BAB 2
TINJAUAN PUSTAKA

Pada bab ini, akan dijelaskan mengenai teori-teori terkait penelitian yang bersumber dari buku, jurnal, artikel maupun media lain yang terpercaya sumbernya. Tujuannya adalah untuk memahami konsep dan teori penyelesaian permasalahan yang digunakan. Teori yang dibahas antara lain Institut Teknologi Kalimantan, *Cyber Security*, *Cyber Resilience*, *Cyber Resilience Review* dan penelitian terdahulu.

2.1 Institut Teknologi Kalimantan

Institut Teknologi Kalimantan merupakan perguruan tinggi yang fokus dalam bidang teknologi untuk menunjang kebutuhan dunia industri. Program pendidikan yang diselenggarakan oleh ITK dibentuk dengan harapan dapat meningkatkan pengetahuan dan keterampilan SDM, dimana yang dimaksud merupakan mahasiswa yang mengambil studi di ITK yang akan berdampak terhadap peningkatan penguasaaan teknologi dan peningkatan produktivitas modal. Sehingga, hal ini juga akan selaras dengan kemunculan industri-industri baru yang ada di Kalimantan. Disamping itu, penelitian-penelitian serta pengembangan terkait sains dan teknologi industri juga akan semakin kaya dengan kehadiran ITK sebagai perguruan tinggi negeri di bidang teknik. Terciptanya inovasi proses dan inovasi produk menjadi hal yang mungkin dengan banyaknya penelitian dalam peningkatan penguasaan teknologi (Institut Teknologi Kalimantan, 2016).

Berdirinya ITK di Kalimantan diharapkan memberikan dampak positif pada masyarakat umum maupun masyarakat industri di sekitarnya. Keberadaan staf pengajar dan hasil penelitian diharapkan dapat berkontribusi positif pada pembangunan wilayah secara optimal. Tujuan tersebut sesuai dengan fokus MP3EI bahwa Kalimantan sebagai koridor ekonomi pusat pengolahan hasil tambang dan lumbung energi nasional. Harapan besar diberikan oleh pemerintah pusat pada wilayah Kalimantan untuk melakukan akselerasi pertumbuhan

ekonomi sehingga dapat terjadi peningkatan pertumbuhan ekonomi secara nasional. Ketersediaan staf pengajar, hasil penelitian dan lulusan akan mempengaruhi faktor-faktor produksi dan pertumbuhan industri baik regional Kalimantan maupun nasional (Institut Teknologi Kalimantan, 2016).

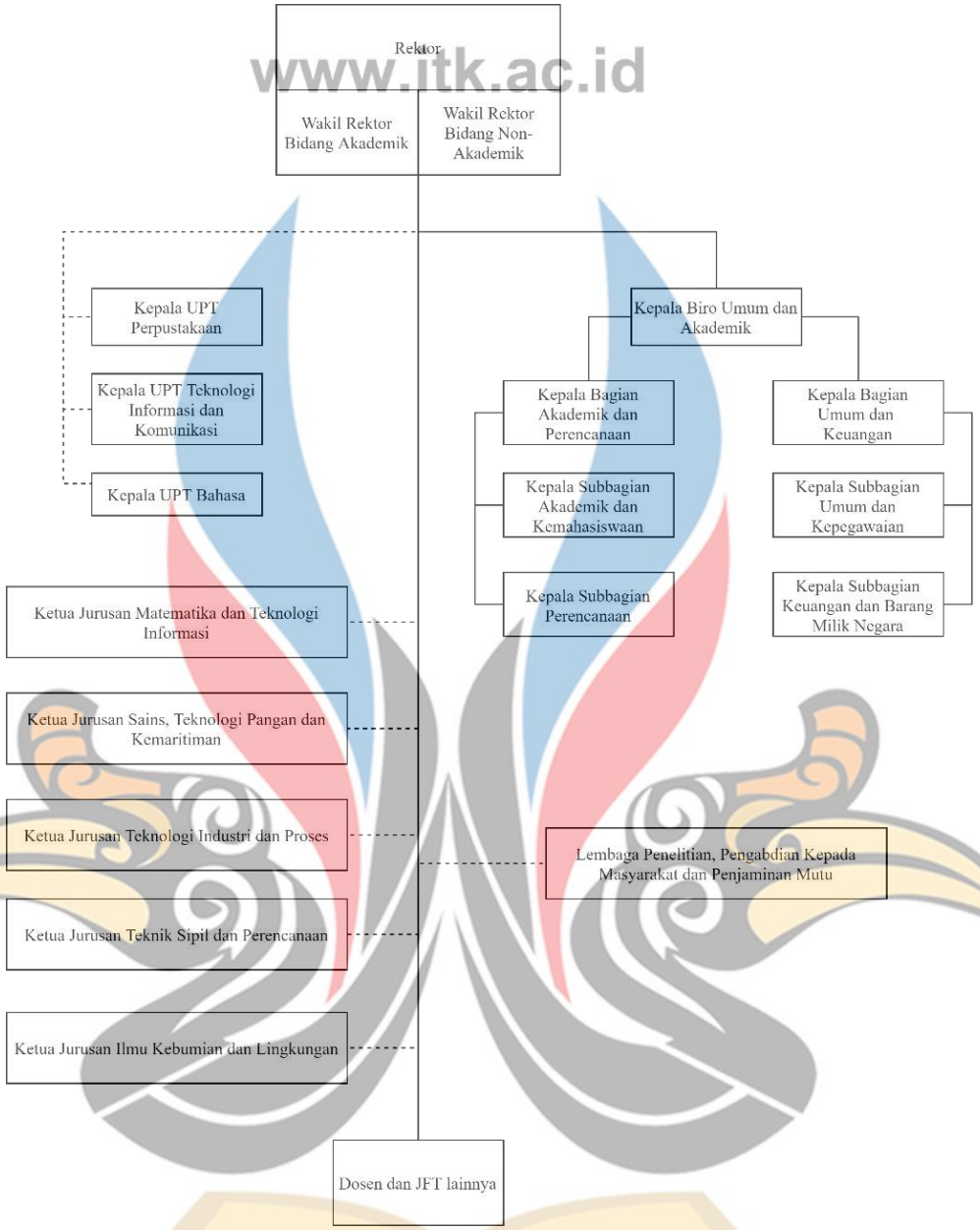
Adapun Visi dari Institut Teknologi Kalimantan sebagai berikut.

"Menjadi perguruan tinggi yang unggul dan berperan aktif dalam pembangunan nasional melalui pemberdayaan potensi daerah Kalimantan pada tahun 2025"

Dengan misi-misi yaitu:

1. Menyelenggarakan proses pendidikan tinggi yang berbasis pada penguasaan ilmu pengetahuan dan teknologi.
2. Berperan aktif dalam penelitian untuk menghasilkan inovasi proses dan produk sebagai upaya untuk memperkaya serta memperkuat ilmu pengetahuan dan teknologi.
3. Membangun kerjasama dan kontribusi pada pengabdian masyarakat yang didasarkan pada hasil penelitian dan potensi daerah untuk meningkatkan kesejahteraan masyarakat.

ITK memiliki berbagai aplikasi untuk menunjang kegiatan akademik dan operasional. Namun, aplikasi utama untuk memberikan layanan akademik yaitu Gerbang ITK, dimana berisikan sistem informasi akademik dan kemahasiswaan. Data-data yang dianggap krusial pada aplikasi Gerbang ITK yaitu data-data akademik mahasiswa maupun dosen, dapat berupa data diri, nilai maupun pencapaian kegiatan mahasiswa. Dalam menjalankan kegiatan akademik, ITK juga memiliki infrastruktur yang mendukung yaitu berupa jaringan internet dan server fisik.



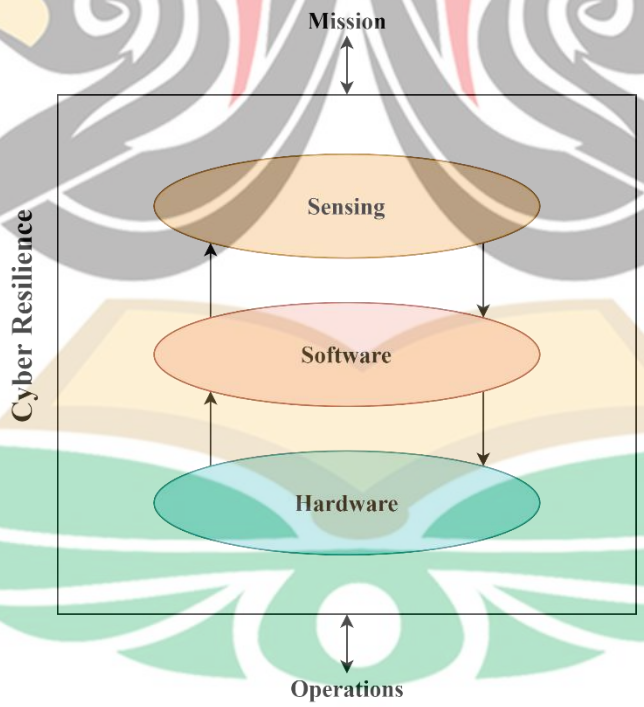
Gambar 2.1 Struktur Organisasi ITK

2.2 *Cyber Security* dan *Cyber Resilience*

Keamanan siber atau *cyber security* adalah serangkaian aktivitas dan pengukuran yang bertujuan untuk melindungi dari serangan, ancaman maupun disrupsi melalui elemen-elemen *cyberspace* (Fischer, 2009). *Cyberspace* merupakan tempat maya dimana suatu komunikasi dapat terjadi (Ardiyanti, 2014). Elemen-elemen *cyberspace* yaitu perangkat keras, perangkat lunak dan jaringan komputer (Islami, 2017). Keamanan siber juga dapat diartikan sebagai mekanisme

yang dibuat dalam perlindungan suatu kerahasiaan, integritas dan ketersediaan informasi (Riyandhika & Pratama, 2020). Mekanisme tersebut dibuat sebagai bentuk perlindungan dari serangan yang dilakukan di dunia maya atau biasa disebut dengan *cyber attack*. Keamanan Siber memiliki fungsi atau peran untuk menemukan, memperbaiki maupun mengurangi tingkat risiko terhadap ancaman siber (*cyber threat*) dan serangan siber (*cyber attack*) (Ramadhani & Pratama, 2020). Istilah keamanan siber dapat berlaku dalam berbagai konteks, dari bisnis ke komputasi perangkat bergerak, dan dapat dibagi menjadi beberapa kategori umum seperti keamanan jaringan, keamanan informasi dan edukasi pengguna akhir (Rahmadi & Pratama, 2020).

Ketahanan siber atau *cyber resilience* adalah kemampuan sistem untuk mempersiapkan, menyerap, memulihkan, dan beradaptasi dengan efek yang dapat merugikan, terutama terkait dengan serangan siber (Linkov & Kott, 2019). Selain itu, ketahanan siber juga dapat diartikan sebagai kemampuan untuk terus memberikan hasil yang diinginkan meskipun terjadi insiden siber yang merugikan (Björck, et al., 2015).



