BADAN SIBER
DAN SANDI
NEGARA

PANDUAN MANAJEMEN RISIKO KEAMANAN SIBER

Disusun:

Direktorat Kebijakan Tata Kelola Keamanan Siber dan Sandi

2024

Panduan Manajemen Risiko Keamanan Siber

Versi 1.0.0: Oktober 2024

Susunan Redaksi

Penanggung Jawab	:	Nunil Pantjawati, B.Sc, M.E.
Ketua Tim	:	Satrio Wicaksono Nugroho Putro, S.ST.
Tim Penyusun	:	Satrio Wicaksono Nugroho Putro, S.ST.
		Aji Setiyo Sukarno, S.ST.
		Fitria Sekarwulan Risdhafany, S.ST
		Ahmad Alinnoor Ulinuha Alby A., S.Tr.Kom
		Almas Fauzia Wibawa, S.Kom.
		Andrian Rizky Moranta, S.Hum., M.Si.
Tim Pendamping Ahli	:	Dr. Bety Hayat Susanti, S.Si, M.E.
		Dr. Susila Windarta, S.Kom., M.Si.
		Septia Ulfa Sunaringtyas, S.Tr.MP., M.T.
		Mareta Wahyu Ardyani, M.Sc.

Direktorat Kebijakan Tata Kelola Keamanan Siber dan Sandi,
Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi
2024
xii + 73 hlm;

VERSI
Versi 1.0.0, Oktober 2024

BADAN SIBER DAN SANDI NEGARA
Jalan Raya Muchtar No. 70, Depok, Jawa Barat 16516

“ Ingatlah bahwa kechilafan satu orang sahaja tjukup sudah menjebabkan keruntuhan negara.

dr. Roebiono Kertopati
Bapak Persandian Indonesia

SAMBUTAN

Direktur Kebijakan Tata Kelola Keamanan Siber dan Sandi

NUNIL PANTJAWATI, B.Sc, M.E.
Direktur Kebijakan Tata Kelola Keamanan Siber dan Sandi

Segala puji bagi Allah SWT atas limpahan rahmat dan karunia-Nya, sehingga penyusunan Dokumen Panduan Manajemen Risiko Keamanan Siber dapat diselesaikan dengan baik. Dewasa ini, ancaman siber telah menjadi salah satu tantangan utama bagi organisasi di seluruh dunia. Ancaman siber yang semakin kompleks dan beragam menuntut setiap institusi untuk tidak hanya menyadari potensi risiko, tetapi juga untuk menerapkan strategi manajemen risiko yang efektif.

Dokumen Panduan Manajemen Risiko Keamanan Siber disusun sebagai upaya untuk membantu dan memberikan panduan bagi organisasi dan Penyelenggara Sistem Elektronik (PSE) untuk memahami, mengidentifikasi, dan mengelola risiko yang mungkin dan akan dihadapi. Dokumen ini menyediakan referensi yang komprehensif mengenai manajemen risiko keamanan siber.

Dokumen ini diharapkan dapat digunakan sebagai acuan yang bermanfaat untuk membantu PSE dalam melakukan identifikasi, pengelolaan, dan pengurangan risiko keamanan siber, sehingga mereka dapat melindungi aset penting dan mengatasi berbagai risiko yang ada. Dengan pemahaman yang lebih baik dan tindakan yang tepat, PSE diharapkan dapat memastikan perlindungan yang optimal terhadap infrastruktur informasi vital mereka.

Direktur Kebijakan Tata Kelola Keamanan Siber dan Sandi

Ditandatangani Secara Elektronik oleh:
DIREKTUR KEBIJAKAN TATA KELOLA KEAMANAN SIBER DAN SANDI

NUNIL PANTJAWATI, B.Sc, M.E.
Pembina Utama Madya (IV/d)

PROFIL

DIREKTORAT KEBIJAKAN TATA KELOLA KEAMANAN SIBER DAN SANDI

BADAN SIBER DAN SANDI NEGARA

Berdasarkan Peraturan Presiden Nomor 53 Tahun 2017

Badan Siber dan Sandi Negara (BSSN) merupakan hasil dari penggabungan beberapa entitas pemerintah sebelumnya, antara lain Lembaga Sandi Negara (Lemsaneg), Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika (Kemenkominfo), serta Indonesia *Security Incident Response Team on Internet Infrastructure* (Id- SIRTII). Proses penggabungan ini diwujudkan melalui Peraturan Presiden Nomor 53 tahun 2017 tentang BSSN.

DIREKTORAT KEBIJAKAN TATA KELOLA KEAMANAN SIBER DAN SANDI

Berdasarkan Peraturan Presiden Nomor 28 Tahun 2021

Presiden Republik Indonesia, Joko Widodo, menandatangani Peraturan Presiden (Perpres) Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (BSSN) pada tanggal 13 April 2021. Penerbitan Perpres ini didasarkan pada kebutuhan untuk merancang kembali struktur organisasi BSSN, dengan tujuan mencapai keamanan, perlindungan, dan kedaulatan siber nasional. Selanjutnya, organisasi dan tata kerja BSSN dijelaskan lebih lanjut dalam Peraturan BSSN Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja BSSN.

Direktorat Kebijakan Tata Kelola Keamanan Siber dan Sandi merupakan bagian dari Deputi Deputi Bidang Strategi dan Kebijakan Keamanan Siber dan Sandi di lingkungan Badan Siber dan Sandi Negara. Direktorat Kebijakan Tata Kelola Keamanan Siber dan Sandi mempunyai tugas melaksanakan koordinasi dan perumusan kebijakan teknis di bidang tata kelola keamanan siber dan sandi. Direktorat Kebijakan Tata Kelola Keamanan Siber dan Sandi melaksanakan fungsi-fungsi berikut:

- Penyiapan koordinasi dan perumusan kebijakan teknis di bidang tata kelola identifikasi, proteksi, deteksi, penanggulangan, dan pemulihan;
- Pelaksanaan pemantauan, evaluasi, dan pelaporan di bidang tata kelola identifikasi, proteksi, deteksi, penanggulangan, dan pemulihan; dan
- Pelaksanaan urusan perencanaan, keuangan, rumah tangga, kepegawaian, ketatalaksanaan, persuratan, kearsipan, serta penyusunan evaluasi dan pelaporan Direktorat.

RINGKASAN

Pelindungan Infrastruktur Informasi Vital (IIV) merupakan urgensi yang mendesak dalam konteks keamanan nasional dan keberlangsungan pelayanan publik. IIV mencakup sistem dan jaringan yang menjadi *backbone* operasional sektor-sektor strategis, seperti administrasi pemerintahan, keuangan, energi, kesehatan, pertahanan, pangan, teknologi informasi dan komunikasi (TIK), dan transportasi. Dalam Rencana Pembangunan Jangka Menengah Nasional (RPJMN) 2020-2024, keamanan siber menjadi salah satu aspek penting yang perlu mendapat perhatian dan tanggung jawab bersama seluruh komponen bangsa. Perkembangan teknologi digital memengaruhi berbagai bidang, termasuk tata kelola pemerintahan melalui *e-government*. Meskipun sudah ada upaya dari pemerintah untuk memperkuat keamanan siber, industri masih menghadapi tantangan. Beberapa regulasi telah dikeluarkan, termasuk Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital, Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, serta Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Pengelolaan Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik. Namun, dengan pertumbuhan pengguna internet yang pesat, perlu terus memperkuat kerangka regulasi dan kelembagaan untuk menghadapi ancaman siber yang semakin kompleks.

Penerapan manajemen risiko pada lingkup organisasi dan sektor, termasuk Penyelenggara IIV umumnya beragam, namun dapat dipastikan organisasi telah mengambil berbagai langkah untuk memitigasi risiko keamanan siber dalam menjalankan proses bisnisnya. Umumnya organisasi telah melakukan prosedur atau upaya manajemen risiko. Meski berbagai upaya telah dilakukan, masih terdapat kesenjangan signifikan yang harus diatasi. Beberapa risiko keamanan siber mungkin tidak dikelola dengan baik karena kurangnya pemahaman mengenai penyebab atau dampak risiko tersebut, informasi yang terbatas, atau karena risiko tersebut relatif baru. Selain itu, ada risiko tertentu yang berada di luar kendali langsung Penyelenggara IIV, seperti kerentanan yang timbul dari ketergantungan pada pihak ketiga, kelemahan dalam rantai pasokan, atau ancaman yang muncul dari jaringan siber yang lebih luas.

Dalam implementasi manajemen risiko, terdapat beberapa pertimbangan penting yang harus diperhatikan. Salah satu pertimbangan utama adalah resistansi yang mungkin muncul akibat ketidaktahuan atau kurangnya pemahaman terhadap risiko yang ada. Aspek lain yang umumnya tidak dipertimbangkan oleh organisasi dalam menjalankan manajemen risiko adalah potensi *cascading effect* atau dampak berjenjang yang mungkin timbul. Dalam sektor infrastruktur informasi vital (IIV), *cascading effect* dapat terjadi ketika satu insiden, seperti serangan siber atau kegagalan sistem, memicu gangguan yang menyebar ke berbagai sektor dan memengaruhi operasi yang lebih luas. Dari penjelasan tersebut, dapat terlihat betapa pentingnya bagi organisasi untuk memahami hubungan keterkaitan atau ketergantungan dengan layanan dan sistem eksternal yang digunakan dalam operasionalnya.

Pada level organisasi, manajemen risiko penting untuk dilakukan untuk menjamin keberlangsungan organisasi dan proses bisnis yang dijalankan. Hal ini membutuhkan kolaborasi dan kerja sama dari berbagai pihak terkait. Selain itu, untuk menjamin manajemen risiko yang efektif dan efisien, setiap pihak yang terkait juga harus memahami masing-masing peran yang dimiliki. Sebelum setiap pihak mengimplementasikan manajemen risiko, perlu untuk memiliki kesamaan persepsi tentang risiko yang ada. Oleh karena itu, risiko yang ada perlu didefinisikan, termasuk di dalamnya sejauh mana toleransi yang dapat diterima oleh organisasi terhadap risiko yang ada.

Dokumen ini menyajikan panduan manajemen risiko keamanan siber. Pada bagian awal, disajikan pemetaan kebijakan manajemen risiko yang diterapkan di tingkat nasional dan sektoral. Selanjutnya, penerapan manajemen risiko secara kolektif mencakup pembentukan wadah komunikasi dan berbagi informasi antar kementerian/lembaga (K/L), *stakeholder*, atau organisasi yang terlibat dalam pelindungan IIV dan penjelasan *cascading effect* atau dampak berjenjang yang mungkin timbul setelah terjadinya suatu insiden. Pada bagian akhir, diberikan panduan Manajemen Risiko Keamanan Siber Organisasi yang menitikberatkan pada peran dan keterlibatan berbagai pihak serta pendefinisian dan toleransi risiko. Selain itu, diberikan juga panduan untuk melakukan penilaian risiko untuk mengidentifikasi risiko yang sesuai dengan lingkungannya dan level dari risikonya serta pelaporan manajemen risiko keamanan siber.

DAFTAR ISI

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

PENDAHULUAN

BAB I
PENDAHULUAN

A. Latar Belakang

Pelindungan Infrastruktur Informasi Vital (IIV) merupakan kebutuhan yang mendesak dalam konteks keamanan nasional dan keberlangsungan pelayanan publik. IIV mencakup sistem dan jaringan yang menjadi *backbone* operasional sektor-sektor strategis, seperti administrasi pemerintahan, keuangan, energi, kesehatan, pertahanan, pangan, teknologi informasi dan komunikasi (TIK) dan transportasi. Gangguan pada IIV berpotensi menimbulkan dampak yang signifikan, mengancam stabilitas nasional, keamanan publik, dan kelangsungan layanan esensial. Dengan meningkatnya ancaman siber yang semakin kompleks dan canggih, risiko terhadap IIV tidak dapat diabaikan. Oleh karena itu, implementasi langkah-langkah pelindungan yang komprehensif dan berkelanjutan sangat penting untuk memastikan keamanan, keandalan, dan ketahanan infrastruktur ini dalam menghadapi berbagai potensi ancaman.

Transformasi digital yang saat ini telah diadaptasi pada seluruh sektor termasuk sektor strategis memberikan manfaat yang signifikan dalam peningkatan efisiensi, kualitas layanan, dan mempercepat *delivery* layanan dan *time to market*. Dalam mendukung transformasi digital, pemerintah melalui Kementerian Komunikasi dan Informatika (Kemenkominfo) telah menyusun Peta Jalan Indonesia Digital tahun 2021-2024 sebagai panduan strategis yang memandu perjalanan transformasi digital bangsa. Percepatan transformasi digital berfokus pada 10 sektor prioritas untuk mempercepat terwujudnya infrastruktur, pemerintahan, ekonomi, dan masyarakat digital.[1] Adopsi transformasi digital juga menimbulkan tantangan dan risiko, terutama yang terkait dengan ancaman keamanan siber, serta dampak *cascading* yang mungkin timbul, seperti gangguan layanan umum, perekonomian, dan layanan vital lain yang memengaruhi hajat hidup orang banyak, akibat ketergantungan infrastruktur vital terhadap infrastruktur teknologi yang menunjang keberlangsungan layanan.

[1] https://www.kominfo.go.id/content/detail/36895/10-sektor-prioritas-untuk-memacu-transformasi-digital/0/artikel

Dalam Rencana Pembangunan Jangka Menengah Nasional (RPJMN) 2020-2024, keamanan siber menjadi salah satu aspek penting yang perlu mendapat perhatian dan tanggung jawab bersama seluruh komponen bangsa. Perkembangan teknologi digital memengaruhi berbagai bidang, termasuk tata kelola pemerintahan melalui *e-government*. Pada RPJMN ini, terdapat fokus pada penguatan ketahanan dan keamanan siber. Salah satu indikator yang diawasi adalah *Global Cybersecurity Index* (GCI), yang mengukur kinerja keamanan siber suatu negara. Indonesia berhasil meningkatkan skor GCI dari tahun 2018 ke 2020, mencapai 94,88 (naik sebesar 17,28 poin).

Meskipun sudah ada upaya dari pemerintah untuk memperkuat keamanan siber, industri masih menghadapi tantangan. Beberapa regulasi telah dikeluarkan, termasuk Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital, Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, serta Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Pengelolaan Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik. Namun, dengan pertumbuhan pengguna internet yang pesat, kerangka regulasi dan kelembagaan untuk menghadapi ancaman siber yang semakin kompleks perlu terus diperkuat.

