Pihak Ketiga

Persyaratan Topik Spesifik

Topical Requirement

Panduan Pengguna

The Institute of
Internal Auditors

Daftar Isi

Overview of Topical Requirements....2

Applicability, Risk, and Professional Judgment 2

Considerations....7

Governance Considerations 7

Risk Management Considerations 8

Control Process Considerations 10

Appendix A. Practical Application Examples....16

Appendix B. Optional Documentation Tool....18

Third-Party Governance 18

Third-Party Risk Management 19

Third Party Controls 20

Gambaran Umum Persyaratan Topik Spesifik

Persyaratan Topik Spesifik adalah komponen penting dari International Professional Practices Framework®, bersama dengan Standar Audit Internal Global™ (Global Internal Audit Standards™) dan Panduan Global. The Institute of Internal Auditor mengharuskan Persyaratan Topik Spesifik untuk digunakan bersama dengan Standar, 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 merupakan dasar 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 saat 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 bertanggung jawab atas tata kelola, manajemen risiko berhubungan dengan lini kedua, dan pengendalian atau proses pengendalian berhubungan dengan lini pertama. Sementara manajemen diwakili di lini pertama dan kedua, fungsi audit internal digambarkan di lini ketiga sebagai penyedia asurans yang independen dan obyektif, yang melapor kepada dewan/ badan yang bertanggung jawab 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, menilai risiko merupakan bagian penting dari perencanaan yang dilakukan oleh 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 individual, auditor internal harus menilai risiko yang relevan dengan penugasan tersebut (Standar 13.2 Asesmen Risiko Penugasan).

Ketika subjek dari Persyaratan Topik Spesifik diidentifikasi selama proses perencanaan audit internal berbasis risiko dan dimasukkan dalam rencana audit, maka persyaratan yang diuraikan dalam Persyaratan Topik Spesifik harus digunakan untuk menilai topik tersebut dalam penugasan yang berlaku. Selain itu, ketika auditor internal melakukan penugasan (baik yang termasuk atau tidak termasuk dalam rencana) dan terdapat elemen dari Persyaratan Topik Spesifik yang muncul, maka Persyaratan Topik Spesifik tersebut harus dinilai relevansinya sebagai bagian dari penugasan. Terakhir, jika ada permintaan penugasan yang awalnya tidak ada dalam rencana dan penugasan itu mencakup dalam topik tersebut, maka Persyaratan Topik Spesifik harus dinilai untuk diterapkan.

Penilaian profesional memainkan peran kunci dalam penerapan Persyaratan Topik Spesifik. Asesmen risiko mendorong keputusan chief audit executive mengenai penugasan mana yang akan dimasukkan ke dalam rencana audit internal (Standar 9.4). 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).

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

Meskipun Persyaratan Topik Spesifik memberikan dasar acuan proses pengendalian untuk dipertimbangkan, organisasi yang mengevaluasi topik tersebut dengan risiko yang sangat tinggi mungkin perlu menilai aspek-aspek tambahan.

Jika fungsi audit internal tidak memiliki kompetensi yang diperlukan untuk melakukan penugasan atas suatu subjek Persyaratan Topik Spesifik, chief audit executive harus menentukan cara memperoleh sumber daya dan mengkomunikasikan secara tepat waktu kepada dewan dan manajemen senior mengenai dampak dari keterbatasan tersebut dan bagaimana kekurangan sumber daya tersebut akan diatasi. Chief audit executive memiliki tanggung jawab utama untuk memastikan kesesuaian fungsi audit internal dengan Persyaratan Topik Spesifik, terlepas dari bagaimana sumber daya diperoleh (Standar 3.1 Kompetensi, 7.2 Kualifikasi Chief Audit Executive, 8.2 Sumber Daya, 10.2 Pengelolaan Sumber Daya Manusia).

Kinerja, Dokumentasi, dan Pelaporan

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

Persyaratan Topik Spesifik dirancang untuk mendukung praktik audit internal yang konsisten dan berkualitas tinggi. Peraturan perundangan, regulasi, ekspektasi pengawasan, dan kerangka kerja lain yang diakui secara profesional dapat menjadi dasar persyaratan tambahan atau lebih spesifik. Auditor internal harus memahami dan mematuhi hukum dan/atau peraturan yang relevan dengan industri dan yurisdiksi tempat organisasi beroperasi, termasuk membuat pengungkapan yang diperlukan, sesuai dengan Standar 1.3 Perilaku Taat Hukum dan Etis. Auditor internal mungkin telah mengintegrasikan persyaratan

tambahan ini ke dalam program audit dan prosedur pengujian dan harus mencocokkannya dengan Persyaratan Topik Spesifik untuk memastikan cakupan yang memadai.

Cakupan Persyaratan Topik Spesifik dapat didokumentasikan dalam rencana audit internal atau kertas kerja penugasan berdasarkan pertimbangan profesional auditor. Satu atau beberapa penugasan audit internal dapat memenuhi 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 suatu pengecualian.

