Rangka Kerja untuk Penambahbaikan Keselamatan Siber Infrastruktur Kritikal

Versi 1.1

Institut Piawaian dan Teknologi Kebangsaan
(National Institute of Standards and Technology-NIST)

16 April 2018

https://doi.org/10.6028/NIST.CSWP.6.may

Diterjemah oleh/Translated by:
Assoc. Prof. Ir. Dr. Mohd Fared Abduul Khir, CISSP, NCSP
Cybersecurity and Systems Research Unit (CSS),
Faculty of Science and Technology (FST),
Universiti Sains Islam Malaysia (USIM),
Bandar Baru Nilai, 71800 Nilai,
Negeri Sembilan, Malaysia

Nota kepada Pembaca tentang Pengemaskinian

Versi 1.1 Rangka Kerja Keselamatan Siber ini memperhalusi, menjelaskan dan mempertingkat Versi 1.0, yang dikeluarkan pada Februari 2014. Versi ini menggabungkan komen yang diterima pada dua draf Versi 1.1.

Versi 1.1 bertujuan untuk dilaksanakan oleh pengguna Rangka Kerja kali pertama dan semasa. Pengguna semasa seharusnya dapat melaksanakan Versi 1.1 dengan gangguan yang minimum atau tanpa gangguan; keserasian dengan Versi 1.0 adalah objektif yang jelas.

Jadual berikut meringkaskan perubahan yang dibuat antara Versi 1.0 dan Versi 1.1.

Jadual NTR-1 - Ringkasan perubahan antara Rangka Kerja Versi 1.0 dan Versi 1.1

Kemas Kini	Penerangan Kemas Kini
Menjelaskan bahawa istilah seperti "pematuhan" boleh mengelirukan dan memberi makna yang sangat berbeza kepada pelbagai pihak berkepentingan Rangka Kerja ini	Menambah kejelasan bahawa Rangka Kerja ini mempunyai utiliti sebagai struktur dan bahasa untuk mengatur dan menyatakan pematuhan terhadap keperluan keselamatan siber organisasi itu sendiri. Walau bagaimanapun, oleh kerana pelbagai cara Rangka Kerja ini boleh digunakan oleh organisasi bermakna frasa seperti "pematuhan terhadap Rangka Kerja ini" boleh mengelirukan.
Bahagian baharu tentang penilaian diri	Menambah Seksyen 4.0 *Menilai Sendiri Risiko Keselamatan Siber dengan Rangka Kerja ini,* untuk menerangkan cara Rangka Kerja ini boleh digunakan oleh organisasi untuk memahami dan menilai risiko keselamatan siber organisasi tersebut, termasuk penggunaan pengukuran.
Penjelasan tentang penggunaan Rangka Kerja yang amat diperluas bagi tujuan Pengurusan Risiko Rantaian Bekalan Siber	Seksyen 3.3 yang diperluas iaitu *Menyampaikan Keperluan Keselamatan Siber kepada Pihak Berkepentingan*, membantu pengguna memahami Pengurusan Risiko Rantaian Bekalan Siber (SCRM) dengan lebih baik, manakala Seksyen 3.4 yang baharu iaitu Keputusan Membeli, mengetengahkan penggunaan Rangka Kerja dalam memahami risiko berkaitan dengan produk dan perkhidmatan komersial di luar rak (*off-the-shelf*). Kriteria tambahan SCRM Siber telah dimasukkan ke dalam Peringkat Pelaksanaan. Akhir sekali, Kategori Pengurusan Risiko Rantaian Bekalan, termasuk berbilang Subkategori, telah dimasukkan ke dalam Teras Rangka Kerja.

Perincian untuk mengambil kira pengesahan (*authentication*), kebenaran (*authorization*) dan pembuktian identiti (*identity proofing*) dengan lebih baik	Penggunaan bahasa bagi Kategori Kawalan Akses telah diperinci untuk mengambil kira pengesahan, kebenaran dan pembuktian identiti dengan lebih baik. Ini termasuk menambahkan satu Subkategori setiap satu untuk Pengesahan dan Pembuktian Identiti. Selain itu, Kategori tersebut telah dinamakan semula kepada Pengurusan Identiti dan Kawalan Akses (PR.AC) untuk menyatakan skop Kategori tersebut dan Subkategori yang sepadan dengan lebih baik.
Penjelasan yang lebih baik tentang hubungan antara Peringkat Pelaksanaan dan Profil	Menambah bahasa kepada Seksyen 3.2 *Mencipta atau Menambah Baik Program Keselamatan Siber* tentang penggunaan Peringkat Rangka Kerja dalam Pelaksanaan Rangka Kerja. Menambah bahasa kepada Peringkat Rangka Kerja mencerminkan integrasi pertimbangan Rangka Kerja dalam program pengurusan risiko organisasi. Konsep Peringkat Rangka Kerja juga telah diperinci. Rajah 2.0 dikemas kini untuk memasukkan tindakan daripada Peringkat Rangka Kerja.
Pertimbangan terhadap Pendedahan Kerentanan Terselaras	Subkategori berkaitan dengan kitaran hayat pendedahan kerentanan ditambahkan.

Seperti Versi 1.0, pengguna Versi 1.1 digalakkan membuat penyesuaian kepada Rangka Kerja bagi memaksimumkan nilai organisasi masing-masing.

Penghargaan

Penerbitan ini ialah hasil usaha kerjasama berterusan yang melibatkan industri, ahli akademik dan kerajaan. Institut Piawaian dan Teknologi Kebangsaan (National Institute of Standards and Technology-NIST) melancarkan projek ini pada tahun 2013 dengan menghimpunkan organisasi dari sektor swasta dan awam serta orang perseorangan. Diterbitkan pada tahun 2014 dan disemak pada tahun 2017 dan 2018, *Rangka Kerja untuk Penambahbaikan Keselamatan Siber Infrastruktur Kritikal* ini telah bergantung pada lapan bengkel awam, pelbagai Permintaan untuk Komen atau Maklumat (*Requests for Comment or Information*) dan ribuan interaksi langsung dengan pihak berkepentingan merentasi semua sektor di Amerika Syarikat bersama banyak sektor lain dari seluruh dunia.

Dorongan untuk mengubah Versi 1.0 dan perubahan yang terdapat dalam Versi 1.1 ini ialah berdasarkan:

- Maklum balas dan soalan lazim kepada NIST sejak penerbitan Rangka Kerja Versi 1.0;
- 105 tindak balas kepada permintaan untuk maklumat (RFI) pada Disember 2015, *Pandangan terhadap Rangka Kerja untuk Penambahbaikan Keselamatan Siber Infrastruktur Kritikal;*
- Lebih 85 komen terhadap cadangan draf kedua Versi 1.1, pada 5 Disember 2017;
- Lebih 120 komen terhadap cadangan draf pertama Versi 1.1, pada 10 Januari 2017; dan
- Input daripada 1,200 peserta bengkel Rangka Kerja 2016 dan 2017

Di samping itu, NIST sebelum ini pernah menerbitkan Versi 1.0 Rangka Kerja Keselamatan Siber bersama dokumen lampiran, *Hala Tuju NIST untuk Menambah Baik Keselamatan Siber Infrastruktur Kritikal*. Hala Tuju ini mengetengahkan “bidang penambahbaikan” utama untuk pembangunan, penjajaran dan kerjasama lanjut. Melalui usaha sektor swasta dan awam, beberapa bidang penambahbaikan telah berjaya mencapai kemajuan secukupnya untuk dimasukkan ke dalam Rangka Kerja Versi 1.1 ini.

NIST menghargai and berterima kasih kepada semua yang telah menyumbang kepada Rangka Kerja ini.

Ringkasan Eksekutif

Amerika Syarikat bergantung pada kefungsian infrastruktur kritikal yang andal. Ancaman keselamatan siber mengeksploitasi pertambahan kekompleksan dan ketersambungan sistem infrastruktur kritikal, mendedahkan keselamatan Negara, ekonomi, serta keselamatan dan kesihatan awam pada risiko. Sama seperti risiko kewangan dan reputasi, risiko keselamatan siber menjejaskan keuntungan syarikat. Risiko ini boleh meningkatkan kos dan menjejaskan hasil syarikat. Ini boleh melemahkan keupayaan organisasi untuk berinovasi serta mendapatkan dan mengekalkan pelanggan. Keselamatan siber boleh menjadi komponen yang penting dan menguatkan lagi keseluruhan pengurusan risiko sesebuah organisasi.

Untuk menangani risiko ini dengan lebih baik, Akta Peningkatan Keselamatan Siber 2014[1] (CEA) mengemaskinikan peranan Institut Piawaian dan Teknologi Kebangsaan (National Institute of Standards and Technology-NIST) supaya memasukkan pengenalpastian dan pembangunan rangka kerja keselamatan siber untuk kegunaan sukarela para pemilik dan pengendali infrastruktur kritikal. Melalui CEA, NIST mesti mengenal pasti "pendekatan pendekatan yang diutamakan, fleksibel, boleh ulang, berasaskan prestasi dan berkesan kos, termasuk langkah dan kawalan keselamatan maklumat yang mungkin boleh diterima pakai secara sukarela oleh para pemilik dan pengendali infrastruktur kritikal bagi membantu mereka mengenal pasti, menilai dan menguruskan risiko siber". Ini memformalkan usaha NIST yang terdahulu dalam membangunkan Rangka Kerja Versi 1.0 di bawah Arahan Eksekutif (Executive Order-EO) 13636, "Menambah Baik Keselamatan Siber Infrastruktur Kritikal" (Februari 2013) dan memberikan panduan untuk evolusi Rangka Kerja yang akan datang. Rangka Kerja yang dibangunkan di bawah EO 13636 dan terus berkembang mengikut CEA, menggunakan bahasa umum untuk menangani dan menguruskan risiko keselamatan siber, secara berkesan kos berdasarkan keperluan perniagaan dan organisasi tanpa meletakkan keperluan kawal selia tambahan pada perniagaan.

Rangka Kerja ini memfokuskan kepada penggunaan pemacu perniagaan untuk membimbing aktiviti keselamatan siber dan mempertimbang risiko keselamatan siber sebagai sebahagian daripada proses pengurusan risiko organisasi. Rangka Kerja ini terdiri daripada tiga bahagian: Teras Rangka Kerja, Peringkat Pelaksanaan dan Profil Rangka Kerja. Teras Rangka Kerja ialah set aktiviti dan hasil keselamatan siber, serta rujukan informatif yang umum merentasi sektor dan infrastruktur kritikal. Elemen Teras menyediakan panduan terpeinci untuk membangunkan Profil organisasi masing-masing. Melalui penggunaan Profil, Rangka Kerja ini akan membantu organisasi menjajarkan dan menentukan keutamaan kepada aktiviti keselamatan siber berdasarkan keperluan perniagaan/misi, toleransi risiko dan sumber. Peringkat pula menyediakan mekanisme untuk organisasi melihat dan memahami ciri-ciri pendekatan masing-masing dalam menguruskan risiko keselamatan siber, yang akan membantu dalam menentukan keutamaan dan mencapai objektif keselamatan siber.

[1] *Lihat* 15 U.S.C. § 272(e)(1)(A)(i). Akta Peningkatan Keselamatan Siber 2014 (S.1353) menjadi undang-undang awam 113-274 pada 18 Disember 2014 dan boleh diperoleh di: https://www.congress.gov/bill/113th-congress/senatebill/1353/text

Walaupun dokumen ini dibangunkan untuk menambah baik pengurusan risiko keselamatan siber dalam infrastruktur kritikal, Rangka Kerja ini boleh digunakan oleh organisasi dalam mana-mana sektor atau komuniti. Rangka Kerja membolehkan organisasi – tanpa mengambil kira saiz, tahap risiko keselamatan siber, atau kecanggihan keselamatan siber – untuk menerapkan prinsip dan amalan terbaik pengurusan risiko bertujuan menambah baik keselamatan dan kebingkasan.

Rangka Kerja ini menyediakan struktur pengaturan umum untuk pelbagai pendekatan kepada keselamatan siber dengan menghimpunkan piawaian, garis panduan dan amalan yang berfungsi dengan berkesan pada hari ini. Tambahan pula, oleh kerana ini merujuk kepada piawaian yang diiktiraf secara global untuk keselamatan siber, Rangka Kerja boleh berfungsi sebagai model untuk kerjasama antarabangsa bertujuan memperkukuh keselamatan siber dalam infrastruktur kritikal serta sektor dan komuniti lain.

Rangka Kerja ini menawarkan cara fleksibel untuk menangani keselamatan siber, termasuk kesan keselamatan siber ke atas fizikal, siber dan dimensi manusia. Rangka Kerja tersebut boleh diterapkan kepada organisasi yang bergantung pada teknologi, sama ada keselamatan siber organisasi tersebut memfokuskan terutamanya kepada teknologi maklumat (IT), sistem kawalan industri (ICS), sistem siber fizikal (CPS), atau peranti bersambung secara umumnya, termasuk Internet Benda (IoT). Rangka Kerja ini boleh membantu organisasi dalam menangani keselamatan siber kerana perkara ini menjejaskan privasi para pelanggan, para pekerja dan pihak lain. Di samping itu, hasil Rangka Kerja ini boleh dijadikan sebagai sasaran untuk aktiviti pembangunan tenaga kerja dan evolusi.

Rangka Kerja ini bukan pendekatan yang sesuai bagi semua keadaan pengurusan risiko keselamatan siber untuk infrastruktur kritikal. Organisasi akan terus mempunyai risiko unik – ancaman, kerentanan dan toleransi risiko yang berbeza. Organisasi juga akan mengendalikan cara masing-masing yang berbeza dalam menyesuaikan amalan yang dihuraikan dalam Rangka Kerja ini. Organisasi boleh menentukan aktiviti yang penting kepada pelaksanaan perkhidmatan kritikal dan boleh menentukan keutamaan dalam pelaburan demi memaksimumkan impak setiap ringgit yang dikeluarkan. Akhirnya, Rangka Kerja ini disasarkan kepada usaha mengurangkan dan menguruskan risiko keselamatan siber dengan lebih baik.

Bagi mengambil kira keperluan unik keselamatan siber organisasi, terdapat pelbagai cara yang luas untuk menggunakan Rangka Kerja ini. Keputusan tentang cara menerapkan Rangka Kerja tersebut terserah kepada organisasi yang melaksanakannya. Sebagai contoh, satu organisasi boleh memilih untuk menggunakan Peringkat Pelaksanaan Rangka Kerja ini bagi menyatakan amalan pengurusan risiko yang dibayangkan. Satu organisasi lain pula boleh menggunakan lima Fungsi Rangka Kerja untuk menganalisis keseluruhan portfolio pengurusan risiko; analisis itu boleh bergantung atau tidak pada panduan lebih terperinci yang disertakan bersama Rangka Kerja, seperti katalog kawalan. Kadangkala terdapat perbincangan mengenai “pematuhan” kepada Rangka Kerja dan Rangka Kerja tersebut mempunyai kebergunaan sebagai struktur dan bahasa untuk mengelola dan menyatakan pematuhan terhadap keperluan keselamatan siber organisasi itu sendiri. Walaupun begitu, pelbagai cara Rangka Kerja ini boleh digunakan oleh organisasi, menunjukkan bahawa ungkapan seperti “pematuhan kepada Rangka Kerja”, boleh menimbulkan kekeliruan dan membawa maksud yang sangat berbeza kepada pelbagai pihak berkepentingan.

Rangka Kerja ini ialah dokumen dinamik dan akan terus dikemaskinikan dan ditambah baik apabila industri memberikan maklum balas mengenai pelaksanaan. NIST akan terus menyelaras dengan sektor swasta dan agensi kerajaan pada semua peringkat. Apabila Rangka Kerja diterapkan menjadi amalan yang lebih baik, pengajaran tambahan akan diintegrasikan ke dalam versi masa hadapan. Ini akan memastikan Rangka Kerja dapat memenuhi keperluan pemilik dan pengendali infrastruktur kritikal dalam persekitaran dinamik dan mencabar dengan ancaman, risiko dan penyelesaian baharu.