Pelaksanaan penilaian risiko nasional adalah salah satu tindakan yang disarankan dalam *Sendai Framework for Disaster Risk Reduction*, 2015-2030. Strategi Internasional Perserikatan Bangsa-Bangsa (PBB) untuk Pengurangan Risiko Bencana (UNISDR) merilis seperangkat pedoman untuk mendukung proses ini. Pada pedoman tersebut, disebutkan mengenai *dynamic cascading* (UNISDR 2017).[2]

Ketergantungan terhadap infrastruktur teknologi informasi mengakibatkan risiko saling ketergantungan (interdependensi) yang menimbulkan *cascading effect*, baik dalam lingkup organisasi maupun antar sektor. Serangan siber atau kegagalan sistem dapat menimbulkan dampak yang luas, baik secara langsung maupun tidak langsung, terhadap keberlangsungan layanan vital. Pada bulan Desember 2020, perusahaan perangkat lunak Orion mengalami insiden *data breach* pada perangkat lunak

[2] Sendai Framework for Disaster Risk Reduction 2015-2030. United Nations (UN)

Solarwind yang banyak digunakan oleh lembaga pemerintahan dan perusahaan swasta yang memungkinkan penyerang mengakses data sensitif dan mengganggu operasional layanan. Kejadian ini termasuk ke dalam *supply chain attack* yang berdampak lintas sektoral.[3] Pada tanggal 19 Juli 2024, kegagalan pembaruan terhadap perangkat atau aplikasi Falcon Sensor oleh Crowdstrike menyebabkan kegagalan 8,5 juta komputer berbasis Windows mengalami *Blue Screen of Death (BSOD)*. Kejadian ini dianggap sebagai *outage* terbesar dalam sejarah pemanfaatan teknologi informasi yang memiliki skala dampak luas multi sektoral yang berpengaruh terhadap layanan operasional maskapai penerbangan, perbankan, ritel, dan rumah sakit, dan membutuhkan waktu yang cukup lama untuk melakukan *recover*.[4]

Kejadian tersebut menunjukkan bahwa ketergantungan layanan, baik dalam satu sektor maupun lintas sektoral pada infrastruktur teknologi, dapat menimbulkan risiko sistemik yang strategis. Kegagalan sistem atau serangan siber pada satu organisasi berpotensi berdampak luas pada organisasi lain, bahkan lintas sektor, sehingga mengancam kelangsungan layanan vital. Upaya pengelolaan risiko kolektif di sektor Infrastruktur Informasi Vital sangat diperlukan agar risiko interdependensi dapat teratasi dengan efektif. Di samping itu, organisasi operator atau Penyelenggara IIV perlu memiliki persepsi yang seragam mengenai risiko, terutama yang dapat menyebabkan efek berantai pada tingkat sektoral maupun nasional.

B. Landasan Peraturan

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
2. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
3. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[3] https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack
[4] https://www.theverge.com/2024/7/24/24205020/crowdstrike-test-software-bug-windows-bsod-issue

4. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
5. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital.
6. Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.
7. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik.
8. Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE) dan Standar Teknis dan Prosedur Keamanan SPBE.
9. Peraturan Badan Siber dan Sandi Negara Nomor 7 Tahun 2023 tentang Identifikasi Infrastruktur Informasi Vital.
10. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2023 tentang Kerangka Kerja Pelindungan Infrastruktur Informasi Vital.
11. Peraturan Badan Siber dan Sandi Negara Nomor 9 Tahun 2023 tentang Peningkatan Kapasitas Sumber Daya Manusia di Bidang Keamanan Siber dan Sandi.
12. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber.
13. Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2024 tentang Rencana Aksi Nasional Keamanan Siber Tahun 2024-2028.
14. Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum.
15. Peraturan Bank Indonesia Nomor 2 Tahun 2024 tentang Keamanan Sistem Informasi dan Ketahanan Siber bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Pasar Valuta Asing, Serta Pihak Lain Yang Diatur dan Diawasi Bank Indonesia.
16. Surat Edaran Otoritas Jasa Keuangan Republik Indonesia Nomor 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber Bagi Bank Umum.

C. Maksud dan Tujuan

Maksud dari penyusunan Dokumen Panduan Manajemen Risiko Keamanan Siber ini adalah mengidentifikasi dan menganalisis kesenjangan penerapan manajemen risiko pada sektor IIV, serta mengidentifikasi pendekatan manajemen risiko yang tepat yang dapat diterapkan pada level organisasi namun dapat dilakukan agregasi ke level sektoral ataupun nasional.

Adapun tujuan dari penyusunan Dokumen Panduan Manajemen Risiko Keamanan Siber adalah:

a. mengetahui perspektif manajemen risiko, khususnya yang terkait keamanan siber pada level organisasi pada sektor IIV, dan strategi mengenai agregasi manajemen risiko organisasi ke level sektoral ataupun nasional;
b. mengidentifikasi kebijakan dan peraturan terkait manajemen risiko, keamanan informasi, dan keamanan siber yang berlaku pada level sektoral; dan
c. merumuskan strategi penerapan manajemen risiko pada level sektoral dan nasional yang efektif dan bersifat kolaboratif yang dapat melibatkan seluruh pemangku kepentingan di sektor IIV.

D. Ruang Lingkup

Penyusunan Dokumen Panduan Manajemen Risiko Keamanan Siber ini dilakukan dengan melakukan *study literatur* menggunakan berbagai sumber, baik berupa peraturan, kebijakan, maupun *best practice* manajemen risiko yang diterapkan di berbagai negara. Fokus studi ini dilakukan pada sektor IIV yang telah didefinisikan pada Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital.

E. Identifikasi Kebijakan Terkait Manajemen Risiko pada Sektor IIV

Kebijakan nasional dan sektoral yang efektif sangat penting untuk melindungi dan mengelola risiko yang mengancam IIV serta memastikan keberlangsungan operasional dan keamanan nasional. Kebijakan ini mencakup regulasi, standar, pedoman, dan inisiatif yang dirancang untuk mengantisipasi berbagai ancaman, seperti serangan siber, bencana alam, kesalahan manusia, dan gangguan teknis. Tabel 1 menguraikan kebijakan mengenai manajemen risiko yang diterapkan di tingkat sektoral dan nasional.

Tabel 1. Pemetaan Regulasi Kebijakan Sektor

No	Sektor	Kementerian/ Lembaga	Kementerian Terkait	Regulasi Nasional Terkait Teknologi Informasi, Keamanan Informasi, Siber, dan Pelindungan Data	Regulasi Sektoral terkait Keamanan Teknologi Informasi, Keamanan Informasi, Siber, dan Manajemen Risiko
1	Administrasi pemerintahan	Badan Siber dan Sandi Negara	✓Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia ✓Kementerian Dalam Negeri	✓ Undang-Undang (UU) No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ✓ UU No. 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik	✓ UU No. 23 tahun 2014 tentang Pemerintahan Daerah ✓ Perpres No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) ✓ Perpres No. 132 Tahun 2022 tentang Arsitektur SPBE Nasional

No	Sektor	Kementerian/ Lembaga	Kementerian Terkait	Regulasi Nasional Terkait Teknologi Informasi, Keamanan Informasi, Siber, dan Pelindungan Data	Regulasi Sektoral terkait Keamanan Teknologi Informasi, Keamanan Informasi, Siber, dan Manajemen Risiko
			✓Kementerian Komunikasi dan Informatika ✓Kementerian Keuangan	✓ UU No. 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik ✓ UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi ✓ Peraturan Pemerintah (PP) No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik ✓ Peraturan Presiden (Perpres) No. 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (IIV) ✓ Perpres No. 47 Tahun 2023 tentang Strategi Keamanan	✓ Perpres No. 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional ✓ Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (PermenPANRB) No. 5 Tahun 2020 tentang Pedoman Manajemen Risiko SPBE ✓ Peraturan Badan Siber dan Sandi Negara (BSSN) No. 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar

No	Sektor	Kementerian/ Lembaga	Kementerian Terkait	Regulasi Nasional Terkait Teknologi Informasi, Keamanan Informasi, Siber, dan Pelindungan Data	Regulasi Sektoral terkait Keamanan Teknologi Informasi, Keamanan Informasi, Siber, dan Manajemen Risiko
				Siber Nasional dan Manajemen Krisis Siber ✓ Perpres No. 39 Tahun 2023 tentang Manajemen Risiko Pembangunan Nasional ✓ Peraturan BSSN No. 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik ✓ Peraturan BSSN No. 7 Tahun 2023 tentang Identifikasi IIV ✓ Peraturan BSSN No. 8 Tahun 2023 tentang Kerangka Kerja Pelindungan IIV ✓ Peraturan BSSN No. 9 Tahun 2023 tentang Peningkatan	Teknis dan Prosedur Keamanan SPBE ✓ PP No. 60 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah (SPIP)

No	Sektor	Kementerian/ Lembaga	Kementerian Terkait	Regulasi Nasional Terkait Teknologi Informasi, Keamanan Informasi, Siber, dan Pelindungan Data	Regulasi Sektoral terkait Keamanan Teknologi Informasi, Keamanan Informasi, Siber, dan Manajemen Risiko
				Kapasitas Sumber Daya Manusia di Bidang Keamanan Siber dan Sandi ✓ Peraturan BSSN No. 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber ✓ Peraturan BSSN No. 1 Tahun 2024 tentang Pengelolaan Insiden Siber ✓ Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 tentang Manajemen Krisis Siber. ✓ Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2024 tentang Rencana Aksi	

No	Sektor	Kementerian/ Lembaga	Kementerian Terkait	Regulasi Nasional Terkait Teknologi Informasi, Keamanan Informasi, Siber, dan Pelindungan Data	Regulasi Sektoral terkait Keamanan Teknologi Informasi, Keamanan Informasi, Siber, dan Manajemen Risiko
				Nasional Keamanan Siber Tahun 2024-2028. ✓ Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2024 tentang Tata Cara Pembuatan Dokumen Elektronik Dan Rekam Cadang Elektronik Serta Mekanisme Penghubungan Ke Pusat Data Tertentu ✓ Peraturan BSSN No. 8 Tahun 2021 tentang Penyelenggaraan Penilaian Kesiapan Penerapan SNI ISO/IEC 27001 Menggunakan Indeks Keamanan Informasi	

No	Sektor	Kementerian/ Lembaga	Kementerian Terkait	Regulasi Nasional Terkait Teknologi Informasi, Keamanan Informasi, Siber, dan Pelindungan Data	Regulasi Sektoral terkait Keamanan Teknologi Informasi, Keamanan Informasi, Siber, dan Manajemen Risiko
2	Energi dan Sumber Daya Alam	Kementerian ESDM	✓Kementerian Koordinator Bidang Kemaritiman dan Investasi ✓Kementerian Badan Usaha Milik Negara		✓ Peraturan Menteri Badan Usaha Milik Negara (BUMN) No. PER-5/MBU/09/2022 Tahun 2022 tentang Penerapan Manajemen Risiko pada BUMN ✓ Keputusan Deputi Bidang Keuangan dan Manajemen Risiko Kementerian BUMN No. SK-8/DKU.MBU/12/2023 tentang Petunjuk Teknis Penilaian Indeks Kematangan Risiko (*Risk Maturity Index*) di Lingkungan BUMN ✓ Keputusan Deputi Bidang Keuangan dan Manajemen Risiko Kementerian BUMN No. SK-6/DKU.MBU/10/2023

No	Sektor	Kementerian/ Lembaga	Kementerian Terkait	Regulasi Nasional Terkait Teknologi Informasi, Keamanan Informasi, Siber, dan Pelindungan Data	Regulasi Sektoral terkait Keamanan Teknologi Informasi, Keamanan Informasi, Siber, dan Manajemen Risiko
					tentang Petunjuk Teknis Proses Manajemen Risiko dan Agregasi pada Taksonomi Risiko Portofolio BUMN
3	Transportasi	Kementerian Perhubungan	✓ Kementerian Koordinator Bidang Kemaritiman dan Investasi ✓ Kementerian Badan Usaha Milik Negara		✓ Peraturan Menteri Perhubungan (Permenhub) No. PM 9 Tahun 2024 tentang Keamanan Penerbangan Nasional ✓ Keputusan Direktur Jenderal Perhubungan Udara Kementerian Perhubungan (Kemenhub) No. PR 24 Tahun 2023 tentang Prosedur Penanganan Informasi Keamanan Penerbangan Sensitif

No	Sektor	Kementerian/ Lembaga	Kementerian Terkait	Regulasi Nasional Terkait Teknologi Informasi, Keamanan Informasi, Siber, dan Pelindungan Data	Regulasi Sektoral terkait Keamanan Teknologi Informasi, Keamanan Informasi, Siber, dan Manajemen Risiko
					✓ Keputusan Menteri Perhubungan (Kepmenhub) No. KM 107 Tahun 2023 tentang Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di Lingkungan Kemenhub ✓ Kepmenhub Nomor KM 69 Tahun 2023 tentang Manajemen Risiko di Lingkungan Kemenhub ✓ Keputusan Direktur Jenderal Perhubungan Darat Kemenhub No. KP-DRJD 1760 Tahun 2022 tentang Pedoman Teknis Manajemen Risiko Direktorat Jenderal Perhubungan Darat

No	Sektor	Kementerian/ Lembaga	Kementerian Terkait	Regulasi Nasional Terkait Teknologi Informasi, Keamanan Informasi, Siber, dan Pelindungan Data	Regulasi Sektoral terkait Keamanan Teknologi Informasi, Keamanan Informasi, Siber, dan Manajemen Risiko
					✓ Surat Edaran (SE) Direktorat Jenderal Perhubungan Laut Kemenhub No. SE-DJPL 16 Tahun 2024 tentang Pengembangan Penilaian dan Prosedur Keamanan Siber (*Cyber Security*) pada Manajemen Keamanan Kapal dan Fasilitas Pelabuhan untuk Penanganan Risiko pada Sistem Jaringan Maya (*Cyber Risk Management*) ✓ Permenhub No. 25 Tahun 2018 tentang Tata Cara Penyelenggaraan SPIP di Lingkungan Kemenhub

No	Sektor	Kementerian/ Lembaga	Kementerian Terkait	Regulasi Nasional Terkait Teknologi Informasi, Keamanan Informasi, Siber, dan Pelindungan Data	Regulasi Sektoral terkait Keamanan Teknologi Informasi, Keamanan Informasi, Siber, dan Manajemen Risiko
					✓ Keputusan Direktur Jenderal Perkeretaapian Kemenhub No. HK.209/3/19/DJKA/2022 tentang Pedoman Teknis Penerapan Manajemen Risiko di Lingkungan Direktorat Jenderal Perkeretaapian ✓ Keputusan Direktur Jenderal Perhubungan Udara Kemenhub No. KP 207 Tahun 2021 tentang Pedoman Identifikasi Terhadap Data dan Sistem Elektronik Penerbangan yang Bersifat Kritis ✓ *International Maritime Organization* (IMO) *Circular* No. MSC-FAL.1/Circ.3/Rev.1

No	Sektor	Kementerian/ Lembaga	Kementerian Terkait	Regulasi Nasional Terkait Teknologi Informasi, Keamanan Informasi, Siber, dan Pelindungan Data	Regulasi Sektoral terkait Keamanan Teknologi Informasi, Keamanan Informasi, Siber, dan Manajemen Risiko
					tanggal 14 Juni 2021 tentang *Guidelines on Maritime Cyber Risk Management* ✓ *International Ship and Port Facility Security (ISPS) Code 2021 Edition* ✓ IMO Resolution MSC.428 (98) tentang *Maritime Cyber Risk Management in Safety Management System*
4	Keuangan	Bank Indonesia, Otoritas Jasa Keuangan	✓ Kementerian Koordinator Bidang Kemaritiman dan Investasi ✓ Badan Koordinasi		✓ Peraturan Otoritas Jasa Keuangan (POJK) No. 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum ✓ SE OJK No. 29/SEOJK.03/2022 tentang Ketahanan dan

No	Sektor	Kementerian/ Lembaga	Kementerian Terkait	Regulasi Nasional Terkait Teknologi Informasi, Keamanan Informasi, Siber, dan Pelindungan Data	Regulasi Sektoral terkait Keamanan Teknologi Informasi, Keamanan Informasi, Siber, dan Manajemen Risiko
			Penanaman Modal ✓ Badan Pengawas Perdagangan Berjangka Komoditi (BAPPEBTI) ✓ Kementerian Keuangan		Keamanan Siber bagi Bank Umum ✓ Peraturan Bank Indonesia (PBI) No. 2 Tahun 2024 tentang Keamanan Sistem Informasi dan Ketahanan Siber bagi Penyelenggara Sistem Pembayaran, Pelaku Pasar Uang dan Pasar Valuta Asing, serta Pihak Lain yang Diatur dan Diawasi Bank Indonesia ✓ POJK No. 8 Tahun 2023 tentang Penerapan Program Anti Pencucian Uang, Pencegahan Pendanaan Terorisme, dan Pencegahan Pendanaan

No	Sektor	Kementerian/ Lembaga	Kementerian Terkait	Regulasi Nasional Terkait Teknologi Informasi, Keamanan Informasi, Siber, dan Pelindungan Data	Regulasi Sektoral terkait Keamanan Teknologi Informasi, Keamanan Informasi, Siber, dan Manajemen Risiko
					Proliferasi Senjata Pemusnah Massal di Sektor Jasa Keuangan ✓ PBI No.19/10/PBI/2017 tentang Penerapan Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme bagi Penyelenggara Jasa Sistem Pembayaran Selain Bank dan Penyelenggara Kegiatan Usaha Penukaran Valuta Asing Bukan Bank (selanjutnya disebut “PBI APU PPT”).

