Cyber-Risk Management Menggunakan NIST *Cybersecurity Framework* (CSF) dan COBIT 2019 pada Instansi XYZ

Andhika Sigit Julianto[1)], Ira Rosianal Hikmah[2)], Ray Novita Yasa[3)]

(1) Jurusan Keamanan Siber, Politeknik Siber dan Sandi Negara, andhika.sigit@bssn.go.id

(2) Jurusan Keamanan Siber, Politeknik Siber dan Sandi Negara, ira.rosianal@poltekssn.ac.id

(3) Jurusan Kriptografi, Politeknik Siber dan Sandi Negara, ray.novita@poltekssn.ac.id

Abstrak

Perkembangan teknologi saat ini memicu perusahaan atau organisasi untuk menggunakan Teknologi Informasi (TI) sebagai basis layanan dan optimalisasi proses bisnis. TI dapat memberi peluang di sektor pemerintah untuk melakukan pembangunan aparatur negara melalui penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE). Instansi Pusat dan Pemerintah Daerah telah menerapkan SPBE dan memberikan kontribusi efisiensi dan efektivitas penyelenggaraan pemerintah. Untuk menjamin keberlangsungan SPBE dan mengurangi dampak risiko merupakan tujuan dari manajemen risiko, dengan proses identifikasi, analisis, pengendalian, pemantauan, dan evaluasi terhadap risiko berdasarkan manajemen risiko yang ditetapkan pemerintah. Instansi XYZ merupakan instansi yang bergerak di bidang komunikasi dan informasi, persandian serta statistik. Instansi XYZ juga melakukan penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE). Pada penelitian ini, dilakukan perancangan cyber-risk management dengan menggunakan NIST CSF dan COBIT 2019. Dalam melakukan perancangan cyber-risk management, menggunakan 6 tahapan yaitu Prioritized and Scope, Orient, Create a Current Profile, Conduct Risk Assessment, Create a Target Profile, dan Determine, Analyze and Prioritize Gaps. Pada penelitian ini, terdapat 28 aset, 17 ancaman, 13 kerentanan dan 12 kontrol yang telah diterapkan. Dengan hasil tersebut didapatkan 111 risiko, terdapat 35 risiko dengan kategori tinggi, 63 risiko dengan kategori sedang, dan 13 risiko dengan kategori rendah. Hasil akhir dari penelitian ini adalah penyusunan rancangan cyber-risk management dengan mengelompokkan aksi-aksi yang telah direkomendasikan berdasarkan Work Products (WP) dan Generic Work Products (GWP) yang menjadi satu program kerja untuk Instansi XYZ.

Kata kunci: cyber risk management, NIST CSF, COBIT 2019, SPBE, penilaian risiko

Abstract

Current technological developments trigger companies or organizations to use Information Technology (IT) as a service base and optimize business processes. IT can provide opportunities in the government sector to develop state apparatus through implementing the Electronic-Based Government System (SPBE). Central and Local Government Agencies have implemented SPBE and contributed to the efficiency and effectiveness of government administration. Ensuring the sustainability of SPBE and reducing the impact of risk is the goal of risk management, with a process of identification, analysis, control, monitoring, and evaluation of risks based on risk management determined by the government. XYZ Agency is an agency that operates in the fields of communication and information, coding and statistics. XYZ Agency also implemented an Electronic Based Government System (SPBE). In this study, cyber-risk management was designed using NIST CSF and COBIT 2019. In designing cyber-risk management, using 6 stages, namely Prioritized and Scope, Orient, Create a Current Profile, Conduct Risk Assessment, Create a Target Profile, and Determine, Analyze, and Prioritize Gaps. In this study, there are 28 assets, 17 threats, 13 vulnerabilities, and 12 controls implemented. With these results obtained 111 risks, there are 35 risks in the high category, 63 risks in the medium category, and 13 risks in the low category. The final result of this research is the preparation preparation of a cyber-risk management design by grouping the recommended actions based on Work Products (WP) and Generic Work Products (GWP) which become a work program for XYZ Agency.

Keywords: cyber risk management, NIST CSF, COBIT 2019, SPBE, risk assessment

1. PENDAHULUAN

Perkembangan teknologi saat ini memicu perusahaan atau organisasi untuk menggunakan Teknologi Informasi (TI) sebagai basis layanan dan optimalisasi proses bisnis. Strategi perencanaan untuk penerapan teknologi informasi dibutuhkan agar dapat selaras dengan bisnis perusahaan atau organisasi. Organisasi dapat terhambat proses bisnisnya dan mengalami kerugian finansial apabila tidak menerapkan TI dengan baik [1]. TI dapat memberi peluang di sektor pemerintah untuk melakukan pembangunan aparatur negara melalui penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE). Instansi Pusat dan Pemerintah Daerah telah menerapkan SPBE dan memberikan kontribusi efisiensi dan efektivitas penyelenggaraan pemerintah [2].

