Indonesian Journal of Computer Science
ISSN 2302-4364 (*print*) dan 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam, No. 1, Padang, Indonesia, Telp. (0751) 7056199, 7058325
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

Cybersecurity Improvement Design in Critical Infrastructure PT XYZ a Case Study

Adi Gunawan[1], Rizal Fathoni Aji[2]
fahrizaladigunawan@gmail.com, rizal@cs.ui.ac.id
[1]Fakultas Ilmu Komputer, Universitas Indonesia
[2]Fakultas Ilmu Komputer, Universitas Indonesia

Informasi Artikel

Diterima : 21 Des 2023
Direview : 23 Des 2023
Disetujui : 30 Des 2023

Kata Kunci

Critical Infrastructure, Keamanan Siber, Penilaian Risiko, NIST.

Abstrak

Pencegahan terhadap serangan siber menjadi faktor penting yang perlu dilakukan organisasi untuk menungjang keberlangsungan proses bisnis yang maksimal. Salah satu faktor penting yang diperlukan adalah perlindungan aset-aset data dan informasi oleh *critical infrastructure* yang dimiliki. Paper ini membahas mengenai peningkatan kapasitas *critical infrastructure* pada organisasi XYZ. Kerangka kerja NIST CSF sebagai alat penilaian tolak ukur terhadap kapasitas *critical infrastructure* di PT XYZ tersebut. Hasil yang didapatkan dari Penilaian digunakan untuk membuat rekomendasi terhadap kontrol-kontrol yang berhubungan dengan *critical infrastructure*. Penilaian risiko yang menemukan 107 macam skenario risiko yang membawa pada 11 rekomendasi area peningkatan *critical infrastructure*. Pembuatan prioritas pada rekomendasi yang dihasilkan diharapkan dapat meningkatkan ketahanan dan kapasitas critical infrastructure di PT XYZ dalam menghadapi ancaman kejahatan siber saat ini dan masa depan.

Keywords

Critical Infrastructure, Cyber Security, Risk Assessment, NIST.

Abstract

Prevention of cyber attacks is an important factor that organizations need to do to support maximum business process continuity. One of the important factors needed is the protection of data and information assets by the critical infrastructure owned. This paper discusses increasing the capacity of critical infrastructure at XYZ organization. The NIST CSF framework is a benchmark assessment tool for critical infrastructure capacity at PT XYZ. The results obtained from the assessment are used to make recommendations for controls related to critical infrastructure. The risk assessment found 107 risk scenarios that led to 11 recommendations for critical infrastructure improvement areas. Prioritization of the resulting recommendations is expected to increase the resilience and capacity of critical infrastructure at PT XYZ in the face of current and future cyber threats.

A. Pendahuluan

Serangan siber dapat didefinisikan sebagai tindakan yang disengaja untuk mengubah, mengganggu, menipu, menurunkan, atau menghancurkan sistem komputer atau jaringan atau informasi dan/atau program yang ada di dalam atau pada sistem tertentu [1]. Serangan siber juga terjadi karena dampak dari ketergantungan terhadap suatu sistem dan teknologi yang diadopsi. Infrastruktur tersebut kemudian menjadi alat untuk melindungi sebuah sistem yang berjalan pada Organisasi. Mengatasi celah keamanan yang tercipta merupakan tantangan nyata bagi sebuah organisasi [2]. Kerahasiaan informasi, integritas data, ketersediaan jaringan, keaslian data, akuntabilitas data, dan keandalan teknologi merupakan aspek-aspek yang perlu diperhatikan untuk menghindari terjadinya pembobolan data. Survei IBM terhadap 550 organisasi pada Maret 2021 hingga Mei 2022 menunjukkan bahwa 83% organisasi mengalami lebih dari satu kali pelanggaran data [3]. Keamanan siber kemudian menjadi bagian dari keamanan informasi yang dapat membantu melindungi aset informasi dari ancaman terhadap informasi yang diproses, disimpan, ditransmisikan oleh sistem informasi yang saling terhubung [4].Tujuan dari perlindungan keamanan siber itu sendiri adalah untuk mencegah, mengatasi, dan mengurangi dampak kerusakan atau kerugian pada sistem.

Menghadapi ancaman keamanan siber yang semakin berkembang saat ini, organisasi perlu melakukan perlindungan terhadap infrastruktur kritis, yang mana hal ini sangat penting untuk menilai apakah keamanan infrastruktur yang dikembangkan sudah mencapai posisi ideal atau belum sehingga kerentanan dapat dihindari [5]. Sebuah organisasi dapat melakukan penilaian secara efektif. Kontrol atau pemantauan sebuah infrastruktur kritis dalam sebuah organisasi harus dilengkapi dengan alat dan aplikasi yang handal, seperti kerangka kerja keamanan siber dan menganalisa risiko organisasi secara keseluruhan. Alat yang dapat digunakan dalam penentuan proses dan prosedur untuk mengidentifikasi dan mengevaluasi kerentanan keamanan telah dikembangkan selama bertahun-tahun. Beberapa di antaranya didefinisikan dalam kerangka kerja keamanan siber, standar, dan pedoman yang ada seperti COBIT dan ISO 27001. Ada juga peneliti lain yang menggunakan kerangka kerja seperti *Cybersecurity Capability Maturity Assessment* (C2M2), *National Institute of Standards and Technology* (NIST) *Cyber Security Framework* (CSF) yang mencakup manajemen keamanan informasi, penilaian keamanan, otorisasi, dan juga *Cyber Security Evaluation Tool* (CSET®) [6].

PT XYZ merupakan perusahaan yang bergerak di bidang sistem integrator, dimana proses bisnis utama PT XYZ adalah berperan untuk menjembatani antara para pelanggang dengan prinsipal dalam mengimplementasikan suatu teknologi. Dalam menjalankan bisnisnya PT XYZ harus menggunakan prinsip-prinsip Tata Kelola yang baik (*Good IT Governance*). Kebijakan keamanan informasi disusun sebagai tolak ukur dalam menerapkan SMKI, dengan harapan segala bentuk ancaman terhadap keamanan informasi di perusahaan dapat dicegah sehingga perusahaan dapat menjalankan bisnisnya dengan berlandaskan pada prinsip-prinsip tata kelola yang baik. PT XYZ pernah mengalami serangan siber yang mengakibatkan terganggunya data operasional, sistem internal seperti CRM (*Customer Relationship Management*), data-data proyek yang sedang berjalan juga tidak dapat diakses, serta terdapat data yang rusak dan tidak bisa dikembalikan

akibat serangan tersebut sehingga membutuhkan pemulihan data dari *Disaster Recovery* [7]. Permasalahan tersebut yang kemudian dalam akan berusaha menyelesaikan. Berangkat dari keadaan tersebut kenyataan yang terjadi adalah *critical infrastructure* di PT XYZ belum memberikan perlindungan yang optimal, pemulihan paska insiden juga belum menggunakan standar pemulihan yang sesuai hal-hal tersebut menjadi permasalahan utama yang akan diselesaikan pada penelitian ini. Penelitian ini akan berfokus pada infrastruktur kritis dimana NIST CSF akan menjadi kerangka kerja utama yang akan digunakan sebagai acuan dalam penilaian tools dan rekomendasi terhadap analisis kesenjangan yang ditemukan sebagai upaya mitigasi risiko keamanan siber di masa mendatang.

Isi dari makalah selanjutnya adalah sebagai studi literatur yang membahas penelitian relevan penelitian sebelumnya serta bagaimana melakukan penelitian tersebut dilakukan oleh peneliti terdahulu. Setelah melakukan studi literatur, pada makalah ini akan membahas mengenai metodologi penelitian diikuti dengan hasil penelitian ada di bagian berikutnya bersamaan dengan analisis utama. Bagian terakhir dijelaskan juga keterbatasan penelitian dan menarik kesimpulan serta penelitian yang bisa dilakukan di masa yang akan datang.