No	Sektor	Kementerian/ Lembaga	Kementerian Terkait	Regulasi Nasional Terkait Teknologi Informasi, Keamanan Informasi, Siber, dan Pelindungan Data	Regulasi Sektoral terkait Keamanan Teknologi Informasi, Keamanan Informasi, Siber, dan Manajemen Risiko
5	Kesehatan	Kementerian Kesehatan			✓ Peraturan Menteri Kesehatan (Permenkes) No. 25 Tahun 2019 tentang Penerapan Manajemen Risiko Terintegrasi di Lingkungan Kementerian Kesehatan ✓ Keputusan Menteri Kesehatan (Kepmenkes) No. HK.01.07/MENKES/2139/2023 tentang Tim Tanggap Insiden Keamanan Siber di Lingkungan Kementerian Kesehatan

No	Sektor	Kementerian/ Lembaga	Kementerian Terkait	Regulasi Nasional Terkait Teknologi Informasi, Keamanan Informasi, Siber, dan Pelindungan Data	Regulasi Sektoral terkait Keamanan Teknologi Informasi, Keamanan Informasi, Siber, dan Manajemen Risiko
6	Teknologi Informasi dan Komunikasi (TIK)	Kementerian Komunikasi dan Informatika	Badan Siber dan Sandi Negara		✓ Pedoman Menteri Komunikasi dan Informatika (Menkominfo) No. 6 Tahun 2017 tentang Manajemen Risiko di Lingkungan Kementerian Komunikasi dan Informatika (Kemenkominfo) ✓ Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) No. 10 Tahun 2021 Perubahan atas Permenkominfo No. 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat ✓ SE Menkominfo No. 3 Tahun 2022 tentang Tanggal Efektif

No	Sektor	Kementerian/ Lembaga	Kementerian Terkait	Regulasi Nasional Terkait Teknologi Informasi, Keamanan Informasi, Siber, dan Pelindungan Data	Regulasi Sektoral terkait Keamanan Teknologi Informasi, Keamanan Informasi, Siber, dan Manajemen Risiko
					Pendaftaran Penyelenggara Sistem Elektronik Lingkup Privat ✓ Permenkominfo No. 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat
7	Pangan	Kementerian Pertanian	✓ Kementerian Koordinator Bidang Kemaritiman dan Investasi ✓ Badan Pangan Nasional ✓ Kementerian Kelautan dan Perikanan		✓ Peraturan Menteri Pertanian (Permentan) No. 38 Tahun 2021 tentang Penerapan Manajemen Risiko Lingkup Kementerian Pertanian ✓ Permentan No. 51/Permentan/TI.100/11/2016 tentang Penyelenggaraan Teknologi Informasi dan

No	Sektor	Kementerian/ Lembaga	Kementerian Terkait	Regulasi Nasional Terkait Teknologi Informasi, Keamanan Informasi, Siber, dan Pelindungan Data	Regulasi Sektoral terkait Keamanan Teknologi Informasi, Keamanan Informasi, Siber, dan Manajemen Risiko
			✓ Badan Urusan Logistik		Komunikasi di Kementerian Pertanian
8	Pertahanan	Kementerian Pertahanan	✓ Kementerian Badan Usaha Milik Negara ✓ Kementerian Koordinator Bidang Politik, Hukum, dan Keamanan ✓ TNI ✓ POLRI		✓ Peraturan Menteri Pertahanan (Permenhan) No. 17 Tahun 2021 tentang Penerapan Manajemen Risiko di Lingkungan Kementerian Pertahanan dan Tentara Nasional Indonesia ✓ Permenhan No. 82 Tahun 2014 tentang Pertahanan Siber ✓ Permenhan No.19 Tahun 2023 tentang Tata Cara Penggunaan Jasa Telekomunikasi di Lingkungan Kementerian Pertahanan dan Tentara Nasional Indonesia

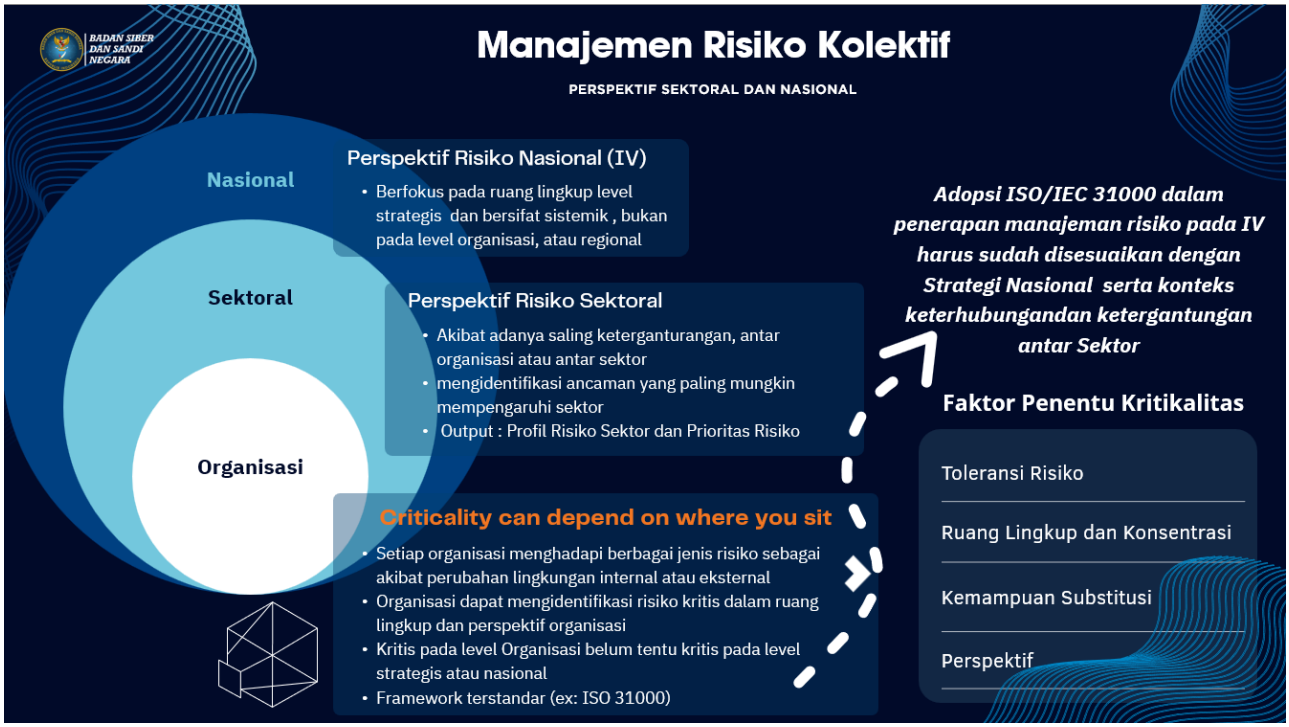
MANAJEMEN RISIKO KOLEKTIF

BAB II
MANAJEMEN RISIKO KEAMANAN SIBER SECARA KOLEKTIF

A. Gambaran Umum Manajemen Risiko Kolektif

Manajemen Risiko Kolektif merujuk pada pendekatan pengelolaan risiko di mana berbagai pemangku kepentingan berkolaborasi untuk mengidentifikasi, mengevaluasi, dan mengelola risiko. Gambaran umum risiko organisasi dan perbedaannya dengan perspektif sektoral dan nasional ditunjukkan pada Gambar 1. Penerapan manajemen risiko pada lingkup organisasi dan sektor, termasuk Penyelenggara IIV umumnya beragam, namun dapat dipastikan organisasi telah mengambil berbagai langkah untuk memitigasi risiko keamanan siber dalam menjalankan proses bisnisnya. Umumnya, organisasi telah melakukan prosedur atau upaya manajemen risiko melalui kombinasi kegiatan berikut:

a. perencanaan strategis untuk menetapkan tujuan, menentukan tindakan, mengalokasikan sumber daya, dan mengukur kemajuan;
b. penilaian risiko untuk mengidentifikasi, menilai, dan mengevaluasi risiko keamanan siber terhadap Penyelenggara IIV;
c. perencanaan manajemen darurat untuk mengintegrasikan dan mengoordinasikan pendekatan untuk mengidentifikasi dan meminimalkan dampak risiko keamanan siber yang berkaitan dengan semua operasi dari suatu Penyelenggara IIV;
d. praktik keberlangsungan bisnis untuk menangani gangguan dan memastikan keberlanjutan layanan vital;
e. langkah-langkah keamanan untuk mengatasi ancaman; dan
f. perencanaan darurat untuk memastikan prosedur tanggap darurat yang memadai tersedia untuk menghadapi keadaan darurat.



Gambar 1. Gambaran Umum Risiko Organisasi dan Perbedaannya dengan Perspektif Sektoral dan Nasional

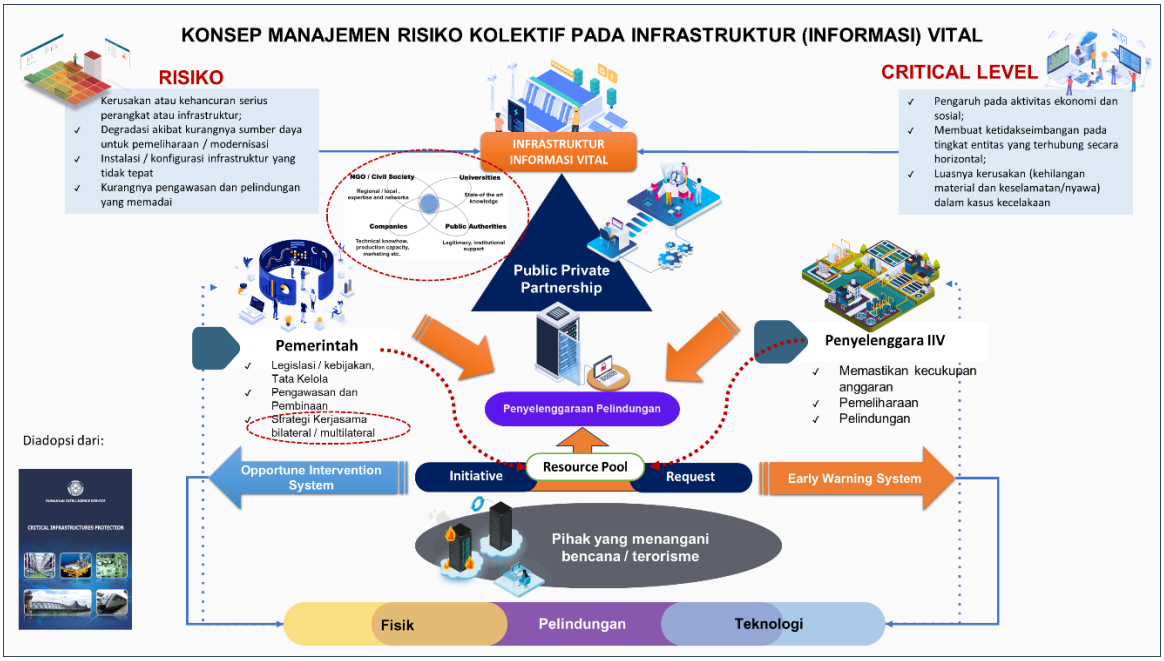
Meski berbagai upaya telah dilakukan, masih terdapat kesenjangan signifikan yang harus diatasi. Beberapa risiko keamanan siber mungkin tidak dikelola dengan baik karena kurangnya pemahaman mengenai penyebab atau dampak risiko tersebut, informasi yang terbatas, atau karena risiko tersebut relatif baru. Selain itu, ada risiko tertentu yang berada di luar kendali langsung Penyelenggara IIV, seperti kerentanan yang timbul dari ketergantungan pada pihak ketiga, kelemahan dalam rantai pasokan, atau ancaman yang muncul dari jaringan siber yang lebih luas.

Akuntabilitas dalam menangani risiko keamanan siber sering kali tidak jelas, disalahpahami, atau tidak terdistribusi dengan baik, sehingga dapat menyebabkan respons yang lambat. Beberapa risiko mungkin terlalu jarang terjadi sehingga tidak mendapatkan perhatian dan sumber daya yang memadai, atau memiliki

dampak yang terlalu besar untuk diatasi oleh organisasi secara mandiri. Untuk mengatasi kesenjangan ini, maka perlu dibentuk suatu wadah yang dapat menjembatani komunikasi dan berbagi informasi antar seluruh *stakeholder* yang terlibat dalam penyelenggaraan pelindungan IIV. Merujuk pada Perpres No. 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital, BSSN, Kementerian atau Lembaga, dan Penyelenggara IIV dapat menyelenggarakan Forum Analisis dan Berbagi Informasi Keamanan Siber. Selain itu, BSSN selaku koordinator penyelenggaraan pelindungan IIV diberikan mandat untuk menyelenggarakan rapat koordinasi secara periodik paling sedikit satu kali dalam satu tahun. Kedua amanat tersebut dapat dijadikan sarana koordinasi lintas sektoral bagi Kementerian atau Lembaga dan Penyelenggara IIV, baik dari pemerintah, swasta, maupun BUMN, untuk saling bertukar pikiran, membahas isu, serta menyusun rencana aksi untuk memperkuat kapabilitas dalam mendukung manajemen risiko keamanan siber di tingkat organisasi dan regional. Selain itu, langkah nyata yang dapat diambil adalah dengan menyusun dan menerapkan Rencana Aksi Nasional Keamanan Siber dan mekanisme lain yang ditetapkan dalam Strategi Keamanan Siber Nasional yang tertuang dalam Perpres No. 47 Tahun 2023 yang memungkinkan keterlibatan seluruh komponen dan *stakeholder* untuk bersinergi dalam memperkuat ketahanan siber nasional.

