Keamanan siber

Topical Requirement

Persyaratan Topik Spesifik

Panduan Pengguna

The Institute of
Internal Auditors

Isi

Gambaran Umum Persyaratan Topik Spesifik

Persyaratan Topik Spesifik merupakan komponen penting dari Kerangka Kerja Praktik Profesional Internasional (International Professional Practices Framework®), bersama dengan Standar Audit Internal Global (Global Internal Audit Standards™) dan Panduan Global. Institute of Internal Auditors mengharuskan Persyaratan Topik Spesifik untuk digunakan bersama dengan Standar Audit Internal Global, yang memberikan dasar otoritatif atas praktik-praktik yang disyaratkan. Referensi ke Standar muncul di seluruh panduan ini sebagai sumber informasi yang lebih rinci.

Persyaratan Topik Spesifik memformalkan bagaimana auditor internal menangani area risiko yang lazim terjadi untuk meningkatkan kualitas dan konsistensi dalam profesi. Persyaratan Topik Spesifik menetapkan batas acuan dan memberikan kriteria yang relevan untuk melaksanakan jasa asurans yang terkait dengan subjek Persyaratan Topik Spesifik (Standar 13.4 Kriteria Evaluasi). Kesesuaian dengan Persyaratan Topik Spesifik adalah wajib untuk jasa asurans dan direkomendasikan untuk dievaluasi dalam pelaksanaan jasa advisori. Persyaratan Topik Spesifik tidak dimaksudkan untuk mencakup semua aspek potensial yang harus dipertimbangkan ketika melakukan penugasan asurans; namun, persyaratan tersebut dimaksudkan untuk memberikan seperangkat persyaratan minimum untuk memungkinkan penilaian yang konsisten dan dapat diandalkan atas topik tersebut.

Persyaratan Topik Spesifik secara jelas terkait dengan Model Tiga Lini IIA dan Standar Audit Internal Global. Tata kelola, manajemen risiko, dan proses pengendalian adalah komponen utama dari Persyaratan Topik Spesifik yang selaras dengan Standar 9.1 Memahami Proses Tata Kelola, Manajemen Risiko, dan Pengendalian. Mengacu pada Model Tiga Lini, tata kelola berhubungan dengan dewan/badan yang bertanggungjawab atas tata kelola, manajemen risiko berhubungan dengan lini kedua, dan pengendalian atau proses pengendalian berhubungan dengan lini pertama. Saat manajemen diwakili di lini pertama dan kedua, fungsi audit internal ditempatkan di lini ketiga sebagai penyedia asurans yang independen dan obyektif, yang melapor kepada dewan/badan yang bertanggungjawab atas tata kelola (Prinsip 8 Pengawasan Dewan).

Penerapan, Risiko, dan Penilaian Profesional

Persyaratan Topik Spesifik harus diikuti ketika fungsi audit internal melakukan penugasan asurans atas subjek yang memiliki Persyaratan Topik Spesifik atau ketika aspek-aspek dari Persyaratan Topik Spesifik diidentifikasi dalam penugasan asurans lainnya.

Sebagaimana dijelaskan dalam Standar, penilaian risiko merupakan bagian penting dari perencanaan chief audit executive. Menentukan penugasan asurans yang akan dimasukkan ke dalam rencana audit internal memerlukan penilaian atas strategi, tujuan, dan risiko organisasi setidaknya setiap tahun (Standar 9.4 Rencana Audit Internal). Ketika merencanakan penugasan asurans individu, auditor internal harus menilai risiko yang relevan dengan penugasan tersebut (Standar 13.2 Asesmen Risiko Penugasan).

Saat subjek dari Persyaratan Topik Spesifik diidentifikasi selama proses perencanaan audit internal berbasis risiko dan termasuk dalam rencana audit, maka persyaratan yang diuraikan dalam Persyaratan Topik Spesifik harus digunakan untuk menilai topik tersebut dalam penugasan. Selain itu, ketika auditor internal melakukan penugasan (baik yang termasuk atau tidak termasuk dalam rencana) dan elemen-elemen dari Persyaratan Topik Spesifik muncul, maka Persyaratan Topik Spesifik tersebut harus dinilai penerapannya sebagai bagian dari penugasan tersebut. Terakhir, jika penugasan yang diminta tidak termasuk dalam rencana dan termasuk dalam topik tersebut, maka Persyaratan Topik Spesifik harus dinilai penerapannya.

Pertimbangan profesional memainkan peran kunci dalam penerapan Persyaratan Topik Spesifik. Penilaian risiko mendorong keputusan chief audit executive mengenai penugasan mana yang akan dimasukkan ke dalam rencana audit internal (Standar 9.4 Rencana Audit Internal). Selain itu, auditor internal menggunakan pertimbangan profesional untuk menentukan aspek-aspek apa saja yang akan dicakup dalam setiap penugasan (Standar 13.3 Tujuan dan Ruang Lingkup Penugasan, 13.4 Kriteria Evaluasi, dan 13.6 Program Kerja). Lampiran A "Contoh Penerapan Praktis" menjelaskan bagaimana auditor internal menentukan apakah Persyaratan Topik Spesifik berlaku.