Gambar 2.2 *Domain* Ketahanan Siber

Sumber: Linkov & Kott, 2019

Pada Gambar 2.2, menjelaskan *domain* ketahanan siber. Ketahanan siber harus dipertimbangkan dalam konteks sistem yang kompleks yang tidak hanya terdiri dari fisik dan informasi tetapi juga ranah kognitif dan sosial (Smith, 2005). Ketahanan siber memastikan bahwa pemulihan sistem terjadi dengan mempertimbangkan perangkat keras, perangkat lunak dan komponen penginderaan infrastruktur siber yang saling berhubungan. Ketahanan siber merupakan jembatan antara pertahanan operasi sistem dengan pelaksanaan misi.

Ketahanan siber (*cyber resilience*) dengan keamanan siber (*cyber security*) memiliki karakteristik yang tidak jauh berbeda. Berikut merupakan perbedaan dari keduanya.

Tabel 2.1 Karakteristik Keamanan Siber dan Ketahanan Siber [*)]

No	Aspek	Keamanan Siber	Ketahanan Siber
1	Objektif	Lindungi sistem dan teknologi informasi	Memastikan keberlanjutan bisnis
2	Rencana	Aman dari kegagalan	Aman untuk gagal
3	Pendekatan	Terapkan keamanan dari luar	Bangun keamanan dari dalam
4	Arsitektur	Perlindungan berlapis tunggal	Perlindungan multi lapis
5	Cakupan	Atomistik, satu organisasi	Holistik, jaringan organisasi

[*)] Björck, et al., 2015

2.3 *Cyber Resilience Review*

Cyber Resilience Review atau disingkat dengan CRR adalah sebuah metode penilaian ringan yang dibuat oleh Department of Homeland Security (DHS) dengan tujuan untuk mengevaluasi praktik keamanan siber dan kontinuitas layanan dari pemilik dan operator infrastruktur kritis. CRR memiliki 299 pertanyaan dalam mengevaluasi praktik keamanan siber. CRR menyediakan dua metode untuk melakukan evaluasi yaitu *six-hour workshop* yang difasilitasi oleh DHS dan *self-assessment*. Kedua metode berisikan pertanyaan, mekanisme penilaian, dan opsi untuk perbaikan yang sama. CRR adalah penilaian berbasis wawancara dari program manajemen keamanan siber organisasi. Wawancara yang dilakukan berupaya untuk memahami manajemen layanan keamanan siber dan aset terkaitnya, yang sangat penting untuk keberhasilan misi organisasi. CRR

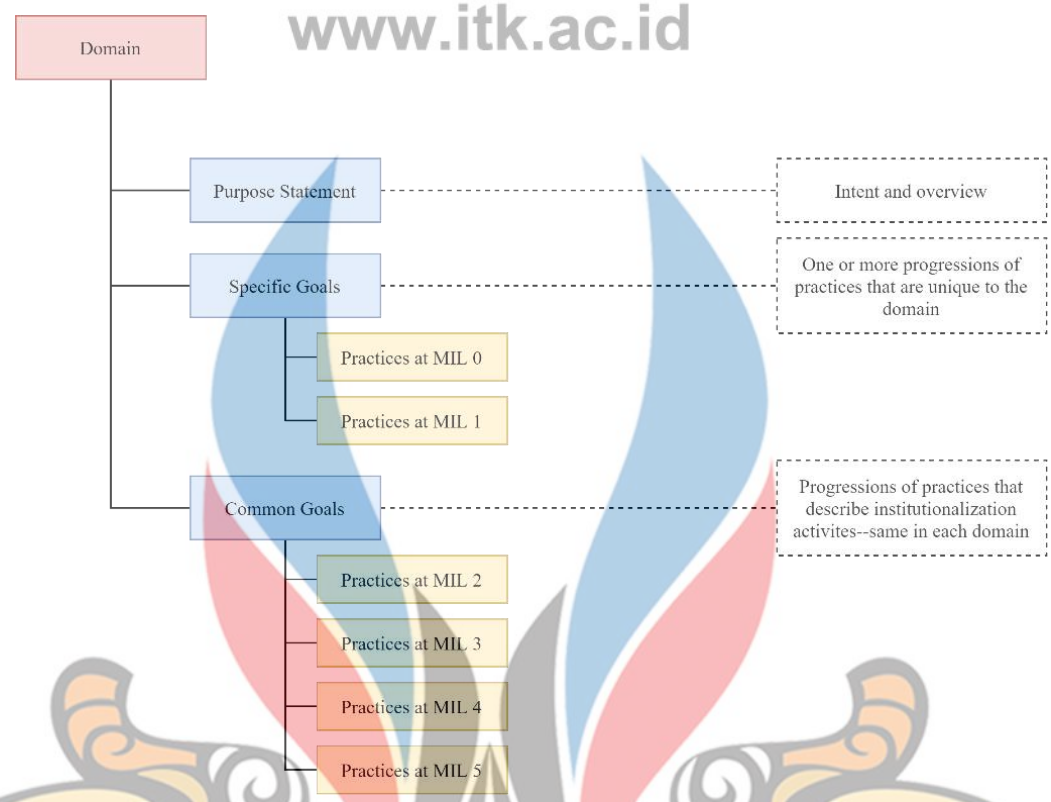
berfokus pada praktik perlindungan dan keberlanjutan dalam area utama yang umumnya berkontribusi pada ketahanan siber keseluruhan organisasi. CRR mengukur kemampuan dan perilaku *cybersecurity* kritis untuk memberikan indikator yang berarti dari ketahanan operasional organisasi selama operasi normal dan selama masa tekanan operasional. CRR menggunakan *Maturity Indicator Levels* (MILs) untuk memberi organisasi perkiraan kematangan praktik yang dilakukan pada 10 *domain* cybersecurity. Pada Tabel 2.2 merincikan *domain* praktik yang diperiksa oleh CRR. Setiap *domain* mewakili kapabilitas penting yang berkontribusi pada ketahanan dunia maya suatu organisasi.

Tabel 2.2 Komposisi CRR *Domains* *)

No	CRR *Domain*	Jumlah Tujuan	Jumlah Praktik Tujuan	Jumlah Praktik MIL
1	*Asset Management*	7	30	13
2	*Controls Management*	4	16	13
3	*Configuration and Change Management*	3	23	13
4	*Vulnerability Management*	4	15	13
5	*Incident Management*	5	23	13
6	*Service Continuity Management*	4	16	13
7	*Risk Management*	5	13	13
8	*External Dependencies Management*	5	14	13
9	*Training and Awareness*	2	11	13
10	*Situational Awareness*	3	8	13

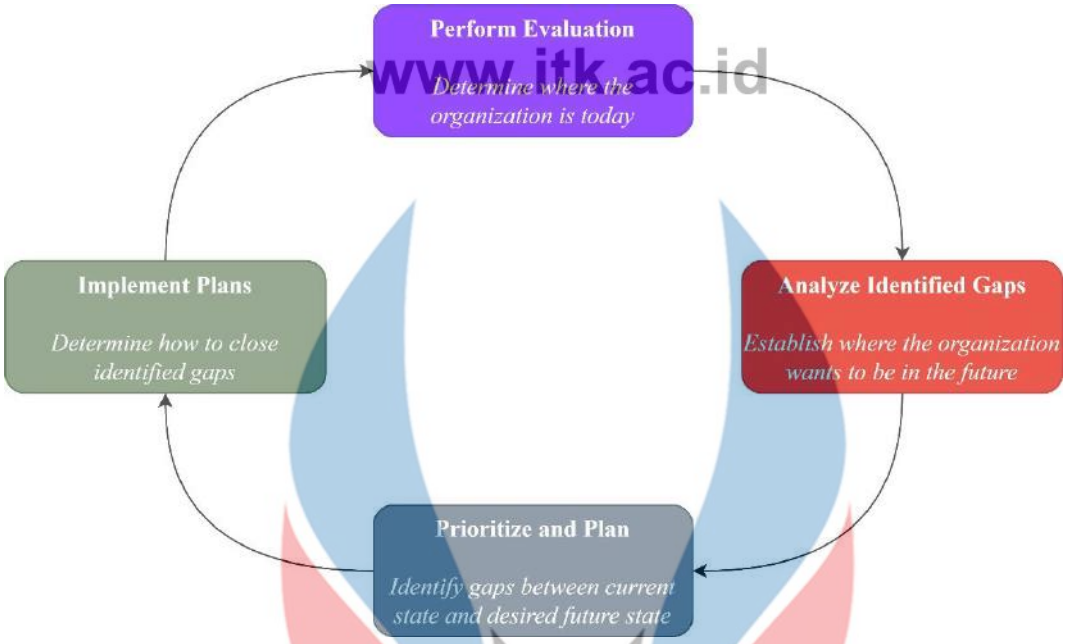
*) CRR, 2020

Setiap *domain* terdiri dari pernyataan tujuan, satu set tujuan spesifik, pertanyaan praktik untuk *domain* tersebut dan satu set standar pertanyaan *Maturity Indicator Level* (MIL). Pertanyaan MIL memeriksa praktik *institutionalization* dalam sebuah organisasi. Gambar 2.3 secara grafis menyajikan arsitektur CRR *domain*. Seperti yang ditunjukkan pada Tabel 2.2, jumlah tujuan dan soal latihan bervariasi menurut *domain*, tetapi set pertanyaan MIL dan konsep yang dicakupnya sama untuk semua *domain*. Semua pertanyaan CRR memiliki tiga kemungkinan respons: "Iya", "Tidak", dan "Tidak lengkap".



Gambar 2.3 Arsitektur CRR *Domains*
Sumber: CRR, 2020

Pada Gambar 2.3, merupakan arsitektur *domain* CRR yang menjelaskan praktik-praktik tiap tingkatan MIL. MIL 0 dan MIL 1 memiliki praktik – praktik unik untuk setiap *domain* yang terdiri dari satu atau lebih praktik. Sedangkan MIL 2 sampai 5 memiliki praktik yang menggambarkan kegiatan *institutionalization* dan praktik tersebut sama di setiap *domain*.



Gambar 2.4 Langkah-Langkah CRR
Sumber: CRR, 2020

Pada Gambar 2.4, merupakan langkah-langkah yang diberikan oleh CRR untuk melakukan evaluasi ketahanan siber. Langkah-langkah tersebut antara lain melakukan evaluasi, analisis dan identifikasi *gaps*, merencanakan dan memprioritaskan serta mengimplementasikan rencana. Pada langkah melakukan evaluasi, akan dilakukan penentuan kondisi organisasi saat ini. Setelah itu, dilakukan analisis dan identifikasi *gaps* untuk menetapkan kondisi masa depan keinginan sebuah organisasi. Selanjutnya, dilakukan memprioritaskan dan merencanakan dengan identifikasi *gaps* antara kondisi saat ini dengan kondisi masa depan yang diinginkan. Terakhir, akan dilakukan implementasi rencana yang telah ditetapkan untuk menutup *gaps* yang telah teridentifikasi. Pada Tabel 2.3 akan dijelaskan rekomendasi *input*, aktivitas dan *output* dari tiap langkah-langkah CRR.

