Kerangka Kerja untuk Meningkatkan Keamanan Siber Infrastruktur Kritis

Versi 1.1

National Institute of Standards and Technology

16 April 2018

Diterjemahkan oleh:
Dr. Baskoro Adi Pratomo
Awaludin Marwan, PhD
Ir. Satriyo Wibowo, ST, MBA, MH, IPM, CERG, CCISO, CBP, CSA, ECIH
Mustasyfa Thabib Kariadi, S.Pd.,M.Pd
Siti Faridah, S.H

Catatan untuk Pembaca dalam Pemutakhiran

Versi 1.1 Kerangka Kerja Keamanan Siber ini menyempurnakan, mengklarifikasi, dan memperbaiki Versi 1.0, yang diterbitkan bulan Februari 2014. Versi ini memuat komentar yang diterima atas dua draf Versi 1.1.

Versi 1.1 ditujukan untuk dilaksanakan oleh pengguna Kerangka Kerja baru dan lama. Pengguna saat ini seharusnya mampu melaksanakan Versi 1.1 dengan minimal atau tanpa halangan; kompatibilitas dengan Versi 1.0 menjadi tujuan eksplisit.

Tabel Berikut ini meringkas perubahan-perubahan yang dilakukan antara Versi 1.0 dan Versi 1.1.

Tabel NTR-1 - Ringkasan perubahan antara Kerangka Kerja Versi 1.0 dan Versi 1.1.

Pemutakhiran	Uraian Pemutakhiran
Mengklarifikasi bahwa istilah seperti "kepatuhan" bisa membingungkan dan berarti sesuatu yang sangat berbeda bagi berbagai pemangku kepentingan Kerangka Kerja	Menambah kejelasan bahwa Kerangka Kerja bermanfaat sebagai struktur dan bahasa untuk pengaturan dan menyatakan kepatuhan terhadap persyaratan keamanan siber organisasi sendiri. Namun, berbagai cara dapat digunakannya Kerangka Kerja oleh organisasi berarti bahwa frasa seperti "kepatuhan terhadap Kerangka Kerja" bisa membingungkan.
Bagian baru pada pengujian mandiri	Bagian 4.0 *Risiko Keamanan Siber Penilaian Diri dengan Kerangka Kerja* ditambahkan untuk menjelaskan bagaimana Kerangka Kerja dapat digunakan organisasi untuk memahami dan menilai risiko keamanan sibernya, termasuk penggunaan pengukuran.
Penjelasan yang sangat luas mengenai penggunaan Kerangka Kerja untuk tujuan Manajemen Risiko Rantai Pasokan Siber	Bagian 3.3 *Mengomunikasikan Persyaratan Keamanan Siber dengan Pemangku Kepentingan* dikembangkan untuk membantu pengguna memahami Manajemen Risiko Rantai Pasokan Siber (MRRP) lebih baik lagi, sementara Bagian baru 3.4 Keputusan Membeli menyoroti penggunaan Kerangka Kerja dalam memahami risiko yang berkaitan dengan produk dan layanan komersial siap pakai. Tambahan kriteria MRRP Siber ditambahkan pada level Pelaksanaan. Akhirnya, sebuah Kategori Manajemen Risiko Rantai Pasokan, termasuk beberapa Sub Kategori, telah ditambahkan pada Inti Kerangka Kerja.
Penyempurnaan keterangan yang lebih baik untuk otentikasi, otorisasi, dan pembuktian identitas	Penjelasan Kategori Kendali Akses telah disempurnakan untuk menjelaskan otentikasi, otorisasi, dan pembuktian identitas lebih baik lagi. Hal ini meliputi penambahan satu Sub Kategori masing-masing untuk Otentikasi dan Pembuktian Identitas. Selain itu, Kategori diubah menjadi Manajemen Identitas dan Kendali Akses (PR.AC) agar merepresentasikan ruang lingkup Kategori dan Sub Kategori terkait lebih baik lagi.

Penjelasan yang lebih baik tentang hubungan antara level dan Profil Implementasi	Tambahan penjelasan pada Bagian 3.2 *Penetapan atau Peningkatan Program Keamanan Siber* pada penggunaan level Kerangka Kerja dalam pelaksanaan Kerangka Kerja ini. Tambahan bahasa pada level Kerangka Kerja agar mencerminkan dimasukkannya pertimbangan Kerangka Kerja dalam program manajemen risiko organisasi. Konsep level Kerangka Kerja juga disempurnakan. Gambar 2.0 dimutakhirkan untuk mencakup tindakan dari level Kerangka Kerja.
Pertimbangan Pengungkapan Kerentanan Terkoordinasi	Ditambahkan sebuah Sub Kategori yang terkait dengan siklus hidup pengungkapan kerentanan.

Sama seperti Versi 1.0, pengguna Versi 1.1 didorong untuk melakukan kustomisasi Kerangka Kerja untuk memaksimalkan nilai organisasi.

Ucapan Terima Kasih

Publikasi ini merupakan hasil upaya kolaboratif berkelanjutan yang melibatkan industri, akademisi, dan pemerintah. *National Institute of Standards and Technology* (NIST) meluncurkan proyek ini setelah bersepakat dengan individu dan organisasi sektor swasta dan publik pada tahun 2013. Dipublikasikan tahun 2014 dan direvisi tahun 2017 dan 2018, Kerangka Kerja untuk meningkatkan Keamanan Siber Infrastruktur Kritis ini bergantung pada delapan lokakarya publik, beberapa Permintaan Komentar atau Informasi, dan ribuan interaksi langsung dengan para pemangku kepentingan dari seluruh sektor di Amerika Serikat bersama dengan banyak sektor di seluruh dunia.

Dorongan untuk mengubah Versi 1.0 dan perubahan-perubahan yang muncul pada Versi 1.1 ini didasarkan pada:

- Umpan balik dan pertanyaan yang sering muncul untuk NIST sejak terbitnya Kerangka Kerja Versi 1.0;
- 105 respons atas permintaan informasi (RFI) Desember 2015, Pandangan Mengenai Kerangka Kerja untuk Peningkatan Keamanan Siber Infrastruktur Kritis;
- Lebih dari 85 komentar pada tanggal 5 Desember 2017 mengusulkan draf kedua Versi 1.1;
- Lebih dari 120 komentar pada tanggal 10 Januari 2017, mengusulkan draf pertama Versi 1.1; dan
- Masukan dari lebih dari 1.200 orang yang hadir pada lokakarya Kerangka Kerja tahun 2016 dan 2017.

Selain itu, NIST sebelumnya merilis Versi 1.0 Kerangka Kerja Keamanan Siber dengan dokumen penyerta, Peta Jalur NIST untuk Peningkatan Keamanan Siber Infrastruktur Kritis. Peta Jalur ini menyoroti “area peningkatan” kunci untuk perkembangan, penyelarasan, dan kolaborasi lebih lanjut. Melalui upaya sektor swasta dan publik, beberapa area peningkatan sudah cukup maju untuk dimasukkan ke dalam Kerangka Kerja Versi 1.1 ini.

NIST mengakui dan mengucapkan terima kasih kepada semua yang telah memberikan kontribusi untuk Kerangka Kerja ini.

Ringkasan Eksekutif

Amerika Serikat bergantung pada berfungsinya Infrastruktur Kritis yang andal. Ancaman Keamanan Siber mengeksploitasi meningkatnya kompleksitas dan konektivitas sistem Infrastruktur Kritis, yang menyebabkan keamanan, ekonomi, dan keselamatan serta kesehatan publik berisiko. Mirip dengan risiko keuangan dan reputasi, risiko keamanan siber berpengaruh pada pendapatan bersih perusahaan. Risiko ini dapat menaikkan biaya dan mempengaruhi pendapatan. Juga dapat membahayakan kemampuan organisasi untuk berinovasi dan mendapatkan serta mempertahankan pelanggan. Keamanan Siber dapat menjadi komponen penting dan yang memperkuat seluruh manajemen risiko organisasi.

Untuk mengatasi risiko-risiko ini dengan lebih baik, Undang-Undang Peningkatan Keamanan Siber Tahun 2014[1] (CEA) memperbarui peran *National Institute of Standards and Technology* (NIST) untuk memasukkan kerangka kerja identifikasi dan pengembangan risiko keamanan siber dari pemilik dan operator Infrastruktur Kritis secara sukarela. Melalui CEA, NIST harus mengidentifikasi "pendekatan berdasarkan prioritas, fleksibilitas, keberulangan, berbasis kinerja, dan tepat biaya, termasuk tindakan dan kendali keamanan informasi yang dapat diadopsi secara sukarela oleh pemilik dan operator Infrastruktur Kritis untuk membantu mereka mengidentifikasi, menilai, dan mengelola risiko siber." Hal ini dirumuskan dalam pekerjaan NIST sebelumnya dalam mengembangkan Kerangka Kerja Versi 1.0 berdasarkan Perintah Eksekutif (EO) 13636, "Meningkatkan Keamanan Siber Infrastruktur Kritis" (Februari 2013), dan memberikan panduan untuk evolusi Kerangka Kerja mendatang. Kerangka Kerja yang dikembangkan berdasarkan EO 13636, dan terus berkembang sesuai dengan CEA, menggunakan bahasa umum untuk mengatasi dan mengelola risiko keamanan siber secara tepat biaya berdasarkan kebutuhan bisnis dan organisasi tanpa menempatkan persyaratan regulasi tambahan pada bisnis.

Kerangka Kerja ini berfokus pada pengembangan bisnis untuk memandu kegiatan keamanan siber dan pertimbangan risiko keamanan siber sebagai bagian dari proses manajemen risiko organisasi. Kerangka Kerja terdiri dari tiga bagian: Inti Kerangka Kerja, level Pelaksanaan, dan Profil Kerangka Kerja. Inti Kerangka Kerja merupakan serangkaian kegiatan, hasil dan referensi informasi keamanan siber yang sudah umum antar sektor dan Infrastruktur Kritis. Unsur Inti memberikan panduan terperinci untuk pengembangan Profil organisasi individu. Melalui penggunaan Profil, Kerangka Kerja akan membantu organisasi menyelaraskan dan memprioritaskan kegiatan keamanan sibernya dengan persyaratan bisnis/misi, toleransi risiko, dan sumber dayanya. level Pelaksanaan memberikan mekanisme bagi organisasi untuk melihat dan memahami karakteristik pendekatannya terhadap pengelolaan risiko keamanan siber, yang akan membantu dalam memprioritaskan dan mencapai tujuan keamanan siber.

Meskipun dokumen ini dikembangkan untuk meningkatkan manajemen risiko keamanan siber pada Infrastruktur Kritis, Kerangka Kerja dapat digunakan oleh organisasi di sektor atau komunitas manapun. Kerangka Kerja memungkinkan organisasi - terlepas dari ukuran, derajat risiko keamanan siber, atau kecanggihan keamanan siber - untuk menerapkan prinsip dan praktik terbaik manajemen risiko pada peningkatan keamanan dan ketahanan.

Kerangka Kerja menyediakan struktur pengorganisasian umum untuk beberapa pendekatan keamanan siber dengan menyusun standar, pedoman, dan praktik yang dapat berjalan efektif saat ini. Terlebih lagi, karena Kerangka Kerja ini mengacu kepada standar keamanan siber yang diakui secara global, Kerangka Kerja ini dapat berfungsi sebagai model untuk kerja sama internasional untuk memperkuat keamanan siber dalam Infrastruktur Kritis serta sektor dan komunitas lainnya.

---

[1] *Lihat* 15 U.S.C. § 272(e)(1)(A)(i). Undang-undang Peningkatan Keamanan Siber Tahun 2014 (S.1353) menjadi hukum umum 113-274 pada tanggal 18 Desember 2014 dan dapat ditemukan di: https://www.congress.gov/bill/113th-congress/senatebill/1353/text.

Kerangka Kerja ini menawarkan cara yang fleksibel untuk mengatasi keamanan siber, termasuk efek keamanan siber pada dimensi fisik, siber, dan personil. Kerangka Kerja ini dapat diterapkan pada organisasi yang mengandalkan teknologi, baik fokus keamanan sibernya pada teknologi informasi (IT), sistem kendali industri (ICS), sistem siber-ke-fisik (CPS), atau perangkat terhubung yang lebih umum, termasuk Internet untuk Segala (IoT). Kerangka Kerja dapat membantu organisasi mengatasi keamanan siber karena berpengaruh pada privasi pelanggan, karyawan, dan pihak lain. Selain itu, hasil Kerangka Kerja berfungsi sebagai target untuk kegiatan pengembangan dan evolusi tenaga kerja.

Kerangka Kerja ini bukan pendekatan (cara satu untuk semua untuk pengelolaan risiko keamanan siber untuk Infrastruktur Kritis. Organisasi akan selalu memiliki risiko unik - ancaman yang berbeda, kerentanan yang berbeda, toleransi risiko yang berbeda. Organisasi juga bervariasi caranya untuk menyesuaikan praktik yang diuraikan dalam Kerangka Kerja. Organisasi dapat menentukan kegiatan yang penting bagi pemberian layanan kritis dan dapat memprioritaskan investasi untuk memaksimalkan dampak setiap dolar yang dihabiskan. Akhirnya, Kerangka Kerja ini ditujukan untuk mengurangi dan mengelola risiko keamanan siber dengan lebih baik.

Untuk menjelaskan kebutuhan keamanan siber unik organisasi, terdapat berbagai cara penggunaan Kerangka Kerja. Keputusan tentang cara menerapkannya terserah organisasi pelaksana. Misalnya, satu organisasi mungkin memilih menggunakan level Pelaksanaan Kerangka Kerja untuk mengartikulasikan visi praktik manajemen risiko. Organisasi lain mungkin menggunakan lima Fungsi Kerangka Kerja untuk menganalisis keseluruhan portofolio manajemen risiko; analisis itu mungkin atau mungkin tidak mengandalkan panduan yang disertakan, seperti katalog kendali. Kadang ada diskusi tentang “kepatuhan” pada Kerangka Kerja, dan Kerangka Kerja berguna sebagai struktur dan bahasa untuk mengatur dan mengekspresikan kepatuhan terhadap persyaratan keamanan siber organisasi itu sendiri. Namun demikian, berbagai cara di mana Kerangka Kerja dapat digunakan oleh suatu organisasi dapat diartikan bahwa frasa seperti “kepatuhan terhadap Kerangka Kerja” bisa membingungkan dan berarti sesuatu yang sangat berbeda bagi berbagai pemangku kepentingan.

Kerangka Kerja merupakan dokumen hidup dan akan terus dimutakhirkan dan ditingkatkan sepanjang industri memberikan umpan balik pelaksanaan. NIST akan selalu berkoordinasi dengan sektor swasta dan lembaga pemerintah di semua level. Semakin Kerangka Kerja dipraktekkan, tambahan pelajaran yang dipetik akan dimasukkan ke dalam versi mendatang. Hal ini akan memastikan Kerangka Kerja memenuhi kebutuhan Infrastruktur Kritis pemilik dan operator di lingkungan yang dinamis dan menantang dengan ancaman, risiko, dan solusi baru.

Penggunaan dan berbagi yang diperluas dan lebih efektif dari praktik terbaik Kerangka Kerja sukarela ini menjadi langkah berikutnya untuk meningkatkan keamanan siber Infrastruktur Kritis Negara - memberikan panduan yang berkembang untuk organisasi individu sementara meningkatkan sikap keamanan siber Infrastruktur Kritis Negara dan ekonomi serta masyarakat yang lebih luas.

Daftar Isi

Daftar Gambar

Daftar Tabel

1.0 Pendahuluan Kerangka Kerja

Amerika Serikat bergantung pada berfungsinya Infrastruktur Kritisnya yang andal. Ancaman Keamanan Siber mengeksploitasi meningkatnya kompleksitas dan konektivitas sistem Infrastruktur Kritis, yang menyebabkan keamanan, ekonomi, dan keselamatan serta kesehatan publik berisiko. Mirip dengan risiko keuangan dan reputasi, risiko keamanan siber berpengaruh pada pendapatan bersih perusahaan. Risiko ini dapat menaikkan biaya dan mempengaruhi pendapatan. Juga dapat membahayakan kemampuan organisasi untuk berinovasi dan mendapatkan serta mempertahankan pelanggan. Keamanan Siber dapat menjadi komponen penting dan yang memperkuat seluruh manajemen risiko organisasi.

