Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.202071940
Vol. 7, No. 3, Juni 2020, hlm. 435-442 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 30/E/KPT/2018 e-ISSN: 2528-6579

PERANCANGAN PERANGKAT AUDIT INTERNAL UNTUK SISTEM KEAMANAN INFORMASI PADA ORGANISASI XYZ

Rizky Aditya Pratama Wijaya[1], Arif Rahman Hakim*[2]

[1,2]Sekolah Tinggi Sandi Negara
Email: [1]rizky.aditya@student.stsn-nci.ac.id, [2]arif.hakim@stsn-nci.ac.id
*Penulis Korespondensi

(Naskah masuk: 16 April 2019, diterima untuk diterbitkan: 22 April 2020)

Abstrak

Organisasi xyz sebagai penyelenggara sistem elektronik strategis harus mempunyai mekanisme audit internal terhadap keamanan sistem elektronik yang dimilikinya. Namun, organisasi xyz belum memiliki perangkat audit (*audit tool*) untuk melakukan audit internal tersebut secara berkala. Di sisi lain, perangkat audit tersebut berperan penting dalam menganalisis kerawanan yang terdapat dalam sistem. Untuk itu, organisasi xyz perlu merancang perangkat audit internal tersebut agar mekanisme audit berkala yang disyaratkan dapat dipenuhi dan risiko kegagalan akibat kerawanan sistem informasi yang dimiliki dapat dimitigasi dengan baik. Pada makalah ini dilakukan penelitian kualitatif berupa perancangan perangkat audit didasarkan pada penggunaan tiga metode dalam penentuan kriteria audit, yaitu analisis risiko menggunakan FMEA, kemudian penentuan kriteria audit berdasarkan pemetaan kontrol menggunakan *Statement of Applicability* (SoA) ISO/IEC 27002:2013 dan analisis proses bisnis menggunakan COBIT 5. Kriteria audit yang telah ditentukan dengan tiga metode tersebut kemudian dilakukan pembentukan perangkat audit, ujicoba impementasi, penilaian dan diakhiri dengan finalisasi perangkat audit. Berdasarkan analisis risiko dengan FMEA didapatkan 22 aset bernilai risiko tinggi, 10 aset bernilai sedang, 18 risiko bernilai rendah, dan 1 risiko bernilai sangat rendah. Selanjutnya pada proses pemetaan kontrol SoA ISO/IEC 27002:2013 dihasilkan 29 kontrol dan pada analisis proses bisnis berdasarkan COBIT 5 didapatkan 9 proses *enabler* yang kemudian digunakan sebagai kriteria audit. Selanjutnya hasil 29 kontrol tersebut kemudian diklasifikasikan menjadi enam kategori audit tingkat kepatuhan dan sembilan proses enabler tersebut diklasifikasikan menjadi sembilan kategori audit level pencapaian, sehingga perangkat audit yang dibentuk mengandung kategori tersebut. Hasil uji coba implementasi, penilaian dan finalisasi perangkat audit menunjukkan bahwa perangkat audit yang dihasilkan sudah sesuai dengan kebutuhan organisasi xyz.

Kata kunci: *perangkat audit, audit internal, COBIT 5, ISO/IEC 27002:2013, FMEA.*

DEVELOPING INTERNAL AUDIT TOOL FOR INFORMATION SECURITY SYSTEM IN XYZ ORGANIZATION

Abstract

The XYZ organization as the operator of electronic systems with strategic characteristic shall have internal audit mechanisms for its electronic systems security. Unfortunately, XYZ organization does not have an internal audit tool to conduct the audit periodically. In other hand, this audit tool plays an important role in determining vulnerability of the systems. For this reason, XYZ organization needs to design the internal audit tool so that periodic audit mechanism required can be conducted and the risk of system failure due to the vulnerability of the system can be properly mitigated. In this paper, we conduct qualitative research to design audit tool using three methods in determining the audit criteria, the first is FMEA in risk analysis process, the second is ISO / IEC 27002: 2013 in control analysis process and the third is COBIT 5 in business process analysis. Our audit tool is design based on the audit criteria that obtained from those three methods. Based on risk analysis using FMEA we obtained 22 assets with high risk, 10 assets with medium risk, 18 assets with low risk, and one asset with very low risk. From control analysis based on SoA ISO/IEC 27002:2013, we obtained 29 risk-based controls and from business process analysis using COBIT 5 we obtained nine enabler processes. Then those 29 controls and nine processes are used as audit criteria. In the next step, we classify these 29 controls into six categories in compliance level and those nine processes into nine categories in achievement level in our audit tool. The results of implementation trials, assessment, and finalization of our audit tool shows that our audit tool has been consistent with the needs of XYZ organization.

Keywords: *audit tool, internal audit, COBIT 5, ISO/IEC 27002:2013, FMEA.*

1. PENDAHULUAN

Organisasi xyz merupakan lembaga pemerintah non-kementerian yang memiliki fungsi strategis bagi negara. Kodifikasi nama organisasi xyz dalam makalah ini ditujukan untuk menghindari penyalahgunaan profil organisasi xyz sebagai salah satu penyelenggara fungsi strategis negara. Dalam menjalankan fungsinya, organisasi xyz memerlukan data dan informasi yang terkait dengan fungsinya tersebut. Untuk mengolah data dan informasi yang telah dihimpun, organisasi xyz memiliki perangkat Teknologi dan Informasi (TIK) yang terdiri dari sistem informasi, aplikasi, dan perangkat teknologi informasi (TI).