Tabel 2.3 Rekomendasi Proses Tahapan CRR *)

No		*Inputs*	Aktivitas	*Outputs*
1	*Perform Evaluation*	• CRR *Self-Assessment* • Kebijakan dan prosedur	Lakukan CRR *Self-Assessment*	CRR *Self-Assessment Report*

No		*Inputs*	Aktivitas	*Outputs*
		organisasi • Memahami manajemen dan operasi keamanan siber saat ini		
2	*Analyze Identified Gaps*	• CRR *Self-Assessment Report* • Memahami tujuan organisasi sehubungan dengan layanan kritis dan dampaknya pada infrastruktur kritis	• Menganalisis kesenjangan dalam konteks organisasi (misalnya, toleransi risiko atau profil ancaman) • Tentukan dampak potensial dari kesenjangan untuk tujuan organisasi dan dampak pada layanan kritis dan infrastruktur kritis • Tentukan celah mana yang harus mendapat perhatian lebih lanjut	Daftar celah dan potensi dampak
3	*Prioritize and Plan*	• Daftar celah dan potensi dampak • Pemahaman tentang kendala organisasi (misalnya, sumber daya, undang-undang)	• Identifikasi tindakan potensial untuk mengatasi kesenjangan • Lakukan analisis biaya-manfaat (CBA) untuk tindakan • Memprioritaskan kesenjangan dan tindakan berdasarkan CBA dan dampak • Mengembangkan rencana untuk melaksanakan tindakan yang diprioritaskan	Rencana implementasi yang diprioritaskan
4	*Implement Plans*	Rencana implementasi yang diprioritaskan	• Memantau dan mengukur kemajuan implementasi terhadap rencana • Mengevaluasi kembali secara	Data pelacakan rencana perbaikan

No	*Inputs*	Aktivitas	*Outputs*
		berkala dan menanggapi perubahan besar dalam lingkungan risiko	

*) CRR, 2020

2.3.1 *Asset Management* (AM)

Domain AM menetapkan metode bagi organisasi untuk merencanakan, mengidentifikasi, mendokumentasikan, dan mengelola asetnya. Tujuan *domain* manajemen aset yaitu mengidentifikasi, mendokumentasikan, dan mengelola aset selama siklus hidupnya untuk memastikan produktivitas yang berkelanjutan guna mendukung layanan penting. Aset adalah bahan mentah yang dibutuhkan layanan untuk beroperasi. CRR mengatur aset ke dalam kategori berikut:

1. Orang-orang untuk mengoperasikan dan memantau layanan
2. Informasi dan data untuk memberi input pada proses dan akan diolah oleh layanan
3. Teknologi untuk mengautomasikan dan mendukung layanan
4. Fasilitas untuk melakukan layanan

Domain AM terdiri dari 7 tujuan dan 30 praktik (Tabel 2.4).

Tabel 2.4 Tujuan dan Praktik *Domain* AM *)

CRR *Domain*	Tujuan	Praktik
Asset Management	Layanan diidentifikasi dan diprioritaskan	Layanan organisasi diidentifikasi
		Layanan organisasi diprioritaskan berdasarkan analisis dampak potensial jika layanan terganggu
		Misi, visi, nilai dan tujuan organisasi, termasuk tempat organisasi dalam infrastruktur kritis, diidentifikasi dan dikomunikasikan
		Misi, tujuan, dan kegiatan organisasi diprioritaskan
	Aset diinventarisasi, dan otoritas serta tanggung jawab untuk aset ini	Aset yang secara langsung mendukung layanan kritis diinventarisasi (teknologi termasuk perangkat keras, perangkat lunak, dan sistem informasi eksternal)
		Uraian aset mencakup persyaratan

CRR *Domain*	Tujuan	Praktik
	ditetapkan	perlindungan dan keberlanjutan
		Pemilik dan penjaga aset didokumentasikan dalam deskripsi aset
		Lokasi fisik aset (baik di dalam maupun di luar organisasi) didokumentasikan dalam inventaris aset
		Komunikasi organisasi dan arus data dipetakan dan didokumentasikan dalam inventaris aset
	Hubungan antara aset dan layanan yang mereka dukung terjalin	Asosiasi antara aset dan layanan kritis yang didukungnya didokumentasikan
		Persyaratan kerahasiaan, integritas, dan ketersediaan ditetapkan untuk setiap aset terkait layanan
	Persediaan aset dikelola	Kriteria perubahan ditetapkan untuk deskripsi aset.
		Deskripsi aset diperbarui ketika terjadi perubahan pada aset
	Akses ke aset dikelola	Akses (termasuk identitas dan kredensial) ke aset diberikan berdasarkan persyaratan perlindungannya.
		Permintaan akses (termasuk identitas dan kredensial) ditinjau dan disetujui oleh pemilik aset.
		Hak istimewa akses ditinjau untuk mengidentifikasi hak istimewa yang berlebihan atau tidak pantas.
		Hak akses diubah sebagai hasil tinjauan.
		Izin akses dikelola dengan memasukkan prinsip hak istimewa terkecil.
		Izin akses dikelola dengan prinsip pemisahan tugas.
		Identitas (misalnya, akun pengguna) dibuktikan sebelum mereka terikat ke kredensial yang ditegaskan dalam interaksi.
	Aset informasi dikategorikan dan dikelola untuk memastikan keberlanjutan dan perlindungan layanan kritis	Aset informasi dikategorikan berdasarkan sensitivitas dan potensi dampak terhadap layanan kritis (seperti publik, penggunaan internal saja, atau rahasia).
		Kategorisasi aset informasi dipantau dan ditegakkan.
		Kebijakan dan prosedur untuk pelabelan yang tepat dan penanganan aset informasi dibuat.
		Semua anggota staf yang menangani aset informasi (termasuk mereka yang berada di

CRR *Domain*	Tujuan	Praktik
		luar organisasi, seperti kontraktor) dilatih dalam penggunaan kategori informasi.
		Aset informasi bernilai tinggi dicadangkan dan disimpan.
		Dibuat pedoman untuk membuang aset informasi dengan benar.
		Kepatuhan terhadap pedoman pembuangan aset informasi dipantau dan ditegakkan.
	Aset fasilitas yang mendukung layanan kritis diprioritaskan dan dikelola	Fasilitas diprioritaskan berdasarkan potensi dampaknya terhadap layanan kritis, untuk mengidentifikasi fasilitas yang harus menjadi fokus kegiatan perlindungan dan pelestarian.
		Prioritas fasilitas ditinjau dan divalidasi.
		Persyaratan perlindungan dan pemeliharaan layanan kritis dipertimbangkan selama pemilihan fasilitas.

*) CRR, 2020

2.3.2 *Controls Management* (CM)

Kontrol internal adalah proses tata kelola yang digunakan oleh organisasi untuk memastikan pencapaian tujuan organisasi yang efektif dan efisien dan untuk memberikan jaminan keberhasilan yang wajar. *Domain CM* yang dijelaskan dalam CRR menyajikan cara bagi organisasi untuk mengidentifikasi tujuan kontrol dan menetapkan kontrol untuk memenuhi tujuan tersebut. *Domain* Manajemen Kontrol juga membahas pentingnya menganalisis dan menilai kontrol tersebut untuk memastikan bahwa proses terus ditingkatkan. Tujuan dari *domain* ini yaitu mengidentifikasi, menganalisis, dan mengelola kontrol dalam lingkungan operasi layanan kritis. *Domain* CM terdiri dari 4 tujuan dan 16 praktik (Tabel 2.5).

Tabel 2.5 Tujuan dan Praktik *Domain* CM *)

CRR *Domain*	Tujuan	Praktik
Controls Management	Tujuan kontrol ditetapkan	Tujuan kontrol ditetapkan untuk aset yang diperlukan untuk penyampaian layanan kritis.
		Sasaran kontrol diprioritaskan sesuai dengan potensinya untuk mempengaruhi layanan kritis.

CRR *Domain*	Tujuan	Praktik
		Kontrol diimplementasikan untuk mencapai tujuan kontrol yang ditetapkan untuk layanan kritis.
		Kontrol diterapkan, menggabungkan pemisahan jaringan jika sesuai, untuk melindungi integritas jaringan.
		Kontrol diterapkan untuk melindungi data saat tidak aktif.
		Kontrol diterapkan untuk melindungi data dalam perjalanan.
		Kontrol diterapkan untuk melindungi dari kebocoran data.
	Kontrol diterapkan	Catatan audit / *log* ditentukan, didokumentasikan, dilaksanakan, dan ditinjau sesuai dengan kebijakan.
		Kontrol diterapkan untuk melindungi dan membatasi penggunaan media yang dapat dipindahkan sesuai dengan kebijakan.
		Kontrol diterapkan untuk melindungi komunikasi dan jaringan kontrol.
		Praktik sumber daya manusia *cybersecurity* diimplementasikan untuk layanan kritis (misalnya, *de-provisioning*, penyaringan personel).
		Akses ke sistem dan aset dikendalikan dengan memasukkan prinsip fungsionalitas paling rendah (misalnya, daftar putih, daftar hitam, dll.).
	Desain kontrol dianalisis untuk memastikannya memenuhi tujuan kontrol	Desain kontrol dianalisis untuk mengidentifikasi celah di mana tujuan kontrol tidak cukup terpenuhi
		Sebagai hasil dari analisis kontrol, kontrol baru diperkenalkan atau kontrol yang ada dimodifikasi untuk mengatasi kesenjangan
	Sistem kontrol internal dinilai untuk memastikan tujuan kontrol terpenuhi	Kinerja kontrol dinilai berdasarkan jadwal untuk memverifikasi bahwa kontrol tersebut terus memenuhi tujuan kontrol
		Sebagai hasil dari penilaian terjadwal, kontrol baru diperkenalkan atau kontrol yang ada dimodifikasi untuk mengatasi area masalah

*) CRR, 2020

2.3.3 *Configuration and Change Management* (CCM)

Infrastruktur aset organisasi terus berkembang seiring dengan perubahan teknologi, informasi diperbarui, dan personel baru dipekerjakan. *Domain* CCM membahas bagaimana organisasi dapat menerapkan proses dan prosedur yang mengelola aset dan memastikan bahwa perubahan yang dilakukan pada aset tersebut dapat meminimalisir gangguan terhadap organisasi. Tujuan dari *domain* ini yaitu menetapkan proses untuk memastikan integritas aset, menggunakan kontrol perubahan dan audit kontrol perubahan. *Domain* CCM terdiri dari 3 tujuan dan 23 praktik (Tabel 2.6).

Tabel 2.6 Tujuan dan Praktik *Domain* CCM [*)]

CRR *Domain*	Tujuan	Praktik
Configuration and Change Management	Siklus hidup aset dikelola	Proses manajemen perubahan digunakan untuk mengelola modifikasi pada aset.
		Persyaratan ketahanan dievaluasi sebagai hasil dari perubahan aset.
		Manajemen kapasitas dan perencanaan dilakukan untuk aset.
		Permintaan perubahan dilacak hingga penutupan.
		Pemangku kepentingan diberitahu ketika mereka terpengaruh oleh perubahan aset.
		Siklus Hidup Pengembangan Sistem diimplementasikan untuk mengelola sistem yang mendukung layanan kritis.
	Integritas aset teknologi dan informasi dikelola	Manajemen konfigurasi dilakukan untuk aset teknologi.
		Teknik digunakan untuk mendeteksi perubahan pada aset teknologi.
		Modifikasi aset teknologi ditinjau.
		Persyaratan integritas digunakan untuk menentukan anggota staf mana yang berwenang untuk mengubah aset informasi.
		Integritas aset informasi dipantau.
		Modifikasi yang tidak sah atau tidak dijelaskan pada aset teknologi ditangani.
		Modifikasi aset teknologi diuji sebelum diterapkan pada sistem produksi.
		Proses untuk mengelola akses ke aset teknologi dilaksanakan.
		Pemeliharaan dan perbaikan aset dilakukan dan dicatat tepat waktu.