Bukti bahwa setiap persyaratan dalam Persyaratan Topik Spesifik telah dinilai penerapannya harus disimpan, termasuk alasan yang menjelaskan pengecualian persyaratan apa pun. Kesesuaian dengan Persyaratan Topik Spesifik harus didokumentasikan dengan menggunakan pertimbangan profesional auditor sebagaimana dijelaskan dalam Standar 14.6 Dokumentasi Penugasan.

Meskipun Persyaratan Topik Spesifik Keamanan Siber memberikan batas acuan proses pengendalian yang perlu dipertimbangkan, organisasi yang menilai risiko siber sangat tinggi mungkin perlu menilai aspek-aspek lainnya.

Jika chief audit executive menetapkan bahwa fungsi audit internal tidak memiliki pengetahuan yang diperlukan untuk melaksanakan penugasan audit atas suatu subjek Persyaratan Topik Spesifik, maka pekerjaan penugasan tersebut dapat dialihdayakan (Standar 3.1 Kompetensi, 7.2 Kualifikasi Chief Audit Executive, 10.2 Pengelolaan Sumber Daya Manusia). Meskipun demikian, alih daya tidak membebaskan fungsi audit internal dari tanggung jawabnya untuk mematuhi Persyaratan Topik Spesifik. Chief audit executive tetap memiliki tanggung jawab utama untuk memastikan kepatuhan. Selain itu, jika chief audit executive menentukan bahwa sumber daya audit internal tidak memadai, chief audit executive harus menginformasikan kepada dewan tentang dampak dari sumber daya yang tidak mencukupi dan bagaimana kekurangan sumber daya tersebut akan diatasi (Standar 8.2 Sumber Daya).

Kinerja, Dokumentasi, dan Pelaporan

Ketika menerapkan Persyaratan Topik Spesifik, auditor internal juga harus mematuhi Standar, melaksanakan pekerjaan mereka sesuai dengan Domain V: Melaksanakan Jasa Audit Internal. Standar dalam Domain V menjelaskan tentang perencanaan penugasan (Prinsip 13 Merencanakan Penugasan Secara Efektif), pelaksanaan penugasan (Prinsip 14 Melaksanakan Penugasan), dan mengomunikasikan hasil penugasan (Prinsip 15 Mengomunikasikan Hasil Penugasan dan Memantau Rencana Perbaikan).

Cakupan Persyaratan Topik Spesifik dapat didokumentasikan dalam rencana audit internal atau kertas kerja penugasan berdasarkan pertimbangan profesional auditor. Satu atau lebih penugasan audit internal dapat mencakup persyaratan tersebut. Selain itu, tidak semua persyaratan dapat diterapkan. Bukti bahwa Persyaratan Topik Spesifik telah dinilai untuk penerapannya harus disimpan, termasuk alasan yang menjelaskan adanya pengecualian.

Alat bantu opsional pada Lampiran C dapat digunakan sebagai referensi dan untuk mendokumentasikan pekerjaan yang dilakukan oleh auditor internal.

Jaminan Kualitas

Standar ini mengharuskan chief audit executive untuk mengembangkan, menerapkan, dan memelihara program asurans dan peningkatan kualitas yang mencakup semua aspek fungsi audit internal (Standar 8.3 Kualitas). Hasilnya harus dikomunikasikan kepada dewan dan manajemen senior. Komunikasi harus melaporkan kesesuaian fungsi audit internal dengan Standar dan pencapaian tujuan kinerja.

Kesesuaian dengan Persyaratan Topik Spesifik akan dievaluasi dalam tinjauan mutu. Untuk mempersiapkan tinjauan kualitas, auditor internal dapat menggunakan alat bantu yang disediakan pada Lampiran C.

Keamanan siber

Keamanan siber adalah topik yang luas yang terkait dengan sebagian besar aspek teknologi di organisasi mana pun. Selain teknologi informasi, keamanan siber biasanya merupakan bagian dari proses bisnis, yang mengharuskan auditor internal untuk menilai risiko terkait siber ketika merencanakan, menetapkan ruang lingkup, dan melakukan penugasan asurans.

National Institute of Standards and Technology (NIST), bagian dari Departemen Perdagangan A.S., mendefinisikan keamanan siber secara sederhana sebagai "Kemampuan untuk melindungi atau mempertahankan penggunaan ruang siber dari serangan siber." Persyaratan Topik Spesifik Keamanan Siber berfokus pada perimeter eksternal yang diamankan oleh organisasi untuk mengurangi risiko dari pengguna yang tidak sah dan ancaman siber yang berbahaya. Keamanan siber merupakan bagian dari keamanan informasi menyeluruh, yang didefinisikan NIST sebagai "Perlindungan informasi dan sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak sah dalam rangka memberikan kerahasiaan, integritas, dan ketersediaan."

Persyaratan dari Persyaratan Topik Spesifik Keamanan Siber meliputi:

- Tata kelola – batas acuan tujuan dan strategi keamanan siber yang didefinisikan dengan jelas yang mendukung tujuan, kebijakan, dan prosedur organisasi.
- Manajemen Risiko - proses untuk mengidentifikasi, menganalisis, mengelola, dan memantau ancaman siber, termasuk proses untuk eskalasi risiko siber dengan segera.
- Pengendalian - proses pengendalian yang ditetapkan oleh manajemen dan dievaluasi secara berkala untuk memitigasi risiko siber.