B. Studi Literatur

Pada bagian ini akan dijelaskan beberapa penelitian serupa yang sudah dilakukan oleh peneliti sebelumnya, bagaimana peneleiti menyelesaikan permasalahan serangan siber pada suatu organiasai. Berikutnya akan dipaparkan mengenai kerangka kerja yang digunakan pada penelitian ini untuk dipahami lebih lanjut sehingga menghasilkan rancangan yang tepat.

1. Penelitian Revelan

Penelitian yang dirujuk pertama melakukan penilaian postur keamanan siber pada organisasi pemerintah di bagian barat negara Australia [8]. Fokus utama penelitian adalah untuk menghasilkan rekomendasi berdasarkan temuan menggunakan kerangka kerja NIST CSF. Selain melakukan penilaian menggunakan *framework* NIST CSF, penelitian ini juga akan membandingkan penggunaan kerangka kerja lain yang serupa dimana relevan dengan studi kasus yang dilakukan. Luaran yang didapatkan dari 5 fungsi pada *framework core* NIST CSF penelitian tersebut berupa rekomendasi pada masing-masing fungsi. 5 rekomendasi pada fungsi *identify*, 6 rekomendasi untuk fungsi *protect*, 3 rekomendasi untuk fungsi *detect*, 4 rekomendasi untuk fungsi *respond*. Selain itu hasil rekomendasi dibandingkan dengan beberapa kerangka kerja yang lain seperti COBIT 5, ISO/ISE 27001:2013, NIST SP 800-53 Rev. 4, ISA 62443-2-1:2009, dan ISA 62442-3-3:2013.

Penelitian serupa lainnya dilakukan dalam upaya mendapatkan rancangan manajemen risiko dalam sebuah aplikasi di salah satu aplikasi SIMKIM Ditjen. Keimigrasian [9]. Adanya insiden yang berdampak negatif pada operasional menjadikan peneliti menggunakannya sebagai latar belakang utama dalam penelitian. Untuk mengembangkan solusi dari masaah yang terjadi, peneliti mengacu kepada beberapa kerangka kerja yang berhubungan dengan keamanan informasi seperti ISO/IEC 27005:2018 dan NIST SP 800-30 Rev 1 sebagai panduan kerangka kerja untuk melakukan Penilaian risiko serta NIST SP 800-53 Rev 5 sebagai kerangka kerja pembuatan rekomendasi berdasarkan Penilaian risiko menggunakan 2 kerangka kerja sebelumnya. Pada hasilnya, penelitian ini sudah

menghasilkan rekomendasi manajemen risiko kemanan informasi sistem informasi manajemen keimigrasian.

Penelitian serupa juga dilakukan pada pembuatan rencana manajemen *cyber-risk* pada divisi Teknologi Informasi (TI) di perusahaan XYZ yang luarannya adalah rencana manajemen cyber-risk dan rekomendasi aksi untuk peningkatan kapabilitas *cyber-risk* yang ada [10]. Dalam melakukan penelitian, peneliti menggunakan kerangkat kerja utama NIST CSF yang diambil total 6 dari 7 langkah yang terdapat di dalam kerangka kerja tersebut. Berikutnya, dalam melakukan analisis peneliti menggunakan kerangka kerja *Center for Internet Security* (CIS) Contols v8 dan NIST SP 800-53 Rev. 5. Hasil dari penelitian ini adalah sebuah rekomendasi dari hasil pemeteaan baik dari CIS v8 ke NIST SP 800-53 Rev 5 begitu juga sebaliknya dengan total rekomendasi yang dihasilkan adalah 14 butir.

Acuan berikutnya penelitian dilakukan pada penggunaan kombinasi dua kerangka kerja bersamaan yaitu NIST SP 800-30 revision 1 dan ISO 27005 untuk menilai risiko pada *information security* di suatu organisasi profit di Indonesia (PT ABC) [11]. Penelitian ini dilakukan untuk memberikan penjelasan dan langkah-langkah secara detil mengenai cara penggunaan teknik kombinasi ISO 27005 dan NIST SP 800-30 revisi 1 serta untuk memudahkan pemangku kepentingan di area manajemen risiko keamanan siber dalam mengimplementasikan metode dengan membuktikan apakah model metode tersebut bisa digunakan pada organisasi profit maupun non-profit. Hasil yang didapatkan dari penelitian ini adalah proses identifikasi risiko didasarkan pada kategori yang terdapat pada ISO 27005, kerangka kerja NIST SP 800-30 revisi 1 dalam penelitian ini digunakan sebagai pendukung analisis yang dari kerangka kerja pertama. Hal tersebut didasarkan pada proses simplifikasi yang bisa dilakukan untuk menilai risiko keamanan informasi.

2. Kerangka Kerja

Bagian kerangka kerja berisikan penjelasan terhadap teori dari kerangka kerja yang akan digunakan dalam penelitian.

2.1 NIST *Cybersecurity Framework* (CSF)

NIST (*Natonal Institute of Standards and Technology*) *framework* berfokus pada aktivitas proses bisnis sebagai panduan aktivitas *cybersecurity* dengan mempertimbangkan risiko *cybersecurity* sebagai bagian dari proses manajemen risiko suatu organisasi. NIST *Cybersecurity Framework* (CSF) terdiri dari 3 bagian utama yaitu *Core, Profile,* dan *Implementation Tiers* (NIST, 2018). Kerangka kerja keamanan siber NIST terdiri dari lima fungsi yang disebut berbeda, yang secara keseluruhan terdiri dari 23 kategori dan 108 subkategori [1]. Fungsi utama pada kerangka kerja tersebut terlihat pada Tabel 1.

Tabel 1. Fungsi pada Kerangka Kerja NIST CSF

Fungsi	Keterangan
Identify	Untuk meningkatkan pemahaman organisasi tentang cara mengelola risiko cybersecurity terhadap sistem, individu, aset, dan data. Kegiatan fungsi identifikasi adalah dasar dari penggunaan rangka kerja yang efektif. Memahami konteks bisnis, sumber daya yang mendukung fungsi kritis dan risiko cybersecurity terkait dengan bagaimana organisasi dapat memprioritaskan dan mengkonsentrasikan upaya yang sesuai dengan strategi manajemen risiko dan berdasarkan kebutuhan bisnis. Manajemen aset, lingkungan bisnis, tugas beresik, dan strategi manajemen risiko adalah hasil dari fungsi identifikasi.

Protect	Menekankan pada pengembangkan dan pernerapan perlindungan yang tepat untuk memastikan layanan yang penting dan mendukung kemampuan organisasi untuk membatasi atau menahan dampak dari peristiwa *cybersecurity* yang berpotensi terjadi.
Detect	Berfokus pada peningkatan dan penerapan aktivitas yang sesuai untuk melakukan identifikasi awal kemungkinan terjadinya peristiwa *cybersecurity*. Fungsi *detect* memungkinkan penemuan peristiwa *cybersecurity* secara tepat waktu.
Respond	Berfokus pada pengembangan dan penerapan aktivitas untuk mengambil tindakan yang berhubungan dengan insiden *cybersecurity* yang terdeteksi. Fungsi *respond* bertujuan untuk mendukung kemampuan mencegah lebih awal terjadinya keamanan siber.
Recover	Berfokus pada pengembangan dan implementasi aktivitas dalam bentuk kebijakan maupun penerapan secara langsung dalam upaya mempertahankan rencana ketahanan dan pemulihan layanan sistem informasi dan critical infrastructure yang terganggu karena insiden *cybersecurity*. Fungsi *recover* mendukung pemulihan secara tepat untuk mengurangi dampak dari insiden *cybersecurity*.