Pelaksanaan SPBE bergantung pada penggunaan teknologi, peraturan undang-undang yang berkaitan dengan SPBE dan keamanan informasi, serta risiko keamanan informasi. Keamanan informasi merupakan suatu kegiatan atau proses untuk melindungi aspek kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) dari suatu aset informasi [2]. Dalam mengatasi risiko keamanan informasi, dapat dilakukan manajemen keamanan informasi yang bertujuan untuk memberi

perlindungan terhadap informasi dan aset organisasi [3]. Manajemen keamanan informasi pada SPBE bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak dari risiko keamanan informasi [3].

Keamanan siber adalah perlindungan yang dilakukan pada sistem siber terhadap ancaman siber [4]. Penerapan SPBE dalam pemerintah pusat dan pemerintah daerah dapat menjadi target terhadap ancaman atau serangan siber yang banyak menyimpan data pribadi masyarakat [5]. Berdasarkan hasil penelusuran di situs komunitas peretas global, terdapat 33.748 kali peretasan terhadap situs yang memiliki domain .go.id atau domain resmi lembaga negara dalam kurun waktu 1 Desember 2020 sampai 4 Agustus 2021 [6]. Situasi tersebut penting bagi instansi pemerintah untuk menerapkan *cyber-risk management* dalam mengelola risiko yang diakibatkan oleh ancaman siber [7].

Instansi XYZ merupakan instansi yang bergerak di bidang komunikasi dan informasi, persandian serta statistik. Instansi XYZ melakukan penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE). Di Indonesia, terdapat Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik, bahwa setiap penyelenggaraan sistem elektronik harus menerapkan manajemen risiko untuk kerusakan dan gangguan yang ditimbulkan [8].

Risiko siber adalah potensi paparan terhadap kerugian atau bahaya yang berasal dari sistem informasi atau komunikasi organisasi. Selain itu, risiko siber memiliki dua tipe ancaman siber yaitu ancaman eksternal dan internal. Ancaman eksternal berarti berasal dari luar organisasi, seperti serangan DDoS, *phising*, dan *ransomware*. Pada ancaman internal, biasanya terdapat kesalahan dari karyawan atau orang di organisasi tersebut yang melakukan kejahatan [9]. Penerapan manajemen risiko menawarkan organisasi untuk mengukur program keamanan siber dalam mengelola risiko agar dapat dimitigasi [10]. Untuk menjelaskan kebutuhan keamanan siber pada organisasi, dibutuhkan kerangka kerja yang dapat digunakan oleh organisasi di sektor manapun seperti NIST *Cybersecurity Framework* (CSF) [11].

NIST CSF dirancang untuk mengikuti perkembangan dari perubahan ancaman, proses, dan teknologi keamanan siber. Kerangka kerja ini dapat digunakan untuk mengurangi dan mengelola risiko keamanan siber dengan lebih baik. NIST CSF menjadi pedoman berbasis risiko dalam membantu organisasi melakukan identifikasi, implementasi, dan meningkatkan praktik keamanan siber. Kerangka kerja yang dirancang tersebut memiliki tiga bagian yaitu *Framework Core*, *Framework Implementation Tiers*, dan *Framework Profile* [11]. NIST CSF merupakan kerangka kerja yang fleksibel untuk digunakan dengan beragam proses manajemen risiko keamanan siber. Dalam proses manajemen risiko, terdapat penilaian risiko untuk menetapkan kemungkinan terjadinya kejadian. Pada penelitian ini, NIST SP 800-30 digunakan untuk melakukan penilaian risiko pada organisasi dan memberikan panduan dalam melaksanakan setiap langkah dalam proses penilaian [12]. Penggunaan NIST CSF bergantung pada kerangka kerja lain untuk mendukung penerapannya [11]. NIST CSF berfokus sebagai guide *cybersecurity activities* dan mempertimbangkan risiko keamanan siber sebagai bagian dari proses dalam manajemen risiko. NIST CSF dikembangkan untuk meningkatkan manajemen risiko dan dapat digunakan untuk organisasi di semua sektor, terlepas dari ukuran, tingkat risiko keamanan siber, atau kecanggihan keamanan siber. Organisasi dapat menentukan hal-hal yang penting dalam kegiatan untuk dapat memprioritaskan di bidang keamanan siber sehingga NIST CSF digunakan untuk mengurangi dan mengelola risiko keamanan siber dengan baik [13].