Pertimbangan

Auditor internal dapat menggunakan pertimbangan berikut ini untuk membantu penilaian mereka terhadap persyaratan dalam Persyaratan Topik Keamanan Siber. Pertimbangan-pertimbangan ini, yang merupakan referensi silang dari persyaratan, bersifat ilustratif tetapi tidak wajib. Auditor internal harus mengandalkan pertimbangan profesional ketika menentukan apa yang harus disertakan dalam penilaian mereka.

Pertimbangan Tata Kelola

Untuk menilai bagaimana proses tata kelola diterapkan pada tujuan keamanan siber, auditor internal dapat meninjau:

A. Rencana dan tujuan strategis keamanan siber yang diformalkan dan didokumentasikan, termasuk bukti bahwa dewan secara berkala (biasanya per triwulan) meninjau pembaruan keamanan siber yang diberikan oleh kepala fungsi keamanan informasi, seperti chief information security officer (CISO). Bukti dapat berupa laporan:
    - Pemantauan pencapaian tujuan strategis.
    - Kebutuhan anggaran untuk mendukung tujuan dan sasaran keamanan siber.
    - Fokus pada risiko dan pengendalian internal, termasuk kemajuan remediasi.
    - Indikator kinerja utama (KPI) untuk mengukur keberhasilan.
    - Sumber daya manusia yang dibutuhkan untuk mempekerjakan, melatih, dan mengembangkan personel keamanan siber.

B. Kebijakan, prosedur, dan dokumentasi terkait lainnya yang digunakan untuk mengelola proses keamanan siber, termasuk:
    - Kebijakan yang ditinjau dan diperbarui setidaknya setiap tahun. Risiko siber yang muncul mungkin mengharuskan peninjauan dan pembaruan dilakukan lebih sering.
    - Sebuah proses untuk menentukan apakah kebijakan dan prosedur sudah cukup untuk mendukung operasi keamanan siber.
    - Kerangka kerja yang diadopsi secara luas (NIST, COBIT, dan lainnya) untuk memperkuat proses keamanan siber dan pengendalian internal.

C. Peran dan tanggung jawab yang mendukung pencapaian tujuan keamanan siber, termasuk struktur yang memastikan bahwa fungsi keamanan siber melapor ke tingkat organisasi yang memiliki visibilitas yang cukup untuk mendapatkan dukungan organisasi.
    - Sebuah proses untuk menilai pengetahuan, keterampilan, dan kemampuan personel yang mengisi peran keamanan siber secara berkala.

D. Bukti keterlibatan dengan pemangku kepentingan yang relevan (misalnya, manajemen senior, operasi, manajemen risiko, sumber daya manusia, hukum, kepatuhan, vendor strategis, dan lainnya), termasuk komunikasi tentang risiko siber yang ada dan yang sedang berkembang serta potensi kerentanan yang diketahui. Bukti komunikasi dapat berupa notulen rapat, laporan, atau surat elektronik.

Pertimbangan Manajemen Risiko

Untuk menilai bagaimana proses manajemen risiko diterapkan untuk mencapai tujuan keamanan siber, auditor internal dapat melakukan peninjauan:

A. Bagaimana organisasi menilai dan mengelola risiko keamanan siber, termasuk bagaimana ancaman dan kerentanannya:
   - Awal identifikasi dan pelaporan.
   - Analisis untuk mengevaluasi risiko terhadap pencapaian tujuan organisasi.
   - Mitigasi, termasuk rencana tindakan untuk mengurangi risiko ke tingkat yang dapat diterima.
   - Pemantauan, termasuk rencana pelaporan yang berkelanjutan hingga ancaman benar-benar teratasi.

B. Bagaimana organisasi memperoleh masukan secara berkala mengenai manajemen risiko keamanan siber dari area fungsional, seperti teknologi informasi, manajemen risiko perusahaan, sumber daya manusia, hukum, kepatuhan, operasi, akuntansi, dan keuangan. Tim keamanan siber lintas fungsi atau komite pengarah TI dapat digunakan untuk mendapatkan informasi.

C. Bagaimana organisasi telah menetapkan akuntabilitas dan tanggung jawab untuk manajemen risiko keamanan siber kepada individu atau tim.
   - Orang yang bertanggung jawab harus mengomunikasikan pembaruan risiko keamanan siber yang sedang berlangsung di seluruh organisasi secara berkala (triwulanan, bulanan, atau sesuai kebutuhan) dan juga dapat menyertakan kebutuhan sumber daya untuk strategi mitigasi risiko.

D. Proses eskalasi untuk risiko keamanan siber, termasuk bagaimana tingkat ancaman atau risiko dievaluasi, ditetapkan, dan diprioritaskan. Peninjauan ini dapat mencakup identifikasi:
   - Tingkat risiko yang ditetapkan organisasi - seperti tinggi, sedang, dan rendah - dengan penjelasan rinci tentang setiap tingkat risiko dan prosedur eskalasi untuk setiap kategori risiko.
   - Daftar risiko keamanan siber yang saat ini teridentifikasi dan status mitigasi dari setiap kejadian risiko.
   - Persyaratan hukum, peraturan, dan kepatuhan yang berlaku.
   - Dampak risiko keuangan dan non-keuangan (misalnya, reputasi).

E. Proses untuk mengomunikasikan risiko keamanan siber kepada manajemen dan karyawan, yang meliputi:
   - Pelatihan keamanan siber karyawan secara berkala (setidaknya setiap tahun), seperti kampanye *phishing* yang disimulasikan tanpa pemberitahuan untuk menguji dan melacak kesadaran organisasi.