Untuk memperkuat ketahanan infrastruktur ini, the Undang-Undang Peningkatan Keamanan Siber Tahun 2014[2] (CEA) memperbarui peran *National Institute of Standards and Technology* (NIST) untuk "memfasilitasi dan mendukung pengembangan" kerangka kerja risiko keamanan siber. Melalui CEA, NIST harus mengidentifikasi "pendekatan berdasarkan prioritas, fleksibilitas, keberulangkan, berbasis kinerja, dan tepat biaya, termasuk tindakan dan kendali keamanan informasi yang dapat diadopsi secara sukarela oleh pemilik dan operator Infrastruktur Kritis untuk membantu mereka mengidentifikasi, menilai, dan mengelola risiko siber." Hal ini memformalkan pekerjaan NIST sebelumnya dalam mengembangkan Kerangka Kerja Versi 1.0 berdasarkan Perintah Eksekutif 13636, "Meningkatkan Keamanan Siber Infrastruktur Kritis," yang dikeluarkan bulan Februari 2013[3], dan memberikan panduan untuk evolusi Kerangka Kerja mendatang.

Infrastruktur Kritis[4] didefinisikan dalam Undang-Undang Patriot AS tahun 2001[5] sebagai "sistem dan aset, baik fisik maupun virtual, yang sangat vital bagi Amerika Serikat sehingga ketidakmampuan atau hancurnya sistem dan aset tersebut akan berdampak melemahkan keamanan, keamanan ekonomi nasional, kesehatan atau keselamatan publik nasional, atau kombinasinya." Karena meningkatnya tekanan dari ancaman eksternal dan internal, organisasi yang bertanggung jawab atas Infrastruktur Kritis harus memiliki pendekatan yang sesuai dan berulang untuk mengidentifikasi, menilai, dan mengelola risiko keamanan siber. Pendekatan ini diperlukan terlepas dari ukuran, paparan ancaman, atau kecanggihan keamanan siber organisasi saat ini.

Komunitas Infrastruktur Kritis meliputi pemilik dan operator publik dan swasta, dan entitas lain dengan peran dalam mengamankan infrastruktur negara. Anggota masing-masing sektor Infrastruktur Kritis melakukan fungsi yang didukung oleh kategori teknologi yang luas, termasuk teknologi informasi (IT), sistem kendali industri (ICS), sistem siber-ke-fisik (CPS), dan perangkat terhubung yang lebih umum, termasuk Internet untuk Segala (IoT). Ketergantungan terhadap teknologi, komunikasi, dan interkonektivitas ini telah mengubah dan memperluas potensi kerentanan dan meningkatnya potensi risiko operasi. Misalnya, karena teknologi dan data yang dihasilkan dan diprosesnya semakin banyak digunakan untuk memberikan keputusan layanan kritis dan bisnis/misi dukungan, potensi dampak

---

[2] *Lihat* 15 U.S.C. § 272(e)(1)(A)(i). Undang-undang Peningkatan Keamanan Siber Tahun 2014 (S.1353) menjadi hukum umum 113- 274 pada tanggal 18 Desember 2014 dapat ditemukan di: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

[3] Putusan Eksekutif no. 13636, *Improving Critical Infrastructure Cybersecurity* [Meningkatkan Keamanan sier Infrastruktur Kritis], DCPD-201300091, 12 Februari 2013. https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf

[4] Kementerian Keamanan Dalam Negeri (DHS) Program Infrastruktur Kritis memberikan daftar sektor dan fungsi kritis terkaitnya dan rantai nilai. http://www.dhs.gov/critical-infrastructure-sectors

[5] *Lihat* 42 U.S.C. § 5195c(e)). Undang-Undang Patriot AS Tahun 2001 (H.R.3162) menjadi hukum umum 107-56 pada tanggal 26 Oktober 2001 dan dapat ditemukan di: https://www.congress.gov/bill/107th-congress/house-bill/3162

insiden keamanan siber pada organisasi, kesehatan dan keselamatan individu, lingkungan, masyarakat, dan ekonomi dan masyarakat lebih luas harus dipertimbangkan.

Untuk mengelola risiko keamanan siber, pemahaman yang jelas atas pendorong bisnis dan pertimbangan keamanan organisasi yang spesifik bagi penggunaan teknologinya diperlukan. Karena masing-masing risiko, prioritas, dan sistem organisasi itu unik, alat, dan metode yang digunakan untuk mencapai hasil yang diuraikan oleh Kerangka Kerja akan bervariasi.

Mengenali adanya peran bahwa perlindungan privasi dan kebebasan sipil dalam menciptakan kepercayaan masyarakat luas, Kerangka Kerja memasukkan sebuah metodologi untuk melindungi privasi dan kebebasan sipil individu ketika organisasi Infrastruktur Kritis melakukan kegiatan keamanan siber. Banyak organisasi yang telah melakukan proses untuk mengatasi privasi dan kebebasan sipil. Metodologi ini dirancang untuk melengkapi proses tersebut dan memberikan panduan untuk memfasilitasi manajemen risiko privasi yang sesuai dengan pendekatan manajemen risiko keamanan siber organisasi. Memasukkan privasi dan keamanan siber dapat menguntungkan organisasi dengan meningkatnya kepercayaan pelanggan, memungkinkan pembagian informasi yang lebih terstandar, dan menyederhanakan pengoperasian lintas rezim hukum.

Kerangka Kerja tetap efektif dan mendukung inovasi teknis karena teknologi netral, sekaligus juga merujuk berbagai standar, pedoman, dan praktik yang ada yang berkembang dengan teknologi. Dengan mengandalkan standar, pedoman, dan praktik global yang dikembangkan, dikelola, dan dimutakhirkan oleh industri itu, alat dan metode yang tersedia untuk mencapai hasil Kerangka Kerja akan melintasi batas, mengakui sifat global risiko keamanan siber, dan berkembang dengan kemajuan teknologi dan kebutuhan bisnis. Penggunaan standar yang ada dan muncul akan memungkinkan keekonomian skala dan mendorong perkembangan produk, layanan, dan praktik efektif yang memenuhi kebutuhan pasar yang teridentifikasi. Persaingan pasar juga mendorong difusi yang lebih cepat dari teknologi dan praktik ini dan realisasi banyak manfaat oleh pemangku kepentingan dalam sektor ini.

Membangun dari standar, pedoman, dan praktik itu, Kerangka Kerja memberikan taksonomi dan mekanisme umum untuk organisasi untuk:

1) Menguraikan postur keamanan siber saat ini;
2) Menguraikan status keamanan siber yang ditargetkan;
3) Mengidentifikasi dan memprioritaskan kesempatan peningkatan di dalam konteks proses berkelanjutan dan keberulangan;
4) Menilai kemajuan menuju target yang ingin dicapai;
5) Mengkomunikasikan risiko keamanan siber di antara pemangku kepentingan internal dan eksternal.

Kerangka Kerja bukan pendekatan satu untuk semua dalam pengelolaan risiko keamanan siber untuk Infrastruktur Kritis. Organisasi akan selalu memiliki risiko unik - ancaman yang berbeda, kerentanan yang berbeda, toleransi risiko yang berbeda. Organisasi juga bervariasi caranya untuk menyesuaikan praktik yang diuraikan dalam Kerangka Kerja. Organisasi dapat menentukan kegiatan yang penting bagi pemberian layanan kritis dan dapat memprioritaskan investasi untuk memaksimalkan dampak setiap dolar yang dihabiskan. Akhirnya, Kerangka Kerja ditujukan untuk mengurangi dan mengelola risiko keamanan siber dengan lebih baik.

Untuk menjelaskan kebutuhan keamanan siber organisasi, terdapat berbagai cara penggunaan Kerangka Kerja. Keputusan tentang cara menerapkannya terserah organisasi pelaksana. Misalnya, satu organisasi mungkin memilih menggunakan level Pelaksanaan Kerangka Kerja untuk mengartikulasikan visi praktik

manajemen risiko. Organisasi lain mungkin menggunakan lima Fungsi Kerangka Kerja untuk menganalisis keseluruhan portofolio manajemen risiko; analisis itu mungkin atau mungkin tidak mengandalkan panduan yang disertakan, seperti katalog kendali. Kadang ada diskusi tentang "kepatuhan" pada Kerangka Kerja, dan Kerangka Kerja berguna sebagai struktur dan bahasa untuk mengatur dan mengekspresikan kepatuhan terhadap persyaratan keamanan siber organisasi itu sendiri. Namun demikian, berbagai cara di mana Kerangka Kerja dapat digunakan oleh suatu organisasi berarti bahwa frasa seperti "kepatuhan terhadap Kerangka Kerja" bisa membingungkan dan berarti sesuatu yang sangat berbeda bagi berbagai pemangku kepentingan.

Kerangka Kerja melengkapi, dan tidak menggantikan, proses manajemen risiko dan program keamanan siber organisasi. Organisasi dapat menggunakan proses berjalannya dan memanfaatkan Kerangka Kerja untuk mengidentifikasi peluang untuk memperkuat dan memberi tahu manajemennya mengenai risiko keamanan siber sembari menyelaraskan dengan praktik industri. Alternatifnya, organisasi tanpa ada program keamanan siber dapat menggunakan Kerangka Kerja sebagai referensi untuk menetapkan suatu program keamanan siber.

Meskipun Kerangka Kerja dikembangkan untuk meningkatkan manajemen risiko keamanan siber karena terkait dengan Infrastruktur Kritis, namun dapat digunakan oleh organisasi di sektor ekonomi atau masyarakat mana pun. Kerangka Kerja dimaksudkan agar bermanfaat bagi perusahaan, lembaga pemerintah, dan organisasi nirlaba terlepas dari fokus atau ukurannya. Taksonomi umum dari standar, pedoman, dan praktik yang disediakannya juga tidak spesifik negara. Organisasi di luar Amerika Serikat juga dapat menggunakan Kerangka Kerja untuk memperkuat upaya keamanan sibernya sendiri, dan Kerangka Kerja dapat berkontribusi terhadap pengembangan bahasa umum untuk kerjasama internasional mengenai keamanan siber Infrastruktur Kritis.

1.1 Ikhtisar Kerangka Kerja

Kerangka Kerja merupakan pendekatan berbasis risiko untuk pengelolaan risiko keamanan siber, dan terdiri dari tiga bagian: Inti Kerangka Kerja, level Pelaksanaan Kerangka Kerja, dan Profil Kerangka Kerja. Masing-masing komponen Kerangka Kerja memperkuat hubungan antara pendorong bisnis/misi dan kegiatan keamanan siber. Komponen-komponen ini dijelaskan berikut ini.

- *Inti Kerangka Kerja* merupakan serangkaian kegiatan keamanan siber, hasil yang diinginkan, dan referensi yang berlaku dan sudah umum lintas sektor Infrastruktur Kritis. Inti menyajikan standar, pedoman, dan praktik industri dengan cara yang memungkinkan komunikasi dan hasil kegiatan keamanan siber antar organisasi dari level eksekutif hingga level pelaksanaan/pengoperasian. Inti Kerangka Kerja terdiri dari lima Fungsi yang bersamaan dan bersinambung—Mengidentifikasi, Melindungi, Mendeteksi, Merespons, dan Memulihkan. Apabila dipertimbangkan bersama, Fungsi-Fungsi ini memberikan pandangan strategis level tinggi tentang siklus hidup manajemen risiko keamanan siber organisasi. Inti Kerangka Kerja kemudian mengidentifikasi Kategori dan Sub Kategori kunci yang melatarbelakangi - yang merupakan hasil diskrit - untuk masing-masing Fungsi, dan mencocokkannya dengan contoh Referensi Informasi seperti standar, pedoman, dan praktik yang sudah ada untuk masing-masing Sub Kategori.
- *level Pelaksanaan Kerangka Kerja* ("level") memberikan konteks tentang bagaimana organisasi memandang risiko keamanan siber dan proses yang ada untuk mengelola risiko itu. level menggambarkan derajat sejauh mana karakteristik yang ditunjukkan oleh praktik manajemen risiko keamanan siber organisasi yang ditetapkan dalam Kerangka Kerja (misalnya, risiko dan ancaman yang disadari, terulangkan, dan adaptif). level menggolongkan praktik organisasi dalam rentang tertentu, dari Parsial (level 1) hingga Adaptif (level 4). level-level ini

mencerminkan kemajuan dari respons reaktif informal hingga pendekatan yang gesit dan berwawasan risiko. Selama proses pemilihan level, organisasi harus mempertimbangkan praktik manajemen risiko, lingkungan ancaman, persyaratan hukum dan regulasi, tujuan bisnis/misi, dan rintangan organisasi berjalannya.

- *Profil Kerangka Kerja* ("Profil") merepresentasikan hasil berdasarkan kebutuhan bisnis yang telah dipilih organisasi dari Kategori dan Sub Kategori Kerangka Kerja. Profil dapat digolongkan sebagai penyelarasan standar, pedoman, dan praktik dengan Inti Kerangka Kerja dalam skenario pelaksanaan tertentu. Profil dapat digunakan untuk mengidentifikasi peluang untuk meningkatkan sikap keamanan siber dengan mempertimbangkan Profil "Berjalan" (kondisi "apa adanya") dengan Profil "Target" (kondisi "seharusnya"). Untuk mengembangkan sebuah Profil, organisasi dapat meninjau semua Kategori dan Sub Kategori dan, berdasarkan pendorong bisnis/misi dan penilaian risiko, menentukan yang terpenting; dapat ditambahkan Kategori dan Sub Kategori bila perlu untuk mengatasi risiko organisasi. Maka Profil Saat Ini dapat digunakan untuk mendukung prioritas dan pengukuran kemajuan menuju Profil Target, sembari memasukkan faktor dalam kebutuhan bisnis lain termasuk ketepatan biaya dan inovasi. Profil dapat digunakan untuk melakukan penilaian diri dan berkomunikasi dalam organisasi atau antar organisasi.

1.2 Manajemen Risiko dan Kerangka Kerja Keamanan Siber

Manajemen risiko adalah proses mengidentifikasi, menilai, dan merespons risiko secara berkelanjutan. Untuk mengelola risiko, organisasi harus memahami kemungkinan bahwa suatu peristiwa akan terjadi dan potensi dampak yang dihasilkan. Dengan informasi ini, organisasi dapat menentukan level risiko berterima untuk mencapai tujuan organisasinya dan dapat menyatakannya sebagai toleransi risikonya.

Dengan pemahaman toleransi risiko, organisasi dapat memprioritaskan kegiatan keamanan siber, sehingga memungkinkan organisasi membuat keputusan berwawasan tentang belanja keamanan siber. Pelaksanaan program manajemen risiko menawarkan kepada organisasi kemampuan mengukur dan mengomunikasikan penyesuaian program keamanan sibernya. Organisasi dapat memilih menangani risiko dengan cara yang berbeda, termasuk mengurangi risiko, mentransfer risiko, menghindari risiko, atau menerima risiko, tergantung pada potensi dampak pada pemberian layanan kritis. Kerangka Kerja menggunakan proses manajemen risiko agar organisasi dapat menginformasikan dan memprioritaskan keputusan mengenai keamanan siber. Hal ini mendukung terulangnya penilaian risiko dan validasi pendorong bisnis untuk membantu organisasi memilih kondisi target untuk kegiatan keamanan siber yang mencerminkan hasil yang diinginkan. Jadi, Kerangka Kerja memberi organisasi kemampuan untuk memilih dan mengarahkan peningkatan secara dinamis dalam manajemen risiko keamanan siber untuk lingkungan IT dan ICS.

Kerangka Kerja bersifat adaptif untuk memberikan pelaksanaan yang fleksibel dan berbasis risiko yang dapat digunakan dengan berbagai proses manajemen risiko keamanan siber. Contoh proses manajemen risiko keamanan siber termasuk Organisasi Standarisasi Internasional (ISO) 3 1 000:2009[6], ISO/Komisi

[6] Organisasi Standarisasi Internasional, *Risk management – Principles and guidelines* [Manajemen risiko – Prinsip dan pedoman], ISO 31000:2009, 2009. http://www.iso.org/iso/home/standards/iso31000.htm

Elektroteknik Internasional (IEC) 27005:2011[7], Publikasi Khusus NIST (SP) 800-39[8], dan pedoman Keamanan Siber Proses Manajemen Risiko (RMP) Subsektor Ketenagalistrikan[9].

