RENCANA PENERAPAN *CYBER-RISK MANAGEMENT* MENGGUNAKAN NIST CSF dan COBIT 5

Obrina Candra Briliyant, Rizqi Aulia Ashari

Sekolah Tinggi Sandi Negara, Jalan Raya Haji Usa Nomor 56 Putat Nutug, Ciseeng, Parung, Bogor, 16120, Indonesia

E-mail: obrina@stsn-nci.ac.id

Abstract

The development of information and communication technology (ICT) has created the cyberspace which enables easier information access and information management fastly and accurately. The use of ICTs that is currently increasing makes the security needs of system used also increase, particularly in regards to the risks. In order to address the issue, a good implementation of cyber-risk management is deemed essential. ABC Organization is one of the government instances managing Indonesia's critical infrastructures. ABC maintains XYZ information system, a strategic IS that is utilized to assist leaders in decision making. In this research, a plan to implement cyber-risk management is proposed using NIST CSF and COBIT 5 to manage cyber risks in XYZ IS. This result of this research are 13 high-value risks and 22 moderate-value risks included COBIT 5 enabler process as risk mitigations. From these, 15 action plans to implement cyber-risk management were developed in accordance with oragnization's capabilities and targets. These action plans were then prioritized based on the needs of the organization.

Keywords: *cyber-risk management, keamanan siber, NIST CSF, COBIT 5*

Abstrak

Kemajuan Teknologi Informasi dan Komunikasi (TIK) membentuk ruang siber yang memudahkan akses informasi maupun pengelolaan informasi secara cepat dan akurat. Pemanfaatan TIK yang meningkat saat ini membuat kebutuhan keamanan pada sistem yang digunakan juga meningkat, terutama terhadap risikonya. Untuk mengatasi hal ini, penerapan *cyber-risk management* yang baik dianggap perlu. Organisasi ABC merupakan salah instansi pemerintah pengelola infrastruktur kritis Indonesia. ABC memelihara sistem informasi XYZ, SI strategis yang digunakan untuk membantu pimpinan dalam pengambilan keputusan. Dalam penelitian ini, diusulkan rencana penerapan *cyber-risk management* menggunakan NIST CSF dan COBIT 5 untuk mengelola risiko-risiko siber pada sistem informasi XYZ. Hasil penelitian berupa 13 risiko bernilai tinggi dan 22 risiko bernilai sedang disertai dengan *enabler process* COBIT 5 sebagai mitigasi risiko. Dari hasil tersebut kemudian disusun 15 rencana aksi (program kerja) penerapan *cyber-risk management* sesuai dengan kapabilitas dan target organisasi. Rencana aksi tersebut kemudian diprioritaskan sesuai kepentingan organisasi.

Kata kunci: *cyber-risk management, keamanan siber, NIST CSF, COBIT 5*

1. Pendahuluan

Ruang siber merupakan sekumpulan komputer yang terhubung dalam satu jaringan termasuk layanan, sistem komputer, *embedded processor, controller,* hingga informasi yang disimpan atau ditransmisikan melaluinya [1]. Terbentuknya ruang siber sebagai akibat dari kemajuan TIK memberikan banyak kemudahan bagi penggunanya [2]. Salah satunya adalah kemudahan akses informasi dan pengelolaan informasi secara cepat dan akurat [3]. Kemudahan tersebut berdampak pada pemanfaatan TIK yang semakin meningkat. Semakin meningkatnya pemanfaatan TIK maka kebutuhan terhadap keamanan sistem, *database,* dan aplikasi juga semakin memingkat, begitu pula dengan risikonya [4]. Risiko yang muncul dapat menyebabkan kerusakan sistem, pencurian informasi, manipulasi informasi atau perangkat istem, dan penyebaran informasi yang

mengakibatkan propaganda [5]. Oleh karena itu, risiko tersebut perlu dikelola dengan menerapkan *cyber-risk management.*

