

Framework for Improving
Critical Infrastructure Cybersecurity

Executive Summary

Keamanan nasional dan ekonomi dari Amerika Serikat tergantung pada fungsi yang dapat diandalkan infrastruktur yang kritis. Ancaman Cybersecurity mengeksplorasi peningkatan kompleksitas dan konektivitas sistem infrastruktur yang kritis, meletakkan keamanan, ekonomi, dan keamanan dan kesehatan publik Bangsa menjadi berisiko. Mirip dengan risiko keuangan dan reputasi, risiko cybersecurity mempengaruhi hal dasar pada perusahaan. Hal ini dapat meningkatkan biaya dan berdampak pada pendapatan. Hal ini dapat membahayakan kemampuan organisasi untuk berinovasi dan untuk mendapatkan dan mempertahankan pelanggan.

Untuk dapat lebih baik mengatasi risiko tersebut, Presiden mengeluarkan Executive Order 13636, "Meningkatkan Cybersecurity Infrastruktur yang kritis," pada tanggal 12 Februari 2013, yang menetapkan bahwa "Itu adalah kebijakan dari Amerika Serikat untuk meningkatkan keamanan dan ketahanan infrastruktur yang kritis dari Bangsa dan untuk menjaga lingkungan cyber yang mendorong efisiensi, inovasi, dan kemakmuran ekonomi saat mempromosikan keselamatan, keamanan, kerahasiaan bisnis, privasi, dan kebebasan sipil. "dalam memberlakukan kebijakan ini, Eksekutif Order memanggil untuk mengembangkan Cybersecurity Framework berbasis risiko secara sukarela - satu set standar industri dan pengalaman lapangan untuk membantu organisasi mengelola risiko cybersecurity. Kerangka yang dihasilkan, diciptakan melalui kolaborasi antara pemerintah dan sektor swasta, menggunakan bahasa yang sama untuk mengatasi dan mengelola risiko cybersecurity dengan cara yang hemat biaya berdasarkan kebutuhan bisnis tanpa meletakkan persyaratan peraturan tambahan pada dunia usaha.

Kerangka ini fokus pada penggunaan pendorong dunia usaha untuk memandu kegiatan cybersecurity dan mempertimbangkan risiko keamanan cyber sebagai bagian dari proses manajemen risiko organisasi. Kerangka ini terdiri dari tiga bagian: Framework Core, Framework Profile, dan Framework Implementasi Tiers. Framework Core merupakan serangkaian kegiatan cybersecurity, hasil, dan referensi informatif yang umum di sektor infrastruktur yang kritis, memberikan panduan rinci untuk mengembangkan profile organisasi individu. Melalui penggunaan profil tersebut, Framework akan membantu organisasi menyelaraskan kegiatan cybersecurity dengan persyaratan dunia usaha, toleransi risiko, dan sumber daya. Tiers menyediakan mekanisme bagi organisasi untuk melihat dan memahami karakteristik pendekatan mereka untuk mengelola risiko cybersecurity.

Framework ini memungkinkan organisasi - terlepas dari ukuran, tingkat risiko cybersecurity, atau kecanggihan cybersecurity - untuk menerapkan prinsip-prinsip dan praktek-praktek terbaik manajemen risiko untuk meningkatkan keamanan dan ketahanan infrastruktur yang kritis. Framework menyediakan organisasi dan struktur untuk beberapa pendekatan saat ini untuk cybersecurity dengan membuat standar, pedoman, dan praktek yang dapat bekerja secara efektif dalam industri saat ini. Selain itu, karena dia mereferensi standard global yang diakui untuk cybersecurity, Kerangka juga dapat digunakan oleh organisasi berada di luar Amerika Serikat dan dapat berfungsi sebagai model untuk kerjasama internasional untuk memperkuat cybersecurity infrastruktur yang kritis.

Framework bukanlah sebuah kerangka cocok untuk semua pendekatan untuk mengelola risiko keamanan cyber untuk infrastruktur yang kritis. Organisasi akan terus memiliki risiko yang unik - ancaman yang berbeda, kerentanan yang berbeda, toleransi risiko yang berbeda - dan bagaimana mereka mengimplementasikan Framework akan bervariasi. Organisasi dapat menentukan kegiatan yang penting untuk layanan kritis dan dapat memprioritaskan investasi untuk memaksimalkan dampak dari setiap dolar yang dihabiskan. Pada akhirnya, Framework tersebut bertujuan untuk mengurangi dan mengelola lebih baik risiko cybersecurity.

Framework tersebut adalah dokumen yang hidup dan akan terus diperbarui dan ditingkatkan ketika industri memberikan umpan balik pada saat implementasi. Saat Framework tersebut di implementasikan dalam praktek, pelajaran yang didapat akan diintegrasikan ke dalam versi selanjutnya. Ini akan memastikan Framework memenuhi kebutuhan pemilik infrastruktur yang kritis dan operator dalam lingkungan yang dinamis dan menantang untuk ancaman, risiko, dan solusi yang baru.

Penggunaan Framework sukarela ini adalah langkah berikutnya untuk meningkatkan cybersecurity infrastruktur yang kritis bagi bangsa kita - memberikan bimbingan untuk masing-masing organisasi, sekaligus meningkatkan postur cybersecurity infrastruktur yang kritis pada Bangsa secara keseluruhan.

Pendahuluan Framework

Keamanan nasional dan ekonomi dari Amerika Serikat tergantung pada fungsi yang dapat diandalkan infrastruktur yang kritis. Untuk memperkuat ketahanan infrastruktur ini, Presiden Obama mengeluarkan Executive Order 13636 (EO), "Meningkatkan Cybersecurity infrastruktur yang kritis," pada tanggal 12 Februari 2013. Executive Order ini memanggil untuk pengembangan Cybersecurity Framework sukarela ("Framework") yang menyediakan "prioritas, fleksibel, dapat berulang, berbasis kinerja, dan pendekatan yang hemat biaya" untuk mengelola risiko keamanan cyber untuk proses, informasi, dan sistem yang langsung terlibat dalam penyediaan layanan infrastruktur yang kritis. Framework, dikembangkan bekerja sama dengan industri, memberikan bimbingan kepada sebuah organisasi pada pengelolaan risiko cybersecurity.

Infrastruktur penting didefinisikan dalam EO sebagai "sistem dan aset, baik fisik maupun virtual, sehingga penting untuk Amerika Serikat bahwa ketidakmampuan atau kerusakan sistem dan aset tersebut akan berdampak melemahkan keamanan, keamanan ekonomi nasional, kesehatan publik nasional atau keselamatan, atau kombinasi dari hal-hal tersebut. "karena tekanan meningkat dari ancaman eksternal dan internal, organisasi yang bertanggung jawab untuk infrastruktur yang kritis harus memiliki pendekatan yang konsisten dan berulang untuk mengidentifikasi, menilai, dan mengelola risiko cybersecurity. Pendekatan ini diperlukan terlepas dari ukuran organisasi, eksposur ancaman, atau cybersecurity kecanggihan hari ini.

Masyarakat infrastruktur yang kritis termasuk pemilik publik dan swasta dan operator, dan entitas lain yang berperan dalam mengamankan infrastruktur Bangsa. Anggota masing-masing sektor infrastruktur yang kritis melakukan fungsi yang didukung oleh teknologi informasi (TI) dan sistem kontrol industri (ICS). Ketergantungan pada teknologi, komunikasi, dan interkoneksi TI dan ICS telah berubah dan memperluas potensi kerentanan dan peningkatan potensi risiko operasi. Misalnya, karena ICS dan data yang dihasilkan dalam operasi ICS semakin digunakan untuk memberikan layanan kritis dan mendukung keputusan bisnis, yang potensi dampak dari insiden cybersecurity pada organisasi bisnis, aset, kesehatan dan keselamatan individu, dan lingkungan harus dipertimbangkan. Untuk mengelola risiko cybersecurity, pemahaman yang jelas tentang driver bisnis organisasi dan pertimbangan keamanan khusus untuk penggunaan TI dan ICS diperlukan. Karena risiko masing-masing organisasi adalah unik, bersama dengan penggunaan TI dan ICS, alat dan metode yang digunakan untuk mencapai hasil yang dijelaskan oleh Framework akan bervariasi.