Sistem informasi yang dimiliki oleh organisasi xyz berisi informasi penting seperti identitas pribadi *user* atau pelanggan organisasi xyz, identitas pribadi target operasi, dan lokasi tempat kejadian perkara. Meninjau peraturan perundangan terkait informasi rahasia di antaranya UU No.11 Tahun 2008, UU No. 31 Tahun 2014, Permenkominfo No. 20 Tahun 2016, Permenkes No. 269 Tahun 2008 maka sistem informasi yang dimiliki oleh organisasi xyz mengelola informasi yang bersifat rahasia, sehingga diperlukan tindakan perlindungan terhadap informasi tersebut. Tindakan perlindungan atau pengamanan telah dilakukan oleh organisasi xyz, seperti penggunaan *username* dan *password* untuk memasuki aplikasi atau sistem informasi organisasi xyz, dan penggunaan algoritma MD5 untuk melakukan *hash* terhadap setiap *password*. Namun masih terdapat permasalahan yang terjadi di organisasi xyz, sistem informasi utama organisasi xyz yang tidak bisa diakses, aplikasi layanan pelanggan milik *Call Canter* yang sering mengalami gangguan, dan data kegiatan hilang di kotak masuk *email* milik *Call Center*.

Pada tahun 2016, dilakukan evaluasi kesiapan keamanan informasi berbasis Indeks Keamanan Informasi (Indeks KAMI) oleh Kementerian Komunikasi dan Informatika terhadap organisasi xyz. Hasil yang didapatkan menunjukkan bahwa sistem elektronik yang dimiliki organisasi xyz bersifat strategis yang memiliki dampak serius terhadap kepentingan umum dan keamanan negara. Status sistem elektronik strategis tersebut mengharuskan organisasi xyz sebagai penyelenggara sistem informasi untuk memperoleh sertifikat manajemen pengamanan informasi. Namun hingga saat ini organisasi xyz belum memiliki sertifikat manajemen pengamanan informasi tersebut.

Menurut Sarno dan Iffano (2009), untuk mengetahui celah-celah keamanan yang terjadi dan mempersiapkan audit sertifikasi manajemen pengamanan informasi, diperlukan audit pada organisasi. Fungsi audit internal pada suatu organisasi harus secara periodik menilai tingkat efektifitas kontrol internal, termasuk kontrol keamanan informasi (Steinbart et al, 2012). Oleh karena itu perlu dilakukan audit internal terhadap organisasi xyz. Namun organisasi ini belum memiliki alat bantu audit untuk melakukan audit tersebut, sehingga pada penelitian ini dilakukan perancangan perangkat audit keamanan informasi yang sesuai dengan kebutuhan organisasi xyz untuk membantu organisasi xyz melakukan audit.

2. AUDIT DAN RISIKO KEAMANAN INFORMASI

Audit merupakan suatu proses untuk melakukan evaluasi terhadap suatu organisasi, sistem, operasi atau produk (F.A. Suryono, 2013). Aktifitas audit ditujukan melakukan evaluasi secara objektif, independen, sistematik, dan terdokumentasi untuk menentukan pemenuhan syarat yang telah ditetapkan disertai dengan bukti-bukti (R. Sarno & I. Iffano, 2009). Guna melaksanakan audit secara efektif, maka diperlukan suatu perencanaan (R. Sarno, 2009).

Dalam pelaksanaan audit, diperlukan pengumpulan bukti audit oleh auditor. Bukti yang telah dikumpulkan kemudian dilakukan evaluasi kekuatan dan kelemahan dari kontrol pengimplementasian proses teknologi informasi (TI). Audit TI menyediakan jaminan yang proporsional atas informasi yang dihasilkan oleh sistem dalam suatu organisasi bersifat akurat, utuh, dan mampu mendukung pengambilan keputusan (A.R. Otero, 2019).

Umumnya, audit terhadap sistem informasi (SI) ataupun TI dilakukan dengan pendekatan risiko (R. Sarno, 2009). Langkah-langkah dalam melakukan audit yaitu: (R. Sarno, 2009)

a. Analisis kondisi saat ini
b. Penentuan tingkat risiko
c. Pelaksanaan audit
d. Penentuan rekomendasi

Menurut Weber (S. Gondodiyoto, 2007), kontrol dan audit menjadi penting didorong oleh faktor berikut:

a. Mendeteksi dengan tujuan pengelolaan komputer menjadi terarah
b. Mendeteksi risiko terjadinya kehilangan data
c. Mendeteksi risiko atas dampak pengambilan keputusan
d. Melindungi asset bernilai tinggi baik *hardware, software* maupun sumber daya manusia
e. Mendeteksi risiko terjadinya kegagalan fungsi pada komputer
f. Mendeteksi risiko terjadinya *fraud* atau penyalahgunaan komputer
g. Melindungi aspek kerahasiaan dari informasi
h. Mengatasi penggunaan komputerisasi yang tidak terkendali.

Langkah dan pentingnya melakukan audit tersebut berkaitan erat dengan risiko. Risiko adalah peluang terjadinya suatu kondisi yang mampu memberikan dampak atau menyebabkan gangguan pada proses bisnis suatu organisasi sehingga tujuan bisnisnya gagal (R. Sarno dan I. Iffano, 2009).

Dalam konteks keamanan informasi, risiko merupakan dampak akibat terjadinya suatu ancaman terhadap keamanan informasi pada suatu organisasi. Ancaman yang dimaksud adalah ancaman terhadap kerahasiaan, keutuhan, dan ketersediaan informasi suatu organisasi. Selain memiliki dampak terhadap informasi, risiko berupa ketidakpastian juga memiliki dampak terhadap pemenuhan tujuan bisnis, tipe risiko ini disebut risiko bisnis (R. Sarno, 2009).