CRR *Domain*	Tujuan	Praktik
		Pemeliharaan dan perbaikan aset dilakukan dengan alat dan / atau metode yang disetujui dan dikendalikan.
		Pemeliharaan dan perbaikan aset dari jarak jauh disetujui, dicatat, dan dilakukan dengan cara yang mencegah akses yang tidak sah.
	Baseline konfigurasi aset ditetapkan	*Baseline* konfigurasi aset teknologi dibuat.
		Persetujuan diperoleh untuk perubahan yang diusulkan pada *baseline*.
		Baseline operasi jaringan ditetapkan.
		Baseline operasi jaringan dikelola.
		Baseline aliran data yang diharapkan untuk pengguna dan sistem dibuat.
		Baseline aliran data yang diharapkan untuk pengguna dan sistem dikelola.

*) CRR, 2020

2.3.4 *Vulnerability Management* (VM)

Vulnerability atau kerentanan adalah kerentanan aset dan layanan kritis terkait terhadap gangguan. Kerentanan dapat mengakibatkan risiko operasional dan harus diidentifikasi serta dikelola untuk menghindari gangguan pada lingkungan pengoperasian layanan kritis. Proses manajemen kerentanan terdiri dari mengidentifikasi dan menganalisis kerentanan sebelum dieksploitasi dan menginformasikan organisasi tentang ancaman yang harus dianalisis dalam proses manajemen risiko untuk menentukan apakah mereka menimbulkan risiko nyata bagi organisasi berdasarkan toleransi risiko organisasi. Tujuan dari *domain* ini yaitu mengidentifikasi, menganalisis, dan mengelola kerentanan di lingkungan operasi layanan kritis. *Domain* VM terdiri dari 4 tujuan dan 15 praktik (Tabel 2.7).

Tabel 2.7 Tujuan dan Praktik *Domain* VM *)

CRR *Domain*	Tujuan	Praktik
Vulnerability Management	Persiapan untuk analisis kerentanan dan kegiatan resolusi	Analisis kerentanan dan strategi resolusi telah dikembangkan.
		Ada seperangkat alat dan / atau metode standar yang digunakan untuk mengidentifikasi kerentanan dalam aset.

CRR *Domain*	Tujuan	Praktik
	dilakukan	Seperangkat alat dan / atau metode standar digunakan untuk mendeteksi kode berbahaya dalam aset.
		Seperangkat alat dan / atau metode standar digunakan untuk mendeteksi kode seluler yang tidak sah dalam aset.
		Seperangkat alat dan / atau metode standar digunakan untuk memantau aset untuk personel, koneksi, perangkat, dan perangkat lunak yang tidak berwenang.
	Sebuah proses untuk mengidentifikasi dan menganalisis kerentanan dibuat dan dipelihara	Sumber informasi kerentanan telah diidentifikasi.
		Informasi dari sumber-sumber ini terus diperbarui.
		Kerentanan secara aktif ditemukan.
		Kerentanan dikategorikan dan diprioritaskan.
		Kerentanan dianalisis untuk menentukan relevansinya dengan organisasi.
		Repositori digunakan untuk mencatat informasi tentang kerentanan dan penyelesaiannya.
	Pemaparan terhadap kerentanan yang teridentifikasi dikelola	Tindakan diambil untuk mengelola keterpaparan terhadap kerentanan yang teridentifikasi.
		Kaji ulang efektivitas mitigasi kerentanan.
		Status kerentanan yang belum terselesaikan dipantau.
	Akar penyebab kerentanan ditangani	Penyebab yang mendasari kerentanan diidentifikasi (melalui analisis akar penyebab atau cara lain) dan ditangani

*) CRR, 2020

2.3.5 *Incident Management* (IM)

Gangguan terhadap lingkungan operasi organisasi terjadi secara teratur. *Domain* IM memeriksa kemampuan organisasi untuk mengenali potensi gangguan, menganalisisnya, dan menentukan bagaimana dan kapan harus merespons. Tujuan dari *domain* ini yaitu menetapkan proses untuk mengidentifikasi dan menganalisis insiden, mendeteksi insiden dan menentukan respon organisasi. *Domain* IM terdiri dari 5 tujuan dan 23 praktik (Tabel 2.8).

Tabel 2.8 Tujuan dan Praktik *Domain* IM *)

CRR *Domain*	Tujuan	Praktik
Incident Management	Sebuah proses untuk mengidentifikasi, menganalisis, menanggapi, dan belajar dari insiden ditetapkan	Organisasi memiliki rencana untuk mengelola insiden.
		Rencana manajemen insiden ditinjau dan diperbarui.
		Peran dan tanggung jawab dalam rencana tersebut tercakup dalam uraian tugas.
		Staf telah ditugaskan untuk peran dan tanggung jawab yang dirinci dalam rencana manajemen insiden.
	Sebuah proses untuk mendeteksi, melaporkan, dan menganalisis insiden ditetapkan	Insiden terdeteksi dan dilaporkan (termasuk insiden keamanan siber yang terkait dengan aktivitas personel, aktivitas jaringan, lingkungan fisik, dan informasi).
		Data insiden dicatat dalam basis pengetahuan insiden atau mekanisme serupa.
		Acara dikategorikan.
		Insiden dianalisis untuk menentukan apakah insiden tersebut terkait dengan insiden lain.
		Acara diprioritaskan.
		Status insiden dilacak.
		Acara dikelola untuk resolusi.
		Persyaratan (aturan, hukum, regulasi, kebijakan, dll.) Untuk mengidentifikasi bukti kejadian untuk tujuan forensik diidentifikasi.
		Sebuah proses untuk memastikan bukti kejadian ditangani seperti yang dipersyaratkan oleh hukum atau kewajiban lainnya diikuti.
	Insiden diumumkan	Insiden diumumkan
		Kriteria untuk deklarasi insiden ditetapkan.
		Insiden dianalisis untuk menentukan tanggapan.
	Sebuah proses untuk menanggapi dan memulihkan dari insiden ditetapkan	Insiden eskalasi ke pemangku kepentingan untuk mendapatkan masukan dan penyelesaian.
		Tanggapan terhadap insiden yang diumumkan dikembangkan dan diterapkan sesuai dengan prosedur yang telah ditentukan sebelumnya.
		Status insiden dan tanggapan dikomunikasikan kepada pihak yang terkena dampak (termasuk staf hubungan

CRR *Domain*	Tujuan	Praktik
		masyarakat dan outlet media eksternal).
		Insiden dilacak ke resolusi.
	Pelajaran pasca insiden diterjemahkan ke dalam strategi perbaikan	Analisis dilakukan untuk menentukan akar penyebab insiden.
		Hubungan antara proses manajemen insiden dan proses terkait lainnya (manajemen masalah, manajemen risiko, manajemen perubahan, dll.) Dibuat.
		Pelajaran yang didapat dari manajemen insiden digunakan untuk meningkatkan perlindungan aset dan strategi kesinambungan layanan.

*) CRR, 2020

2.3.6 *Service Continuity Management* (SCM)

Keberlangsungan layanan merupakan proses menilai, memprioritaskan, merencanakan dan menanggapi, serta meningkatkan rencana untuk mengatasi insiden yang mengganggu. Tujuan dari keberlangsungan layanan adalah untuk memitigasi dampak insiden yang mengganggu dengan memanfaatkan rencana yang diuji atau dilaksanakan yang memfasilitasi kelangsungan layanan kritis yang dapat diprediksi dan konsisten. *Domain* SCM dibuat dengan tujuan memastikan kelangsungan operasi layanan kritis dan aset terkait jika terjadi gangguan sebagai akibat dari insiden, bencana, atau insiden lainnya. *Domain* SCM terdiri dari 4 tujuan dan 16 praktik (Tabel 2.9).

Tabel 2.9 Tujuan dan Pratik *Domain* SCM *)

CRR *Domain*	Tujuan	Praktik
Service Continuity Management	Rencana kesinambungan layanan untuk layanan bernilai tinggi dikembangkan	Rencana kesinambungan layanan dikembangkan dan didokumentasikan untuk aset (orang, informasi, teknologi, dan fasilitas) yang diperlukan untuk penyampaian layanan kritis.
		Rencana kesinambungan layanan dikembangkan dengan menggunakan standar, pedoman, dan templat yang ditetapkan.
		Anggota staf ditugaskan untuk melaksanakan rencana kesinambungan layanan tertentu.
		Kontak kunci diidentifikasi dalam rencana

CRR *Domain*	Tujuan	Praktik
		kesinambungan layanan.
		Rencana kesinambungan layanan disimpan dengan cara yang terkendali dan tersedia untuk semua orang yang perlu tahu.
		Persyaratan ketersediaan seperti tujuan waktu pemulihan dan tujuan titik pemulihan ditetapkan.
		Mekanisme (misalnya, keselamatan dari kegagalan, penyeimbangan beban, kemampuan *hot swap*) diterapkan untuk mencapai persyaratan ketahanan dalam situasi normal dan buruk.
	Rencana kesinambungan layanan ditinjau untuk menyelesaikan konflik antar rencana	Rencana ditinjau untuk mengidentifikasi dan menyelesaikan konflik
	Rencana kesinambungan layanan diuji untuk memastikannya memenuhi tujuan yang telah ditetapkan	Standar untuk pengujian rencana kesinambungan layanan telah diterapkan.
		Jadwal pengujian rencana kesinambungan layanan telah ditetapkan.
		Rencana kesinambungan layanan diuji.
		Prosedur pencadangan dan penyimpanan untuk aset informasi bernilai tinggi diuji.
		Hasil pengujian dibandingkan dengan tujuan pengujian untuk mengidentifikasi perbaikan yang diperlukan untuk rencana kesinambungan layanan.
	Rencana kesinambungan layanan dijalankan dan ditinjau	Kondisi telah diidentifikasi yang memicu pelaksanaan rencana kesinambungan layanan.
		Pelaksanaan rencana kesinambungan layanan ditinjau.
		Perbaikan diidentifikasi sebagai hasil dari pelaksanaan rencana kesinambungan layanan.

*) CRR, 2020

2.3.7 *Risk Management* (RM)

Manajemen risiko adalah aktivitas dasar untuk setiap organisasi dan dipraktikkan di semua tingkatan, dari eksekutif hingga individu dalam unit bisnis.