Dalam lingkup intra sektoral Kementerian atau Lembaga dapat menyelenggarakan atau membentuk Forum Koordinasi Sektoral yang terdiri dari perwakilan Penyelenggara IIV di lingkup sektornya, *Computer Security Incident Response Team* (CSIRT) atau Tim Tanggap Insiden Siber (TTIS), dan pihak lain yang diperlukan dalam mendukung implementasi manajemen risiko keamanan siber dalam lingkup sektor. Keterlibatan dalam Forum Koordinasi Sektoral memungkinkan mitra publik dan swasta untuk meningkatkan respons terhadap keadaan darurat, mengidentifikasi kerentanan dengan lebih baik melalui saling ketergantungan, mengalokasikan sumber daya secara kolektif ke area prioritas,

serta mengembangkan langkah-langkah mitigasi risiko keamanan siber yang lebih tepat sesuai dengan pemahaman mendalam tentang operasi dan persyaratan sektor.



Gambar 2. Konsep Manajemen Risiko Kolektif pada IIV

Gambar 2 menjelaskan konsep manajemen kolektif pada IIV yang meliputi kolaborasi pihak-pihak yang berkepentingan, peran dari masing-masing entitas, serta sumber daya dan kapabilitas pihak tersebut dalam mengelola risiko. Pemerintah dan pemangku kepentingan terkait bekerja sama untuk memperjelas dan mendefinisikan peran dan tanggung jawab, jika diperlukan, serta membangun kemitraan terpercaya di dalam sektor dan lintas sektor. Kegiatan manajemen risiko keamanan siber kolektif memungkinkan pemerintah untuk melakukan hal-hal berikut:

a. mengidentifikasi dan mengatasi kesenjangan legislatif dan kebijakan;

b. memberikan analisis dan informasi yang lebih tepat waktu, akurat, dan berguna kepada penyelenggara dan operator tentang ancaman dan risiko keamanan siber;
c. bekerja sama dengan penyelenggara dan operator untuk menekankan manfaat berinvestasi dalam langkah-langkah keamanan dan meningkatkan ketahanan;
d. menyediakan alat bantu, praktik terbaik, dan panduan lain untuk mendukung kegiatan manajemen risiko keamanan siber dalam sektor infrastruktur vital; dan
e. memperkuat pembagian informasi yang sensitif terhadap waktu selama situasi manajemen ancaman dan insiden yang muncul.

Kegiatan manajemen risiko keamanan siber kolektif menghasilkan manfaat bagi seluruh komunitas infrastruktur vital, termasuk:

a. mengidentifikasi dan menangani risiko-risiko strategis, sistemik, atau nasional;
b. mengidentifikasi dan menangani risiko akibat ketergantungan;
c. respons yang lebih cepat dan lebih efektif terhadap serangan dan gangguan;
d. pemulihan aset vital dan layanan penting dengan cepat ketika terjadi gangguan;
e. memanfaatkan keahlian dan sumber daya sektor publik-swasta secara kolektif untuk menghadapi ancaman yang ada dan yang akan muncul; dan
f. memperkuat ketahanan infrastruktur informasi vital Indonesia, sehingga membangun keamanan siber Indonesia yang lebih aman dan terjamin.

CASCADING EFFECT

B. Cascading Effect

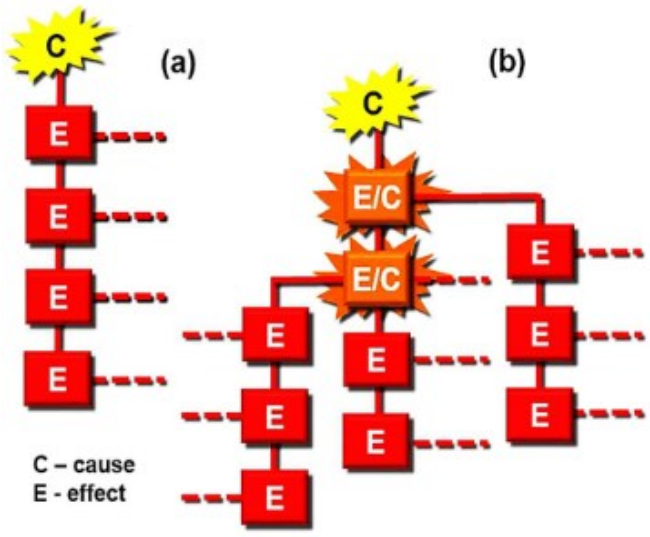
1. Keterkaitan Pertimbangan dalam Penerapan Manajemen Risiko pada Level Organisasi dan *Cascading Effect* pada Level Sektoral

Dalam implementasi manajemen risiko, terdapat beberapa pertimbangan penting yang harus diperhatikan. Salah satu pertimbangan utama adalah resistansi yang mungkin muncul akibat ketidaktahuan atau kurangnya pemahaman terhadap risiko yang ada. Ketidaktahuan ini dapat menghambat proses penerapan manajemen risiko yang efektif. Selain itu, penerapan kontrol keamanan yang tidak sesuai dengan spesifikasi risiko yang ada juga menjadi tantangan tersendiri. Kontrol yang tidak spesifik terhadap risiko tertentu dapat mengakibatkan efektivitas manajemen risiko menjadi kurang optimal.

Aspek lain yang umumnya tidak dipertimbangkan oleh organisasi dalam menjalankan manajemen risiko adalah potensi *cascading effect*/dampak berjenjang yang mungkin timbul. *Cascading effect* dalam konteks keamanan siber merujuk pada dampak yang meluas dari suatu insiden siber yang memengaruhi berbagai sistem yang saling terhubung. Dalam sektor infrastruktur informasi vital (IIV), *cascading effect* dapat terjadi ketika satu insiden, seperti serangan siber atau kegagalan sistem, memicu gangguan yang menyebar ke berbagai sektor dan memengaruhi operasi yang lebih luas.[5] Dalam referensi lain, *cascading effect* dapat didefinisikan sebagai dinamika yang ada dalam bencana, di mana dampak awal dari suatu kejadian fisik atau perkembangan kegagalan teknologi atau manusia memicu serangkaian peristiwa di sub-sistem manusia yang mengakibatkan gangguan fisik, sosial, atau ekonomi.

[5] Palleti, V., Adepu, S., Mishra, V. et al. Cascading effects of cyber-attacks on interconnected critical infrastructure. Cybersecury 4, 8 (2021). https://doi.org/10.1186/s42400-021-00071-z

Pada kondisi adanya dampak berjenjang, dampak awal dapat memicu fenomena lain yang menyebabkan konsekuensi dengan magnitudo yang signifikan. *Cascading effect* bersifat kompleks dan multidimensional serta terus berkembang seiring berjalannya waktu. ***Cascading effect* lebih memiliki keterkaitan dengan besarnya kerentanan daripada dengan bahaya itu sendiri. *Bahaya dengan tingkat rendah dapat menghasilkan efek rantai yang luas jika kerentanannya tersebar luas dalam sistem atau tidak ditangani dengan baik di sub-sistem*.** [6] Atas dasar hal tersebut, terdapat kemungkinan untuk mengisolasi elemen-elemen dalam rantai dan melihatnya sebagai bencana individual (sub-sistem) yang berdiri sendiri. Secara khusus, *cascading effect* dapat berinteraksi dengan efek sekunder atau *intangible effect* dari sebuah bencana.[7]



Gambar 3. Gambaran Cascading Effect

[6] Pescaroli, Gianluca & Turner, Sandra & Gould, T & Alexander, D & Wicks, Robert. (2017). Cascading Effects And Escalations In Wide Area Power Failures.- A Summary For Emergency Planners.
[7] Pescaroli, Gianluca & Turner, Sandra & Gould, T & Alexander, D & Wicks, Robert. (2017). Cascading Effects And Escalations In Wide Area Power Failures.- A Summary For Emergency Planners.

Gambar 3 mengilustrasikan perbedaan antara: (a) jalur linier dari *cascading effect*, dan (b) jalur kompleks dari *cascading effect*. Dalam "*cascading disaster*", keadaan darurat sekunder dapat meningkat dan menjadi pusat krisis yang menantang koordinasi bantuan darurat dan pemulihan jangka panjang.

Contoh kasus *cascading effect* dapat terlihat ketika sistem imigrasi yang berada di sektor administrasi pemerintahan mengalami serangan siber. Misalnya, serangan *ransomware* menyebabkan sistem imigrasi tidak dapat diakses, sehingga seluruh proses verifikasi, pengecekan data penumpang, dan izin masuk-keluar negara terhenti. Dampak langsung dari serangan ini akan dirasakan oleh sektor transportasi, terutama penerbangan internasional, di mana bandara harus menghentikan sementara penerbangan karena tidak dapat memproses penumpang yang datang maupun pergi. Akibatnya, terjadi penundaan penerbangan, penumpukan penumpang, dan potensi kerugian finansial yang signifikan bagi maskapai penerbangan serta bandara.

Contoh kasus di atas menunjukkan betapa pentingnya bagi organisasi untuk memahami hubungan keterkaitan atau ketergantungan dengan layanan dan sistem eksternal yang digunakan dalam operasionalnya. Ketergantungan sistem imigrasi pada infrastruktur transportasi memperlihatkan bahwa gangguan di satu sektor dapat menimbulkan efek berantai yang memengaruhi sektor lain. Oleh karena itu, pengelolaan risiko tidak hanya harus mempertimbangkan risiko internal tetapi juga perlu mengevaluasi risiko yang berasal dari hubungan dengan pihak ketiga atau sistem eksternal yang menjadi bagian dari ekosistem operasional organisasi. Dengan memahami ketergantungan ini, organisasi dapat mengembangkan strategi mitigasi yang

lebih komprehensif dan meningkatkan ketahanan terhadap serangan siber yang dapat berdampak luas pada sektor-sektor terkait.

Untuk menjawab permasalahan ini perlu dirumuskan langkah perbaikan yang dapat diambil oleh organisasi. Selain itu, perlu juga dilakukan peninjauan perspektif risiko sektoral yang mungkin tidak dipertimbangkan oleh organisasi dan kaitannya dengan potensi risiko sektoral serta *cascading effect* yang mungkin timbul, yang dijelaskan pada Tabel 2. Tabel 2 berikut menjelaskan poin-poin indikator tantangan dalam penerapan manajemen risiko beserta langkah perbaikan, potensi, serta situasi di mana satu kejadian atau insiden memicu serangkaian dampak berantai yang memengaruhi berbagai sistem, proses, atau infrastruktur lainnya.

Tabel 2. Keterkaitan Pertimbangan Dalam Penerapan Manajemen Risiko Pada Level Organisasi dan *Cascading Effect* Akibat Potensi Risiko Pada Level Sektoral

Pertimbangan	Deskripsi	Langkah Perbaikan	Contoh Potensi Risiko Sektoral	*Cascading effect*
Resistansi Akibat Ketidaktahuan Terhadap Risiko	Kurangnya pemahaman tentang risiko yang ada.	✓ Edukasi dan sosialisasi mengenai pentingnya manajemen risiko. ✓ Pelatihan dan *workshop* untuk semua pihak terkait.	Risiko serangan siber yang menargetkan sistem kontrol industri (ICS) yang dapat menyebabkan kerusakan fisik pada infrastruktur.	Risiko ini dapat menimbulkan efek *cascading*, seperti gangguan pada pasokan listrik yang memengaruhi fasilitas kesehatan atau layanan darurat.

Pertimbangan	Deskripsi	Langkah Perbaikan	Contoh Potensi Risiko Sektoral	*Cascading effect*
Penerapan Kontrol Keamanan yang Tidak Sesuai	Kontrol yang tidak sesuai dapat mengurangi efektivitas mitigasi.	✓ Evaluasi kembali kontrol keamanan berdasarkan jenis dan tingkat risiko. ✓ Menyesuaikan kontrol dengan spesifikasi risiko.	Risiko siber yang berkaitan dengan perangkat IoT yang digunakan dalam infrastruktur kritikal, seperti sensor dan aktuator.	serangan terhadap perangkat IoT bisa menyebabkan gangguan pada data monitoring yang krusial, yang kemudian dapat memengaruhi keputusan operasional dan menyebabkan kegagalan sistem lebih luas.
Kurangnya Dukungan dari Top Level Manajemen	Manajemen puncak tidak mendukung penerapan manajemen risiko.	✓ Meningkatkan kesadaran manajemen puncak tentang pentingnya manajemen risiko. ✓ Melibatkan manajemen puncak dalam proses penilaian risiko.	Risiko kegagalan sistem akibat kurangnya investasi dalam teknologi keamanan yang diperlukan untuk melindungi IIV.	Risiko ini dapat memperpanjang dampak serangan karena keterlambatan dalam mengidentifikasi dan mengatasi kerentanan.

Pertimbangan	Deskripsi	Langkah Perbaikan	Contoh Potensi Risiko Sektoral	*Cascading effect*
Ketidakcukupan Sumber Daya	Sumber daya yang tidak mencukupi untuk penerapan manajemen risiko.	✓ Mengalokasikan sumber daya yang memadai untuk manajemen risiko. ✓ Mencari dukungan eksternal jika diperlukan.	Risiko serangan siber terkoordinasi dari aktor negara atau kelompok kriminal yang menargetkan IIV untuk sabotase atau spionase.	Serangan terkoordinasi dapat menyebabkan gangguan berantai (*cascading effects*) yang memengaruhi beberapa sektor sekaligus, misalnya gangguan pada jaringan komunikasi yang memengaruhi sektor perbankan dan layanan publik.
Kekurangan dalam Pemantauan dan Evaluasi Risiko	Pemantauan dan evaluasi risiko tidak dilakukan secara berkelanjutan.	✓ Mengimplementasikan sistem pemantauan risiko yang berkelanjutan. ✓ Melakukan evaluasi risiko secara periodik.	Risiko ketidakmampuan mendeteksi dan merespons insiden siber secara cepat, yang dapat menyebabkan	Risiko ini bisa menyebabkan efek domino, di mana gangguan awal yang tidak tertangani dengan baik berkembang menjadi masalah yang lebih besar

Pertimbangan	Deskripsi	Langkah Perbaikan	Contoh Potensi Risiko Sektoral	*Cascading effect*
			kerusakan lebih besar.	dan menyebar ke berbagai bagian infrastruktur.