COBIT 2019 merupakan kerangka kerja untuk membantu tata kelola dan manajemen informasi serta teknologi organisasi. COBIT 2019 memiliki dua prinsip yaitu prinsip yang menjelaskan persyaratan inti dari sistem tata kelola untuk informasi dan teknologi organisasi, serta prinsip kerangka tata kelola untuk membangun sistem tata kelola organisasi. COBIT 2019 merupakan komponen untuk membangun dan mempertahankan sistem tata kelola dengan mempertimbangkan faktor desain [14]. COBIT 2019 mengelompokkan komponen tata kelola yang relevan ke dalam tujuan tata kelola dan manajemen yang dapat dikelola hingga tingkat kemampuan yang diperlukan. COBIT 2019 menggunakan COBIT *Performance Management* (CPM) untuk mengetahui tingkat kemampuan dan tingkat kematangan pada organisasi. Terdapat peningkatan pada COBIT 2019 dari versi sebelumnya, yaitu COBIT 5. COBIT 2019 menggunakan faktor desain untuk dapat menyesuaikan dengan kondisi perusahaan sedangkan COBIT 5 belum menggunakan faktor desain sehingga tidak dapat menyesuaikan dengan kemajuan zaman dan tidak ada acuan untuk keselarasan dengan perusahaan. Selain itu, domain pada COBIT 5 masih menyatakan bahwa proses tidak menekankan pada hasil saja, sedangkan pada COBIT 2019 selain domain lebih lengkap karena adanya penambahan, COBIT 2019 juga lebih menekankan pada hasil yang dicapai sehingga lebih terarah.

Berdasarkan penjelasan di atas, penelitian ini akan melakukan perancangan *Cyber-risk Management* dengan menggunakan NIST CSF dan COBIT 2019 pada Instansi XYZ sebagai kerangka kerja dan panduan tata kelola. Hasil yang diharapkan penelitian ini berupa profil target pada organisasi terhadap keamanan siber, nilai risiko, dan rancangan *cyber-risk management*.

2. LANDASAN TEORI

2.1 *Cyber-Risk Management*

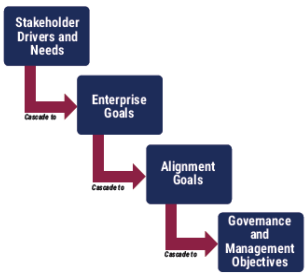
Risiko merupakan potensi terjadinya suatu kesalahan atau insiden yang dapat menyebabkan kerugian terhadap suatu aset [4]. Risiko siber adalah potensi paparan terhadap kerugian atau bahaya yang berasal dari sistem informasi atau komunikasi organisasi. Selain itu, risiko siber memiliki dua tipe ancaman siber yaitu ancaman eksternal dan internal [4]. *Cyber-risk management* berkaitan dengan risiko yang disebabkan oleh ancaman siber. Ancaman siber yang menyebabkan terjadinya risiko disebut risiko siber. Dalam melaksananan *cyber-risk management*, harus dilakukan penilaian risiko siber (*Cyber-risk Assessment*) yang memiliki lima tahapan di dalamnya yaitu, pembentukan konteks (*Context Establishment*), identifikasi risiko (*Risk Identification*), analisis risiko (*Risk Analysis*), evaluasi risiko (*Risk Evaluation*), dan perlakuan risiko (*Risk Treatment*) [4].

2.2 NIST CSF

NIST CSF dikembangkan untuk meningkatkan manajemen risiko dan dapat digunakan untuk organisasi di semua sektor, terlepas dari ukuran, tingkat risiko keamanan siber, atau kecanggihan keamanan siber. Organisasi dapat menentukan hal-hal yang penting dalam kegiatan untuk dapat memprioritaskan di bidang keamanan siber sehingga NIST CSF digunakan untuk mengurangi dan mengelola risiko keamanan siber dengan baik [11]. NIST CSF memiliki pendekatan berbasis risiko dalam mengelola risiko keamanan siber yang terdiri dari tiga bagian yaitu *Framework Core, Framework Implementation Tiers,* dan *Framework Profile* [11].

2.3 COBIT 2019

COBIT 2019 merupakan kerangka kerja untuk membantu tata kelola dan manajemen informasi dan teknologi organisasi. COBIT 2019 memiliki dua prinsip yaitu prinsip yang menjelaskan persyaratan inti dari sistem tata kelola untuk informasi dan teknologi organisasi dan prinsip kerangka tata kelola untuk dapat digunakan dalam membangun sistem tata kelola organisasi [14]. Kebutuhan *stakeholder* harus terus diubah dan dijadikan strategi perusahaan. *Goal cascade* memiliki empat tahapan untuk mendukung tujuan perusahaan.