CRR berfokus pada risiko terhadap operasi yang bergantung pada siber yang berpotensi mengganggu pengiriman layanan kritis yang sedang diperiksa. Meskipun CRR berfokus pada risiko operasional, perlu dicatat bahwa manajemen risiko operasional memerlukan pendekatan yang komprehensif agar efektif. Tujuan dari *domain* ini yaitu mengidentifikasi, menganalisis, dan memitigasi risiko terhadap aset layanan penting yang dapat berdampak negatif terhadap operasi dan penyampaian layanan. *Domain* RM terdiri dari 5 tujuan dan 13 praktik (Tabel 2.10)

Tabel 2.10 Tujuan dan Pratik *Domain* RM [*)]

CRR *Domain*	Tujuan	Praktik
Risk Management	Strategi untuk mengidentifikasi, menganalisis, dan memitigasi risiko dikembangkan.	Sumber risiko yang dapat mempengaruhi operasi telah diidentifikasi.
		Kategori risiko telah ditetapkan.
		Rencana pengelolaan risiko operasional telah ditetapkan.
		Rencana pengelolaan risiko operasional telah dikomunikasikan kepada pemangku kepentingan.
	Toleransi risiko diidentifikasi, dan fokus kegiatan manajemen risiko ditetapkan	Area dampak, seperti reputasi, kesehatan keuangan, dan kepatuhan peraturan, telah diidentifikasi.
		Daerah dampak telah diprioritaskan untuk menentukan kepentingan relatifnya.
		Parameter toleransi risiko telah ditetapkan untuk setiap area dampak.
		Ambang batas toleransi risiko, yang memicu tindakan, ditetapkan untuk setiap kategori risiko.
	Risiko diidentifikasi	Risiko operasional yang dapat mempengaruhi penyampaian layanan kritis diidentifikasi
	Risiko dianalisis dan diberi disposisi	Risiko dianalisis untuk menentukan dampak potensial terhadap layanan kritis.
		Disposisi (menerima, mentransfer, mengurangi, dll.) Ditugaskan untuk risiko yang teridentifikasi.
	Risiko terhadap aset dan layanan dimitigasi dan dikendalikan	Rencana dikembangkan untuk risiko yang diputuskan oleh organisasi untuk dikurangi.
		Risiko yang teridentifikasi dilacak hingga penutupan.

*) CRR, 2020

2.3.8 *External Dependencies Management* (EDM)

Pengalihdayaan layanan, pengembangan, dan produksi telah menjadi bagian operasi normal dan rutin bagi banyak organisasi karena pengalihdayaan dapat menggunakan keterampilan dan peralatan khusus dengan penghematan biaya daripada opsi internal. *Domain* EDM pada CRR menyajikan metode bagi organisasi untuk mengidentifikasi dan memprioritaskan dependensi eksternal tersebut dan kemudian berfokus pada pengelolaan dan pemeliharaan dependensi tersebut. Tujuan dari *domain* ini yaitu menetapkan proses untuk mengelola tingkat kontrol yang sesuai untuk memastikan keberlanjutan dan perlindungan layanan dan aset yang bergantung pada tindakan entitas eksternal. *Domain* EDM terdiri dari 5 tujuan dan 14 praktik (Tabel 2.11).

Tabel 2.11 Tujuan dan Pratik *Domain* EDM *)

CRR *Domain*	Tujuan	Praktik
External Dependencies Management	Ketergantungan eksternal diidentifikasi dan diprioritaskan untuk memastikan pengoperasian layanan bernilai tinggi	Ketergantungan pada hubungan eksternal yang penting untuk layanan diidentifikasi.
		Sebuah proses telah ditetapkan untuk membuat dan memelihara daftar dependensi eksternal.
		Dependensi eksternal diprioritaskan.
	Risiko akibat ketergantungan eksternal diidentifikasi dan dikelola	Risiko akibat ketergantungan eksternal diidentifikasi dan dikelola
	Hubungan dengan entitas eksternal secara formal dibentuk dan dipertahankan	Persyaratan ketahanan layanan kritis ditetapkan yang berlaku khusus untuk setiap ketergantungan eksternal.
		Persyaratan ini ditinjau dan diperbarui.
		Kemampuan entitas eksternal untuk memenuhi persyaratan ketahanan layanan kritis dipertimbangkan dalam proses pemilihan.
		Persyaratan ketahanan dicantumkan dalam perjanjian formal dengan entitas eksternal.

CRR *Domain*	Tujuan	Praktik
		Kinerja entitas eksternal dipantau terhadap persyaratan ketahanan.
	Kinerja entitas eksternal dikelola	Tanggung jawab untuk memantau kinerja entitas eksternal ditetapkan (sebagaimana terkait dengan persyaratan ketahanan).
		Tindakan korektif diambil seperlunya untuk mengatasi masalah dengan kinerja entitas eksternal (sebagaimana terkait dengan persyaratan ketahanan).
		Tindakan korektif dievaluasi untuk memastikan masalah diperbaiki.
	Ketergantungan pada layanan publik dan penyedia layanan infrastruktur diidentifikasi	Layanan publik tempat layanan kritis bergantung (layanan tanggap kebakaran dan penyelamatan, penegakan hukum, dll.) Diidentifikasi.
		Penyedia infrastruktur tempat layanan kritis bergantung (layanan telekomunikasi dan telepon, sumber energi, dll.) Diidentifikasi.

*) CRR, 2020

2.3.9 *Training and Awareness* (TA)

Pelatihan dan kesadaran berfokus pada proses yang digunakan organisasi untuk merencanakan, mengidentifikasi kebutuhan, melakukan, dan meningkatkan pelatihan dan kesadaran untuk memastikan persyaratan dan tujuan ketahanan siber operasional organisasi diketahui dan dipenuhi. Sebuah organisasi merencanakan dan melakukan kegiatan pelatihan dan kesadaran yang membuat anggota staf menyadari peran mereka dalam masalah dan kebijakan ketahanan siber organisasi. Anggota staf juga menerima pelatihan khusus untuk memungkinkan mereka menjalankan peran mereka dalam mengelola ketahanan siber organisasi. Tujuan Pelatihan dan Kesadaran adalah untuk mengembangkan keterampilan dan meningkatkan kesadaran bagi orang-orang dengan peran yang mendukung layanan kritis. *Domain* TA terdiri dari 2 tujuan dan 11 praktik (Tabel 2.12).

Tabel 2.12 Tujuan dan Pratik *Domain* TA *)

CRR *Domain*	Tujuan	Praktik
Training and Awareness	Kesadaran cybersecurity dan program pelatihan	Kebutuhan kesadaran keamanan siber telah diidentifikasi untuk layanan kritis.
		Keterampilan yang diperlukan telah

CRR *Domain*	Tujuan	Praktik
	ditetapkan	diidentifikasi untuk peran tertentu (administrator, teknisi, dll.) Untuk layanan kritis.
		Kesenjangan keterampilan yang ada pada personel yang bertanggung jawab atas keamanan siber diidentifikasi.
		Kebutuhan pelatihan telah diidentifikasi.
	Dilakukan kegiatan penyadaran dan pelatihan	Dilakukan aktivitas kesadaran keamanan siber untuk layanan kritis.
		Dilakukan kegiatan pelatihan keamanan siber untuk layanan kritis.
		Efektivitas program kesadaran dan pelatihan dievaluasi.
		Kegiatan kesadaran dan pelatihan direvisi sesuai kebutuhan.
		Pengguna yang memiliki hak istimewa dilatih dalam peran dan tanggung jawab khusus mereka dalam mendukung layanan kritis.
		Eksekutif senior dilatih dalam peran dan tanggung jawab khusus mereka untuk mendukung layanan kritis.
		Personel keamanan fisik dan informasi dilatih tentang peran dan tanggung jawab khusus mereka dalam mendukung layanan kritis.

*) CRR, 2020

2.3.10 *Situational Awareness* (SA)

Kegiatan kesadaran situasional dilakukan di seluruh organisasi untuk memberikan informasi yang tepat waktu dan akurat terkait keadaan proses operasional saat ini. Kegiatan harus mendukung komunikasi dengan berbagai pemangku kepentingan internal dan eksternal untuk mendukung persyaratan ketahanan layanan kritis. Tujuan dari *domain* ini yaitu secara aktif menemukan dan menganalisis informasi yang terkait dengan stabilitas dan keamanan operasional langsung dan untuk mengoordinasikan informasi tersebut di seluruh perusahaan untuk memastikan bahwa semua unit organisasi bekerja di bawah gambaran operasi yang sama. *Domain* SA terdiri dari 3 tujuan dan 8 praktik (Tabel 2.13).

Tabel 2.13 Tujuan dan Pratik *Domain* SA [*)]

CRR *Domain*	Tujuan	Praktik
Situational Awareness	Pemantauan ancaman dilakukan	Tanggung jawab untuk memantau sumber informasi ancaman telah ditetapkan.
		Prosedur pemantauan ancaman telah dilaksanakan.
		Sumber daya telah ditugaskan dan dilatih untuk melakukan pemantauan ancaman.
	Persyaratan untuk mengkomunikasikan informasi ancaman ditetapkan	Pemangku kepentingan internal (seperti pemilik layanan kritis dan staf manajemen insiden) kepada siapa informasi ancaman harus dikomunikasikan telah diidentifikasi.
		Pemangku kepentingan eksternal (seperti personel manajemen darurat, regulator, dan organisasi berbagi informasi) kepada siapa informasi ancaman harus dikomunikasikan telah diidentifikasi.
	Informasi ancaman dikomunikasikan	Informasi ancaman dikomunikasikan kepada pemangku kepentingan.
		Sumber daya telah diberi wewenang dan akuntabilitas untuk mengkomunikasikan informasi ancaman.
		Sumber daya telah dilatih sehubungan dengan peran khusus mereka dalam mengkomunikasikan informasi ancaman.

[*)] CRR, 2020

2.3.11 *Maturity Indicator Level* (MIL)

CRR menggunakan *Maturity Indicator Levels* (MILs) untuk memberi organisasi perkiraan kematangan praktik mereka di 10 *domain* keamanan data dan informasi. Dalam pendekatan ini, kematangan organisasi didasarkan pada seberapa lengkap praktik keamanan siber di setiap *domain* telah *institutionalization* dalam organisasi. *Institutionalization* berarti bahwa praktik keamanan siber menjadi bagian organisasi yang lebih dalam dan tahan lama karena dikelola dan didukung dengan cara yang bermakna. Ketika praktik keamanan siber menjadi lebih diperhatikan dan dilakukan, manajer dapat lebih percaya pada prediktabilitas dan keandalan praktik tersebut. Praktik tersebut juga menjadi lebih mungkin dipertahankan selama gangguan atau tekanan pada organisasi. Kematangan juga dapat mengarah pada keselarasan yang lebih erat

antara aktivitas keamanan siber dan pendorong bisnis organisasi. Misalnya, dalam organisasi yang lebih matang, manajer akan memberikan pengawasan ke *domain* tertentu dan mengevaluasi efektivitas aktivitas keamanan yang terdiri dari *domain* tersebut. Skala MIL menggunakan enam tingkat kematangan, masing-masing dengan komponen yang ditentukan dan ketat yaitu *Incomplete*, *Performed*, *Planned*, *Managed*, *Measured* dan *Defined*. Deskripsi tiap skala dijelaskan pada Tabel 2.14.