Manajemen risiko merupakan bagian dari keamanan siber yang didefinisikan oleh *International Telecommunications Union* (ITU) [6]. Keamanan siber saat ini ditujukan secara khusus terhadap instansi pemerintah pengelola infrastruktur kritis seperti pertahanan keamanan, energi, transportasi, sistem keuangan, dan layanan publik lainnya [7]. Hal tersebut dapat dilihat berdasarkan laporan Kementerian Komunikasi dan Informatika (Kominfo) pada tahun 2015 yang menyatakan bahwa sebagian besar dari 28.430.843 serangan siber terjadi pada *website* pemerintah dengan domain .go.id [8].

Organisasi ABC merupakan salah satu instansi pemerintah pengelola infratsruktur kritis di Indonesia. Organisasi ABC melaksanakan fungsinya melalui Unit Organisasi (UO) ABC berdasarkan peraturan internal organisasi yang dimiliki [7][9]. UO ABC bertugas melakukan pemeliharaan sistem informasi XYZ yang merupakan sistem informasi strategis bagi organisasi [10][11]. Berdasarkan hal tersebut, pada penelitian ini dilakukan penyusunan rencana penerapan *cyber-risk management* menggunakan NIST CSF dan COBIT 5 untuk mengurangi dan mengelola risiko siber sistem informasi XYZ. NIST CSF digunakan sebagai kerangka kerja yang akan diterapkan dan COBIT 5 sebagai kerangka kerja pendukung. Hasil yang akan didapatkan adalah rencana-rencana penerapan (program kerja) yang dapat diterapkan oleh UO ABC untuk mengelola risiko siber sistem informasi XYZ.

2. Landasan Teori

Keamanan siber

International Telecommunications Union (ITU) mendefinisikan bahwa keamanan siber adalah sekumpulan alat, kebijakan, konsep keamanan, usaha perlindungan, pedoman, manajemen risiko, aksi, pelatihan, praktik, jaminan, dan teknologi yang digunakan untuk melindungi ruang siber dan dimaksud berupa perangkat komputer, personil, infrastruktur, aplikasi, layanan, dan sistem telekomunikasi [6]. Keamanan siber berkaitan erat dengan keamanan informasi yang dikatakan bahwa kedua hal tersebut mempunyai tujuan sama, yaitu mempertahankan kerahasiaan, keutuhan dan ketersediaan. Tujuan keamanan siber adalah untuk mempertahankan kerahasiaan, keutuhan, dan ketersediaan baik informasi maupun lingkungan siber dan seluruh aset organisasi yang berkaitan dengan TI [12].

Cyber-risk management

Risiko siber merupakan risiko yang disebabkan oleh adanya ancaman siber di dalam ruang siber. Ruang siber merupakan sekumpulan komputer yang terhubung dalam satu jaringan termasuk layanan, sistem komputer, *embedded processor, controller,* hingga informasi yang disimpan atau ditransmisikan melaluinya [1]. Pada umumnya, ancaman siber ditujukan terhadap *cyber-system. Cyber-system* merupakan suatu sistem yang dibuat dan penggunaannya bergantung pada ruang siber. Adanya *cyber-system* tersebut menuntut organisasi untuk menyadari kerawanan sistemnya terhadap ancaman siber. *Cyber-risk management* dapat diartikan sebagai langkah pengelolaan berkelanjutan dalam menghadapi risiko siber dan ketidakpastian agar mampu memaksimalkan pencapaian tujuan organisasi [5].

NIST CSF

NIST CSF *for Improving Critical Infrastructure* merupakan kerangka kerja yang dapat digunakan untuk mengarahkan organisasi pada aktivitas keamanan siber dan mempertimbangkan risiko keamanan siber sebagai bagian dari proses manajemennya. Kerangka kerja ini memberikan panduan dan tahapan dalam meningkatkan keamanan siber melalui analisis risiko keamanan siber. Untuk menerapkannya, kerangka kerja ini memerlukan kerangka kerja yang lain karena sifatnya sangat bergantung pada kerangka kerja lain. Kerangka kerja lain yang dapat digunakan adalah COBIT 5, ISO/IEC 27001, NIST SP.800-53 CCS CSC dan ISA 62443 [13].