Mengakui bahwa perlindungan privasi dan kebebasan sipil berperan dalam menciptakan kepercayaan publik yang lebih besar, Orde Eksekutif mengharuskan Framework ini termasuk metodologi untuk melindungi privasi individu dan kebebasan sipil ketika organisasi infrastruktur yang kritis melakukan kegiatan cybersecurity. Banyak organisasi telah memiliki proses untuk menangani privasi dan kebebasan sipil. Metodologi ini dirancang untuk proses tersebut dan memberikan bimbingan untuk memfasilitasi manajemen risiko privasi yang konsisten dengan pendekatan organisasi untuk manajemen risiko cybersecurity. Mengintegrasikan privasi dan keamanan dunia maya bisa mendapatkan keuntungan organisasi dengan meningkatkan kepercayaan nasabah, memungkinkan berbagi lebih standar informasi, dan menyederhanakan operasi di seluruh rezim hukum.

Untuk memastikan pengembangan dan kemungkinan inovasi teknis, Framework adalah teknologi netral. Framework bergantung pada berbagai standar, pedoman, dan praktik yang ada untuk memungkinkan penyedia infrastruktur yang kritis untuk mencapai ketahanan. Dengan mengandalkan standar, pedoman, dan praktek yang global dikembangkan, dikelola, dan diperbarui oleh industri, alat dan metode yang tersedia untuk mencapai hasil Framework agar lintas batas, mengakui sifat global dari risiko cybersecurity, dan berkembang dengan kemajuan teknologi dan

persyaratan dunia usaha. Penggunaan standar yang muncul akan memungkinkan skala ekonomi dan mendorong pengembangan produk yang efektif, jasa, dan praktek-praktek yang memenuhi kebutuhan pasar yang teridentifikasi. Persaingan pasar juga mempromosikan difusi lebih cepat dari teknologi ini dan praktek-praktek dan realisasi banyak manfaat oleh pemangku kepentingan di sektor ini.

Membangun dari standar-standar, pedoman, dan praktek, Framework menyediakan taksonomi umum dan mekanisme organisasi untuk:

1. Jelaskan postur cybersecurity mereka saat ini;
2. Jelaskan tahapan target mereka untuk cybersecurity;
3. Mengidentifikasi dan memprioritaskan peluang untuk perbaikan dalam konteks proses yang berkesinambungan dan berulang;
4. Menilai kemajuan menuju tahapan sasaran;
5. Berkomunikasi antara para pemangku kepentingan internal dan eksternal tentang risiko cybersecurity.

Framework ini melengkapi, dan tidak menggantikan, proses manajemen risiko organisasi dan program cybersecurity. Organisasi dapat menggunakan proses saat ini dan memanfaatkan Framework untuk mengidentifikasi peluang untuk memperkuat dan berkomunikasi manajemen risiko cybersecurity sementara menyelaraskan dengan praktik industri. Atau, sebuah organisasi tanpa program cybersecurity yang ada dapat menggunakan Framework sebagai referensi untuk membangun sebuah program cybersecurity.

Framework ini tidak spesifik industri, taksonomi umum dari standar, pedoman, dan praktik yang menyediakan juga tidak spesifik negara. Organisasi di luar Amerika Serikat juga dapat menggunakan Framework untuk memperkuat upaya cybersecurity mereka sendiri, dan Framework dapat berkontribusi untuk mengembangkan bahasa yang umum untuk kerja sama internasional untuk cybersecurity infrastruktur yang kritis.

Framework secara umum.

Framework tersebut adalah pendekatan berbasis risiko untuk mengelola risiko cybersecurity, dan terdiri dari tiga bagian: Framework Core / Inti, Framework Implementation Tiers, dan Framework Profile. Setiap komponen Framework memperkuat hubungan antara dorongan dunia usaha dan kegiatan cybersecurity. Komponen-komponen ini dijelaskan di bawah ini.

- Framework Core / Inti merupakan serangkaian kegiatan cybersecurity, dengan hasil yang diinginkan, dan referensi yang berlaku yang umum di seluruh sektor infrastruktur yang kritis. Core menyajikan standar industri, pedoman, dan praktik dengan cara yang memungkinkan untuk mengkomunikasikan kegiatan cybersecurity dan hasil seluruh organisasi dari tingkat eksekutif untuk tingkat penerapan / operasi. Framework Core terdiri dari lima fungsi yang bersamaan dan terus menerus - Identifikasi, Lindungi, Deteksi, Tanggapi, Recover. Ketika dipertimbangkan secara bersama-sama, fungsi ini memberikan pandangan tingkat tinggi, strategis dari siklus hidup manajemen resiko organisasi cybersecurity. Framework Core kemudian mengidentifikasi kategori kunci yang mendasari dan subkategori untuk setiap fungsi, dan mencocokkannya dengan contoh informasi referensi seperti standar yang ada, pedoman, dan praktek untuk setiap subkategori.
- Framework Implementation Tiers (“Tiers”) memberikan konteks tentang bagaimana sebuah organisasi memandang risiko cybersecurity dan proses yang dijalankan untuk mengelola risiko itu. Tiers menggambarkan sejauh mana praktik manajemen risiko cybersecurity organisasi mengacu pada karakteristik yang didefinisikan dalam Framework (misalnya, kesadaran risiko dan ancaman, berulang, dan adaptif). Tiers mencirikan praktek organisasi dalam sebuah rentang, dari Partial (Tier 1) ke Adaptive (Tier 4). Tiers ini mencerminkan perkembangan dari tanggapan informal, reaktif hingga pendekatan yang lincah dan terinformasi-risiko. Selama proses seleksi Tier, sebuah organisasi harus mempertimbangkan praktek manajemen risiko saat ini, ancaman lingkungan, persyaratan hukum dan peraturan, tujuan bisnis / misi, dan kendala organisasi.
- Framework Profile (“Profil”) merupakan keluaran berdasarkan kebutuhan bisnis bahwa organisasi telah dipilih dari kategori dan subkategori Framework. Profil yang dapat dicirikan sebagai penyelarasan standar, pedoman, dan praktek untuk Framework Corei dalam skenario implementasi tertentu. Profil dapat digunakan untuk mengidentifikasi peluang untuk meningkatkan postur cybersecurity dengan membandingkan “Current” Profil (kondisi “apa adanya”) dengan “Target” Profil (kondisi “akhir”). Untuk mengembangkan Profil, organisasi dapat meninjau semua kategori dan subkategori dan, berdasarkan dorongan bisnis dan penilaian risiko, menentukan mana yang paling penting; mereka dapat menambahkan kategori dan subkategori yang diperlukan untuk mengatasi risiko organisasi. Profil saat ini kemudian dapat digunakan untuk mendukung prioritas dan pengukuran kemajuan menuju Profil Sasaran, sedangkan disinkronkan dengan kebutuhan bisnis lainnya termasuk efektivitas biaya dan inovasi. Profil dapat digunakan untuk melakukan penilaian diri dan berkomunikasi dalam sebuah organisasi atau antar organisasi.

Risk Management and the Cybersecurity Framework

Manajemen risiko adalah proses yang berkelanjutan untuk mengidentifikasi, menilai, dan menanggapi risiko. Untuk mengelola risiko, organisasi harus memahami kemungkinan bahwa suatu peristiwa akan terjadi dan dampak yang dihasilkan. Dengan informasi ini, organisasi dapat menentukan tingkat risiko yang dapat diterima untuk pengiriman layanan dan dapat mengekspresikan ini sebagai toleransi risiko mereka.

Dengan pemahaman tentang toleransi risiko, organisasi dapat memprioritaskan kegiatan cybersecurity, memungkinkan organisasi untuk membuat keputusan tentang pengeluaran cybersecurity. Pelaksanaan program manajemen risiko menawarkan organisasi kemampuan untuk mengukur dan berkomunikasi penyesuaian untuk program cybersecurity mereka. Organisasi dapat memilih untuk menangani risiko dengan cara yang berbeda, termasuk mengurangi risiko, mentransfer risiko, menghindari risiko, atau menerima risiko, tergantung pada dampak potensial terhadap pelayanan kritis.