1.3 Ikhtisar Dokumen

Bagian selanjutnya dokumen berisi bagian dan Lampiran berikut ini:

- Bagian 2 menggambarkan komponen Kerangka Kerja: Inti, level, dan Profil Kerangka Kerja.
- Bagian 3 menyajikan contoh cara penggunaan Kerangka Kerja.
- Bagian 4 menggambarkan cara penggunaan Kerangka Kerja untuk penilaian diri dan mendemonstrasikan keamanan siber melalui pengukuran.
- Lampiran A menyajikan Inti Kerangka Kerja dalam format tabel: Fungsi, Kategori, Sub Kategori, dan Referensi Informasi.
- Lampiran B berisi glosarium istilah terpilih.
- Lampiran C berisi daftar akronim yang digunakan dalam dokumen ini.

---

[7] Organisasi Standarisasi Internasional/Komisi Elektroteknik Internasional, *Information technology – Security techniques – Information security risk management* [Teknologi Informasi – Teknik keamanan – Manajemen risiko keamanan informasi], ISO/IEC 27005:2011, 2011. https://www.iso.org/standard/56742.html

[8] Inisiatif Transformasi Gugus Tugas Gabungan, *Managing Information Security Risk: Organization, Mission, and Information System View* [Mengelola Risiko Keamanan Informasi: Pandangan Organisasi, Misi, dan Sistem Informasi], Publikasi Khusus NIST 800-39, March 2011. https://doi.org/10.6028/NIST.SP.800-39

[9] Kementerian Energi AS, *Electricity Subsector Cybersecurity Risk Management Process* [Proses Manajemen Risiko Keamanan Siber Sub Sektor Ketenagalistrikan], DOE/OE-0003, Mei 2012. https://energy.gov/sites/prod/files/Cybersecurity Risk Management Process Guideline - Final - May 2012.pdf

2.0 Dasar-Dasar Kerangka Kerja

Kerangka Kerja memberikan bahasa umum untuk pemahaman, pengelolaan, dan pengungkapan risiko keamanan siber kepada para pemangku kepentingan internal dan eksternal. Kerangka Kerja dapat digunakan untuk membantu mengidentifikasi dan memprioritaskan tindakan untuk mengurangi risiko keamanan siber, dan merupakan alat untuk penyelarasan pendekatan kebijakan, bisnis, dan teknologi terhadap pengelolaan risiko itu. Juga dapat digunakan untuk mengelola risiko keamanan siber antar seluruh organisasi atau dapat difokuskan pada pemberian layanan kritis di dalam organisasi. Jenis entitas yang berbeda - termasuk struktur, asosiasi, dan organisasi koordinasi sektor - juga dapat menggunakan Kerangka Kerja untuk tujuan yang berbeda, termasuk pembuatan Profil umum.

2.1 Inti Kerangka Kerja

Inti Kerangka Kerja memberikan serangkaian kegiatan untuk mencapai *hasil* keamanan siber spesifik, dan mereferensikan contoh panduan untuk mencapai hasil itu. Inti bukan daftar cek tindakan yang harus dilakukan. Inti menyajikan hasil keamanan siber kunci yang teridentifikasi bermanfaat oleh pemangku kepentingan dalam mengelola risiko keamanan siber. Inti terdiri dari empat unsur: Fungsi, Kategori, Sub Kategori, dan Referensi Informasi, yang digambarkan pada Gambar 1:

[10]

Gambar 1: Struktur Inti Kerangka Kerja

Unsur-unsur Inti Kerangka Kerja bekerja sama sebagai berikut:

- **Fungsi** mengatur kegiatan keamanan siber dasar pada level tertingginya. Fungsi-fungsi ini yaitu Mengidentifikasi, Melindungi, Mendeteksi, Merespons, dan Memulihkan. Juga membantu organisasi menyatakan manajemen risiko keamanan sibernya dengan mengatur informasi, sehingga memungkinkan keputusan manajemen risiko, mengatasi ancaman, dan meningkat dengan belajar dari kegiatan sebelumnya. Fungsi ini juga selaras dengan metodologi yang ada untuk manajemen insiden dan membantu menunjukkan dampak investasi pada keamanan

[10] Kerangka Fungsi-Fungsi: identifikasi, proteksi, deteksi, respons, dan pemulihan. Kategori-kategori, sub-kategori-kategori, referensi-referensi information.

siber. Misalnya, investasi dalam perencanaan dan pelaksanaan mendukung tindakan respons dan pemulihan secara tepat waktu, yang mengakibatkan berkurangnya dampak pada pemberian layanan.

- **Kategori** adalah subdivisi dari suatu Fungsi dalam kelompok hasil keamanan siber yang terikat erat dengan kebutuhan terprogram dan kegiatan tertentu. Contoh Kategori meliputi "Manajemen Aset," "Manajemen Identitas dan Kendali Akses," dan "Proses Deteksi."
- **Sub Kategori** selanjutnya membagi Kategori menjadi hasil teknis dan/atau manajemen kegiatan spesifik. Sub kategori memberikan serangkaian hasil yang, meskipun tidak menyeluruh, membantu mendukung pencapaian hasil pada masing-masing Kategori. Contoh Sub Kategori termasuk "Sistem informasi eksternal dikatalogkan," "Data tidak aktif dilindungi," dan "Pemberitahuan untuk sistem deteksi diselidiki."
- **Referensi Informasi** adalah bagian khusus dari standar, pedoman, dan praktik yang umum di antara sektor Infrastruktur Kritis yang mengilustrasikan metode untuk mencapai hasil yang berkaitan dengan masing-masing Sub Kategori. Referensi Informasi yang disajikan pada Inti Kerangka Kerja bersifat ilustratif dan tidak menyeluruh. Referensi Informasi didasarkan pada panduan lintas sektor yang paling sering direferensikan selama proses pengembangan Kerangka Kerja.

Kelima Inti Kerangka Kerja Fungsi didefinisikan sebagai berikut. Fungsi-fungsi ini tidak dimaksudkan untuk membentuk rangkaian tersambung atau mengantarkan pada kondisi akhir statis yang diinginkan. Sebaliknya, fungsi-fungsi ini harus dilaksanakan bersamaan dan berkelanjutan untuk membentuk budaya operasional yang menangani risiko keamanan siber dinamis. Lihat Lampiran A untuk daftar lengkap Inti Kerangka Kerja.

- **Mengidentifikasi** - Mengembangkan pemahaman organisasi untuk mengelola risiko keamanan siber terhadap sistem, orang, aset, data, dan kemampuan.

  Kegiatan dalam Fungsi Mengidentifikasi merupakan pondasi penggunaan Kerangka Kerja secara efektif. Memahami konteks bisnis, sumber daya yang mendukung fungsi kritis, dan risiko keamanan siber terkait memungkinkan organisasi fokus dan memprioritaskan upayanya, sesuai dengan strategi manajemen risiko dan kebutuhan bisnisnya. Contoh Kategori hasil dalam Fungsi ini meliputi: Manajemen Aset; Lingkungan Bisnis; Tata Kelola; Penilaian Risiko; dan Strategi Manajemen Risiko.

- **Melindungi** - Mengembangkan dan melaksanakan keamanan yang sesuai untuk memastikan diberikannya layanan kritis.

  Fungsi Melindungi mendukung kemampuan membatasi atau memuat dampak dari potensi peristiwa keamanan siber. Contoh Kategori hasil dalam Fungsi ini meliputi: Manajemen Identitas dan Kendali Akses; Kesadaran dan Pelatihan; Keamanan Data; Proses dan Prosedur Perlindungan Informasi; Pemeliharaan; dan Teknologi Pelindung.

- **Mendeteksi** - Mengembangkan dan melaksanakan kegiatan yang sesuai untuk mengidentifikasi kejadian peristiwa keamanan siber.

  Fungsi Mendeteksi memungkinkan ditemukannya peristiwa keamanan siber secara tepat waktu. Contoh Kategori hasil dalam Fungsi ini meliputi: Anomali dan Peristiwa; Pemantauan Keamanan Berkelanjutan; dan Proses Deteksi.

- **Merespons** - Mengembangkan dan melaksanakan kegiatan yang sesuai untuk mengambil tindakan mengenai insiden keamanan siber yang terdeteksi.

Fungsi Merespons mendukung kemampuan untuk memuat dampak potensi insiden keamanan siber. Contoh Kategori hasil dalam Fungsi ini meliputi: Perencanaan Respons; Komunikasi; Analisis; Mitigasi; dan Peningkatan.

- **Memulihkan** - Mengembangkan dan melaksanakan kegiatan yang sesuai untuk mempertahankan rencana ketahanan dan mengembalikan kemampuan atau layanan yang terganggu karena insiden keamanan siber.

  Fungsi Memulihkan mendukung pengembalian ke pengoperasian normal secara tepat waktu untuk mengurangi dampak dari insiden keamanan siber. Contoh Kategori hasil dalam Fungsi ini meliputi: Perencanaan Pemulihan; Peningkatan; dan Komunikasi.

2.2 Level/Tingkatan Pelaksanaan Kerangka Kerja

Level Pelaksanaan Kerangka Kerja ("Level") memberikan konteks tentang bagaimana organisasi memandang risiko keamanan siber dan proses yang ada untuk mengelola risiko itu. Mulai dari Parsial (level 1) hingga Adaptif (level 4), level menggambarkan meningkatnya derajat ketelitian dan kecanggihan dalam praktik manajemen risiko keamanan siber. Mereka membantu menentukan sejauh mana manajemen risiko keamanan siber mengetahui kebutuhan bisnis dan terintegrasi ke dalam keseluruhan praktik manajemen risiko organisasi. Pertimbangan manajemen risiko meliputi banyak aspek keamanan siber, termasuk derajat di mana pertimbangan privasi dan kebebasan sipil terintegrasi ke dalam manajemen risiko keamanan siber dan respons potensi risiko organisasi.

Proses pemilihan level mempertimbangkan praktik manajemen risiko organisasi saat ini, ancaman lingkungan, persyaratan hukum dan regulasi, praktik berbagai informasi, tujuan bisnis/misi, persyaratan keamanan siber rantai pasokan, dan rintangan organisasi. Organisasi harus menentukan level yang diinginkan, yang memastikan bahwa level terpilih memenuhi tujuan organisasi, layak dilaksanakan, dan mengurangi risiko keamanan siber atas aset dan sumber daya kritis hingga level yang dapat diterima oleh organisasi. Organisasi harus mempertimbangkan memanfaatkan panduan eksternal yang diperoleh dari departemen dan lembaga Pemerintah Federal, Pusat Berbagi dan Analisis Informasi (ISAC), Organisasi Berbagi dan Analisis Informasi (ISAO), model maturitas yang ada, atau sumber lain untuk membantu menentukan level yang diinginkannya.

Meskipun organisasi yang teridentifikasi sebagai level 1 (Parsial) didorong untuk meningkatkan diri ke level 2 atau lebih tinggi, level tidak merepresentasikan tingkatan maturitas. Level ini dimaksudkan untuk mendukung keputusan organisasi dalam hal cara mengelola risiko keamanan siber, serta dimensi organisasi mana yang lebih tinggi prioritasnya dan dapat menerima sumber daya tambahan. Kemajuan ke level yang lebih tinggi didorong apabila analisis manfaat biaya mengindikasikan pengurangan risiko keamanan siber yang layak dan tepat biaya.

Keberhasilan pelaksanaan Kerangka Kerja berdasarkan pada pencapaian hasil yang diuraikan dalam Profil Target organisasi dan bukan berdasarkan penentuan level. Juga, pemilihan dan penunjukan level secara wajar mempengaruhi Profil Kerangka Kerja. Rekomendasi tingkatan oleh manajer Bisnis/Proses, sebagaimana disetujui oleh level Eksekutif Senior, akan membantu menetapkan keseluruhan nuansa bagaimana risiko keamanan siber akan dikelola di dalam organisasi, dan harus mempengaruhi prioritas di dalam Profil Target dan penilaian kemajuan dalam mengatasi kesenjangan.

Definisi level adalah sebagai berikut:

Level 1: Parsial

- *Proses Manajemen Risiko* - Praktik manajemen risiko keamanan siber organisasi tidak diformalkan, dan risiko dikelola secara *ad hoc* dan secara reaktif. Prioritas kegiatan keamanan

siber tidak dapat langsung diketahui melalui sasaran risiko organisasi, lingkungan ancaman, atau persyaratan bisnis/misi.

- *Program Manajemen Risiko Terintegrasi* - Terdapat kesadaran terbatas atas risiko keamanan siber pada level organisasi. Organisasi melaksanakan manajemen risiko keamanan siber secara tidak rutin dan kasus demi kasus karena pengalaman atau informasi yang diperoleh dari sumber luar bervariasi. Organisasi tidak dapat memiliki proses yang memungkinkan informasi keamanan siber dibagikan di dalam organisasi.
- *Partisipasi Eksternal* - Organisasi tidak memahami perannya dalam ekosistem yang lebih besar berkenaan dengan kemandirian atau ketergantungannya. Organisasi tidak mengkolaborasikan atau menerima informasi (misalnya, intelijen ancaman, praktik terbaik, teknologi) dari entitas lain (misalnya, pembeli, pemasok, dependensi, dependen, ISAO, peneliti, pemerintah), dan tidak berbagi informasi. Organisasi biasanya tidak mengetahui risiko rantai pasokan siber dari produk dan layanan yang diberikannya dan yang digunakannya.

Level 2: Berwawasan Risiko

- *Proses Manajemen Risiko* - Praktik manajemen risiko disetujui oleh manajemen tetapi mungkin tidak ditetapkan sebagai kebijakan di seluruh organisasi. Prioritas kegiatan keamanan siber dan kebutuhan perlindungan diketahui langsung melalui sasaran risiko organisasi, lingkungan ancaman, atau persyaratan bisnis/misi.
- *Program Manajemen Risiko Terintegrasi* - Terdapat kesadaran risiko keamanan siber di level organisasi, tetapi pendekatan di seluruh organisasi terhadap pengelolaan risiko keamanan siber belum ditetapkan. Informasi Keamanan Siber dibagikan di dalam organisasi secara informal. Pertimbangan keamanan siber dalam sasaran dan program organisasi dapat terjadi pada beberapa tetapi tidak semua level organisasi. Penilaian risiko siber organisasi dan aset eksternal terjadi, tetapi biasanya tidak terulangkan atau terjadi kembali.
- *Partisipasi Eksternal* - Pada umumnya, organisasi memahami perannya dalam ekosistem yang lebih besar berkenaan dengan dependensi atau dependennya sendiri, tetapi tidak keduanya. Organisasi mengelaborasi dan menerima beberapa informasi dari entitas lain dan menghasilkan beberapa informasinya sendiri, tetapi tidak dapat berbagi informasi dengan pihak lain. Selain itu, organisasi mengetahui risiko rantai pasokan siber yang berkaitan dengan produk dan layanan yang diberikan dan digunakannya, tetapi tidak bertindak sesuai dengan atau secara formal terhadap risiko-risiko itu.

Level 3: Terulangkan

- *Proses Manajemen Risiko* - Praktik manajemen risiko organisasi disetujui dan diungkapkan secara formal sebagai kebijakan. Praktik keamanan siber organisasi dimutakhirkan secara berkala berdasarkan penerapan proses manajemen risiko pada perubahan persyaratan bisnis/misi dan lanskap ancaman dan teknologi yang berubah-ubah.
- *Program Manajemen Risiko Terintegrasi* - Terdapat pendekatan di seluruh organisasi untuk pengelolaan risiko keamanan siber. Kebijakan, proses, dan prosedur berwawasan risiko ditetapkan, dilaksanakan seperti yang dimaksudkan, dan ditinjau. Metode yang sesuai diterapkan untuk merespons perubahan risiko secara efektif. Personel memiliki pengetahuan dan keterampilan untuk melakukan peran dan tanggung jawab yang mereka tanggung. Organisasi secara konsisten dan akurat memantau risiko keamanan siber dari aset organisasi. Eksekutif senior keamanan siber dan non-keamanan siber berkomunikasi secara rutin

mengenai risiko keamanan siber. Eksekutif senior memastikan pertimbangan keamanan siber melalui semua lini operasi dalam organisasi.