Penggunaan dan perkongsian amalan terbaik Rangka Kerja sukarela yang diperluas dan lebih berkesan ini ialah langkah seterusnya untuk menambah baik keselamatan siber infrastruktur kritikal Negara kita – menyediakan panduan yang berkembang untuk organisasi individu sambil meningkatkan postur keselamatan siber infrastruktur kritikal Negara, serta ekonomi dan masyarakat yang lebih luas.

Isi Kandungan

Senarai Rajah

Senarai Jadual

1.0 Pengenalan Rangka Kerja

Amerika Syarikat bergantung pada kefungsian infrastruktur kritikal yang andal. Ancaman keselamatan siber mengeksploitasi pertambahan kekompleksan dan ketersambungan sistem infrastruktur kritikal, mendedahkan keselamatan Negara, ekonomi, serta keselamatan dan kesihatan awam pada risiko. Sama seperti risiko kewangan dan reputasi, risiko keselamatan siber menjejaskan keuntungan syarikat. Risiko ini boleh meningkatkan kos dan menjejaskan hasil syarikat. Ini boleh melemahkan keupayaan organisasi untuk berinovasi serta mendapatkan dan mengekalkan pelanggan. Keselamatan siber boleh menjadi komponen yang penting dan menguatkan lagi keseluruhan pengurusan risiko sesebuah organisasi.

Untuk mengukuhkan kebingkasan infrastruktur ini, Akta Peningkatan Keselamatan Siber 2014[2] (CEA) mengemaskinikan peranan Institut Piawaian dan Teknologi Kebangsaan (National Institute of Standards and Technology-NIST) untuk "memudahkan dan menyokong pembangunan" rangka kerja risiko keselamatan siber. Melalui CEA, NIST mesti mengenal pasti "pendekatan pendekatan yang diutamakan, fleksibel, boleh ulang, berasaskan prestasi dan berkesan kos, termasuk langkah dan kawalan keselamatan maklumat yang mungkin boleh diterima pakai secara sukarela oleh para pemilik dan pengendali infrastruktur kritikal bagi membantu mereka mengenal pasti, menilai dan menguruskan risiko siber". Ini memformalkan usaha NIST yang terdahulu dalam membangunkan Rangka Kerja Versi 1.0 di bawah Arahan Eksekutif (Executive Order-EO) 13636, "Menambah Baik Keselamatan Siber Infrastruktur Kritikal" (Februari 2013[3]) dan memberikan panduan untuk evolusi Rangka Kerja yang akan datang.

Infrastruktur Kritikal[4] ditakrifkan dalam Akta Patriot Amerika Syarikat 2001[5] sebagai "sistem dan aset, sama ada fizikal atau maya, sangat penting kepada Amerika Syarikat sehingga ketidakupayaan atau kemusnahan sistem dan aset tersebut akan memberikan impak yang melemahkan keselamatan, keselamatan ekonomi negara, kesihatan dan keselamatan awam negara, atau mana-mana gabungan perkara tersebut". Disebabkan oleh peningkatan tekanan daripada ancaman luaran dan dalaman, organisasi yang bertanggungjawab ke atas infrastruktur kritikal perlu mempunyai pendekatan yang konsisten dan berulang untuk mengenal pasti, menilai dan menguruskan risiko keselamatan siber. Pendekatan ini adalah perlu tanpa mengira saiz organisasi, pendedahan ancaman, atau kecanggihan keselamatan siber pada hari ini.

Pergantungan pada teknologi, komunikasi dan kesalinghubungan ini telah mengubah dan meluaskan potensi kerentanan dan meningkatkan potensi risiko kepada operasi. Sebagai contoh, apabila teknologi dan data yang dihasilkan dan diproses semakin digunakan untuk

---

[2] *Lihat* 15 U.S.C. § 272(e)(1)(A)(i). Akta Peningkatan Keselamatan Siber 2014 (S.1353) menjadi undang-undang awam 113-274 pada 18 Disember 2014 dan boleh diperoleh di: https://www.congress.gov/bill/113th-congress/senatebill/1353/text

[3] No. Arahan Eksekutif 13636, *Menambah Baik Keselamatan Siber Infrastruktur Kritikal*, DCPD-201300091, 12 Februari 2013. https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf

[4] Program Jabatan Keselamatan Dalam Negeri (Department of Homeland Security-DHS) Program Infrastruktur Kritikal menyediakan senarai sektor dan fungsi kritikal yang berkaitan serta rantaian nilai.. http://www.dhs.gov/critical-infrastructure-sectors

[5] Lihat 42 U.S.C. § 5195c(e)). Akta PatriotAmerika Syarikat 2001 (H.R.3162) menjadi undang-undang awam 107-56 pada 26 Oktober 2001 di: https://www.congress.gov/bill/107th-congress/house-bill/3162

menyampaikan perkhidmatan kritikal dan menyokong keputusan perniagaan/misi, potensi impak kejadian keselamatan siber terhadap organisasi, kesihatan dan keselamatan individu, alam sekitar, komuniti, serta ekonomi dan masyarakat lebih luas perlu dipertimbangkan.

Untuk menguruskan risiko keselamatan siber, pemahaman yang jelas mengenai pemacu perniagaan organisasi dan pertimbangan keselamatan khusus bagi penggunaan teknologi diperlukan. Oleh kerana setiap risiko, keutamaan dan sistem organisasi adalah unik, maka peralatan dan kaedah yang digunakan untuk mencapai hasil yang diterangkan oleh Rangka Kerja akan berbeza.

Sebagai mengiktiraf peranan yang dimainkan oleh pelindungan privasi dan kebebasan awam dalam mewujudkan kepercayaan awam, Rangka Kerja memasukkan kaedah untuk melindungi privasi individu dan kepercayaan awam semasa organisasi infrastruktur kritikal menjalankan aktiviti keselamatan siber. Banyak organisasi telah pun mempunyai proses untuk menangani privasi dan kebebasan awam. Pengkaedahan ini direka bentuk untuk melengkapi proses tersebut dan memberikan panduan bertujuan memudahkan pengurusan risiko privasi yang konsisten dengan pendekatan organisasi kepada pengurusan keselamatan siber. Mengintegrasikan privasi dan keselamatan siber boleh memberikan manfaat kepada organisasi dengan meningkatkan keyakinan pelanggan, membolehkan perkongsian maklumat yang lebih seragam dan memudahkan pengendalian merentasi pengurusan undang-undang.

Rangka Kerja ini kekal berkesan dan menyokong inovasi teknikal kerana rangka ini neutral terhadap teknologi, di samping turut merujuk kepada pelbagai piawaian, garis panduan dan amalan yang berkembang dengan teknologi. Dengan bergantung pada piawaian, garis panduan dan amalan global yang dibangunkan, diuruskan dan dikemaskinikan oleh industri, maka peralatan dan kaedah yang tersedia untuk mencapai hasil Rangka Kerja akan melangkaui sempadan, mengiktiraf sifat global risiko keselamatan dan berkembang dengan kemajuan teknologi dan keperluan perniagaan. Penggunaan piawaian sedia ada dan baharu muncul akan membolehkan ekonomi ikut bidangan dan memacu pembangunan produk, perkhidmatan dan amalan yang berkesan, memenuhi keperluan pasaran yang dikenal pasti. Persaingan pasaran turut menggalakkan penyebaran teknologi dan amalan ini dengan lebih pantas, serta merealisasikan banyak manfaat oleh pihak berkepentingan dalam sektor ini.

Membina daripada piawaian, garis panduan dan amalan tersebut, Rangka Kerja memberikan taksonomi dan mekanisme untuk organisasi:

1) Menerangkan postur keselamatan siber semasa;
2) Menerangkan keadaan sasaran keselamatan siber organisasi;
3) Mengenal pasti dan menentukan keutamaan kepada peluang untuk penambahbaikan dalam konteks proses berterusan dan boleh ulang;
4) Menilai kemajuan ke arah keadaan sasaran;
5) Berkomunikasi dalam kalangan pihak berkepentingan dalaman dan luaran tentang risiko keselamatan siber.

Rangka Kerja ini bukan pendekatan yang sesuai bagi semua keadaan pengurusan risiko keselamatan siber untuk infrastruktur kritikal. Organisasi akan terus mempunyai risiko unik – ancaman, kerentanan dan toleransi risiko yang berbeza. Organisasi juga akan mengendalikan

cara masing-masing yang berbeza dalam menyesuaikan amalan yang dihuraikan dalam Rangka Kerja ini. Organisasi boleh menentukan aktiviti yang penting kepada pelaksanaan perkhidmatan kritikal dan boleh menentukan keutamaan dalam pelaburan demi memaksimumkan impak setiap ringgit yang dikeluarkan. Akhirnya, Rangka Kerja ini disasarkan kepada usaha mengurangkan dan menguruskan risiko keselamatan siber dengan lebih baik.

Bagi mengambil kira keperluan unik keselamatan siber organisasi, terdapat pelbagai cara yang luas untuk menggunakan Rangka Kerja ini. Keputusan tentang cara menerapkan Rangka Kerja tersebut terserah kepada organisasi yang melaksanakannya. Sebagai contoh, satu organisasi boleh memilih untuk menggunakan Peringkat Pelaksanaan Rangka Kerja ini bagi menyatakan amalan pengurusan risiko yang dibayangkan. Satu organisasi lain pula boleh menggunakan lima Fungsi Rangka Kerja bagi menganalisis keseluruhan portfolio pengurusan risiko; analisis itu boleh bergantung atau tidak pada panduan lebih terperinci yang disertakan bersama Rangka Kerja, seperti katalog kawalan. Kadangkala terdapat perbincangan mengenai "pematuhan" kepada Rangka Kerja dan Rangka Kerja tersebut mempunyai kebergunaan sebagai struktur dan bahasa untuk mengelola dan menyatakan pematuhan terhadap keperluan keselamatan siber organisasi itu sendiri. Walaupun begitu, pelbagai cara Rangka Kerja ini boleh digunakan oleh organisasi, menunjukkan bahawa ungkapan seperti "pematuhan kepada Rangka Kerja", boleh menimbulkan kekeliruan dan membawa maksud yang sangat berbeza kepada pelbagai pihak berkepentingan.

Rangka Kerja ini melengkapkan dan bukan menggantikan proses pengurusan risiko dan program keselamatan siber organisasi. Organisasi boleh menggunakan proses sedia ada dan memanfaatkan Rangka Kerja untuk mengenal pasti peluang bertujuan mengukuhkan dan menyampaikan maklumat mengenai pengurusan risiko keselamatan siber sambil menjajarkan dengan amalan industri. Sebagai alternatif, organisasi tanpa program keselamatan siber sedia ada boleh menggunakan Rangka Kerja sebagai rujukan untuk mencipta program tersebut.

Walaupun Rangka Kerja ini telah dibangunkan untuk menambah baik pengurusan risiko keselamatan siber yang berkaitan dengan infrastruktur kritikal, namun Rangka Kerja ini juga boleh digunakan oleh organisasi dalam mana-mana sektor ekonomi atau masyarakat. Ini bertujuan untuk kegunaan syarikat, agensi kerajaan dan organisasi bukan untung, tanpa mengambil kira fokus dan saiz masing-masing. Taksonomi umum piawaian, garis panduan dan amalan yang disediakan juga bukan khusus kepada mana-mana negara. Organisasi di luar Amerika Syarikat boleh juga menggunakan Rangka Kerja tersebut untuk mengukuhkan usaha keselamatan siber masing-masing dan Rangka Kerja ini boleh menyumbang kepada pembangunan bahasa umum untuk kerjasama antarabangsa ke atas keselamatan siber infrastruktur kritikal.

1.1 Gambaran Keseluruhan Rangka Kerja

Rangka Kerja ini menggunakan pendekatan berasaskan risiko untuk menguruskan risiko keselamatan siber dan terdiri daripada tiga bahagian: Teras Rangka Kerja, Peringkat Pelaksanaan Rangka Kerja dan Profil Rangka Kerja. Setiap komponen Rangka Kerja mengukuhkan hubungan antara pemacu perniagaan/misi dan aktiviti keselamatan siber. Komponen ini dijelaskan di bawah.

- *Teras Rangka Kerja* ialah set aktiviti keselamatan siber, hasil yang diinginkan dan rujukan berkenaan yang umum merentasi sektor infrastruktur kritikal. Teras menunjukkan piawaian, garis panduan dan amalan industri dengan cara yang membolehkan komunikasi aktiviti dan hasil keselamatan siber merentasi organisasi daripada aras eksekutif hingga aras pelaksanaan/pengendalian. Teras Rangka Kerja terdiri daripada lima Fungsi serentak dan berterusan—Kenal Pasti, Lindung, Kesan, Tindak Balas, Pulih. Apabila dipertimbangkan bersama, Fungsi ini memberikan pandangan strategik peringkat tinggi mengenai kitaran hayat pengurusan risiko keselamatan siber organisasi. Kemudian, Teras Rangka Kerja mengenal pasti Kategori dan Subkategori asas yang utama di bawahnya – yang merupakan hasil diskret – bagi setiap Fungsi dan memadankan hasil tersebut dengan contoh Rujukan Informatif seperti piawaian, garis panduan dan amalan sedia ada untuk setiap Subkategori.
- *Peringkat Pelaksanaan Rangka Kerja* ("Peringkat") memberikan konteks mengenai cara organisasi melihat risiko keselamatan siber dan proses yang disediakan untuk menguruskan risiko tersebut. Peringkat menerangkan sejauh mana amalan pengurusan risiko keselamatan siber organisasi mempamerkan ciri-ciri yang ditakrifkan dalam Rangka Kerja (misalnya, menyedari risiko dan ancaman, boleh ulang dan mudah suai). Peringkat tersebut mencirikan amalan organisasi dalam julat, daripada Separa (Peringkat 1) kepada Mudah Suai (Peringkat 4). Peringkat ini mencerminkan kemajuan daripada tindak balas tidak formal dan reaktif kepada pendekatan yang tangkas dan termaklum risiko. Semasa proses pemilihan Peringkat, organisasi perlu mempertimbang amalan pengurusan risiko semasa, persekitaran ancaman, keperluan undang-undang dan kawal selia, objektif perniagaan/misi dan kekangan organisasi.
- *Profil Rangka Kerja* ("Profil") mewakili hasil berdasarkan keperluan perniagaan yang telah dipilih oleh organisasi daripada Kategori dan Subkategori Rangka Kerja. Profil boleh dicirikan sebagai penjajaran piawaian, garis panduan dan amalan kepada Teras Rangka Kerja dalam senario pelaksanaan tertentu. Profil boleh digunakan bagi mengenal pasti peluang untuk meningkatkan postur keselamatan siber dengan membandingkan Profil "Semasa" (keadaan "sedia ada") dengan sebuah Profil "Sasaran" (keadaan "sasaran"). Untuk membangunkan Profil, organisasi boleh menyemak semua Kategori dan Subkategori dan, berdasarkan pemacu perniagaan/misi dan penilaian risiko, tentukan perkara paling penting; boleh tambahkan Kategori dan Subkategori mengikut keperluan untuk menangani risiko organisasi. Kemudian, Profil Semasa boleh digunakan untuk menyokong keutamaan dan pengukuran kemajuan ke arah Profil Sasaran, sambil mengambil kira keperluan perniagaan lain termasuk keberkesanan kos dan inovasi. Profil boleh digunakan untuk menjalankan penilaian diri dan berkomunikasi dalam organisasi atau antara organisasi.

1.2 Pengurusan Risiko dan Rangka Kerja Keselamatan Siber

Pengurusan Risiko ialah proses berterusan untuk mengenal pasti, menilai dan memberikan tindak balas terhadap risiko. Untuk menguruskan risiko, organisasi perlu memahami kemungkinan bahawa sesuatu peristiwa akan berlaku dan berpotensi memberikan impak. Dengan maklumat ini, organisasi dapat menentukan tahap risiko yang boleh diterima untuk mencapai objektif organisasi dan boleh menyatakan ini sebagai toleransi risiko organisasi tersebut.