Framework ini menggunakan proses manajemen risiko untuk memungkinkan organisasi untuk menginformasikan dan memprioritaskan keputusan mengenai cybersecurity. Framework ini mendukung penilaian risiko berulang dan validasi pendorong bisnis untuk membantu organisasi pilih tahapan target untuk kegiatan cybersecurity yang mencerminkan hasil yang diinginkan. Dengan demikian, Framework memberikan organisasi kemampuan untuk secara dinamis memilih dan peningkatan langsung dalam manajemen risiko keamanan cyber untuk lingkungan IT dan ICS.

Framework adalah adaptif untuk menyediakan implementasi yang fleksibel dan berbasis risiko yang dapat digunakan dengan array yang luas dari proses manajemen risiko cybersecurity. Contoh dari proses manajemen risiko cybersecurity termasuk Organisasi Internasional untuk Standardisasi (ISO) 31000: 2009, ISO / IEC 27005: 2011, Institut Nasional Standar dan Teknologi (NIST) Publikasi Khusus (SP) 800-39, dan Pedoman Electricity Subsector Cybersecurity Risk Management Process (RMP).

Framework Basics

Framework menyediakan bahasa umum untuk memahami, mengelola, dan mengekspresikan risiko cybersecurity baik secara internal maupun eksternal. Hal ini dapat digunakan untuk membantu mengidentifikasi dan memprioritaskan tindakan untuk mengurangi risiko cybersecurity, dan Framework adalah alat untuk menyelaraskan kebijakan, dunia usaha, dan pendekatan teknologi untuk mengelola risiko itu. Hal ini dapat digunakan untuk mengelola risiko cybersecurity di seluruh organisasi atau dapat difokuskan pada pemberian layanan yang penting dalam sebuah organisasi. Berbagai jenis entitas - termasuk sektor koordinasi struktur, asosiasi, dan organisasi - dapat menggunakan Framework untuk tujuan yang berbeda, termasuk penciptaan Profiles yang umum.

Framework Core

Framework Core menyediakan satu set kegiatan untuk mencapai hasil cybersecurity tertentu, dan referensi contoh pedoman untuk mencapai hasil tersebut. Core bukanlah daftar tindakan untuk dilaksanakan. Core menyajikan hasil cybersecurity utama yang diidentifikasi oleh industri sebagai membantu dalam mengelola risiko cybersecurity. Core terdiri dari empat elemen: Fungsi, Kategori, Subkategori, dan Referensi Informatif, digambarkan pada Gambar 1:

Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Struktur Framework Core

Unsur-unsur Framework Core bekerja sama sebagai berikut:

- **Functions** mengatur kegiatan cybersecurity dasar pada tingkat tertinggi. Fungsi ini adalah Identifikasi, Lindungi, Deteksi, Tanggapi, dan Recover. Mereka membantu organisasi dalam mengungkapkan manajemen risiko cybersecurity dengan mengorganisir informasi, memungkinkan keputusan manajemen risiko, mengatasi ancaman, dan meningkatkan dengan belajar dari kegiatan sebelumnya. Function juga sejalan dengan metodologi yang ada untuk manajemen insiden dan membantu menunjukkan dampak dari investasi di cybersecurity. Misalnya, investasi dalam perencanaan dan latihan mendukung respon dan pemulihan tindakan tepat waktu, sehingga mengurangi dampak terhadap pemberian layanan.

- **Categories** adalah subdivisi dari Function dalam kelompok hasil cybersecurity erat dengan kebutuhan program dan kegiatan tertentu. Contoh Kategori termasuk “Asset Management,” “Access Control,” dan “Proses Deteksi.”
- **Subcategories** membagi lebih lanjut Category menjadi hasil spesifik teknis dan / atau kegiatan manajemen. Mereka menyediakan satu set hasil yang, sementara tidak lengkap, membantu pencapaian dukungan dari hasil di setiap Kategori. Contoh Subkategori termasuk “sistem informasi eksternal di katalogkan,” “Data-at-rest dilindungi,” dan “Pemberitahuan dari sistem deteksi diselidiki.”
- **Informative Reference** adalah bagian tertentu dari standar, pedoman, dan praktek umum di antara sektor-sektor infrastruktur yang kritis yang menggambarkan sebuah metode untuk mencapai hasil yang terkait dengan setiap Subkategori. Referensi Informatif disajikan dalam Framework Core secara ilustrasi dan tidak lengkap. Mereka didasarkan pada bimbingan lintas sektor yang paling sering dirujuk selama proses pengembangan Framework.

Fungsi lima Framework Core didefinisikan di bawah ini. Fungsi ini tidak dimaksudkan untuk membentuk jalur serial, atau mengarah ke keadaan akhir yang diinginkan secara statis. Sebaliknya, Fungsi dapat dilakukan secara bersamaan dan terus menerus untuk membentuk budaya operasional yang membahas risiko cybersecurity secara dinamis.

- **Identifikasi** - Mengembangkan pemahaman organisasi untuk mengelola risiko cybersecurity untuk sistem, aset, data, dan kemampuan.
Kegiatan dalam fungsi Identifikasi merupakan dasar untuk penggunaan yang efektif dari Framework. Memahami konteks bisnis, sumber daya yang mendukung fungsi kritis, dan risiko cybersecurity terkait memungkinkan organisasi untuk fokus dan memprioritaskan upaya, konsisten dengan strategi manajemen risiko dan kebutuhan bisnis. Contoh Categories hasil dalam Fungsi ini meliputi: Manajemen Aset; Lingkungan bisnis; Governance; Risiko Tugas; dan Strategi Manajemen Risiko.
- **Lindungi** - Mengembangkan dan melaksanakan pengamanan yang memadai untuk memastikan pengiriman layanan infrastruktur yang kritis.
Fungsi Protect mendukung kemampuan untuk membatasi atau mengandung dampak dari potensi kejadian cybersecurity. Contoh Categories hasil dalam Fungsi ini meliputi: Kontrol akses; Kesadaran dan Pelatihan; Keamanan data; Proses dan Prosedur Perlindungan informasi; Pemeliharaan; dan pelindung Teknologi.
- **Tanggapi** - Mengembangkan dan melaksanakan kegiatan sesuai untuk mengambil tindakan pada kejadian cybersecurity yang terdeteksi.
Fungsi Respond mendukung kemampuan untuk mengkarantina dampak dari potensial kejadian cybersecurity. Contoh dari keluaran Categories dalam Fungsi ini meliputi: Perencanaan Respon; Komunikasi; Analisa; mitigasi; dan Perbaikan.
- **Recover** - Mengembangkan dan melaksanakan kegiatan mempertahankan rencana untuk ketahanan dan untuk memulihkan setiap kemampuan atau jasa yang terganggu karena kejadian cybersecurity.
Fungsi Recover mendukung pemulihan tepat waktu untuk operasi yang normal untuk mengurangi dampak dari kejadian cybersecurity. Contoh Categories keluaran dalam fungsi ini meliputi: Recovery Planning; perbaikan; dan Komunikasi.

Framework Implementation Tiers

Framework Implementation Tiers (“Tiers”) memberikan konteks tentang bagaimana sebuah organisasi memandang risiko cybersecurity dan proses yang di jalankan untuk mengelola risiko itu. Tiers berkisar dari Partial (Tier 1) ke Adaptive (Tier 4) dan menggambarkan tingkat kekakuan dan kecanggihan dalam praktek manajemen risiko cybersecurity dan sejauh mana manajemen risiko cybersecurity diinformasikan oleh kebutuhan bisnis dan terintegrasi ke dalam risiko secara keseluruhan organisasi praktek manajemen. Pertimbangan manajemen risiko meliputi banyak aspek cybersecurity, termasuk sejauh mana privasi dan kebebasan sipil pertimbangan diintegrasikan ke dalam manajemen organisasi risiko cybersecurity dan tanggapan potensi risiko.