- *Partisipasi Eksternal* - Organisasi memahami peran, dependensi, dan ketergantungannya dalam ekosistem yang lebih besar dan dapat berkontribusi terhadap pemahaman yang lebih luas atas risiko komunitas. Organisasi mengkolaborasikan dan menerima informasi dari entitas lain secara berkala yang melengkapi informasi yang dihasilkan secara internal, dan berbagi informasi dengan entitas lain. Organisasi mengetahui risiko rantai pasokan siber yang berkaitan dengan produk dan layanan yang diberikan dan yang digunakannya. Selain itu, organisasi biasanya bertindak secara formal atas risiko-risiko itu, termasuk mekanisme seperti perjanjian tertulis untuk mengomunikasikan persyaratan dasar, struktur tata kelola (misalnya, dewan risiko), dan pelaksanaan serta pemantauan kebijakan.

Level 4: Adaptif

- *Proses Manajemen Risiko* - Organisasi mengadaptasikan praktik keamanan siber berdasarkan kegiatan keamanan siber berjalan dan sebelumnya, termasuk pelajaran yang dipetik dan indikator yang diprediksi. Melalui proses peningkatan berkelanjutan dengan memasukkan teknologi maju dan praktik keamanan siber, organisasi secara aktif beradaptasi terhadap perubahan lanskap ancaman dan teknologi dan merespons ancaman yang berkembang dan canggih secara tepat waktu dan efektif.
- *Program Manajemen Risiko Terintegrasi* - Terdapat pendekatan di seluruh organisasi terhadap pengelolaan risiko keamanan siber yang menggunakan kebijakan, proses, dan prosedur berwawasan risiko untuk mengatasi potensi peristiwa keamanan siber. Hubungan antara risiko keamanan siber dan tujuan organisasi dipahami secara jelas dan dipertimbangkan saat membuat keputusan. Eksekutif senior memantau risiko keamanan siber dalam konteks yang sama seperti risiko keuangan dan risiko organisasi lainnya. Anggaran organisasi didasarkan pada pemahaman lingkungan risiko dan toleransi risiko saat ini dan yang diprediksi. Unit bisnis melaksanakan visi eksekutif dan menganalisis risiko selevel sistem dalam konteks toleransi risiko organisasi. Manajemen risiko keamanan siber adalah bagian dari budaya organisasi dan berkembang dari kegiatan sebelumnya dan pengetahuan terus-menerus dari kegiatan pada sistem dan jaringannya. Organisasi dapat secara cepat dan efisien memperhitungkan perubahan terhadap tujuan bisnis/misi dalam hal bagaimana risiko didekati dan dikomunikasikan.
- *Partisipasi Eksternal* - Organisasi memahami peran, dependensi, dan dependennya dalam ekosistem yang lebih besar dan berkontribusi bagi pemahaman yang lebih luas atas risiko masyarakat. Organisasi menerima, menghasilkan, dan meninjau informasi yang diprioritaskan yang menginformasikan analisis berkelanjutan atas resikonya karena lanskap ancaman dan teknologi berkembang. Organisasi membagikan informasi itu secara internal dan eksternal dengan kolaborator lain. Organisasi menggunakan informasi waktu-nyata atau mendekati waktu-nyata untuk memahami dan bertindak secara konsisten atas risiko rantai pasokan siber yang berkaitan dengan produk dan layanan yang diberikan dan yang digunakannya. Selain itu, organisasi berkomunikasi secara proaktif, dengan menggunakan mekanisme formal (misalnya perjanjian) dan informal untuk mengembangkan dan menjaga hubungan rantai pasokan yang kuat.

2.3 Profil Kerangka Kerja

Profil Kerangka Kerja (“Profil”) merupakan penyelarasan Fungsi, Kategori, dan Sub Kategori dengan persyaratan bisnis, toleransi risiko, dan sumber daya organisasi.Profil memungkinkan organisasi

menetapkan peta jalur untuk mengurangi risiko keamanan siber yang diselaraskan dengan baik dengan tujuan organisasi dan sektor, mempertimbangkan persyaratan hukum/regulasi dan praktik terbaik industri, dan mencerminkan prioritas manajemen risiko. Mengingat kompleksnya banyak organisasi, mereka dapat memilih beberapa profil, yang selaras dengan komponen tertentu dan yang mengakui kebutuhan individunya masing-masing.

Profil Kerangka Kerja dapat digunakan untuk menggambarkan kondisi saat ini atau target kondisi yang diinginkan atas kegiatan keamanan siber spesifik. Profil Saat Ini mengindikasikan hasil keamanan siber yang tercapai saat ini. Profil Target mengindikasikan hasil yang diperlukan untuk mencapai tujuan manajemen risiko keamanan siber yang diinginkan. Profil mendukung persyaratan bisnis/misi dan membantu mengkomunikasikan risiko di dalam dan antar organisasi. Kerangka Kerja ini tidak menetapkan templat Profil, yang memungkinkan fleksibelnya pelaksanaan.

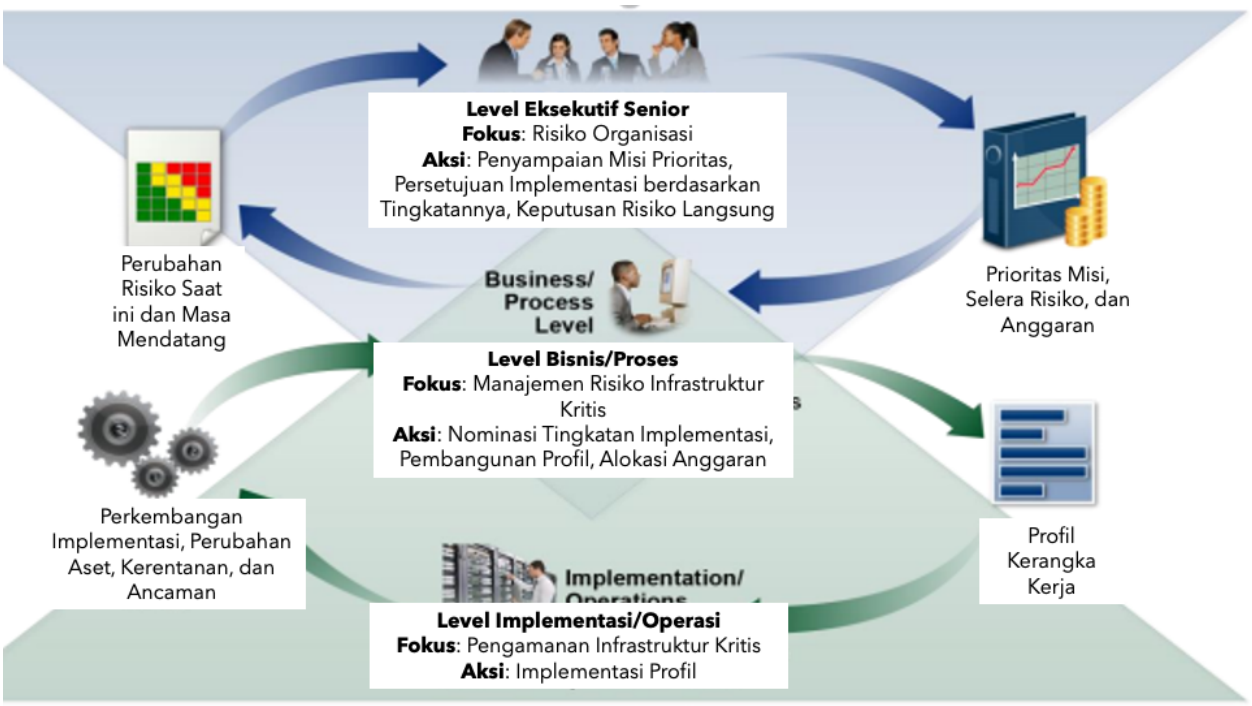
Perbandingan Profil (misalnya, Profil Saat Ini dan Profil Target) dapat menampakkan celah yang harus diatasi untuk memenuhi tujuan manajemen risiko keamanan siber. Rencana tindakan untuk mengatasi celah-celah ini untuk mengisi Kategori atau Subkategori yang dimaksud dapat berkontribusi terhadap peta jalur yang diuraikan di atas. Prioritas mitigasi celah didorong oleh kebutuhan bisnis dan proses manajemen risiko organisasi. Pendekatan berbasis risiko ini memungkinkan organisasi mengukur sumber daya yang diperlukan (misalnya, penyusunan staf, pendanaan) untuk mencapai tujuan keamanan siber secara tepat biaya dan terprioritas. Lebih lanjut, Kerangka Kerja merupakan pendekatan berbasis risiko di mana keterterapan dan pemenuhan Sub Kategori yang dimaksud tunduk pada ruang lingkup Profil.

2.4 Koordinasi Pelaksanaan Kerangka Kerja

Gambar 2 menggambarkan aliran informasi dan keputusan pada level-level di bawah ini dalam sebuah organisasi:

- Eksekutif
- Bisnis/Proses
- Pelaksanaan/Pengoperasian

Level eksekutif mengomunikasikan prioritas misi, sumber daya yang tersedia, dan keseluruhan toleransi risiko terhadap level bisnis/proses. Level bisnis/proses menggunakan informasi sebagai masukan proses manajemen risiko, dan kemudian berkolaborasi dengan level pelaksanaan/pengoperasian untuk mengkomunikasikan kebutuhan bisnis dan membuat Profil. Level pelaksanaan/pengoperasian mengkomunikasikan kemajuan pelaksanaan Profil kepada level bisnis/proses. Level bisnis/proses menggunakan informasi ini untuk melakukan penilaian dampak. Manajemen level bisnis/proses melaporkan hasil penilaian dampak itu kepada level eksekutif untuk memberitahukan keseluruhan proses manajemen risiko organisasi dan kepada level pelaksanaan/pengoperasian agar mengetahui dampak bisnis.



Gambar 2: Informasi Gagasan dan Alur Keputusan di dalam Organisasi

3.0 Cara Menggunakan Kerangka Kerja

Organisasi dapat menggunakan Kerangka Kerja sebagai bagian kunci dari proses sistematis untuk mengidentifikasi, menilai, dan mengelola risiko keamanan siber. Kerangka Kerja tidak didesain untuk mengganti proses yang sudah ada; organisasi dapat menggunakan proses yang sedang berjalan dan menambahkan proses tersebut pada Kerangka Kerja untuk menentukan celah pada pendekatan risiko keamanan siber yang sedang berlangsung dan mengembangkan peta jalan peningkatannya. Menggunakan Kerangka Kerja sebagai alat manajemen risiko keamanan siber, organisasi dapat menentukan kegiatan yang paling penting untuk pemberian layanan kritis dan memprioritaskan belanja untuk memaksimalkan dampak investasi.

Kerangka Kerja dirancang untuk melengkapi pengoperasian bisnis dan keamanan siber yang sudah ada. Kerangka Kerja dapat bertindak sebagai pondasi untuk program keamanan siber baru atau mekanisme untuk meningkatkan program yang sudah ada. Kerangka Kerja memberikan cara menyatakan persyaratan keamanan siber bagi mitra bisnis dan pelanggan dan dapat membantu mengidentifikasi celah dalam praktik keamanan siber organisasi. Juga memberikan serangkaian pertimbangan dan proses umum untuk mempertimbangkan implikasi kebijakan dan kebebasan sipil dalam konteks program keamanan siber.

Kerangka Kerja dapat diaplikasikan di seluruh fase siklus hidup, dari perencanaan, desain, pembangunan/pembelian, penempatan, pengoperasian, dan penonaktifan. Fase perencanaan memulai siklus sistem dan meletakkan dasar untuk segala sesuatu yang mengikutinya. Pertimbangan menyeluruh keamanan siber harus dinyatakan dan diuraikan sejelas mungkin. Rencana harus mengakui bahwa pertimbangan dan persyaratan kemungkinan akan berubah selama sisa siklus hidup. Fase desain haus memperhitungkan persyaratan keamanan siber sebagai bagian dari proses rekayasa sistem multi disiplin

yang lebih besar.[11] Tahapan pencapaian kunci fase desain merupakan validasi bahwa spesifikasi keamanan siber sistem cocok dengan kebutuhan dan disposisi risiko organisasi seperti yang terdapat pada Profil Kerangka Kerja. Hasil keamanan siber yang diinginkan yang diprioritaskan dalam Profil Target harus dimasukkan saat a) mengembangkan sistem selama fase bangun dan b) membeli atau mengalihdayakan sistem selama fase beli. Profil Target yang sama itu bertindak sebagai daftar fitur keamanan siber sistem yang harus dinilai saat menempatkan sistem untuk memverifikasi semua fitur diimplementasikan. Hasil keamanan siber yang ditentukan dengan penggunaan Kerangka Kerja kemudian harus bertindak sebagai dasar untuk operasi sistem secara berkelanjutan. Hal ini mencakup penilaian ulang berkala, menangkap hasil dalam Profil Saat Ini, untuk memverifikasi bahwa persyaratan keamanan siber masih terpenuhi. Biasanya, jaringan dependensi yang kompleks (misalnya, kendali kompensasi dan umum) di antara sistem berarti hasil yang didokumentasikan dalam Profil Target dari sistem terkait harus dipertimbangkan dengan hati-hati saat sistem dinonaktifkan.

Bagian berikut ini menyajikan cara yang berbeda bagi organisasi untuk menggunakan Kerangka Kerja.

3.1 Tinjauan Dasar Praktik Keamanan Siber

Kerangka Kerja dapat digunakan untuk membandingkan kegiatan keamanan siber berjalan organisasi dengan kegiatan keamanan siber yang diuraikan dalam Inti Kerangka Kerja. Melalui pembuatan Profil Saat Ini, organisasi dapat menguji sejauh mana profil itu mencapai hasil yang digambarkan dalam Kategori Inti dan Sub Kategori, yang selaras dengan lima level Fungsi utama : Mengidentifikasi, Melindungi, Mendeteksi, Merespons, dan Memulihkan. Organisasi mungkin mendapati bahwa hasil yang diinginkan sudah tercapai, jadi pengelolaan keamanan siber sepadan dengan risiko yang diketahui. Alternatifnya, organisasi dapat menentukan bahwa ia memiliki peluang untuk (atau perlu) meningkat. Organisasi dapat menggunakan informasi itu untuk mengembangkan rencana tindakan untuk memperkuat praktik keamanan siber yang ada dan mengurangi risiko keamanan siber. Organisasi juga mungkin mendapati bahwa mencapai hasil tertentu merupakan investasi yang berlebihan. Organisasi dapat menggunakan informasi ini untuk memprioritaskan kembali sumber daya.

Meskipun tidak menggantikan proses manajemen risiko, kelima Fungsi utama ini akan memberikan cara ringkas bagi eksekutif senior dan yang lainnya untuk menyaring konsep fundamental tentang risiko keamanan siber sehingga mereka dapat menilai bagaimana risiko yang teridentifikasi dikelola, dan bagaimana organisasi mereka menyimpulkan pada level tinggi terhadap standar, pedoman, dan praktik keamanan siber yang ada. Kerangka Kerja juga dapat membantu organisasi menjawab pertanyaan fundamental, termasuk “Bagaimana keadaan kita?” Kemudian mereka dapat bergerak secara lebih berwawasan untuk memperkuat praktik keamanan sibernya di tempat dan waktu yang dianggap perlu.

3.2 Penetapan atau Peningkatan Program Keamanan Siber

Langkah-langkah berikut ini mengilustrasikan bagaimana organisasi dapat menggunakan Kerangka Kerja untuk membuat program keamanan siber baru atau meningkatkan program berjalan yang sudah ada. Langkah-langkah ini harus di ulangi bila perlu untuk terus meningkatkan keamanan siber.

Langkah 1: Memprioritaskan dan Mencakup. Organisasi mengidentifikasi tujuan bisnis/misi dan prioritas organisasi level tingginya. Dengan informasi ini, organisasi membuat keputusan strategis mengenai pelaksanaan keamanan siber dan menentukan ruang lingkup sistem dan aset yang mendukung lini atau proses bisnis yang dipilih. Kerangka Kerja dapat diadaptasi untuk mendukung lini

[11] Publikasi Khusus NIST 800-160 Volume 1, *System Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* [Rekayasa Keamanan Sistem, Pertimbangan Pendekatan Multidisiplin dalam Rekayasa Sistem Aman dan Terpercaya], Ross et al, November 2016 (dimutakhirkan 21 Maret 2018), https://doi.org/10.6028/NIST.SP.800-160v1

atau proses bisnis yang berbeda dalam organisasi, yang mungkin memiliki kebutuhan bisnis dan toleransi risiko terkait yang berbeda. Toleransi risiko dapat tercermin dalam Pelaksanaan level target.