Bagian utama dalam kerangka kerja ini adalah *framework core* yang merupakan satu rangkaian aktivitas keamanan siber, *outcome* yang diinginkan, dan beberapa referensi informatif yang dapat digunakan untuk mencapainya. *Framework core* terdiri dari 5 fungsi, yaitu identifikasi (*identify*); perlindungan (*protect*); deteksi (*detect*); respon (*respond*); dan pemulihan (*recovery*), 22 kategori dan 100 subkategori yang cocok dengan contoh referensi informatifnya. Terdapat 7 tahapan untuk menerapkan *framework core*, yaitu:

1) *Prioritize and scope*
   Tahapan ini ditujukan untuk mengidentifikasi sasaran misi dan prioritas kebutuhan organisasi.
2) *Orient*
   Tahapan ini ditujukan untuk mengidentifikasi sistem yang terkait dengan pencapaian sasaran misi dan asetnya, ancaman dan kerawanan terhadapnya.
3) *Create a current profile*
   Tahapan ini ditujukan untuk menentukan

profil organisasi dengan mengindikasi *outcome* dari kategori atau subkategori yang dicapai.

4) *Conduct risk assessment*
Tahapan ini ditujukan untuk menganalisis kecenderungan risiko siber dan dampak yang mungkin terjadi terhadap organisasi.

5) *Create a target profile*
Tahapan ini ditujukan untuk menentukan target profil organisasi berdasarkan hasil penilaian kategori atau subkategori pada profil organisasi. Kategori dan subkategori yang ditentukan mempertimbangkan hasil analisis risiko. Selanjutnya, organisasi dapat memberikan subkategori tambahan untuk mengatasi risiko organisasi yang unik, yang tidak dapat diatasi dengan pilihan subkategori yang ada.

6) *Determine, analyze, and prioritize*
Tahapan ini ditujukan untuk membandingkan profil dan target profil organisasi sehingga didapatkan gap. Selanjutnya, ditentukan rencana aksi dan proritasnya yang dapat digunakan untuk mengatasi gap yang ada.

7) *Implementation action plan*Tahapan ini ditujukan untuk mengimplementasikan rencana aksi yang telah dibuat. Implementasi rencana aksi dapat digunakan untuk mengaswasi praktik keamanan siber organisasi.

COBIT 5

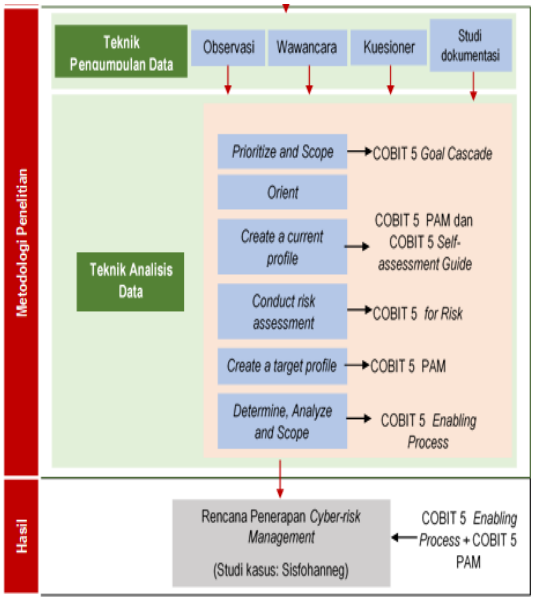
COBIT 5 merupakan kerangka kerja yang bersifat komprehensif yang digunakan untuk membantu organisasi mencapai tujuan dalam sudut pandang tata kelola dan manajemen bagi organisasi TI [14]. Penelitian ini menggunakan COBIT 5 *family framework* yang terdiri dari COBIT 5 *Goal Cascade*, COBIT 5 *Process Assessment Model* (PAM), COBIT 5 *Self-assessment Guide*, COBIT 5 *for Risk*, dan COBIT 5 *Enabling Process* sebagai kerangka kerja pendukung NIST CSF.