Risiko dan kendalinya harus dipahami dengan baik sehingga dapat dicegah dan ditangani dengan baik. Untuk mengetahui risiko yang sering muncul beserta tingkat dampaknya, maka diperlukan proses penilaian risiko dan analisis risiko (R. Sarno, 2009). Penilaian risiko merupakan penilaian terhadap kemungkinan risiko yang terjadi pada setiap proses bisnis yang ada. Tahap selanjutnya yaitu menentukan tingkat risiko dari setiap aset dan proses bisnis terkait. Penentuan tersebut diawali dengan menentukan tingkat besarnya dampak dan probabilitas kemungkinan terjadinya suatu risiko dalam tingkatan rendah, sedang, dan tinggi.

2.1. Analisis Risiko dengan Metode FMEA

Metode *Failure Mode Effect Analysis* (FMEA) merupakan rangkaian proses identifikasi, evaluasi, dan pencegahan risiko kegagalan suatu sistem disertai perkiraan dampak dari kegagalan yang terjadi pada sistem tersebut (L.J. Susilo & V.R. Kaho, 2009). Tujuan utama dari FMEA adalah untuk mengidentifikasi kegagalan yang potensial, mengevaluasi penyebab dan dampaknya serta menentukan hal apa yang dapat mengurangi potensi terjadinya kegagalan yang berisiko tinggi (Liu et al, 2015).

Manfaat penggunaan FMEA pada organisasi atau perusahaan antara lain untuk meningkatkan kualitas, daya saing, efisiensi waktu/biaya pengembangan produk, dan kepuasan pelanggan dengan memperkirakan tindakan dan dokumen yang sesuai dengan risiko yang terjadi (A. Shekari & S. Fallahian, 2007).

Terdapat sepuluh langkah dalam menerapkan metode FMEA., yaitu:

1. Reviu proses.
2. Inventarisir bentuk kesalahan yang mungkin terjadi melalui *brainstorming.*
3. Menyusun daftar dampak untuk setiap bentuk kesalahan.
4. Menentukan tingkat dampak (*severity*) kesalahan.
5. Menentukan tingkat kemungkinan terjadinya *(occurrence*) kesalahan.
6. Menentukan tingkat kemungkinan deteksi dari tiap kesalahan atau dampaknya.
7. Menentukan tingkat prioritas risiko (RPN) dari masing-masing kesalahan dan dampak.
8. Menentukan prioritas kesalahan yang memerlukan penanganan yang lebih lanjut.
9. Melakukan tindakan mitigasi.
10. Menghitung kembali RPN yang tersisa untuk melihat hasil dari tindak lindung yang dilakukan.

Dalam proses analisis risiko FMEA perlu dilakukan penentuan nilai *severity*, *occurence*, dan *detection*. *Severity* merupakan tahapan awal yang digunakan untuk menganalisis risiko-risiko dengan memberikan skala berdasarkan dampak dari risiko tersebut bagi perusahaan atau organisasi. Skala yang diberikan dimulai dari satu hingga sepuluh. Hubungan antara skala dengan nilai *severity* dijelaskan pada tabel 1.

Tahapan *occurence* merupakan pengukuran terhadap tingkat frekuensi terjadinya suatu permasalahan atau risiko yang dapat menyebabkan suatu kegagalan. Hubungan antara skala dan nilai *occurrence* ditunjukkan pada tabel 2.

Tabel 1. Skala *Severity*

skala	***effect***	***severity***
10	Berbahaya tanpa peringatan	Menyebabkan proses bisnis terhenti untuk waktu yang lama (lebih dari 1 minggu)
9	Berbahaya dengan peringatan	Menyebabkan proses bisnis terhenti untuk waktu cukup lama (lebih dari 1 hari)
8	Sangat tinggi	Menyebabkan proses bisnis terhenti (kurang dari 1 hari)
7	Tinggi	Menghambat berjalannya proses bisnis

Tabel 2. Skala *Occurence*

skala	***effect***	***Occurence***
10	**Sangat tinggi:** Kegagalan hampir tidak bisa dihindari	Kegagalan terjadi lebih dari sekali setiap hari
9		Kegagalan terjadi sekali dalam setiap hari
8	**Tinggi:** Kegagalan kadang terjadi	Kegagalan terjadi setiap tiga atau empat hari sekali
7		Kegagalan terjadi setiap minggu
6	**Sedang:** Kegagalan kadang terjadi namun dalam jumlah yang tidak begitu besar	Kegagalan terjadi setiap dua minggu
5		Kegagalan terjadi setiap satu bulan
4		Kegagalan terjadi setiap tiga bulan
3	**Rendah:** Kegagalan terjadi relatif kecil	Kegagalan terjadi setiap enam bulan
2	**Sangat Jarang**: Kegagalan yang terjadi relatif kecil dan jarang	Kegagalan terjadi setiap tahun
1	***Remote*:** Kegagalan tidak pernah terjadi	Kegagalan terjadi beberapa tahun

Tahapan *detection* merupakan tahapan pengukuran terhadap kemampuan suatu organisasi dalam mengontrol kegagalan yang nantinya dapat terjadi. Nilai *detection* didasarkan pada pengendalian organisasi atau perusahaan yang terjadi saat ini. Indeks skala *detection* yaitu dari satu hingga sepuluh sebagaimana tertera pada Tabel 3.

