Pihak Ketiga

Persyaratan Topik Spesifik

Topical Requirement

The Institute of
Internal Auditors

Persyaratan Topik Spesifik Pihak Ketiga

The International Professional Practices Framework® terdiri dari Standar Audit Internal Global™ (Global Internal Audit Standards™), Persyaratan Topik Spesifik, dan Panduan Global. Persyaratan Topik Spesifik 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 dasar acuan minimum untuk mengaudit area 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 dapat diterapkan jika topiknya adalah salah satu dari:

1. Subjek penugasan dalam rencana audit internal.
2. Diidentifikasi saat pelaksanaan penugasan.
3. Subjek dari penugasan yang diminta tidak ada 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 penilaian kualitas.

Pihak Ketiga

Pihak ketiga adalah individu, kelompok, atau entitas eksternal yang menjalin hubungan bisnis dengan sebuah organisasi ("organisasi utama") untuk mendapatkan produk atau layanan. Hubungan tersebut dapat diformalkan melalui kontrak, perjanjian, atau cara lain. Persyaratan Topik Spesifik ini menggunakan istilah "pihak ketiga" untuk merujuk pada vendor, pemasok, kontraktor, subkontraktor, penyedia layanan alih daya, lembaga lain, dan konsultan. Istilah ini mencakup perjanjian antara pihak ketiga dan subkontraktornya, yang sering dikenal sebagai subkontraktor "hilir".

Persyaratan Topik Spesifik berlaku ketika fungsi audit internal melaksanakan penugasan asurans terhadap pihak ketiga dan/atau hubungan subkontrak lainnya, termasuk hubungan keempat dan seterusnya ke hilir, yang diizinkan oleh kontrak atau perjanjian pihak ketiga dengan organisasi utama. Auditor internal harus memprioritaskan pihak ketiga dan pihak hilir berdasarkan risiko, seperti yang dijelaskan dalam bagian manajemen risiko di bawah ini. Auditor internal harus menerapkan semua persyaratan sebagaimana diindikasikan oleh hasil penilaian risiko, dan pengecualian harus didokumentasikan.

Persyaratan Topik Spesifik ini tidak dimaksudkan untuk membahas hubungan eksternal tidak langsung, kepentingan, atau keterlibatan dengan organisasi utama, seperti regulator, agen, wali amanat/anggota dewan, atau hubungan internal, seperti karyawan.

Istilah "pihak ketiga" dapat didefinisikan dan digunakan secara berbeda berdasarkan industri atau konteks lainnya. Auditor internal diberikan fleksibilitas dan harus mengandalkan pertimbangan profesional mereka untuk menyesuaikan Persyaratan Topik Spesifik dengan definisi organisasi utama tentang pihak ketiga.

Organisasi utama (organisasi yang mengadakan perjanjian dengan pihak ketiga) tetap bertanggung jawab atas risiko yang terkait dengan pencapaian tujuannya, bahkan ketika organisasi tersebut melibatkan pihak ketiga untuk membantunya mencapai satu atau beberapa tujuan. Bekerja dengan pihak ketiga menimbulkan risiko yang harus diidentifikasi, dinilai, dan dikelola melalui tata kelola, manajemen risiko, dan proses pengendalian yang tepat, sebagaimana diuraikan dalam Persyaratan Topik Spesifik ini. Jika pihak ketiga gagal melaksanakan tugas sesuai kontrak, berpartisipasi dalam praktik yang tidak etis, atau mengalami gangguan bisnis, organisasi utama dapat mengalami dampaknya. Kategori dan contoh risiko yang terkait dengan pihak ketiga meliputi:

- Strategis, seperti kemampuan untuk mencapai misi utama organisasi dan/atau tujuan tingkat tinggi atau untuk mengelola dampak merger dan akuisisi.
- Reputasi, seperti kerusakan yang disebabkan oleh lingkungan atau hubungan dan kepercayaan organisasi utama dengan klien, pelanggan, dan pemangku kepentingan.
- Etis, seperti kegagalan integritas, konflik kepentingan, suap, dan korupsi.
- Operasional, seperti keamanan fisik dan informasi, risiko orang dalam, gangguan layanan, dan tidak tercapainya tujuan.
- Finansial, seperti kebangkrutan pihak ketiga dan penipuan.
- Kepatuhan terhadap persyaratan peraturan lokal, nasional, dan internasional yang berlaku.
- Keamanan siber dan perlindungan data lainnya, seperti kompromi dan kebocoran data sensitif.
- Teknologi informasi, seperti kurangnya layanan untuk mendukung operasi penting.
- Hukum, seperti konflik kepentingan, perselisihan, dan litigasi untuk pelanggaran kontrak.
- Keberlanjutan, seperti lingkungan, sosial, dan tata kelola. Contohnya adalah risiko yang berkaitan dengan dampak organisasi terhadap lingkungan alam dan risiko yang berkaitan dengan interaksi organisasi dengan masyarakat.
- Geopolitik, seperti sengketa/sanksi perdagangan dan ketidakstabilan politik.