Tabel 2.14 Skala *Maturity Indicator Level* *)

Skala MIL	Indikator	Deskripsi
MIL0	*Incomplete*	Praktik di *domain* tidak dilakukan seperti yang diukur oleh tanggapan atas pertanyaan CRR yang relevan di *domain*.
MIL1	*Performed*	Semua praktik yang mendukung tujuan dalam *domain* sedang dilakukan yang diukur dengan tanggapan atas pertanyaan CRR yang relevan
MIL2	*Planned*	Semua praktik khusus dalam *domain* CRR tidak hanya dilakukan tetapi juga didukung oleh perencanaan, pemangku kepentingan, serta standar dan pedoman yang relevan. Proses atau praktik yang direncanakan: • ditetapkan oleh organisasi melalui kebijakan dan rencana yang didokumentasikan • didukung oleh pemangku kepentingan • didukung oleh standar dan pedoman yang relevan
MIL3	*Managed*	Semua praktik dalam *domain* dilakukan, direncanakan, dan memiliki infrastruktur tata kelola dasar untuk mendukung proses tersebut. Proses atau praktik yang dikelola adalah: • diatur oleh organisasi • memiliki staf yang sesuai dengan orang-orang yang memenuhi syarat • didanai secara memadai • dikelola untuk risiko
MIL4	*Measured*	Semua praktik dalam *domain* dilakukan, direncanakan, dikelola, dipantau, dan dikendalikan. Proses atau praktik terukur adalah: • dievaluasi secara berkala untuk

Skala MIL	Indikator	Deskripsi
		efektivitas • dievaluasi secara objektif terhadap deskripsi dan rencana praktiknya • ditinjau secara berkala dengan manajemen tingkat yang lebih tinggi
MIL5	*Defined*	Semua praktik dalam *domain* dilakukan, direncanakan, dikelola, diukur, dan konsisten di semua konstituen dalam organisasi yang memiliki kepentingan dalam kinerja praktik. Di MIL5, sebuah proses atau praktik: • ditentukan oleh organisasi dan disesuaikan oleh unit operasi individu dalam organisasi untuk digunakan • didukung oleh perbaikan informasi yang dikumpulkan oleh dan dibagikan di antara unit-unit operasi untuk kepentingan organisasi secara keseluruhan

*) CRR, 2020

2.3.12 *Scores*

Dalam tahap *analyze and identified gaps*, akan dilakukan perhitungan skor untuk melihat *gaps* di setiap *domain* yang dapat dianalisis lebih lanjut. Terdapat 2 skor yang dapat digunakan, yaitu MIL dan performa keseluruhan setiap *domain*. MIL adalah tingkat perkiraan kematangan dalam organisasi. Skala MIL sangat berguna sebagai cara yang efisien untuk fokus pada peningkatan dan membandingkan kematangan di berbagai domain. Berikut merupakan rumus untuk menghitung MIL pada setiap *domain*.

$$\frac{\text{Jumlah "Iya"} + (0.5 \times \text{Jumlah "Belum Lengkap"})}{\text{Total Praktik Domain pada MIL n}}$$

Selanjutnya, terdapat performa keseluruhan untuk setiap *domain*. Performa keseluruhan dapat memberikan beberapa wawasan awal tentang area yang dapat diberikan perhatian khusus dalam peningkatan keamanan siber. Organisasi dapat melakukan praktik yang belum dilakukan untuk meningkatkan ketahanan siber.

Berikut merupakan rumus untuk menghitung performa keseluruhan pada setiap *domain*.

$$\frac{\text{Jumlah "Iya"}}{\text{Total Praktik MIL1} - \text{MIL5}} \times 100\%$$

Adapun perhitungan total MIL1 sampai dengan MIL5 didapatkan dari:

$$\text{Total Praktik MIL1} + \text{Total Praktik MIL2} - \text{MIL5}$$

Sebagai contoh, untuk menghitung total praktik MIL1 – MIL5 pada *domain Asset Management* sebagai berikut.

$$\text{Total Praktik MIL1 AM} + \text{Total Praktik MIL2} - \text{MIL5 AM}$$
$$65 + 13 = 78 \text{ Praktik}$$

Total praktik mengacu pada Lampiran A, hal ini dikarenakan terdapat praktik yang dibagi sesuai aset (manusia, informasi, teknologi dan fasilitas). Sehingga, total praktik tujuan akan bertambah sesuai dengan total pertanyaan *Self-Assessment* yang diajukan.

2.4 Analisis Perbandingan Metode

Dalam menilai sebuah ketahanan siber di organisasi, dapat dilakukan dengan beberapa metode yaitu *Industrial Control System Cyber Resilience Assessment Tool* atau ICS-CRAT, NIST *Cybersecurity Framework* dan *Cyber Resilience Review* atau CRR. ICS-CRAT merupakan alat simulasi kualitatif untuk menilai ketahanan siber pada Sistem Kontrol Industri atau ICS. Keluaran simulasi ICS-CRAT dapat membantu untuk memahami penggunaan dan dasar pemikiran serta gambaran tentang sejauh mana CRAT dapat memberikan penilaian yang realistis dari ketahanan ICS. Dengan hasil penilaian menggunakan ICS-CRAT, sebuah organisasi yang menerapkan ICS dapat meningkatkan ketahanan siber berdasarkan hasil yang realistis (Haque, et al., 2019).

Setelah itu, terdapat metode lain yaitu NIST *Cybersecurity Framework*. NIST *Cybersecurity Framework* (NIST CF) merupakan sebuah kerangka kerja berdasarkan standar, pedoman, dan praktik yang ada bagi organisasi untuk mengelola dan mengurangi risiko keamanan siber dengan lebih baik. Selain membantu organisasi mengelola dan mengurangi risiko, NIST CF dirancang untuk mendorong komunikasi manajemen risiko dan keamanan siber di antara pemangku kepentingan organisasi internal dan eksternal. Kerangka kerja ini dibuat melalui kolaborasi antara industri dan pemerintah. Pendekatan yang digunakan untuk penyusunan kerangka kerja dapat membantu pemilik dan operator infrastruktur penting untuk mengelola risiko terkait keamanan siber. Kerangka ini berfokus pada penggunaan pendorong bisnis untuk memandu aktivitas keamanan siber dan mempertimbangkan risiko keamanan siber sebagai bagian dari proses manajemen risiko organisasi (NIST, 2018).

ICS-CRAT hanya dapat digunakan oleh sebuah organisasi yang menerapkan sebuah sistem kontrol industri atau ICS. ITK tidak menerapkan sebuah sistem kontrol industri, melainkan sebuah sistem dan teknologi informasi yang umum digunakan oleh instansi pendidikan. Oleh karena itu, ICS-CRAT tidak digunakan dalam penelitian ini sebagai metode penilaian agar hasil yang dicapai dapat maksimal. Hal ini juga dikemukakan oleh CRR yang tertulis bahwa CRR dirancang untuk menjadi metode penilaian universal yang dapat mengevaluasi kemampuan ketahanan siber dari berbagai organisasi baik dalam hal layanan kritis yang berbeda atau sektor infrastruktur kritis dan dalam hal ukuran dan kematangan organisasi.

NIST *Cybersecurity Framework* juga dapat digunakan untuk mengevaluasi ketahanan siber di sebuah organisasi. NIST CF juga sebuah metode yang universal layaknya CRR. Namun, keamanan siber berbeda dengan ketahanan siber. Perbedaan lebih lanjut dapat dilihat pada Tabel 2.1 yang berisikan ketahanan siber dan keamanan siber. Oleh karena itu, CRR mengadopsi beberapa pendekatan yang digunakan oleh NIST CF agar dapat mempertajam lingkup penilaian menjadi ketahanan siber. CRR memiliki keselarasan dengan NIST CF, dimana CRR mendahului pembentukan NIST CF, namun prinsip yang melekat dan praktik yang direkomendasikan dalam CRR selaras dengan prinsip utama

NIST CF. Sehingga, CRR menjadi metode penilaian yang tepat dalam mengevaluasi dan meningkatkan ketahanan siber di ITK. Selain itu, penelitian terkait keamanan siber telah dilakukan di ITK, sehingga ketahanan siber sebagai salah satu proses penting di ITK juga perlu dilakukan.

2.5 Penelitian Terdahulu

Berikut adalah rangkuman hasil penelitian terdahulu yang memiliki keterkaitan dengan penelitian yang telah dilakukan.

Tabel 2.15 Penelitian Terdahulu

No	Peneliti	Tahun	Studi Kasus	Permasalahan	Metode	Hasil
1	Chodhury, Dkk	2015	Ketahanan siber di sistem informasi	Perangkat lunak, penyimpanan data dan perangkat keras atau jaringan yang rumit dengan ketergantungan yang kompleks, sering tidak didefinisikan secara ketat oleh perusahaan.	Metode *unifying graph-based model* untuk merepresentasikan infrastruktur	Penelitian ini menghasilkan *multi-network model* untuk menangkap perilaku perusahaan dan algoritma untuk merekomendasikan tindakan ketahanan berbasis pembaruan model secara dinamis.
2	Hagen, Janne	2018	Sektor energi	Serangan dunia maya telah memengaruhi setiap sektor infrastruktur penting di Norwegia. Terlebih lagi, sektor energi memiliki kerentanan yang melekat dan dapat ditargetkan untuk mendatangkan bencana.	Penilaian dalam bentuk Laporan Resmi Norwegia (NOU)	Laporan tersebut mencakup beberapa sektor infrastruktur penting, termasuk sektor energi, yang menghasilkan 50 rekomendasi untuk meningkatkan ketahanan terhadap serangan siber.
3	Haque, Dkk	2018	*Industrial Control Systems* (ICS)	Sistem Kontrol Industri (ICS) adalah komponen penting yang memfasilitasi operasi di industri penting. Saat ini, penggunaan Teknologi Informasi dan Komunikasi (TIK) yang ekstensif di ICS membuat sistem rentan	*R4 framework of disaster resilience* yaitu *robustness, redundancy, resourcefulness* dan *rapidity*.	Proses perumusan metrik ketahanan ini dapat digunakan untuk mengevaluasi dan menganalisis ketahanan jaringan ICS secara keseluruhan.

No	Peneliti	Tahun	Studi Kasus	Permasalahan	Metode	Hasil
				terhadap serangan dunia maya.		
4	Koelemeijer, Dorien	2018	Infrastruktur kritis	Ketidakmampuan untuk mengevaluasi kinerja sistem adaptif kritis mungkin memiliki dampak bencana pada individu dan masyarakat pada umumnya, karena ketergantungan masyarakat yang meningkat pada sistem ini. Namun, saat ini tidak ada metodologi evaluasi yang secara memadai menilai keselamatan dan keamanan sistem adaptif kritis.	Metodologi Evaluasi Berdasarkan Kasus Penjaminan	Hasil penelitian menunjukkan bahwa metodologi evaluasi memberikan peluang untuk membangun dan meninjau secara otomatis. Metodologi yang ditetapkan sebagian besar memungkinkan untuk evaluasi *runtime*, namun beberapa tindakan tetap menuntut interaksi manusia untuk memastikan operasi sistem adaptif kritis yang aman dan terjamin.
5	Tonhauser, Dkk	2019	Negara Czechia, Hungary, Poland dan Slovakia	Perlunya pembahasan terkait elemen - elemen siber dan bagaimana pengaruhnya terhadap pemerintah, sektor publik dan swasta yang berfokus pada transportasi.	Perbandingan data-data statistik di beberapa negara terkait level ketahanan siber	Hasil dari penelitian ini berupa langkah-langkah untuk dapat meningkatkan ketahanan siber yang perlu difokuskan oleh pemerintah.
6	Babiceanu, Dkk	2019	Ketahanan industri IoT	Gangguan dalam operasi sistem dan layanan mempengaruhi tidak hanya kinerja *nominal system*, tetapi juga dapat menyebabkan kerugian besar bagi keselamatan dan keamanan pelaku sistem dan masyarakat secara keseluruhan.	*Software-defined networking approach* untuk memproteksi ketahanan industri *internet of things*	Penelitian ini mengusulkan *testbed manufacturing* berbasis SDN dan gabungan ontologi ketahanan-keamanan siber untuk memenuhi persyaratan tahap desain jaringan manufaktur virtual.
7	Rehak, Dkk	2019	Elemen Infrastruktur Kritis	Ketahanan elemen dalam sistem infrastruktur kritis merupakan faktor utama yang menentukan keandalan layanan	Penilaian statistik tingkat ketahanan elemen infrastruktur kritis	Penerapan metode disajikan dalam bentuk studi kasus yang difokuskan pada penilaian ketahanan elemen infrastruktur energi