Pada NIST CSF juga terdapat fungsi implementasi dan *profile* yang mendukung fungsi utamanya yaitu *Core*. Fungsi Implementation terdapat 4 level yang dapat membantu organisasi melihat sejauh apa praktik keamanan siber diterapkan dan dijalankan pada organisasi [8]. Fungsi tersebut diantaranya *Tier* 1 *(Partial), Tier* 2 *(Risk Informed), Tier* 3 *(Repeatable),* dan *Tier* 4 *(Adaptive).* Fungsi profile yang kemudian membantu organisasi dalam menentukan langkah-langkah untuk mencapai *profile* yang sudah ditentukan yang digunakan juga sebagai alat penilaian [10]. Langkah-langkah tersbeut antara lain *current profiile* dan *target profile*.

2.2 NIST Special Publication 800-53 Rev. 5

NIST 800-53 SP Rev.5 memberikan pedoman untuk memilih dan menentukan kontrol terhadap keamanan untuk organisasi dan sistem informasi (NIST SP800-53, 2020). Pemilihan spesifikasi kontrol keamanan sistem informasi dilakukan sebagai bagian dari program keamanan informasi untuk pengelolaan risiko. Risiko yang dimaksud adalah risiko terhadap operasi dan aset organisasi, individu yang terkait dengan pengoperasian sistem informasi. *Framework* ini menggunakan tiga pendekatan untuk mengintegrasikan proses manajemen risiko yaitu pada level organisasi, pada level misi atau proses bisnis yang dilakukan dan pada area sistem informasi itu sendiri. NIST 800-53 membagi kontrol ke dalam 18 *families*. Setiap *families* berisi kontrol keamanan yang terkait dengan topik keamanan umum *difamily*-nya. Kontrol yang terdapat pada NIST SP 800-53 Rev. 5 tertuang pada Tabel 2.

Tabel 2. Kontrol pada NIST SP 800-53 Rev. 5

ID	Keluarga	ID	Keluarga
AC	*Access Control*	MP	*Media Protection*
AT	*Awareness and Training*	PE	*Physical and Environmental Protection*
AU	*Audit and Accountability*	PL	*Planning*
CA	*Security Assessment and Authorization*	PS	*Personnel Security*
CM	*Configuration Management*	RA	*Risk Assessment*
CP	*Contingency Planning*	SA	*System and Services Acquisition*
IA	*Identification and Authentication*	SC	*System and Communications Protection*
IR	*Incident Response*	SI	*System and Information Integrity*
MA	*Maintenance*	PM	*Program Management*

Berdasarkan pemaparan penelitian relevan sebelumnya yang sudah dilakukan sebelumnya, penelitian ini akan melakukan penilaian risiko pada PT XYZ dengan melakukan cara-cara seperti pada kerangka kerangka kerja yang sudah dijelaskan pada poin B.2. Penelitian ini dilaksanakan dengan menggunakan 2 kerangka kerja dengan mempertimbangkan NIST CSF akan digunakan sebagai sebagai kerangka untuk melakukan identifikasi keadaan *as-is* yang terdapat di PT XYZ serta NIST SP 800-53 Rev 5 yang akan digunakan sebagai panduan untuk menentukan strategi peningkatan *cybersecurity* berdasarkan temuan-temuan pada hasil *assessment* menggunakan NIST CSF.

C. Metode Penelitian

Penelitian yang dilakukan ini menggunakan pendekatan kualitatif yakni dengan melakukan wawancara kepada pihak-pihak yang bertanggung jawab terhadap critical infrastructure di PT XYZ. Pertanyaan penelitian diambil dari NIST CSF dengan melakukan validasi untuk total 108 subkategori yang ada. Pada setiap kategori diberikan keterangan comply, partially comply, dan not comply dimana untuk keadaan akan diberikan masing-masing nilai 10, 5, dan 0. Total 108 validasi akan hitung menggunakan persamaan (1) sebagai berikut.

$$C = \frac{\sum R}{\sum N' \; X \; 10} \tag{1}$$

C adalah total *compliance score* pada setiap *core function framework* NIST. R adalah adalah *compliance* pada masing-masing kategori, sedangkan N adalah jumlah persyaratan yang harus dipenuhi pada setiap sub kategorinya. Setelah mendapatkan nilai *Compliance* (C) pada 108 subkategori NIST CSF penelitian juga melakukan penilaian terhadap kondisi *as-is* pada aset *critical infrastructure* menggunakan wawancara dimana pertanyaan sebanyak 12 butir pertanyaan menggunakan referensi dari penelitian sebelumnya [9]. Keseluruhan wawancara tersebut dilakukan kepada 6 narasumber yang masing-masing memiliki tanggung jawab terhadap keamanan siber di PT XYZ ini yaitu kepada *compliance head, infrastructure head, computing development head, technical infrastructure advisor, staff IT infrastructure,* dan *staff computing development*. Hasil wawancara digunakan untuk menganalisis temuan menggunakan *framework profile* NIST CSF pada 6 langkah sebagai berikut.

1. *Prioritize and Scope*
   Pada tahap ini yang dilakukan adalah mencari tahu bagaimana *critical infrastructure* dapat mendukung proses bisnis yang dilakukan serta prioritas organisasi terhadap *critical infrastructure* [12].
2. *Orient*
   Pada tahap yang kedua proses yang dilakukan adalah mencari tahu dan melakukan pendataan terhadap aset *critical infrastructure* yang digunakan untuk mendukung proses bisnis. Daftar aset kemudian menjadikan acuan untuk melihat dan melakukan analisis terhadap kerentanan yang mungkin terjadi [10].
3. *Create a current profile*
   Current profile merupakan kondisi *as-is* suatu perusahaan atau organisasi terhadap ancaman keamanan siber pada saat tersebut. NIST menggunakan 4 level untuk menentukan suatu *profile* yaitu *Partial, Risk Informed, Repeatable*, dan *Adaptive*. Tahapan pada setiap level seperti pada Tabel 3.

Tabel 3. *Implementation Tiers* NIST CSF

No	***Risk Management Process* (RMP)**	***Integrated Risk Management Program***	**Partisipasi pihak Luar**
		***Tier* 1 (*Partial*)**	
1.	▪ Praktik manajemen risiko *cybersecurity* organisasi tidak diformalisasi. ▪ Risiko dikelola dengan cara *ad-hoc* dan reaktif	▪ Kesadaran akan risiko *cybersecurity* di tingkat organisasi masih sangat terbatas. ▪ Organisasi menerapkan manajemen risiko *cybersecurity* secara tidak teratur.	▪ Organisasi belum memahami perannya dalam ekosistem yang lebih besar sehubungan dengan tanggung jawabnya. ▪ Organisasi tidak berkolaborasi dengan atau menerima informasi.
		***Tier* 2 (*Risk Informed*)**	
2.	▪ Praktik manajemen risiko disetujui oleh manajemen tetapi tidak ditetapkan sebagai kebijakan organisasi secara keseluruhan.	▪ Ada kesadaran akan risiko *cybersecurity* di tingkat organisasi, tetapi pendekatan di seluruh organisasi untuk mengelola risiko *cybersecurity* belum ditetapkan.	▪ Organisasi memahami perannya dalam ekosistem yang lebih besar sehubungan dengan ketergantungan atau tanggungannya sendiri, tetapi tidak keduanya. ▪ Organisasi berkolaborasi dengan dan menerima beberapa informasi dari entitas lain dan menghasilkan beberapa informasi.
		Tier* 3 (*Repeatable)	
3.	▪ Praktik manajemen risiko organisasi secara formal disetujui dan dinyatakan sebagai kebijakan.	▪ Ada pendekatan di seluruh organisasi untuk mengelola risiko *cybersecurity*. ▪ Kebijakan, proses, dan prosedur yang diinformasikan, risiko ditetapkan, diterapkan sebagaimana dimaksud, dan ditinjau. ▪ Metode yang konsisten tersedia untuk merespons secara efektif terhadap perubahan risiko	▪ Organisasi memahami peran, ketergantungan, dan tanggungannya dalam ekosistem yang lebih besar dan dapat berkontribusi pada pemahaman masyarakat yang lebih luas tentang risiko. ▪ Organisasi berkolaborasi dengan dan menerima informasi dari entitas lain secara