Dengan pemahaman tentang toleransi risiko, organisasi boleh menentukan keutamaan kepada aktiviti keselamatan siber, membolehkan organisasi membuat keputusan termaklum berkenaan perbelanjaan keselamatan siber. Pelaksanaan program pengurusan risiko menawarkan organisasi keupayaan mengukur dan menyampaikan pelarasan kepada program keselamatan siber masing-masing. Organisasi boleh memilih untuk mengendalikan risiko dengan cara berbeza, termasuk mengurangkan, memindahkan, mengelakkan, atau menerima risiko, bergantung pada potensi impak kepada penyampaian perkhidmatan kritikal. Rangka Kerja menggunakan proses pengurusan risiko untuk membolehkan organisasi memaklumkan dan menentukan keutamaan dalam keputusan berkenaan keselamatan siber. Rangka Kerja ini menyokong penilaian risiko dan pengesahan pemacu perniagaan berulang bagi membantu organisasi memilih keadaan sasaran untuk aktiviti keselamatan siber yang mencerminkan hasil seperti diinginkan. Oleh itu, Rangka Kerja ini memberikan organisasi keupayaan untuk memilih dan mengarahkan penambahbaikan secara dinamik dalam pengurusan risiko keselamatan siber bagi persekitaran IT dan ICS.

Rangka Kerja ini bersifat mudah suai supaya dapat memberikan pelaksanaan fleksibel dan berasaskan risiko yang boleh digunakan dengan pelbagai proses pengurusan risiko keselamatan siber. Contoh proses pengurusan risiko keselamatan siber termasuk Pertubuhan Pemiawaian Antarabangsa (International Organization for Standardization-ISO) 31000:2009[6], ISO/Suruhanjaya Elektroteknik Antarabangsa (International Electrotechnical Commission-IEC) 27005:2011[7], Penerbitan Khas NIST (Special Publication-SP) 800-39[8] dan garis panduan Proses Pengurusan Risiko Keselamatan Siber Subsektor Elektrik (*Electricity Subsector Cybersecurity Risk Management Process*-RMP)[9].

1.3 Gambaran Keseluruhan Dokumen

Bahagian selebihnya daripada dokumen ini mengandungi seksyen dan lampiran berikut :

- Seksyen 2 menerangkan komponen Rangka Kerja: Teras Rangka Kerja, Peringkat dan Profil.
- Seksyen 3 menunjukkan contoh cara Rangka Kerja boleh digunakan.
- Seksyen 4 menerangkan cara menggunakan Rangka Kerja untuk penilaian diri dan mempamerkan keselamatan siber melalui pengukuran.

---

[6] Pertubuhan Pemiawaian Antarabangsa (International Organization for Standardization), *Pengurusan risiko – Prinsip dan garis panduan (Risk management – Principles and guidelines)*, ISO 31000:2009, 2009. http://www.iso.org/iso/home/standards/iso31000.htm

[7] Pertubuhan Pemiawaian Antarabangsa (International Organization for Standardization)/Suruhanjaya Elektroteknik Antarabangsa, *Teknologi maklumat – Teknik keselamatan – Pengurusan risiko keselamatan maklumat*, (International Electrotechnical Commission, *Information technology – Security techniques – Information security risk management)*, ISO/IEC 27005:2011, 2011. https://www.iso.org/standard/56742.html

[8] Inisiatif Transformasi Pasukan Petugas Bersama, *Menguruskan Risiko Keselamatan Maklumat: Organisasi, Misi dan Paparan Sistem Maklumat,* Penerbitan Khas NIST (Joint Task Force Transformation Initiative, *Managing Information Security Risk: Organization, Mission, and Information System View*, NIST Special Publication) 800-39, Mac 2011. https://doi.org/10.6028/NIST.SP.80039

[9] Jabatan Tenaga Amerika Syarikat, *Proses Pengurusan Risiko Keselamatan Siber Subsektor Elektrik* (U.S. Department of Energy, *Electricity Subsector Cybersecurity Risk Management Process)*, DOE/OE-0003, May 2012. https://energy.gov/sites/prod/files/Cybersecurity_Risk_Management_Process_Guideline_-_Final_-_May_2012.pdf

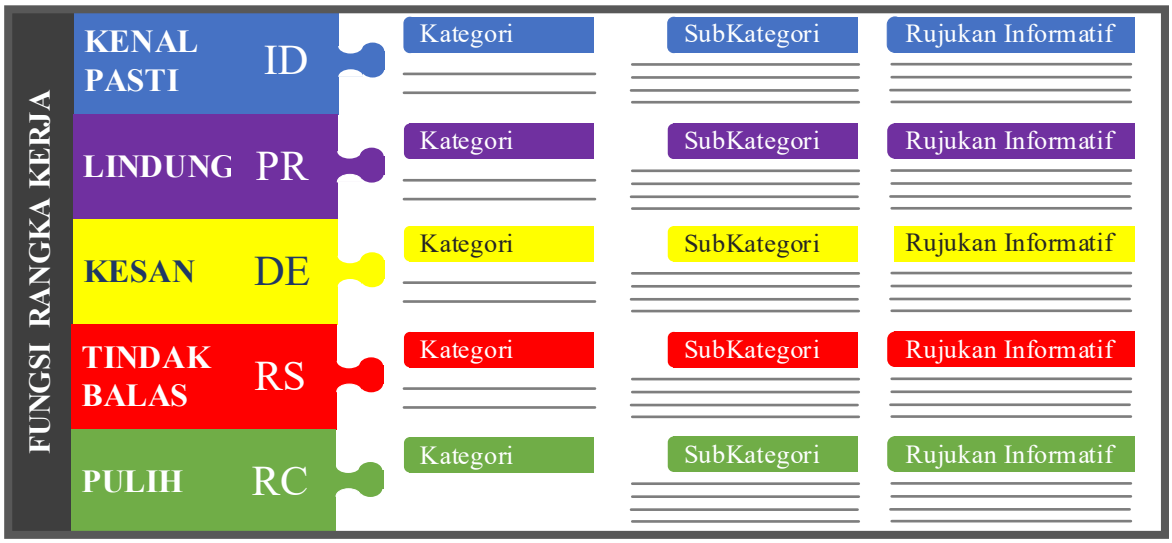
- Lampiran A menunjukkan Teras Rangka Kerja dalam format jadual: Fungsi, Kategori, Subkategori dan Rujukan Informatif.
- Lampiran B mengandungi glosari istilah terpilih.
- Lampiran C menyenaraikan akronim yang digunakan dalam dokumen ini.

2.0 Asas Rangka Kerja

Rangka Kerja menyediakan bahasa umum untuk memahami, menguruskan dan menjelaskan risiko keselamatan siber kepada pihak berkepentingan dalaman dan luaran. Rangka Kerja ini boleh digunakan untuk membantu mengenal pasti dan menentukan keutamaan kepada tindakan untuk mengurangkan risiko keselamatan siber dan merupakan alat untuk menjajarkan pendekatan dasar, perniagaan dan teknologi bagi menguruskan risiko tersebut. Rangka Kerja ini juga boleh digunakan untuk menguruskan risiko keselamatan siber merentasi keseluruhan organisasi atau difokuskan kepada penyampaian perkhidmatan kritikal dalam organisasi. Jenis entiti berbeza – termasuk struktur, persatuan dan organisasi penyelarasan sektor – boleh menggunakan Rangka Kerja untuk tujuan berbeza termasuk penciptaan Profil umum.

2.1 Teras Rangka Kerja

Teras Rangka Kerja menyediakan set aktiviti untuk mencapai hasil keselamatan siber yang khusus dan contoh rujukan panduan untuk mencapai hasil tersebut. Teras bukan senarai semak tindakan yang perlu dilaksanakan. Teras membentangkan hasil utama keselamatan siber yang dikenal pasti oleh pihak berkepentingan sebagai berguna dalam menguruskan risiko keselamatan siber. Teras terdiri daripada empat elemen: Fungsi, Kategori, Subkategori dan Rujukan Informatif, ditunjukkan dalam **Rajah 1**:



Rajah 1: Struktur Teras Rangka Kerja

Elemen Teras Rangka Kerja berfungsi bersama seperti berikut:

- **Fungsi** mengatur aktiviti asas keselamatan siber pada tahap tertinggi masing-masing. Fungsi ini ialah Kenal pasti, Lindung, Kesan, Tindak balas, Pulih. Semua fungsi ini membantu organisasi dalam menyatakan pengurusan risiko keselamatan siber dengan mengatur maklumat, membolehkan keputusan pengurusan risiko, menangani ancaman dan menambah baik dengan mempelajari daripada aktiviti terdahulu. Fungsi ini juga sejajar dengan pengkaedahan sedia ada bagi pengurusan kejadian dan membantu

menunjukkan impak pelaburan dalam keselamatan siber. Sebagai contoh, pelaburan dalam perancangan dan latihan menyokong tindak balas yang tepat pada masanya dan tindakan pemulihan, menghasilkan impak yang berkurangan kepada penyampaian perkhidmatan.

- **Kategori** ialah subbahagian Fungsi kepada kumpulan hasil keselamatan siber yang berkait rapat dengan keperluan program dan aktiviti tertentu. Contoh Kategori termasuk "Pengurusan Aset", "Pengurusan Identiti dan Kawalan Akses" dan "Proses Pengesanan".
- **SubKategori** membahagikan lagi Kategori kepada hasil khusus aktiviti teknikal dan/atau pengurusan. Subkategori ini menyediakan set keputusan yang, walaupun tidak menyeluruh, membantu menyokong pencapaian hasil dalam setiap Kategori. Contoh Subkategori termasuk "Sistem maklumat luaran dikatalogkan", "Data-dalam-simpanan dilindungi" dan "Pemberitahuan daripada sistem pengesanan disiasat".
- **Rujukan Informatif** ialah seksyen piawaian, garis panduan dan amalan khusus yang umum dalam kalangan sektor infrastruktur kritikal yang menggambarkan kaedah untuk mencapai hasil berkaitan dengan setiap Subkategori. Rujukan informatif yang dibentangkan dalam Teras Rangka Kerja ialah sekadar ilustrasi dan bukan menyeluruh. Rujukan adalah berdasarkan panduan merentasi sektor yang paling kerap dirujuk semasa proses pembangunan Rangka Kerja.

Lima Fungsi Teras Rangka Kerja ditakrifkan di bawah. Fungsi ini bukan bertujuan membentuk laluan bersiri atau menjuruskan kepada keadaan akhir statik yang diingini. Sebaliknya, Fungsi ini perlu dilakukan serentak dan berterusan untuk membentuk budaya pengendalian yang menangani risiko keselamatan siber yang dinamik. Lihat Lampiran A untuk penyenaraian lengkap Teras Rangka Kerja.

- **Kenal pasti** – Membangunkan pemahaman organisasi untuk menguruskan risiko keselamatan siber terhadap sistem, warga kerja, aset, data dan keupayaan.

  Aktiviti dalam Fungsi Kenal Pasti ialah asas untuk penggunaan Rangka Kerja secara berkesan. Memahami konteks perniagaan, sumber yang menyokong fungsi kritikal dan risiko keselamatan siber yang berkaitan membolehkan organisasi memfokuskan dan memberikan keutamaan kepada usaha, selaras dengan strategi pengurusan risiko dan keperluan perniagaan. Contoh Kategori hasil dalam Fungsi ini termasuk: Pengurusan Aset; Persekitaran Perniagaan; Tadbir Urus, Penilaian Risiko dan Strategi Pengurusan Risiko.

- **Lindung** – Membangunkan dan melaksanakan perlindungan yang sesuai untuk memastikan penyampaian perkhidmatan kritikal. Fungsi Lindung menyokong keupayaan mengehadkan atau membendung impak peristiwa keselamatan siber yang berpotensi berlaku. Contoh Kategori hasil dalam Fungsi ini termasuk: Pengurusan Identiti dan Kawalan Akses; Kesedaran dan Latihan; Keselamatan Data; Proses dan Prosedur Perlindungan Maklumat; Penyelenggaraan; dan Teknologi Perlindungan.

- **Kesan** – Membangunkan dan melaksanakan aktiviti yang sesuai untuk mengenal pasti peristiwa keselamatan siber yang berlaku.

  Fungsi Kesan membolehkan penemuan peristiwa keselamatan siber tepat pada masanya. Contoh Kategori hasil dalam Fungsi ini termasuk:
  Anomali dan Peristiwa, Pemantauan Keselamatan Secara Berterusan dan Proses Pengesanan.
- **Tindak balas** – Membangunkan dan melaksanakan aktiviti yang sesuai untuk mengambil tindakan berhubung kejadian keselamatan siber yang dikesan.

  Fungsi Tindak balas menyokong keupayaan untuk membendung impak kejadian keselamatan siber yang berpotensi berlaku. Contoh Kategori hasil dalam Fungsi ini termasuk: Perancangan Tindak balas; Komunikasi; Analisis; Pengurangan; dan Penambahbaikan.

- **Pulih** – Membangunkan dan melaksanakan aktiviti yang sesuai bagi mengekalkan rancangan untuk kebingkasan dan memulihkan apa-apa keupayaan atau perkhidmatan yang terjejas akibat kejadian keselamatan siber.

  Fungsi Pulih menyokong pemulihan yang tepat pada masanya kepada pengendalian normal bagi mengurangkan impak daripada kejadian keselamatan siber. Contoh Kategori hasil dalam Fungsi ini termasuk: Perancangan Pemulihan; Penambahbaikan; dan Komunikasi.

2.2 Peringkat Pelaksanaan Rangka Kerja

Peringkat Pelaksanaan Rangka Kerja ("Peringkat") memberikan konteks mengenai cara organisasi melihat risiko keselamatan siber dan proses yang disediakan untuk menguruskan risiko tersebut. Bermula daripada Separa (Peringkat 1) hingga Mudah Suai (Peringkat 4), Peringkat menerangkan tahap ketegasan dan kecanggihan yang semakin meningkat dalam amalan pengurusan risiko keselamatan siber. Peringkat ini membantu menentukan sejauh mana pengurusan risiko keselamatan siber dimaklumkan oleh keperluan perniagaan dan diintegrasikan ke dalam keseluruhan amalan pengurusan risiko organisasi. Pertimbangan pengurusan risiko merangkumi banyak aspek keselamatan siber, termasuk sejauh mana pertimbangan privasi dan kebebasan awam diintegrasikan ke dalam pengurusan risiko keselamatan siber organisasi dan tindak balas risiko yang berpotensi berlaku.

Proses pemilihan Peringkat mempertimbang amalan pengurusan risiko semasa, persekitaran ancaman, keperluan undang-undang dan kawal selia , amalan-amalan perkongsian maklumat, objektif-objektif perniagaan/misi, keperluan keselamatan siber rantaian bekalan dan kekangan organisasi. Organisasi perlu menentukan Peringkat yang diingini, memastikan bahawa tahap yang dipilih memenuhi matlamat organisasi, boleh dilaksanakan dan mengurangkan risiko keselamatan siber terhadap aset dan sumber kritikal kepada tahap yang boleh diterima oleh organisasi Organisasi perlu mempertimbang untuk memanfaatkan panduan luaran yang diperoleh daripada jabatan dan agensi kerajaan Persekutuan, Pusat Perkongsian dan Analisis Maklumat (ISAC), Organisasi Perkongsian dan Analisis Maklumat (ISAO), model kematangan sedia ada, atau sumber lain untuk membantu dalam menentukan peringkat yang diingini. Walaupun organisasi yang dikenal pasti sebagai Peringkat 1 (Separa) digalakkan untuk mempertimbang bergerak ke arah Peringkat 2 atau lebih tinggi, Peringkat tidak mewakili tahap kematangan.

Peringkat bertujuan menyokong pembuatan keputusan organisasi tentang cara menguruskan risiko keselamatan siber, serta dimensi organisasi yang lebih diutamakan dan boleh menerima sumber tambahan. Kemajuan kepada Peringkat lebih tinggi digalakkan apabila analisis kos faedah menunjukkan pengurangan risiko keselamatan siber yang boleh dilaksanakan dan berkesan kos.

Pelaksanaan Rangka Kerja yang berjaya adalah berdasarkan pencapaian hasil yang diterangkan dalam Profil Sasaran organisasi dan bukan berdasarkan penentuan Peringkat. Namun begitu, pemilihan dan penetapan peringkat secara semula jadi mempengaruhi Profil Rangka Kerja. Saranan Peringkat oleh para pengurus Aras Perniagaan/Proses, seperti yang diluluskan oleh Aras Eksekutif Kanan, akan membantu menetapkan nada keseluruhan tentang cara risiko keselamatan siber akan diuruskan dalam organisasi dan perlu mempengaruhi keutamaan dalam Profil Sasaran dan penilaian kemajuan semasa menangani jurang.