No	Peneliti	Tahun	Studi Kasus	Permasalahan	Metode	Hasil
				dan komoditas yang diberikan oleh sistem infrastruktur kritis kepada masyarakat.		listrik terpilih.
8	Srinivas, Dkk	2019	Regulasi pemerintah di keamanan siber	Regulasi keamanan dunia maya diperlukan dalam hal perlindungan teknologi informasi dengan sistem komputer.	NIST Cybersecurity Framework	Penelitian ini memberikan beberapa rekomendasi yang penting untuk keamanan dunia maya dan pertahanan dunia maya
9	Meilani, Dkk	2019	ICT in Andalas University	Saat ini, tidak ada dokumentasi formal tentang prosedur tanggap darurat. Jika terjadi bencana, dapat menyebabkan hilangnya dan rusaknya semua informasi.	Pembuatan dokumen perencanaan pemulihan bencana dengan metode ISO 27031	Penelitian ini menghasilkan rancangan *Disaster Recovery Plan* Unit Pengembangan Teknologi Informasi dan Komunikasi Universitas Andalas.
10	Nguyen, Dkk	2019	Ketahanan sistem fisik siber (CPS)	Tingkat keterkaitan yang tinggi dalam CPS, dapat meningkatkan kerentanan terhadap *malware* dan serangan terkoordinasi.	Model CRDP/ED	Penelitian menunjukkan bahwa protokol yang dikembangkan untuk mempertahankan jaringan yang terganggu.
11	Haque, Dkk	2019	*Industrial Control System* (ICS)	Kebutuhan yang besar untuk menilai postur ketahanan ICS dengan menghasilkan metrik ketahanan berbasis simulasi.	ICS-CRAT (*Industrial Control System Cyber Resilience Assessment Tool*)	Penelitian ini menghasilkan sebuah alat untuk dapat menilai dan mengevaluasi ketahanan siber di industrial control system. Setelah itu, alat ini juga dapat menghasilkan modul rekomendasi berdasarkan evaluasi yang telah dilakukan.
12	Zhu, Dkk	2020	Sistem Perjalanan Perkotaan	Ketahanan siber dapat membawa sistem dengan interpretasi strategi mitigasi baru, khususnya ketika terganggu oleh curah hujan	*Cyber-Physical Resilience metric of the urban roadway system* dengan model 4I (*Infrastructure, Individuality, Instrument* dan	Dalam model CBN yang mendasari, kapasitas absorpsi yang menunjukkan kesesuaian yang baik dengan analisis data RFID dibandingkan

No	Peneliti	Tahun	Studi Kasus	Permasalahan	Metode	Hasil
				dan risiko genangan air.	*Information*) melalui data RFID (*Radio Frequency Identification*).	dengan keadaan asli dalam skenario hujan lebat.
13	Chen, Dkk	2020	Sistem rantai pasok	Dalam CPS, ketika rantai pasokan terganggu dan terjadi gangguan, pengukuran ketahanan rantai pasokan penting dilakukan untuk mengurangi kehilangan pesanan dalam rantai pasokan.	Perhitungan ketahanan siber untuk sistem rantai pasok dengan pertimbangan gangguan sistem fisik siber.	Penelitian ini akan menghasilkan karakteristik operasional dari berbagai ukuran ketahanan siber, model pengukuran ketahanan rantai pasokan dan hasil kuantitatif dari pengukuran ketahanan rantai pasokan.
14	Annarelli, Dkk	2020	Sistem manajemen ketahanan siber	Diperlukan sebuah kerangka kerja sistem manajemen ketahanan siber untuk memperjelas peran konteks dalam pemilihan yang benar dan penerapan alat dan praktik yang berbeda.	Kerangka kerja yang menggambarkan penerapan sistem tangguh siber.	Penelitian ini mengidentifikasi tindakan manajerial utama untuk memastikan ketahanan dunia maya dalam konteks yang berbeda.
15	Sep´ulveda-Estay, Dkk	2020	Ketahanan siber	Organisasi yang bergantung pada Teknologi Informasi (TI) memperoleh nilai tidak hanya dari mencegah serangan dunia maya, tetapi juga dari merespons dengan cepat dan secara koheren ketika serangan dunia maya terjadi untuk meminimalkan efek gangguannya pada operasi.	Kajian sistematis pada kerangkat kerja penilaian ketahanan siber (CRF)	Penelitian ini menghasilkan peta ikhtisar dari lanskap penelitian CRF saat ini, mengidentifikasi kesenjangan penelitian yang relevan, menyoroti kesamaan dan sinergi antara CRF dan mengusulkan peluang untuk penelitian lintas disiplin.
16	Hausken, Kjell	2020	Ketahanan siber di perusahaan, organisasi dan masyarakat	Ketahanan telah dianalisis secara ekstensif dalam analisis risiko, terutama yang terkait dengan infrastruktur fisik. Ketahanan siber saat ini mengalami banyak	Kajian literatur terkait ketahanan siber	Penelitian ini meninjau aspek-aspek yang dibutuhkan dalam memperhatikan ketahanan siber, anatara lain definisi umum ketahanan siber, aktor dan hubungan antara

No	Peneliti	Tahun	Studi Kasus	Permasalahan	Metode	Hasil
				perkembangan, dimana menjadi perhatian bagi di setiap organisasi.		ketahanan siber dengan asuransi siber.
17	Cicilio, Dkk	2020	Ketahanan jaringan listrik	Ketahanan dalam jaringan listrik sangat penting untuk kesejahteraan masyarakat setelah kejadian yang mengganggu seperti bencana alam atau serangan dunia maya.	Kerangka kerja ketahanan jaringan listrik	Penelitian ini menyajikan metode untuk memasukkan ketidakpastian dalam kerangka ketahanan yang diusulkan.
18	Severson, Dkk	2020	Sistem fisik siber (CPS)	Representasi yang salah dari data yang diumpankan dari sensor utama dapat menyebabkan gangguan layanan atau kerusakan pada pabrik yang lebih luas melalui proses fisik yang saling berhubungan.	Kerangka kerja ketahanan untuk penyerangan berbasis sensor pada sistem fisik siber	Kerangka tersebut secara fisik diuji pada sistem konduksi panas dua dimensi dengan dua jenis sensor sekunder.
19	Alghamdi dan Rastogi	2020	Penilaian risiko keamanan siber	Untuk memastikan keselamatan keamanan siber, maka perlu mengadopsi standar keselamatan dan keamanan dalam keamanan siber yang diterapkan secara ad-hoc.	*Data flow material model* (DFMM)	DFMM yang diusulkan menunjukkan bahwa serangan secara signifikan mencegah risiko dalam sistem kontrol. Dalam skenario tempat pengujian, serangan siber berkurang secara signifikan.
20	Chang dan Coppel	2020	Negara berkembang	Meskipun peningkatan kesadaran dan pengembangan kapasitas cybersecurity sekarang ditampilkan dalam sejumlah program bantuan pembangunan, tidak ada studi akademis tentang tantangan dalam melaksanakannya secara efektif.	Pengembangan kesadaran akan keamanan siber	Kunci di antara pelajaran yang didapat adalah perlunya pemahaman yang kuat tentang bagaimana internet diakses dan digunakan di negara tuan rumah, dan kebutuhan akan konten lokal untuk menarik perhatian audiens target.
21	Ahmad	2021	Ketahanan	Manajemen	*Cyber Resilience*	Hasil dari penelitian

No	Peneliti	Tahun	Studi Kasus	Permasalahan	Metode	Hasil
	Maulana Fikri		siber di Institut Teknologi Kalimantan	keamanan TI di ITK merupakan proses yang penting dan perlu mendapatkan perhatian yang khusus berdasarkan rancangan Tata Kelola Teknologi Informasi di ITK. Namun, praktik untuk ketahanan siber belum dilakukan oleh ITK melalui penerapan kerangka kerja. Oleh karena itu, dapat dikatakan bahwa proses dalam memanajemen keamanan TI khususnya ketahanan siber di ITK belum maksimal.	*Review*	berupa laporan praktik-praktik ketahanan siber dari CRR yang belum dilakukan oleh ITK untuk dapat meningkatkan ke level selanjutnya. Sehingga, dapat dibuat rekomendasi untuk peningkatan ketahanan siber di ITK.

Penelitian ke-1 dilakukan oleh Chodhury Dkk (2015) yang menghasilkan *multi network model* untuk menangkap perilaku perusahaan. Selain itu, dibuat algoritma untuk merekomendasikan tindakan ketahanan berbasis pembaruan model secara dinamis. Penelitian ini didasari dengan permasalahan yaitu perangkat lunak, penyimpanan data dan perangkat keras atau jaringan yang rumit dengan ketergantungan yang kompleks, sering tidak didefinisikan secara ketat oleh perusahaan. Metode yang digunakan yaitu Metode *unifying graph-based* model untuk merepresentasikan infrastruktur kritis di perusahaan (Choudhury, et al., 2015).

Penelitian ke-2 dilakukan oleh Hagen (2018) yang menghasilkan sebuah 50 rekomendasi untuk meningkatkan ketahanan terhadap serangan siber. Penelitian ini didasari dengan permasalahan yaitu serangan dunia maya telah memengaruhi setiap sektor infrastruktur penting di Norwegia. Terlebih lagi, sektor energi memiliki kerentanan yang melekat dan dapat ditargetkan untuk mendatangkan

bencana. Metode yang digunakan yaitu penilaian dalam bentuk Laporan Resmi Norwegia atau NOU (Hagen, 2018).

Penelitian ke-3 dilakukan oleh Haque Dkk (2018) yang menghasilkan sebuah Proses perumusan metrik ketahanan ini dapat digunakan untuk mengevaluasi dan menganalisis ketahanan jaringan ICS secara keseluruhan. Penelitian ini didasari dengan permasalahan dimana Sistem Kontrol Industri (ICS) adalah komponen penting yang memfasilitasi operasi di industri penting. Saat ini, penggunaan Teknologi Informasi dan Komunikasi (TIK) yang ekstensif di ICS membuat sistem rentan terhadap serangan dunia maya. Metode yang digunakan pada penelitian ini yaitu R4 *framework of disaster resilience* yaitu *robustness, redundancy, resourcefulness dan rapidity* (Haque, et al., 2018).

Penelitian ke-4 dilakukan oleh Koelemeijer (2018) yang menghasilkan bahwa metodologi evaluasi memberikan peluang untuk membangun dan meninjau secara otomatis. Metodologi yang ditetapkan sebagian besar memungkinkan untuk evaluasi *runtime*, namun beberapa tindakan tetap menuntut interaksi manusia untuk memastikan operasi sistem adaptif kritis yang aman dan terjamin. Penelitian ini didasari dengan permasalahan dimana ketidakmampuan untuk mengevaluasi kinerja sistem adaptif kritis mungkin memiliki dampak bencana pada individu dan masyarakat pada umumnya, karena ketergantungan masyarakat yang meningkat pada sistem ini. Namun, saat ini tidak ada metodologi evaluasi yang secara memadai menilai keselamatan dan keamanan sistem adaptif kritis. Metode yang digunakan pada penelitian ini yaitu metodologi evaluasi berdasarkan kasus penjaminan (Koelemeijer, 2018).