			teratur yang melengkapi informasi yang dihasilkan secara internal.
***Tier 4* (*Adaptive*)**			
4.	▪ Organisasi menyesuaikan praktik *cybersecurity* berdasarkan aktivitas *cybersecurity* sebelumnya dan saat ini, termasuk pelajaran yang didapat dan indikator prediktif	▪ Terdapat pendekatan di seluruh organisasi untuk mengelola risiko *cybersecurity* yang menggunakan kebijakan, proses, dan prosedur yang diinformasikan tentang risiko untuk mengatasi potensi peristiwa *cybersecurity*.	▪ Organisasi memahami peran, ketergantungan, dan tanggungannya dalam ekosistem yang lebih besar dan berkontribusi pada pemahaman masyarakat yang lebih luas tentang risiko. ▪ Organisasi menerima, menghasilkan, dan meninjau informasi yang diprioritaskan dan menginformasikan analisis kelanjutan atas risikonya seiring berkembangnya lanskap ancaman dan teknologi.

4. *Conduct risk assessment*
   Pada tahap ke empat proses yang dilakukan adalah melakukan analisis bagaimana kerentanan yang terjadi dapat memengaruhi proses bisnis yang ada di PT XYZ dan menentukan sejauh apa potensi tersebut akan terjadi.
5. *Create a target profile*
   Penentuan target profile juga menggunakan *Implementation Tiers* seperti pada Tabel 3 dan biasanya didapatkan melalui wawancara dengan pemangku kepentingan pada suatu organisasi.
6. *Determine, analyze, and prioritize*
   Proses yang ke enam adalah melakukan analisis bagaimana untuk mencapai *target profile* dari *current profile* dengan mempertimbangakan penilaian risiko dan analisis yang sudah dilakukan.

D. Hasil dan Pembahasan

Pada bagian ini diuraikan hasil penelitian beserta analisis yang sudah dilakukan. NIST CSF berperan sebagai alat yang digunakan untuk melakukan *assessment* dalam tahap ini. Berikut adalah hasil dan analisis dari 6 tahap yang sudah dilakukan.

1. *Prioritize and Scope*

Hasil wawancara dengan yang sudah dilakukan dengan *Technical Solution Architect* pada *Critical Infrastructure* di PT XYZ dijelaskan bahwa, untuk peningkatan kapasitas infrastruktur difokuskan pada pemindahan internet yang sebelumnya menggunakan bantuan pihak ketiga dalam pengelolaan serta ingin meningkatkan kapasitas keamanan dari ancaman dengan mengadopsi teknologi yang sesuai dengan hasil assessment dan prioritas PT XYZ itu sendiri. Hal tersebut sudah direncanakan sejak dari tahun 2019 dan dijadwalkan akan dikerjakan pada tahun 2020. Selain 2 prioritas untuk peningkatan kapasitas koneksi internet dan peningkatan kapasitas keamanan, *scope* peningkatan *cybersecurity* juga akan dilakukan penggantian perangkat-perangkat infrastruktur yang sudah memasuki masa *obsolete* dengan perangkat baru seperti server-server serta peningkatan kapasitas ketersediaan seluruh sistem yang ada. Seluruh pekerjaan yang sudah disebutkan sebelumnya akan dikerjakan oleh tim IT *Infrastructure* dan tim *Computing Development* di PT XYZ.

2. *Orient*

Pada tahap yang kedua dilakukan pendataan aset infrastruktur dan seluruh sistem yang digunakan disertai analisis mengenai ancaman dan sumber ancaman yang bisa terjadi pada aset tersebut. Analisis yang dilakukan adalah menganalisis sumber ancaman pada aset menggunakan klasifikasi *Adversarial Threat Source* (ATS) dan *Non-Adversarial Threat Source* (NATS) yang kemudian dikategorikan ke dalam beberapa kelompok sebagai berikut Hi = High, Mo = Moderate, dan Lo = Low sebagaimana yang ditunjukkan pada Tabel 4 dan Tabel 5 berikut.

Tabel 4. Daftar *Adversarial Threat Source* (ATS) Aset PT XYZ

No	Kode Identifikasi	Ketarangan	*In Scope* (Y/T)	*Capability (Hi/Mo/Lo)*	*Intent (Hi/Mo/Lo)*	*Target (Hi/Mo/Lo)*
1.	ATS-1	Hacker	Y	*Hi*	*Mo*	*Mo*
2.	ATS-2	Phisher	Y	*Mo*	*Hi*	*Mo*
3.	ATS-3	Malware	Y	*Hi*	*Lo*	*Mo*
4.	ATS-4	Insider	Y	*Lo*	*Lo*	*Mo*
5.	ATS-5	Social-Engineering	Y	*Lo*	*Lo*	*Mo*

Tabel 5. Daftar *Non-Adversarial Threat Source* (NATS) Aset PT XYZ

No	Kode Identifikasi	Ketarangan	*In Scope* (Y/T)	Dampak *(Hi/Mo/Lo)*
1.	NATS-1	Bencana Alam	Y	*Mo*
2.	NATS-2	*Human Error*	Y	*Lo*
3.	NATS-3	Listrik Padam	Y	*Mo*
4.	NATS-4	Kegagalan perangkat keras dan perangkat lunak	Y	*Lo*
5.	NATS-5	Perubahan Regulasi	Y	*Lo*

Dari kedua tabel diatas proses analisis dilakukan untuk dengan melakukan pemetaan terhadap setiap aset yang ada di PT XYZ. Aset yang terdapat pada PT XYZ ditunjukkan pada Tabel 5 berikut.

Tabel 6. Daftar Aset Infrastruktur PT XYZ

No	Kategori Aset	Nama Aset	Kode Aset
1.	Perangkat Jaringan	*Firewall*	AS-1
		Switch	AS-2
		Wireless LAN *Controller*	AS-3
		Access Point	AS-4
		Router (*Voice Gateway*)	AS-5
		Email Security	AS-6
2.	Perangkat Server	*Identity Service Engine*	AS-7
		Service Directory	AS-8
		Baremetal Server	AS-9
		Virtual Server	AS-10
3.	Sistem Informasi	*Mail App*	AS-11
		e-Requisition	AS-12
		Customer Relationship Management (CRM)	AS-13
		Project Costing	AS-14
		Pre-proc	AS-15
		Lapor – TAC	AS-16
		Sistem *Human Resource*	AS-17
		Knowledge Management System (KMS)	AS-18

Setelah menentukan *Adversarial Threat Source* (ATS) dan *Non-Adversarial* Threat Source (NATS) maka dilakukan pemetaan semua asset terhadap sumber ancaman baik untuk ATS dan NATS. Pada Tabel 7 merupakan daftar aset yang sudah dipetakan ke dalam masing-masing ancaman yang ada.