2. **Identifikasi *Cascading Effect***

Interdependensi antara sistem dan proses dalam organisasi berpotensi menimbulkan dampak luas akibat satu insiden siber. Efek berantai muncul ketika insiden siber memicu kegagalan atau gangguan pada sistem lain yang saling terkait. Pemahaman dan identifikasi atas efek berantai ini menjadi aspek penting bagi organisasi dalam mengelola risiko siber secara efektif dan melindungi infrastruktur kritis. Identifikasi efek berantai (*cascading effect*) pada risiko siber yang dapat meluas dari level organisasi hingga sektoral atau nasional dapat dilakukan melalui beberapa langkah berikut:

a. **Pemetaan Interdependensi Sistem**

Pemetaan semua sistem dan proses yang saling bergantung dalam organisasi mencakup infrastruktur teknologi, proses bisnis, dan hubungan dengan pihak eksternal. Pemahaman interdependensi ini mendukung identifikasi dampak potensial dari kegagalan pada satu sistem terhadap sistem lainnya[8].

b. **Analisis Skenario**

Adanya analisis skenario memungkinkan dilaksanakannya simulasi berbagai jenis serangan siber dan dampaknya pada sistem yang saling bergantung sehingga membantu dalam mengidentifikasi potensi efek berantai. Studi kasus pada infrastruktur kritis menunjukkan efektivitas

[8] Palleti, V., Adepu, S., Mishra, V. et al. Cascading effects of cyber-attacks on interconnected critical infrastructure. Cybersecur 4, 8 (2021).

pendekatan ini dalam mengungkap titik lemah serta potensi dampak berantai [9].

c. **Penilaian Risiko Terintegrasi**

Penilaian risiko terintegrasi mencakup semua aset, fungsi, dan proses dalam organisasi. Hal ini dapat membantu dalam mengidentifikasi risiko yang berpotensi menyebar ke sektor lain atau ke tingkat nasional. Dengan penilaian ini, organisasi memperoleh gambaran yang lebih menyeluruh tentang potensi dampak serangan siber.

d. **Kolaborasi Antar Organisasi**

Kolaborasi dengan organisasi lain dalam sektor yang sama atau terkait memungkinkan pertukaran informasi dan strategi mitigasi risiko. Pendekatan ini membantu dalam proses identifikasi dan pengelolaan risiko yang mungkin berdampak lintas organisasi. Sinergi semacam ini memperkuat ketahanan terhadap serangan siber dan mengurangi dampak berantai yang mungkin terjadi.

e. **Penggunaan Model dan Simulasi**

Model dan simulasi memberikan prediksi tentang penyebaran serangan siber melalui berbagai sistem dan infrastruktur. Hal ini dapat membantu perencanaan langkah mitigasi yang tepat. Pemanfaatan model ini mendukung organisasi dalam memahami dampak dari ketergantungan internal maupun eksternal serta risiko yang mungkin timbul akibat hubungan tersebut. Salah satu contohnya adalah skenario eskalasi dan dampak berjenjang dalam situasi gangguan pada *Internet Exchange* (*Internet Exchange Outage*). *Internet Exchange Outage* adalah situasi di mana layanan yang disediakan oleh sebuah *Internet Exchange* mengalami gangguan atau kegagalan sehingga lalu lintas internet yang melewati

9 Schauer, S., Grafenauer, T., König, S., Warum, M., & Rass, S. (2019). Estimating cascading effects in Cyber-Physical critical infrastructures. In Lecture notes in computer science (pp. 43–56). https://doi.org/10.1007/978-3-030-37670-3_4

infrastruktur tersebut tidak dapat berfungsi dengan baik. Hal ini dapat memengaruhi konektivitas internet antara berbagai penyedia layanan (*Internet Service Provider* atau ISP) dan organisasi lain yang terhubung ke *Internet Exchange* tersebut. Tabel 3 menyajikan beberapa sektor yang terdampak, efek yang meluas akibat kegagalan operasional internet, beserta kondisi yang merujuk pada penyebab atau keadaan spesifik yang memicu efek berantai (*cascading effects*) dan eskalasi yang berdampak pada sektor. [10]

Tabel 3. Eskalasi dan dampak berjenjang dalam situasi *Internet Exchange Outage*

Eskalasi dan dampak berjenjang dalam situasi *Internet Exchange Outage*		
Sektor Terdampak	***Cascading Effects* dan Eskalasi**	**Kondisi Situasional**
Trigger: Internet Exchange Outage	Kehilangan konektivitas internet antar penyedia layanan menyebabkan putusnya akses data dan komunikasi yang luas, memengaruhi layanan esensial seperti perbankan, kesehatan, dan pemerintahan.	Kegagalan infrastruktur *Internet Exchange* karena serangan siber (DDoS, *malware*), kesalahan konfigurasi, atau pemadaman daya tanpa *backup* yang memadai.

[10] Diadposi dari paper Cascading Effects And Escalations In Wide Area Power Failures.- A Summary For Emergency Planners.

Eskalasi dan dampak berjenjang dalam situasi *Internet Exchange Outage*		
Sektor Terdampak	***Cascading Effects* dan Eskalasi**	**Kondisi Situasional**
Compounding Factors	Ketergantungan pada *Internet Exchange* yang berfungsi sebagai pusat penghubung utama dalam ekosistem internet nasional tanpa adanya redundansi geografis atau *Internet Exchange* alternatif. Dampak diperburuk oleh kurangnya kapasitas cadangan dan keterbatasan sumber daya untuk pemulihan cepat.	*Internet Exchange* yang terpusat dan tidak memiliki sistem *failover* yang efektif, serta tidak adanya perjanjian pemulihan cepat dengan penyedia layanan *Internet Exchange*.
Direct Threats to Life	Gangguan layanan kesehatan, termasuk *telemedicine*, sistem rekam medis digital, dan koordinasi antar rumah sakit yang mengandalkan internet, yang berpotensi mengancam keselamatan pasien dengan kondisi kritis atau yang membutuhkan penanganan jarak jauh secara segera.	Rumah sakit yang menggunakan sistem TI terintegrasi berbasis *cloud*, dan layanan kesehatan digital yang tidak memiliki jaringan cadangan.

Eskalasi dan dampak berjenjang dalam situasi *Internet Exchange Outage*		
Sektor Terdampak	***Cascading Effects* dan Eskalasi**	**Kondisi Situasional**
Telecommunications	Pemutusan akses layanan komunikasi digital seperti VoIP, *e-mail*, aplikasi pesan instan, dan konferensi video, yang mengakibatkan hambatan serius dalam komunikasi antar institusi, pemerintah, dan masyarakat.	Perusahaan dan lembaga publik bergantung pada layanan internet untuk komunikasi sehari-hari tanpa alternatif telekomunikasi independen.
Financial Services	Hilangnya akses ke ATM, sistem pembayaran digital, dan aplikasi perbankan *online* yang menyebabkan transaksi keuangan terhenti, gangguan besar pada pasar keuangan, dan meningkatnya risiko penipuan karena terganggunya sistem keamanan berbasis internet.	Perbankan dan pasar modal yang mengandalkan koneksi internet *real-time* untuk operasi sehari-hari dan tidak memiliki jalur komunikasi alternatif.
Transportation	Disrupsi pada sistem manajemen transportasi, termasuk pengendalian lalu lintas berbasis internet, sistem tiket elektronik, dan GPS, menyebabkan penundaan besar dalam	Sistem transportasi pintar dan logistik yang sangat bergantung pada koneksi internet untuk operasional dan navigasi, tanpa alternatif operasional.

Eskalasi dan dampak berjenjang dalam situasi *Internet Exchange Outage*		
Sektor Terdampak	***Cascading Effects* dan Eskalasi**	**Kondisi Situasional**
	transportasi publik, kebingungan di jalan raya, dan gangguan logistik.	
Public Safety	Pemadaman pada sistem keamanan publik seperti CCTV, kontrol akses pintar, dan alarm keamanan yang dihubungkan melalui internet, yang mengurangi efektivitas penegakan hukum dan meningkatkan risiko kejahatan, serta mempersulit investigasi insiden.	Kota pintar yang bergantung pada jaringan keamanan terintegrasi berbasis internet dengan sedikit atau tanpa opsi pemantauan manual.
Emergency Response	Hambatan besar dalam koordinasi dan komunikasi antar layanan darurat, seperti pemadam kebakaran, polisi, dan ambulans, yang meningkatkan waktu respons dan memperparah dampak dari situasi darurat. Kesulitan dalam mengakses informasi vital juga memperlambat pengambilan keputusan dalam situasi kritis.	Layanan darurat yang bergantung pada jaringan komunikasi digital dan data berbasis *cloud* tanpa redundansi jaringan radio atau satelit.

Eskalasi dan dampak berjenjang dalam situasi *Internet Exchange Outage*		
Sektor Terdampak	***Cascading Effects* dan Eskalasi**	**Kondisi Situasional**
Economic Impact	Gangguan luas pada bisnis, termasuk *e-commerce*, aplikasi bisnis berbasis *cloud*, dan operasi manufaktur yang bergantung pada konektivitas internet, yang menyebabkan penurunan produktivitas, gangguan rantai pasokan, dan potensi kerugian ekonomi yang signifikan.	Industri yang menggunakan teknologi *IoT, e-commerce* yang tidak dapat mengakses layanan transaksi, dan manufaktur dengan kendali jarak jauh.
Social Impact	Ketidakmampuan masyarakat mengakses layanan digital penting seperti media sosial, platform pembelajaran *online*, dan hiburan, yang menyebabkan peningkatan stres sosial, ketidakpastian, dan potensi keresahan publik. Penggunaan layanan alternatif seperti jaringan seluler dapat terbatas akibat *overloading* atau masalah teknis.	Penggunaan internet yang tinggi untuk kebutuhan sehari-hari, tanpa ada edukasi atau persiapan terhadap kondisi tanpa konektivitas.

Eskalasi dan dampak berjenjang dalam situasi *Internet Exchange Outage*		
Sektor Terdampak	***Cascading Effects* dan Eskalasi**	**Kondisi Situasional**
Operational Capability Challenges	Penurunan drastis kapasitas operasional di berbagai sektor kritikal, termasuk infrastruktur TI yang tidak dapat melakukan monitoring dan kontrol jarak jauh, mengakibatkan kehilangan kontrol sistem secara keseluruhan dan meningkatnya risiko kesalahan operasional.	Kurangnya *backup* manual atau mekanisme pengendalian fisik di sektor-sektor kritikal yang bergantung pada kontrol berbasis internet.

MANAJEMEN RISIKO ORGANISASI

BAB III
MANAJEMEN RISIKO KEAMANAN SIBER ORGANISASI

A. Pihak yang Terlibat

Manajemen risiko pada level organisasi menjadi esensial dalam menjamin keberlangsungan organisasi serta kelancaran proses bisnis. Kebutuhan akan kolaborasi dan kerja sama antara berbagai pihak sangat penting. Demi tercapainya manajemen risiko yang efektif dan efisien, pemahaman mendalam mengenai peran masing-masing pihak sangat diperlukan. Setidaknya terdapat lima pihak yang harus memahami peran mereka dalam manajemen risiko organisasi, antara lain:

a. Pemimpin Organisasi

Pemimpin Organisasi yang dimaksud merupakan pimpinan tertinggi dalam suatu organisasi, misalnya Ketua, Kepala, Direktur Utama, CEO, dan lain-lain. Sebagai pimpinan tertinggi, Pemimpin Organisasi memiliki peran penting untuk menjamin dan memastikan terlaksananya manajemen risiko pada level organisasi sesuai dengan kondisi/profil risiko setiap organisasi. Pemimpin Organisasi juga memiliki wewenang dan kekuatan untuk mendukung perannya tersebut.

b. Top Level Management

Top Level Management merupakan orang atau pihak yang bertanggung jawab atas keberlangsungan proses bisnis pada suatu organisasi, misalnya Direktur Operasional, Direktur Logistik, Direktur Keuangan, dan lain-lainnya. *Top Level Management* memiliki wewenang untuk menyampaikan dampak akibat adanya gangguan terhadap proses bisnis.

c. Unit Kerja/Fungsi Manajemen Risiko

Fungsi Manajemen Risiko merupakan tim atau unit kerja yang bertanggung jawab atas manajemen risiko pada keseluruhan organisasi. Fungsi Manajemen Risiko bertanggung jawab untuk mengoordinasikan dan menjadi penghubung pihak-pihak terkait, khususnya terkait proses bisnis dan teknis atau operasional di organisasi dalam hal penilaian risiko. Fungsi Manajemen Risiko juga harus memastikan keputusan yang diambil oleh pimpinan telah berdasarkan pada risiko yang ada.

d. Fungsi Operasional dan Teknologi

Fungsi operasional merupakan tim atau unit kerja yang bertanggung jawab atas operasional dan pemeliharaan infrastruktur dan teknologi, termasuk jaringan internet, aplikasi, perangkat keras, teknologi operasi, dan lain-lainnya yang menunjang keberlangsungan proses bisnis organisasi. Fungsi ini harus memahami secara menyeluruh operasional infrastruktur teknologi yang dioperasikan beserta dampak yang ditimbulkan akibat gangguan terhadap operasional terhadap proses bisnis organisasi.

e. Fungsi Keamanan Siber

Fungsi Keamanan Siber merupakan tim atau unit kerja dalam organisasi yang bertanggung jawab atas penerapan dan pemeliharaan kontrol keamanan siber dalam sistem yang mendukung aktivitas bisnis. Fungsi Keamanan Siber memiliki tugas untuk mengidentifikasi potensi ancaman terhadap suatu sistem, menyusun konsep skenario risiko, menentukan kemungkinan risiko, dan memberikan masukan terkait langkah yang harus diambil untuk mengatasi ancaman/serangan tersebut.

B. Pertimbangan

Dalam mengimplementasikan manajemen risiko, terdapat beberapa hal yang perlu diperhatikan oleh setiap pihak terkait yang dapat menjadi hambatan dalam pelaksanaan manajemen risiko, antara lain:

a. Resistansi akibat ketidaktahuan terhadap risiko yang ada

Organisasi terkadang memiliki resistansi dalam menerapkan manajemen risiko terhadap organisasinya karena kurangnya pemahaman pihak-pihak terkait terhadap risiko yang muncul pada organisasi tersebut. Hal ini dapat terjadi akibat tidak adanya fungsi manajemen risiko maupun kurangnya pemahaman Pimpinan Organisasi terhadap pentingnya manajemen risiko pada level organisasi.

b. Menerapkan kontrol keamanan yang tidak sesuai

Organisasi sering kali salah atau menerapkan kontrol keamanan yang tidak sesuai dengan penyebab atau risiko yang ada. Hal ini disebabkan oleh pendekatan yang diambil oleh organisasi terlalu luas yang diakibatkan oleh kurangnya pemahaman tentang skenario risiko atau risiko yang ada secara keseluruhan.