Takrifan Peringkat ialah seperti berikut:

Peringkat 1: Separa

- *Proses Pengurusan Risiko* – Amalan pengurusan risiko siber organisasi tidak diformalkan dan risiko diuruskan secara ad hoc dan Kadangkala secara reaktif. Pengutamaan aktiviti keselamatan siber mungkin tidak dimaklumkan secara langsung oleh objektif risiko organisasi, persekitaran ancaman, atau keperluan perniagaan/misi
- *Program Pengurusan Risiko Berintegrasi* – Terdapat kesedaran terhad tentang risiko keselamatan siber pada peringkat organisasi. Organisasi mungkin melaksanakan pengurusan risiko keselamatan siber secara tidak teratur, mengikut kes demi kes disebabkan oleh pengalaman atau maklumat yang diperoleh daripada sumber luar. Organisasi mungkin tidak mempunyai proses yang membolehkan maklumat keselamatan siber dikongsi dalam organisasi.
- *Penyertaan Luaran* – Organisasi tidak memahami peranan sendiri dalam ekosistem yang lebih besar berkenaan dengan sama ada kebergantungan atau tanggungan. Organisasi secara umumnya tidak bekerjasama atau menerima maklumat (misalnya, risikan ancaman, amalan terbaik, teknologi) daripada entiti lain (misalnya pembeli, pembekal, kebergantungan, tanggungan, ISAO, penyelidik, kerajaan) dan tidak juga berkongsi maklumat. Organisasi tersebut secara umumnya tidak menyedari risiko rantaian bekalan siber bagi produk dan perkhidmatan yang sediakan dan digunakan.

Peringkat 2: Risiko Dimaklumkan

- *Proses Pengurusan Risiko* – Amalan pengurusan risiko diluluskan oleh pihak pengurusan tetapi mungkin tidak ditetapkan sebagai dasar seluruh organisasi. Pengutamaan aktiviti keselamatan siber dan keperluan perlindungan dimaklumkan secara langsung oleh objektif risiko organisasi, persekitaran ancaman atau keperluan perniagaan/misi.
- *Program Pengurusan Risiko Berintegrasi* – Terdapat kesedaran mengenai risiko keselamatan siber pada peringkat organisasi, tetapi pendekatan seluruh organisasi untuk menguruskan risiko keselamatan siber belum diwujudkan. Maklumat keselamatan siber dikongsi dalam organisasi secara tidak formal. Pertimbangan keselamatan siber dalam objektif dan program organisasi mungkin berlaku pada beberapa tahap tetapi bukan

semua tahap dalam organisasi. Penilaian risiko siber aset organisasi dan luaran berlaku, tetapi kebiasaanya tidak berulang atau berlaku lagi.

- *Penyertaan Luaran* – Secara umumnya, organisasi memahami peranan yang dimainkan dalam ekosistem lebih besar berkenaan sama ada kebergantungan atau tanggungan sendiri, tetapi bukan kedua-duanya. Organisasi bekerjasama dan menerima sebahagian maklumat daripada entiti lain, serta menghasilkan sebahagian maklumat sendiri, tetapi mungkin tidak berkongsi maklumat berkenaan dengan yang lain. Selain itu, organisasi menyedari risiko rantaian bekalan siber yang dikaitkan dengan produk dan perkhidmatan yang disediakan dan digunakan oleh organisasi, tetapi tidak bertindak secara konsisten atau formal terhadap risiko tersebut.

Peringkat 3: Boleh Ulang

- *Proses Pengurusan Risiko* – Amalan pengurusan risiko organisasi diluluskan dan dinyatakan secara formal sebagai dasar. Amalan keselamatan siber organisasi sentiasa dikemas kini berdasarkan penerapan proses pengurusan risiko kepada perubahan dalam keperluan perniagaan/misi, serta ancaman dan landskap teknologi yang berubah.
- *Program Pengurusan Risiko Berintegrasi* – Terdapat pendekatan seluruh organisasi untuk menguruskan risiko keselamatan siber. Dasar, proses dan prosedur yang risiko dimaklumkan ditakrifkan, dilaksanakan seperti yang dimaksudkan dan disemak. Kaedah yang konsisten disediakan untuk bertindak balas secara berkesan terhadap perubahan dalam risiko. Kakitangan mempunyai pengetahuan dan kemahiran untuk melaksanakan peranan dan tanggungjawab yang diberikan. Organisasi tersebut secara konsisten dan tepat memantau risiko keselamatan siber aset organisasi. Para eksekutif kanan keselamatan siber dan bukan keselamatan siber berkomunikasi dengan kerap berkenaan risiko keselamatan siber. Para eksekutif kanan memastikan pertimbangan keselamatan siber berada pada semua barisan pengendalian dalam organisasi.
- *Penyertaan Luaran* – Organisasi memahami peranan, kebergantungan dan tanggungan sendiri dalam ekosistem yang lebih besar dan boleh menyumbang kepada pemahaman komuniti yang lebih luas mengenai risiko. Organisasi juga bekerjasama dan menerima maklumat daripada entiti lain dengan kerap yang melengkapkan maklumat yang dihasilkan secara dalaman dan berkongsi maklumat dengan entiti lain. Organisasi sedar tentang risiko rantaian bekalan siber yang dikaitkan dengan produk dan perkhidmatan yang disediakan dan digunakan. Di samping itu, organisasi kebiasaannya bertindak secara formal ke atas risiko tersebut, termasuk mekanisme seperti perjanjian bertulis untuk menyampaikan keperluan garis dasar, struktur tadbir urus (misalnya, majlis risiko), serta pelaksanaan dan pemantauan dasar.

Peringkat 4: Mudah Suai

- *Proses Pengurusan Risiko* – Organisasi menyesuaikan amalan keselamatan siber berdasarkan aktiviti keselamatan siber terdahulu dan semasa, termasuk pengajaran yang diperoleh dan petunjuk ramalan. Melalui proses penambahbaikan berterusan yang menggabungkan teknologi dan amalan keselamatan siber termaju, organisasi secara aktif menyesuaikan diri dengan perubahan ancaman dan landskap teknologi, serta bertindak

balas tepat pada masanya dan berkesan terhadap ancaman yang semakin berkembang dan canggih.

- *Program Pengurusan Risiko Berintegrasi* – Terdapat pendekatan seluruh organisasi untuk menguruskan risiko keselamatan siber yang menggunakan dasar, proses dan prosedur risiko dimaklumkan untuk menangani peristiwa keselamatan siber yang berpotensi berlaku. Hubungan antara risiko keselamatan siber dan objektif organisasi difahami dengan jelas dan dipertimbangkan semasa membuat keputusan. Eksekutif kanan memantau risiko keselamatan siber dalam konteks yang sama seperti risiko kewangan dan risiko organisasi yang lain. Belanjawan organisasi adalah berdasarkan pemahaman tentang persekitaran risiko semasa dan diramalkan, serta toleransi risiko. Unit perniagaan melaksanakan visi eksekutif dan menganalisis risiko tahap sistem dalam konteks toleransi risiko organisasi. Pengurusan risiko keselamatan siber ialah sebahagian daripada budaya organisasi dan berkembang daripada kesedaran tentang aktiviti terdahulu dan kesedaran berterusan aktiviti dalam sistem dan rangkaian organisasi berkenaan. Organisasi boleh dengan pantas dan cekap mengambil kira perubahan kepada objektif perniagaan/misi dengan cara risiko diuruskan dan disampaikan.

- *Penyertaan Luaran* – Organisasi memahami peranan, kebergantungan dan tanggungan sendiri dalam ekosistem yang lebih besar dan boleh menyumbang kepada pemahaman komuniti yang lebih luas tentang risiko. Organisasi juga menerima, menghasilkan dan menyemak maklumat yang diberi keutamaan yang memaklumkan analisis berterusan mengenai risiko apabila ancaman dan landskap teknologi berkembang. Organisasi berkongsi maklumat tersebut secara dalaman dan luaran dengan rakan usaha sama lain. Organisasi menggunakan maklumat masa nyata atau hampir masa nyata untuk memahami dan bertindak secara konsisten terhadap risiko rantaian bekalan siber yang berkaitan dengan produk dan perkhidmatan yang disediakan dan digunakan. Selain itu, organisasi berkomunikasi secara proaktif, menggunakan mekanisme formal (misalnya, perjanjian) dan tidak formal untuk membangunkan dan mengekalkan hubungan rantaian bekalan yang kukuh.

2.3 Profil Rangka Kerja

Profil Rangka Kerja (“Profil”) ialah penjajaran Fungsi, Kategori dan Subkategori dengan keperluan perniagaan, toleransi risiko dan sumber organisasi. Profil membolehkan organisasi mewujudkan hala tuju untuk mengurangkan risiko keselamatan siber yang sejajar dengan matlamat organisasi dan sektor, dengan mempertimbang keperluan undang-undang/kawal selia dan amalan terbaik industri, serta mencerminkan keutamaan pengurusan risiko. Memandangkan keadaan yang kompleks dalam banyak organisasi, berbilang profil mungkin menjadi pilihan, sejajar dengan komponen tertentu dan mengiktiraf keperluan masing-masing.

Profil Rangka Kerja boleh digunakan untuk menerangkan keadaan semasa atau keadaan sasaran yang diingini bagi aktiviti keselamatan siber tertentu. Profil Semasa menunjukkan hasil keselamatan siber yang dicapai. Profil Sasaran menunjukkan hasil yang diperlukan untuk mencapai matlamat pengurusan risiko keselamatan siber yang diingini. Profil menyokong

keperluan perniagaan/misi dan membantu dalam menyampaikan risiko dalaman dan antara organisasi. Rangka Kerja ini tidak menetapkan templat Profil, membenarkan fleksibiliti dalam pelaksanaan.

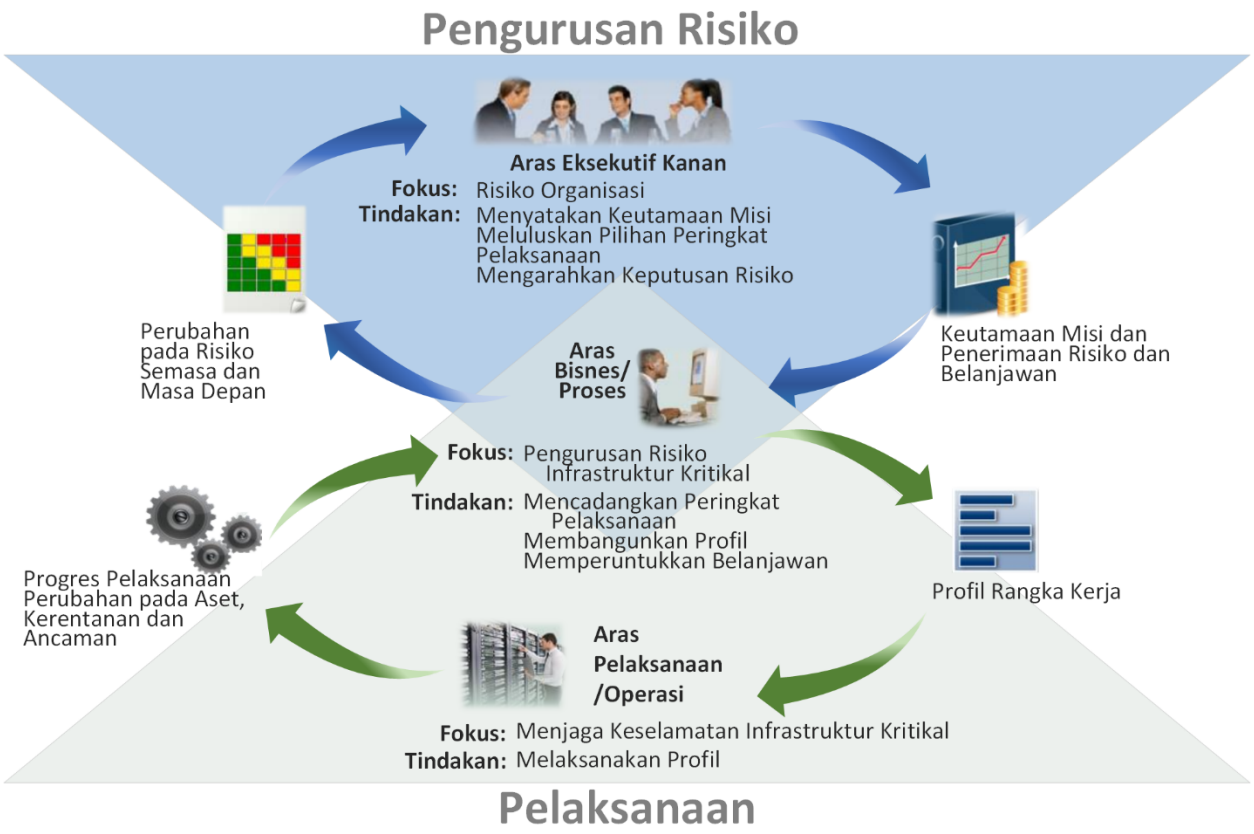
Perbandingan Profil (misalnya, Profil Semasa dan Profil Sasaran) mungkin mendedahkan jurang yang perlu ditangani bagi memenuhi objektif pengurusan risiko keselamatan siber. Pelan tindakan untuk menangani jurang ini bagi memenuhi Kategori atau Subkategori tertentu boleh menyumbang kepada hala tuju yang diterangkan di atas. Memberikan keutamaan kepada pengurangan jurang didorong oleh keperluan perniagaan dan proses pengurusan risiko organisasi. Pendekatan berasaskan risiko ini membolehkan organisasi mengukur sumber yang diperlukan (misalnya, perjawatan, pembiayaan) untuk mencapai matlamat keselamatan siber dengan cara berkesan kos dan ditentukan keutamaan. Tambahan pula, Rangka Kerja ini ialah pendekatan berasaskan risiko yang kebolehgunaan dan pemenuhan Subkategori tertentu adalah tertakluk kepada skop Profil.

2.4 Penyelarasan Pelaksanaan Rangka Kerja

Rajah 2 menerangkan aliran umum maklumat dan keputusan pada aras berikut dalam organisasi:

- Eksekutif
- Perniagaan/Proses
- Pelaksanaan/Pengendalian

Aras eksekutif menyampaikan keutamaan misi, sumber yang tersedia dan toleransi risiko keseluruhan kepada aras perniagaan/proses. Aras perniagaan/proses menggunakan maklumat tersebut sebagai input ke dalam proses pengurusan risiko dan kemudian bekerjasama dengan aras pelaksanaan/pengendalian untuk menyampaikan keperluan perniagaan dan mencipta Profil. Aras pelaksanaan/pengendalian menyampaikan kemajuan pelaksanaan Profil pada aras perniagaan/proses. Aras perniagaan/proses menggunakan maklumat ini untuk melaksanakan penilaian impak. Pengurusan aras perniagaan/proses melaporkan hasil penilaian impak tersebut kepada aras eksekutif untuk memaklumkan keseluruhan proses pengurusan risiko organisasi dan kepada aras pelaksanaan/operasi untuk kesedaran tentang impak perniagaan.



Rajah 2: Maklumat Cadangan dan Aliran Keputusan dalam Organisasi

3.0 Cara Menggunakan Rangka Kerja

Organisasi boleh menggunakan Rangka Kerja sebagai bahagian utama dalam proses sistematik bagi mengenal pasti, menilai dan menguruskan risiko keselamatan siber. Rangka Kerja tidak direka bentuk untuk menggantikan proses sedia ada; organisasi boleh menggunakan proses semasa dan memadankan dengan Rangka Kerja ini untuk menentukan jurang dalam pendekatan risiko keselamatan siber semasa dan membangunkan hala tuju ke arah penambahbaikan. Menggunakan Rangka Kerja sebagai alat pengurusan risiko keselamatan siber, organisasi boleh menentukan aktiviti yang paling penting untuk penyampaian perkhidmatan kritikal dan menentukan keutamaan dalam perbelanjaan, bagi memaksimumkan impak pelaburan.