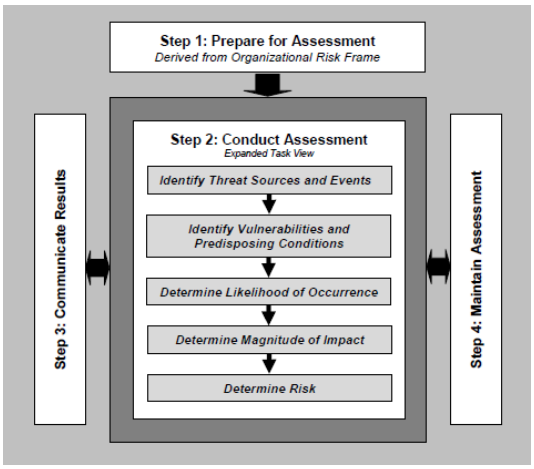


Gambar 1. *Goals Cascade* COBIT 2019 [14]

Setiap *Governance and Management Objective* akan berkaitan dengan suatu proses. Proses tersebut digunakan untuk mencapai suatu tujuan tata kelola dan manajemen. *Core Model* mewakili semua proses yang berkaitan dengan TI pada perusahaan. Terdapat 40 proses tata kelola dan manajemen pada *Core Model* COBIT 2019.

2.4 NIST SP 800-30

NIST SP 800-30 bertujuan untuk memberikan panduan dalam melakukan penilaian risiko. Terdapat beberapa langkah dalam proses penilaian risiko yaitu mempersiapkan penilaian risiko (*preparing for the risk assessment*), melakukan penilaian risiko (*conducting the risk assessment*), mengomunikasikan hasil penilaian risiko (*communicating the results of the risk assessment*), dan mempertahankan penilaian risiko (*maintaining the risk assessment*).



Gambar 2. Proses Penilian Risiko [12]

2.5 COBIT 5 PAM

COBIT 5 PAM (*Process Assessment Model*) merupakan proses kapabilitas dengan berdasarkan pada model dua dimensi sesuai dengan persyaratan ISO/IEC 15504-2. Dimensi pertama yaitu dimensi proses yang didefinisikan dan diklarifikasikan dalam kategori proses COBIT 5. Kategori proses tersebut didapatkan dari hasil *Goals Cascade* yang akan digunakan untuk menentukan proses yang akan dinilai. Dimensi kedua yaitu dimensi kapabilitas merupakan satu set atribut proses COBIT 5 yang dikelompokkan ke dalam skala kapabilitas pada COBIT 5 PAM [15].

3. METODE PENELITIAN

3.1 Objek

Objek penelitian ini adalah Bidang Aplikasi Informatika dan Bidang Infrastruktur Teknologi pada Instansi XYZ.

3.2 Tahapan Penelitian

Tahap penelitian menjelaskan secara rinci desain penelitian mulai dari persiapan, proses *cyber-risk*

management, metode pengumpulan data dan hasil yang didapatkan.

a. *Prioritize and Scope*

Pada tahap *Prioritize and Scope*, dilakukan identifikasi terhadap tujuan, misi, bisnis, struktur, dan tingkat prioritas di Instansi XYZ. Informasi tersebut dapat membuat keputusan terkait ruang lingkup, aset, dan prioritas sesuai dengan masalah yang dihadapi. Terdapat relasi pada COBIT 2019 dengan tahapan ini yaitu dengan COBIT 2019 *Goal Cascade* digunakan untuk membantu dalam menentukan domain *Governance and Management Objectives*. Pada tahap ini, dapat dilakukan dengan melakukan wawancara.

b. *Orient*

Tahap *Orient* dilakukan untuk mendapat informasi terkait dengan proses bisnis Instansi XYZ, mengidentifikasi aset dan sistem, dan melakukan pendekatan risiko sesuai dengan ruang lingkup. Pada tahap ini, dihasilkan daftar-daftar aset, ancaman, dan kerentanan. Tahap ini dilakukan dengan melakukan observasi.

c. *Create a Current Profile*

Tahap *Create a Current Profile* memiliki tujuan untuk mengetahui sejauh mana kondisi Instansi XYZ saat ini dengan cara menunjukkan hasil kategori dan subkategori. Pada tahap ini dapat menggunakan metode kuesioner untuk mendapatkan pengukuran dan pemetaan *tier* organisasi.

d. *Conduct a Risk Assessment*

Pada tahap *Conduct a Risk Assessment* dilakukan penilaian risiko untuk mengetahui kemungkinan peristwa keamanan siber dan dampak peristiwa bagi Instansi XYZ. Dalam melakukan penilaian risiko dilakukan berdasarkan NIST SP 800-30.