Tabel 7. Identifikasi Kerentanan dan Kontrol

No	Kode Aset	Ancaman (T)	Kerentanan (V)	Penerapan Kontrol
Perangkat keras				
1.	AS-1, AS-6	1. *Denial of Service Attack* (DoS).	1. *Firewall* tidak menjalankan	1. Menutup port yang tidak digunakan;

		2. *Distributed Denial of Service Atack* (DDoS). 3. *Malware and Exploits.* 4. *Zero Day* 5. *Brute Force Attack*	service yang dibutuhkan (Hang). 2. *Malware* masuk pada port yang tidak ditutup.	2. Menjalankan *high availability*; 3. Mengikuti panduan konfigurasi *best practices*; 4. Mengaktifkan fitur-fitur seperti antivirus dan anti *malware*
2.	AS-2, AS-3, AS-4, AS-5	6. *Packet Sniffing.* 7. *VLAN Hopping.* 8. *Spoofing Attack*	3. Terjadinya *looping* membuat jaringan down. 4. pencurian data.	5. Mengaktifkan fitur *spanning tree* pada *switch* 6. Menentukan jaringan yang terpercaya
3.	AS-7, AS-8, AS-9	*9.* Pencurian data. *10. Physical security risk* *11. container vulnerability* *12. Insecure* API	5. Eksploitasi pada server. 6. *Service disruption*	7. Penggunaan *credentials yang kuat* 8. Menerapkan Multifaktor *Authentication* 9. Menggunakan *Web Application firewall* (WAF)
Perangkat Lunak				
4.	AS-10, AS-11, AS-12, AS-13, AS-14, AS-15, AS-16, AS-17, AS-18	13. *Databreaches.* 14. *Unauthorizes Access.* 15. *Phissing Attack.* 16. *Ransomware*	7. *System Malfunction* 8. *Data Corrupted* 9. *Services Down*	10. Meningkatkan *coding* sistem aplikasi 11. Menggunakan antivirus dengan maksimal 12. Melakukan update *firmware* secara berkala 13. Penggunaan *firewall* 14. Penerapan DRC dan *Backup Restore* 15. Pemberian hak akses untuk *tracking*.

3. *Create a current profile*

Dari pemetaan *framework Implementation Tiers* NIST CSF, PT XYZ saat ini menempati Tier 3. Level tersebut di dapatkan dari hasil wawancara dan hasil

studi dokumen pendukung yang saat ini ada di PT XYZ. Risiko target harus dievaluasi sebagai tahapan yang lebih lanjut dan yang akan dilakukan. Langkah ini memiliki beberapa keuntungan seperti mengetahui potensi ancaman dan sumber ancaman, termasuk meminimalkan risiko, mengidentifikasi kelemahan keamanan, dan menetapkan standar keamanan yang dapat mencegah terjadinya risiko tersebut.

4. *Conduct Risk Assessment*

Pada tahap ini dilakukan pembuatan skenario risiko menggunakan semua informasi tentang aset, ancaman, dan kerentanan yang sudah dianalisis pada tahap sebelumnya. Berikutnya menggunakan *likelihood* dan *impact factor* dari setiap skenario risiko dihitung dan diperkirakan tingkat risiko terhadap ancaman tersebut. Tingkat risiko kemudian digunakan untuk menentukan respon terhadap resiko yang muncul. Respon yang diambil didasarkan pada matrik risiko hasil analisis berdasarkan hasil wawancara dan studi dokumen yang sudah dilakukan seperti yang disajikan pada Tabel 8 berikut, dimana VL = *Very Low*; L = *Low*; M = *Medium*; H = *High*; VH = *Very High*; AC = *Accept*; dan MT = *Mitigate*.

Tabel 8. Matriks Risiko

		Likelihood				
		VL	**L**	**M**	**H**	**VH**
Impact	**VH**	AC	AC	MT	MT	MT
	H	AC	AC	MT	MT	MT
	M	AC	AC	MT	MT	MT
	L	AC	AC	AC	AC	MT
	VL	AC	AC	AC	AC	AC

Skenario yang didapatkan dari hasil analisis terdapat 107 skenario resiko yang bisa dikenali berdasarkan aset-aset *critical infrastructure* yang ada, dengan 68 skenario risiko yang perlu dilakukan mitigasi dan 39 diantaranya dapat diterima seperti pada Tabel 9 berikut.

Tabel 9. Hasil Penilaian Risiko terhadap *Critical Infrastructure*

No	Skenario Risiko	Aset	T	V	Dampak	*Likelihood*	Risiko	Respon
1.	SR-1	AS-1	T1	V1	*Hi*	*Mo*	*Mo*	MT
2.	SR-2	AS-1	T2	V1	*Hi*	*Mo*	*Mo*	MT
3.	SR-3	AS-1	T3	V2	*Mo*	*Mo*	*Mo*	MT
4.	SR-4	AS-1	T4	V2	*Hi*	*Mo*	*Hi*	MT
5.	SR-5	AS-1	T5	V2	*Hi*	*Hi*	*Mo*	MT
6.	SR-6	AS-2	T6	V4	*Lo*	*Lo*	*Lo*	AC
7.	SR-7	AS-2	T6	V5	*Lo*	*Lo*	*Lo*	AC
8.	SR-8	AS-2	T7	V4	*Lo*	*Lo*	*Lo*	AC
9.	SR-9	AS-2	T7	V5	*Lo*	*Lo*	*Lo*	AC
10.	SR-10	AS-2	T8	V4	*Lo*	*Lo*	*Lo*	AC
11.	SR-11	AS-2	T8	V5	*Lo*	*Lo*	*Lo*	AC
12.	SR-12	AS-3	T6	V4	*Lo*	*Lo*	*Lo*	AC
13.	SR-13	AS-3	T6	V5	*Lo*	*Lo*	*Lo*	AC

14.	SR-14	AS-3	T7	V4	*Lo*	*Lo*	*Lo*	AC
15.	SR-15	AS-3	T7	V5	*Lo*	*Lo*	*Lo*	AC
16.	SR-16	AS-3	T8	V4	*Lo*	*Lo*	*Lo*	AC
17.	SR-17	AS-3	T8	V5	*Lo*	*Lo*	*Lo*	AC
18.	SR-18	AS-4	T6	V4	*Lo*	*Lo*	*Lo*	AC
19.	SR-19	AS-4	T6	V5	*Lo*	*Lo*	*Lo*	AC
20.	SR-20	AS-4	T7	V4	*Lo*	*Lo*	*Lo*	AC
21.	SR-21	AS-4	T7	V5	*Lo*	*Lo*	*Lo*	AC
22.	SR-22	AS-4	T8	V4	*Lo*	*Lo*	*Lo*	AC
23.	SR-23	AS-4	T8	V5	*Lo*	*Lo*	*Lo*	AC
24.	SR-24	AS-5	T6	V4	*Lo*	*Lo*	*Lo*	AC
25.	SR-25	AS-5	T6	V5	*Lo*	*Lo*	*Lo*	AC
26.	SR-26	AS-5	T7	V4	*Lo*	*Lo*	*Lo*	AC
27.	SR-27	AS-5	T7	V5	*Lo*	*Lo*	*Lo*	AC
28.	SR-28	AS-5	T8	V4	*Lo*	*Lo*	*Lo*	AC
29.	SR-29	AS-5	T8	V5	*Lo*	*Lo*	*Lo*	AC
30.	SR-30	AS-6	T1	V1	*Hi*	*Mo*	*Mo*	MT
31.	SR-31	AS-6	T2	V1	*Hi*	*Mo*	*Mo*	MT
32.	SR-32	AS-6	T3	V2	*Mo*	*Mo*	*Mo*	MT
33.	SR-33	AS-7	T1	V6	*Hi*	*Mo*	*Mo*	MT
34.	SR-34	AS-7	T2	V6	*Mo*	*Mo*	*Mo*	MT
35.	SR-35	AS-7	T10	V6	*Lo*	*Lo*	*Lo*	AC
36.	SR-36	AS-8	T9	V5	*Hi*	*Mo*	*Hi*	MT
37.	SR-37	AS-8	T10	V6	*Lo*	*Mo*	*Lo*	AC
38.	SR-38	AS-8	T12	V6	*Lo*	*Lo*	*Lo*	AC
39.	SR-39	AS-9	T10	V6	*Lo*	*Mo*	*Lo*	AC
40.	SR-40	AS-9	T10	V7	*Lo*	*Mo*	*Lo*	AC
41.	SR-41	AS-10	T11	V5	*Mo*	*Lo*	*Lo*	AC
42.	SR-42	AS-10	T11	V6	*Mo*	*Lo*	*Lo*	AC
43.	SR-43	AS-10	T11	V7	*Lo*	*Lo*	*Lo*	AC
44.	SR-44	AS-10	T12	V5	*Lo*	*Lo*	*Lo*	AC
45.	SR-45	AS-10	T12	V6	*Lo*	*Lo*	*Lo*	AC
46.	SR-46	AS-10	T12	V7	*Lo*	*Lo*	*Lo*	AC
47.	SR-47	AS-11	T13	V7	*Hi*	*Mo*	*Mo*	MT
48.	SR-48	AS-11	T13	V8	*Hi*	*Mo*	*Mo*	MT
49.	SR-49	AS-11	T13	V9	*Hi*	*Mo*	*Hi*	MT
50.	SR-50	AS-11	T14	V7	*Hi*	*Mo*	*Mo*	MT
51.	SR-51	AS-11	T14	V8	*Hi*	*Mo*	*Mo*	MT
52.	SR-52	AS-11	T14	V9	*Hi*	*Mo*	*Hi*	MT
53.	SR-53	AS-11	T15	V7	*Hi*	*Mo*	*Mo*	MT
54.	SR-54	AS-11	T15	V8	*Hi*	*Mo*	*Mo*	MT
55.	SR-55	AS-11	T15	V9	*Hi*	*Mo*	*Hi*	MT
56.	SR-56	AS-12	T13	V7	*Hi*	*Mo*	*Mo*	MT
57.	SR-57	AS-12	T13	V8	*Hi*	*Mo*	*Mo*	MT
58.	SR-58	AS-12	T13	V9	*Hi*	*Mo*	*Hi*	MT
59.	SR-59	AS-12	T14	V7	*Hi*	*Mo*	*Mo*	MT
60.	SR-60	AS-12	T14	V8	*Hi*	*Mo*	*Mo*	MT
61.	SR-61	AS-12	T14	V9	*Hi*	*Mo*	*Hi*	MT