COBIT 5 *Goal Cascade* merupakan mekanisme untuk menerjemahkan tujuan atau target organisasi sesuai dengan kebutuhan *stakeholder* secara spesifik yang kemudian ditindaklanjuti dan disesuaikan dengan tujuan TI dan *enabler*-nya [14]. COBIT 5 PAM merupakan model dua dimensi yang digunakan untuk menilai kapabilitas proses organisasi [15].

COBIT 5 *Self-assessment Guide* merupakan salah satu bagian dari COBIT 5 *Assessment Programme* yang menyediakan cara untuk melakukan penilaian kapabilitas proses TI organisasi secara sedehana tanpa harus menyertakan bukti. Organisasi dapat menggunakan cara ini apabila ingin melaksanakan penilaian secara mandiri tanpa harus melibatkan *certified assesor* [16]. COBIT 5 *for Risk* merupakan salah satu produk dari COBIT 5 *Product Family* yang menangani secara khusus risiko pada TI [17]. COBIT 5 *Enabling Process* berisi petunjuk penggunaan setiap *enabler* proses. Pada setiap *enabler* diberikan petunjuk secara detail bagaimana setiap *enabler process* tersebut digunakan [14]

3. Metode

Metodologi penelitian yang digunakan pada penelitian ini disesuaikan dengan tahapan pada dokumen *Implementing* NIST *The Cybersecurity Framework* [18] yang memberikan panduan implementasi NIST CSF menggunakan COBIT 5 dengan tahapan seperti pada Gambar 1.



Gambar 1. Metodologi penelitian

4. Hasil dan Analisa

Prioritize and scope

Pada tahap ini dilakukan identifikasi sasaran misi UO ABC dan prioritasnya terhadap sasaran misi yang akan dicapai. Tahapan ini menghasilkan 18 *enabler process* COBIT 5 yang selaras dengan sistem informasi XYZ sebagai sasaran misi UO ABC. 18 *enabler process* tersebut kemudian dipetakan dengan NIST CSF sehingga menghasilkan 15 *enabler process* yang memberikan *cybersecurity outcomes* pada sistem informasi XYZ. Dari 15 *enabler process* tersebut, kemudian diprioritaskan 9 *enabler process* sesuai dengan kebutuhan UO ABC saat ini, yaitu EDM03, APO10, APO12, BAI01, BAI06, DSS01, DSS03, DSS04, dan MEA03.

Orient* dan *create a current profile

Pada tahap ini dilakukan identifikasi aset, ancaman, dan kerawanan terhadap sistem informasi XYZ sekaligus mendefinisikan *current profile* UO ABC dalam perspektif manajemen risiko. Teridentifikasi 43 aset, 11 ancaman, 23 kontrol keamanan dan 26 kerawanan terhadap sistem informasi XYZ. Selanjutnya dilakukan penilaian kapabilitas UO ABC sebagai *current profile* menggunakan COBIT 5 PAM dan COBIT 5 *Self-assessment Guide*. Penilaian dilakukan terhadap 26 subkategori NIST CSF yang relevan dengan 9 *enabler process* COBIT 5 terpilih pada tahapan sebelumnya. Penilaian kapabilitas menunjukkan bahwa 19 subkategori berada pada level 0 COBIT 5 PAM dan 7 subkategori berada pada level 1 COBIT 5 PAM. Berdasarkan hal tersebut, dapat disimpulkan bahwa *current profile* UO ABC berada pada *tier 1* NIST CSF yang berarti bahwa proses manajemen risiko organisasi belum terbentuk secara formal.