Proses seleksi Tier akan menilai praktek manajemen risiko saat ini di organisasi, lingkungan ancaman, persyaratan hukum dan peraturan, tujuan bisnis / misi, dan kendala organisasi. Organisasi harus menentukan Tier yang diinginkan, memastikan bahwa tingkat yang dipilih memenuhi tujuan organisasi, layak untuk melaksanakan, dan mengurangi risiko cybersecurity untuk aset kritis dan sumber daya untuk tingkat yang dapat diterima untuk organisasi. Organisasi harus mempertimbangkan memanfaatkan bimbingan eksternal yang diperoleh dari departemen di pemerintah federal dan lembaga-lembaga, Information Sharing and Analysis Center (ISACs), model tingkat kesiapan yang ada, atau sumber lain untuk membantu dalam menentukan tingkat yang diinginkan.

Sementara organisasi diidentifikasi sebagai Tier 1 (Partial) didorong untuk mempertimbangkan bergerak menuju Tier 2 atau lebih, Tiers tidak mewakili tingkat kematangan. Kenaikan ke Tiers yang lebih tinggi didorong ketika perubahan tersebut akan mengurangi risiko cybersecurity dan biaya efektif. Keberhasilan pelaksanaan Framework ini didasarkan pada pencapaian hasil yang dijelaskan dalam target profil organisasi dan bukan pada penentuan Tier.

Definisi Tier adalah sebagai berikut:

Tier 1: Partial

- *Risk Management Process* - praktek manajemen risiko cybersecurity di organisasi tidak diformalkan, dan risiko dikelola secara ad hoc dan kadang-kadang reaktif. Prioritas kegiatan cybersecurity mungkin tidak secara langsung diinformasikan oleh resiko tujuan organisasi, ancaman lingkungan, atau kebutuhan bisnis / misi.
- *Integrated Risk Management Program* - Ada kesadaran terbatas risiko cybersecurity di tingkat organisasi dan pendekatan keseluruhan organisasi untuk mengelola risiko cybersecurity belum ditetapkan. Organisasi menerapkan manajemen risiko cybersecurity secara tidak teratur, kasus per kasus karena pengalaman bervariasi atau informasi yang diperoleh dari sumber-sumber luar. Organisasi mungkin tidak memiliki proses yang memungkinkan informasi cybersecurity untuk dibagikan dalam organisasi.
- *External Partisipation* - Sebuah organisasi mungkin tidak memiliki proses untuk berpartisipasi dalam koordinasi atau kerjasama dengan pihak lain.

Tier 2: Risk Informed

- *Risk Management Process* - praktek manajemen risiko yang disetujui oleh manajemen tetapi tidak dapat ditetapkan sebagai kebijakan untuk keseluruhan organisasi. Prioritas kegiatan cybersecurity langsung diinformasikan oleh resiko tujuan organisasi , ancaman lingkungan, atau kebutuhan bisnis / misi.

- *Integrated Risk Management Program* - Ada kesadaran risiko cybersecurity pada tingkat organisasi tetapi pendekatan keseluruhan organisasi untuk mengelola risiko cybersecurity belum ditetapkan. Proses dan prosedur manajemen di approved, risiko-informasi didefinisikan dan diimplementasikan, dan staf memiliki sumber daya yang memadai untuk melakukan tugas cybersecurity mereka. Informasi Cybersecurity dibagi dalam organisasi secara informal.
- *External Participation* - Organisasi tahu perannya dalam ekosistem yang lebih besar, namun belum diformalkan kemampuan untuk berinteraksi dan berbagi informasi eksternal.

Tier 3: Repeatable

- *Risk Management Process* - praktek manajemen risiko organisasi secara resmi disetujui dan dinyatakan sebagai kebijakan. Praktek cybersecurity organisasi secara teratur diperbarui berdasarkan penerapan proses manajemen risiko perubahan kebutuhan bisnis / misi dan perubahan ancaman dan teknologi.
- *Integrated Risk Management Program* - Ada sebuah pendekatan dalam keseluruhan organisasi untuk mengelola risiko cybersecurity. kebijakan risiko-informasi, proses, dan prosedur yang ditetapkan, dilaksanakan sebagaimana dimaksud, dan ditinjau. metode yang konsisten diletakan untuk merespons secara efektif terhadap perubahan risiko. Personil memiliki pengetahuan dan keterampilan untuk melakukan peran yang diberikan pada mereka dan bertanggung jawab.
- *External Participation* - Organisasi memahami ketergantungan dan kemitraan dan menerima informasi dari mitra ini yang memungkinkan kolaborasi dan pengambilan keputusan manajemen berbasis risiko dalam organisasi dalam menanggapi peristiwa.

Tier 4: Adaptive

- *Risk Management Process* - Organisasi menyesuaikan praktek cybersecurity berdasarkan pada pelajaran dan indikator prediktif berasal dari kegiatan cybersecurity sebelumnya dan saat ini. Melalui proses perbaikan yang terus menerus menggabungkan teknologi cybersecurity canggih dan praktik, organisasi secara aktif menyesuaikan dengan lanskap cybersecurity berubah dan merespon berkembang dan ancaman canggih pada waktu yang tepat.
- *Integrated Risk Management Program* - Beroperasinya sebuah pendekatan untuk keseluruhan organisasi untuk mengelola risiko cybersecurity yang menggunakan kebijakan yang terinformasikan resiko, proses, dan prosedur untuk mengatasi potensi kejadian cybersecurity. Manajemen risiko cybersecurity merupakan bagian dari budaya organisasi dan berkembang dari kesadaran kegiatan sebelumnya, informasi bersama oleh sumber-sumber lain, dan kesadaran terus menerus akan aktifitas pada sistem dan jaringan mereka.
- *External Participation* - organisasi mengelola risiko dan secara aktif berbagi informasi dengan mitra untuk memastikan bahwa informasi yang akurat terkini yang sedang didistribusikan dan dikonsumsi untuk meningkatkan cybersecurity sebelum serangan cybersecurity terjadi.

Framework Profile

Framework Profile (“Profil”) adalah penyelarasan Fungsi, Kategori, dan Subkategori dengan kebutuhan bisnis, toleransi risiko, dan sumber daya organisasi. Sebuah Profil memungkinkan organisasi untuk menetapkan peta jalan untuk mengurangi risiko cybersecurity yang selaras dengan tujuan organisasi dan sektor, memperhitungkan persyaratan hukum / peraturan dan praktik terbaik yang dilakukan di industri, dan mencerminkan prioritas manajemen risiko. Mengingat kompleksitas banyak organisasi, mereka mungkin memilih untuk memiliki beberapa profil, selaras dengan komponen tertentu dan mengakui kebutuhan masing-masing.

Framework Profile dapat digunakan untuk menggambarkan keadaan terkini atau tahapan target yang diinginkan dari aktivitas cybersecurity tertentu. Profil terkini menunjukkan keluaran cybersecurity terkini sedang dicapai. Target Profil menunjukkan keluaran yang dibutuhkan untuk mencapai tujuan manajemen risiko cybersecurity yang diinginkan. Profil mendukung kebutuhan bisnis / misi dan bantuan dalam komunikasi risiko dalam dan antar organisasi. Dokumen Kerangka ini tidak menyarankan template profil, sehingga memungkinkan untuk fleksibilitas dalam implementasi.