Rangka Kerja ini direka bentuk untuk melengkapkan pengendalian perniagaan dan keselamatan siber sedia ada. Rangka Kerja boleh berfungsi sebagai asas untuk program keselamatan siber baharu atau mekanisme untuk menambah baik program sedia ada. Rangka Kerja ini menyediakan cara untuk menyatakan keperluan keselamatan siber kepada rakan kongsi perniagaan dan para pelanggan, serta boleh membantu mengenal pasti jurang dalam amalan keselamatan siber organisasi. Rangka Kerja ini juga memberikan set pertimbangan dan proses umum bagi mengambil kira implikasi privasi dan kebebasan awam dalam konteks program keselamatan siber.

Rangka Kerja boleh digunakan sepanjang fasa kitaran hayat pelan, reka bentuk, bina/beli, penggunaan, pengendalian dan penyahtauliahan. Fasa pelan memulakan kitaran mana-mana sistem dan meletakkan asas untuk semua perkara yang menyusul selepas itu. Pertimbangan keselamatan siber yang menyeluruh perlu diisytiharkan dan diterangkan sejelas mungkin. Pelan tersebut perlu mengiktiraf bahawa pertimbangan dan keperluan tersebut berkemungkinan akan berkembang dalam tempoh baki kitaran hayat. Fasa reka bentuk perlu mengambil kira keperluan keselamatan siber sebagai sebahagian daripada proses kejuruteraan sistem pelbagai disiplin yang lebih besar.[10] Pencapaian penting dalam fasa reka bentuk ialah pengesahan bahawa spesifikasi keselamatan siber sistem adalah sepadan dengan keperluan dan kecenderungan risiko organisasi seperti yang direkodkan dalam Profil Rangka Kerja. Hasil keselamatan siber yang diingini, serta ditentukan keutamaan dalam Profil Sasaran perlu digabungkan apabila a) membangunkan sistem semasa fasa binaan dan b) membeli atau menyumber luar sistem semasa fasa pembelian. Profil Sasaran yang sama itu berfungsi sebagai senarai ciri-ciri keselamatan siber sistem yang perlu dinilai apabila menggunakan sistem untuk mengesahkan semua ciri dilaksanakan. Hasil keselamatan siber yang ditentukan dengan menggunakan Rangka Kerja ini, kemudian menjadi asas untuk pengendalian berterusan sistem tersebut. Ini termasuk penilaian semula secara sekali-sekala, dengan merekodkan keputusan dalam Profil Semasa, untuk mengesahkan bahawa keperluan keselamatan siber masih dipenuhi. Lazimnya, rangkaian kebergantungan yang kompleks (misalnya, pampasan dan kawalan umum) antara sistem bermaksud hasil yang didokumenkan dalam Profil Sasaran sistem berkaitan perlu dipertimbangkan dengan teliti kerana sistem telah dilucutkan tauliah.

Seksyen berikut membentangkan cara berbeza organisasi boleh menggunakan Rangka Kerja.

[10] NIST Special Publication 800-160 Volume 1, *System Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, Ross et al, November 2016 (updated March 21, 2018), https://doi.org/10.6028/NIST.SP.800-160v1

3.1 Penilaian Asas Amalan Keselamatan Siber

Rangka Kerja boleh digunakan untuk membandingkan aktiviti keselamatan siber semasa organisasi dengan aktiviti yang digariskan dalam Teras Rangka Kerja. Melalui penciptaan Profil Semasa, organisasi boleh mengkaji sejauh mana hasil dicapai seperti yang diterangkan dalam Kategori Teras dan Subkategori, sejajar dengan lima Fungsi tahap tinggi: Kenal Pasti, Lindung, Kesan, Tindak Balas dan Pulih. Organisasi mungkin mendapati bahawa hasil yang diingini sudah dicapai, sekaligus menguruskan keselamatan siber yang sepadan dengan risiko yang diketahui. Sebagai alternatif, organisasi boleh menentukan bahawa terdapat peluang untuk (atau perlu) menambah baik. Organisasi boleh menggunakan maklumat tersebut untuk membangunkan pelan tindakan bagi mengukuhkan amalan keselamatan siber sedia ada dan mengurangkan risiko keselamatan siber. Organisasi juga mungkin mendapati bahawa terlalu banyak pelaburan dibuat untuk mencapai hasil tertentu. Organisasi boleh menggunakan maklumat ini untuk memberikan semula keutamaan kepada sumber.

Walaupun organisasi tidak menggantikan proses pengurusan risiko, lima Fungsi tahap tinggi ini menyediakan cara ringkas bagi eksekutif kanan dan individu lain untuk menyaring konsep asas risiko keselamatan siber supaya mereka boleh menilai cara risiko yang dikenal pasti diuruskan dan cara organisasi mereka disusun pada tahap tinggi berbanding piawaian, garis panduan dan amalan keselamatan siber sedia ada. Rangka Kerja ini juga boleh membantu organisasi menjawab soalan asas, termasuk "Bagaimanakah keadaan kita?" Kemudian organisasi boleh bergerak dengan cara yang lebih termaklum untuk mengukuhkan amalan keselamatan siber di tempat dan pada masa yang sesuai apabila dianggap perlu.

3.2 Mencipta atau Menambah Baik Program Keselamatan Siber

Langkah berikut menggambarkan cara organisasi boleh menggunakan Rangka Kerja untuk mewujudkan program keselamatan siber baharu atau menambah baik program sedia ada. Langkah ini perlu diulangi menurut keperluan untuk terus menambah baik keselamatan siber

Langkah 1: Memberikan Keutamaan dan Skop. Organisasi mengenal pasti objektif perniagaan/misi dan keutamaan organisasi tahap tinggi. Dengan maklumat ini, organisasi membuat keputusan strategik berkenaan pelaksanaan keselamatan siber dan menentukan skop sistem dan aset yang menyokong barisan atau proses perniagaan yang dipilih. Rangka Kerja boleh disesuaikan untuk menyokong barisan atau proses perniagaan yang berbeza dalam organisasi yang mungkin mempunyai keperluan perniagaan berbeza dan toleransi risiko yang berkaitan. Toleransi risiko mungkin ditunjukkan dalam Peringkat Pelaksanaan sasaran.

Langkah 2: Mengorientasikan. Setelah skop program keselamatan siber ditentukan untuk barisan atau proses perniagaan, organisasi mengenal pasti sistem dan aset, keperluan kawal selia dan pendekatan risiko keseluruhan yang berkaitan. Kemudian, organisasi merujuk kepada sumber untuk mengenal pasti ancaman dan kerentanan yang berkenaan dengan sistem dan aset tersebut.

Langkah 3: Mewujudkan Profil Semasa. Organisasi membangunkan Profil Semasa dengan menunjukkan hasil Kategori dan Subkategori daripada Teras Rangka Kerja yang dicapai pada masa ini. Jika hanya sebahagian hasil dicapai, dengan mengambil perhatian mengenai fakta ini akan membantu menyokong langkah seterusnya melalui penyediaan maklumat asas.

Langkah 4: Melakukan Penilaian Risiko. Penilaian ini boleh dipandu oleh keseluruhan proses pengurusan risiko organisasi atau aktiviti penilaian risiko terdahulu. Organisasi menganalisis persekitaran pengendalian bertujuan melihat kemungkinan peristiwa keselamatan siber berlaku dan impak yang boleh diberikan oleh peristiwa itu ke atas organisasi. Penting bagi organisasi mengenal pasti risiko yang muncul dan menggunakan maklumat ancaman siber daripada sumber dalaman dan luaran untuk mendapatkan pemahaman yang lebih baik tentang kemungkinan peristiwa keselamatan siber berlaku dan impak yang diberikan.

Langkah 5: Mewujudkan Profil Sasaran. Organisasi ~~mencipta~~ mewujudkan Profil Sasaran yang memfokuskan kepada penilaian Rangka Kerja Kategori dan Subkategori yang menerangkan hasil keselamatan siber yang diinginkan oleh organisasi. Organisasi juga boleh membangunkan Kategori dan Subkategori tambahan masing-masing untuk mengambil kira risiko organisasi yang unik. Organisasi juga boleh mempertimbang pengaruh dan keperluan pihak berkepentingan luar seperti entiti sektor, pelanggan dan rakan kongsi perniagaan semasa mencipta Profil Sasaran. Profil Sasaran perlu mencerminkan kriteria yang sesuai dalam Peringkat Pelaksanaan sasaran.

Langkah 6: Menentukan, Menganalisis dan Memberikan Keutamaan kepada Jurang. Organisasi membandingkan Profil Semasa dan Profil Sasaran untuk menentukan jurang. Seterusnya, organisasi mencipta pelan tindakan yang memberikan keutamaan untuk menangani jurang – merangkumi pemacu, kos dan faedah serta risiko misi – untuk mencapai hasil dalam Profil Sasaran. Kemudian organisasi menentukan sumber, termasuk pembiayaan dan tenaga kerja yang diperlukan untuk menangani jurang tersebut. Menggunakan Profil dengan cara ini akan menggalakkan organisasi membuat keputusan termaklum tentang aktiviti keselamatan siber, menyokong pengurusan risiko dan membolehkan organisasi melaksanakan penambahbaikan bersasaran secara berkesan kos.

Langkah 7: Melaksanakan Pelan Tindakan. Organisasi menentukan tindakan yang perlu diambil untuk menangani jurang, jika ada, yang dikenal pasti dalam langkah terdahulu dan kemudian melaraskan amalan keselamatan siber semasa untuk mencapai Profil Sasaran. Untuk panduan lanjut, Rangka Kerja mengenal pasti contoh Rujukan Informatif berkenaan Kategori dan Subkategori, tetapi organisasi perlu menentukan piawaian, garis panduan dan amalan, termasuk yang khusus mengikut sektor, paling sesuai untuk keperluan masing-masing.

Organisasi mengulangi langkah seperti yang diperlukan untuk terus menilai dan meningkatkan keselamatan siber. Sebagai contoh, organisasi mungkin mendapati bahawa pengulangan langkah mengorientasikan dengan lebih kerap menambah baik kualiti penilaian risiko. Tambahan pula, organisasi boleh memantau kemajuan melalui kemas kini berulang kepada Profil Semasa, seterusnya membandingkan Profil Semasa dengan Profil Sasaran. Organisasi juga boleh menggunakan proses ini untuk menyelaraskan program keselamatan siber masing-masing dengan Peringkat Pelaksanaan Rangka Kerja yang diingini.

3.3 Menyampaikan Keperluan Keselamatan Siber kepada Pihak Berkepentingan

Rangka Kerja menyediakan bahasa umum bagi menyampaikan keperluan dalam kalangan pihak berkepentingan yang saling bergantung dan bertanggungjawab untuk penghantaran produk dan penyampaian perkhidmatan infrastruktur kritikal yang amat penting. Misalnya termasuk:

- Organisasi boleh menggunakan Profil Sasaran untuk menyatakan keperluan pengurusan risiko keselamatan siber kepada penyedia perkhidmatan luaran (misalnya penyedia perkhidmatan awan yang mengeksport data).
- Organisasi boleh menyatakan keadaan keselamatan siber melalui Profil Semasa bertujuan melaporkan keputusan atau membandingkan dengan keperluan pemerolehan.
- Pemilik/pengendali infrastruktur kritikal, setelah mengenal pasti rakan kongsi luaran yang bergantung pada infrastruktur tersebut, boleh menggunakan Profil Sasaran untuk membawa Kategori dan Subkategori yang diperlukan.
- Sektor infrastruktur kritikal boleh mewujudkan Profil Sasaran yang boleh digunakan dalam kalangan unsur yang ada sebagai Profil garis dasar awal untuk membina Profil Sasaran yang disesuaikan.
- Organisasi boleh menguruskan risiko keselamatan siber dengan lebih baik dalam kalangan pihak berkepentingan dengan menilai kedudukan masing-masing dalam infrastruktur kritikal dan ekonomi digital yang lebih luas menggunakan Peringkat Pelaksanaan.

Komunikasi amat penting dalam kalangan pihak berkepentingan di bahagian atas dan bawah rantaian bekalan. Rantaian bekalan ialah set sumber dan proses yang kompleks, teragih secara global dan saling berkaitan antara pelbagai tahap organisasi. Rantaian bekalan bermula dengan penyumberan produk dan perkhidmatan, serta diperluas daripada reka bentuk, pembangunan, pembuatan, pemprosesan, pengendalian dan penghantaran produk, serta penyampaian perkhidmatan kepada pengguna akhir. Memandangkan hubungan yang kompleks dan saling berkaitan ini, pengurusan risiko rantaian bekalan (SCRM) menjadi fungsi organisasi yang kritikal..[11]

SCRM siber ialah set aktiviti yang perlu untuk menguruskan risiko keselamatan siber yang dikaitkan dengan pihak luar. Lebih khusus lagi, SCRM siber menangani kesan keselamatan siber oleh organisasi terhadap pihak luar dan juga kesan keselamatan siber pihak luar terhadap organisasi tersebut.

Objektif utama SCRM siber ialah mengenal pasti, menilai dan mengurangkan "produk dan perkhidmatan yang mungkin mengandungi kefungsian berpotensi berniat jahat, palsu, atau rentan berpunca daripada amalan pembuatan dan pembangunan yang lemah dalam rantaian bekalan siber [12]". Aktiviti SCRM siber boleh merangkumi:

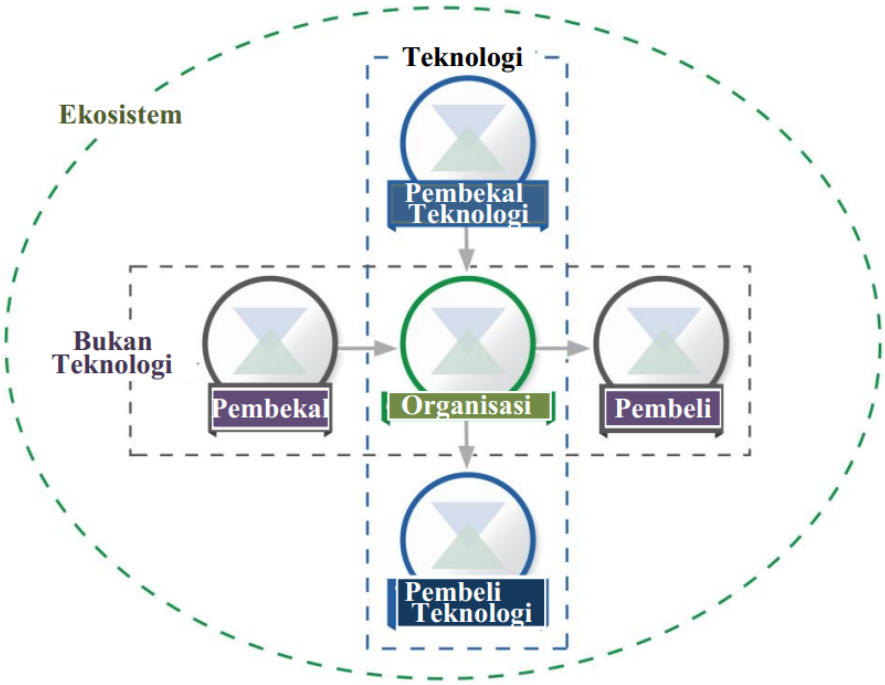
- Menentukan keperluan keselamatan siber untuk pembekal,
- Menggubal keperluan keselamatan siber melalui perjanjian formal (misalnya, kontrak),

[11] Menyampaikan Keperluan Keselamatan Siber (Seksyen 3.3) dan Keputusan Membeli (Seksyen 3.4) hanya menyatakan dua kegunaan Rangka Kerja ini untuk SCRM siber dan tidak bertujuan menangani SCRM siber secara menyeluruh.

[12] Penerbitan Khas NIST 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, Boyens et al, April 2015, https://doi.org/10.6028/NIST.SP.800-161

- Berkomunikasi kepada pembekal mengenai cara keperluan keselamatan siber tersebut akan disahkan dan diperakui,
- Mengesahkan bahawa keperluan keselamatan siber dipenuhi melalui pelbagai pengkaedahan penilaian dan
- Mentadbir urus dan menguruskan aktiviti di atas.