C. Kontak Risiko

Sebelum setiap pihak terkait mengimplementasikan manajemen risiko, setiap pihak terkait perlu untuk memiliki kesamaan persepsi tentang risiko yang ada. Oleh karena itu, risiko yang ada perlu didefinisikan, termasuk di dalamnya sejauh mana toleransi yang dapat diterima oleh organisasi terhadap risiko yang ada.

a. Definisi Risiko

Dalam melihat risiko keamanan siber secara umum, kita dapat melihat kemungkinan terjadinya peristiwa ancaman tertentu terhadap kerentanan suatu aset, atau *likelihood*, dan dampak yang dihasilkan dari terjadinya peristiwa ancaman tersebut, atau *impact*. Risiko pada organisasi sendiri dapat didefinisikan dengan fungsi dari *likelihood* dan *impact*.

Risiko = fungsi (*Likelihood*, *Impact*)

b. Toleransi Risiko

Toleransi Risiko adalah tingkat risiko yang dapat diterima oleh organisasi dalam mencapai tujuan bisnis. Penetapan toleransi risiko membantu organisasi memahami sejauh mana risiko dapat diterima sesuai dengan kemampuan dan tujuan yang ingin dicapai.

Toleransi risiko siber pada organisasi Penyelenggara IIV terdiri atas lima tingkat risiko yang terdiri dari rendah, menengah, menengah-tinggi, tinggi, dan sangat tinggi. Setiap tingkat risiko menggambarkan kondisi ambang batas yang dapat diterima oleh organisasi dan apa yang harus dilakukan organisasi saat mencapai toleransi risiko tersebut.

Tabel 4 menjelaskan tingkat risiko berdasarkan deskripsi toleransi risiko dalam suatu organisasi. Risiko dikategorikan dari **sangat tinggi** hingga **rendah**, dengan tindakan yang berbeda sesuai tingkatannya.

Tabel 4. Tingkat Risiko

Tingkat Risiko	Deskripsi Toleransi Risiko
Sangat tinggi	Tingkat risiko sangat tinggi tidak dapat diterima oleh organisasi dan akan menimbulkan dampak yang sangat serius. Seluruh aktivitas (fungsi) terkait harus segera dihentikan. Strategi untuk memitigasi risiko dan pengalihan (fungsi) harus segera diterapkan.
Tinggi	Tingkat risiko tinggi tidak dapat diterima oleh organisasi. Strategi penanganan yang bertujuan untuk mengurangi tingkat risiko harus dikembangkan dan diterapkan dalam jangka waktu satu bulan ke depan.
Menengah-tinggi	Tingkat risiko menengah-tinggi tidak dapat diterima oleh organisasi. Strategi penanganan yang bertujuan untuk mengurangi tingkat risiko harus dikembangkan dan diterapkan dalam jangka waktu 3-6 bulan ke depan.
Menengah	Tingkat risiko menengah dapat diterima oleh organisasi jika belum terdapat strategi penanganan yang dapat diterapkan dengan mudah dan ekonomis untuk mengurangi tingkat risiko. Risiko yang ada harus dipantau secara berkala untuk memastikan setiap perubahan selalu terawasi dan dapat ditindaklanjuti dengan tepat.
Rendah	Tingkat risiko rendah dapat diterima oleh organisasi jika belum terdapat strategi penanganan yang dapat diterapkan dengan mudah dan ekonomis untuk mengurangi tingkat risiko. Risiko yang ada harus dipantau secara berkala untuk memastikan bahwa setiap perubahan selalu terawasi dan dapat ditindaklanjuti dengan tepat.

PENILAIAN RISIKO ORGANISASI

BAB IV
PENILAIAN RISIKO ORGANISASI

A. Konteks Risiko

Tahapan pertama dalam melaksanakan penilaian risiko organisasi yaitu identifikasi risiko yang dilaksanakan melalui tiga tahapan utama yang terdiri dari:

1. Identifikasi Aset

Identifikasi aset berguna untuk memahami aset fisik dan logis yang menunjang berjalannya fungsi atau sistem di organisasi sesuai dengan ruang lingkup penilaian risiko. Dalam melakukan identifikasi terhadap aset yang ada, perlu diperhatikan jenis aset *crown jewel* dan jenis aset perantara.

Aset *crown jewel* merupakan aset utama yang mendukung kelancaran fungsi bisnis, seperti Sistem Elektronik dalam operasional layanan di infrastruktur vital yang berperan langsung dalam menjaga layanan tersebut. Gangguan pada Sistem Elektronik ini berpotensi menghambat operasional layanan secara signifikan.

Aset perantara adalah aset yang berpotensi dikendalikan dan dimanfaatkan oleh penyerang sebagai sarana perpindahan antarsegmen jaringan dalam upaya mencapai titik tertinggi atau aset *crown jewel*. Contohnya mencakup sistem elektronik yang digunakan oleh pihak ketiga dan terhubung ke infrastruktur atau layanan vital. Ketika berhasil dikuasai, aset ini dapat menjadi akses awal yang memungkinkan eskalasi terhadap sistem yang mendukung layanan vital.

Penyerang akan berusaha untuk mengeksploitasi aset *crown jewel* dan memengaruhi fungsi di suatu organisasi, termasuk di dalamnya melalui aset perantara. Oleh karena itu, daftar aset yang dimiliki oleh organisasi dapat digabungkan untuk menciptakan diagram arsitektur jaringan yang menggambarkan saling keterkaitan antaraset. Dengan mengidentifikasi kedua aset ini beserta titik masuk serangan, termasuk di dalamnya *attack vectors*, aset *crown jewel*, serta aset perantara pada

diagram arsitektur jaringan, dapat membantu mengidentifikasi ancaman yang ada.

2. Pemodelan Ancaman

Proses pemodelan ancaman mencakup tiga tahapan utama: 1) identifikasi ruang lingkup (*scope*) dan dekomposisi sistem, 2) identifikasi ancaman, dan 3) pemodelan ancaman. Tahap pertama, identifikasi ruang lingkup dan dekomposisi sistem, berjalan seiring dengan identifikasi aset yang telah dilakukan sebelumnya. Tahap kedua, identifikasi ancaman, dilakukan organisasi melalui pendekatan sistematis terhadap peristiwa yang memungkinkan penyerang untuk mengeksploitasi aset. Tahap ketiga, pemodelan ancaman, menggabungkan peristiwa-peristiwa (*events*) yang teridentifikasi ke dalam suatu rangkaian serangan (*sequence of attack*). Dengan pemodelan ini, organisasi dapat memprioritaskan kontrol yang perlu diterapkan pada sistem yang harus dilindungi.

Sebagai contoh, operator pembangkit listrik mengidentifikasi ruang lingkup sistem yang digunakan dalam operasional, mencakup SCADA, sistem komunikasi, dan perangkat lapangan. Dekomposisi sistem dilakukan pada masing-masing bagian, seperti SCADA yang memiliki SCADA *Master Station*. Setelah itu, operator mengidentifikasi potensi ancaman terhadap sistem SCADA, misalnya *spoofing*, *tampering*, *information disclosure*, hingga *privilege escalation*.

Setelah ancaman diidentifikasi, selanjutnya dapat dilakukan pemodelan ancaman menjadi sebuah urutan serangan. Dalam kasus ini misalnya, penyerang yang mendapatkan akses melakukan *spoofing*, kemudian melakukan *tampering* terhadap parameter yang ada, selanjutnya melakukan *privilege escalation* untuk mendapatkan hak admin sehingga mendapatkan akses kepada informasi rahasia yang ada, untuk selanjutnya disebarkan atau melakukan *information disclosure*. Dengan adanya pemodelan ancaman, operator dapat menyiapkan kontrol yang sesuai terhadap sistem SCADA dan ancaman-ancaman tersebut.

3. Penyusunan Skenario Risiko

Tahap terakhir, yaitu penyusunan skenario risiko, bertujuan memberikan gambaran realistis mengenai potensi kesalahan serta risiko yang mungkin terjadi dengan mempertimbangkan konteks bisnis, lingkungan sistem, dan ancaman yang ada. Skenario risiko yang dirancang secara cermat mempermudah komunikasi kepada pihak-pihak berkepentingan serta mendukung analisis risiko yang terstruktur.

Dalam penyusunan skenario risiko, terdapat empat faktor utama yang perlu dicakup: 1) aset sebagai objek berharga yang telah diidentifikasi, 2) kejadian ancaman (*threat event*) sebagai insiden serangan yang telah diidentifikasi, 3) kerentanan yang mencakup kelemahan pada aset atau proses pendukung yang dapat dieksploitasi, serta 4) konsekuensi sebagai dampak dari kejadian ancaman tersebut.

Diberikan 2 (dua) contoh skenario risiko. Pada Contoh 1, dapat dilihat kerentanan pada sistem internal (aset) dieksploitasi sehingga menjadi suatu kejadian ancaman (*threat event*) dan menimbulkan konsekuensi.

Contoh 1:

Hacker mengeksploitasi CVE[11] pada server pusat data yang belum diperbarui untuk menyisipkan dan menjalankan *ransomware* sehingga data pada server tidak dapat diakses oleh pengguna.

Keterangan:

Kejadian Ancaman (*Threat Event*)

Kerentanan

Aset

Konsekuensi

[11] CVE (*Common Vulnerabilities and Exposures*) adalah standar yang digunakan untuk mengidentifikasi, mendefinisikan, dan melacak kerentanan keamanan informasi yang dikelola oleh MITRE Corporation.
Manjunatha, A., Kota, K., Babu, A. S., & Vivek, S. S. (2024). CVE severity prediction from vulnerability description - A deep learning approach. *Procedia Computer Science, 235*, 3105–3117.

Pada Contoh 2, dapat dilihat bahwa serangan siber memungkinkan terjadi diakibatkan oleh kerentanan pada rantai pasok dan ketergantungan pada pihak ketiga yang menyebabkan gangguan sistem. Pada contoh ini, terdapat variabel kejadian ancaman, aset, dan konsekuensi.

Contoh 2:

Kegagalan pembaruan perangkat lunak Falcon Sensor (CrowdStrike) menyebabkan terjadinya insiden Blue Screen On Dead pada jutaan PC dengan OS Windows di seluruh dunia yang berdampak pada terhentinya layanan vital seperti perbankan, penerbangan, dan layanan penting lainnya, akibat ketergantungan tinggi pada satu komponen keamanan tanpa mekanisme uji pembaruan dan rollback otomatis yang memadai.

Keterangan:

Kejadian Ancaman (*Threat Event*)

Kerentanan

Aset

Konsekuensi

Kasus tersebut menunjukkan bahwa kegagalan sistem dapat disebabkan oleh gangguan rantai pasok, yang juga menjadi titik lemah organisasi karena ketergantungan pada pihak ketiga dalam mendukung operasional bisnis.

B. Analisis Risiko Organisasi

Analisis risiko merupakan proses untuk menganalisis setiap elemen pada skenario risiko untuk menentukan kemungkinan terjadinya skenario dan dampak dari terjadinya skenario tersebut.

1. Menentukan Kemungkinan (*Likelihood*)

Secara umum, kemungkinan (*likelihood*) ditentukan dengan mempertimbangkan ancaman dan kerentanan, bukan berdasarkan data historis saja. Hal tersebut dikarenakan perkembangan ancaman keamanan

siber yang sangat cepat memungkinkan untuk terjadinya risiko yang belum pernah terjadi. Selain itu, dalam menentukan kemungkinan, beberapa faktor yang perlu diperhatikan antara lain:

a. ***Discoverability***, menggambarkan kemudahan bagi penyerang dalam menemukan kerentanan pada aset. Faktor yang memengaruhinya mencakup ketersediaan informasi mengenai aset dan kerentanannya. Ketersediaan informasi ini dapat tercermin pada peraturan atau regulasi yang menjelaskan kerentanan yang perlu dilindungi.
b. ***Exploitability***, menggambarkan sejauh mana suatu kerentanan pada aset dapat dieksploitasi dengan mudah. Faktor-faktor yang memengaruhi *exploitability* mencakup hak akses, kompleksitas alat yang dibutuhkan, dan keterampilan teknis yang diperlukan dalam melancarkan serangan.
c. ***Reproducibility***, menunjukkan seberapa mudah penyerang dapat mengulang serangan terhadap aset dalam suatu organisasi. Beberapa faktor yang memengaruhi tingkat *reproducibility* meliputi kompleksitas eksploitasi dan kondisi lingkungan yang mendukung pelaksanaan serangan.

Tabel 5 berikut dapat digunakan untuk menilai kemungkinan risiko keamanan siber berdasarkan faktor *discoverability*, *exploitability*, dan *reproducibility*. Penilaian dimulai dengan menetapkan skor untuk setiap faktor menggunakan skala 1 hingga 5. Total nilai yang diperoleh kemudian dibagi dan dirata-ratakan, sebelum kemudian dibulatkan. Nilai akhir yang dihasilkan menggambarkan tingkat kemungkinan dari suatu skenario risiko, dengan skala dari sangat kecil hingga sangat besar.

Tabel 5. Tingkat Kemungkinan

Tingkat Kemungkinan	*Discoverability*	*Exploitability*	*Reproducibility*
Kemungkinan Sangat Besar (5)	▪ Kerentanan dapat ditemukan dengan mencari/memindai *domain public*. ▪ Kerentanan dapat ditemukan dan diserang dari jaringan eksternal.	▪ Serangan dapat dilakukan tanpa hak akses dari target. ▪ Serangan dapat dilakukan dengan menggunakan *tools* yang tersedia untuk publik tanpa memerlukan pengetahuan teknis.	▪ Serangan dapat diulangi tanpa memerlukan konfigurasi tertentu ataupun suatu kondisi tertentu. ▪ Serangan dapat diulangi tanpa memerlukan penyesuaian apa pun terhadap metode/alat eksploitasi yang tersedia untuk publik.
Kemungkinan Besar (4)	▪ Kerentanan dapat ditemukan dengan menyelidiki target (contoh: *port scanning*). ▪ Kerentanan dapat ditemukan dan diserang dari *subnet* atau segmen jaringan yang berdekatan.	▪ Serangan dapat dilakukan dengan menggunakan hak akses terbatas dari target serangan. ▪ Serangan dapat dilakukan dengan menggunakan *tools* yang tersedia untuk publik dengan menggunakan pengetahuan teknis dasar.	▪ Serangan dapat diulangi dengan menggunakan konfigurasi tertentu pada target. ▪ Serangan dapat diulangi melalui penyesuaian minimal pada metode/alat eksploitasi yang tersedia untuk publik (misalnya, perubahan parameter).