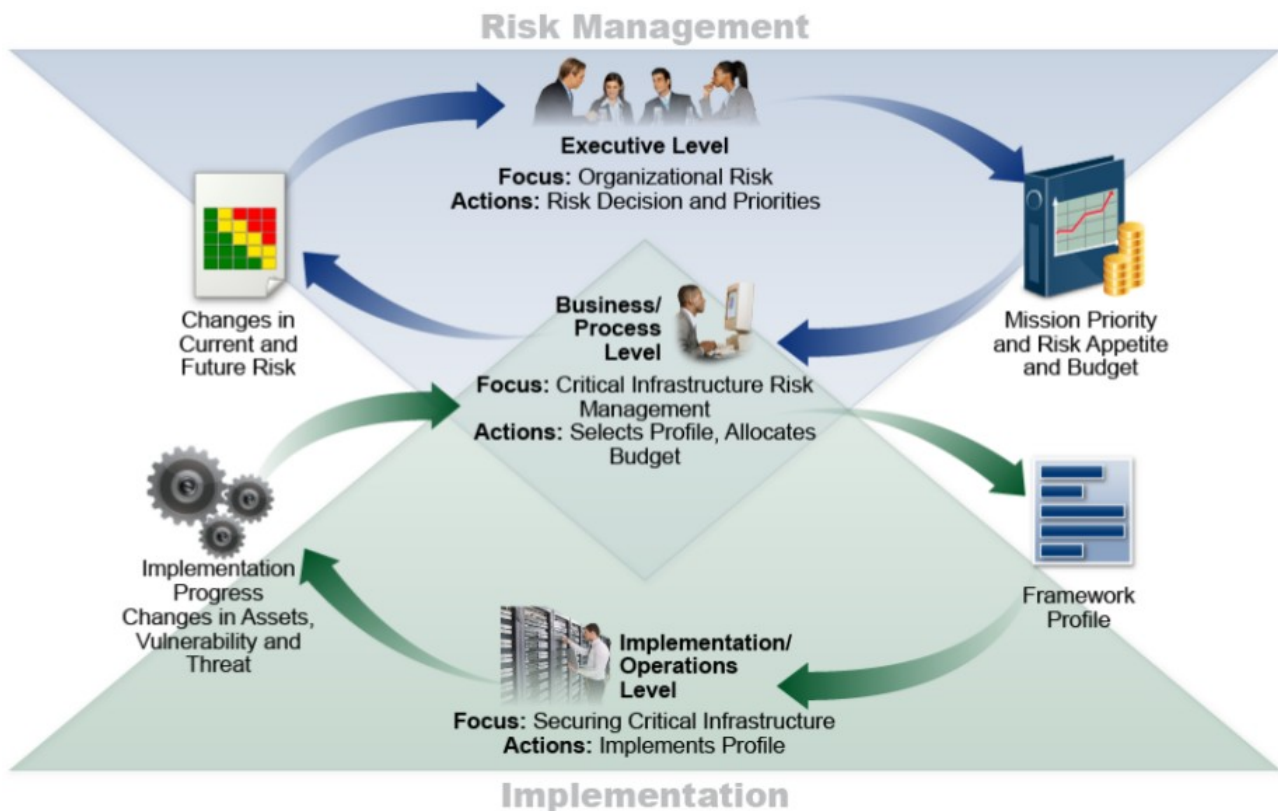
Perbandingan Profil (misalnya, Profil saat ini dan Profil Target) dapat mengungkapkan kesenjangan yang harus ditangani untuk memenuhi tujuan manajemen risiko cybersecurity. Rencana aksi untuk mengatasi kesenjangan ini dapat berkontribusi pada roadmap yang dijelaskan di atas. Prioritas mitigasi kesenjangan didorong oleh kebutuhan bisnis organisasi dan proses manajemen risiko. Pendekatan berbasis risiko ini memungkinkan organisasi untuk mengukur estimasi sumber daya (misalnya, staf, pendanaan) untuk mencapai tujuan cybersecurity secara hemat biaya, dan berprioritas.

Coordination of Framework Implementation

Gambar 2 menggambarkan aliran umum dari informasi dan keputusan-keputusan di tingkat berikut dalam suatu organisasi:

- Executive
- Business/Process
- Implementation/Operations

Tingkat eksekutif mengkomunikasikan prioritas misi, sumber daya yang tersedia, dan toleransi risiko secara keseluruhan untuk tingkat bisnis / proses. Tingkat bisnis / proses menggunakan informasi sebagai masukan ke dalam proses manajemen risiko, dan kemudian bekerja sama dengan pelaksanaan tingkat / operasi untuk berkomunikasi kebutuhan bisnis dan membuat Profil. Tingkat implementasi / operasi mengkomunikasikan Profil pelaksanaan kemajuan ke tingkat bisnis / proses. Tingkat bisnis / proses menggunakan informasi ini untuk melakukan penilaian dampak. Bisnis / proses manajemen tingkat melaporkan hasil bahwa penilaian dampak ke tingkat eksekutif untuk menginformasikan proses manajemen risiko organisasi secara keseluruhan dan untuk pelaksanaan / operasional tingkat kesadaran dari dampak bisnis.



How to Use the Framework

Sebuah organisasi dapat menggunakan Framework sebagai bagian penting dari proses yang sistematis untuk mengidentifikasi, menilai, dan mengelola risiko cybersecurity. Framework ini tidak dirancang untuk menggantikan proses yang ada; suatu organisasi dapat menggunakan proses saat ini dan meng-overlay-nya ke Framework untuk menentukan kesenjangan dalam pendekatan risiko cybersecurity saat ini dan mengembangkan peta jalan untuk perbaikan. Memanfaatkan Framework sebagai alat manajemen risiko cybersecurity, sebuah organisasi dapat menentukan kegiatan yang paling penting untuk pelayanan kritis dan memprioritaskan pengeluaran untuk memaksimalkan dampak investasi.

Framework ini dirancang untuk operasi bisnis dan cybersecurity yang saat ini digunakan. Framework ini dapat berfungsi sebagai dasar untuk program cybersecurity baru atau mekanisme untuk meningkatkan program yang sudah ada. Framework menyediakan sarana untuk membangun persyaratan cybersecurity untuk mitra bisnis dan pelanggan dan dapat membantu mengidentifikasi kesenjangan dalam praktek cybersecurity sebuah organisasi. Framework ini juga menyediakan satu set pertimbangan umum dan proses untuk mempertimbangkan privasi dan implikasi kebebasan sipil dalam konteks program cybersecurity.

Basic Review of Cybersecurity Practices

Framework ini dapat digunakan untuk membandingkan aktivitas cybersecurity organisasi saat ini dengan yang digariskan dalam Framework Core. Melalui penciptaan Profil saat ini, organisasi dapat memeriksa sejauh mana mereka mencapai hasil yang dijelaskan dalam Core kategori dan subkategori, selaras dengan lima Fungsi tingkat tinggi: Identifikasi, Lindungi, Deteksi, Tanggapi, dan Recover. Sebuah organisasi mungkin menemukan bahwa mereka sudah mencapai hasil yang diinginkan, sehingga mengelola cybersecurity sepadan dengan risiko yang diketahui. Sebaliknya, sebuah organisasi dapat menentukan bahwa mereka memiliki kesempatan untuk (atau perlu) meningkatkan. Organisasi dapat menggunakan informasi tersebut untuk mengembangkan rencana aksi untuk memperkuat praktek cybersecurity yang ada dan mengurangi risiko cybersecurity. Suatu organisasi juga dapat menemukan bahwa mereka telah investasi berlebihan untuk mencapai hasil tertentu. Organisasi dapat menggunakan informasi ini untuk memprioritaskan ulang sumber daya untuk memperkuat praktik cybersecurity lainnya.

Framework tidak menggantikan proses manajemen risiko, lima Fungsi tingkat tinggi ini akan memberikan cara ringkas untuk eksekutif senior dan lain-lain untuk mengerti konsep dasar risiko cybersecurity sehingga mereka dapat menilai bagaimana risiko yang teridentifikasi dikelola, dan bagaimana struktur organisasi mereka pada tingkat tinggi bersinergi terhadap standar cybersecurity, pedoman, dan praktek yang ada. Framework ini juga dapat membantu organisasi menjawab pertanyaan mendasar, termasuk “How are we doing?” Kemudian mereka bisa bergerak dengan cara yang lebih terinformasikan untuk memperkuat praktek cybersecurity mereka di mana dan kapan dianggap perlu.

Establishing or Improving a Cybersecurity Program

Langkah-langkah berikut menggambarkan bagaimana sebuah organisasi bisa menggunakan Framework untuk membuat program cybersecurity baru atau meningkatkan program yang ada. Langkah-langkah ini harus diulang seperlunya untuk terus meningkatkan cybersecurity.