62.	SR-62	AS-12	T15	V7	*Hi*	*Mo*	*Mo*	MT
63.	SR-63	AS-12	T15	V8	*Hi*	*Mo*	*Mo*	MT
64.	SR-64	AS-12	T15	V9	*Hi*	*Mo*	*Hi*	MT
65.	SR-65	AS-12	T16	V7	*Hi*	*Hi*	*Hi*	MT
66.	SR-66	AS-12	T16	V8	*Hi*	*Hi*	*Hi*	MT
67.	SR-67	AS-12	T16	V9	*Hi*	*Hi*	*Hi*	MT
68.	SR-68	AS-13	T13	V7	*Hi*	*Mo*	*Mo*	MT
69.	SR-69	AS-13	T13	V8	*Hi*	*Mo*	*Mo*	MT
70.	SR-70	AS-13	T13	V9	*Hi*	*Mo*	*Hi*	MT
71.	SR-71	AS-13	T14	V7	*Hi*	*Mo*	*Mo*	MT
72.	SR-72	AS-13	T14	V8	*Hi*	*Mo*	*Mo*	MT
73.	SR-73	AS-13	T14	V9	*Hi*	*Mo*	*Hi*	MT
74.	SR-74	AS-13	T15	V7	*Hi*	*Mo*	*Mo*	MT
75.	SR-75	AS-13	T15	V8	*Hi*	*Mo*	*Mo*	MT
76.	SR-76	AS-13	T15	V9	*Hi*	*Mo*	*Hi*	MT
77.	SR-77	AS-13	T16	V7	*Hi*	*Hi*	*Hi*	MT
78.	SR-78	AS-13	T16	V8	*Hi*	*Hi*	*Hi*	MT
79.	SR-79	AS-13	T16	V9	*Hi*	*Hi*	*Hi*	MT
80.	SR-80	AS-14	T13	V7	*Hi*	*Mo*	*Mo*	MT
81.	SR-81	AS-14	T13	V8	*Hi*	*Mo*	*Mo*	MT
82.	SR-82	AS-14	T13	V9	*Hi*	*Mo*	*Hi*	MT
83.	SR-83	AS-14	T14	V7	*Hi*	*Mo*	*Mo*	MT
84.	SR-84	AS-14	T14	V8	*Hi*	*Mo*	*Mo*	MT
85.	SR-85	AS-14	T14	V9	*Hi*	*Mo*	*Hi*	MT
86.	SR-86	AS-14	T15	V7	*Hi*	*Mo*	*Mo*	MT
87.	SR-87	AS-14	T15	V8	*Hi*	*Mo*	*Mo*	MT
88.	SR-88	AS-14	T15	V9	*Hi*	*Mo*	*Hi*	MT
89.	SR-89	AS-14	T16	V7	*Hi*	*Hi*	*Hi*	MT
90.	SR-90	AS-14	T16	V8	*Hi*	*Hi*	*Hi*	MT
91.	SR-91	AS-14	T16	V9	*Hi*	*Hi*	*Hi*	MT
92.	SR-92	AS-15	T13	V7	*Mo*	*Mo*	*Lo*	MT
93.	SR-93	AS-15	T13	V8	*Mo*	*Mo*	*Lo*	MT
94.	SR-94	AS-15	T13	V9	*Mo*	*Mo*	*Lo*	MT
95.	SR-95	AS-15	T14	V7	*Mo*	*Mo*	*Lo*	MT
96.	SR-96	AS-15	T14	V8	*Mo*	*Mo*	*Lo*	MT
97.	SR-97	AS-15	T14	V9	*Mo*	*Mo*	*Lo*	MT
98.	SR-98	AS-15	T15	V7	*Mo*	*Mo*	*Lo*	MT
99.	SR-99	AS-15	T15	V8	*Mo*	*Mo*	*Lo*	MT
100.	SR-100	AS-15	T15	V9	*Mo*	*Mo*	*Lo*	MT
101.	SR-101	AS-15	T16	V7	*Mo*	*Mo*	*Lo*	MT
102.	SR-102	AS-15	T16	V8	*Mo*	*Mo*	*Lo*	MT
103.	SR-103	AS-15	T16	V9	*Mo*	*Mo*	*Lo*	MT
104.	SR-104	AS-16	T14	V9	*Lo*	*Lo*	*Lo*	AC
105.	SR-105	AS-17	T14	V9	*Lo*	*Lo*	*Lo*	AC
106.	SR-106	AS-18	T13	V8	*Lo*	*Lo*	*Lo*	AC
107.	SR-107	AS-18	T15	V8	*Lo*	*Lo*	*Lo*	AC

5. *Create a Target profile*

Berdasarkan wawancara yang sudah dilakukan dengan beberapa narasumber IT *Infrastructure Head*, IT *Computing Development*, dan *Technical Advisor Infrastructure* di PT XYZ bahwa saat ini PT XYZ sudah menerapkan beberapa antisipasi terkait dengan *cybersecurity*. Hal tersebut masih akan terus ditingkatkan sebagaimana PT XYZ adalah perusahaan Sistem Integrator penyedia solusi keamanan yang andal yang sudah seharusnya menerapkan keamanan pada organisasi itu sendiri. Target yang dibuat dengan NSIT CSF ini adalah pada *Tier* 4 yaitu *Adaptive*. Dengan *Tier* 4 harapannya PT XYZ mampu untuk melakukan praktik *cybersecurity* berdasarkan aktivitas keamanan siber yang sebelumnya dan yang terkini, termasuk pelajaran yang dipelajari dari indikator prediktif untuk mendukung operasional bisnis yang lebbih baik

6. *Determine, Analyze, and Prioritize*

Pada tahap 1 sampai dengan 5 sudah ditentukan bahwa target yang dibuat adalah untuk mencapai *Tier* 4 yaitu berada pada level *Adaptive*. Untuk mencapai level *Adaptive* tersebut perlu dilakukan apa saja *Gap* pada keadaan saat ini dengan keadaan yang ingin dituju. Dari skenario risiko yang sudah dianalisis kemudian dikategorikan berdasarkan dampak dan kemungkinan risiko terjadi. Menggunakan framework NIST CSF yang dipetakan ke dalam framework NIST SP 800-53 Rev5 kontrol dari seluruh risiko dapat dibuat pendekatan penyelesaiannya. Penyelesaian permasalahan yang ada adalah sebagai berikut.