Tabel 3. Skala *Detection*

skala	*effect*	*detection*
10	Hampir tidak mungkin	Potensi penyebab tidak terdeteksi atau tidak dapat dikontrol
9	Sangat jarang	Sangat sulit untuk mendeteksi risiko atau sangat sulit dikendalikan
8	Jarang	Sulit dideteksi dan sulit dikendalikan
7	Sangat rendah	Cukup sulit dideteksi atau cukup sulit untuk dikendalikan
6	Rendah	Dapat dideteksi dengan usaha ekstra dan dapat dikendalikan dengan usaha ekstra
5	Sedang	Dapat dideteksi dan dapat dikendalikan
4	Agak tinggi	Cukup mudah dideteksi dan cukup mudah dikendalikan
3	Tinggi	Mudah dideteksi dan mudah dikendalikan
2	Sangat tinggi	Sangat mudah dideteksi dan sangat mudah dikendalikan
1	Hampir pasti	Terlihat jelas dan sangat mudah pengendaliannya

Setelah dilakukan penilaian terhadap *severity, occurency, detection* dilakukan perhitungan nilai *Risk Priority Number* atau RPN. Nilai RPN diperoleh dari persamaan berikut:

$$RPN = Severity * Occurrence * Detection \quad (1)$$

Setelah dilakukan perhitungan nilai RPN maka dilakukan penentuan level risiko berdasarkan nilai RPN. Level risiko ini kemudian dibuat skala untuk menentukan risiko mana yang paling tinggi. Skala ini digunakan untuk menentukan tindakan organisasi atau perusahaan untuk mencegah risiko yang bernilai tinggi. Tabel 4 menunjukkan skala RPN.

Tabel 4. Skala RPN

RPN	Level Risiko
>= 200	Sangat Tinggi
120-199	Tinggi
80-119	Sedang
20-79	Rendah
0-19	Sangat Rendah

2.2. Pemetaan Kontrol dengan *Statement of Applicability* (SoA) ISO/IEC 27002:2013

Risiko yang telah dianalisis pada tahapan sebelumnya, dijadikan dasar dalam pemetaan kontrol yang akan dipilih untuk diimplementasikan pada sistem keamanan informasi. *Statement of Applicability* (SoA) merupakan pernyataan suatu kontrol dipilih atau tidak dipilih oleh suatu organisasi untuk diimplementasikan berdasarkan hasil analisis risiko yang dimiliki.

Pada makalah ini, kontrol dipilih berasal dari ISO/IEC 27002:2013 yang merupakan suatu standar yang memberikan *best practice* bagi suatu perusahaan, instansi maupun organisasi untuk mengembangkan dan mengelola keamanan yang sesuai dengan standar keamanan dan meningkatkan keamanan informasi bagi satu perusahaan, instansi maupun organisasi. Sebelum adanya ISO/IEC 27002:2013 terdapat ISO/IEC 27002:2005. Perbedaan antara ISO/IEC 27002:2005 dengan ISO/IEC 27002:2013 adalah jumlah kontrol yang diberikan. ISO/IEC 27002:2005 memiliki sebelas bagian kontrol sedangkan ISO/IEC 27002:2013 memiliki empat belas bagian kontrol [5].

2.3. COBIT 5

Control Objectives for Information and Related Technology atau COBIT mengandung serangkaian praktik terbaik pada domain tata kelola TI. COBIT 5 memberikan kerangka kerja komprehensif yang dapat membantu suatu perusahaan untuk mendapatkan tujuan dalam kerangka *governance* dan *management* organisasi TI [ISACA, 2013]. COBIT 5 memiliki peran dalam menyelaraskan tujuan bisnis atau *bussiness goals* dengan tujuan TI (*IT goals*), menyediakan alat ukur atau *metrics* dan model kematangan. Model kematangan atau *maturity* model digunakan untuk mengukur pencapaian kinerja dan digunakan untuk mengidentifikasi tanggung jawab dari masing-masing proses TI dan bisnis. Secara lebih mudahnya, COBIT 5 membantu perusahaan untuk mengoptimalkan nilai dari pengelolaan TI dengan menyeimbangkan keuntungan, meminimalkan risiko, dan penggunaan sumber daya.

3. PENENTUAN KRITERIA AUDIT

Pada makalah ini, perancangan perangkat audit bergantung pada kriteria audit yang ditentukan organisasi zyz. Kriteria audit tersebut ditentukan berdasarkan pada dua analisis, yaitu analisis kontrol dan analisis proses bisnis. Gambar 1 menunjukkan tahapan dari kedua analisis tersebut. Dapat dilihat bahwa analisis kontrol terdiri dari tahapan identifikasi aset, pemetaan aset, analisis risiko, penetapan *Statement of Applicability* (SoA), dan pemetaan kontrol yang digunakan untuk kemudian menjadi kriteria audit. Uraian detail dari analisis kontrol tersebut dapat dilihat pada bagian 3.1.

