaan dan kemampuan sumber daya.

2. Ruang Lingkup

Dokumen ini mencakup keseluruhan kontrol keamanan yang sudah diterapkan maupun yang direncanakan untuk diterapkan pada dokumen [*Statement of Applicability*].

3. Dokumen Sasaran Keamanan Informasi

Hasil dari pembuatan dokumen Sasaran Keamanan Informasi dapat dilihat pada halaman dibawah ini.

Tabel L.1 Sasaran Keamanan Informasi

No Annex	Kontrol Keamanan	Sasaran	Metode Pengukuran	Periode Pengukuran
A.5.1.1	Kebijakan keamanan informasi	Semua kebijakan tersedia dan disetujui/sesuai kesetiaan pihak yang terkait.	• Jumlah dokumen kebijakan yang sudah dibuat **dibagi** jumlah dokumen kebijakan yang direncanakan. • Jumlah karyawan yang telah mengikuti sosialisasi kebijakan **dibagi** jumlah total karyawan.	Per 1 tahun
A.5.1.2	Peninjauan kebijakan keamanan informasi	Semua kebijakan yang ada dilakukan secara berkala.	Jumlah kebijakan yang telah ditinjau **dibagi** jumlah total kebijakan.	Per 1 tahun
A.6.1.1	Peran dan tanggung jawab keamanan informasi	Semua peran dan tanggung jawab diterapkan dan dilaksanakan oleh pihak yang terkait.	Periksa SKP karyawan yang diberikan peran dan tanggung jawab keamanan informasi.	Per 1 tahun

Gambar 9. Sasaran Keamanan Informasi

4. KESIMPULAN

Berikut ini adalah beberapa kesimpulan yang diberikan untuk penelitian tentang perancangan SMKI ini:

1. Jumlah resiko di DPTSI-ITS yang berhasil diidentifikasi adalah 228, dimana sebesar 168 resiko merupakan resiko yang diterima dan 60 resiko merupakan resiko yang tidak diterima.
2. Dari 60 resiko yang tidak diterima, terdapat 58 resiko yang dilakukan *risk modification*, 1 resiko yang dilakukan *risk avoidance*, dan 1 resiko yang dilakukan *risk sharing*.
3. Berdasarkan 60 resiko yang tidak diterima sebelum dilakukan perencanaan penanganan resiko, hasil analisis kesenjangan sebelum yang didapatkan adalah 14 kontrol keamanan *compliant*, 70 kontrol keamanan yang *partially compliant*, 21 kontrol keamanan yang *non-compliant*. Setelah resiko yang tidak diterima dilakukan perencanaan penanganan resiko, hasil analisis kesenjangan sesudah yang didapatkan adalah 35 kontrol keamanan yang *compliant*, 54 kontrol keamanan yang *partially compliant*, 16 kontrol keamanan yang *non-compliant*.

4. Berdasarkan perbandingan dari hasil analisis kesenjangan sebelum dengan hasil analisis kesenjangan sesudah, ditemukan sebesar 13% penambahan pada kontrol keamanan yang *compliant*, 6% pengurangan pada kontrol keamanan yang *partially compliant* dan 7% pengurangan pada kontrol keamanan yang *non-compliant*.

5. SARAN

Berikut ini adalah beberapa saran yang diberikan untuk penelitian tentang perancangan SMKI ini:

1. DPTSI-ITS dapat memperluas area ruang lingkup SMKI untuk perlindungan yang lebih luas dan lengkap.
2. DPTSI-ITS disarankan melakukan proses manajemen resiko keamanan informasi secara berkala maupun ketika terjadinya perubahan fungsional besar-besaran pada organisasi agar resiko yang ada dapat ditangani dan diantisipasi secara tepat dan cepat.

DAFTAR PUSTAKA

[1] Symantec, 2015, *Internet Security Threat Report Vol.20*, Symantec, Mountain View.

[2] Tempo, 2015, Cyber Crime Costs Indonesia More than Rp33 M, Tempo, http://en.tempo.co/read/news/2015/08/26/240695173/cyber-crime-costs-indonesia-more-than-rp33-m, diakses tgl 03/11/15.

[3] Kementrian Komunikasi dan Informatika Indonesia, 2011, *Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik*, Edisi ke-2, KEMENKOMINFO, Jakarta.

[4] Putra, A.A., Oky D.N., dan Ike P.W., 2016, Perencanaan dan Implementasi Information Security Management System Menggunakan Framework ISO/IEC 27001, *Jurnal Teknologi dan Sistem Komputer*, No.1, Vol.4, 60-66.

[5] Badan Standarisasi Nasional, 2014, *SNI ISO/IEC 27000:2014 – Teknologi Informasi – Teknik Keamanan – Sistem Manajemen Keamanan Informasi – Gambaran Umum dan Kosakata (ISO/IEC 27000:2012, IDT)*, BSN, Bandung.

[6] Itradat, Awni, Sari Sultan, Maram Al-Junaidi, Rawa'a Qaffaf, Feda'a Mashal, dan Fatima Daas, 2014, Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study, *Jordan Journal of Mechanical and Industrial Engineering*, No.2, Vol.8, 102-118.

[7] Ritzkal, Arif Goeritno, dan A.H. Hendrawan, 2016, Implementasi ISO/IEC 27001:203 untuk Sistem Manajemen Keamanan Informasi (SMKI) pada Fakultas Teknik UIKA-Bogor, *Seminar Nasional Sains dan Teknologi Universitas Muhamadiyah*, Jakarta.

[8] Badan Standarisasi Nasional, 2013, *SNI ISO/IEC 27001:2013 – Teknologi Informasi – Teknik Keamanan – Sistem Manajemen Keamanan Informasi (ISO/IEC 27001:2013, IDT)*, BSN, Bandung.

[9] Deloitte, 2009, ISO 27001 Information Security Standard Gap Analysis Executive Summary Report, *Final Internal Audit Report*, Deloitte.