Langkah 2: Mengorientasikan. Setelah ruang lingkup program keamanan siber telah ditentukan untuk lini atau proses bisnis, organisasi mengidentifikasi sistem dan aset terkait, persyaratan regulasi, dan seluruh pendekatan risiko. Organisasi selanjutnya memeriksa sumber untuk mengidentifikasi ancaman dan kerentanan yang berlaku pada sistem dan aset itu.

Langkah 3: Membuat Profil Saat Ini. Organisasi mengembangkan Profil Saat Ini dengan mengindikasikan hasil Kategori dan Sub Kategori mana dari Inti Kerangka Kerja yang saat ini tercapai. Apabila hasilnya tercapai sebagian, memperhatikan fakta ini akan membantu mendukung langkah berikutnya dengan memberikan informasi dasar.

Langkah 4: Melakukan Penilaian Risiko. Penilaian ini dapat dipandu dengan keseluruhan proses manajemen risiko atau kegiatan penilaian risiko sebelumnya organisasi. Organisasi menganalisis lingkungan operasional untuk melihat kemungkinan peristiwa keamanan siber dan dampak yang dapat diakibatkan peristiwa itu terhadap organisasi. Penting agar organisasi mengidentifikasi risiko yang muncul dan menggunakan informasi ancaman siber dari sumber internal dan eksternal untuk memperoleh pemahaman yang lebih baik atas kemungkinan dan dampak peristiwa keamanan siber.

Langkah 5: Membuat Profil Target. Organisasi membuat Profil Target yang fokus pada penilaian Kategori dan Sub Kategori Kerangka Kerja yang menguraikan hasil keamanan siber organisasi yang diinginkan. Organisasi juga dapat mengembangkan Kategori dan Sub Kategori tambahannya sendiri untuk memperhitungkan risiko unik organisasi. Organisasi juga dapat mempertimbangkan pengaruh dan permintaan pemangku kepentingan eksternal seperti entitas sektor, pelanggan, dan mitra bisnis saat membuat Profil Target. Profil Target harus mencerminkan criteria secara tepat dalam Pelaksanaan level target.

Langkah 6: Menentukan, Menganalisis, dan Memprioritaskan Celah. Organisasi membandingkan Profil Saat Ini dan Profil Target untuk menentukan celah. Selanjutnya, membuat rencana tindakan prioritas untuk mengatasi celah - yang mencerminkan pendorong, biaya dan manfaat misi, dan risiko - untuk mencapai hasil dalam Profil Target. Organisasi kemudian menentukan sumber daya, termasuk pendanaan dan tenaga kerja, yang diperlukan untuk mengatasi celah-celah tersebut. Menggunakan Profil dengan cara ini mendorong organisasi untuk membuat keputusan berwawasan tentang kegiatan keamanan siber, mendukung manajemen risiko, dan memungkinkan organisasi untuk melakukan peningkatan tertarget yang tepat biaya.

Langkah 7: Melaksanakan Rencana Tindakan. Organisasi menentukan tindakan mana yang akan diambil untuk mengatasi celah, bila ada, yang teridentifikasi dalam langkah sebelumnya dan kemudian menyesuaikan praktik keamanan siber berjalannya untuk mencapai Profil Target. Untuk panduan lebih lanjut, Kerangka Kerja mengidentifikasi Referensi Informasi contoh mengenai Kategori dan Sub Kategori, tetapi organisasi harus menentukan standar, pedoman, dan praktik mana, termasuk yang spesifik sektor, berfungsi terbaik bagi kebutuhannya.

Organisasi mengulangi langkah-langkah yang diperlukan untuk terus menilai dan meningkatkan keamanan sibernya. Misalnya, organisasi mungkin menemukan bahwa pengulangan lebih sering dari orientasi langkah meningkatkan mutu penilaian risiko. Lebih lanjut, organisasi dapat memantau kemajuannya melalui pemutakhiran berulang pada Profil Saat Ini, kemudian membandingkan Profil Saat Ini dengan Profil Target. Organisasi juga dapat menggunakan proses ini untuk menyelaraskan program keamanan sibernya dengan level Pelaksanaan Kerangka Kerja yang diinginkan.

3.3 Mengkomunikasikan persyaratan Keamanan Siber dengan Pemangku Kepentingan

Kerangka Kerja memberikan bahasa umum untuk mengomunikasikan persyaratan di antara para pemangku kepentingan yang saling bergantung yang bertanggung jawab atas pemberian produk dan layanan Infrastruktur Kritis esensial. Contoh:

- Organisasi dapat menggunakan Profil Target untuk menyatakan persyaratan manajemen risiko keamanan siber kepada penyedia layanan eksternal (misalnya, penyedia awan di mana data diekspor).
- Organisasi dapat menyatakan kondisi keamanan sibernya melalui Profil Saat Ini untuk melaporkan hasil atau membandingkan persyaratan akuisisi.
- Pemilik/operator Infrastruktur Kritis, setelah mengidentifikasi mitra eksternal di mana infrastruktur bergantung, dapat menggunakan Profil Target untuk menyampaikan Kategori dan Sub Kategori yang diminta.
- Sektor Infrastruktur Kritis dapat menetapkan Profil Target yang dapat digunakan di antara konstituennya sebagai Profil dasar awal untuk membangun Profil Target yang disesuaikan.
- Organisasi dapat mengelola risiko keamanan siber dengan lebih baik di antara para pemangku kepentingan dengan menilai posisi mereka pada Infrastruktur Kritis dan ekonomi digital yang lebih luas yang menggunakan level Pelaksanaan.

Komunikasi sangat penting di antara para pemangku kepentingan rantai pasokan, baik ke atas maupun ke bawah. Rantai pasokan merupakan rangkaian sumber daya dan proses yang kompleks, didistribusikan secara global, dan saling terkait antara beberapa level organisasi. Rantai pasokan rantai pasokan dimulai dengan sumber produk dan layanan dan meluas dari desain, pengembangan, manufaktur, pemrosesan, penanganan, dan penyerahan produk dan layanan kepada pengguna akhir. Mengingat hubungan-hubungan ini cukup kompleks dan saling terkait, Manajemen Risiko Rantai Pasokan (MRRP) merupakan fungsi organisasi yang kritis.[12]

MRRP Siber merupakan rangkaian kegiatan yang diperlukan untuk mengelola risiko keamanan siber yang berkaitan dengan pihak eksternal. Lebih spesifik, MRRP siber mengatasi efek keamanan siber yang dimiliki organisasi pada pihak eksternal dan efek keamanan siber yang dimiliki pihak eksternal pada organisasi.

Tujuan utama MRRP siber adalah mengidentifikasi, menilai, dan mengurangi "produk dan layanan yang mungkin mengandung fungsionalitas yang berpotensi berbahaya, palsu, atau rentan karena rendahnya praktik manufaktur dan pengembangan di dalam rantai pasokan siber[13]." Kegiatan MRRP Siber dapat meliputi:

- Menentukan persyaratan keamanan siber bagi pemasok,
- Menetapkan persyaratan keamanan siber melalui perjanjian formal (misalnya, kontrak),
- Mengkomunikasikan kepada pemasok cara persyaratan keamanan siber itu akan diverifikasi dan divalidasi,

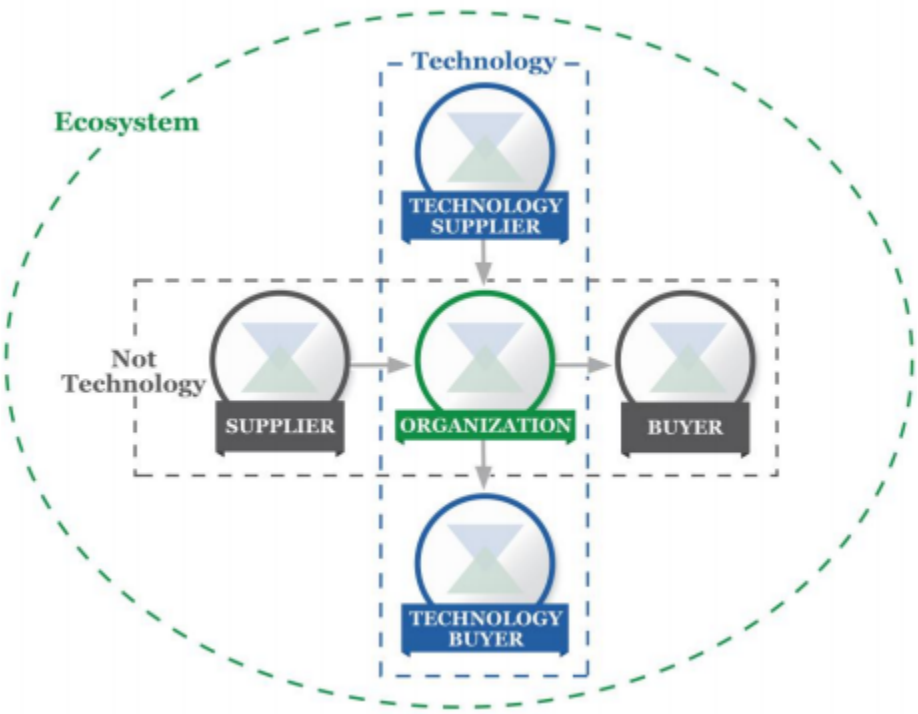
[12] Mengomunikasikan Persyaratan Keamanan Siber (Bagian 3.3) dan Keputusan Membeli (Bagian 3.4) hanya membahas penggunaan Kerangka Kerja untuk MRRP siber dan tidak ditujukan untuk membahas MRRP siber secara komprehensif.

[13] Publikasi Khusus NIST 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* [Praktik Manajemen Risiko Rantai Pasokan untuk Sistem Organisasi Federal dan Organisasi], Boyens et al, April 2015, https://doi.org/10.6028/NIST.SP.800-161

- Memverifikasi bahwa persyaratan keamanan siber terpenuhi melalui berbagai metodologi penilaian, dan
- Mengatur dan mengelola kegiatan-kegiatan di atas.

Sebagaimana digambarkan pada Gambar 3, MRRP siber meliputi pemasok dan pembeli teknologi, serta pemasok dan pembeli non teknologi, di mana teknologi minimal terdiri dari teknologi informasi (IT), sistem kendali industri (ICS), sistem siber-ke-fisik (CPS), dan perangkat terhubung yang lebih umum, termasuk Internet untuk Segala (IoT). Gambar 3 menggambarkan organisasi pada satu titik waktu. Namun, melalui berjalannya operasi bisnis normal, sebagian besar organisasi akan menjadi pemasok hulu dan pembeli hilir terkait dengan organisasi lain atau pengguna akhir.

Kerangka Kerja Keamanan Siber



Gambar 3: Hubungan Rantai Pasokan Siber[14]

Pihak yang diuraikan pada Gambar 3 merupakan ekosistem keamanan siber organisasi. Hubungan-hubungan ini menyoroti peran krusial MRRP siber dalam mengatasi risiko keamanan siber pada Infrastruktur Kritis dan ekonomi digital yang lebih luas. Hubungan-hubungan ini, produk dan layanan yang diberikannya, dan risiko yang direpresentasikan harus diidentifikasi dan difaktorkan ke dalam kemampuan perlindungan dan deteksi organisasi, serta protokol pemulihan dan responsnya.

Pada gambar di atas, “Pembeli” merujuk pada orang atau organisasi hilir yang mengkonsumsi produk atau layanan yang dimaksud dari organisasi, termasuk organisasi laba dan nirlaba. “Pemasok” meliputi penyedia produk dan layanan hulu yang digunakan untuk tujuan internal organisasi (misalnya, infrastruktur IT) atau yang diintegrasikan ke dalam produk atau layanan yang diberikan kepada Pembeli.

[14] Pemasok, teknologi pemasok, organisasi, pembeli, pembeli teknologi

Istilah-istilah ini dapat diterapkan pada produk dan layanan berbasis teknologi dan non berbasis teknologi.

Dalam mempertimbangkan Sub Kategori individu dari Inti atau pertimbangan komprehensif dari suatu Profil, Kerangka Kerja menawarkan kepada organisasi dan mitranya metode untuk membantu memastikan produk atau layanan memenuhi hasil keamanan kritis. Dengan memilih hasil yang relevan dengan konteks terlebih dahulu (misalnya, transmisi Informasi Identifikasi Pribadi (PII), pelayanan misi kritikal, layanan verifikasi data, integritas produk atau layanan) organisasi selanjutnya dapat mengevaluasi mitra terhadap kriteria-kriteria itu. Misalnya, jika suatu sistem dibeli memantau Teknologi Operasional (OT) akan adanya anomali komunikasi jaringan, ketersediaan mungkin menjadi tujuan keamanan siber yang sangat penting untuk dicapai dan harus mendorong evaluasi Pemasok Teknologi terhadap Sub Kategori yang berlaku (misalnya, ID.BE-4, ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6, PR.DS-7, PR.DS-8, PR.IP-1, DE.AE-5).

3.4 Keputusan Pembelian

Karena Profil Target Kerangka Kerja merupakan daftar prioritas dari persyaratan keamanan siber organisasi, Profil Target dapat digunakan untuk menginformasikan keputusan tentang pembelian produk dan layanan. Transaksi ini bervariasi dari Mengomunikasikan Persyaratan Keamanan Siber dengan Pemangku Kepentingan (dibahas di Bagian 3.3) di mana mungkin tidak layak untuk memberlakukan serangkaian persyaratan keamanan siber pada pemasok. Tujuannya seharusnya membuat keputusan pembelian terbaik di antara beberapa pemasok, mengingat daftar persyaratan keamanan siber ditentukan dengan hati-hati. Biasanya, hal ini berarti beberapa derajat kompromi, dengan membandingkan beberapa produk atau layanan dengan celah yang diketahui dengan Profil Target.

Setelah suatu produk atau layanan dibeli, Profil tersebut juga dapat digunakan untuk melacak dan mengatasi sisa risiko keamanan siber. Misalnya, bila layanan atau produk yang dibeli tidak memenuhi semua tujuan yang diuraikan dalam Profil Target, organisasi dapat mengatasi sisa risiko melalui tindakan manajemen lain. Profil juga memberi organisasi metode penilaian bila produk memenuhi hasil keamanan siber melalui mekanisme peninjauan dan pengujian berkala.

3.5 Mengidentifikasi Peluang untuk Referensi Informasi Baru atau Revisi

Kerangka Kerja dapat digunakan untuk mengidentifikasi peluang untuk standar, pedoman, atau praktik baru atau revisi di mana Referensi Informasi tambahan akan membantu organisasi menyelesaikan kebutuhan yang muncul. Dalam melaksanakan Sub Kategori yang dimaksud, atau mengembangkan Sub Kategori baru, organisasi mungkin menemukan bahwa terdapat beberapa Referensi Informasi, bila ada, untuk kegiatan terkait. Untuk mengatasi kebutuhan itu, organisasi dapat berkolaborasi dengan pimpinan teknologi dan/atau badan standar untuk menyusun, mengembangkan, dan mengkoordinasikan standar, pedoman, atau praktik.

3.6 Metodologi untuk Melindungi Privasi dan Kebebasan Sipil

Bagian ini menggambarkan metodologi untuk mengatasi implikasi privasi individu dan kebebasan sipil yang mungkin diakibatkan oleh keamanan siber. Metodologi ini dimaksudkan menjadi serangkaian pertimbangan dan proses umum karena implikasi privasi dan kebebasan sipil mungkin berbeda menurut sektor atau dari waktu ke waktu dan organisasi dapat mengatasi pertimbangan dan proses ini dengan berbagai pelaksanaan teknis. Meskipun demikian, tidak semua kegiatan dalam program keamanan siber menimbulkan pertimbangan privasi dan kebebasan sipil. Standar privasi teknis, pedoman, dan tambahan praktik terbaik mungkin perlu dikembangkan untuk mendukung implementasi teknis yang lebih baik.