- Pembaruan tentang perbaikan masalah keamanan siber yang ada, dengan tanggal penyelesaian yang diantisipasi.
- Memantau ketidakpatuhan yang mencakup informasi terbaru kepada dewan direksi dan manajemen senior.
- Menilai kembali ancaman ketika selera risiko dan toleransi risiko organisasi berubah.

F. Proses yang telah diterapkan organisasi terkait respons dan pemulihan insiden, yang meliputi:

- Rencana terdokumentasi yang ditinjau dan diperbarui seiring dengan perubahan operasional organisasi dari waktu ke waktu. Rencana tersebut harus mencakup:
  - Bagaimana insiden terdeteksi dan dilaporkan.
  - Bagaimana insiden dapat diatasi untuk mencegah kerusakan lebih lanjut.
  - Bagaimana organisasi akan pulih dan merespons untuk melanjutkan operasi.
  - Bagaimana insiden tersebut akan dianalisis untuk mengidentifikasi pelajaran yang dapat dipetik dan bagaimana mencegah kejadian serupa di masa depan.
- Pengujian berkala *tabletop exercise* (setidaknya setiap tahun) dan melaporkan hasilnya kepada manajemen senior dan pemangku kepentingan yang relevan. Rencana tindak dapat dihasilkan dari pengujian tersebut.

Pertimbangan Proses Pengendalian

Untuk menilai bagaimana proses pengendalian diterapkan pada tujuan keamanan siber, auditor internal dapat meninjau:

A. Pendekatan manajemen untuk membangun lingkungan pengendalian internal keamanan siber yang efektif, termasuk:

- Menilai dan menerapkan pengendalian internal yang diperlukan untuk memitigasi risiko yang meningkat dan melindungi data sensitif, penting, pribadi, atau rahasia, yang diinformasikan oleh proses penilaian risiko organisasi.
- Menentukan kebutuhan sumber daya untuk mempertahankan pengendalian keamanan siber utama.
- Mempertimbangkan pengendalian berbasis vendor sebagai bagian dari lingkungan pengendalian, yang mencakup peninjauan laporan pengendalian organisasi layanan (SOC) dari vendor sebelum memulai hubungan bisnis dan selama jangka waktu hubungan.
- Pengujian berkala bahwa pengendalian keamanan siber berfungsi dengan cara yang dapat mengurangi risiko dan mendukung pencapaian tujuan keamanan siber.

- Proses untuk memperbaiki kekurangan pengendalian internal atau menangani temuan dari penilaian yang dilakukan oleh fungsi audit internal atau penyedia jasa asurans lainnya (misalnya, pengujian penetrasi).

B. Proses manajemen talenta organisasi untuk merekrut dan melatih profesional keamanan siber, termasuk bagaimana organisasi mengidentifikasi peluang untuk meningkatkan kemampuan profesional keamanan siber untuk mendukung pengetahuan teknis dan meningkatkan kesadaran organisasi akan isu-isu yang muncul.
   - Contohnya termasuk partisipasi dalam pelatihan, keterlibatan dengan kelompok berbagi pengetahuan, dan pendidikan profesional berkelanjutan yang mencakup pencapaian sertifikasi terkait dunia maya.

C. Proses manajemen untuk mengidentifikasi, memprioritaskan, memantau, dan melaporkan ancaman dan kerentanan keamanan siber yang muncul secara terus menerus yang difokuskan pada operasi sehari-hari. Tinjauan ini dapat mencakup proses yang ditetapkan untuk menilai ancaman dan kerentanan yang terkait dengan teknologi baru atau yang sedang berkembang seperti penggunaan kecerdasan buatan.

D. Proses dan pengendalian manajemen yang dibuat untuk mengelola dan melindungi aset TI sepanjang siklus hidup termasuk pemilihan, penggunaan, pemeliharaan, dan penonaktifan perangkat keras, perangkat lunak, dan layanan vendor. Perangkat keras meliputi server, peralatan jaringan (seperti *router* atau *firewall*), *desktop*, *laptop*, ponsel, tablet, dan periferal. Perangkat lunak mencakup sistem operasi (seperti Windows), perangkat lunak perencanaan sumber daya perusahaan, aplikasi, program antivirus, dan lainnya. Pertimbangan perangkat keras dan perangkat lunak dapat mencakup:
   - Penggunaan enkripsi, perangkat lunak antivirus, manajemen perangkat seluler, persyaratan kata sandi yang rumit, *virtual private network* (VPN)/ *zero trust networking* (ZTN) untuk otentikasi, dan pembaruan *firmware* secara berkala.
   - Proses manajemen aset yang memastikan bahwa perangkat keras yang digunakan perusahaan memiliki konfigurasi keamanan yang sesuai pada saat penggunaan dan pemusnahan yang tepat saat aset tidak digunakan lagi.
   - Pengendalian terkait basis data yang mencakup pembatasan akses pengguna dan administrator, memastikan penggunaan enkripsi, pencadangan dan pengujian basis data, dan adanya pengendalian keamanan jaringan yang kuat.
   - Bagaimana ancaman atau kerentanan keamanan siber dipertimbangkan dalam siklus hidup pengembangan sistem (SDLC).
   - Pendekatan yang digunakan oleh pengembangan, keamanan, dan operasi (DevSecOps) untuk memastikan proses pengembangan perangkat lunak mencakup keamanan siber untuk mengidentifikasi kerentanan secara proaktif.