Penelitian ke-5 dilakukan oleh Tonhauser Dkk (2019) yang menghasilkan berupa langkah-langkah untuk dapat meningkatkan ketahanan siber yang perlu difokuskan oleh pemerintah. Penelitian ini didasari dengan permasalahan dimana perlunya pembahasan terkait elemen - elemen siber dan bagaimana pengaruhnya terhadap pemerintah, sektor publik dan swasta yang berfokus pada transportasi. Metode yang digunakan pada penelitian ini yaitu perbandingan data-data statistik di beberapa negara terkait level ketahanan siber (Tonhauser & Ristvej, 2019).

Penelitian ke-6 dilakukan oleh Babiceanu Dkk (2019) yang mengusulkan *testbed manufacturing* berbasis SDN dan gabungan ontologi ketahanan-keamanan

siber untuk memenuhi persyaratan tahap desain jaringan manufaktur virtual. Penelitian ini didasari dengan permasalahan dimana gangguan dalam operasi sistem dan layanan mempengaruhi tidak hanya kinerja *nominal system*, tetapi juga dapat menyebabkan kerugian besar bagi keselamatan dan keamanan pelaku sistem dan masyarakat secara keseluruhan. Metode yang digunakan pada penelitian ini yaitu *software-defined networking approach* untuk memproteksi ketahanan industri *internet of things* (Babiceanu & Seker, 2019).

Penelitian ke-7 dilakukan oleh Rehak Dkk (2019) yang menghasilkan penerapan metode dalam bentuk studi kasus yang difokuskan pada penilaian ketahanan elemen infrastruktur energi listrik terpilih.. Penelitian ini didasari dengan permasalahan dimana Ketahanan elemen dalam sistem infrastruktur kritis merupakan faktor utama yang menentukan keandalan layanan dan komoditas yang diberikan oleh sistem infrastruktur kritis kepada masyarakat. Metode yang digunakan pada penelitian ini yaitu Penilaian statistik tingkat ketahanan elemen infrastruktur kritis (Rehak, et al., 2019).

Penelitian ke-8 dilakukan oleh Srinivas Dkk (2019) yang menghasilkan beberapa rekomendasi yang penting untuk keamanan dunia maya dan pertahanan dunia maya. Penelitian ini didasari dengan permasalahan dimana regulasi keamanan dunia maya diperlukan dalam hal perlindungan teknologi informasi dengan sistem komputer. Metode yang digunakan pada penelitian ini yaitu NIST Cybersecurity Framework (Srinivas, et al., 2019).

Penelitian ke-9 dilakukan oleh Meilani Dkk (2019) yang menghasilkan rancangan *Disaster Recovery Plan* Unit Pengembangan Teknologi Informasi dan Komunikasi Universitas Andalas. Penelitian ini didasari dengan permasalahan dimana tidak adanya dokumentasi formal tentang prosedur tanggap darurat. Jika terjadi bencana, dapat menyebabkan hilangnya dan rusaknya semua informasi. Metode yang digunakan pada penelitian ini yaitu ISO 27031 (Meilani, et al., 2019).

Penelitian ke-10 dilakukan oleh Nguyen Dkk (2019) yang menunjukkan bahwa protokol yang dikembangkan untuk mempertahankan jaringan yang terganggu dapat secara signifikan menekankan kemampuan ketahanan CPS. Penelitian ini didasari dengan permasalahan dimana Tingkat keterkaitan yang

tinggi dalam CPS, dapat meningkatkan kerentanan terhadap *malware* cerdas dan serangan terkoordinasi. Metode yang digunakan pada penelitian ini yaitu Model CRDP/ED (Nguyen, et al., 2019).

Penelitian ke-11 dilakukan oleh Haque Dkk (2019) yang menghasilkan sebuah alat untuk dapat menilai dan mengevaluasi ketahanan siber di industrial control system. Setelah itu, alat ini juga dapat menghasilkan modul rekomendasi berdasarkan evaluasi yang telah dilakukan. Penelitian ini didasari dengan permasalahan dimana kebutuhan yang besar untuk menilai postur ketahanan ICS dengan menghasilkan metrik ketahanan berbasis simulasi.. Metode yang digunakan pada penelitian ini yaitu ICS-CRAT (*Industrial Control System Cyber Resilience Assessment Tool*).

Penelitian ke-12 dilakukan oleh Zhu, Dkk (2020) yang menghasilkan sebuah kapasitas absorpsi yang menunjukkan kesesuaian yang baik dengan analisis data RFID dibandingkan dengan keadaan asli dalam skenario hujan lebat. Penelitian ini didasari dengan permasalahan dimana ketahanan siber dapat membawa sistem dengan interpretasi strategi mitigasi baru, khususnya ketika terganggu oleh curah hujan dan risiko genangan air. Metode yang digunakan pada penelitian ini yaitu *Cyber-Physical Resilience metric of the urban roadway system* dengan model 4I (*Infrastructure, Individuality, Instrument* dan *Information*) melalui data RFID (*Radio Frequency Identification*) (Zhu, et al., 2020).

Penelitian ke-13 dilakukan oleh Chen Dkk (2020) yang menghasilkan karakteristik operasional dari berbagai ukuran ketahanan siber, model pengukuran ketahanan rantai pasokan dan hasil kuantitatif dari pengukuran ketahanan rantai pasokan. Penelitian ini didasari dengan permasalahan dimana dalam CPS, ketika rantai pasokan terganggu dan terjadi gangguan, pengukuran ketahanan rantai pasokan penting dilakukan untuk mengurangi kehilangan pesanan dalam rantai pasokan. Metode yang digunakan pada penelitian ini yaitu Perhitungan ketahanan siber untuk sistem rantai pasok dengan pertimbangan gangguan sistem fisik siber (Chen, et al., 2020).

Penelitian ke-14 dilakukan oleh Annarelli Dkk (2020) yang mengidentifikasi tindakan manajerial utama untuk memastikan ketahanan dunia maya dalam konteks yang berbeda. Penelitian ini didasari dengan permasalahan dimana

diperlukan sebuah kerangka kerja sistem manajemen ketahanan siber untuk memperjelas peran konteks dalam pemilihan yang benar dan penerapan alat dan praktik yang berbeda. Metode yang digunakan pada penelitian ini yaitu kerangka kerja yang menggambarkan penerapan sistem tangguh siber (Annarelli, et al., 2020).

Penelitian ke-15 dilakukan oleh Sep´ulveda-Estay Dkk (2020) yang menghasilkan peta ikhtisar dari lanskap penelitian CRF saat ini, mengidentifikasi kesenjangan penelitian yang relevan, menyoroti kesamaan dan sinergi antara CRF dan mengusulkan peluang untuk penelitian lintas disiplin.. Penelitian ini didasari dengan permasalahan dimana organisasi yang bergantung pada Teknologi Informasi (TI) memperoleh nilai tidak hanya dari mencegah serangan dunia maya, tetapi juga dari merespons dengan cepat dan secara koheren ketika serangan dunia maya terjadi untuk meminimalkan efek gangguannya pada operasi. Metode yang digunakan pada penelitian ini yaitu kajian sistematis pada kerangkat kerja penilaian ketahanan siber (CRF) (Sep´ulveda-Estay, et al., 2020).

Penelitian ke-16 dilakukan oleh Hausken (2020) yang meninjau aspek-aspek yang dibutuhkan dalam memperhatikan ketahanan siber, anatara lain definisi umum ketahanan siber, aktor dan hubungan antara ketahanan siber dengan asuransi siber. Penelitian ini didasari dengan permasalahan dimana ketahanan telah dianalisis secara ekstensif dalam analisis risiko, terutama yang terkait dengan infrastruktur fisik. Ketahanan siber saat ini mengalami banyak perkembangan, dimana menjadi perhatian bagi di setiap organisasi. Metode yang digunakan pada penelitian ini yaitu Kajian literatur terkait ketahanan siber (Hausken, 2020).

Penelitian ke-17 dilakukan oleh Cicilio Dkk (2020) yang menyajikan metode untuk memasukkan ketidakpastian dalam kerangka ketahanan yang diusulkan. Penelitian ini didasari dengan permasalahan dimana ketahanan dalam jaringan listrik sangat penting untuk kesejahteraan masyarakat setelah kejadian yang mengganggu seperti bencana alam atau serangan dunia maya. Metode yang digunakan pada penelitian ini yaitu kerangka kerja ketahanan jaringan listrik (Cicilio, et al., 2020).

Penelitian ke-18 dilakukan oleh Severson Dkk (2020) yang menghasilkan kerangka tersebut secara fisik diuji pada sistem konduksi panas dua dimensi dengan dua jenis sensor sekunder. Penelitian ini didasari dengan permasalahan dimana representasi yang salah dari data yang diumpankan dari sensor utama dapat menyebabkan gangguan layanan atau kerusakan pada pabrik yang lebih luas melalui proses fisik yang saling berhubungan. Metode yang digunakan pada penelitian ini yaitu kerangka kerja ketahanan untuk penyerangan berbasis sensor pada sistem fisik siber (Severson, et al., 2020).

Penelitian ke-19 dilakukan oleh Alghamdi (2020) yang menghasilkan serangan secara signifikan mencegah risiko dalam sistem kontrol. Dalam skenario tempat pengujian, serangan siber berkurang secara signifikan. Penelitian ini didasari dengan permasalahan untuk memastikan keselamatan keamanan siber, maka perlu mengadopsi standar keselamatan dan keamanan dalam keamanan siber yang diterapkan secara ad-hoc. Metode yang digunakan pada penelitian ini yaitu *Data flow material model* (DFMM) (Alghamdi & Rastogi, 2020).

Penelitian ke-20 dilakukan oleh Chang (2020) yang menghasilkan pemahaman yang kuat tentang bagaimana internet diakses dan digunakan di negara tuan rumah, dan kebutuhan akan konten lokal untuk menarik perhatian audiens target. Penelitian ini didasari dengan permasalahan dimana peningkatan kesadaran dan pengembangan kapasitas *cybersecurity* sekarang ditampilkan dalam sejumlah program bantuan pembangunan, tidak ada studi akademis tentang tantangan dalam melaksanakannya secara efektif.. Metode yang digunakan pada penelitian ini yaitu Pengembangan kesadaran akan keamanan siber (Chang & Coppel, 2020).

Telah didapatkan bahwa untuk merespon sebuah ancaman siber, sebuah organisasi perlu untuk meningkatkan ketahanan siber atau *cyber resilience*. Beberapa studi telah menerapkan metode untuk mengevaluasi ketahanan siber di sebuah sistem maupun perusahaan. Salah satunya yaitu *Cyber Resilience Review* dan ICS-CRAT. Namun, Institut Teknologi Kalimantan menerapkan sebuah teknologi informasi dan komunikasi yang umum digunakan dan tidak menerapkan sistem kontrol industri atau *Industrial Control System* (ICS). Oleh karena itu, digunakan kerangka kerja *Cyber Resilience Review* (CRR) dikarenakan CRR

dapat mengakomodir semua jenis teknologi informasi, termasuk teknologi yang digunakan di Institut Teknologi Kalimantan.