Seperti yang digambarkan dalam Rajah 3, SCRM siber merangkumi pembekal dan pembeli teknologi, serta pembekal dan pembeli bukan teknologi, iaitu teknologi yang hanya terdiri daripada teknologi maklumat (IT), sistem kawalan industri (ICS), sistem fizikal siber (CPS) dan peranti yang disambungkan secara lebih umum, termasuk Internet Benda (IoT). Rajah 3 menggambarkan organisasi pada satu-satu masa. Walau bagaimanapun, dalam perjalanan biasa pengendalian perniagaan, kebanyakan organisasi akan menjadi pembekal huluan dan pembeli hiliran, jika dilihat dari sudut organisasi lain atau pengguna akhir.



Rajah 3: Hubungan Rantaian Bekalan Siber

Pihak yang diterangkan dalam Rajah 3 terdiri daripada ekosistem keselamatan siber organisasi. Hubungan ini mengetengahkan peranan penting SCRM siber untuk menangani risiko keselamatan siber dalam infrastruktur kritikal dan ekonomi digital yang lebih luas. Hubungan, produk dan perkhidmatan yang disediakan ini dan risiko yang SCRM siber tunjukkan perlu dikenal pasti dan difaktorkan ke dalam keupayaan perlindungan dan pengesanan organisasi, serta tindak balas dan protokol pemulihan masing-masing.

Dalam rajah di atas, "Pembeli" merujuk kepada individu atau organisasi hiliran yang menggunakan produk atau perkhidmatan tertentu daripada organisasi, termasuk organisasi berorientasikan keuntungan dan bukan membuat untung. "Pembekal" merangkumi pembekal

produk dan penyedia perkhidmatan huluan yang digunakan untuk tujuan dalaman organisasi (misalnya, infrastruktur IT) atau diintegrasikan ke dalam produk atau perkhidmatan yang disediakan kepada Pembeli. Istilah ini terpakai untuk produk dan perkhidmatan berasaskan teknologi dan bukan teknologi.

Sama ada mempertimbang Subkategori Teras individu atau pertimbangan menyeluruh Profil, Rangka Kerja menawarkan organisasi dan rakan kongsi kaedah untuk membantu memastikan produk atau perkhidmatan baharu memenuhi hasil keselamatan kritikal. Dengan memilih hasil yang relevan dengan konteks terlebih dahulu (misalnya, penghantaran Maklumat Pengenalpastian Peribadi (PII), penyampaian perkhidmatan kritikal misi, perkhidmatan pengesahan data, integriti produk atau perkhidmatan) organisasi kemudiannya boleh menilai rakan kongsi berdasarkan kriteria tersebut. Sebagai contoh, jika terdapat sistem yang dibeli bertujuan memantau Teknologi Pengendalian (OT) untuk komunikasi rangkaian anomali dalam komunikasi rangkaian, ketersediaan mungkin menjadi objektif keselamatan siber yang amat penting untuk dicapai dan perlu mendorong penilaian Pembekal Teknologi terhadap Subkategori yang berkenaan (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 Membeli

Oleh kerana Profil Sasaran Rangka Kerja merupakan senarai keutamaan keperluan keselamatan siber organisasi, Profil Sasaran boleh digunakan untuk memaklumkan keputusan tentang membeli produk dan perkhidmatan. Transaksi ini berbeza daripada Menyampaikan Keperluan Keselamatan Siber dengan Pihak Berkepentingan (dikemukakan dalam Seksyen 3.3) kerana organisasi mungkin tidak berupaya mewajibkan set keperluan keselamatan siber ke atas pembekal. Objektif tindakan ini ialah untuk membuat keputusan pembelian terbaik dalam kalangan pelbagai pembekal, memandangkan senarai keperluan keselamatan siber ditentukan dengan teliti. Selalunya, ini bermakna beberapa tahap penggantian, membandingkan berbilang produk atau perkhidmatan dengan jurang Profil Sasaran yang diketahui.

Sebaik sahaja produk atau perkhidmatan dibeli, Profil tersebut juga boleh digunakan untuk menjejaki dan menangani risiko keselamatan siber yang tinggal. Sebagai contoh, jika perkhidmatan atau produk yang dibeli tidak memenuhi semua objektif yang diterangkan dalam Profil Sasaran, organisasi boleh menangani risiko yang tinggal melalui tindakan pengurusan lain. Profil itu juga memberikan organisasi, kaedah untuk menilai sekiranya produk memenuhi hasil keselamatan siber melalui semakan berkala dan mekanisme pengujian.

3.5 Mengenal Pasti Peluang untuk Rujukan Informatif Baharu atau Dipinda

Rangka Kerja boleh digunakan untuk mengenal pasti peluang bagi piawaian, garis panduan, atau amalan baharu atau dipinda yang Rujukan Informatif tambahan akan membantu organisasi menangani keperluan yang baharu muncul. Organisasi yang melaksanakan Subkategori tertentu, atau membangunkan Subkategori baharu, mungkin mendapati ada sedikit Rujukan Informatif, yang boleh digunakan untuk aktiviti berkaitan. Untuk menangani keperluan tersebut, organisasi mungkin boleh bekerjasama dengan peneraju teknologi dan/atau badan piawaian bertujuan merangka, membangunkan dan menyelaraskan piawaian, garis panduan atau amalan.

3.6 Pengkaedahan untuk Melindungi Privasi dan Kebebasan Awam

Seksyen ini menerangkan pengkaedahan untuk menangani implikasi privasi individu dan kebebasan awam yang boleh terhasil daripada keselamatan siber. Pengkaedahan ini bertujuan menjadi set pertimbangan dan proses umum memandangkan implikasi privasi dan kebebasan awam mungkin berbeza mengikut sektor atau dari masa ke masa dan organisasi boleh menangani pertimbangan dan proses ini dengan pelbagai pelaksanaan teknikal. Namun begitu, bukan semua aktiviti dalam program keselamatan siber melibatkan pertimbangan privasi dan kebebasan awam. Piawaian privasi teknikal, garis panduan dan amalan terbaik tambahan mungkin perlu dibangunkan untuk menyokong pelaksanaan teknikal yang lebih baik.

Privasi dan keselamatan siber mempunyai hubungan yang kukuh. Aktiviti keselamatan siber organisasi juga boleh menimbulkan risiko kepada privasi dan kebebasan awam apabila maklumat peribadi digunakan, dikumpul, diproses, diselenggara, atau didedahkan. Beberapa contoh termasuk: aktiviti keselamatan siber yang mengakibatkan pengumpulan atau penyimpanan maklumat peribadi secara berlebihan; pendedahan atau penggunaan maklumat peribadi yang tidak berkaitan dengan aktiviti keselamatan siber; dan aktiviti pengurangan keselamatan siber yang mengakibatkan penafian perkhidmatan atau impak buruk lain yang serupa serta berpotensi untuk berlaku, termasuk beberapa jenis pengesanan atau pemantauan kejadian yang boleh menghalang kebebasan bersuara atau berpersatuan.

Kerajaan dan ejen mempunyai tanggungjawab melindungi kebebasan awam yang timbul daripada aktiviti keselamatan siber. Seperti yang dirujuk dalam pengkaedahan di bawah, kerajaan atau ejen yang memiliki atau mengendalikan infrastruktur kritikal perlu mempunyai proses untuk menyokong pematuhan aktiviti keselamatan siber dengan undang-undang privasi, kawal selia dan keperluan Perlembagaan yang berkenaan.

Untuk menangani implikasi privasi, organisasi boleh mempertimbang sejauh mana program keselamatan siber masing-masing mungkin menggabungkan prinsip privasi seperti: peminimuman data dalam pengumpulan, pendedahan dan pengekalan bahan maklumat peribadi yang berkaitan dengan kejadian keselamatan siber; mengenakan had dalam aktiviti di luar keselamatan siber ke atas mana-mana maklumat yang dikumpulkan secara khusus untuk aktiviti keselamatan siber; ketelusan untuk aktiviti keselamatan siber tertentu; persetujuan individu dan pembetulan untuk impak buruk yang timbul daripada penggunaan maklumat peribadi dalam aktiviti keselamatan siber; kualiti data, integriti dan keselamatan; serta kebertanggungjawaban dan pengauditan.

Semasa organisasi menilai Teras Rangka Kerja dalam Lampiran A, proses dan aktiviti berikut boleh dipertimbang sebagai cara untuk menangani implikasi privasi dan kebebasan awam yang diterangkan di atas:

Tadbir urus risiko keselamatan siber

- Penilaian organisasi terhadap risiko keselamatan siber dan kemungkinan tindak balas risiko ada mempertimbang implikasi privasi yang berpunca daripada program keselamatan sibernya.
- Individu yang mempunyai tanggungjawab terhadap privasi berkaitan keselamatan siber, melaporkan kepada pengurusan berkenaan dan dilatih dengan sewajarnya.

- Proses disediakan untuk menyokong pematuhan aktiviti keselamatan siber dengan undang-undang privasi, kawal selia dan keperluan Perlembagaan berkenaan
- Proses disediakan untuk menilai pelaksanaan langkah dan kawalan organisasi seperti di atas.

Pendekatan untuk mengenal pasti, mengesahkan dan memberi kebenaran kepada individu untuk mengakses aset dan sistem organisasi

- Langkah diambil untuk mengenal pasti dan menangani implikasi privasi berpunca daripada pengurusan identiti dan langkah kawalan akses yang melibatkan pengumpulan, pendedahan, atau penggunaan maklumat peribadi.

Langkah kesedaran dan latihan

- Maklumat yang boleh digunakan daripada dasar privasi organisasi disertakan dalam aktiviti latihan dan kesedaran bagi tenaga kerja keselamatan siber.
- Penyedia perkhidmatan yang memberikan perkhidmatan berkaitan keselamatan siber untuk organisasi dimaklumkan tentang dasar privasi organisasi berkenaan.

Pengesanan aktiviti anomali dan pemantauan sistem dan aset

- Proses disediakan untuk menjalankan semakan privasi terhadap pengesanan aktiviti anomali dan pemantauan keselamatan siber organisasi

Aktiviti tindak balas, termasuk perkongsian maklumat atau usaha pengurangan lain

- Proses disediakan untuk menilai dan menangani sama ada, masa, cara dan sejauh mana maklumat peribadi dikongsi di luar organisasi sebagai sebahagian daripada aktiviti perkongsian maklumat keselamatan siber.
- Proses disediakan untuk menjalankan semakan privasi terhadap usaha pengurangan keselamatan siber organisasi.

4.0 Menilai Sendiri Risiko Keselamatan Siber dengan Rangka Kerja ini

Rangka Kerja Keselamatan Siber ini direka bentuk untuk mengurangkan risiko dengan menambah baik pengurusan risiko keselamatan siber kepada objektif organisasi. Sebaiknya, organisasi yang menggunakan Rangka Kerja ini akan dapat mengukur dan menetapkan nilai ke atas risiko masing-masing dengan kos dan manfaat bagi langkah yang diambil untuk mengurangkan risiko kepada tahap yang boleh diterima. Semakin baik organisasi dapat mengukur risiko, kos dan manfaat strategi dan langkah keselamatan siber, maka semakin rasional, berkesan dan bernilai pendekatan dan pelaburan keselamatan siber tersebut.

Dari masa ke masa, penilaian sendiri dan pengukuran perlu menambah baik pembuatan keputusan tentang keutamaan pelaburan. Sebagai contoh, mengukur – atau sekurang-kurangnya melakukan pencirian dengan mantap – aspek keadaan keselamatan siber organisasi dan arah aliran dari masa ke masa boleh membuatkan organisasi tersebut memahami dan menyampaikan maklumat risiko yang bermakna kepada pihak yang bergantung pada organisasi, para pembekal,

pembeli dan pihak lain. Organisasi boleh mencapai ini secara dalaman atau dengan mendapatkan penilaian pihak ketiga. Jika dilakukan dengan betul dan mengambil kira had yang ada, pengukuran ini boleh menyediakan asas untuk hubungan yang kukuh dan boleh dipercayai, di dalam dan di luar organisasi.

Untuk mengkaji keberkesanan pelaburan, organisasi mula-mula mesti mempunyai pemahaman yang jelas tentang objektif organisasi, hubungan antara objektif tersebut dan hasil sokongan keselamatan siber dan cara hasil diskret keselamatan siber tersebut dilaksana dan diuruskan. Walaupun pengukuran semua item tersebut berada di luar skop Rangka Kerja, hasil keselamatan siber Teras Rangka Kerja menyokong penilaian kendiri keberkesanan pelaburan dan aktiviti keselamatan siber dengan cara berikut:

- Membuat pilihan tentang sejauh mana bahagian pengendalian keselamatan siber yang berbeza perlu mempengaruhi pemilihan Peringkat Pelaksanaan Sasaran,
- Menilai pendekatan organisasi terhadap pengurusan risiko keselamatan siber dengan menentukan Peringkat Pelaksanaan Semasa,
- Menentukan keutamaan hasil keselamatan siber dengan membangunkan Profil Sasaran,
- Menentukan tahap sejauh mana langkah keselamatan siber tertentu mencapai hasil keselamatan siber yang diingini dengan menilai Profil Semasa dan
- Mengukur tahap pelaksanaan untuk katalog kawalan atau panduan teknikal yang disenaraikan sebagai Rujukan Informatif.

Pembangunan metrik prestasi keselamatan siber sedang berkembang. Organisasi perlu menjadi bijak, kreatif dan berhati-hati tentang cara menggunakan pengukuran dalam mengoptimumkan penggunaan, sambil mengelakkan kebergantungan pada penunjuk buatan keadaan semasa dan kemajuan dalam menambah baik pengurusan risiko keselamatan siber. Menilai risiko siber memerlukan disiplin dan perlu dikaji semula secara berkala. Apa-apa ukuran masa digunakan sebagai sebahagian daripada proses Rangka Kerja ini, organisasi digalakkan untuk mengenal pasti dengan jelas dan mengetahui sebab pengukuran tersebut penting dan cara ini akan menyumbangkan kepada pengurusan keseluruhan risiko keselamatan siber. Organisasi juga perlu jelas tentang had ukuran yang digunakan.

Sebagai contoh, menjejaki langkah keselamatan dan hasil perniagaan boleh memberikan cerapan bermakna tentang sejauh mana perubahan dalam kawalan keselamatan yang granul iaitu terpisah-pisah kepada beberapa bahagian kecil, mempengaruhi penyempurnaan objektif organisasi. Pengesahan pencapaian beberapa objektif organisasi memerlukan analisis data yang hanya dilakukan selepas objektif itu dicapai. Pengukuran seperti ini adalah lebih mutlak. Walau bagaimanapun, selalunya ini menjadi lebih berguna untuk meramalkan sama ada risiko keselamatan siber boleh berlaku dan impak yang diberikan, dengan menggunakan ukuran utama.

Organisasi digalakkan berinovasi dan menyesuaikan cara menggabungkan pengukuran ke dalam penggunaan Rangka Kerja masing-masing dengan memanfaatkan sepenuhnya kegunaan dan hadnya.

Lampiran A: Teras Rangka Kerja

Lampiran ini membentangkan Teras Rangka Kerja: senarai Fungsi, Kategori, Subkategori dan Rujukan Informatif yang menerangkan aktiviti keselamatan siber khusus yang biasa bagi semua sektor infrastruktur kritikal. Format pembentangan yang dipilih untuk Teras Rangka Kerja tidak mencadangkan susunan pelaksanaan tertentu atau membayangkan tahap kepentingan Kategori, Subkategori dan Rujukan Informatif. Teras Rangka Kerja yang dibentangkan dalam lampiran ini mewakili satu set aktiviti biasa untuk mengurus risiko keselamatan siber. Walaupun Rangka Kerja ini tidak menyeluruh, ia boleh diperluaskan, membenarkan organisasi, sektor dan entiti lain menggunakan Subkategori dan Rujukan Informatif yang berkesan kos dan cekap serta membolehkan mereka mengurus risiko keselamatan siber mereka. Aktiviti boleh dipilih daripada Teras Rangka Kerja semasa proses pembangunan Profil dan daripada Kategori, Subkategori dan Rujukan Informatif tambahan boleh ditambahkan pada Profil. Proses pengurusan risiko organisasi, keperluan undang-undang/peraturan, objektif perniagaan/misi dan kekangan organisasi dijadikan penduan dalam pemilihan aktiviti semasa pembangunan Profil. Maklumat peribadi dianggap sebagai komponen data atau aset yang dirujuk dalam Kategori apabila menilai risiko dan perlindungan keselamatan.