e. *Create a target Profile*

Tahap *Create a Target Profile* bertujuan untuk menentukan target Instansi XYZ dalam penerapan keamanan siber. Pada tahap menetukan profil target, ditentukan dengan mengacu pada level kapabilitas proses CPM yang disetarakan dengan *tier* pada NIST CSF. Untuk melakukan penentuan target dapat dilakukan dengan wawancara.

f. *Determine, Analyze, and Prioritize Gaps*

Tahap *Determine, Analyze, and Prioritize Gaps* bertujuan untuk melakukan analisis dengan membandingkan *current profile* dan *target profile*. Dari aksi-aksi yang telah direkomendasikan berdasarkan *Work Products* (WP) dan *Generic Work Products* (GWP), dikelompokkan menjadi satu program kerja.

4. HASIL DAN PEMBAHASAN

4.1 *Prioritize and Scope*

Dalam penelitian ini, ruang lingkup dan prioritas ditentukan dengan melihat visi misi organisasi, struktur organisasi, rencana strategis, dan arah kebijakan. Selanjutnya, ruang lingkup dan prioritas ditentukan oleh *enabler process* dari *proses Goal Cascade* COBIT 2019. *Goal Cascade* COBIT 2019 digunakan untuk menerjemahkan kebutuhan organisasi agar selaras. Sasaran strategis Instansi XYZ ditetapkan sebagai kebutuhan yang diselaraskan dengan *enterprise goals*. *Alignment Goals* terhadap *Governance and Management Objectives* dapat dilihat pada Tabel 1.

Tabel 1. *Alignment Goals* terhadap *Governance and Management Objectives*

Alignment Goals	Enabler Process COBIT 2019	Enabler Process COBIT 2019 yang selaras dengan NIST CSF	Hasil Pemetaan
AG02	EDM03	EDM01	**EDM03**
	APO12	EDM03	APO02
	DSS05	APO01	APO03
AG04	APO06	APO02	APO06
	BAI09	APO03	APO07
AG07	EDM02	APO06	APO08
	APO12	APO07	**APO11**
	APO13	APO08	**APO12**
	BAI10	APO10	APO13
	DSS04	APO11	BAI05
	DSS05	APO12	BAI09
AG08	APO02	APO13	BAI10
	APO03	APO20	DSS04
	BAI05	BAI01	**DSS05**
	DSS06	BAI02	DSS06
AG10	EDM05	BAI04	
	APO11	BAI05	
	APO13	BAI06	
	MEA01	BAI07	
AG12	APO07	BAI09	
	APO08	BAI10	
	BAI08	DSS01	
		DSS02	
		DSS03	
		DSS04	
		DSS05	
		DSS06	
		MEA03	

Didapatkan 19 *enabler process* yang selaras dengan Instansi XYZ. Sembilan belas *enabler process* tersebut dipetakan dengan 28 *enabler process* yang selaras dengan *cybersecurity outcomes* pada NIST CSF. Hasil pemetaan yang selaras antara keduanya kemudian menghasilkan 15 *enabler process*. Kemudian dari 15 *enabler process*, dipilih empat *enabler process* dengan ditandai cetak tebal pada kolom Hasil Pemetaan Tabel 1 yang sesuai dengan kebutuhan Instansi XYZ. Dari empat *enabler process* yang telah dipilih oleh Instansi XYZ akan dijadikan sebagai profil saat ini pada organisasi.

4.2 *Orient*

Identifikasi Aset dilakukan untuk mengetahui aset-aset yang dimiliki organisasi. Aset-aset didapatkan dari hasil observasi dan melihat dari dokumen yang dimiliki oleh organisasi. Daftar aset hasil identifikasi dapat dilihat pada Tabel 2.

Tabel 2. Daftar Aset

No.	Kategori Aset	Nama Aset	Kode Aset
1	Aplikasi	Aplikasi Pengaduan *Online*	A1
		Aplikasi *Dashboard* SmartCity	A2
		Portal Resmi (*website*)	A3
		Portal *Email* Resmi (*website*)	A4
		Aplikasi PPID	A5
		Aplikasi *eSign*	A6
		Aplikasi *Monitoring* Jaringan	A7
2	Informasi	Data Pegawai	A8
		Data Aplikasi	A9
		Data Statistik	A10
3	*Software*/ Perangkat Lunak	OS	A11
		VMware	A12
		Software Sign Box	A13
		Anti Virus	A14
		Google Cloud Storage	A15
4	*Hardware*/ Perangkat Keras	Komputer	A16
		Router Mikrotik CCR	A17
		Switch D-Link Managable	A18
		Access Point	A19
		Firewall Sangfor	A20
		UPS Server	A21
		Memory Server	A22
		RAM Server	A23
		Mail Server	A24
		Patch Panel	A25
5	SDM	Personil Bidang Aplikasi Informatika	A26
		Personil Bidang Infrastruktur Teknologi	A27
		Personil Bidang Persandian dan Statistik	A28

Identifikasi ancaman dilakukan untuk mengetahui ancaman yang dapat menyebabkan kerugian bagi organisasi. Ancaman yang dipilih merupakan ancaman yang pernah terjadi dengan melihat dokumen *Risk Register* pada Instansi XYZ. Daftar ancaman sebagai hasil tahapan identifikasi ancaman dapat dilihat pada Tabel 3.