E. Proses yang digunakan untuk memperkuat keamanan siber, termasuk:
   - Konfigurasi pengaturan keamanan untuk meminimalkan risiko keamanan siber.
   - Administrasi perangkat seluler (termasuk penggunaan surat elektronik dan aplikasi) dikonfigurasikan untuk mengurangi risiko keamanan siber dan dikelola dari jarak jauh jika perangkat pengguna disusupi.
   - Penggunaan enkripsi untuk data yang "tidak aktif", seperti informasi yang disimpan di *hard drive*, atau data yang "sedang dalam perjalanan", seperti mengenkripsi surat elektronik.
   - Menambal server atau perangkat lunak (seperti sistem operasi) dengan rilis keamanan terbaru.
   - Manajemen akses pengguna seperti penggunaan otentikasi multifaktor (MFA) dan ID pengguna yang unik dengan kata sandi kompleks yang kedaluwarsa secara berkala.
   - Memantau pengendalian yang ada untuk menentukan apakah ketersediaan dan pemanfaatan sumber daya berjalan dengan baik, memungkinkan peninjauan dan analisis potensi masalah keamanan siber yang mengancam kinerja.
   - Integrasi keamanan siber ke dalam SDLC untuk mengidentifikasi dan mengatasi kerentanan keamanan siber sebelum perangkat lunak dipindahkan ke produksi.

F. Pengendalian terkait jaringan yang mengamankan perimeter organisasi, termasuk bagaimana organisasi memanfaatkannya:
   - Segmentasi jaringan.
   - *Firewall*. tabletop exercise
   - Pengendalian akses pengguna.
   - Keterbatasan koneksi eksternal dan internal.
   - Pengendalian seputar Internet of Things (IoT) untuk jaringan yang saling terhubung.
   - Sistem deteksi/pencegahan penyusupan untuk mencegah, mendeteksi, dan memulihkan diri dari serangan keamanan siber.

G. Pengendalian seputar pengendalian keamanan komunikasi titik akhir yang berlaku untuk layanan seperti surat elektronik, browser internet, konferensi video, *messaging* (Zoom, MS Teams, dan lainnya), media sosial, *cloud*, dan protokol berbagi file. Pengendalian dapat mencakup pembatasan penggunaan ekstensi file tertentu (seperti file .exe) dan otentikasi multifaktor untuk berbagi file.

Lampiran A. Contoh Aplikasi Praktis

Contoh-contoh berikut ini menjelaskan skenario di mana Persyaratan Topik Spesifik Keamanan Siber dapat diterapkan:

Contoh 1: Keamanan siber diidentifikasi untuk penugasan audit internal yang termasuk dalam rencana audit internal.

Ketika fungsi audit internal menyelesaikan proses perencanaan berbasis risiko dan memasukkan satu atau beberapa penugasan terkait keamanan siber dalam rencana audit internal, maka Persyaratan Topik Spesifik menjadi mandat ketika melakukan penugasan tersebut. Kesesuaian dapat dicapai dengan memasukkan persyaratan di satu atau beberapa penugasan dalam rencana audit internal.

Keamanan siber merupakan topik yang luas, dan tidak semua persyaratan dalam Persyaratan Topik dapat diterapkan dalam setiap penugasan. Ketika auditor internal menerapkan pertimbangan profesional dan menentukan bahwa satu atau beberapa persyaratan dalam Persyaratan Topik Spesifik Keamanan Siber tidak dapat diterapkan dan oleh karena itu harus dikecualikan dari penugasan, auditor internal harus mendokumentasikan dan menyimpan alasan untuk mengecualikan persyaratan tersebut. Sebagai contoh, alasan untuk mengecualikan beberapa persyaratan dapat berupa bahwa fungsi audit internal melakukan berbagai penugasan keamanan siber secara bergilir atau telah menentukan bahwa signifikansi risiko dalam penugasan tersebut rendah.

Contoh 2: Risiko keamanan siber diidentifikasi selama penugasan audit yang tidak berfokus pada keamanan siber.

Auditor internal dapat mengidentifikasi risiko keamanan siber ketika menilai proses yang tidak terkait langsung dengan keamanan siber. Sebagai contoh, auditor internal mungkin menilai proses penilaian *accounts payable* dalam penugasan yang tidak berfokus pada keamanan siber dan tidak mengidentifikasi risiko keamanan siber sebagai bagian dari ruang lingkup saat merencanakan penugasan. Namun, setelah melakukan penelusuran awal, auditor internal menentukan bahwa risiko tersebut harus berada dalam ruang lingkup; misalnya, mereka mengidentifikasi risiko keamanan siber yang terkait dengan pengajuan permintaan pesanan pembelian awal berbasis web (Standar 13.2 Asesmen Risiko Penugasan).

Setelah risiko yang relevan diidentifikasi, auditor internal harus meninjau Persyaratan Topik Spesifik Keamanan Siber dan menentukan persyaratan mana yang berlaku. Dalam contoh ini, mereka mungkin mengecualikan proses tata kelola keamanan siber atau proses manajemen risiko keamanan siber. Mereka harus mendokumentasikan dalam kertas kerja penugasan alasan untuk mengecualikan persyaratan lain dari Persyaratan Topik Keamanan Siber dan menyimpan dokumentasi tersebut.