Conduct risk assessment* dan *create a target profile

Pada tahap ini dilakukan penilaian risiko siber terhadap sistem informasi XYZ sekaligus penentuan *target profile* UO ABC. Dari hasil identifikasi aset, ancaman, dan kerawanan pada tahap sebelumnya, ditemukan 35 risiko mungkin terjadi terhadap sistem informasi XYZ. Selanjutnya risiko-risiko tersebut dinilai menggunakan matriks ISO 27005:2011 yang dapat dilihat pada

TABEL *1*.

TABEL 1.
MATRIKS NILAI RISIKO ISO 27005:2011

	Kecenderungan skenario terjadi	Sangat Rendah (SR)	Rendah (R)	Sedang (S)	Tinggi (T)	Sangat Tinggi (ST)
Dampak Bisnis	Sangat Rendah (SR)	0	1	2	3	4
	Rendah (R)	1	2	3	4	5
	Sedang (S)	2	3	4	5	6
	Tinggi (T)	3	4	5	6	7
	Sangat Tinggi (ST)	4	5	6	7	8

Penilaian risiko menghasilkan 13 risiko bernilai tinggi dan 22 risiko bernilai sedang. Setelah mengetahui nilai risiko, UO ABC menentukan respon risiko berdasarkan COBIT 4 *for Risk* yang membagi respon risiko menjadi 4 jenis yaitu menghindari risiko, menerima risiko, membagi risiko dan mitigasi risiko. Hasil nilai respon risiko dapat dilihat pada TABEL 2.

TABEL 2.
NILAI DAN RESPON RISIKO

No.	ID risiko	Nilai risiko	Respon risiko
1.	R1	Tinggi	Dimitigasi
2.	R2	Sedang	Dimitigasi
3.	R3	Tinggi	Dimitigasi
4.	R4	Tinggi	Dimitigasi
5.	R5	Tinggi	Dimitigasi
6.	R6	Tinggi	Dimitigasi
7.	R7	Sedang	Dimitigasi
8.	R8	Tinggi	Dimitigasi
9.	R9	Sedang	Dimitigasi
10.	R10	Sedang	Dimitigasi
11.	R11	Sedang	Dimitigasi
12.	R12	Tinggi	Dimitigasi
13.	R13	Sedang	Dimitigasi
14.	R14	Tinggi	Dimitigasi
15.	R15	Sedang	Ditransfer
16.	R16	Sedang	Dimitigasi
17.	R17	Sedang	Dimitigasi
18.	R18	Sedang	Ditransfer
19.	R19	Tinggi	Ditransfer
20.	R20	Tinggi	Dimitigasi
21.	R21	Sedang	Dimitigasi
22.	R22	Sedang	Dimitigasi
23.	R23	Sedang	Dimitigasi
24.	R24	Tinggi	Dimitigasi
25.	R25	Sedang	Dimitigasi
26.	R26	Sedang	Dimitigasi
27.	R27	Sedang	Ditransfer
28.	R28	Sedang	Dimitigasi
29.	R29	Tinggi	Dimitigasi
30.	R30	Sedang	Dimitigasi
31.	R31	Sedang	Dimitigasi
32.	R32	Tinggi	Dimitigasi
33.	R33	Sedang	Dimitigasi
34.	R34	Sedang	Dimitigasi
35.	R35	Sedang	Ditransfer

Hasil respon risiko menunjukkan bahwa terdapat 30 risiko akan dimitigasi dan 5 risiko ditransfer kepada pihak ketiga. Berdasarkan hal tersebut, UO ABC kemudian menentukan *enabler process* COBIT 5 yang akan digunakan untuk memitigasi

risiko. Setelah *enabler process* mitigasi terpilih, ditentukan subkategori NIST CSF yang relevan terhadap *enabler process* tersebut sehingga dapat ditentukan subkategori NIST CSF yang akan diterapkan. Hasil penentuan mitigasi risiko dan subkategori NIST CSF dapat dilihat pada

TABEL *3*.