Identifikasi kerentanan dilakukan untuk mengetahui kelemahan aset yang bisa dieksploitasi oleh suatu ancaman. Kerentanan yang ditentukan merupakan kerentanan yang pernah terjadi dengan melihat dokumen *Risk Register* pada Instansi XYZ. Daftar kerentanan sebagai hasil tahapan identifikasi kerentanan dapat dilihat pada Tabel 4.

4.3. *Create a Current Profile*

Pada tahap ini, ditentukan *current profile* yang ada di Instansi XYZ. *Current profile* dapat ditentukan dengan tingkat kapabilitas pada COBIT 2019. Empat *enabler process* yang telah ditentukan sebelumnya pada tahap *Prioritize and Scope* menghasilkan 67 subkategori NIST CSF. Terdapat tingkat kapabilitas pada masing-masing *level* dan rekapitulasi pada nilai kapabilitas. Penelitian ini berfokus pada *level* 1 dan *level* 2 dimana pada *level* tersebut, subkategori harus ditingkatkan untuk menjadi profil target organisasi. Diketahui status implementasi dari subkategori NIST CSF bahwa tujuh subkategori *fully achieved* dengan presentase 90%, tujuh subkategori *partially achieved* dengan presentase 45% dan 15%, serta dua subkategori belum diimplementasikan pada *level* 1. Selanjutnya, tujuh subkategori fully achived pada *level* 1 yang dinyatakan memenuhi, penilaian dilanjutkan pada *level* 2. Hasil penilaian *level* 2 menunjukkan bahwa satu subkategori *largely achieved* dan enam subkategori *partially achieved*.

Tabel 3. *Daftar Ancaman*

No.	Nama Ancaman	Kode Ancaman
1	DDoS, DoS	T1
2	*Malware*	T2
3	Penyalahgunaan Protokol	T3
4	SQL *Injection*	T4
5	Perangkat Rusak	T5
6	*Phising*	T6
7	*Defacement*	T7
8	Penyusupan Siber	T8
9	*Spam*	T9
10	Kesalahan SDM	T10
11	Kehilangan Data	T11
12	Pencurian Data	T12
13	Modifikasi Data	T13
14	*Social Engineering*	T14
15	Terdapat *Downtime*	T15
16	Kesulitan dalam *Tracking* Insiden	T16
17	Kegagalan Penanganan Insiden	T17

Tabel 4. *Daftar Kerentanan*

No.	Nama Kerentanan	Kode Kerentanan
1	Penggunaan *password* lemah	V1
2	*Password* tidak diganti secara berkala	V2
3	*Sharing password*	V3
4	Kurangnya inventarisasi dan pembaruan perangkat	V4
5	Tidak melakukan logout setelah menggunakan akun	V5
6	Tidak melakukan pengujian keamanan secara berkala	V6
7	Kesalahan kode pada pemrograman	V7
8	Kesalahan konfigurasi	V8
9	Konfigurasi tidak sesuai prosedur	V9
10	Menggunakan konfigurasi *default*	V10
11	Tidak melakukan *backup* secara berkala	V11
12	Tidak melakukan *update system* secara berkala	V12
13	Kurangnya pengetahuan SDM	V13

4.4. *Conduct a Risk Assessment*

Risk determination dilakukan untuk mengetahui nilai akhir risiko berdasarkan hasil dari identifikasi kemungkinan risiko dan identifikasi dampak risiko. Pada penelitian ini, terdapat 111 risiko, yang sebagian *risk determination*-nya dapat dilihat pada Tabel 5.

