Keamanan siber

Topical Requirement

Persyaratan Topik Spesifik

The Institute of
Internal Auditors

Persyaratan Topik Spesifik Keamanan Siber

Kerangka Kerja Praktik Profesional Internasional (International Professional Practices Framework®) terdiri dari Standar Audit Internal Global (Global Internal Audit Standards™), Persyaratan Khusus, dan Panduan Global. Persyaratan Khusus bersifat wajib dan harus digunakan bersama dengan Standar, yang memberikan dasar otoritatif untuk praktik-praktik yang diwajibkan.

Persyaratan Topik Spesifik memberikan ekspektasi yang jelas bagi auditor internal dengan menetapkan batas acuan minimum untuk mengaudit topik risiko tertentu. Profil risiko organisasi mungkin mengharuskan auditor internal untuk mempertimbangkan aspek-aspek tambahan dari topik tersebut.

Kesesuaian dengan Persyaratan Topik Spesifik akan meningkatkan konsistensi pelaksanaan jasa audit internal dan meningkatkan kualitas dan keandalan jasa dan hasil audit internal. Pada akhirnya, Persyaratan Topik Spesifik akan meningkatkan profesi audit internal.

Auditor internal harus menerapkan Persyaratan Topik Spesifik sesuai dengan Standar Audit Internal Global. Kesesuaian dengan Persyaratan Topik Spesifik adalah wajib untuk jasa asurans dan direkomendasikan untuk jasa advisori.

Persyaratan Topik Spesifik berlaku jika topiknya adalah salah satu dari:

A. Subjek penugasan dalam rencana audit internal.
B. Diidentifikasi saat pelaksanaan penugasan.
C. Subjek suatu permintaan penugasan tidak terdapat dalam rencana awal audit internal.

Bukti bahwa setiap persyaratan dalam Persyaratan Topik Spesifik telah dinilai penerapannya harus didokumentasikan dan disimpan. Tidak semua persyaratan individu dapat diterapkan dalam setiap penugasan; jika persyaratan dikecualikan, alasan pengecualian harus didokumentasikan dan disimpan. Kesesuaian dengan Persyaratan Topik Spesifik adalah wajib dan akan dievaluasi selama asesmen kualitas.

Untuk informasi lebih lanjut, lihat Panduan Pengguna Persyaratan Topik Spesifik Keamanan Siber.

Keamanan siber

National Institute of Standards and Technology (NIST) mendefinisikan keamanan siber secara sederhana sebagai, "Kemampuan untuk melindungi atau mempertahankan penggunaan ruang siber dari serangan siber." 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 untuk memberikan kerahasiaan, integritas, dan ketersediaan."

Keamanan siber mengurangi risiko dengan memperkuat lingkungan pengendalian secara menyeluruh dan melindungi aset informasi organisasi dari akses yang tidak sah, gangguan, perubahan, atau perusakan. Serangan siber dapat menyebabkan dampak langsung dan tidak langsung yang sering kali signifikan, karena komputer, jaringan, program, data, dan informasi sensitif merupakan komponen penting bagi sebagian besar organisasi.

Mengevaluasi dan Menilai Tata Kelola Keamanan Siber, Manajemen Risiko, dan Proses Pengendalian

Persyaratan Topik Spesifik ini memberikan pendekatan yang konsisten dan komprehensif untuk menilai desain dan implementasi tata kelola keamanan siber, manajemen risiko, dan proses pengendalian. Persyaratan ini mewakili batas acuan minimum untuk menilai keamanan siber dalam suatu organisasi.

TATA KELOLA: Mengevaluasi dan Menilai Tata Kelola Keamanan Siber

Persyaratan:

Auditor internal harus menilai hal-hal terkait dengan tata kelola keamanan siber organisasi sebagai berikut:

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 dan diperbarui secara berkala untuk memperkuat lingkungan kontrol.
C. Peran dan tanggung jawab yang mendukung tujuan keamanan siber ditetapkan, dan terdapat proses untuk menilai pengetahuan, keterampilan, dan kemampuan individu yang mengisi peran tersebut secara berkala.
D. Para 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, operasional, manajemen risiko, sumber daya manusia, hukum, kepatuhan, vendor, dan lainnya.

MANAJEMEN RISIKO: Mengevaluasi dan Menilai Manajemen Risiko Keamanan Siber

Persyaratan:

Auditor internal harus menilai hal-hal terkait dengan manajemen risiko keamanan siber organisasi sebagai berikut:

A. Penilaian risiko organisasi dan proses manajemen risiko termasuk mengidentifikasi, menganalisis, memitigasi, dan memantau 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 pasok, akuntansi, keuangan, dan lain-lain.

C. Akuntabilitas dan tanggung jawab manajemen risiko untuk keamanan siber ditetapkan. Seseorang atau tim ditetapkan 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 dengan cepat mengeskalasi adanya risiko keamanan siber (yang baru muncul atau 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 nonfinansial dari risiko keamanan siber harus dipertimbangkan.

E. Sebuah proses dibuat untuk mengkomunikasikan kesadaran akan risiko keamanan siber kepada manajemen dan karyawan dan bagi manajemen untuk meninjau masalah, kesenjangan, kekurangan, atau kegagalan kontrol secara berkala dengan pelaporan dan perbaikan tepat waktu.

F. Organisasi telah menerapkan proses respons dan pemulihan insiden keamanan siber yang mencakup deteksi, penahanan, pemulihan, dan analisis pasca insiden. Proses respons dan pemulihan insiden diuji secara berkala.

PENGENDALIAN: Mengevaluasi dan Menilai Proses Kontrol Keamanan Siber

Persyaratan:

Auditor internal harus menilai hal-hal terkait dengan proses pengendalian keamanan siber organisasi sebagai berikut:

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 secara 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 serta 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.

E. Proses dibuat untuk memperkuat 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 network* (VPN)/*zero trust network access* (ZTNA); pengendalian jaringan *Internet of Things* (IoT); dan sistem deteksi/pencegahan penyusupan (IDS dan IPS).

G. Kontrol keamanan komunikasi *end-point* dibuat untuk layanan seperti surat elektronik, peramban internet, konferensi video, layanan pesan, 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, IIA diakui di seluruh dunia sebagai pemimpin profesi audit internal dalam hal standar, sertifikasi, pendidikan, penelitian, dan bimbingan teknis. Untuk informasi lebih lanjut, kunjungi www.theiia.org.

Hak Cipta

Februari 2025

Kantor Pusat Global
1035 Greenwood Blvd, Suite 401
Lake Mary, FL 32746, USA
Telepon: +1-407-937-1111
Faksimili: +1-407-937-1101