Contoh 3: Penugasan keamanan siber yang awalnya tidak termasuk dalam rencana audit internal diminta.

Pemangku kepentingan seperti dewan, manajemen, atau regulator dapat meminta auditor internal untuk melakukan penilaian keamanan siber di luar rencana audit awal. Misalnya, ketika organisasi menjadi target serangan siber, dewan direksi dapat meminta penugasan audit internal untuk menilai pengendalian keamanan siber. Persyaratan Topik Spesifik berlaku, persyaratan harus dinilai, dan setiap pengecualian didokumentasikan.

Lampiran B. Pemetaan ke Kerangka Kerja

Organisasi mungkin memiliki upaya keamanan sibernya sendiri, dengan menggunakan kerangka kerja manajemen risiko dan tata kelola seperti COBIT atau NIST. Auditor internal mungkin telah mengembangkan program audit dan prosedur pengujian berdasarkan kerangka kerja ini. Auditor internal harus merekonsiliasi pengujian pengendalian keamanan siber yang dimaksudkan dengan Persyaratan Topik Spesifik untuk memastikan cakupan yang memadai. Bagan di bawah ini memetakan Persyaratan Topik Spesifik Keamanan Siber ke tiga kerangka kerja yang umum digunakan: Kerangka Kerja Keamanan Siber NIST 2.0, COBIT 2019, dan NIST 800-53. Kerangka kerja ini telah dipetakan karena sudah tersedia tanpa biaya.

Persyaratan Tata Kelola	Referensi Kerangka Kerja		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. Strategi dan tujuan keamanan siber formal ditetapkan dan diperbarui secara berkala. Pembaruan tentang pencapaian tujuan keamanan siber dikomunikasikan dan ditinjau secara berkala oleh dewan, termasuk sumber daya dan pertimbangan anggaran untuk mendukung strategi keamanan siber.	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.OC-02; GV.RR-03; GV.RR-04; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-03	PM-1, PM-4; AT-2; AT-3; PM-9; PM-28	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12
B. Kebijakan dan prosedur yang terkait dengan keamanan siber dibuat, diperbarui secara berkala, dan memperkuat lingkungan pengendalian.	GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03; GV.SC-01; GV.SC-03; GV.RR-03	AC-1, PM-9; AC-1; AT-1; CA-1; CM-1; IA-1; IR-1; MP-1; PE-1	EDM01; EDM02; EDM03; APO01; APO11
C. Peran dan tanggung jawab yang mendukung tujuan keamanan siber ditetapkan, dan ada proses untuk menilai pengetahuan, keterampilan, dan kemampuan mereka yang mengisi peran tersebut secara berkala.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

D. Pemangku kepentingan yang relevan dilibatkan untuk mendiskusikan dan menindaklanjuti kerentanan yang ada dan ancaman yang muncul di lingkungan keamanan siber. Pemangku kepentingan termasuk manajemen senior, operasi, manajemen risiko, sumber daya manusia, hukum, kepatuhan, vendor, dan lainnya.	GV.OC-02; GV.RM-01; GV.RM-05; GV.RM-07; GV.OV-03; GV.SC-03	AC-1; CM-1	EDM05; EDM01.01; EDM03; MEA01.02; APO01; APO08; APO11; APO13; MEA02
Persyaratan Manajemen Risiko	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. Penilaian risiko organisasi dan proses manajemen risiko mencakup identifikasi, analisis, mitigasi, dan pemantauan ancaman keamanan siber serta pengaruhnya terhadap pencapaian tujuan strategis.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
B. Manajemen risiko keamanan siber dilakukan di seluruh organisasi, yang dapat mencakup bidang-bidang berikut: teknologi informasi, manajemen risiko perusahaan, sumber daya manusia, hukum, kepatuhan, operasi, rantai pasokan, akuntansi, keuangan, dan lain-lain.	GV.RM-01; GV.RM-05; GV.RR-01; GV.RR-02; GV.OC-03; GV.SC-07	PM-29; AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
C. Akuntabilitas dan tanggung jawab untuk manajemen risiko keamanan siber ditetapkan dan individu atau tim diidentifikasi untuk memantau dan melaporkan secara berkala bagaimana risiko keamanan siber dikelola, termasuk sumber daya yang diperlukan untuk mengurangi risiko dan mengidentifikasi ancaman keamanan siber yang muncul.	GV.RR-01; GV.RR-02; GV.RR-03; GV.0V-01; GV.OV-02; GV.OV-03	PM-9; PM-29	EDM03; APO01; APO10; APO12

D. Sebuah proses dibuat untuk dengan cepat mengeskalasi risiko keamanan siber (yang muncul atau diidentifikasi sebelumnya) yang naik ke tingkat yang tidak dapat diterima berdasarkan pedoman manajemen risiko yang telah ditetapkan oleh organisasi atau untuk mematuhi persyaratan hukum dan peraturan yang berlaku. Dampak finansial dan non-finansial dari risiko keamanan siber harus dipertimbangkan.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
E. Sebuah proses dibuat untuk mengomunikasikan kesadaran akan risiko keamanan siber kepada manajemen dan karyawan, dan untuk tinjauan berkala oleh manajemen atas masalah, kesenjangan, kekurangan, atau kegagalan pengendalian dengan pelaporan dan perbaikan.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. Organisasi telah menerapkan proses respons dan pemulihan insiden keamanan siber yang mencakup deteksi, pengurungan, pemulihan, dan analisis pasca insiden. Proses tanggap darurat dan pemulihan insiden diuji secara berkala.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07