Privasi dan keamanan siber memiliki hubungan yang kuat. Kegiatan keamanan siber organisasi juga dapat menciptakan risiko bagi privasi dan kebebasan sipil apabila informasi pribadi digunakan,

dikumpulkan, diproses, dipelihara, atau diungkapkan. Contoh: kegiatan keamanan siber yang mengakibatkan pengumpulan berlebihan atau penyimpanan berlebihan informasi pribadi; pengungkapan atau penggunaan informasi pribadi yang tidak terkait dengan kegiatan keamanan siber; dan kegiatan mitigasi keamanan siber yang mengakibatkan penolakan pelayanan atau dampak serupa lain yang berpotensi merugikan, termasuk beberapa jenis deteksi atau pemantauan insiden yang dapat menghambat kebebasan berekspresi atau berkumpul.

Pemerintah dan agennya bertanggung jawab melindungi kebebasan sipil yang timbul dari kegiatan keamanan siber. Sebagaimana direferensikan dalam metodologi di bawah ini, pemerintah atau agennya yang memiliki atau mengoperasikan Infrastruktur Kritis harus memiliki proses yang tersedia untuk mendukung kepatuhan kegiatan keamanan siber terhadap hukum, peraturan, dan persyaratan Konstitusional tentang privasi yang berlaku.

Untuk mengatasi implikasi privasi, organisasi dapat mempertimbangkan bagaimana program keamanan sibernya dapat memasukkan prinsip-prinsip privasi seperti: minimalisasi data dalam pengumpulan, pengungkapan, dan penyimpanan materi informasi pribadi yang terkait dengan insiden keamanan siber; batasan penggunaan di luar kegiatan keamanan siber atas informasi yang dikumpulkan secara khusus untuk kegiatan keamanan siber; transparansi untuk kegiatan keamanan siber tertentu; persetujuan individu dan ganti rugi untuk dampak merugikan yang timbul dari penggunaan informasi pribadi dalam kegiatan keamanan siber; kualitas, integritas, dan keamanan data; dan akuntabilitas serta pengauditan.

Saat menilai Inti Kerangka Kerja pada Lampiran A, organisasi dapat mempertimbangkan proses dan kegiatan berikut ini sebagai cara untuk mengatasi implikasi privasi dan kebebasan sipil yang disebutkan di atas:

Tata Kelola risiko keamanan siber

- Penilaian risiko keamanan siber dan respons potensi risiko organisasi mempertimbangkan implikasi privasi dari program keamanan sibernya.
- Individu yang memiliki tanggung jawab privasi terkait keamanan siber melapor kepada manajemen yang sesuai dan terlatih dengan baik.
- Berlaku proses untuk mendukung kepatuhan kegiatan keamanan siber terhadap hukum, peraturan, dan persyaratan Konstitusional tentang privasi yang berlaku.
- Berlaku proses untuk menilai pelaksanaan tindakan dan kendali organisasi di atas.

Pendekatan terhadap identifikasi, otentikasi, dan otorisasi individu untuk mengakses aset dan sistem organisasi

- Diambil langkah untuk mengidentifikasi dan mengatasi implikasi privasi manajemen identitas dan tindakan kendali akses sejauh melibatkan pengumpulan, pengungkapan, atau penggunaan informasi pribadi.

Pengukuran kesadaran dan pelatihan

- Informasi yang berlaku dari kebijakan privasi organisasi dimasukkan dalam kegiatan pelatihan dan kesadaran tenaga kerja keamanan siber.
- Penyedia layanan yang memberikan layanan terkait keamanan siber untuk organisasi diinformasikan tentang kebijakan privasi organisasi yang berlaku.

Deteksi kegiatan anomali dan pemantauan sistem dan aset

- Terdapat proses untuk melakukan peninjauan privasi atas deteksi kegiatan anomali dan pemantauan keamanan siber organisasi.

Kegiatan respons, termasuk berbagi informasi atau upaya mitigasi lainnya

- Terdapat proses untuk menilai dan mengatasi apakah, kapan, bagaimana, dan sejauh mana informasi pribadi dibagikan di luar organisasi sebagai bagian dari kegiatan berbagi keamanan siber informasi.
- Terdapat proses untuk melakukan peninjauan privasi atas upaya mitigasi keamanan siber organisasi.

4.0 Penilaian Risiko Keamanan Siber Mandiri berdasar Kerangka Kerja

Kerangka Kerja Keamanan Siber dirancang untuk mengurangi risiko dengan meningkatkan manajemen risiko keamanan siber terhadap tujuan organisasi. Idealnya, organisasi yang menggunakan Kerangka Kerja akan mampu mengukur dan menetapkan nilai terhadap risikonya bersama dengan biaya dan manfaat langkah yang diambil untuk mengurangi level risiko berterima. Semakin baik organisasi mampu mengukur risiko, biaya, dan manfaat strategi dan langkah keamanan sibernya, semakin rasional, efektif, dan bernilai pendekatan dan investasi keamanan sibernya.

Seiring waktu, penilaian diri dan pengukuran seharusnya meningkatkan pengambilan keputusan tentang prioritas investasi. Misalnya, mengukur - atau setidaknya menggolongkan secara kuat - aspek-aspek kondisi dan tren keamanan siber organisasi seiring waktu dapat memungkinkan organisasi itu memahami dan menyampaikan informasi risiko yang berarti kepada dependen, pemasok, pembeli, dan pihak lain. Organisasi dapat mencapai hal ini secara internal atau dengan mengupayakan penilaian pihak ketiga. Bila dilakukan dengan benar dan dengan apresiasi batasan, pengukuran-pengukuran ini dapat memberikan dasar untuk hubungan yang kuat dan terpercaya, baik di dalam maupun di luar organisasi.

Untuk mengukur keefektifan investasi, terlebih dahulu organisasi harus memiliki pemahaman yang jelas mengenai tujuan organisasinya, hubungan antara tujuan itu dan hasil keamanan siber yang mendukung, dan bagaimana hasil-hasil keamanan siber yang terpisah itu diimplementasikan dan dikelola. Meskipun pengukuran semua item itu berada di luar lingkup Kerangka Kerja, hasil keamanan siber dari Inti Kerangka Kerja mendukung penilaian diri atas keefektifan investasi dan kegiatan keamanan siber dengan cara berikut ini:

- Membuat pilihan tentang perbedaan apa bagian operasi keamanan siber seharusnya mempengaruhi pilihan Pelaksanaan Target level,
- Mengevaluasi pendekatan manajemen risiko keamanan siber organisasi dengan menentukan level implementasi yang saat ini sedang berjalan,
- Memprioritaskan hasil keamanan siber dengan mengembangkan Profil Target,
- Menentukan derajat di mana langkah keamanan siber spesifik mencapai hasil keamanan siber yang diinginkan dengan menilai Profil Saat Ini, dan
- Mengukur derajat pelaksanaan untuk katalog kendali atau panduan teknis yang tercantum sebagai Referensi Informasi.

Pengembangan matriks kinerja keamanan siber berkembang. Organisasi harus bijaksana, kreatif, dan hati-hati tentang cara menggunakan pengukuran untuk mengoptimalkan penggunaan, sekaligus menghindari ketergantungan pada indikator buatan dari keadaan dan kemajuan saat ini dalam meningkatkan manajemen risiko keamanan siber. Menilai risiko siber memerlukan disiplin dan harus ditinjau kembali secara berkala. Setiap kali pengukuran digunakan sebagai bagian dari proses Kerangka Kerja, organisasi didorong untuk mengidentifikasi secara jelas dan mengetahui mengapa pengukuran-pengukuran ini penting dan bagaimana pengukuran-pengukuran ini berkontribusi terhadap keseluruhan manajemen risiko keamanan siber. Organisasi juga harus mengetahui dengan baik tentang batasan pengukuran yang digunakan.

Misalnya, melacak tindakan keamanan dan hasil bisnis dapat memberikan pengetahuan yang mendalam yang bermanfaat tentang bagaimana perubahan dalam kendali keamanan granular mempengaruhi penyelesaian tujuan organisasi. Memverifikasi pencapaian beberapa tujuan organisasi membutuhkan analisis data hanya setelah tujuan itu telah tercapai. Jenis ukuran yang tertinggal ini lebih mutlak.

Namun, biasanya lebih bernilai untuk menilai apakah risiko keamanan siber mungkin terjadi, dan dampak yang dihasilkannya, menggunakan ukuran yang terkemuka.

Organisasi didorong untuk berinovasi dan menyesuaikan cara mereka memasukkan pengukuran ke dalam aplikasi Kerangka Kerjanya dengan apresiasi penuh dari kemanfaatan dan batasannya.

Lampiran A: Inti Kerangka Kerja

Lampiran ini menyajikan Inti Kerangka Kerja: daftar Fungsi, Kategori, Sub Kategori, dan Referensi Informasi yang menguraikan kegiatan keamanan siber spesifik yang sudah umum di semua sektor Infrastruktur Kritis. Format presentasi yang dipilih untuk Inti Kerangka Kerja tidak menyarankan urutan pelaksanaan spesifik atau menyiratkan derajat kepentingan Kategori, Sub Kategori, dan Referensi Informasi. Inti Kerangka Kerja yang disajikan dalam Lampiran ini menyajikan kembali set umum kegiatan untuk pengelolaan risiko keamanan siber. Meskipun Kerangka Kerja tidak menyeluruh, namun dapat diperluas, sehingga memungkinkan organisasi, sektor, dan entitas lain menggunakan Sub Kategori dan Referensi Informasi yang tepat biaya dan efisien dan yang memungkinkan mereka mengelola risiko keamanan sibernya. Kegiatan dapat dipilih dari Inti Kerangka Kerja selama proses pembuatan Profil dan tambahan Kategori, Sub Kategori, dan Referensi Informasi dapat ditambahkan ke Profil. Proses manajemen risiko organisasi, persyaratan hukum/regulasi, tujuan bisnis/misi, dan rintangan organisasi memandu pemilihan kegiatan-kegiatan ini selama pembuatan Profil. Informasi pribadi dianggap sebagai komponen data atau aset yang direferensikan dalam Kategori saat menilai risiko dan perlindungan keamanan.

Meskipun hasil yang dimaksudkan yang diidentifikasi dalam Fungsi, Kategori, dan Sub Kategori sama untuk IT dan ICS, lingkungan operasional dan pertimbangan untuk IT dan ICS berbeda. ICS memiliki efek langsung pada dunia fisik, termasuk potensi risiko bagi kesehatan dan keselamatan individu, dan dampak pada lingkungan. Selain itu, ICS memiliki persyaratan kinerja dan keandalan unik dibandingkan dengan IT, dan tujuan keselamatan dan efisiensi harus dipertimbangkan saat melaksanakan tindakan keamanan siber.

Demi kemudahan penggunaan, masing-masing komponen Inti Kerangka Kerja diberikan penanda unik. Fungsi dan Kategori masing-masing memiliki penanda abjad unik, seperti ditampilkan pada Tabel 1. Sub Kategori di dalam masing-masing Kategori direferensikan secara numerik; penanda unik untuk setiap Sub Kategori dimasukkan dalam Tabel 2.

Tambahan materi pendukung, termasuk Referensi Informasi, yang terkait dengan Kerangka Kerja dapat ditemukan di situs web NIST di http://www.nist.gov/cyberframework/.

Tabel 1: Pengenal Unik Fungsi dan Kategori

Penanda Unik Fungsi	Fungsi	Penanda Unik Kategori	Kategori
ID	Mengidentifikasi	ID.AM	Manajemen Aset
		ID.BE	Lingkungan Bisnis
		ID.GV	Tata Kelola
		ID.RA	Penilaian Risiko
		ID.RM	Strategi Manajemen Risiko
		ID.SC	Manajemen Risiko Rantai Pasokan
PR	Melindungi	PR.AC	Manajemen Identitas dan Kendali Akses
		PR.AT	Kampanye Kesadaran dan Pelatihan
		PR.DS	Keamanan Data
		PR.IP	Proses dan Prosedur Proteksi Informasi

		PR.MA	Pemeliharaan
		PR.PT	Teknologi Proteksi
DE	Mendeteksi	DE.AE	Anomali dan Kejadian Keamanan
		DE.CM	Pemantauan Keamanan Berkelanjutan
		DE.DP	Proses Deteksi
RS	Merespons	RS.RP	Perencanaan Respons
		RS.CO	Komunikasi
		RS.AN	Analisis
		RS.MI	Mitigasi
		RS.IM	Peningkatan
RC	Memulihkan	RC.RP	Perencanaan Pemulihan
		RC.IM	Pengembangan
		RC.CO	Komunikasi

Tabel 2: Inti Kerangka Kerja

Fungsi	Kategori	Sub Kategori	Referensi Informasi
MENGIDENTIFIKASI (ID)	**Manajemen Aset (ID.AM):** Data, personel, perangkat, sistem, dan infrastruktur yang memungkinkan organisasi mencapai tujuan bisnis teridentifikasi dan dikelola sesuai dengan kepentingan relatifnya terhadap tujuan organisasi dan strategi risiko organisasi.	**ID.AM-1:** Perangkat dan sistem fisik di dalam organisasi diinventarisir	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Platform perangkat lunak dan aplikasi di dalam organisasi diinventarisir	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Komunikasi organisasi dan alur data dipetakan	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: Sistem informasi eksternal dikatalogkan	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.04, DSS01.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Sumber daya (misalnya, perangkat keras, perangkat, data, waktu, personel, dan perangkat lunak) diprioritaskan berdasarkan klasifikasi, kekritisan, dan nilai bisnisnya	· **CIS CSC** 13, 14 · **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Peran dan tanggung jawab keamanan siber untuk seluruh tenaga kerja dan pemangku kepentingan pihak ketiga (misalnya, pemasok, pelanggan, mitra) ditetapkan	· **CIS CSC** 17, 19 · **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Lingkungan Bisnis (ID.BE): Misi, tujuan, pemangku kepentingan, dan kegiatan organisasi	**ID.BE-1:** Peran organisasi dalam rantai pasokan diidentifikasi dan dikomunikasikan	· **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2

	dipahami dan diprioritaskan; informasi ini digunakan untuk memberitahukan peran, tanggung jawab, dan keputusan manajemen risiko keamanan siber.		· **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: Tempat organisasi dalam Infrastruktur Kritis dan sektor industrinya diidentifikasi dan dikomunikasikan	· **COBIT 5** APO02.06, APO03.01 · **ISO/IEC 27001:2013** klausul 4.1 · **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Prioritas untuk misi, tujuan, dan kegiatan organisasi ditetapkan dan dikomunikasikan	· **COBIT 5** APO02.01, APO02.06, APO03.01 · **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 · **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Ketergantungan dan fungsi kritis untuk penyerahan layanan kritis ditetapkan	· **COBIT 5** APO10.01, BAI04.02, BAI09.02 · **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 · **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Persyaratan ketahanan untuk mendukung penyerahan layanan kritis ditetapkan untuk semua keadaan operasional (misalnya di bawah paksaan/serangan, selama operasi pemulihan, operasional normal)	· **COBIT 5** BAI03.02, DSS04.02 · **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14
	Tata Kelola (ID.GV): Kebijakan, prosedur, dan proses untuk mengelola dan memantau persyaratan regulasi, hukum, risiko, lingkungan dan operasional organisasi dipahami dan memberitahukan kepada manajemen mengenai manajemen risiko keamanan siber.	**ID.GV-1:** Kebijakan keamanan siber organisasi ditetapkan dan dikomunikasikan	· **CIS CSC** 19 · **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 · **ISA 62443-2-1:2009** 4.3.2.6 · **ISO/IEC 27001:2013** A.5.1.1 · **NIST SP 800-53 Rev. 4** -1 kendali dari semua keluarga kendali keamanan
		ID.GV-2: Peran dan tanggung jawab keamanan siber dikoordinasikan dan diselaraskan dengan peran internal dan mitra eksternal	· **CIS CSC** 19 · **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 · **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
		ID.GV-3: Persyaratan hukum dan regulasi mengenai keamanan siber, termasuk kewajiban privasi dan kebebasan sipil, dipahami dan dikelola	· **CIS CSC** 19 · **COBIT 5** BAI02.01, MEA03.01, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.7 · **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 · **NIST SP 800-53 Rev. 4** -1 kendali dari semua keluarga kendali keamanan
		ID.GV-4: Proses tata kelola dan manajemen	· **COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02