Mungkin (3)	▪ Kerentanan dapat ditemukan dengan memeriksa respon target, perilaku, dan komunikasi (misalnya, *fuzzing* dengan paket jaringan, *sniffing* jaringan). ▪ Kerentanan dapat ditemukan dan diserang dari dalam subnet atau segmen jaringan yang sama.	▪ Serangan dapat dilakukan dengan menggunakan hak akses istimewa dari target. ▪ Serangan dapat dilakukan dengan menggunakan *tools* yang tersedia untuk umum yang memerlukan pengetahuan teknis moderat.	▪ Serangan dapat diulangi dengan kondisi kejadian tertentu yang dapat diprediksi ▪ Serangan dapat diulangi melalui penyesuaian khusus untuk target.
Kemungkinan Kecil (2)	▪ Kerentanan dapat ditemukan dengan mengoperasikan dan berinteraksi dengan pengaturan aktual atau serupa dari target. ▪ Kerentanan dapat ditemukan dan diserang dengan akses lokal logis.	▪ Serangan dapat dilakukan dengan menggunakan hak akses istimewa (contoh: admin/SISTEM/*root*). ▪ Serangan dapat dilakukan dengan alat yang tersedia untuk umum/khusus yang memerlukan pengetahuan teknis tingkat lanjut.	▪ Serangan dapat diulangi dengan kondisi kejadian acak tertentu. ▪ Serangan secara teori dan konsep dapat diulangi (berdasarkan pada bukti eksploitasi konsep yang telah dipublikasikan).

		▪ Serangan mungkin memerlukan rangkaian beberapa eksploitasi.	
Kemungkinan Sangat Kecil (1)	▪ Kerentanan dapat ditemukan dengan mempelajari cetak birunya (contoh: *source code*). ▪ Kerentanan dapat ditemukan dan diserang dengan akses fisik.	▪ Serangan dapat dilakukan dengan hak akses istimewa (misalnya, admin/*root*/SYSTEM) dan memerlukan otentikasi multifaktor. ▪ Serangan dapat dilakukan dengan alat khusus yang memerlukan pengetahuan teknis ahli. ▪ Serangan membutuhkan rangkaian beberapa eksploitasi.	▪ Serangan tidak dapat diperbanyak sesuai sasaran. ▪ Serangan dapat diulangi dengan eksploitasi spesifik terhadap target yang tidak dipublikasikan.

2. Menentukan Dampak (Impact)

Dampak risiko terhadap organisasi umumnya dapat dianalisis melalui tiga aspek utama: 1) kerahasiaan (*confidentiality*), 2) integritas (*integrity*), dan 3) ketersediaan (*availability*), atas aset yang dikelola, terutama terkait data, informasi, peralatan, dan operasi. Analisis ini mencakup tiga tingkatan: nasional, organisasi, dan individu.

Pada tingkat nasional, risiko dapat memengaruhi keamanan, kepentingan umum, dan perekonomian. Di tingkat organisasi, dampak risiko terlihat dari gangguan operasional, kerusakan reputasi, dan kerugian finansial. Sementara pada tingkat individu, dampaknya dapat berupa hilangnya nyawa atau cedera.

Untuk menyesuaikan analisis dengan kebutuhan spesifik, organisasi perlu menggunakan kriteria yang lebih jelas dan tidak ambigu, sesuai dengan konteks bisnis yang bersifat multiperspektif. Kriteria yang tidak ambigu mencakup rentang kuantitatif yang terukur, sementara kriteria sesuai konteks bisnis terkait dengan tujuan dan kinerja organisasi. Selain itu, kriteria multiperspektif mencakup identifikasi subkategori dampak di tingkat nasional, organisasi, dan individu.

Tabel 6 menampilkan contoh penilaian dampak risiko menggunakan skala dari 1 hingga 5, yang berkisar antara sangat minor hingga sangat berat. Setiap skenario risiko dapat memiliki peringkat dampak yang berbeda dalam hal kerahasiaan, integritas, dan ketersediaan. Nilai akhir ditentukan berdasarkan peringkat dampak tertinggi yang diperoleh.

Tabel 6. Tingkat Dampak

Tingkat Dampak	Kerahasiaan	Integritas	Ketersediaan
Sangat Berat (5)	Pengungkapan informasi yang tidak sah dapat menimbulkan dampak buruk yang sangat besar terhadap organisasi, individu, atau negara.	Modifikasi atau penghancuran informasi yang tidak sah dapat menimbulkan dampak buruk yang sangat serius terhadap organisasi, individu, atau negara.	Gangguan terhadap akses atau penggunaan informasi atau sistem komputer diperkirakan akan menimbulkan dampak buruk yang sangat serius terhadap organisasi, individu, atau negara.
Berat (4)	Pengungkapan informasi yang tidak sah dapat menimbulkan dampak buruk yang serius terhadap organisasi, individu, atau negara.	Modifikasi atau penghancuran informasi yang tidak sah dapat menimbulkan dampak buruk yang serius terhadap organisasi, individu, atau negara.	Gangguan terhadap akses atau penggunaan informasi atau sistem komputer diperkirakan akan menimbulkan dampak buruk yang serius terhadap organisasi, individu, atau negara.
Sedang (3)	Pengungkapan informasi yang tidak sah diperkirakan akan menimbulkan dampak buruk terhadap organisasi, individu, atau negara.	Modifikasi atau penghancuran informasi yang tidak sah diperkirakan akan menimbulkan dampak buruk terhadap organisasi, individu, atau negara.	Gangguan terhadap akses atau penggunaan informasi atau sistem komputer diperkirakan akan menimbulkan dampak buruk terhadap organisasi, individu, atau negara.

Minor (2)	Pengungkapan informasi yang tidak sah diperkirakan mempunyai dampak merugikan yang terbatas terhadap organisasi, atau individu.	Modifikasi atau pemusnahan informasi yang tidak sah diperkirakan akan mempunyai dampak merugikan yang terbatas terhadap organisasi, atau individu.	Gangguan terhadap akses atau penggunaan informasi atau sistem komputer diperkirakan mempunyai dampak merugikan yang terbatas terhadap organisasi, atau individu.
Sangat Minor (1)	Pengungkapan informasi yang tidak sah diperkirakan akan berdampak kecil terhadap organisasi atau individu.	Modifikasi atau penghancuran informasi yang tidak sah diperkirakan akan berdampak kecil terhadap organisasi, atau individu.	Gangguan terhadap akses atau penggunaan informasi atau sistem komputer diperkirakan mempunyai dampak yang dapat diabaikan terhadap organisasi, atau individu.

C. Evaluasi Risiko Organisasi

Evaluasi risiko merupakan proses untuk menentukan dan memahami pentingnya tingkat risiko. Secara umum, evaluasi risiko terdiri atas penentuan risiko dan prioritas risiko dan dokumentasi risiko.

1. Penentuan Risiko dan Prioritas Risiko

Penentuan risiko dan prioritas risiko dijelaskan melalui diagram matriks risiko. Matriks risiko 5x5 digunakan untuk menentukan tingkat risiko pada setiap skenario. Matriks ini didasarkan pada fungsi dampak yang dikalikan dengan kemungkinan, sebagaimana diuraikan dalam definisi risiko. Contoh matriks 5x5 dapat dilihat pada Tabel 7.

Tabel 7. Penentuan Prioritasi Risiko (sumber: National Cyber Risk Assessment Toolkit)

Impact	**5 - Sangat Besar**	5 - Cenderung Rendah (Moderate Low)	10 - Tinggi (High)	15 - Tinggi (High)	20 - Sangat Tinggi (Very High)	25 - Sangat Tinggi (Very High)
	4 - Besar	4 - Cenderung Rendah (Moderate Low)	8 - Cenderung Tinggi (Moderate High)	12 - Tinggi (High)	16 - Tinggi (High)	20 - Sangat Tinggi (Very High)
	3 - Sedang	3 - Rendah (Low)	6 - Cenderung Tinggi (Moderate High)	9 - Cenderung Tinggi (Moderate High)	12 - Tinggi (High)	15 - Tinggi (High)
	2 - Kecil	2 - Rendah (Low)	4 - Cenderung Rendah (Moderate Low)	6 - Cenderung Tinggi (Moderate High)	8. Cenderung Tinggi (Moderate High)	10 - Tinggi (High)
	1 - Sangat Kecil	1 - Rendah (Low)	2 - Rendah (Low)	3 - Rendah (Low)	4 - Cenderung Rendah (Moderate Low)	5 - Cenderung Rendah (Moderate Low)
		1 - Langka	**2 - Kecil Kemungkinan**	**3 - Mungkin Terjadi**	**4 - Dapat Terjadi**	**5 - Hampir Pasti Terjadi**
		***Likelihood* (Kemungkinan Terjadinya Kejadian yang Berakibat Buruk)**				

Hasil tingkat risiko organisasi yang diperoleh dari matriks ini dapat dibandingkan dengan tingkat toleransi risiko yang telah diukur sebelumnya. Skenario risiko dengan nilai tertinggi berdasarkan matriks ini perlu diprioritaskan untuk penanganan.

2. Dokumentasi Risiko

Tahapan terakhir yang perlu dilakukan oleh organisasi adalah dokumentasi risiko, yang mencakup pengumpulan langkah-langkah yang telah dilaksanakan sebelumnya. Dokumentasi ini penting agar para pemangku kepentingan dapat memahami informasi mengenai penilaian risiko yang telah dilakukan dalam organisasi.

Proses sebelumnya, termasuk skenario risiko dan tingkatannya, dapat disusun dalam bentuk daftar risiko (*risk register*). Daftar risiko berfungsi sebagai dokumen hidup (*living document*) yang perlu ditinjau dan diperbarui secara berkala. Pembaruan ini bertujuan memastikan bahwa daftar risiko mencerminkan kondisi terkini terkait risiko keamanan siber organisasi.

Daftar risiko harus mencakup beberapa elemen penting, seperti skenario risiko, tanggal identifikasi risiko, langkah-langkah yang telah

diterapkan untuk mengatasi risiko, status risiko saat ini, rencana penanganan risiko, kemajuan penerapan penanganan risiko, risiko sisa (*residual risk*), dan pemilik risiko. Berikut adalah definisi dari masing-masing elemen yang termasuk dalam daftar risiko tersebut:

1) Skenario risiko, merupakan skenario yang menjelaskan bagaimana peristiwa ancaman dapat mengeksploitasi potensi kerentanan suatu aset untuk menciptakan dampak buruk.
2) Tanggal identifikasi, merupakan tanggal ketika skenario risiko diidentifikasi.
3) Langkah-langkah yang telah ada, merupakan langkah-langkah yang ada saat ini untuk mengatasi skenario risiko.
4) Risiko saat ini, merupakan tingkat risiko yang ditentukan (kombinasi kemungkinan dan dampak) dari skenario risiko setelah memperhitungkan langkah-langkah yang ada (yaitu risiko bawaan dengan langkah-langkah yang ada diterapkan).
5) Rencana penanganan risiko, merupakan kegiatan yang direncanakan (misalnya, penerapan tindakan tambahan) dan jangka waktu untuk menangani risiko saat ini hingga tingkat yang dapat diterima (yaitu dalam tingkat toleransi risiko organisasi).
6) Kemajuan (*progress*) penerapan penanganan risiko, merupakan status penerapan rencana penanganan risiko yang telah dilaksanakan.
7) Risiko sisa (*residual risk*), merupakan tingkat risiko yang ditentukan dengan kombinasi kemungkinan dan dampak dari skenario risiko setelah rencana penanganan risiko diterapkan.
8) Pemilik risiko, merupakan individu atau tim yang bertanggung jawab untuk memastikan bahwa risiko yang tersisa tetap berada dalam tingkat toleransi organisasi.

D. Respon Terhadap Risiko

Setelah mengidentifikasi setiap risiko yang ada, respons yang tepat diperlukan untuk menghadapi risiko tersebut. Terdapat empat pilihan respons yang dapat diambil oleh pihak terkait, yaitu menerima risiko (*accept*), menghindari risiko (*avoid*), memindahkan risiko (*transfer*), dan memitigasi

risiko (*mitigation*). Berikut adalah definisi dan contoh dari masing-masing respons terhadap risiko tersebut.

1. **Menerima Risiko (*accept*)**, dapat diartikan sebagai menerima risiko apa adanya tanpa mengambil langkah lebih lanjut untuk mengurangi risiko tersebut. Perlu diingat bahwa menerima risiko hanya boleh dipilih jika risiko tersebut telah berada dalam tingkat toleransi risiko organisasi.
2. **Menghindari risiko (*avoid*)**, dapat diartikan sebagai menghentikan tindakan/aktivitas yang memaparkan organisasi pada risiko yang teridentifikasi. Hal ini mungkin tampak ekstrem, namun mungkin merupakan tindakan terbaik jika risikonya lebih besar daripada manfaatnya. Contoh dari menghindari risiko adalah tidak mengoperasikan suatu sistem operasi untuk menghindari risiko serangan terhadap sistem operasi tersebut.
3. **Memindahkan risiko (*transfer*)**, dapat diartikan sebagai membagi sebagian risiko kepada pihak atau entitas lain. Pemindahan risiko ini dilakukan untuk mengurangi dampak dari suatu risiko. Contoh dari memindahkan risiko seperti mengasuransikan aset yang ada.
4. **Memitigasi risiko (*mitigation*)**, dapat diartikan sebagai menerapkan langkah-langkah untuk mengurangi tingkat risiko. Mitigasi risiko dapat dilakukan melalui penerapan kontrol-kontrol keamanan. Contoh dari mitigasi risiko adalah memasang *firewall* untuk mengurangi risiko ancaman dari luar sistem. Hal yang perlu diingat dalam memitigasi risiko adalah memastikan kontrol keamanan yang diambil relevan dengan risiko yang berusaha ditanggulangi.

PELAPORAN MANAJEMEN RISIKO

BAB V
PELAPORAN MANAJEMEN RISIKO

Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (IIV) mengatur manajemen risiko keamanan siber pada Pasal 10. Setiap Penyelenggara IIV diwajibkan menerapkan manajemen risiko keamanan siber secara efektif. Persyaratan yang harus dipenuhi dalam penerapan manajemen risiko keamanan siber mencakup:

a) **Kepatuhan terhadap peraturan perundang-undangan**: Manajemen risiko harus mematuhi aturan hukum yang berlaku.
b) **Kesesuaian dengan standar sektor IIV**: Manajemen risiko harus sesuai dengan standar keamanan yang berlaku di sektor IIV masing-masing.
c) Sistem pengendalian internal: Penyelenggara IIV harus memiliki sistem pengendalian internal yang sesuai untuk mengelola risiko keamanan siber.

Mekanisme pelaporan manajemen risiko merupakan proses sistematis yang dirancang guna memantau, menganalisis, dan melaporkan berbagai risiko yang dihadapi. Berikut adalah penjelasan mengenai mekanisme pelaporan manajemen risiko.

A. Pelaporan Penyelenggara IIV

Merujuk pada Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan IIV, Penyelenggara IIV diwajibkan melaporkan hasil penerapan manajemen risiko keamanan siber kepada Kementerian atau Lembaga di sektornya. Apabila Kementerian atau Lembaga tersebut juga berperan sebagai Penyelenggara IIV, mekanisme pelaporan manajemen risiko dilakukan secara berjenjang sebagai berikut:

1. **Pelaporan Penyelenggara IIV**
    a) Penyelenggara IIV melakukan penilaian risiko keamanan siber secara mandiri minimal satu kali dalam setahun dengan menggunakan ***Toolkit Penilaian Risiko Keamanan Siber***.
    b) Penilaian risiko keamanan siber meliputi identifikasi, analisis, dan evaluasi risiko terhadap Sistem Elektronik yang dimiliki dan/atau dikelola. Pada proses ini Penyelenggara IIV juga menentukan kemungkinan dan dampak dari risiko yang teridentifikasi.

c) Penyelenggara IIV mendokumentasikan hasil penilaian risiko keamanan siber dalam bentuk laporan penilaian risiko keamanan siber, yang paling sedikit berisi:
   i. deskripsi risiko utama yang dihadapi oleh organisasi;
   ii. tingkat atau level risiko (misalnya, rendah, sedang, tinggi, atau kritis);
   iii. tindakan mitigasi yang diterapkan atau direncanakan;
   iv. hasil evaluasi efektivitas pengendalian risiko yang teridentifikasi.