- Rekomendasi Peningkatan 1 (RP-1)
  RP 1 merupakan ruang lingkup untuk menyelesaikan permasalah mengenai seluruh aset *critical infrastructure* yang ada di PT XYZ. NIST SP 800-53 Rev mempunyai beberapa kontrol untuk meningkatkan permasalahan terhadap manajemen aset yaitu AC-20 (*Use of External System*), PM-5 (*System Inventory*), SA-9 (*External System Services*), CP-2 (*Contingency Plan*), RA-2 (*Security Categorization*), RA-9 (*Criticality Analysis*), SC-6 (*Resource Availability*), dan PM-29 (*Risk Management Program Leaership*).
- Rekomendasi Peningkatan 2 (RP-2)
  RP 2 merupakan ruang lingkup untuk menyelesaikan permasalah mengenai seluruh lingkungan *critical infrastructure* yang ada di PT XYZ untuk mendukung keberlangsungan bisnis pada organisasi. NIST SP 800-53 Rev mempunyai beberapa kontrol untuk meningkatkan dampak *ciritical infrastructure* dalam mendukung lingkungan bisnis yaitu PM-8 (*Critical Infrastructure Plan*), CP-8 (*Telecommunication Services*), PE-11 (*Emergency Power*), dan SR-12 (*Component Disposal*).
- Rekomendasi Peningkatan 3 (RP-3)
  RP 3 merupakan kumpulan kontrol-kontrol yang dapat meningkatkan penanganan dan panduan dalam melakukan penilaian risiko terhadap *critical infrastructure* yang dimiliki di PT XYZ. Kontrol yang dapat digunakan untuk meningkatkan prose tersebut adalah CA-2 (*Control Assessment*), CA-5 (*Plan of Action and Milestones*), CA-7 (*Continuous Monitoring*), CA-8 (*Penetration Testing*), dan PM-4 (*Plan of Action and Milestones Process*)
- Rekomendasi Peningkatan 4 (RP-4)
  RP 4 merupakan kumpulan kontrol yang mengatur untuk meningkatkan kemampuan pemrosesan informasi di area lingkungan *critical infrastructure* di PT XYZ. Kontrol-kontrol pada NIST SP 800-53 Rev5 tersebut adalah CP-4

(*Contingency Plan Testing*), IR-3 (*Incident Response Testing*), PM-14 (*Testing, Training, and Monitoring*), PS-6 (*Access Agreement*), dan PS-7 (*External Personnel Security*).

- Rekomendasi Peningkatan 5 (RP-5)
  RP 5 merupakan kumpulan kontrol yang dapat meningkatkan kemampuan pendeteksian terhadap kejadian dan anomali di area lingkungan *critical infrastructure* di PT XYZ. Kontrol-kontrol pada NIST SP 800-53 Rev5 tersebut antara lain AU-6 (*Audit, Record, Review, and Reporting*), CA-7 (*Continuous Monitoring*), RA-5 (*Vulnerability Monitoring and Scanning*), IR-4 (*Incident Handling*), SI-4 (*System Monitoring*), dan IR-8 (*Incident Response Plan*).
- Rekomendasi Peningkatan 6 (RP-6)
  RP 6 merupakan kumpulan kontrol yang dapat meningkatkan kemampuan pemantauan terhadap kejadian dan anomali di area lingkungan *critical infrastructure* di PT XYZ sebagai tindakan yang berkelanjutan. Kontrol-kontrol pada NIST SP 800-53 Rev5 tersebut antara lain AC-2 (*Account Management*), AU-13 (*Monitoring for Information Disclosure*), CA-7 (*Continuous Monitoring*), dan SI-4 (*System Monitoring*).
- Rekomendasi Peningkatan 7 (RP-7)
  RP 7 merupakan kumpulan kontrol yang dapat meningkatkan kemampuan pendeteksian ancaman di area lingkungan *critical infrastructure* di PT XYZ. Kontrol-kontrol pada NIST SP 800-53 Rev5 tersebut antara lain CA-2 (*Control Assessment*), CA-7 (*Continuous Monitoring*), dan PM-14 (*Testing, Training, and Monitoring*).
- Rekomendasi Peningkatan 8 (RP-8)
  RP 8 merupakan kumpulan kontrol yang dapat meningkatkan kemampuan proses menganalisis ancaman yang terjadi di area lingkungan *critical infrastructure* di PT XYZ. Kontrol-kontrol pada NIST SP 800-53 Rev5 tersebut adalah CP-2 (*Contingency Plan*), IR-4 (*Incident Handling*), dan RA-3 (*Risk Assessment*).
- Rekomendasi Peningkatan 9 (RP-9)
  RP 9 merupakan rekomendasi yang berisikan kontrol untuk peningkatan terhadap kontrol akses ke dalam sistem *critical* di PT XYZ. Total terdapat 7 kontrol yang direkomendasikan untuk seluruh skenario yang sudah dianalisis pada tahap sebelumnya yaitu CA-2 (*Control Assessment*), CA-7 (*Continuous Monitoring*), CA-8 (*Penetration Testing*), CP-2 (*Contingency Plan*), CP-4 (*Contingency Plan Testing*), IR-3 (*Incident Response Testing*), dan PM-6 (*Measure of Performance*).
- Rekomendasi Peningkatan 10 (RP-10)
  RP 10 merupakan rekomendasi yang berisikan kontrol untuk peningkatan terhadap keamanan data dimulai dari media penyimpanan sampai dengan proteksi yang dianjurkan. Total terdapat 20 kontrol yang direkomendasikan untuk seluruh skenario yang sudah dianalisis pada tahap sebelumnya yaitu MP-2 (*Media Access*), MP-3 (*Media Marking*), MP-4 (*Media Storage*), MP-5 (*Media Transport*), MP-6 (*Media Sanitation*), SC-28 (*Protection Information at Rest*), SC-8 (*Transmission Confidentiality and Integrity*), CM-8 (*System Component Inventory*), PE-20 (*Asset Monitoring and Tracking*), AU-4 (*Audit Log Capacity*), SC-5 (*Denial of Services Protection*), AC-4 (*Information Flow*

Enforcement), AC-6 (*Least Privilege*), SI-7 (*Software, Firmware, and Information Integrity*), dan SI-10 (*Information Input Validation*).

- Rekomendasi Peningkatan 11 (RP-11)
  RP 11 merupakan rekomendasi yang berisikan kontrol untuk peningkatan Solusi keamanan teknis untuk memastikan keamanan dan ketahanan sistem dan aset, konsisten dengan kebijakan dan prosedur. Kontrol yang dapat digunakan untuk menyelesaikan permasalah ini antara lain CP-7 (*Alternate Processing Site*), CP-13 (*Alternate Security Mechanism),* PL-8 (*Security and Privacy Architecture),* dan SC-6 (*Resource Availability*).

Untuk melengkapi rekomendasi yang sudah dibuat, hasil dari pada NIST CSF pada *framework core* yakni pada masing-masing fungsi didapatkan nilai *compliance* seperti pada Tabel 10 berikut.