		risiko membicarakan risiko keamanan siber	· **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · **ISO/IEC 27001:2013** klausul 6 · **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	Penilaian Risiko (ID.RA): Organisasi memahami risiko keamanan siber terhadap pengoperasian organisasi termasuk misi, fungsi, citra, atau reputasi), aset organisasi, dan individu.	**ID.RA-1:** Kerentanan aset diidentifikasi dan didokumentasikan	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Intelijen ancaman siber diperoleh dari forum berbagi informasi dan sumber lainnya	· **CIS CSC** 4 · **COBIT 5** BAI08.01 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16
		ID.RA-3: Ancaman, baik internal maupun eksternal, diidentifikasi dan didokumentasikan	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** klausul 6.1.2 · **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Dampak dan kemungkinan potensi bisnis diidentifikasi	· **CIS CSC** 4 · **COBIT 5** DSS04.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013 A.16.1.6,** klausul 6.1.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11
		ID.RA-5: Ancaman, kerentanan, kemungkinan, dan dampak digunakan untuk menentukan risiko	· **CIS CSC** 4 · **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: Respons risiko diidentifikasi dan diprioritaskan	· **CIS CSC** 4 · **COBIT 5** APO12.05, APO13.02 · **ISO/IEC 27001:2013** klausul 6.1.3 · **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Strategi Manajemen Risiko (ID.RM): Prioritas, rintangan, toleransi risiko, dan	**ID.RM-1:** Proses manajemen risiko ditetapkan, dikelola, dan disetujui oleh para	· **CIS CSC** 4 · **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2

	asumsi organisasi ditetapkan dan digunakan untuk mendukung keputusan risiko operasional.	pemangku kepentingan organisasi	· **ISO/IEC 27001:2013** klausul 6.1.3, klausul 8.3, klausul 9.3 · **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Toleransi risiko organisasi ditentukan dan dinyatakan dengan jelas	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.2.6.5 · **ISO/IEC 27001:2013** klausul 6.1.3, klausul 8.3 · **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-3: Penentuan toleransi risiko organisasi diinformasikan oleh perannya dalam Infrastruktur Kritis dan analisis risiko sektor terkait	· **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** klausul 6.1.3, klausul 8.3 · **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11
	Manajemen Risiko Rantai Pasokan (ID.SC): Prioritas, rintangan, toleransi risiko, dan asumsi organisasi ditetapkan dan digunakan untuk mendukung keputusan risiko yang terkait dengan pengelolaan risiko rantai pasokan. Organisasi telah menetapkan dan mengimplementasikan proses untuk mengidentifikasi, menilai dan mengelola risiko rantai pasokan.	**ID.SC-1:** Proses manajemen risiko rantai pasokan siber diidentifikasi, ditetapkan, dinilai, dikelola, dan disetujui oleh para pemangku kepentingan organisasi	· **CIS CSC** 4 · **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Pemasok dan mitra pihak ketiga dari sistem informasi, komponen, dan layanan diidentifikasi, diprioritaskan, dan dinilai menggunakan proses penilaian risiko rantai pasokan siber	· **COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: Kontrak dengan pemasok dan mitra pihak ketiga digunakan untuk mengimplementasikan tindakan yang sesuai yang dirancang untuk memenuhi tujuan program keamanan siber organisasi dan rencana manajemen risiko rantai pasokan siber.	· **COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 · **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Pemasok dan mitra pihak ketiga dinilai secara rutin menggunakan audit, hasil uji, atau bentuk evaluasi	· **COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 · **ISA 62443-2-1:2009** 4.3.2.6.7 · **ISA 62443-3-3:2013** SR 6.1

		lain untuk menegaskan bahwa mereka memenuhi kewajiban kontraktualnya.	· **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: Respons dan perencanaan dan uji pemulihan dilakukan dengan pemasok dan penyedia pihak ketiga	· **CIS CSC** 19, 20 · **COBIT 5** DSS04.04 · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
MELINDUNGI (PR)	**Manajemen Identitas, Otentikasi dan Kendali Akses (PR.AC):** Akses aset fisik dan logis dan sarana terkait terbatas pada pengguna, proses, dan perangkat berizin, dan dikelola sesuai dengan risiko yang dinilai dari akses tak berizin atas kegiatan dan transaksi berizin.	**PR.AC-1:** Identitas dan kredensial dikeluarkan, dikelola, diverifikasi, dicabut, dan diaudit untuk perangkat, pengguna, dan proses terizin	· **CIS CSC** 1, 5, 15, 16 · **COBIT 5** DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.5.1 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Akses fisik aset dikelola dan dilindungi	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 · **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: Akses jarak jauh dikelola	· **CIS CSC** 12 · **COBIT 5** APO13.01, DSS01.04, DSS05.03 · **ISA 62443-2-1:2009** 4.3.3.6.6 · **ISA 62443-3-3:2013** SR 1.13, SR 2.6 · **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Izin dan otorisasi akses dikelola, yang menggabungkan prinsip-prinsip hak istimewa terendah dan pemisahan tugas	· **CIS CSC** 3, 5, 12, 14, 15, 16, 18 · **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.7.3 · **ISA 62443-3-3:2013** SR 2.1 · **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
			· **CIS CSC** 9, 14, 15, 18

		PR.AC-5: Integritas jaringan dilindungi (misalnya, pemisahan jaringan, segmentasi jaringan)	· **COBIT 5** DSS01.05, DSS05.02 · **ISA 62443-2-1:2009** 4.3.3.4 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8 · **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7
		PR.AC-6: Identitas dibuktikan dan terikat dengan kredensial dan ditegaskan dalam interaksi	· **CIS CSC**, 16 · **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 · **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Pengguna, perangkat, dan aset lainnya diotentikasi (misalnya, faktor-tunggal, multi-faktor) sepadan dengan risiko transaksi (misalnya, risiko keamanan dan privasi individu dan risiko organisasi lainnya)	· **CIS CSC** 1, 12, 15, 16 · **COBIT 5** DSS05.04, DSS05.10, DSS06.10 · **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 · **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Pengetahuan dan Pelatihan (PR.AT): Personel dan mitra organisasi diberikan pendidikan pengetahuan keamanan siber dan dilatih untuk menjalankan tugas dan tanggung jawabnya terkait dengan keamanan siber sesuai dengan kebijakan, prosedur, dan perjanjian terkait.	**PR.AT-1:** Semua pengguna mengetahui dan terlatih	· **CIS CSC** 17, 18 · **COBIT 5** APO07.03, BAI05.07 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 · **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Pengguna istimewa memahami peran dan tanggung jawabnya	· **CIS CSC** 5, 17, 18 · **COBIT 5** APO07.02, DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: Pemangku kepentingan pihak ketiga (misalnya, pemasok, pelanggan, mitra) memahami peran dan tanggung jawabnya	· **CIS CSC** 17 · **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16

		PR.AT-4: Eksekutif senior memahami peran dan tanggung jawabnya	· **CIS CSC** 17, 19 · **COBIT 5** EDM01.01, APO01.02, APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-5: Personel fisik dan keamanan siber memahami peran dan tanggung jawabnya	· **CIS CSC** 17 · **COBIT 5** APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, IR-2, PM-13
	Keamanan Data (PR.DS): Informasi dan catatan (data) dikelola sesuai dengan strategi risiko organisasi untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi.	**PR.DS-1:** Data-tak-aktif terlindungi	· **CIS CSC** 13, 14 · **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 · **ISA 62443-3-3:2013** SR 3.4, SR 4.1 · **ISO/IEC 27001:2013** A.8.2.3 · **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28
		PR.DS-2: Data-saat-transit terlindungi	· **CIS CSC** 13, 14 · **COBIT 5** APO01.06, DSS05.02, DSS06.06 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12
		PR.DS-3: Aset dikelola secara formal melalui penghapusan, transfer, dan disposisi	· **CIS CSC** 1 · **COBIT 5** BAI09.03 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 · **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: Kapasitas yang memadai untuk memastikan ketersediaan terjaga	· **CIS CSC** 1, 2, 13 · **COBIT 5** APO13.01, BAI04.04 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 · **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Perlindungan dari kebocoran data diimplementasikan	· **CIS CSC** 13 · **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 · **ISA 62443-3-3:2013** SR 5.2 · **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4,

			A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Mekanisme pengecekan integritas digunakan untuk memverifikasi integritas perangkat lunak, perangkat tegar, dan informasi	· **CIS CSC** 2, 3 · **COBIT 5** APO01.06, BAI06.01, DSS06.02 · **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 · **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** SC-16, SI-7
		PR.DS-7: Lingkungan pengembangan dan pengujian terpisah dari lingkungan produksi	· **CIS CSC** 18, 20 · **COBIT 5** BAI03.08, BAI07.04 · **ISO/IEC 27001:2013** A.12.1.4 · **NIST SP 800-53 Rev. 4** CM-2
		PR.DS-8: Mekanisme pengetesan integritas digunakan untuk memverifikasi integritas perangkat keras	· **COBIT 5** BAI03.05 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISO/IEC 27001:2013** A.11.2.4 · **NIST SP 800-53 Rev. 4** SA-10, SI-7
	Proses dan Prosedur Perlindungan Informasi (PR.IP): Kebijakan (yang membahas tujuan, ruang lingkup, tanggung jawab, komitmen manajemen, dan koordinasi antar entitas organisasi), proses, dan prosedur keamanan mengelola perlindungan sistem dan aset informasi.	**PR.IP-1:** Konfigurasi dasar teknologi informasi/sistem kendali industri diciptakan dan dipelihara dengan menggabungkan prinsip-prinsip keamanan (misalnya konsep fungsionalitas minimum)	· **CIS CSC** 3, 9, 11 · **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: Siklus Hidup Pengembangan Sistem untuk mengelola sistem diimplementasikan	· **CIS CSC** 18 · **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 · **ISA 62443-2-1:2009** 4.3.4.3.3 · **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: Proses kendali perubahan konfigurasi berjalan	· **CIS CSC** 3, 11 · **COBIT 5** BAI01.06, BAI06.01 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
			· **CIS CSC** 10

		PR.IP-4: Pencadangan informasi dilakukan, dipelihara, dan diuji	· **COBIT 5** APO13.01, DSS01.01, DSS04.07 · **ISA 62443-2-1:2009** 4.3.4.3.9 · **ISA 62443-3-3:2013** SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 · **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
		PR.IP-5: Kebijakan dan regulasi mengenai lingkungan operasional fisik untuk aset organisasi terpenuhi	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data dimusnahkan sesuai kebijakan	· **COBIT 5** BAI09.03, DSS05.06 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · **NIST SP 800-53 Rev. 4** MP-6
		PR.IP-7: Proses perlindungan ditingkatkan	· **COBIT 5** APO11.06, APO12.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 · **ISO/IEC 27001:2013 A.16.1.6,** klausul 9, klausul 10 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Keefektifan teknologi proteksi dibagikan	· **COBIT 5** BAI08.04, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Rencana respons (Respons Insiden dan Kelanjutan Bisnis) dan rencana pemulihan (Pemulihan Insiden dan Pemulihan Bencana) berjalan dan dikelola	· **CIS CSC** 19 · **COBIT 5** APO12.06, DSS04.03 · **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: Rencana respons dan pemulihan diuji	· **CIS CSC** 19, 20 · **COBIT 5** DSS04.04 · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
		PR.IP-11: Keamanan siber dimasukkan dalam praktik sumber daya	· **CIS CSC** 5, 16 · **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05

		manusia (misalnya, pencabutan akses, penyaringan personel)	· **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 · **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 · **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
		PR.IP-12: Rencana manajemen kerentanan dikembangkan dan diimplementasikan	· **CIS CSC** 4, 18, 20 · **COBIT 5** BAI03.10, DSS05.01, DSS05.02 · **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 · **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Pemeliharaan (PR.MA): Pemeliharaan dan perbaikan kendali industri dan komponen sistem informasi dilakukan sesuai dengan kebijakan dan prosedur.	**PR.MA-1:** Pemeliharaan dan perbaikan aset organisasi dilakukan dan dicatat, dengan alat yang disetujui dan terkendali	· **COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 · **ISA 62443-2-1:2009** 4.3.3.3.7 · **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 · **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6
		PR.MA-2: Pemeliharaan jarak jauh aset organisasi disetujui, dicatat, dan dilakukan sedemikian rupa sehingga dapat mencegah akses tanpa izin	· **CIS CSC** 3, 5 · **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 · **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 · **NIST SP 800-53 Rev. 4** MA-4
	Teknologi Perlindungan (PR.PT): Solusi keamanan teknis dikelola untuk memastikan keamanan dan ketahanan sistem dan aset, sesuai dengan kebijakan, prosedur, dan perjanjian terkait.	**PR.PT-1:** Catatan audit/log ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan	· **CIS CSC** 1, 3, 5, 6, 14, 15, 16 · **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · **NIST SP 800-53 Rev. 4** AU Keluarga
		PR.PT-2: Media-dapat-dilepas terlindungi dan penggunaannya terbatas sesuai dengan kebijakan	· **CIS CSC** 8, 13 · **COBIT 5** APO13.01, DSS05.02, DSS05.06 · **ISA 62443-3-3:2013** SR 2.3 · **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · **NIST SP 800-53 Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: Prinsip fungsionalitas minimum digabungkan dengan mengonfigurasi sistem	· **CIS CSC** 3, 11, 14 · **COBIT 5** DSS05.02, DSS05.05, DSS06.06 · **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4,

		untuk memberikan hanya kemampuan mendasar	4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · **ISO/IEC 27001:2013** A.9.1.2 · **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Komunikasi dan jaringan kendali terlindungi	· **CIS CSC** 8, 12, 15 · **COBIT 5** DSS05.02, APO13.01 · **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Mekanisme (misalnya, gagal aman, pengimbang beban, *hot swap*) diimplementasikan untuk mencapai persyaratan ketahanan dalam situasi normal dan situasi yang merugikan	· **COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 · **ISA 62443-2-1:2009** 4.3.2.5.2 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
MENDETEKSI (DE)	**Anomali dan Peristiwa (DE.AE):** Kegiatan anomali terdeteksi dan potensi dampak peristiwa dipahami.	**DE.AE-1:** Garis dasar pengoperasian jaringan dan alur data yang diharapkan untuk pengguna dan sistem ditetapkan dan dikelola	· **CIS CSC** 1, 4, 6, 12, 13, 15, 16 · **COBIT 5** DSS03.01 · **ISA 62443-2-1:2009** 4.4.3.3 · **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Kejadian keamanan yang terdeteksi dianalisis untuk memahami target dan metode serangan	· **CIS CSC** 3, 6, 13, 15 · **COBIT 5** DSS05.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Data kejadian dikumpulkan dan dihubungkan dari	· **CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 · **COBIT 5** BAI08.02

		beberapa sumber dan sensor	· **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Dampak peristiwa ditentukan	· **CIS CSC** 4, 6 · **COBIT 5** APO12.06, DSS03.01 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Ambang batas peringatan insiden ditetapkan	· **CIS CSC** 6, 19 · **COBIT 5** APO12.06, DSS03.01 · **ISA 62443-2-1:2009** 4.2.3.10 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Pemantauan Keamanan Berkelanjutan (DE.CM): Sistem informasi dan aset dipantau untuk mengidentifikasi peristiwa keamanan siber dan memverifikasi keefektifan tindakan perlindungan.	**DE.CM-1:** Jaringan dipantau untuk mendeteksi potensi peristiwa keamanan siber	· **CIS CSC** 1, 7, 8, 12, 13, 15, 16 · **COBIT 5** DSS01.03, DSS03.05, DSS05.07 · **ISA 62443-3-3:2013** SR 6.2 · **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: Lingkungan fisik dipantau untuk mendeteksi potensi peristiwa keamanan siber	· **COBIT 5** DSS01.04, DSS01.05 · **ISA 62443-2-1:2009** 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 · **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Kegiatan personel dipantau untuk mendeteksi potensi peristiwa keamanan siber	· **CIS CSC** 5, 7, 14, 16 · **COBIT 5** DSS05.07 · **ISA 62443-3-3:2013** SR 6.2 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 · **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Kode berbahaya dideteksi	· **CIS CSC** 4, 7, 8, 12 · **COBIT 5** DSS05.01 · **ISA 62443-2-1:2009** 4.3.4.3.8 · **ISA 62443-3-3:2013** SR 3.2 · **ISO/IEC 27001:2013** A.12.2.1 · **NIST SP 800-53 Rev. 4** SI-3, SI-8
		DE.CM-5: Kode Bergerak yang tak berizin dideteksi	· **CIS CSC** 7, 8 · **COBIT 5** DSS05.01 · **ISA 62443-3-3:2013** SR 2.4 · **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 · **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44
			· **COBIT 5** APO07.06, APO10.05