Walaupun hasil yang dimaksudkan yang dikenal pasti dalam Fungsi, Kategori dan Subkategori adalah sama untuk IT dan ICS, persekitaran operasi dan pertimbangan untuk IT dan ICS berbeza. ICS mempunyai kesan langsung ke atas dunia fizikal, termasuk potensi risiko kepada kesihatan dan keselamatan individu, dan kesan kepada alam sekitar. Selain itu, ICS mempunyai prestasi unik dan keperluan kebolehpercayaan berbanding dengan IT, dan matlamat keselamatan dan kecekapan mesti dipertimbangkan semasa melaksanakan langkah keselamatan siber.

Untuk kemudahan penggunaan, setiap komponen Teras Rangka Kerja ini diberikan pengecam yang unik. Fungsi dan Kategori masing-masing mempunyai pengecam abjad yang unik, seperti yang ditunjukkan dalam Jadual 1. Subkategori dalam setiap Kategori dirujuk secara berangka; pengecam unik untuk setiap Subkategori disertakan dalam Jadual 2.

Bahan sokongan tambahan, termasuk Rujukan Informatif, yang berkaitan dengan Rangka Kerja ini boleh boleh didapati di laman web NIST di http://www.nist.gov/cyberframework/.

Jadual 1: Pengecam Unik Setiap Fungsi dan Kategori

Pengecam Unik Fungsi	Fungsi	Pengecam Unik Kategori	Kategori
ID	Kenal Pasti	ID.AM	Pengurusan Aset
		ID.BE	Persekitaran Perniagaan
		ID.GV	Tadbir Urus
		ID.RA	Penilaian Risiko
		ID.RM	Strategi Pengurusan Risiko
		ID.SC	Pengurusan Risiko Rantaian Bekalan
PR	Lindung	PR.AC	Pengurusan Identiti dan Kawalan Akses

		PR.AT	Kesedaran dan Latihan
		PR.DS	Keselamatan Data
		PR.IP	Proses dan Prosedur Perlindungan Maklumat
		PR.MA	Penyelenggaraan
		PR.PT	Teknologi Perlindungan
DE	Kesan	DE.AE	Anomali dan Peristiwa
		DE.CM	Pemantauan Berterusan Keselamatan
		DE.DP	Proses Pengesanan
RS	Tindak Balas	RS.RP	Perancangan Tindak Balas
		RS.CO	Komunikasi
		RS.AN	Analisis
		RS.MI	Pengurangan
		RS.IM	Penambahbaikan
RC	Pulih	RC.RP	Perancangan Pemulihan
		RC.IM	Penambahbaikan
		RC.CO	Komunikasi

Jadual 2: Teras Rangka Kerja

Fungsi	Kategori	SubKategori	Rujukan Informatif
KENAL PASTI (ID)	**Pengurusan Aset (ID.AM):** Data, kakitangan, peranti, sistem dan kemudahan yang membolehkan organisasi mencapai tujuan perniagaan dikenal pasti dan diuruskan selaras dengan kepentingan relatif masing-masing kepada objektif organisasi dan strategi risiko organisasi.	**ID.AM-1:** Peranti dan sistem fizikal dalam organisasi diinventorikan	**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 perisian dan aplikasi dalam organisasi diinventorikan	**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 aliran 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 maklumat luaran 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 (misalnya, perkakasan, peranti, data, masa, kakitangan dan perisian) ditentukan keutamaan berdasarkan klasifikasi, kritikal dan nilai perniagaan	**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

Fungsi	Kategori	SubKategori	Rujukan Informatif
		ID.AM-6: Peranan dan tanggungjawab Keselamatan Siber untuk seluruh tenaga kerja dan pihak berkepentingan dari kalangan pihak ketiga (misalnya, pembekal, pelanggan, rakan kongsi) diwujudkan	**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
	Persekitaran Perniagaan (ID.BE): Misi, objektif, pihak berkepentingan dan aktiviti organisasi difahami dan ditentukan keutamaan; maklumat ini digunakan untuk memaklumkan peranan, tanggungjawab dan keputusan pengurusan risiko keselamatan siber.	**ID.BE-1:** Peranan organisasi dalam rantaian bekalan dikenal pasti dan dimaklumkan.	**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 **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: Kedudukan organisasi dalam infrastruktur kritikal dan sektor industri dikenal pasti dan dimaklumkan	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Klausa 4.1 **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Keutamaan untuk misi, objektif dan aktiviti organisasi, diwujudkan dan dimaklumkan	**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: Kebergantungan dan fungsi kritikal untuk penyampaian perkhidmatan kritikal diwujudkan	**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: Keperluan kebingkasan untuk menyokong penyampaian perkhidmatan kritikal diwujudkan untuk semua keadaan pengendalian (misalnya, di bawah tekanan/serangan, semasa pemulihan, pengendalian biasa)	**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, SA14

Fungsi	Kategori	SubKategori	Rujukan Informatif
	Tadbir Urus (ID.GV): Dasar, prosedur dan proses untuk menguruskan dan memantau kawal selia, undang-undang, risiko, persekitaran dan keperluan pengendalian organisasi difahami dan memaklumkan pengurusan risiko keselamatan siber.	**ID.GV-1:** Dasar keselamatan siber organisasi diwujudkan dan dimaklumkan	**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 kawalan daripada semua keluarga kawalan keselamatan
		ID.GV-2: Peranan dan tanggungjawab keselamatan siber diselaraskan dan dijajarkan dengan peranan dalaman serta rakan kongsi luaran	**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: Keperluan undang-undang dan kawal selia berkenaan keselamatan siber, termasuk privasi dan kewajipan kebebasan awam, difahami dan diuruskan	**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 kawalan daripada semua keluarga kawalan keselamatan
		ID.GV-4: Tadbir urus dan proses pengurusan risiko menangani risiko keselamatan siber	**COBIT 5** EDM03.02, APO12.02, APO12.05, 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 **ISO/IEC 27001:2013** Klausa 6 **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11

Fungsi	Kategori	SubKategori	Rujukan Informatif
	Penilaian Risiko (ID.RA): Organisasi memahami risiko keselamatan siber kepada pengendalian organisasi (termasuk misi, fungsi, imej, atau reputasi), aset organisasi dan individu.	**ID.RA-1:** Kerentanan aset dikenal pasti dan didokumenkan	**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, RA3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Risikan ancaman siber diterima daripada forum dan sumber perkongsian maklumat	**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, dalaman dan luaran, dikenal pasti dan didokumenkan	**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** Klausa 6.1.2 **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM16
		ID.RA-4: Potensi impak terhadap perniagaan dan kemungkinan sesuatu peristiwa berlaku dikenal pasti	**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, Klausa 6.1.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM9, PM-11

Fungsi	Kategori	SubKategori	Rujukan Informatif
		ID.RA-5: Ancaman, kerentanan, kemungkinan sesuatu peristiwa berlaku dan impak 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: Tindak balas risiko dikenal pasti dan ditentukan keutamaan	**CIS CSC** 4 **COBIT 5** APO12.05, APO13.02 **ISO/IEC 27001:2013** Klausa 6.1.3 **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Strategi Pengurusan Risiko (ID.RM): Keutamaan, kekangan, toleransi risiko organisasi dan andaian diwujudkan, serta digunakan untuk menyokong keputusan risiko pengendalian.	**ID.RM-1:** Proses pengurusan risiko diwujudkan, diuruskan dan dipersetujui oleh pihak berkepentingan organisasi	**CIS CSC** 4 **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** Klausa 6.1.3, Klausa 8.3, Klausa 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** Klausa 6.1.3, Klausa 8.3 **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-3: Penentuan toleransi risiko organisasi dimaklumkan oleh peranan yang dimainkan dalam infrastruktur kritikal dan analisis risiko khusus sektor	**COBIT 5** APO12.02 **ISO/IEC 27001:2013** Klausa 6.1.3, Klausa 8.3 **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM11

Fungsi	Kategori	SubKategori	Rujukan Informatif
	Pengurusan Risiko Rantaian Bekalan (ID.SC): Keutamaan, kekangan, toleransi risiko dan andaian organisasi diwujudkan dan digunakan untuk menyokong keputusan risiko berkaitan dengan pengurusan risiko rantaian bekalan. Organisasi telah mewujudkan dan melaksanakan proses untuk mengenal pasti, menilai dan menguruskan risiko rantaian bekalan.	**ID.SC-1:** Proses pengurusan risiko rantaian bekalan siber dikenal pasti, diwujudkan, dinilai, diuruskan dan dipersetujui oleh pihak berkepentingan 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: Pembekal dan rakan kongsi pihak ketiga sistem maklumat, komponen dan perkhidmatan dikenal pasti, ditentukan keutamaan dan dinilai menggunakan proses penilaian risiko rantaian bekalan 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, SA14, SA-15, PM-9
		ID.SC-3: Kontrak dengan pembekal dan rakan kongsi pihak ketiga digunakan untuk melaksanakan langkah yang sesuai dan direka bentuk untuk memenuhi objektif program keselamatan siber organisasi dan Pelan Pengurusan Risiko Rantaian Bekalan 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

Fungsi	Kategori	SubKategori	Rujukan Informatif
		ID.SC-4: Pembekal dan rakan kongsi pihak ketiga dinilai secara rutin menggunakan audit, keputusan ujian, atau bentuk penilaian lain untuk mengesahkan bahawa kedua-duanya memenuhi kewajipan kontrak masing-masing.	**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 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU16, PS-7, SA-9, SA-12
		ID.SC-5: Perancangan dan pengujian tindak balas dan pemulihan dijalankan dengan pembekal 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
LINDUNG (PR)	**Pengurusan Identiti, Pengesahan dan Kawalan Akses (PR.AC):** Akses kepada aset fizikal dan logik, serta kemudahan berkaitan adalah terhad kepada pengguna, proses dan peranti yang dibenarkan, dan diuruskan selaras dengan penilaian risiko akses yang tidak dibenarkan kepada aktiviti dan transaksi yang dibenarkan.	**PR.AC-1:** Identiti dan bukti kelayakan dikeluarkan, diuruskan, disahkan, dibatalkan dan diaudit untuk peranti, pengguna dan proses yang dibenarkan	**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 fizikal kepada aset diuruskan 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

Fungsi	Kategori	SubKategori	Rujukan Informatif
		PR.AC-3: Akses jauh diuruskan	**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: Keizinan dan kebenaran akses diuruskan dengan menggabungkan prinsip keistimewaan terendah dan pengasingan 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
		PR.AC-5: Integriti rangkaian dilindungi (misalnya, pengasingan rangkaian, pembahagian rangkaian)	**CIS CSC** 9, 14, 15, 18 **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

Fungsi	Kategori	SubKategori	Rujukan Informatif
		PR.AC-6: Identiti dibuktikan dan terikat kepada kelayakan 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, AC16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Pengguna, peranti dan aset lain disahkan (misalnya, faktor tunggal, faktor berbilang) sepadan dengan risiko transaksi (misalnya, risiko keselamatan dan privasi individu serta risiko organisasi yang lain)	**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, AC11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Kesedaran dan Latihan (PR.AT): Kakitangan dan rakan kongsi organisasi diberikan pendidikan mengenai kesedaran keselamatan siber dan dilatih melaksanakan tugas dan tanggungjawab berkaitan keselamatan siber mereka selaras dengan dasar, prosedur dan perjanjian berkaitan.	**PR.AT-1:** Semua pengguna dimaklumkan dan dilatih	**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 dengan hak istimewa memahami peranan dan tanggungjawab masing-masing	**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

Fungsi	Kategori	SubKategori	Rujukan Informatif
		PR.AT-3: Pihak berkepentingan dari kalangan pihak ketiga (misalnya, pembekal, pelanggan, rakan kongsi) memahami peranan dan tanggungjawab masing-masing	**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 kanan memahami peranan dan tanggungjawab mereka	**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: Kakitangan fizikal dan keselamatan siber memahami peranan dan tanggungjawab mereka	**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
	Keselamatan Data (PR.DS): Maklumat dan rekod (data) diuruskan selaras dengan strategi risiko organisasi untuk melindungi kerahsiaan, integriti dan ketersediaan maklumat.	**PR.DS-1:** Data dalam storan dilindungi	**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 dalam transit dilindungi	**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

Fungsi	Kategori	SubKategori	Rujukan Informatif
		PR.DS-3: Aset diurus secara formal sepanjang penghapusan, pemindahan dan pelupusan	**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: Kapasiti yang mencukupi untuk memastikan ketersediaan dikekalkan	**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 terhadap kebocoran data dilaksanakan	**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 semakan integriti digunakan untuk mengesahkan integriti perisian, perisian tegar dan maklumat	**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

Fungsi	Kategori	SubKategori	Rujukan Informatif
		PR.DS-7: Persekitaran pembangunan dan pengujian adalah berasingan daripada persekitaran pengeluaran	**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 semakan integriti digunakan untuk mengesahkan integriti perkakasan	**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 Maklumat (PR.IP): Dasar keselamatan (yang menangani tujuan, skop, peranan, tanggungjawab, komitmen pengurusan dan penyelarasan dalam kalangan entiti organisasi), proses dan prosedur diselenggara dan digunakan untuk menguruskan perlindungan sistem maklumat dan aset.	**PR.IP-1:** Konfigurasi garis dasar teknologi maklumat/sistem kawalan industri dicipta dan dikekalkan dengan memasukkan prinsip keselamatan (misalnya konsep kefungsian paling sedikit)	**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, CM5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: Kitaran Hayat Pembangunan Sisten untuk menguruskan sistem dilaksanakan	**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, SI13, SI-14, SI-16, SI-17

Fungsi	Kategori	SubKategori	Rujukan Informatif
		PR.IP-3: Proses kawalan perubahan konfigurasi disediakan	**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
		PR.IP-4: Sandaran maklumat dikendalikan, diselenggarakan dan diuji	**CIS CSC** 10 **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: Dasar dan kawal selia berkenaan persekitaran pengendalian fizikal untuk aset organisasi dipenuhi	**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, PE14, PE-15, PE-18
		PR.IP-6: Data dimusnahkan mengikut dasar	**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

Fungsi	Kategori	SubKategori	Rujukan Informatif
		PR.IP-7: Proses perlindungan ditambah baik	**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, Klausa 9, Klausa 10 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Keberkesanan teknologi perlindungan dikongsi bersama	**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: Pelan tindak balas (Tindak Balas Kejadian dan Kesinambungan Perniagaan) dan pelan pemulihan (Pemulihan Kejadian dan Pemulihan Bencana) disediakan dan diuruskan	**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, CP13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: Pelan tindak balas 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: Keselamatan Siber dimasukkan ke dalam amalan sumber manusia (misalnya, nyahperuntukan, saringan kakitangan)	**CIS CSC** 5, 16 **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.7.1.2, 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

Fungsi	Kategori	SubKategori	Rujukan Informatif
		PR.IP-12: Pelan pengurusan kerentanan dibangunkan dan dilaksanakan	**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
	Penyelenggaraan (PR.MA): Penyelenggaraan dan baik pulih komponen sistem kawalan dan maklumat industri dilakukan selaras dengan dasar dan prosedur.	**PR.MA-1:** Penyelenggaraan dan baik pulih aset organisasi dilakukan dan dilog, dengan alat yang diluluskan dan dikawal	**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: Penyelenggaraan jauh aset organisasi diluluskan, dilog dan dilakukan dengan cara yang menghalang akses tanpa kebenaran	**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): Penyelesaian keselamatan teknikal diuruskan untuk memastikan keselamatan dan kebingkasan sistem dan asset, selaras dengan dasar, prosedur dan perjanjian yang berkaitan.	**PR.PT-1:** Rekod audit/log ditentukan, didokumenkan, dilaksanakan dan disemak mengikut dasar.	**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 Family

Fungsi	Kategori	SubKategori	Rujukan Informatif
		PR.PT-2: Media boleh alih dilindungi dan penggunaan dihadkan mengikut dasar	**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, MP5, MP-7, MP-8
		PR.PT-3: Prinsip kefungsian paling sedikit digabungkan dengan mengkonfigurasikan sistem untuk hanya menyediakan keupayaan penting	**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, 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: Rangkaian komunikasi dan kawalan dilindungi	**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