Untuk analisis proses bisnis terdiri dari penentuan kebutuhan utama organisasi xyz, pemetaan kebutuhan utama organisasi xyz ke *stakeholder needs* COBIT 5, proses *cascading* dari *stakeholder needs* ke *enterprise goals* COBIT 5, proses *cascading* dari *enterprise goals* ke *IT-related goals*, dan *cascading* dari *IT-related goals* ke *enabler goals*. Tahapan-

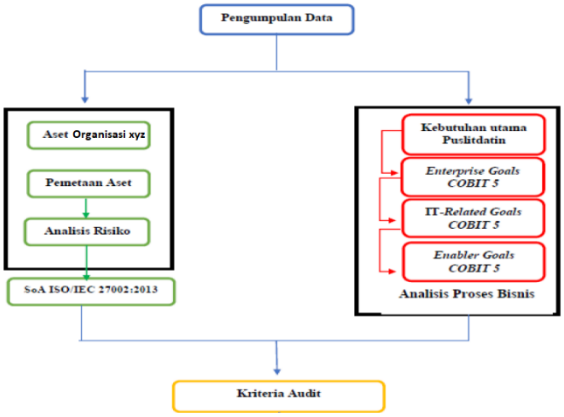
tahapan analisis proses bisnis tersebut diuraikan secara detail pada bagian 3.2.

3.1. Analisis Kontrol Organisasi XYZ

Analisis kontrol diawali dengan melakukan analisis risiko berdasarkan aset organisasi xyz yang telah dipetakan. Kemudian dilakukan identifikasi dan penetapan *Statement of Applicability* (SoA) ISO/IEC 27002:2013.

3.1.1. Analisis Risiko dengan FMEA

Langkah pertama yang dilakukan pada tahap analisis risiko yaitu melakukan identifikasi ancaman dan kelemahan untuk ditentukan risiko dari setiap aset. Pada tabel 5 merupakan ancaman dan kelemahan yang terjadi pada seluruh aset yang dimiliki organisasi xyz.



Gambar 1. Penentuan kriteria audit

Tabel 5. Jenis Ancaman dan Kelemahan

nomor	jenis ancaman	jenis kelemahan
1	Kehilangan aset	Tempat penyimpanan belum dilakukan secara terpusat
2	Modifikasi aset	Prosedur pengamanan dokumen belum ada
3	Tempat penyimpanan aset rusak	Belum ada backup data
4	Akses yang tidak sah	Masih ada perbaikan pada sistem informasi
5	*Hacking*	Belum ada prosedur pengelolaan password
6	*Cracking*	Belum ada prosedur pengelolaan jaringan
7	Media aset rusak	Belum ada peraturan pengelolaan aplikasi
8	*System error*	Belum dilakukan pemeliharaan secara berkala
9	Pencurian password	Belum ada prosedur pengelolaan perangkat
10	Kesalahan konfigurasi	Belum dilengkapi fasilitas monitoring
11	Serangan virus	Belum ada pengelolaan komputer
12	Gangguan listrik	Kurangnya kesadaran keamanan informasi
13	Gangguan perangkat	Belum dilakukan konfigurasi
14	Kebakaran	Prosedur pengamanan belum ada
15	*Human error*	Belum adanya pelatihan SDM secara rutin
16	*Social engineering*	Kurangnya perhatian terhadap keamanan informasi

Setelah dilakukan pemetaan ancaman dan kelemahan, maka dilakukan perhitungan nilai *severity* (S), *occurence* (O), dan *detection* (D) untuk didapatkan nilai RPN dari setiap aset. Berdasarkan hasil perhitungan tersebut didapatkan 22 aset bernilai risiko tinggi, 10 aset bernilai sedang, 18 risiko bernilai rendah, dan 1 risiko bernilai sangat rendah. Risiko yang memiliki nilai tinggi yaitu seluruh aset perangkat lunak dan perangkat keras. Risiko bernilai sedang yaitu dokumen *source code*, dokumen konfigurasi jaringan, dan seluruh aset perangkat jaringan organisasi xyz. Risiko bernilai rendah dan sangat rendah yaitu aset dokumen dan sumber daya manusia. Pada tabel 6 ditampilkan contoh hasil analisis risiko menggunakan FMEA.

Tabel 6. Jenis Ancaman dan Kelemahan

jenis aset	S	O	D	RPN	level
Dokumen kontrak	4	2	6	48	Rendah
Dokumen SLA	3	2	6	36	Rendah
Sistem informasi utama	8	2	8	128	Tinggi
Aplikasi layanan	8	2	8	128	Tinggi
PC	8	3	5	120	Tinggi
LAN	8	2	7	112	Sedang
Ruang server	8	3	4	96	Rendah
PNS	6	2	5	60	Rendah

3.1.2. Pemetaan Kontrol SoA ISO/IEC 27002:2013

Setelah dilakukan analisis risiko, langkah selanjutnya melakukan identifikasi dan penetapan *Statement of Applicability* (SoA) ISO/IEC 27002:2013. SoA ini merupakan pernyataan yang berupa alasan memilih atau tidak memilih kontrol ISO/IEC 27002:2013. Pada tabel 7 ditampilkan contoh kontrol hasil SoA ISO/IEC 27002:2013 yang dilakukan di organisasi xyz.

Tabel 7. SoA ISO/IEC 27002:2013

klausul	implementasi	justifikasi
6.1.2	Tidak ada	Tidak ditemukan kebijakan keamanan informasi di organisasi xyz sehingga pembagian tugas dan tanggung jawab terkait keamanan informasi tidak didefinsisikan
7.1.1	Ada	Terdapat pelaksanaan mekanisme seleksi pegawai baru dengan melihat latar belakang calon karyawan
8.1.2	Ada	Kontrol ini dilakukan berdasarkan Permenkeu No 181/PMK/2016
9.1.2	Ada	Organisasi xyz memiliki kebijakan terkait hak akses jaringan
11.1.3	Ada	Organisasi xyz menempatkan perangkat, aset, dan barang lainnya sesuai dengan peraturan pengelolaan TIK yang berlaku di organisasi xyz

Berdasarkan hasil pemetaan kontrol SoA ISO/IEC 27002:2013, didapatkan 29 kontrol. Berikut contoh hasil kontrol risiko aset yang dijadikan sebagai kriteria audit.