		DE.CM-6: Kegiatan penyedia layanan eksternal dipantau untuk mendeteksi potensi peristiwa keamanan siber	· **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Pemantauan personel, koneksi, perangkat, dan perangkat lunak yang tak berizin dilakukan	· **CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 · **COBIT 5** DSS05.02, DSS05.05 · **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Pemindaian kerentanan dilakukan	· **CIS CSC** 4, 20 · **COBIT 5** BAI03.10, DSS05.01 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-5
	Proses Deteksi (DE.DP): Proses dan prosedur deteksi dipelihara dan diuji untuk memastikan diketahuinya peristiwa anomali.	**DE.DP-1:** Peran dan tanggung jawab pendeteksian ditetapkan dengan baik untuk memastikan pertanggungjawaban	· **CIS CSC** 19 · **COBIT 5** APO01.02**,** DSS05.01, DSS06.03 · **ISA 62443-2-1:2009** 4.4.3.1 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Kegiatan pendeteksian mematuhi semua persyaratan yang berlaku	· **COBIT 5** DSS06.01, MEA03.03, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 · **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: Proses pendeteksian diuji	· **COBIT 5** APO13.02, DSS05.02 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.14.2.8 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Informasi pendeteksian kejadian keamanan diberitahukan	· **CIS CSC** 19 · **COBIT 5** APO08.04, APO12.06, DSS02.05 · **ISA 62443-2-1:2009** 4.3.4.5.9 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 · **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Proses pendeteksian selalu ditingkatkan	· **COBIT 5** APO11.06, APO12.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6

			· **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
MERESPONS (RS)	**Perencanaan Respons (RS.RP):** Proses dan prosedur respons dilaksanakan dan dipertahankan, untuk memastikan respons mendeteksi insiden keamanan siber.	**RS.RP-1:** Rencana respons dilakukan saat atau setelah insiden	· **CIS CSC** 19 · **COBIT 5** APO12.06, BAI01.10 · **ISA 62443-2-1:2009** 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Komunikasi (RS.CO): Kegiatan respons dikoordinasikan dengan para pemangku kepentingan internal dan eksternal (misalnya dukungan eksternal untuk lembaga penegak hukum).	**RS.CO-1:** Personel mengetahui perannya dan urutan pengoperasian bila respons diperlukan	· **CIS CSC** 19 · **COBIT 5** EDM03.02, APO01.02, APO12.03 · **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Insiden dilaporkan sesuai dengan kriteria yang ditetapkan	· **CIS CSC** 19 · **COBIT 5** DSS01.03 · **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 · **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Informasi dibagikan sesuai dengan rencana respons	· **CIS CSC** 19 · **COBIT 5** DSS03.04 · **ISA 62443-2-1:2009** 4.3.4.5.2 · **ISO/IEC 27001:2013 A.16.1.2, klausul 7.4, klausul 16.1.2** · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Koordinasi dengan para pemangku kepentingan sesuai dengan rencana respons	· **CIS CSC** 19 · **COBIT 5** DSS03.04 · **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013 klausul 7.4** · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: Berbagi informasi secara sukarela terjadi dengan para pemangku kepentingan eksternal untuk mencapai kesadaran situasi keamanan siber yang lebih luas	· **CIS CSC** 19 · **COBIT 5** BAI08.04 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Analisis (RS.AN): Analisis dilakukan untuk memastikan kegiatan respons dan pemulihan dukungan efektif.	**RS.AN-1:** Pemberitahuan dari sistem pendeteksian diselidiki	· **CIS CSC** 4, 6, 8, 19 · **COBIT 5** DSS02.04, DSS02.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 6.1

			· **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: Dampak insiden dipahami	· **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 · **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Forensik dilakukan	· **COBIT 5** APO12.06, DSS03.02, DSS05.07 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 · **ISO/IEC 27001:2013** A.16.1.7 · **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Insiden dikategorikan sesuai dengan rencana respons	· **CIS CSC** 19 · **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Proses ditetapkan untuk menerima, menganalisis dan merespons kerentanan yang diungkapkan kepada organisasi dari sumber internal dan eksternal (misalnya pengujian internal, buletin keamanan, atau dari peneliti keamanan)	· **CIS CSC** 4, 19 · **COBIT 5** EDM03.02, DSS05.07 · **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Mitigasi (RS.MI): Kegiatan dilakukan untuk mencegah meluasnya kejadian keamanan, memitigasi efeknya, dan mengatasi insiden.	**RS.MI-1:** Insiden diisolasi	· **CIS CSC** 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-2: Insiden di mitigasi	· **CIS CSC** 4, 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: Kerentanan yang baru diidentifikasi	· **CIS CSC** 4 · **COBIT 5** APO12.06

		dimitigasi atau didokumentasikan sebagai risiko yang diterima	· **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Penyempurnaan (RS.IM): Kegiatan respons organisasi ditingkatkan dengan menggabungkan pelajaran yang dipetik dari kegiatan deteksi/respons saat ini dan sebelumnya.	**RS.IM-1:** Rencana respons menggabungkan pelajaran yang dipetik dari insiden sebelumnya	· **COBIT 5** BAI01.13 · **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 · **ISO/IEC 27001:2013 A.16.1.6, klausul 10** · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Strategi respons diperbarui	· **COBIT 5** BAI01.13, DSS04.08 · **ISO/IEC 27001:2013 A.16.1.6, klausul 10** · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
MEMULIHKAN (RC)	**Perencanaan Pemulihan (RC.RP):** Proses dan prosedur pemulihan dilaksanakan dan dipelihara untuk memastikan restorasi sistem atau aset yang terdampak oleh insiden keamanan siber.	**RC.RP-1:** Rencana pemulihan dilakukan saat atau setelah insiden keamanan siber	· **CIS CSC** 10 · **COBIT 5** APO12.06, DSS02.05, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Penyempurnaan (RC.IM): Perencanaan dan proses pemulihan ditingkatkan dengan menggabungkan pelajaran yang dipetik ke dalam kegiatan mendatang.	**RC.IM-1:** Rencana pemulihan menggabungkan pelajaran yang dipetik	· **COBIT 5** APO12.06, BAI05.07, DSS04.08 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013 A.16.1.6, klausul 10** · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Strategi pemulihan diperbarui	· **COBIT 5** APO12.06, BAI07.08 · **ISO/IEC 27001:2013 A.16.1.6, klausul 10** · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Komunikasi (RC.CO): Kegiatan restorasi dikoordinasikan dengan pihak internal dan eksternal (misalnya pusat koordinasi, Penyedia Layanan Internet, pemilik sistem yang diserang, korban, dan CSIRT lainnya, dan vendor).	**RC.CO-1:** Hubungan publik dikelola	· **COBIT 5** EDM03.02 · **ISO/IEC 27001:2013 A.6.1.4, klausul 7.4**
		RC.CO-2: Reputasi diperbaiki setelah insiden	· **COBIT 5** MEA03.02 · **ISO/IEC 27001:2013 klausul 7.4**
		RC.CO-3: Kegiatan pemulihan diberitahukan kepada para pemangku kepentingan internal dan eksternal serta tim eksekutif dan manajemen	· **COBIT 5** APO12.06 · **ISO/IEC 27001:2013 klausul 7.4** · **NIST SP 800-53 Rev. 4** CP-2, IR-4

Informasi mengenai Referensi Informasi yang diuraikan dalam Lampiran A dapat ditemukan di lokasi berikut ini:

- Tujuan Kendali untuk Informasi dan Teknologi Terkait (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- Kendali Keamanan Kritis CIS untuk Pertahanan Siber Efektif (Kendali CIS): https://www.cisecurity.org
- American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009, Keamanan untuk Sistem Otomatisasi dan Kendali Industri: Membangun Program Keamanan Sistem Otomatisasi dan Kendali Industri: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
- ANSI/ISA-62443-3-3 (99.03.03)-2013, Keamanan untuk Sistem Otomatisasi dan kendali Industri: Persyaratan Keamanan dan level Keamanan Sistem: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
- ISO/IEC 27001, Teknologi informasi -- Teknik keamanan -- Sistem manajemen keamanan informasi -- Persyaratan: https://www.iso.org/standard/54534.html
- NIST SP 800-53 Rev. 4 - Publikasi Khusus NIST 800-53 Revisi 4, Kendali keamanan dan Privasi untuk Sistem dan Organisasi Informasi Federal, April 2013 (termasuk pemutakhiran tanggal 22 Januari 2015). https://doi.org/10.6028/NIST.SP.800-53r4. Referensi Informasi hanya dipetakan hingga level kendali, meskipun peningkatan kendali mungkin berguna dalam mencapai hasil sub kategori.

Pemetaan antara Inti Kerangka Kerja Sub Kategori dan bagian yang disebutkan dalam Referensi Informasi tidak dimaksudkan untuk secara definitif menentukan apakah bagian-bagian yang disebutkan dalam Referensi Informasi memberikan hasil Sub Kategori yang diinginkan.

Referensi Informasi tidak bersifat eksklusif, di mana tidak setiap unsur (misalnya, kendali, persyaratan) Referensi Informasi yang dimaksud dipetakan ke Inti Kerangka Kerja Sub Kategori.

Lampiran B: Glosarium

Lampiran ini mendefinisikan istilah terpilih yang digunakan dalam publikasi.

Tabel 3: Glosarium Kerangka Kerja

Pembeli	Orang atau organisasi yang mengkonsumsi produk atau layanan yang diberikan.
Kategori	Subdivisi suatu Fungsi menjadi kelompok hasil keamanan siber, yang terikat erat dengan kebutuhan terprogram dan kegiatan tertentu. Contoh Kategori termasuk “Manajemen Aset,” “Manajemen Identitas dan Kendali Akses,” dan “Proses Deteksi.”
Infrastruktur Kritis	Sistem dan aset, fisik atau virtual, yang vital bagi Amerika Serikat sehingga ketidakmampuan atau hancurnya sistem dan aset tersebut akan berdampak melemahkan keamanan siber, keamanan ekonomi nasional, kesehatan atau keselamatan umum nasional, atau kombinasinya.
Keamanan Siber	Proses perlindungan informasi dengan mencegah, mendeteksi, dan merespons serangan.
Peristiwa Keamanan Siber	Perubahan keamanan siber yang dapat berdampak pada operasi organisasi (termasuk misi, kemampuan, atau reputasi).
Insiden Keamanan Siber	Peristiwa keamanan siber - yang telah ditentukan berdampak pada organisasi - yang mendorong perlunya respons dan pemulihan.
(Fungsi) Mendeteksi	Mengembangkan dan melaksanakan kegiatan yang sesuai untuk mengidentifikasi kejadian peristiwa keamanan siber.
Kerangka Kerja	Pendekatan berbasis risiko untuk mengurangi risiko keamanan siber yang terdiri dari tiga bagian: Inti Kerangka Kerja, Profil Kerangka Kerja, dan level Pelaksanaan Kerangka Kerja. Juga dikenal sebagai “Kerangka Kerja Keamanan Siber.”
Inti Kerangka Kerja	Serangkaian kegiatan keamanan siber dan referensi yang sudah umum antar sektor Infrastruktur Kritis dan diatur seputar hasil tertentu. Inti Kerangka Kerja terdiri dari empat jenis unsur: Fungsi, Kategori, Sub Kategori, dan Referensi Informasi.
Tingkatan/Level Pelaksanaan Kerangka Kerja	Lensa untuk melihat karakteristik pendekatan risiko organisasi—bagaimana organisasi melihat risiko keamanan siber dan proses yang digunakan untuk mengelola risiko itu.
Profil Kerangka Kerja	Representasi dari hasil yang telah dipilih sistem atau organisasi tertentu dari Kerangka Kerja Kategori dan Sub Kategori.

Fungsi	Salah satu komponen utama Kerangka Kerja. Fungsi memberikan level struktur tertinggi untuk mengatur kegiatan keamanan siber dasar ke dalam Kategori dan Sub Kategori. Kelima fungsinya adalah Mengidentifikasi, Melindungi, Mendeteksi, Merespons, dan Memulihkan.
Mengidentifikasi (Fungsi)	Mengembangkan pemahaman organisasi untuk mengelola risiko keamanan siber atas sistem, aset, data, dan kemampuan.
Referensi Informasi	Bagian spesifik dari standar, pedoman, dan praktik yang sudah umum di antara sektor Infrastruktur Kritis yang mengilustrasikan metode untuk mencapai hasil yang berkaitan dengan masing-masing Sub Kategori. Contoh Referensi Informasi adalah ISO/IEC 27001 Control A.10.8.3, yang mendukung Sub Kategori “Data-saat-transit dilindungi” dari Kategori “Keamanan Data” dalam fungsi “Melindungi”.
Kode Bergerak	Program (misalnya, skrip, makro, atau instruksi portabel lain) yang dapat dikirimkan tanpa berubah ke kumpulan platform heterogen dan dieksekusi dengan semantik yang identik.
Melindungi (Fungsi)	Mengembangkan dan melaksanakan pengamanan yang sesuai untuk memastikan diberikannya layanan Infrastruktur Kritis.
Pengguna Istimewa	Pengguna yang diotorisasi (dan, oleh karenanya, terpercaya) melakukan fungsi terkait keamanan yang otoritas tersebut tidak diberikan kepada pengguna biasa.
Memulihkan (Fungsi)	Mengembangkan dan melaksanakan kegiatan yang sesuai untuk memelihara rencana ketahanan dan memulihkan kemampuan atau layanan yang terganggu karena peristiwa keamanan siber.
Merespons (Fungsi)	Mengembangkan dan melaksanakan kegiatan yang sesuai untuk mengambil tindakan mengenai peristiwa keamanan siber yang terdeteksi.
Risiko	Ukuran sejauh mana suatu entitas terancam oleh potensi keadaan atau peristiwa, dan khususnya fungsi dari: (i) dampak merugikan yang akan timbul bila keadaan atau peristiwa tersebut terjadi; dan (ii) kemungkinan kejadian.
Manajemen Risiko	Proses mengidentifikasi, menilai, dan merespons risiko.
Sub Kategori	Subdivisi Kategori menjadi hasil spesifik dari kegiatan teknis dan/atau manajemen. Contoh Sub Kategori termasuk “Sistem informasi eksternal

	dikatalogkan," "Data tidak aktif dilindungi," dan "Pemberitahuan untuk sistem deteksi diselidiki."
Pemasok	Penyedia produk dan layanan yang digunakan untuk tujuan internal organisasi (misalnya, infrastruktur IT) atau diintegrasikan ke dalam produk layanan yang diberikan kepada Pembeli organisasi itu.
Taksonomi	Skema klasifikasi.

Lampiran C: Akronim

Lampiran ini mendefinisikan akronim terpilih yang digunakan dalam publikasi.

ANSI	American National Standards Institute
CEA	Undang-Undang Peningkatan Keamanan Siber Tahun 2014
CIS	Pusat Keamanan Internet
COBIT	Sasaran Kendali Informasi dan Teknologi Terkait
CPS	Sistem siber-ke-fisik
CSC	Kendali Keamanan Kritis
DHS	Kementerian Keamanan Dalam Negeri
EO	Perintah Eksekutif
ICS	Sistem Kendali Industri
IEC	Komisi Elektroteknik Internasional
IoT	Internet untuk Segala
IR	Laporan antar Agensi
ISA	Masyarakat Otomatisasi Internasional
ISAC	Pusat Berbagi dan Analisis Informasi
ISAO	Organisasi Berbagi dan Analisis Informasi
ISO	Organisasi Standarisasi Internasional
IT	Teknologi Informasi
NIST	National Institute of Standards and Technology
OT	Teknologi Operasional
PII	Informasi Identitas Pribadi
RFI	Permintaan Informasi
RMP	Proses Manajemen Risiko
MRRP	Manajemen Risiko Rantai Pasokan
SP	Publikasi Khusus