TABEL 3.
MITIGASI RISIKO

Generic risk scenario	*Enabler process* COBIT 5 sebagai mitigasi	Subkategori NIST CSF yang akan diterapkan	Tambahan proses yang akan diterapkan
Staff operasional	DSS01-01	-	DSS01-01
	DSS01-04	PR.IP-5 PR.AC-2 PR.AC-3	-
	DSS01-05	-	DSS01-05
Informasi	DSS01-01	-	DSS01-01
	DSS01-05	-	DSS01-05
Perangkat lunak	BAI06-01	PR.DS-1 PR.IP-3	-
	BAI06-02	-	BAI06-02
	BAI06-03	-	BAI06-03
	BAI06-04	-	BAI06-04

Berdasarkan Tabel 3, terdapat 7 *enabler process* terpilih sebagai mitigasi risiko. Namun, hanya 2 *enabler process* (DSS01-04 dan BAI06-01) yang relevan dengan subkatgori NIST CSF sehingga 5 *enabler process* lainnya (DSS01-01, DSS01-05, BAI06-02, BAI06-03, BAI06-04) diterapkan sebagai proses tambahan.

Selanjutnya *target profile* ditentukan terhadap subkategori NIST CSF yang akan diterapkan. Berdasarkan *current profile* yang telah diketahui, UO ABC menentukan *target profile* mencapai *tier* 3 NIST CSF (level 3 COBIT 5 PAM) agar *cyber-risk management* sistem informasi XYZ dapat dituangkan dalam sebuah kebijakan resmi dan dilaksanakan secara formal.

Determine, analyze, and prioritize

Pada tahap ini dilakukan analisis gap antara *current profile* yang telah diketahui dan *target profile* yang telah ditentukan serta memprioritaskan rencana aksi (program kerja) yang disusun. Hasil analisis gap dapat dilihat pada TABEL 4.

TABEL 4. HASIL ANALISIS GAP

No	ID Subkategori	*Current level*	Presentase pencapaian indikator (%)	*Target level*	Gap
1.	PR.IP-5	0	50	3	3
2.	PR.AC-2	0	50	3	3
3.	PR.AC-3	0	50	3	3
4.	PR.DS-1	0	50	3	3
5.	PR.IP-3	0	50	3	3

Tabel 4. menunjukkan bahwa nilai gap yang didapatkan adalah 3. Hal ini berarti UO ABC perlu meningkatkan kapabilitas subkategori yang akan diterapkan melalui 3 level, yaitu level 0 menuju level 1, level 1 menuju level 2, dan level 2 menuju level 3.

Setelah mengetahui nilai gap, selanjutnya menentukan rencana-rencana aksi untuk mengatasi gap tersebut sesuai dengan indikator pada setiap levelnya. Rencana aksi pada level 0 menuju level 1 ditentukan dengan mengacu pada aktivitas COBIT 5 *Enabling Process*. Rencana aksi pada level 1 menuju level 2 dan level 2 menuju level 3 ditentukan dengan mengacu pada COBIT 5 PAM. Berikut adalah rencana aksi yang telah disusun menjadi program kerja dan telah diprioritaskan.

Rencana aksi level 0 menuju level 1

Rencana aksi seperti pada Tabel 5. disusun berdasarkan *Base Practices* (BP) pada setiap *enabler process* COBIT 5 yang relevan dengan subkategori yang akan diterapkan.