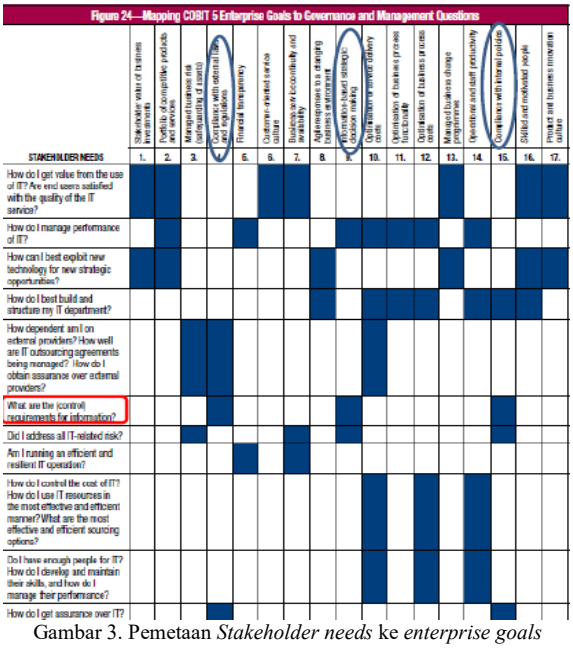
Tabel 8. Kontrol Risiko ISO/IEC 27002:2013

nomor	kontrol	nama kontrol
1	8.1.1	Inventarisasi aset
2	8.2.1	Klasifikasi informasi
3	9.4.1	Pembatasan akses informasi
4	11.1.1	Perimeter pengamanan fisik
5	11.2.1	Penempatan dan proteksi peralatan
6	12.2.1	Kontrol terhadap malware
7	13.1.3	Pemisahan jaringan

3.2. Analisis Proses Bisnis Organisasi XYZ Berbasis COBIT 5

Pada analisis proses bisnis, terdapat tiga tahap untuk menentukan kriteria audit. Tahap tersebut antara lain *stakeholder needs cascade to enabler goals*, *enabler goals cascade to IT-related goals, IT-related goals cascade to enabler goals*.

Pada tahap *stakeholder needs cascade to enabler goals*, tujuan strategis organisasi xyz harus ditentukan terlebih dahulu. Berdasarkan dokumen Rencana Strategis (Renstra) organisasi xyz tahun 2015-2019, maka tujuan dan sasaran strategis Organisasi xyz adalah "meningkatkan ketersediaan data dan informasi yang berkualitas dan berskala nasional". Tujuan strategis tersebut memiliki makna bahwa data dan informasi harus berkualitas disesuaikan dengan syarat yang telah ditentukan. Oleh karena itu tujuan tersebut sama halnya dengan pertanyaan tata kelola COBIT 5 yaitu "*what are the (control) requirements for information?*". Berdasarkan pertanyaan tersebut didapatkan 3 *enterprise goals*. Namun hanya dipilih satu *enterprise goals* yang sesuai dengan tujuan tersebut. *Enterprise goals* yang dipilih adalah *information-based strategic decision making* karena ketersediaan data dan informasi digunakan sebagai bahan pengambilan keputusan. Proses pemetaan tersebut dapat dilihat pada gambar 3.



Gambar 3. Pemetaan *Stakeholder needs* ke *enterprise goals*

Dari *enterprise goals* tersebut didapatkan 2 *IT-related goals* yaitu *alignment of IT and business strategy* dan *availabillity of reliable and useful information for decision making*. Proses *cascading* dapat dilihat pada tabel 9.

Setelah itu dilakukan proses *cascading* kembali untuk menemukan *enabler goals* sesuai dengan *IT-related goals*. Didapatkan 16 enabler goals dari hasil cascading tersebut. Namun tidak semua digunakan. *Enabler goals* yang memiliki tingkat kepentingan (*improvement*) tinggi dan pelaksanaan (*performance*) rendah di Organisasi xyz, maka didapat 9 proses *enabler*. 9 proses tersebut antara lain EDM 01, APO 01, APO 02, APO 03, APO 07, APO 08, APO 09, APO 13, BAI 10. 9 Proses inilah yang digunakan sebagai kriteria audit.

Tabel 9. Pemetaan *enterprise goals* ke IT-*related goals*

			Enterprise Goals
			Information-based strategic decision making
			14
IT-related goals			*Customer*
Financial	*01*	*Alignment of IT and business strategy*	*P*
Internal	*14*	*Availability of reliable and useful information for decision making*	*P*

4. PERANCANGAN PERANGKAT AUDIT

Kriteria audit yang telah ditentukan pada bagian sebelumnya, dijadikan acuan dalam merancang perangkat audit.

Gambar 2. Perancangan perangkat audit

Gambar 2 menunjukkan perangkat audit yang terdiri dari alat bantu audit kepatuhan dan level audit disertai panduan auditnya dirancang dengan mengacu pada kriteria audit yang telah ditentukan.

4.1. Pembentukan Perangkat Audit

Pada tahap analisis kontrol yang telah dilakukan didapatkan 29 kontrol risiko hasil analisis risiko, dan 9 proses hasil analisis proses bisnis. 29 kontrol tersebut kemudian dibagi menjadi 6 kategori audit tingkat kepatuhan yang dapat digambarkan pada tabel

9 dan 9 proses menjadi 9 kategori audit level pencapaian yang dapat digambarkan pada tabel 10.