Persyaratan Proses Pengendalian	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. Sebuah proses dibuat untuk memastikan bahwa pengendalian internal dan pengendalian berbasis vendor tersedia untuk melindungi kerahasiaan, integritas, dan ketersediaan sistem dan data organisasi. Pengendalian dievaluasi secara berkala untuk menentukan apakah pengendalian tersebut berfungsi dengan cara yang mendorong pencapaian tujuan keamanan siber organisasi dan penyelesaian masalah secara tepat waktu.	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2	MEA02; MEA04; EDM03; APO09; APO10; DSS01
B. Proses manajemen talenta dibuat dan ditinjau secara berkala untuk operasi keamanan siber yang mencakup kesempatan pelatihan untuk mengembangkan dan memelihara kompetensi teknis.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. Sebuah proses dibuat untuk terus memantau dan melaporkan ancaman dan kerentanan keamanan siber yang muncul dan untuk mengidentifikasi, memprioritaskan, dan mengimplementasikan peluang untuk meningkatkan operasi keamanan siber.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. Keamanan siber termasuk dalam manajemen siklus hidup (pemilihan, penggunaan, pemeliharaan, dan penonaktifan) semua aset TI, termasuk perangkat keras, perangkat lunak, dan layanan vendor.	ID.AM; PR.PS-03; PR.IR; DE.CM-09; ID.AM-08; ID.RA-09; PR.PS-06	AU-9; CM-7; SC-49; SC-51; CM-2; SA-3; SA-10; SA-15; SA-17; SA-20; AU-6; IR-7	DSS05.03; BAI03; BAI09; BAI03; BAI11; DSS05.01; DSS02; DSS03; DSS06.06

E. Proses dibuat untuk meningkatkan keamanan siber termasuk konfigurasi, administrasi perangkat pengguna akhir, enkripsi, penambalan, manajemen akses pengguna, dan pemantauan ketersediaan dan kinerja. Pertimbangan keamanan siber disertakan dalam pengembangan perangkat lunak (DevSecOps).	PR.PS-01; PR.PS-06; PR.DS-01; PR.DS-02; PR.PS-05; DE.CM-03	CM-6; SI-2; AC-3; CA-7; SA-4; AC-16; AC-18	BAI10; DSS05; DSS06.03; DSS01.03; MEA01
F. Pengendalian terkait jaringan dibuat, seperti pengendalian dan segmentasi akses jaringan; penggunaan dan penempatan *firewall*; koneksi terbatas dari dan ke jaringan eksternal; *virtual private network* (VPN)*/zero trust network access* (ZTNA), penyertaan pengendalian jaringan *Internet of Things* (IoT), dan sistem pendeteksian/pencegahan penyusupan (IDS dan IPS).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; AC-20; SC-7; SC-10; CA-8	DSS05.02
G. Pengendalian keamanan komunikasi *end point* dibuat terkait layanan seperti surat elektronik, browser internet, konferensi video, *messaging*, media sosial, *cloud*, dan protokol berbagi file.	PR.DS-01; PR.DS-02; PR.DS-10; PR.IR	AC-2; AC-16; AU-10; CA-3; SI-8; SI-20; SC-8	BAI10

Lampiran C. Alat Dokumentasi Opsional

Auditor internal diharapkan untuk menggunakan pertimbangan profesional dalam menentukan penerapan persyaratan berdasarkan penilaian risiko dan mendokumentasikan dengan tepat pengecualian persyaratan tertentu. Persyaratan Topik Spesifik dapat didokumentasikan dalam rencana audit internal atau dalam kertas kerja penugasan berdasarkan pertimbangan profesional auditor. Satu atau lebih penugasan audit internal dapat mencakup persyaratan tersebut. Selain itu, tidak semua persyaratan dapat diterapkan. Formulir yang dapat dicetak di bawah ini menyediakan satu opsi untuk mendokumentasikan kesesuaian dengan Persyaratan Topik Spesifik Keamanan Siber, tetapi penggunaannya tidak wajib.

Keamanan siber - Tata Kelola

Persyaratan	Cakupan yang Dieksekusi atau Alasan Pengecualian	Referensi Dokumentasi
A. Strategi dan tujuan keamanan siber ditetapkan secara formal dan diperbarui secara berkala. Pembaruan tentang pencapaian tujuan keamanan siber dikomunikasikan dan ditinjau secara berkala oleh dewan, termasuk sumber daya dan pertimbangan anggaran untuk mendukung strategi keamanan siber.		
B. Kebijakan dan prosedur yang terkait dengan keamanan siber dibuat, diperbarui secara berkala, dan memperkuat lingkungan pengendalian.		
C. Peran dan tanggung jawab yang mendukung tujuan keamanan siber ditetapkan, dan ada proses untuk menilai pengetahuan, keterampilan, dan kemampuan mereka yang mengisi peran tersebut secara berkala.		

Persyaratan	Cakupan yang Dieksekusi atau Alasan Pengecualian	Referensi Dokumentasi
D. Pemangku kepentingan yang relevan dilibatkan untuk mendiskusikan dan menindaklanjuti kerentanan yang ada dan ancaman yang muncul di lingkungan keamanan siber. Pemangku kepentingan termasuk manajemen senior, operasi, manajemen risiko, sumber daya manusia, hukum, kepatuhan, vendor, dan lainnya.		