4.5. *Create a Target Profile*

Pada tahap ini dilakukan penentuan *target profile* yang ingin dicapai berdasarkan *current profile* dan penilaian risiko. Berdasarkan kategori *generic risk scenario*, mitigasi risiko dapat dilakukan dengan *enabler process* COBIT 2019. *Enabler process* tersebut ditentukan berdasarkan hasil dari *goal cascade* yang sudah diketahui dan nilai kapabilitas pada tahap *create a current profile*. *Enabler process* yang telah ditentukan dipetakan berdasarkan kategori *generic risk scenario* dimana *enabler process* tersebut merepresentasikan subkategori pada NIST CSF. Selanjutnya, *enabler process* dipilih oleh Instansi XYZ sehingga diperoleh 12 *enabler process* yang merepresentasikan 20 subkategori NIST CSF. Instansi XYZ menentukan *target profile* dalam menerapkan 20 subkategori NIST CSF tersebut. Instansi XYZ melihat bahwa 20 subkategori tersebut dalam nilai kapabilitasnya masih di bawah *level* 3. Oleh karena itu, Instansi XYZ menyatakan bahwa 20 subkategori tersebut akan ditingkatkan menuju *level* 3. Dengan demikian, hal tersebut menunjukkan bahwa *level* yang ditargetkan oleh organisasi adalah *level* 3.

4.6. *Determine, Analyze, and Prioritize Gap*s

Tahap ini merupakan analisis *gap* dengan membandingkan *current profile* dan *target profile* yang sebelumnya telah ditentukan. Prioritas *gap* dilakukan untuk mencapai *target profile* yang diinginkan yaitu pada *level* 3 di setiap subkategori. Analisis *gap* dilakukan terhadap setiap subkategori yang dipilih sebelumnya.

Tabel 5. *Sebagian Risk Determination*

Kode Risiko	Kode Aset	Kode Ancaman	Kode Kerentanan	Nilai Risiko
R1	A1	T1	V6	Sedang
R2		T2	V12	Sedang
R3		T4	V6	Rendah
R4		T8	V5	Sedang
R5		T15	V12	Tinggi
R6	A2	T1	V6	Sedang
R7		T2	V12	Sedang
R8		T4	V6	Rendah
R9		T8	V5	Sedang
R10		T15	V12	Tinggi
...	...	...	...	...
R109	A28	T10	V13	Tinggi
R110		T14	V13	Tinggi
R111		T17	V13	Tinggi

Selanjutnya, ditentukan rencana aksinya. Kemudian, diperoleh program kerja untuk mengelola risiko siber dengan melihat aktivitas yang dijelaskan pada COBIT 5 *Process Assessment Model* (PAM). Penyusunan tersebut dilakukan dengan mengelompokkan aksi-aksi yang telah direkomendasikan berdasarkan *Work Products* (WP) dan *Generic Work Products* (GWP) yang menjadi satu program kerja.

Tabel 6. *Contoh Rekomendasi Perancangan pada Subkategori ID.RA-6 dan ID.RM-1*

Kode Program	01
Subkategori yang Diterapkan	ID.RA-6, ID.RM-1
Keterangan	Respon risiko diidentifikasi dan diprioritaskan, proses manajemen risiko ditetapkan, dikelola, dan disetujui oleh pemangku kepentingan organisasi
Enabler Process COBIT 2019 yang Relevan	APO13.02
Rekomendasi Aktivitas	1. Pembuatan kebijakan dan standar operasi yang merupakan bagian dari Sistem Manajemen Keamanan Informasi (SMKI). 2. Melakukan strategi dan dokumentasi perencanaan SMKI. 3. Melakukan penilaian risiko berdasarkan profil risiko. 4. Kasus bisnis keamanan informasi apalagi diperlukan untuk program keamanan informasi. 5. Mengelola pelaporan audit internal keamanan informasi yang diintegrasikan ke dalam sistem pelaporan. 6. Melakukan pemantauan dan pelaporan pada SMKI
Hasil	1. Membuat rencana penanganan risiko keamanan informasi 2. Kasus bisnis keamanan informasi
Prioritas	Tinggi
Penanggung Jawab Program	Bidang Persandian dan Statistik

Setiap program kerja berisi kode program, subkategori yang diterapkan, keterangan, *enabler process* COBIT 2019 yang relevan, rekomendasi aktivitas, hasil, prioritas, dan penanggung jawab program. Prioritas dan penanggung jawab program ditentukan oleh Instansi XYZ. Tabel 6 merupakan contoh program kerja untuk mengelola risiko siber yang direkomendasikan setiap subkategori.