Tabel 10. Kategori Audit Tingkat Kepatuhan

nomor kategori	klausul	jenis kategori
P1	8	Manajemen Aset
P2	9	Akses Kontrol
P3	11	Keamanan Fisik dan Lingkungan
P4	12	Keamanan Operasional
P5	13	Keamanan Komunikasi
P6	14	Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan

Setelah dilakukan pemetaan kategori, selanjutnya dilakukan pembuatan daftar pertanyaan audit. Pada tabel 11 merupakan contoh daftar pertanyaan audit tingkat dan audit level pencapaian.

Tabel 11. Kategori Audit Level Pencapaian

nomor kategori	proses	jenis kategori
T1	EDM 01	Pengaturan dan pemeliharaan kerangka tata kelola
T2	APO 01	Pengelolaan kerangka tata kelola TI
T3	APO 02	Pengelolaan strategi
T4	APO 03	Pengelolaan arsitektur
T5	APO 07	Pengelolaan sumber daya manusia
T6	APO 08	Pengelolaan hubungan
T7	APO 09	Pengelolaan layanan
T8	APO 13	Pengelolaan sistem manajemen keamanan informasi
T9	BAI 10	Pengelolaan konfigurasi

Kategori tersebut kemudian dikembangkan menjadi alat bantu audit dalam bentuk dokumen *excel* dan *webdesk*.

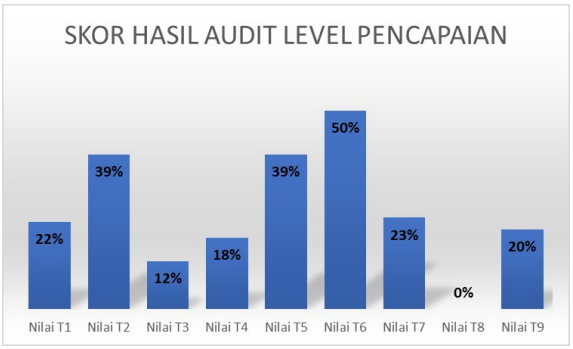
Tabel 12. Daftar Pertanyaan Audit Tingkat Kepatuhan

no.	audit tingkat kepatuhan	audit level pencapaian
1	Apakah organisasi anda melakukan inventarisasi terhadap seluruh aset yang dimiliki?	Apakah organisasi anda melakukan kegiatan evaluasi sistem tata kelola saat ini?
2	Apakah seluruh aset yang dimiliki sudah diidentifikasi secara jelas pemilknya?	Apakah organisasi anda memiliki aturan, konstitusi atau statuta organisasi terkait tata kelola TI?
3	Apakah organisasi anda memiliki aturan mengenai pengembalian aset bagi karyawan yang telah berhenti atau dipindah tugaskan?	Apakah organisasi anda melakukan pengawasan terhadap tata kelola TI ?
4	Apakah aset yang dimiliki sudah diklasifikasikan berdasarkan tingkat kepentingannya dengan organisasi?	Apakah organisasi anda memiliki dokumen persyaratan berubah?
5	Apakah organisasi anda memiliki dan menerapkan prosedur pelabelan aset brdasarkan tingkat klasifikasinya	Apakah organisasi anda memiliki dokumen laporan audit tata kelola atau kewajiban tata kelola TI?

4.2. Uji Coba Implementasi Perangkat Audit

Setelah dilakukan pembuatan alat bantu audit, maka langkah selanjunya adalah melakukan penerapan atau uji coba alat tersebut di organisasi xyz. Tahap pertama dilakukan uji coba terhadap alat bantu audit level pencapaian. Hasil uji coba tersebut dapat dilihat pada Gambar 4. Berdasarkan hasil uji coba tersebut, Organisasi xyz berada pada level 1 atau level *managed* dengan mendapat dua skala yaitu skala N atau *Not achieved* dan skala P atau *Partially achieved*. Skala N diperoleh pada kategori T3 dan T8 dan skala P diperoleh pada kategori T1, T2, T4, T5, T6, T7, dan T9.

Setelah dilakukan uji coba pada tahap pertama, maka langkah selanjutnya dilakukan tahap kedua. Pada tahap kedua, dilakukan uji coba audit tingkat kepatuhan. Hasil uji coba tingkat kepatuhan tersebut dapat dilihat pada tabel 13.



Gambar 4. Hasil audit level pencapaian

Tabel 13. Hasil Audit Tingkat Kepatuhan

nomor	kategori audit	hasil
1	P1	Hanya terpenuhi tiga kriteria dari enam kriteria
2	P2	Hanya terpenuhi tiga kriteria dari lima kriteria
3	P3	Tidak ada kriteria yang terpenuhi
4	P4	Hanya terpenuhi dua kriteria dari sebelas kriteria
5	P5	Hanya terpenuhi dua kriteria dari lima kriteria
6	P6	Tidak ada kriteria yang terpenuhi

Berdasarkan hasil tersebut, organisasi xyz telah menerapkan tiga kriteria pada kategori pertama dan kedua. Pada kategori keempat dan kelima hanya menerapkan dua kriteria. Hanya pada kategori ketiga dan keenam, organisasi xyz tidak menerapkan kriteria yang ada.