Keamanan Siber - Manajemen Risiko

Persyaratan	Cakupan yang Dieksekusi atau Alasan Pengecualian	Referensi Dokumentasi
A. Penilaian risiko dan proses manajemen risiko organisasi mencakup identifikasi, analisis, mitigasi, dan pemantauan ancaman keamanan siber serta pengaruhnya terhadap pencapaian tujuan strategis.		
B. Manajemen risiko keamanan siber dilakukan di seluruh organisasi dan dapat mencakup bidang-bidang berikut: teknologi informasi, manajemen risiko perusahaan, sumber daya manusia, hukum, kepatuhan, operasi, rantai pasokan, akuntansi, keuangan, dan lain-lain.		

Persyaratan	Cakupan yang Dieksekusi atau Alasan Pengecualian	Referensi Dokumentasi
C. Akuntabilitas dan tanggung jawab untuk manajemen risiko keamanan siber ditetapkan. Seorang individu atau tim diidentifikasi untuk memantau dan melaporkan secara berkala bagaimana risiko keamanan siber dikelola, termasuk sumber daya yang diperlukan untuk mengurangi risiko dan mengidentifikasi ancaman keamanan siber yang muncul.		
D. Sebuah proses dibuat untuk secara cepat mengeskalasi risiko keamanan siber (yang muncul atau yang telah diidentifikasi sebelumnya) yang mencapai tingkat yang tidak dapat diterima sesuai dengan pedoman manajemen risiko yang telah ditetapkan oleh organisasi atau persyaratan hukum dan peraturan yang berlaku. Dampak finansial dan non-finansial dari risiko keamanan siber harus dipertimbangkan.		
E. Sebuah proses dibuat untuk mengomunikasikan kesadaran akan risiko keamanan siber kepada manajemen dan karyawan dan bagi manajemen untuk meninjau masalah, kesenjangan, kekurangan, atau kegagalan pengendalian secara berkala dengan pelaporan dan perbaikan tepat waktu.		
F. Organisasi telah menerapkan proses tanggap dan pemulihan insiden keamanan siber, termasuk deteksi, penahanan, pemulihan, dan analisis pasca insiden. Proses tanggap darurat dan pemulihan insiden diuji secara berkala.		

Keamanan siber - Proses Pengendalian

Persyaratan	Cakupan yang Dieksekusi atau Alasan Pengecualian	Referensi Dokumentasi
A. Sebuah proses dibuat untuk memastikan bahwa pengendalian internal dan pengendalian berbasis vendor tersedia untuk melindungi kerahasiaan, integritas, dan ketersediaan sistem dan data organisasi. Evaluasi dilakukan secara berkala untuk menentukan apakah pengendalian berfungsi dengan cara yang mendorong pencapaian tujuan keamanan siber organisasi dan penyelesaian masalah yang cepat.		
B. Proses manajemen talenta dibuat dengan mencakup pelatihan untuk mengembangkan dan memelihara kompetensi teknis yang terkait dengan operasi keamanan siber. Proses ini ditinjau secara berkala.		
C. Sebuah proses dibuat untuk terus memantau dan melaporkan ancaman dan kerentanan keamanan siber yang muncul dan untuk mengidentifikasi, memprioritaskan, dan mengimplementasikan peluang untuk meningkatkan operasi keamanan siber.		
D. Keamanan siber termasuk dalam manajemen siklus hidup (pemilihan, penggunaan, pemeliharaan, dan penonaktifan) semua aset TI, termasuk perangkat keras, perangkat lunak, dan layanan vendor.		

Persyaratan	Cakupan yang Dieksekusi atau Alasan Pengecualian	Referensi Dokumentasi
E. Proses dibuat untuk meningkatkan keamanan siber, termasuk konfigurasi, administrasi perangkat pengguna akhir, enkripsi, penambalan, manajemen akses pengguna, dan pemantauan ketersediaan dan kinerja. Pertimbangan keamanan siber disertakan dalam pengembangan perangkat lunak (DevSecOps).		
F. Pengendalian terkait jaringan dibuat, seperti pengendalian dan segmentasi akses jaringan; penggunaan dan penempatan *firewall*; koneksi terbatas dari dan ke jaringan eksternal; *virtual private networ*k (VPN)/*zero trust network access* (ZTNA), pengendalian jaringan *Internet of Things* (IoT), dan sistem deteksi/pencegahan penyusupan (IDS dan IPS).		
G. Pengendalian keamanan komunikasi *end point* dibuat untuk layanan seperti surat elektronik, *browser* internet, konferensi video, *messaging*, media sosial, cloud, dan protokol berbagi file.		

Tentang Institut Auditor Internal

The Institute of Internal Auditors (The IIA) adalah asosiasi profesional internasional yang melayani lebih dari 255.000 anggota global dan telah memberikan lebih dari 200.000 sertifikasi Certified Internal Auditor® (CIA®) di seluruh dunia. Didirikan pada tahun 1941, The IIA diakui di seluruh dunia sebagai pemimpin profesi audit internal dalam hal standar, sertifikasi, pendidikan, penelitian, dan bimbingan teknis. Untuk informasi lebih lanjut www.theiia.org.

Disclaimer

Hak Cipta

Februari 2025

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101