Step 1: Prioritize and Scope. organisasi mengidentifikasi objektif bisnis / misi dan prioritas organisasi pada tingkat tinggi. Dengan informasi ini, organisasi membuat keputusan-keputusan strategis mengenai implementasi cybersecurity dan menentukan ruang lingkup sistem dan aset yang mendukung lini bisnis atau proses yang dipilih. Kerangka yang dapat disesuaikan untuk mendukung lini bisnis atau proses yang berbeda dalam sebuah organisasi, yang mungkin memiliki kebutuhan bisnis yang berbeda dan toleransi risiko yang terkait.

Step 2: Orient. Setelah lingkup program cybersecurity telah ditentukan untuk lini bisnis atau proses, organisasi mengidentifikasi sistem terkait dan aset, persyaratan peraturan, dan pendekatan risiko secara keseluruhan. Organisasi kemudian mengidentifikasi ancaman terhadap, dan kerentanan dari, sistem tersebut dan aset.

Step 3: Create a Current Profile. Organisasi mengembangkan Profil saat ini dengan menunjukkan keluaran kategori dan subkategori dari Framework Core saat ini sedang dicapai.

Step 4: Conduct a Risk Assessment. Penilaian ini bisa dipandu oleh proses manajemen risiko secara keseluruhan organisasi atau kegiatan penilaian risiko sebelumnya. organisasi menganalisa lingkungan operasional untuk membedakan kemungkinan kejadian cybersecurity dan dampak bahwa kejadian tersebut bisa saja terjadi pada organisasi. Adalah penting bahwa organisasi berusaha untuk memasukkan risiko yang muncul dan ancaman dan kerentanan data untuk memfasilitasi pemahaman yang kuat tentang kemungkinan dan dampak kejadian cybersecurity.

Step 5: Create a Target Profile. Organisasi menciptakan profil sasaran yang berfokus pada penilaian dari kategori dan subkategori pada Framework untuk menggambarkan hasil cybersecurity yang diinginkan organisasi. Organisasi juga dapat mengembangkan kategori dan subkategori tambahan mereka sendiri untuk memperhitungkan risiko organisasi yang unik. Organisasi ini juga dapat mempertimbangkan pengaruh dan persyaratan stakeholder eksternal seperti entitas sektor, pelanggan, dan mitra bisnis saat membuat profil sasaran.

Step 6: Determine, Analyze, and Prioritize Gaps. Organisasi membandingkan profil saat ini dan profil sasaran untuk menentukan kesenjangan. Berikutnya menciptakan rencana aksi yang diprioritaskan untuk mengatasi kesenjangan tersebut yang mengacu pada dorongan misi, analisa biaya / manfaat, dan pemahaman risiko untuk mencapai hasil dalam profil sasaran. Organisasi kemudian menentukan sumber daya yang diperlukan untuk mengatasi kesenjangan. Menggunakan profil dengan cara ini memungkinkan organisasi untuk membuat keputusan tentang kegiatan cybersecurity, mendukung manajemen risiko, dan memungkinkan organisasi untuk melakukan hemat biaya, pentargetan perbaikan.

Step 7: Implement Action Plan. Organisasi menentukan tindakan yang harus dilakukan dalam hal kesenjangan, jika ada, yang diidentifikasi pada langkah sebelumnya. Kemudian memonitor praktek cybersecurity saat ini dibandingkan dengan Profil Target. Untuk panduan lebih lanjut, Framework mengidentifikasi contoh Referensi Informatif mengenai kategori dan subkategori, tetapi organisasi harus menentukan standar, pedoman, dan praktik, termasuk yang spesifik sektor, yang dapat bekerja terbaik untuk kebutuhan organisasi.

Sebuah organisasi dapat mengulangi langkah-langkah yang diperlukan untuk terus menilai dan meningkatkan cybersecurity nya. Misalnya, organisasi mungkin menemukan bahwa lebih sering pengulangan langkah orientasi meningkatkan kualitas penilaian risiko. Selanjutnya, organisasi dapat memantau kemajuan melalui update berulang ke Profil Saat ini, kemudian membandingkan Profil Saat ini untuk Target Profil. Organisasi juga dapat memanfaatkan proses ini untuk menyelaraskan program yang cybersecurity mereka dengan yang diinginkan Framework Implementation Tier.

Communicating Cybersecurity Requirements with Stakeholders

Framework menyediakan bahasa umum untuk berkomunikasi tentang kebutuhan antara para pemangku kepentingan saling bertanggung jawab untuk penyediaan layanan infrastruktur kritis yang penting. Contoh termasuk:

- Sebuah organisasi dapat memanfaatkan Target Profil untuk menyampaikan kebutuhan manajemen risiko cybersecurity ke penyedia layanan eksternal (misalnya, penyedia cloud yang mana organisasi melakukan mengeksport data).
- Sebuah organisasi dapat menyatakan kondisi cybersecurity melalui Profil Saat ini untuk melaporkan hasil atau untuk membandingkan dengan kebutuhan pengadaan.
- Pemilik / operator infrastruktur yang kritis, setelah diidentifikasi mitra eksternal pada siapa infrastruktur tersebut yang tergantung, dapat menggunakan target profil untuk menyampaikan kategori dan subkategori yang diperlukan.

Identifying Opportunities for New or Revised Informative References

Framework yang dapat digunakan untuk mengidentifikasi peluang untuk standar, pedoman, atau praktik dimana Referensi Informatif tambahan yang baru akan membantu organisasi mengatasi kebutuhan yang muncul. Sebuah organisasi menerapkan Subkategori diberikan, atau mengembangkan Subkategori baru, mungkin menemukan bahwa ada beberapa Referensi Informatif, jika ada, untuk kegiatan terkait. Untuk mengatasi kebutuhan itu, organisasi mungkin berkolaborasi dengan para pemimpin teknologi dan / atau badan standar untuk merancang, mengembangkan, dan mengkoordinasikan standar, pedoman, atau praktek.

Methodology to Protect Privacy and Civil Liberties

Bagian ini menjelaskan metodologi yang diperlukan oleh Executive Order untuk menjamin privasi individu dan implikasi kebebasan sipil yang mungkin timbul dari operasi cybersecurity. Metodologi ini dimaksudkan untuk menjadi satu set umum pertimbangan dan proses sejak privasi dan kebebasan sipil implikasi mungkin berbeda antar sektor atau dari waktu ke waktu dan organisasi dapat mengatasi pertimbangan dan proses dengan berbagai implementasi teknis. Meskipun demikian, tidak semua kegiatan dalam program cybersecurity dapat menimbulkan hal ini. Konsisten dengan Bagian 3.4, standar privasi teknis, pedoman, dan praktik terbaik tambahan mungkin perlu dikembangkan untuk mendukung peningkatan implementasi teknis.

Privasi dan implikasi kebebasan sipil mungkin timbul ketika informasi pribadi digunakan, dikumpulkan, diproses, dipelihara, atau diungkapkan sehubungan dengan kegiatan cybersecurity organisasi. Beberapa contoh kegiatan yang menanggung pertimbangan privasi atau kebebasan sipil mungkin termasuk: kegiatan cybersecurity yang mengakibatkan over-koleksi atau over-retensi informasi pribadi; pengungkapan atau penggunaan informasi pribadi yang tidak terkait dengan

kegiatan cybersecurity; kegiatan mitigasi cybersecurity yang mengakibatkan denial of service atau dampak yang berpotensi merugikan serupa lainnya, termasuk kegiatan seperti beberapa jenis deteksi insiden atau pemantauan yang dapat mempengaruhi kebebasan berekspresi atau asosiasi.

Pemerintah dan agen pemerintah memiliki tanggung jawab langsung untuk melindungi kebebasan sipil yang timbul dari kegiatan cybersecurity. Seperti disebutkan dalam metodologi dibawah ini, pemerintah atau agen pemerintah yang memiliki atau mengoperasikan infrastruktur yang kritis harus memiliki proses yang beroperasi untuk mendukung kepatuhan kegiatan cybersecurity dengan kebutuhan hukum privasi, peraturan, dan konstitusi.