TABEL 5.
RENCANA AKSI LEVEL 0 MENUJU LEVEL 1

Subkategori NIST CSF yang akan diterapkan	*Current profile*	*Target profile*	*Rencana aksi*
PR.IP-5	0	3	• Mengidentifikasi gangguan pada lingkungan operasional baik yang disengaja (*malicious*) maupu tidak disengaja (*non-malicious*) • Mendokumentasikan dan melakukan pengujian terhadap prosedur yang mencakup peringatan terhadap gangguan lingkungan operasional • Membandingkan pengukuran dan rencana kontingensi terhadpa hasil laporan dan persyaratan kebijakan secara tepat waktu saat ditemukan ketidakpatuhan prosedur
PR.AC-2	0	3	
PR.AC-3	0	3	

Subkategori NIST CSF yang akan diterapkan	*Current profile*	*Target profile*	*Rencana aksi*
PR.DS-1	0	3	• Membuat permintaan perubahan konfigurasi dilakukan secara formal • Mengkategorikan seluruh oermintaan perubahan (seperti proses bisnis, infrastruktur, sistem operasi, jaringan, sistem aplikasi, *software package*) • Memprioritaskan semua perubahan atau konfigurasi yang diminta berdasarkan persyaratan bisnis dan teknis, sumber daya yang diperlukan dan hukum, peraturan, serta alasan kontraktual terhadap perubahan yang diminta
PR.IP-3	0	3	

Rencana aksi level 1 menuju level 2

Rencana aksi seperti pada Tabel 6. disusun berdasarkan *Generic Practices* (GP) dan *Generic Work Product* (GWP) level 2 pada COBIT 5 PAM.

TABEL 6.
RENCANA AKSI LEVEL 1 MENUJU LEVEL 2

No	Rencana aksi	Hasil
1.	Mengidentifikasi tujuan dan ruang lingkup proses	Dokuemn/pedoman yang menerangkan ruang lingkup pelaksanaan proses
	Mendefinisikan kewenangan dan tanggung jawab dalam melaksanakan proses dengan mengacu pada RACI *chart* COBIT 5	
	Menjalin komunikasi yang baik dengan pihak-pihak yang terlibat dalam proses dengan menyusun mekanisme proses komunikasi	
	Mendokumentasikan rincian kontrol terhadap *output* proses dalam dokumen perencanaan proses atau *Quality plan*	
	Mengidentifikasi tujuan dan ruang lingkup proses	Dokumen perencanaan proses yang mencakup sasaran proses yang dilaksanakan
	Merencanakan rincian sasaran yag akan dicapai pada setiap proses	
	Menyusun standar kompetensi yang mencakup definisi pengalaman, pengetahuan, dan keahlian yang dibutuhkan	
	Mengidentifikasi dan memastikan ketersediaan sumberdaya termasuk informasi yang dibutuhkan dalam melaksanakan proses	
	Menjalin komunikasi yang baik dengan pihak-pihak yang terlibat dalam proses	

Rencana aksi level 2 menuju level 3

Rencana aksi seperti pada Tabel 7. disusun berdasarkan *Generic Practices* (GP) dan *Generic Work Product* (GWP) level 2 pada COBIT 5 PAM.

TABEL 7.
RENCANA AKSI LEVEL 2 MENUJU LEVEL 3

No	Rencana aksi	Hasil
1.	Mengidentifikasi elemen dasar yang diperlukan dalam pembuatan standar proses meliputi rincian sasaran proses, standar minimum kinerja proses, SOP, dan persyaratan laporan *monitoring*	Dokumen standar dan kebijakan pelaksanaan proses
	Menentukan pembagian tugas dan kompetensi yang dibutuhkan dalam setiap proses dan mencantumkannya dalam standar proses yang dibuat	
	Mengidentifikasi kebutuhan infrastruktur (fasilitas, *tools*, metode dll) serta lingkungan implementasi proses dan mencantumkannya dalam standar proses	
	Menentukan metode evaluasi terhadap kesesuaian standar proses yang dibuat (*audit internal* atau *management review*)	
	Menentukan metode/atribut pengukuran yang dapat dilakukan untuk memastikan apakah proses yang diterapkan sesuai dengan standar proses yang dibuat	
	Mengkomunikasikan kewenangan dan tanggung jawab yang telah disusun dalam standar proses kepada *stakeholder* terkait	
2.	Memastikan bahwa standar kompetensi untuk implementasi proses yang dicantumkan dalam standar proses ditentukan dengan tepat	Dokumen yang menerangkan ruang lingkup pelaksasnaan proses