Daur hidup pihak ketiga terdiri atas pemilihan, proses kontrak, orientasi, pemantauan, dan *offboarding*. Auditor internal harus mempertimbangkan tahapan-tahapan ini ketika menilai persyaratan tata kelola, manajemen risiko, dan proses pengendalian.

Mengevaluasi dan Menilai Tata Kelola, Manajemen Risiko, dan Proses Pengendalian Pihak Ketiga

Persyaratan Topik Spesifik ini memberikan pendekatan yang konsisten dan komprehensif untuk menilai desain dan implementasi tata kelola, manajemen risiko, dan proses pengendalian pihak ketiga. Persyaratan tersebut mewakili dasar acuan minimum dalam penilaian.

TATA KELOLA

Persyaratan:

Auditor internal harus menilai aspek-aspek berikut dari tata kelola organisasi utama terhadap pihak ketiga, termasuk pengawasan dewan:

A. Pendekatan formal dibuat, diterapkan, dan ditinjau secara berkala untuk menentukan apakah akan melakukan kontrak dengan pihak ketiga. Pendekatan ini mencakup kriteria yang tepat untuk menentukan dan menilai sumber daya yang diperlukan dan tersedia untuk memenuhi tujuan dengan menyediakan produk atau layanan.

B. Kebijakan dan prosedur dibuat untuk mendefinisikan, menilai, dan mengelola hubungan dan risiko dengan pihak ketiga di seluruh daur hidup pihak ketiga. Kebijakan dan prosedur diselaraskan dengan persyaratan peraturan yang berlaku dan secara berkala ditinjau dan diperbarui untuk memperkuat lingkungan pengendalian.

C. Peran dan tanggung jawab manajemen pihak ketiga organisasi didefinisikan, dengan merinci siapa yang memilih, mengarahkan, mengelola, berkomunikasi, dan memantau pihak ketiga serta siapa yang harus diinformasikan tentang aktivitas pihak ketiga. Terdapat proses untuk memastikan individu yang memberikan peran dan tanggung jawab bagi pihak ketiga memiliki kompetensi yang memadai.

D. Protokol untuk berkomunikasi dengan para pemangku kepentingan yang relevan telah ditetapkan dan mencakup pelaporan yang tepat waktu mengenai status kinerja, risiko, dan kepatuhan (khususnya pelanggaran hukum dan peraturan) dari pihak ketiga yang diprioritaskan. Pihak ketiga diprioritaskan berdasarkan risiko. Pemangku kepentingan yang relevan dapat mencakup dewan, manajemen senior, pengadaan, operasional, manajemen risiko, kepatuhan, hukum, teknologi informasi, keamanan informasi, sumber daya manusia, dan lain-lain.

MANAJEMEN RISIKO

Persyaratan:

Auditor internal harus menilai aspek-aspek berikut dari manajemen risiko pihak ketiga organisasi.

A. Proses untuk manajemen risiko pihak ketiga dan layanan mereka terstandar dan komprehensif, termasuk peran dan tanggung jawab yang jelas, dan cukup menangani risiko utama yang relevan bagi organisasi (seperti risiko strategis, reputasi, etika, operasional, keuangan, kepatuhan, keamanan siber, teknologi informasi, hukum, keberlanjutan, dan geopolitik). Kepatuhan terhadap proses dipantau, dan tindakan korektif diterapkan untuk setiap penyimpangan.

B. Risiko yang terkait dengan pihak ketiga di seluruh daur hidup diidentifikasi dan dinilai secara teratur. Penilaian risiko digunakan untuk menentukan peringkat dan memprioritaskan pihak

ketiga, termasuk pihak-pihak yang berada jauh di hilir. Tanggapan terhadap risiko juga diberi peringkat dan diprioritaskan. Penilaian risiko ditinjau dan diperbarui secara berkala.