Untuk mengatasi implikasi privasi, organisasi dapat mempertimbangkan bagaimana, dalam keadaan di mana tindakan tersebut pantas dilakukan, program cybersecurity mereka mungkin memasukkan prinsip-prinsip privasi seperti: minimalisasi data dalam pengumpulan, pengungkapan, dan retensi bahan informasi pribadi yang berkaitan dengan insiden cybersecurity; menggunakan pembatasan untuk kegiatan diluar cybersecurity pada setiap informasi yang dikumpulkan secara khusus untuk kegiatan cybersecurity; transparansi untuk kegiatan cybersecurity tertentu; persetujuan individual dan ganti rugi atas dampak buruk yang timbul dari penggunaan informasi pribadi dalam kegiatan cybersecurity; kualitas data, integritas, dan keamanan; dan akuntabilitas dan audit.

Sebagai organisasi menilai Framework Core dalam Lampiran A, proses dan kegiatan-kegiatan berikut dapat dianggap sebagai sarana untuk mengatasi implikasi privasi dan kebebasan sipil:

Governance of cybersecurity risk

- Assessment organisasi terhadap risiko cybersecurity dan tanggapan potensi risiko mempertimbangkan implikasi privasi dari program cybersecurity-nya.
- Individu dengan tanggung jawab privasi terkait cybersecurity melaporkan kepada manajemen yang tepat dan terlatih dengan baik.
- Proses di tempat untuk mendukung kepatuhan kegiatan cybersecurity dengan hukum privasi, peraturan, dan kebutuhan konstitusi yang berlaku.
- Proses di tempatkan untuk menilai pelaksanaan langkah-langkah dan kontrol organisasi.

Approaches to identifying and authorizing individuals to access organizational assets and systems

- Langkah-langkah untuk mengidentifikasi dan mengatasi implikasi privasi dari tindakan kontrol akses sejauh mana mereka terlibat dalam pengumpulan, pengungkapan, atau penggunaan informasi pribadi

Awareness and training measures

- Informasi yang berlaku dari kebijakan privasi organisasi termasuk dalam pelatihan cybersecurity pekerja dan aktifitas awareness.
- Penyedia layanan yang menyediakan layanan terkait keamanan cyber untuk organisasi mengetahui tentang kebijakan privasi yang berlaku di organisasi.

Anomalous activity detection and system and assets monitoring

- Proses di tempatkan untuk melakukan peninjauan privasi dari aktifitas deteksi anomali dan pemantauan cybersecurity di organisasi.

Response activities, including information sharing or other mitigation efforts

- Proses di tempatkan untuk menilai dan melihat apakah, kapan, bagaimana, dan sejauh mana informasi pribadi dibagikan ke luar organisasi sebagai bagian dari kegiatan berbagi informasi cybersecurity.
- Proses di tempatkan untuk melakukan peninjauan privasi pada upaya mitigasi cybersecurity di organisasi

Appendix A: Framework Core

Lampiran ini menyajikan Framework Core: sebuah daftar dari Fungsi, Kategori, Subkategori, Referensi Informatif yang menggambarkan kegiatan cybersecurity tertentu yang umum di semua sektor infrastruktur kritis. Format presentasi yang dipilih untuk Framework Core tidak menyarankan agar pelaksanaan tertentu atau menyiratkan tingkat pentingnya Categories, Subkategori, dan Referensi Informatif. Framework Core disajikan dalam lampiran ini merupakan seperangkat kegiatan untuk mengelola risiko cybersecurity. Sementara Framework tidak lengkap, karena bisa dikembangkan, sehingga memungkinkan organisasi, sektor, dan entitas lain untuk menggunakan Subkategori dan Referensi Informatif yang hemat biaya dan efisien dan memungkinkan mereka untuk mengelola risiko cybersecurity mereka. Kegiatan dapat dipilih dari Framework Core selama proses pembuatan Profil dan Kategori tambahan, Subkategori, dan Referensi Informatif dapat ditambahkan ke Profil. Proses manajemen risiko, persyaratan hukum / peraturan persyaratan, tujuan bisnis / misi organisasi, dan kendala organisasi memandu pemilihan kegiatan ini saat pembuatan Profil. Informasi pribadi dianggap sebagai komponen data atau aset yang dirujuk dalam Kategori ketika menilai risiko keamanan dan perlindungan.

Hasil yang diharapkan bisa diidentifikasi dalam Fungsi, Kategori, dan Subkategori adalah sama untuk TI dan ICS, akan tetapi lingkungan operasional dan pertimbangan untuk IT dan ICS berbeda. ICS memiliki efek langsung pada dunia fisik, termasuk potensi risiko terhadap kesehatan dan keselamatan individu, dan dampak terhadap lingkungan. Selain itu, ICS memiliki kinerja dan kehandalan persyaratan unik dibandingkan dengan IT, dan tujuan keamanan dan efisiensi harus dipertimbangkan ketika menerapkan langkah-langkah keamanan cyber.

Untuk memudahkan penggunaan, setiap komponen Framework Core diberikan pengenal unik. Fungsi dan Kategori masing-masing memiliki pengenal abjad unik, seperti yang ditunjukkan pada Tabel 1. Subkategori dalam setiap Kategori direferensikan numerik; pengenal unik untuk setiap Subkategori termasuk dalam Tabel 2.

Bahan pendukung tambahan yang berkaitan dengan Framework dapat ditemukan di situs web NIST di <http://www.nist.gov/cyberframework/>.

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
		ID.AM	Asset Management
		ID.BE	Business Environment
ID	Identify	ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		PR.AC	Access Control
		PR.AT	Awareness and Training
PR	Protect	PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
		DE.AE	Anomalies and Events
DE	Detect	DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
		RS.RP	Response Planning
		RS.CO	Communications
RS	Responds	RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
		RC.RP	Recovery Planning
RC	Recover	RC.IM	Improvements
		RC.CO	Communications

Table 2: Framework Core

Function	Category	Subcategory	Informative References
		ID.AM-1: Physical devices and systems within the organization are inventoried	CCS 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
		ID.AM-2: Software platforms and applications within the organization are inventoried	CCS 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 NIST SP 800-53 Rev. 4 CM-8
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-3: Organizational communication and data flows are mapped	CCS CSC 1 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	COBIT 5 APO02.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources	COBIT 5 APO03.03,

		(e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	APO03.04, 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
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	COBIT 5 APO01.02, 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
		ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	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: Dependencies and critical functions for delivery of critical services are established	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: Resilience requirements to support delivery of critical services are established	COBIT 5 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-14
		ID.GV-1: Organizational information security policy is established	COBIT 5 APO01.03, 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 controls from all families
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	COBIT 5 APO13.12 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 NIST SP 800-53 Rev. 4 PM-1, PS-7
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	COBIT 5 MEA03.01, MEA03.04 ISA 62443-2-1:2009 4.4.3.7 ISO/IEC 27001:2013 A.18.1 NIST SP 800-53 Rev. 4 -1 controls from all

			families (except PM-1)
		ID.GV-4: Governance and risk management processes address cybersecurity risks	COBIT 5 DSS04.02 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 NIST SP 800-53 Rev. 4 PM-9, PM-11
		ID.RA-1: Asset vulnerabilities are identified and documented	CCS CSC 4 COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 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: Threat and vulnerability information is received from information sharing forums and sources	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 PM-15, PM-16, SI-5
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-3: Threats, both internal and external, are identified and documented	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 NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	COBIT 5 DSS04.02 ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9,