5. KESIMPULAN

Berdasarkan tahapan yang dilakukan untuk perancangan *cyber-risk management* menggunakan NIST CSF dan COBIT 2019 pada Instansi XYZ, diperoleh beberapa kesimpulan. Berdasarkan hasil *Goals Cascade*, dari 15 *enabler process* dipilih empat *enabler process* yang sesuai dengan kebutuhan Instansi XYZ. Empat e*nabler process* tersebut dijadikan sebagai profil organisasi saat ini. Terdapat tingkat kapabilitas pada setiap *level* dan rekapitulasi pada nilai kapabilitas dengan tujuh subkategori *fully achieved* dengan presentase 90%, tujuh subkategori *partially achieved* dengan presentase 45% dan 15%, serta dua subkategori belum diimplementasikan pada *level* 1. Tujuh subkategori *fully achived* pada *level* 1 dinyatakan memenuhi sehingga penilaian dilanjutkan pada *level* 2. Hasil penilaian *level* 2 menunjukkan bahwa satu subkategori *largely achieved* dan enam subkategori *partially achieved*.

Hasil dari identifikasi aset, ancaman, dan kerentanan yang ada menjadi acuan untuk mengidentifikasi risiko. Selanjutnya, ditentukan nilai

risiko berdasarkan matriks penentuan risiko dan didapatkan bahwa dari 111 risiko, terdapat 35 risiko dengan kategori tinggi, 63 risiko dengan kategori sedang, dan 13 risiko dengan kategori rendah. Terdapat 98 risiko yang dikategorikan ke dalam lima *generic risk scenario* yaitu 29 risiko dengan kategori serangan logis, 12 risiko dengan kategori manajemen data dan informasi, 9 risiko dengan kategori kegagalan perangkat lunak, 39 risiko dengan kategori insiden perangkat keras, serta 9 risiko dengan kategori keahlian, keterampilan, dan perilaku TI.

Instansi XYZ melihat bahwa 20 subkategori NIST CSF, nilai kapabilitasnya masih di bawah *level* 3. Oleh karena itu, Instansi XYZ menyatakan bahwa 20 subkategori tersebut ditingkatkan ke *level* 3. Apabila disetarakan dengan *tier* NIST CSF maka berada pada *tier* 3. Penyusunan program kerja dilakukan dengan mengelompokkan aksi-aksi yang telah direkomendasikan berdasarkan *Work Products* (WP) dan *Generic Work Products* (GWP) yang menjadi satu program kerja. Aksi-aksi tersebut didapatkan dari setiap subkategori dan *enabler process* berdasarkan COBIT 5 PAM. Dari 20 subkategori, didapatkan 12 program kerja sebagai rekomendasi dalam mengelola risiko siber pada Instansi XYZ.

REFERENSI

[1] P. Burnap, "Risk Management and Governance," dalam *The Cyber Security Body of Knowledge*, vol. 1.0, A. Rashid, H. Chivers, G. Danezis, E. Lupu, dan A. Martin, Ed., Bristol: The National Cyber Security Centre, 2019, 2, hlm. 19–48.

[2] Pemerintah Kabupaten Bogor, "Peraturan Bupati Bogor Nomor 63 Tahun 2020 Tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik," 2020, *Bogor*.

[3] B. Supradono, "Manajemen Risiko Keamanan Informasi dengan Menggunakan Metode Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation)," *Media Elektrika*, vol. 2, no. 1, hlm. 4–8, Jun 2009.

[4] A. Refsdal, B. Solhaug, dan K. Stolen, *Cyber-Risk Management*. London: Springer, 2015.

[5] S. C. Dewanti, "Urgensi pembenahan Sistem Keamanan Siber Pemerintah," *Info Singkat: Kajian Singkat Terhadap Isu Aktual Dan Strategis*, vol. 13, no. No.9/II/Puslit/Agustus/2021, hlm. 25–30, Agu 2021.

[6] K. Y. Rahayu, "Laman Daring Pemerintah Jadi Sasaran Empuk Peretasan," Jakarta, Agu 2021.

[7] W. Miron dan K. Muita, "Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure," *Technology Innovation Management Review*, hlm. 33–39, Okt 2014.

[8] Pemerintah Republik Indonesia, "Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik," 2019, *Jakarta*.

[9] G. Strupczewski, "Defining cyber risk," *Saf Sci*, vol. 135, hlm. 1–10, Mar 2020.

[10] P. Taveras, "Cyber Risk Management, Procedures and Considerations to Address the Threats of a Cyber Attack," dalam *Proceedings of the ForenSecure: Cybersecurity and Forensics Conference*, Chicago, Apr 2019, hlm. 1–10.

[11] National Institute of Standards and Technology, "Cybersecurity Framework," dalam *Framework for Improving Critical Infrastructure Cybersecurity*, vol. 1.1, 2018.

[12] R. M. Blank dan P. D. Gallagher, *Information Security*. Gaithersburg: National Institute of Standards and Technology, 2012.

[13] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," Apr 2018.

[14] ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*. Schaumburg, 2018.

[15] ISACA, *COBIT® 5 Supplementary guide for the COBIT 5 Process Assessment Model (PAM)*. Schaumburg, 2012.