Fungsi	Kategori	SubKategori	Rujukan Informatif
		PR.PT-5: Mekanisme (misalnya, pasti selamat, pengimbangan beban, pertukaran panas dilaksanakan untuk mencapai keperluan kebingkasan dalam situasi biasa dan buruk	**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, CP13, PL-8, SA-14, SC-6
KESAN (DE)	**Anomali dan Peristiwa (DE.AE):** Aktiviti anomali dikesan dan potensi impak peristiwa difahami.	**DE.AE-1:** Garis dasar pengendalian rangkaian dan aliran data yang dijangkakan untuk pengguna dan sistem diwujudkan dan diuruskan	**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: Peristiwa yang dikesan dianalisis untuk memahami sasaran dan kaedah 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 peristiwa dikumpul dan dikaitkan daripada pelbagai sumber dan penderia	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02 **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: Impak 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

Fungsi	Kategori	SubKategori	Rujukan Informatif
		DE.AE-5: Ambang amaran kejadian diwujudkan	**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 Berterusan Keselamatan (DE.CM): Sistem maklumat dan aset dipantau untuk mengenal pasti peristiwa keselamatan siber dan mengesahkan keberkesanan langkah perlindungan.	**DE.CM-1:** Rangkaian dipantau untuk mengesan potensi peristiwa keselamatan siber berlaku	**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, CM3, SC-5, SC-7, SI-4
		DE.CM-2: Persekitaran fizikal dipantau untuk mengesan potensi peristiwa keselamatan siber berlaku	**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: Aktiviti kakitangan dipantau untuk mengesan potensi peristiwa keselamatan siber berlaku	**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: Kod hasad dikesan	**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: Kod mudah alih yang tidak dibenarkan dikesan	**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

Fungsi	Kategori	SubKategori	Rujukan Informatif
		DE.CM-6: Aktiviti penyedia perkhidmatan luaran dipantau untuk mengesan potensi peristiwa keselamatan siber berlaku	**COBIT 5** APO07.06, APO10.05 **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 untuk kakitangan, sambungan, peranti dan perisian yang tidak dibenarkan 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: Imbasan 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 Pengesanan (DE.DP): Proses dan prosedur pengesanan dikekalkan dan diuji untuk memastikan kesedaran tentang peristiwa anomali.	**DE.DP-1:** Peranan dan tanggungjawab untuk pengesanan ditakrifkan dengan baik bagi memastikan kebertanggungjawaban	**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: Aktiviti pengesanan mematuhi semua keperluan berkenaan	**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, SA18, SI-4, PM-14

Fungsi	Kategori	SubKategori	Rujukan Informatif

		DE.DP-3: Proses pengesanan 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: Maklumat pengesanan peristiwa disampaikan	**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, RA5, SI-4
		DE.DP-5: Proses pengesanan ditambah baik secara berterusan	**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, RA5, SI-4, PM-14

Fungsi	Kategori	SubKategori	Rujukan Informatif
TINDAK BALAS (RS)	**Perancangan Tindak Balas (RS.RP):** Proses dan prosedur tindak balas dilaksanakan dan dikekalkan, untuk memastikan tindak balas terhadap kejadian keselamatan siber yang dikesan.	**RS.RP-1:** Pelan tindak balas dilaksanakan semasa atau selepas kejadian	**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): Aktiviti tindak balas diselaraskan dengan pihak berkepentingan dalaman dan luaran (misalnya sokongan luaran daripada agensi penguatkuasaan undang-undang).	**RS.CO-1:** Kakitangan mengetahui peranan dan arahan pengendalian mereka apabila tindak balas 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: Kejadian dilaporkan selaras dengan kriteria yang diwujudkan	**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: Maklumat dikongsi selaras dengan pelan tindak balas	**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, Klausa 7.4, Klausa 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: Penyelarasan dengan pihak berkepentingan berlaku selaras dengan pelan tindak balas	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** Klausa 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

Fungsi	Kategori	SubKategori	Rujukan Informatif
		RS.CO-5: Perkongsian maklumat secara sukarela berlaku dengan pihak berkepentingan luaran, untuk mencapai kesedaran situasi keselamatan 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 dijalankan untuk memastikan tindak balas yang berkesan dan menyokong aktiviti pemulihan.	**RS.AN-1:** Pemberitahuan daripada sistem pengesanan disiasat	**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: Impak kejadian itu difahamkan	**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: Kejadian dikategorikan selaras dengan pelan tindak balas	**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

Fungsi	Kategori	SubKategori	Rujukan Informatif
		RS.AN-5: Proses diwujudkan untuk menerima, menganalisis dan bertindak balas terhadap kerentanan yang didedahkan kepada organisasi daripada sumber dalaman dan luaran (misalnya pengujian dalaman, buletin keselamatan, atau penyelidik keselamatan)	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Pengurangan (RS.MI): Aktiviti dilakukan untuk mencegah peristiwa daripada tersebar, mengurangkan kesannya dan menyelesaikan kejadian tersebut.	**RS.MI-1:** Kejadian dibendung	**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: Kejadian dikurangkan	**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 baharu dikenal pasti dikurangkan atau didokumenkan sebagai risiko yang diterima	**CIS CSC** 4 **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Penambahbaikan (RC.IM): Aktiviti tindak balas organisasi ditambah baik dengan menggabungkan pengajaran yang diperoleh daripada aktiviti pengesanan/tindak balas semasa dan terdahulu.	**RS.IM-1:** Pelan tindak balas menggabungkan pengajaran yang diperoleh	**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, Klausa 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Strategi tindak balas dikemaskinikan	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, Klausa 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8

Fungsi	Kategori	SubKategori	Rujukan Informatif
	Perancangan Pemulihan (RC.RP): Proses dan prosedur pemulihan dilaksanakan dan dikekalkan untuk memastikan pemulihan sistem atau aset yang terjejas oleh kejadian keselamatan siber.	**RC.RP-1:** Pelan pemulihan dilaksanakan semasa atau selepas kejadian keselamatan 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
	Penambahbaikan (RC.IM): Perancangan dan proses pemulihan ditambah baik dengan menggabungkan pengajaran yang diperoleh ke dalam aktiviti masa depan.	**RC.IM-1:** Pelan pemulihan menggabungkan pengajaran yang diperoleh	**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, Klausa 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Strategi pemulihan dikemaskinikan	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, Klausa 10 **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Komunikasi (RC.CO): Aktiviti pemulihan diselaraskan dengan pihak dalaman dan luaran (misalnya pusat penyelarasan, Penyedia Perkhidmatan Internet, pemilik sistem penyerang, mangsa, CSIRT lain dan vendor).	**RC.CO-1:** Perhubungan awam diuruskan	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, Klausa 7.4
		RC.CO-2: Reputasi dibaik pulih selepas kejadian	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Klausa 7.4
		RC.CO-3: Aktiviti pemulihan dimaklumkan kepada pihak berkepentingan dalaman dan luaran serta pasukan eksekutif dan pengurusan	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Klausa 7.4 **NIST SP 800-53 Rev. 4** CP-2, IR-4

Maklumat berkenaan Rujukan Informatif yang diterangkan dalam Lampiran A boleh didapati di lokasi berikut:

- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): https://www.cisecurity.org
- American National Standards Institute/International Society of Automation (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*: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels*: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
- ISO/IEC 27001, *Information technology -- Security techniques -- Information security management systems -- Requirements*: https://www.iso.org/standard/54534.html
- 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 (termasuk kemas kini setakat 22 Januari 2015). https://doi.org/10.6028/NIST.SP.800-53r4. Rujukan Informatif hanya dipetakan kepada tahap kawalan, walaupun apa-apa peningkatan kawalan mungkin didapati berguna dalam mencapai hasil subkategori.

Pemetaan antara Subkategori Teras Rangka Kerja dan seksyen tertentu dalam Rujukan Informatif tidak bertujuan untuk menentukan secara muktamad sama ada seksyen tertentu dalam Rujukan Informatif memberikan hasil Subkategori yang diingini.

Rujukan Informatif tidak menyeluruh, kerana bukan semua elemen (misalnya, kawalan, keperluan) Rujukan Informatif yang diberikan dipetakan kepada Subkategori Teras Rangka Kerja.

Lampiran B: Glosari

Lampiran ini mentakrifkan istilah terpilih yang digunakan dalam penerbitan ini.

Jadual 3: Glosari Rangka Kerja

Pembeli (*Buyer*)	Orang atau organisasi yang menggunakan produk atau perkhidmatan tertentu.
Kategori (*Category*)	Pembahagian Fungsi kepada kumpulan hasil keselamatan siber, berkait rapat dengan keperluan program dan aktiviti tertentu. Contoh Kategori termasuk "Pengurusan Aset", "Pengurusan Identiti dan Kawalan Akses" dan "Proses Pengesanan."
Infrastruktur Kritikal (*Critical Infrastructure*)	Sistem dan aset, sama ada fizikal atau maya, sangat penting kepada Amerika Syarikat sehingga ketidakupayaan atau kemusnahan sistem dan aset tersebut akan memberikan impak yang melemahkan ke atas keselamatan siber, keselamatan ekonomi negara, kesihatan atau keselamatan awam negara, atau mana-mana gabungan perkara tersebut.
Keselamatan siber (*Cybersecurity*)	Proses melindungi maklumat dengan mencegah, mengesan dan bertindak balas terhadap serangan.
Peristiwa Keselamatan Siber (*Cybersecurity Event*)	Perubahan keselamatan siber yang boleh memberikan impak ke atas pengendalian organisasi (termasuk misi, keupayaan, atau reputasi).
Kejadian Keselamatan Siber (*Cybersecurity Incident)*	Peristiwa keselamatan siber yang telah ditentukan untuk memberikan impak kepada organisasi yang mendorong keperluan untuk bertindak balas dan pemulihan.
Kesan (fungsi) (*Detect (function)*)	Membangunkan dan melaksanakan aktiviti yang sesuai untuk mengenal pasti peristiwa keselamatan siber yang berlaku.
Rangka Kerja (*Framework*)	Pendekatan berasaskan risiko untuk mengurangkan risiko keselamatan siber yang terdiri daripada tiga bahagian: Teras Rangka Kerja, Profil Rangka Kerja dan Peringkat Pelaksanaan Rangka Kerja. Dikenali juga sebagai "Rangka Kerja Keselamatan Siber."
Teras Rangka Kerja (*Framework Core*)	Set aktiviti dan rujukan keselamatan siber yang biasa merentasi sektor infrastruktur kritikal dan disusun mengikut hasil tertentu. Teras Rangka Kerja terdiri daripada empat jenis elemen: Fungsi, Kategori, Subkategori dan Rujukan Informatif.
Peringkat Pelaksanaan Rangka Kerja (*Framework Implementation Tier*)	Lensa untuk melihat ciri pendekatan organisasi terhadap risiko—cara organisasi melihat risiko keselamatan siber dan proses yang disediakan untuk menguruskan risiko tersebut.

Profil Rangka Kerja (*Framework Profile*)	Perwakilan hasil yang sistem atau organisasi tertentu telah pilih daripada Kategori Rangka Kerja dan Subkategori.
Fungsi (*Function*)	Satu daripada komponen utama Rangka Kerja. Fungsi menyediakan tahap struktur tertinggi untuk mengatur aktiviti asas keselamatan siber ke dalam Kategori dan Subkategori. Lima fungsi tersebut ialah Kenal pasti, Lindung, Kesan, Tindak Balas dan Pulih.
Kenal Pasti (fungsi) (*Identify (function))*	Membangunkan pemahaman organisasi untuk menguruskan risiko keselamatan siber kepada sistem, aset, data dan keupayaan.
Rujukan Informatif (*Informative Reference*)	Bahagian piawaian, garis panduan dan amalan khusus yang biasa dalam kalangan sektor infrastruktur kritikal yang menggambarkan kaedah untuk mencapai hasil yang dikaitkan dengan setiap Subkategori. Contoh Rujukan Informatif ialah ISO/IEC 27001 Kawalan A.10.8.3, yang menyokong Subkategori "Data dalam transit dilindungi" bagi Kategori "Keselamatan Data" dalam fungsi "Lindung".
Kod Mudah Alih (*Mobile Code*)	Program (misalnya, skrip, makro, atau arahan mudah alih lain) yang boleh dihantar dalam keadaan tidak berubah kepada koleksi platform heterogen (pelbagai jenis) dan dilaksanakan dengan semantik yang sama.
Lindung (fungsi) (*Protect (function)*)	Membangunkan dan melaksanakan perlindungan yang sesuai untuk memastikan penyampaian perkhidmatan infrastruktur kritikal.
Pengguna Istimewa (*Privileged User*)	Pengguna yang dibenarkan (dan, oleh itu, dipercayai) untuk menjalankan fungsi berkaitan keselamatan yang pengguna biasa tidak dibenarkan melakukannya.
Pulih (fungsi) (*Recover (function)*)	Membangunkan dan melaksanakan aktiviti yang sesuai bagi mengekalkan rancangan untuk kebingkasan dan memulihkan apa-apa keupayaan atau perkhidmatan yang terjejas disebabkan oleh peristiwa keselamatan siber.
Tindak Balas (*Respond (function)*)	Membangunkan dan melaksanakan aktiviti yang sesuai untuk mengambil tindakan berkenaan peristiwa keselamatan siber yang dikesan.
Risiko (*Risk*)	Ukuran sejauh mana entiti diancam oleh keadaan atau peristiwa yang berpotensi berlaku dan biasanya fungsi: (i) impak buruk yang akan timbul jika keadaan atau peristiwa itu berlaku; dan (ii) kemungkinan berlaku.
Pengurusan Risiko (*Risk Management*)	Proses mengenal pasti, menilai dan bertindak balas terhadap risiko.

Subkategori (*Subcategory*)	Pembahagian Kategori kepada hasil khusus aktiviti teknikal dan/atau pengurusan. Contoh Subkategori termasuk "Sistem maklumat luaran dikatalogkan," "Data dalam storan dilindungi" dan "Pemberitahuan daripada sistem pengesanan disiasat."
Pembekal (*Supplier*)	Pembekal produk dan penyedia perkhidmatan yang digunakan untuk tujuan dalaman organisasi (misalnya, infrastruktur IT) atau diintegrasikan ke dalam produk perkhidmatan yang disediakan kepada Pembeli organisasi tersebut.
Taksonomi (*Taxonomy*)	Skim klasifikasi.

Lampiran C: Akronim

Lampiran ini mentakrifkan akronim terpilih yang digunakan dalam penerbitan ini.

ANSI	Institut Piawaian Kebangsaan Amerika (American National Standards Institute)
CEA	Akta Peningkatan Keselamatan Siber 2014 (Cybersecurity Enhancement Act of 2014)
CIS	Pusat Keselamatan Internet (Center for Internet Security)
COBIT	Objektif Kawalan untuk Maklumat dan Teknologi Berkaitan (Control Objectives for Information and Related Technology)
CPS	Sistem Siber-Fizikal (Cyber-Physical Systems)
CSC	Kawalan Keselamatan Kritikal (Critical Security Control)
DHS	Jabatan Keselamatan Dalam Negeri (Department of Homeland Security)
EO	Arahan Eksekutif (Executive Order)
ICS	Sistem Kawalan Industri (Industrial Control Systems)
IEC	Suruhanjaya Elektroteknik Antarabangsa (International Electrotechnical Commission)
IoT	Internet Benda (Internet of Things)
IR	Laporan Antara Agensi (Interagency Report)
ISA	Persatuan Automasi Antarabangsa (International Society of Automation)
ISAC	Pusat Perkongsian dan Analisis Maklumat (Information Sharing and Analysis Center)
ISAO	Pertubuhan Perkongsian dan Analisis Maklumat (Information Sharing and Analysis Organization)
ISO	Pertubuhan Pemiawaian Antarabangsa (International Organization for Standardization)
IT	Teknologi Maklumat (Information Technology)
NIST	Institut Piawaian dan Teknologi Kebangsaan (National Institute of Standards and Technology)
OT	Teknologi Pengendalian (Operational Technology)
PII	Maklumat Pengenalpastian Peribadi (Personally Identifiable Information)
RFI	Permintaan Maklumat (Request for Information)
RMP	Proses Pengurusan Risiko (Risk Management Process)
SCRM	Pengurusan Risiko Rantaian Bekalan (Supply Chain Risk Management)
SP	Penerbitan Khas (Special Publication)