			PM-11, SA-14
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	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: Risk responses are identified and prioritized	COBIT 5 APO12.05, APO13.02 NIST SP 800-53 Rev. 4 PM-4, PM-9
		ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 NIST SP 800-53 Rev. 4 PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	COBIT 5 APO12.06 ISA 62443-2-1:2009 4.3.2.6.5 NIST SP 800-53 Rev. 4 PM-9
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14
		PR.AC-1: Identities and credentials are managed for authorized devices and users	CCS CSC 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.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-2, IA Family
		PR.AC-2: Physical access to assets is managed and protected	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.11.1.4, A.11.1.6, A.11.2.3 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	PR.AC-3: Remote access is managed	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.6.2.2, A.13.1.1, A.13.2.1 NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	CCS CSC 12, 15 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 NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	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 NIST SP 800-53 Rev. 4 AC-4, SC-7

		PR.AT-1: All users are informed and trained	CCS CSC 9 COBIT 5 APO07.03, BAI05.07 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.7.2.2 NIST SP 800-53 Rev. 4 AT-2, PM-13
		PR.AT-2: Privileged users understand roles & responsibilities	CCS CSC 9 COBIT 5 APO07.02, 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
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	CCS CSC 9 COBIT 5 APO07.03, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 PS-7, SA-9
		PR.AT-4: Senior executives understand roles & responsibilities	CCS CSC 9 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, PM-13
		PR.AT-5: Physical and information	CCS CSC 9 COBIT 5 APO07.03

		security personnel understand roles & responsibilities	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.DS-1: Data-at-rest is protected	CCS CSC 17 COBIT 5 APO01.06, BAI02.01, BAI06.01, 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 SC-28
		PR.DS-2: Data-in-transit is protected	CCS CSC 17 COBIT 5 APO01.06, 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
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	COBIT 5 BAI09.03 ISA 62443-2-1:2009 4.4.3.3.3.9, 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.11.2.7 NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained	COBIT 5 APO13.01 ISA 62443-3-3:2013 SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.12.3.1 NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5
	Data Security (PR.DS):	PR.DS-5: Protections against data leaks	CCS CSC 17 COBIT 5 APO01.06

	Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	are implemented	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.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: Integrity checking mechanisms are used to verify software, firmware, and information integrity	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 NIST SP 800-53 Rev. 4 SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	COBIT 5 BAI07.04 ISO/IEC 27001:2013 A.12.1.4 NIST SP 800-53 Rev. 4 CM-2
		PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	CCS CSC 3, 10 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: A System Development Life	COBIT 5 APO13.01 ISA 62443-2-1:2009

		Cycle to manage systems is implemented	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 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
		PR.IP-3: Configuration change control processes are in place	COBIT 5 BAI06.01, BAI01.06 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
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	COBIT 5 APO13.01 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.17.1.2A.17.1.3, A.18.1.3 NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	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

	systems and assets.		
		PR.IP-6: Data is destroyed according to policy	COBIT 5 BAI09.03 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: Protection processes are continuously improved	COBIT 5 APO11.06, 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 NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	ISO/IEC 27001:2013 A.16.1.6 NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	COBIT 5 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 NIST SP 800-53 Rev. 4 CP-2, IR-8
		PR.IP-10: Response and recovery plans are tested	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: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 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.7.3.1, A.8.1.4 NIST SP 800-53 Rev. 4 PS Family
		PR.IP-12: A vulnerability management plan is developed and implemented	ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	COBIT 5 BAI09.03 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 NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	COBIT 5 DSS05.04 ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 NIST SP 800-53 Rev. 4 MA-4
		PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	CCS CSC 14 COBIT 5 APO11.04 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 Family

		PR.PT-2: Removable media is protected and its use restricted according to policy	COBIT 5 DSS05.02, APO13.01 ISA 62443-3-3:2013 SR 2.3 ISO/IEC 27001:2013 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-4, MP-5, MP-7
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	COBIT 5 DSS05.02 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, 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: Communications and control networks are protected	CCS CSC 7 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 NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7

		DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	COBIT 5 DSS03.01 ISA 62443-2-1:2009 4.4.3.3 NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4
	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DE.AE-2: Detected events are analyzed to understand attack targets and methods	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.16.1.1, A.16.1.4 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	ISA 62443-3-3:2013 SR 6.1 NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	COBIT 5 APO12.06 NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI - 4
		DE.AE-5: Incident alert thresholds are established	COBIT 5 APO12.06 ISA 62443-2-1:2009 4.2.3.10 NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8
		DE.CM-1: The network is monitored to detect potential cybersecurity events	CCS CSC 14, 16 COBIT 5 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: The physical environment is monitored to detect potential cybersecurity events	ISA 62443-2-1:2009 4.3.3.3.8 NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel	ISA 62443-3-3:2013 SR

		activity is monitored to detect potential cybersecurity events	6.2 ISO/IEC 27001:2013 A.12.4.1 NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-4: Malicious code is detected	CCS CSC 5 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
		DE.CM-5: Unauthorized mobile code is detected	ISA 62443-3-3:2013 SR 2.4 ISO/IEC 27001:2013 A.12.5.1 NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	COBIT 5 APO07.06 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: Monitoring for unauthorized personnel, connections, devices, and software is performed	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: Vulnerability scans are performed	COBIT 5 BAI03.10 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
		DE.DP-1: Roles and responsibilities for	CCS CSC 5 COBIT 5 DSS05.01

		detection are well defined to ensure accountability	ISA 62443-2-1:2009 4.4.3.1 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	ISA 62443-2-1:2009 4.4.3.2 ISO/IEC 27001:2013 A.18.1.4 NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DE.DP-3: Detection processes are tested	COBIT 5 APO13.02 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, PM-14, SI-3, SI-4
		DE.DP-4: Event detection information is communicated to appropriate parties	COBIT 5 APO12.06 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 NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved	COBIT 5 APO11.06, 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
	Response Planning (RS.RP):	RS.RP-1: Response plan is executed	COBIT 5 BAI01.10 CCS CSC 18

	Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	during or after an event	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
		RS.CO-1: Personnel know their roles and order of operations when a response is needed	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.16.1.1 NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Events are reported consistent with established criteria	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
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	RS.CO-3: Information is shared consistent with response plans	ISA 62443-2-1:2009 4.3.4.5.2 ISO/IEC 27001:2013 A.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: Coordination with stakeholders occurs consistent with response plans	ISA 62443-2-1:2009 4.3.4.5.5 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	NIST SP 800-53 Rev. 4 PM-15, SI-5

		RS.AN-1: Notifications from detection systems are investigated	COBIT 5 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: The impact of the incident is understood	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.16.1.6 NIST SP 800-53 Rev. 4 CP-2, IR-4
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	RS.AN-3: Forensics are performed	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: Incidents are categorized consistent with response plans	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.MI-1: Incidents are contained	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.16.1.5 NIST SP 800-53 Rev. 4 IR-4
	Mitigation (RS.MI): Activities are performed to	RS.MI-2: Incidents are mitigated	ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 ISO/IEC 27001:2013

	prevent expansion of an event, mitigate its effects, and eradicate the incident.		A.12.2.1, A.16.1.5 NIST SP 800-53 Rev. 4 IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	ISO/IEC 27001:2013 A.12.6.1 NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	RS.IM-1: Response plans incorporate lessons learned	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 NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8
		RC.CO-1: Public relations are managed	COBIT 5 EDM03.02
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	RC.CO-2: Reputation after an event is repaired	COBIT 5 MEA03.02
		RC.CO-3: Recovery activities are	NIST SP 800-53 Rev. 4 CP-2, IR-4

		communicated to internal stakeholders and executive and management teams	

Information regarding Informative References described in Appendix A may be found at the following locations:

- Control Objectives for Information and Related Technology (COBIT): <http://www.isaca.org/COBIT/Pages/default.aspx>
- Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC): <http://www.counciloncybersecurity.org>
- ANSI/ISA-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program: <http://www.isa.org/Template.cfm?Section=Standards8&Template=/Ecommerce/ProductDisplay.cfm&ProductID=10243>
- ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels: <http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=13420>
- ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems -- Requirements: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534
- NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (including updates as of January 15, 2014). <http://dx.doi.org/10.6028/NIST.SP.800-53r4>.

Mappings between the Framework Core Subcategories and the specified sections in the Informative References represent a general correspondence and are not intended to definitively determine whether the specified sections in the Informative References provide the desired Subcategory outcome.