4.3. Penilaian Perangkat Audit

Setelah dilakukan uji coba terhadap alat bantu audit keamanan informasi, maka tahap selanjutnya dilakukan penilaian alat bantu tersebut oleh Kepala Bidang TIK yang dibantu oleh Kepala Subbidang Jaringan. Menurut penilaian dari Kepala Bidang TIK, alat audit keamanan informasi yang telah dirancang sudah sesuai dengan kondisi organisasi xyz dan dapat membantu dalam pelaksanaan audit karena alat bantu audit yang dihasilkan dilengkapi dengan langkah

audit dan temuan atau bukti yang memperkuat jawaban audit. Dengan adanya langkah tersebut, maka auditor maupun *auditee* dapat dengan cepat menemukan setiap bukti dari masing-masing jawaban pertanyaan audit yang tersedia.

4.4. Finalisasi Perangkat Audit

Proses terakhir dari tahap penelitian ini adalah melakukan finalisasi alat bantu audit keamanan informasi yang telah dibuat. Proses finalisasi terdiri dari dua tahap. Tahap pertama yaitu melakukan validasi hasil alat bantu audit kepada ahli TI dan tahap kedua melakukan finalisasi kepada Kepala Bidang TIK organisasi xyz. Tahap pertama bertujuan untuk memastikan bahwa kriteria yang terdapat pada alat bantu audit keamanan informasi sudah sesuai dengan standar dan kerangka kerja yang digunakan, sedangkan pada tahap kedua bertujuan sebagai hasil validasi bahwa alat bantu audit keamanan informasi yang telah dibuat sudah sesuai dengan kondisi dan dapat diterima oleh organisasi xyz.

5. KESIMPULAN

Perangkat audit dengan kriteria yang sesuai kebutuhan organisasi xyz ditentukan oleh dua faktor yaitu faktor kontrol risiko dan faktor proses bisnis organisasi xyz. Pada tahap analisis risiko didapatkan dua puluh sembilan kontrol dan dikelompokkan menjadi enam kategori kriteria audit yaitu manajemen aset, akses kontrol, keamanan fisik dan lingkungan, keamanan operasional, keamanan komunikasi, dan akuisisi sistem informasi, pembangunan dan pemeliharaan. Analisis proses bisnis menghasilkan sembilan kategori kriteria audit yaitu pengaturan dan pemeliharaan kerangka tata kelola, pengelolaan kerangka tata kelola TI, pengelolaan strategi, pengelolaan arsitektur, pengelolaan sumber daya manusia, pengelolaan sistem manajemen keamanan informasi, pengelolaan layanan, pengelolaan hubungan, dan pengelolaan konfigurasi. Setelah dilakukan proses penerapan, penilaian, dan finalisasi perangkat audit, diperoleh simpulan yaitu perangkat audit dengan lima belas kriteria audit tersebut sudah sesuai dengan kebutuhan organisasi xyz.

DAFTAR PUSTAKA

R. SARNO & I. IFFANO, 2009. *Sistem Manajemen Keamanan Informasi Berbasis ISO 27001*. Surabaya: itspress.

PAUL JOHN STEINBART, ROBYN L. RASCHKE, GRAHAM GAL, WILLIAM N. DILLA, 2012. *The Relationship between Internal Audit and Information Security: An Exploratory Investigation.* International Journal of Accounting Information Systems 13 : 228-243.

ANGEL. R. OTERO, 2019. *Information Technology Control and Audit.* 5th Edition. CRC Press.

F. A. SURYONO, 2013. *"Perancangan Perangkat Audit Keamanan Informasi: Studi Kasus Pusat Komunikasi Kementerian Luar Negeri*," Universitas Indonesia, Depok.

R. SARNO, 2009. *Audit Sistem & Teknologi Informasi*. Surabaya: ITS Press.

S. GONDODIYOTO, 2007. *Audit Sistem Informasi Pendekatan CobIT*. Jakarta: Mitra Wacana Media.

Praxiom Reserach Group Limited, 2016. *"ISO 27002 Old versus New*," [Online]. Tersedia di: <http://www.praxiom.com/iso-27002-old-new.htm> [Diakses 1 Januari 2019]

L. J. SUSILO & V. R. KAHO, 2009. *Manajemen Risiko Berbasis ISO 3100 Untuk Industri Non-Perbankan*. Jakarta: PPM Manajemen.

LIU HC, YOU JX, DING XF, SU Q, 2015. *Improving risk evaluation in FMEA with a hybrid multiple criteria decision making method*. International Journal of Quality and Reliability Management 32(7):763–782

A. SHEKARI & S. FALLAHIAN, 2007. *"Improvement of Learn Methodology With FMEA,"* [Online]. Tersedia di: <https://www.pomsmeetings.org/ConfProceedings/007/CDProgram/Topics/full_length_papers_files/007-0520.pdf> [Diakses 1 Januari 2019]

ISACA, 2013. *A Business Framework for the Governance and Management of Enterprise IT*.

Undang-undang Republik Indonesia nomor 31 tahun 2014 tentang Perlindungan Saksi dan Korban. Jakarta: Kementerian Sekretariat Negara Republik Indonesia.

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia nomor 20 tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Jakarta: Kementerian Sekretariat Negara Republik Indonesia.

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia nomor 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. Jakarta: Kementerian Sekretariat Negara Republik Indonesia.

Peraturan Menteri Keuangan Republik Indonesia nomor 181 tahun 2016 tentang Penatausahaan Barang Milik Negara. Jakarta: Kementerian Sekretariat Negara Republik Indonesia.

Peraturan Menteri Kesehatan Republik Indonesia nomor 20 tahun 2016 tentang Rekam Medis. Jakarta: Kementerian Sekretariat Negara Republik Indonesia.