C. Tanggapan risiko memadai dan akurat, sesuai dengan peringkat. Tanggapan terhadap risiko diimplementasikan, ditinjau, disetujui, dipantau, dievaluasi, dan disesuaikan sesuai kebutuhan.

D. Proses-proses yang ada untuk mengelola dan mengeskalasi, jika diperlukan, masalah-masalah yang muncul dari pihak ketiga, memastikan akuntabilitas hasil dan meningkatkan kemungkinan tercapainya persyaratan kontrak atau perjanjian lainnya. Jika pihak ketiga gagal merespons kekhawatiran yang telah dieskalasi, maka terdapat proses bagi manajemen untuk mengevaluasi risiko hubungan bisnis yang sedang berlangsung dan mengambil tindakan lebih lanjut, perbaikan, atau pemutusan hubungan kerja, sebagaimana telah dijamin.

PENGENDALIAN

Persyaratan:

Auditor internal harus menilai pengendalian berikut ini untuk pihak ketiga yang diprioritaskan berdasarkan risiko. Evaluasi harus mencakup proses manajemen untuk penilaian dan pemantauan yang sedang berlangsung terhadap pihak ketiga organisasi.

A. Proses *due diligence* yang menyeluruh untuk mencari dan memilih pihak ketiga tersedia dengan kasus bisnis yang didokumentasikan dan disetujui atau dokumen terkait lainnya yang menjelaskan dan membenarkan kebutuhan dan sifat hubungan dengan pihak ketiga.

B. Kontrak dan persetujuan dilakukan sesuai dengan kebijakan dan prosedur manajemen risiko pihak ketiga organisasi dan mencakup kolaborasi di antara bagian-bagian organisasi yang sesuai.

C. Kontrak atau perjanjian akhir ditinjau dan disetujui oleh semua pemangku kepentingan terkait, termasuk bagian hukum dan kepatuhan, ditandatangani oleh orang yang berwenang dari kedua belah pihak, dan disimpan dengan aman. Seorang manajer kontrak atau administrator ditugaskan bertanggung jawab untuk setiap kontrak.

D. Daftar semua hubungan dengan pihak ketiga yang akurat, lengkap, dan terkini ditata, seperti dalam sistem manajemen kontrak terpusat.

E. Proses orientasi yang terdokumentasi dibuat dan diikuti sebagai dasar bagi pihak ketiga untuk memenuhi persyaratan kontrak atau perjanjian.

F. Proses pemantauan yang sedang berlangsung dilakukan untuk menilai apakah pihak ketiga berkinerja sesuai dengan ketentuan kontrak atau perjanjian selama daur hidup dan apakah pihak ketiga memenuhi kewajiban kontraktual mereka. Proses ini mencakup verifikasi keandalan informasi yang diberikan dan evaluasi ulang kinerja secara berkala dan setiap kali perjanjian berubah.

G. Protokol dibuat untuk memulai tindakan korektif jika pihak ketiga gagal memenuhi harapan atau menimbulkan risiko yang meningkat atau tidak terduga. Protokol ini mencakup eskalasi insiden berdasarkan tingkat keparahan, melakukan tinjauan pasca insiden, dan menganalisis akar penyebab insiden.

H. Tanggal berakhirnya kontrak dan perpanjangan kontrak dipantau, dan tindakan perpanjangan dilakukan sesuai kebutuhan.

I. Rencana *offboarding* yang telah diformalkan diimplementasikan dan diikuti untuk memastikan persyaratan kontrak yang melibatkan waktu dan ekspektasi ditangani secara memadai. Proses meliputi tata cara:

- Penghentian pihak ketiga.
- Penggantian pihak ketiga jika diperlukan.
- Pengaturan ulang *custody* dan mengembalikan atau memusnahkan data sensitif organisasi yang disimpan pada pihak ketiga.
- Mencabut akses pihak ketiga ke sistem, alat, dan fasilitas.

Tentang Institut Auditor Internal

IIA adalah asosiasi profesional internasional yang melayani lebih dari 265.000 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 standar, sertifikasi, pendidikan, penelitian, dan bimbingan teknis. Untuk informasi lebih lanjut, kunjungi theiia.org.

Hak Cipta

September 2025

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