2. **Pelaporan Hasil Penilaian Risiko kepada Kementerian atau Lembaga**

a) Laporan hasil penilaian risiko yang telah disusun oleh Penyelenggara IIV disampaikan kepada Kementerian atau Lembaga yang mengawasi sektor terkait. Dalam hal Kementerian atau Lembaga berperan sebagai Penyelenggara IIV, Kementerian atau Lembaga harus melaporkan hasil penerapan manajemen risiko keamanan siber kepada Badan Siber dan Sandi Negara (BSSN).

b) Kementerian atau Lembaga melakukan verifikasi terhadap laporan yang diterima guna memastikan kesesuaian dengan ketentuan yang berlaku serta memeriksa kualitas informasi yang disampaikan. Penyelenggara IIV diperiksa efektivitas penerapan manajemen risikonya melalui pengawasan dan pemeriksaan data dukung yang diberikan. Tabel 8 menyajikan beberapa kriteria pengawasan atau pemeriksaan laporan manajemen risiko yang dapat dipertimbangkan.

Tabel 8. Kriteria Pengawasan atau Pemeriksaan Laporan Manajemen Risiko

No	Kriteria	Deskripsi	Kriteria Efektivitas	Bukti Data Dukung
1	**Kebijakan dan Prosedur Manajemen Risiko**	Pemeriksaan terhadap keberadaan dan kelengkapan kebijakan, prosedur,	Kebijakan terdokumentasi, mutakhir, dan	Dokumen kebijakan, prosedur, pedoman

No	Kriteria	Deskripsi	Kriteria Efektivitas	Bukti Data Dukung
		dan pedoman manajemen risiko keamanan siber.	selaras dengan standar.	manajemen risiko.
2	**Identifikasi dan Analisis Risiko**	Evaluasi proses identifikasi dan analisis risiko yang dilakukan oleh Penyelenggara IIV.	Risiko diidentifikasi secara komprehensif dan dianalisis dengan benar.	Daftar risiko teridentifikasi, analisis risiko, laporan penilaian risiko.
3	**Penilaian Risiko**	Pemeriksaan penilaian risiko berdasarkan probabilitas dan dampak serta penentuan tingkat risiko.	Penilaian risiko konsisten dan didukung oleh data relevan.	Matriks risiko, laporan penilaian risiko, dokumentasi penilaian (*scoring*) risiko.
4	**Rencana Mitigasi Risiko**	Pemeriksaan rencana tindakan mitigasi untuk mengurangi dampak atau kemungkinan terjadinya risiko.	Rencana mitigasi jelas, relevan, dan dilaksanakan sesuai jadwal.	Rencana mitigasi, laporan kemajuan (*progress*) mitigasi, bukti implementasi tindakan.
5	**Implementasi Pengendalian**	Verifikasi implementasi pengendalian risiko, termasuk kontrol teknis dan operasional yang diterapkan.	Pengendalian diterapkan dengan benar dan teruji efektivitasnya.	Catatan implementasi kontrol, hasil pengujian kontrol, audit kontrol.

No	Kriteria	Deskripsi	Kriteria Efektivitas	Bukti Data Dukung
6	***Monitoring* dan *Review* Risiko**	Pemeriksaan terhadap kegiatan pemantauan dan tinjauan berkala risiko yang dilakukan untuk memastikan risiko tetap dikelola.	*Monitoring* dan *review* dilakukan rutin dan hasilnya terdokumentasi.	Laporan *monitoring*, hasil *review*, log pemantauan risiko.
7	**Komunikasi dan Pelaporan Risiko**	Evaluasi efektivitas komunikasi risiko internal dan eksternal serta kepatuhan terhadap prosedur pelaporan risiko kepada Kementerian/Lembaga.	Pelaporan tepat waktu, lengkap, dan disampaikan kepada pihak yang berwenang.	Laporan komunikasi risiko, bukti pengiriman laporan ke pihak berwenang.
8	**Program Peningkatan Kesadaran Keamanan Siber dan Pelatihan**	Pemeriksaan program peningkatan kesadaran dan pelatihan keamanan siber bagi staf Penyelenggara IIV.	Program pelatihan rutin dan diikuti oleh seluruh staf terkait.	Jadwal pelatihan, daftar hadir peserta, materi pelatihan, sertifikat pelatihan.
9	**Penilaian Kematangan Manajemen Risiko**	Verifikasi terhadap pengukuran tingkat kematangan manajemen risiko keamanan siber yang dilakukan secara mandiri oleh Penyelenggara IIV.	Penilaian kematangan dilakukan setidaknya satu kali setahun.	Laporan penilaian kematangan, hasil evaluasi kematangan, rekomendasi peningkatan.

No	Kriteria	Deskripsi	Kriteria Efektivitas	Bukti Data Dukung
10	**Pemeriksaan Kepatuhan**	Evaluasi kepatuhan terhadap peraturan perundang-undangan dan standar yang berlaku, termasuk audit eksternal jika ada.	Tingkat kepatuhan tinggi dan tidak ada temuan mayor dari audit.	Laporan audit, bukti kepatuhan, catatan tindakan korektif atas temuan audit.
11	**Efektivitas Tindakan Korektif**	Pemeriksaan terhadap tindakan korektif yang diambil setelah terjadinya insiden siber atau audit, serta efektivitas tindakan tersebut.	Tindakan korektif sesuai rencana dan menyelesaikan isu yang ada.	Laporan tindakan korektif, bukti implementasi, evaluasi efektivitas tindakan.
12	**Penggunaan Teknologi Keamanan**	Evaluasi penerapan teknologi keamanan siber, termasuk perangkat lunak dan perangkat keras yang digunakan untuk mitigasi risiko.	Teknologi keamanan sesuai standar dan dioperasikan dengan baik.	Daftar teknologi keamanan, laporan implementasi, hasil pengujian teknologi.
13	**Kolaborasi dan Koordinasi**	Pemeriksaan kolaborasi dengan Tim Tanggap Insiden Siber sektoral dan nasional serta pihak terkait lainnya dalam penanganan risiko dan insiden.	Kolaborasi aktif dan dokumentasi koordinasi tersedia.	Bukti rapat koordinasi, laporan kolaborasi, komunikasi dengan Tim Tanggap Insiden Siber sektoral

No	Kriteria	Deskripsi	Kriteria Efektivitas	Bukti Data Dukung
				dan/atau nasional.

B. Penyampaian Ringkasan Risiko Sektoral kepada BSSN

Salah satu tugas BSSN sebagai Koordinator Pelindungan Infrastruktur Informasi Vital (IIV) sesuai dengan Perpres No. 82 Tahun 2022 adalah mengevaluasi implementasi kebijakan pelindungan IIV. Dalam evaluasi, terutama terkait penerapan manajemen risiko keamanan siber pada sektor IIV, BSSN memerlukan gambaran lengkap tentang penerapan manajemen risiko di tingkat sektor. Selain itu, BSSN diamanatkan untuk melaporkan penyelenggaraan pelindungan IIV setiap tahun kepada Presiden. Ringkasan profil risiko sektoral menjadi bahan bagi BSSN dalam menyusun Profil Risiko Keamanan Siber Nasional. Berikut adalah mekanisme penyampaian ringkasan risiko sektoral kepada BSSN:

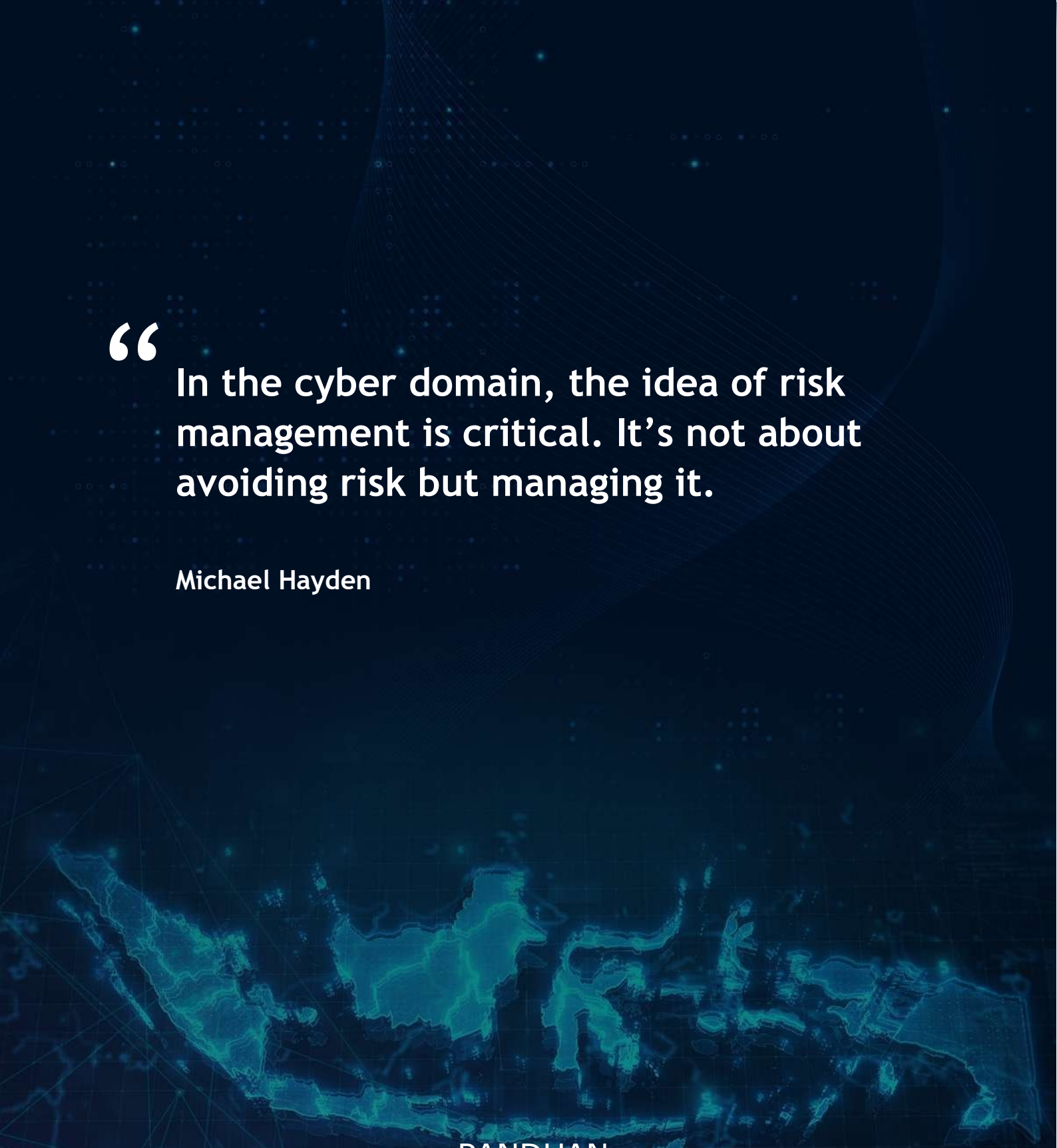
a. Kementerian atau Lembaga menyusun ringkasan risiko sektoral berdasarkan laporan-laporan yang diterima oleh Penyelenggara IIV. Ringkasan ini paling sedikit berisi:
   a) tren risiko keamanan siber sektoral,
   b) kesenjangan pengendalian risiko, dan
   c) rekomendasi peningkatan keamanan siber pada lingkup sektor.
b. Ringkasan Risiko Sektoral disampaikan oleh Kementerian/Lembaga kepada BSSN secara periodik.
c. Ringkasan ini harus sesuai dengan format yang ditetapkan oleh BSSN untuk memudahkan kompilasi di tingkat nasional.
d. Mekanisme pelaporan dievaluasi secara berkala untuk memastikan efektivitas dan kesesuaiannya dengan perkembangan ancaman siber.
e. Jika diperlukan, mekanisme pelaporan diperbarui dan disesuaikan dengan kebutuhan baru yang muncul.
f. Untuk memfasilitasi pelaporan yang efisien, Kementerian/Lembaga dan BSSN dapat mengembangkan sistem pelaporan elektronik yang aman dan dapat diakses oleh Penyelenggara IIV.

g. Pelatihan bagi Penyelenggara IIV dan Kementerian/Lembaga mengenai prosedur pelaporan dan standar penilaian risiko diperlukan untuk memastikan pemahaman dan kepatuhan.

REFERENSI

1. *Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure*. (February 2021). Cybersecurity Agency of Singapore.
2. Kominfo. (n.d.). 10 Sektor Prioritas untuk Memacu Transformasi Digital. Diakses pada 30 Oktober 2024, dari https://www.kominfo.go.id/content/detail/36895/10-sektor-prioritas-untuk-memacu-transformasi-digital/0/artikel
3. United Nations. (2015). Sendai Framework for Disaster Risk Reduction 2015-2030. United Nations.
4. Fortinet. (n.d.). SolarWinds Cyber Attack. Diakses pada 30 Oktober 2024, dari https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack
5. Warren, T. (2024, July 24). CrowdStrike Test Software Bug Causes Windows BSOD Issue. The Verge. Diakses pada 30 Oktober 2024, dari https://www.theverge.com/2024/7/24/24205020/crowdstrike-test-software-bug-windows-bsod-issue
6. Palleti, V., Adepu, S., Mishra, V., et al. (2021). Cascading effects of cyber-attacks on interconnected critical infrastructure. Cybersecurity, 4(8). https://doi.org/10.1186/s42400-021-00071-z
7. Pescaroli, G., Turner, S., Gould, T., Alexander, D., & Wicks, R. (2017). Cascading Effects and Escalations in Wide Area Power Failures: A Summary for Emergency Planners.
8. Schauer, S., Grafenauer, T., König, S., Warum, M., & Rass, S. (2019). Estimating cascading effects in Cyber-Physical critical infrastructures. Lecture Notes in Computer Science, 43–56. https://doi.org/10.1007/978-3-030-37670-3_4
9. Manjunatha, A., Kota, K., Babu, A. S., & Vivek, S. S. (2024). CVE severity prediction from vulnerability description - A deep learning approach. *Procedia Computer Science, 235*, 3105–3117. https://doi.org/10.1016/j.procs.2024.04.294

> In the cyber domain, the idea of risk management is critical. It’s not about avoiding risk but managing it.
>
> Michael Hayden



PANDUAN MANAJEMEN RISIKO KEAMANAN SIBER

2024

BADAN SIBER DAN SANDI NEGARA