5. Kesimpulan

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa *current profile* UO ABC mencapai *tier* 1 (level 0 dan 1 COBIT 5 PAM) NIST CSF yang berarti, proses manajemen risiko organisasi belum terbentuk secara formal. Setelah diketahui bahwa UO ABC memiliki 13 risiko tinggi dan 12 risiko sedang yang mungkin terjadi pada sistem informasi XYZ, UO ABC menentukan 5 subkategori NIST CSF akan diterapkan sebagai mitigasi risiko dengan 5 *enabler process* COBIT 5 sebagai proses tambahan. Penerapan subkategori tersebut ditargetkan untuk mencapai *tier* 3 NIST CSF agar organisasi dapat menuangkan proses *cyber-risk management* sistem informasi XYZ dalam sebuah kebijakan resmi sehingga prosesnya dapat dilakukan secara formal.

Rencana aksi yang dihasilkan untuk menuju *tier* 3 disusun sesuai dengan indikator pencapaian proses pada setiap level. Secara umum pada level 0 dan 1 (*tier* 1) UO ABC akan mencapai *outcomes* proses yang diimplementasikan. Pada level 2 (*tier 2*) UO ABC akan mencapai kondisi bahwa proses disetujui untuk diterapkan namun belum memiliki kebijakan yang mengaturnya. Pada level 3 UO ABC akan mencapai kondisi bahwa organisasi memiliki kebijakan yang mengatur bagaimana proses diimplementasi.

Referensi

Jurnal

[2] Y. Chen, P. P. Chong, and B. Zhang, "Cyber security management and e-government," vol. 1, no. 3, pp. 316–327, 2004.

[4] M. J. Hutchins, R. Bhinge, M. K. Micali, S. L. Robinson, J. W. Sutherland, and D. Dornfeld, "Framework for Identifying Cybersecurity Risks in Manufacturing," *Procedia Manuf.*, vol. 1, pp. 47–63, 2015.

[5] I. Rahmawati, "Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense," *J. Pertahanan dan Bela Negara*, vol. 7, no. 2, pp. 51–66, 2017.

Publikasi elektronik atau informasi dari internet

[8] Kominfo, "Tren Serangan Siber Nasional 2016 dan Prediksi 2017," 2017. https://www.owasp.org/images/4/47/Iwan-OWASP-Cyber-Security-Trends-2017.pdf

[12] F. Wamala, *ITU National Cybersecurity Strategy Guide*. 2011. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

[13] NIST, "Framework for Improving Critical Infrastructure Cybersecurity Version 1.0," United State, 2014. https://www.nist.gov/document-3766

Buku

[1] A. Refsdal, B. Solhaug, and K. Stolen, *Cyber-Risk Management*. 2015.

[14] ISACA, *COBIT 5 Enabling Processes*. 2012.

[15] ISACA, *Process Assessment Model (PAM): Using COBIT ® 5*. 2013.

[16] ISACA, *Self-assessment Guide: Using COBIT ® 5*. Canada, 2013.

[17] ISACA, *Using COBIT 5 for Risk Management*, vol. 4, no. October. 2013.

[18] ISACA, *Implementing The NIST Cybersecurity Framework*. 2014.

Tugas Akhir

[3] C. W. Hardani, *Analisis Risiko Flight Clearance Information System Menggunaka Risk Scenario COBIT 5 for Risk dan NIST SP 800-30 Revisi 1*. 2016.

Paper dan Laporan

[6] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, pp. 2–7, 2013.

Data Spesial

[7] Peraturan internal. 2014, pp. 1–64.

[9] Peraturan internal. 2014, pp. 1–250.

[10] Peraturan internal. 2011, pp. 4–19.

[11] Laporan internal, "Sistem informasi XYZ" 2017.