Tabel 10. NIST CSF *compliance* matriks

No	Fungsi	Kategori	*Complaince*	Total
1	*Identify* (ID)	*Asset Management* (ID.AM)	50%	
		Business Environment (ID.BE)	50%	
		Governance (ID.GV)	75%	
		Risk Assessment (ID.RA)	42%	**59%**
		Risk Management Strategy (ID.RM)	83%	
		Supply Chain Risk Management (ID.SC)	70%	
2	*Protect* (PR)	*Access Control* (PR.AC):	86%	
		Awareness and Training (PR.AT)	90%	
		Data Security (PR.DS)	94%	
		Information Processes and Procedures (PR.IP)	88%	**90%**
		Maintenance (PR.MA)	100%	
		Protective Technology (PR.PT)	90%	
3	*Detect* (DR)	*Anomalies and Events* (DE.AE	70%	
		Security Continuous Monitoring (DE.CM)	69%	**75%**
		Detection Processes (DE.DP)	90%	
4	*Respond* (RS)	*Respon Planning* (RS.RP)	100%	
		Communications (RS.CO)	60%	
		Analysis (RS.AN)	50%	**64%**
		Mitigations (RS.MI)	100%	
		Improvements (RS.IM)	100%	
5	*Recover* (RC)	*Recovery Planning* (RC.RP)	100%	
		*Improvement*s (RC.IM)	100%	**100%**
		Communications (RC.CO)	100%	

Hasil penelitian yang sudah dianalisis kali ini sesuai dengan penelitian lain bahwa kerangka kerja *cybersecurity* dapat membantu melakukan peningkatan

kapasitas. Pada penelitian [10] kontrol-kontrol pada NIST SP 800-53 Rev. 5 membantu untuk mencapai level *tier 3* sesuai yang ditargerkan pada suatu divisi organisasi PT XYZ dan juga mempersiapkan untuk menghadapi ancaman risiko keamanan siber yang semakin marak terjadi [8]. Sebuah kerangka kerja keaman siber juga dapat meningkatkan tingkat kesuksesan penanganan *cyberattack* dengan cara melakukan manajemen keamanan secara tepat [2] bahkan dalam penelitian yang lain mengungkapkan karena penanganan yang berbeda-beda setiap kerangka kerja keamanan siber dapat diadaptasi sesuai dengan kebutuhan sehingga menjadi panduan yang *best practices* untuk organisasi tersebut [13] [14].

E. Simpulan

Pada paper ini peneliti melakukan serangkaian Penilaian risiko terhadap suatu organisasi XYZ dalam rangka meningkatkan kapasitas critical infrastructure. Penilaian dilakukan menggunakan kerangka kerja NIST CSF melalui 6 tahapan dan nilai compliance NIST pada fungsi core. Hasil yang didapatkan pada penilaian tersebut digunakan untuk memberikan peningkatan berupa rekomendasi perbaikan kapasitas critical infrastructure melalui kontrol-kontrol yang terdapat pada kerangka kerja NIST SP 800-53 Rev. 3. Penilaian risiko yang menemukan 107 macam skenario risiko yang membawa pada 11 rekomendasi area peningkatan *critical infrastructure* yaitu pembuatan inventori aset critical infrastructure, mendefinisikan setiap aset untuk kegiatan proses bisnis, melakukan analisis pada setiap aset *critical infrastructure*, peningkatan kapasitas pemrosesan informasi, meningkatkan kemampuan pendeteksian terhadap anomali keamanan siber, meningkatkan analisis kejadian anomali pada sistem pemantauan yang dimiliki, meningkatkan kemampuan pendeteksian terhadap ancaman keamanan siber, menerapkan kontrol terhadap akses ke dalam aset *critical infrastruktur*, peningkatan kualitas dan pemrosesan data, dan pembuatan roadmap solusi untuk peningkatan kapasistas *critical infrastructure* berdasarkan Penilaian risiko yang dilakukan. Dari temuan yang dihasilkan yang paling krusial dilakukan untuk peningkatan kapasitas tersebut adalah mengetahui risiko-risiko kejahatan siber, sehingga membuat organisasi menjadi lebih siap dalam menghadapinya.

Untuk selanjutnya, Penelitian ini juga masih membutuhkan validasi kepada *expert* untuk memastikan bahwa rekomendasi yang diberikan melalui penelitian bisa dilakukan dengan cakupan suatu organisasi XYZ. Penggunaan kerangka kerja sebagai alat penilaian risiko yang bervariasi juga bisa saling memvalidasi antara satu dengan yang lain untuk memastikan tercapainya tujuan keamanan siber organisasi yang mungkin bisa dilakukan penelitian di waktu yang akan datang.

F. Ucapan Terima Kasih

Terima kasih penulis ucapkan kepada PT XYZ yang sudah memberikan izin untuk organisasi tersebut digunakan sebagai tempat studi kasus, berikut dengan pihak-pihak yang terlibat dalam penyusunan penelitian ini.

G. Referensi

[1] B. Krumay, E. W. N. Bernroider, and R. Walser, *Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework*, vol. 11252 LNCS. Springer International Publishing, 2018. doi: 10.1007/978-3-030-03638-

6_23.
[2] M. Zammani and R. Razali, "An empirical study of information security management success factors," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 6, no. 6, pp. 904–913, 2016, doi: 10.18517/ijaseit.6.6.1371.
[3] IBM, "IBM security's cost of a data breach report 2022," 2022.
[4] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss," *Int. J. Informatics Vis.*, vol. 4, no. 4, pp. 225–230, 2020, doi: 10.30630/joiv.4.4.482.
[5] S. N. G. Gourisetti, M. Mylrea, and H. Patangia, "Cybersecurity vulnerability mitigation framework through empirical paradigm: Enhanced prioritized gap analysis," *Futur. Gener. Comput. Syst.*, vol. 105, pp. 410–431, 2020, doi: 10.1016/j.future.2019.12.018.
[6] M. Touhiduzzaman, S. N. G. Gourisetti, C. Eppinger, and A. Somani, "A Review of Cybersecurity Risk and Consequences for Critical Infrastructure," *Proc. - 2019 Resil. Week, RWS 2019*, pp. 7–13, 2019, doi: 10.1109/RWS47064.2019.8971975.
[7] PT XYZ, "Kebijakan Manajemen Sistem Keamanan Informasi," 2022.
[8] A. Ibrahim, C. Valli, I. McAteer, and J. Chaudhry, "A security review of local government using NIST CSF: a case study," *J. Supercomput.*, vol. 74, no. 10, pp. 5171–5186, 2018, doi: 10.1007/s11227-018-2479-2.
[9] R. Rahmawati, "Perancangan Manajemen Risiko Keamanan Informasi Sistem Informasi Manajemen Keimigrasian," University of Indonesia, 2023.
[10] A. Amiruddin, H. G. Afiansyah, and H. A. Nugroho, "Cyber-Risk Management Planning Using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8," *Proc. - 3rd Int. Conf. Informatics, Multimedia, Cyber, Inf. Syst. ICIMCIS 2021*, pp. 19–24, 2021, doi: 10.1109/ICIMCIS53775.2021.9699337.
[11] M. Al, F. Aditya, Y. Suryanto, and K. Ramli, "Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization : Case Study Combination Technique in Profit-Based O," *Procedia Comput. Sci.*, vol. 161, pp. 1206–1215, 2019, doi: 10.1016/j.procs.2019.11.234.
[12] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," 2014.
[13] A. Fernandes, A. Oliveira., L. Santos, and C. Rabadão, "A strategy for implementing a Security Incident Response Plan," pp. 1–10, 2021, doi: 10.34190/EWS.21.080.
[14] A. Aborujilah, A. Z. Al-othmani, N. S. Hussien, S. A. Mokhtar, Z. A. Long, and M. Nizam, "Cybersecurity Risk Assessment Approach for Malaysian Organizations : Malaysian Universities as Case Study," *IEEE*, pp. 440–450, 2022.