Asurans 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. Laporan komunikasi harus mencakup kesesuaian fungsi audit internal dengan Standar dan pencapaian tujuan kinerja.

Kesesuaian dengan Persyaratan Topik Spesifik akan dievaluasi dalam penilaian kualitas.

Pihak Ketiga

Pihak ketiga adalah individu, kelompok, atau entitas eksternal yang memiliki hubungan bisnis dengan sebuah organisasi ("organisasi utama") untuk mendapatkan produk atau jasa. Hubungan tersebut dapat diformalkan melalui kontrak, perjanjian, atau cara lain untuk menyediakan produk, jasa, tenaga kerja, manufaktur, atau solusi teknologi informasi kepada organisasi, seperti penyimpanan, pemrosesan, dan pemeliharaan data.

> Catatan
>
> Persyaratan Topik Spesifik menggunakan terminologi audit internal umum sebagaimana didefinisikan dalam Standar Audit Internal Global. Pembaca harus mengacu pada istilah dan definisi dalam daftar istilah Standar.

Istilah "pihak ketiga" dapat digunakan secara berbeda berdasarkan industri atau konteks lainnya. Setiap fungsi audit internal memiliki fleksibilitas untuk menggunakan penilaiannya dalam penerapan Persyaratan Topik Spesifik sesuai dengan bagaimana organisasi utama (organisasi yang mengadakan perjanjian dengan pihak ketiga) mendefinisikan pihak ketiga. Dalam Persyaratan Topik Spesifik Pihak Ketiga dan panduan pengguna, istilah "pihak ketiga" mengacu pada vendor, pemasok, kontraktor, subkontraktor, penyedia jasa alih daya, lembaga lain, dan konsultan. Istilah "pihak ketiga" mencakup semua pengaturan tersebut, termasuk pengaturan antara pihak ketiga dan sub kontraktornya, yang sering dikenal sebagai subkontraktor "hilir", atau "pihak keempat", "pihak kelima", atau "pihak ke-N"

Persyaratan Topik Spesifik ini tidak dimaksudkan untuk membahas hubungan eksternal tidak langsung, kepentingan, atau keterlibatan dengan organisasi utama, seperti regulator, agen, pialang, investor, pengawas/anggota dewan, jasa publik, dan anggota masyarakat umum, atau hubungan internal, seperti karyawan atau penyedia jasa dalam grup.

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.

Efektivitas proses organisasi dalam mengelola hubungan dengan pihak ketiga dapat dinilai di seluruh organisasi dan/atau pada tingkat satu atau beberapa kontrak, perjanjian, atau hubungan individu. Auditor internal harus menggunakan pendekatan dari atas ke bawah (top-down) untuk mengembangkan pemahaman atas kebijakan, prosedur, proses, kerangka kerja, dan daur hidup pihak ketiga organisasi. Auditor internal harus menggunakan pertimbangan untuk memahami nuansa dalam risiko pihak ketiga berdasarkan industri, organisasi, dan topik penugasan. Sejalan dengan Standar 5.1 Penggunaan Informasi, auditor internal harus mengetahui dan mematuhi kebijakan dan prosedur yang terkait dengan informasi pihak ketiga yang dapat mereka akses.

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

Persyaratan Topik Spesifik Pihak Ketiga dan panduan pengguna mengacu pada tahapan dalam hubungan organisasi dengan pihak ketiganya, yang juga dikenal sebagai tahapan siklus hidup: seleksi, proses kontrak, onboarding, pemantauan, dan *offboarding*. Tahapan-tahapan ini akan digunakan untuk keperluan Persyaratan Topik Spesifik Pihak Ketiga dan panduan pengguna, meskipun beberapa industri memiliki versi daur hidup mereka sendiri. Tahapan-tahapannya adalah:

- Seleksi: mencakup proses untuk menentukan kebutuhan akan pihak ketiga, rencana penggunaannya, dan *due diligence* dalam seleksi. Selain itu, seleksi harus mencakup asesmen risiko pihak ketiga yang potensial dan terlibat.
- Proses Kontrak: mencakup proses *due diligence* untuk merancang, menegosiasikan, menyetujui, dan melaksanakan perjanjian hukum dengan pihak ketiga.
- *Onboarding*: dimulai saat kontrak ditandatangani untuk memulai hubungan dan menetapkan landasan bagi pihak ketiga untuk memenuhi ketentuan kontrak atau perjanjian.
- Pemantauan: mencakup proses pengelolaan selama masa berlaku kontrak "*in-life management*" dan pemantauan berkelanjutan terhadap pihak ketiga setelah kontrak dibuat dan disetujui. Pendekatan ini biasanya sistematis dan berbasis risiko serta harus mempertimbangkan perbaikan berkelanjutan. Pemantauan termasuk memperbarui kontrak atau perjanjian pihak ketiga yang sedang berlangsung bila diperlukan.
- *Offboarding*: mencakup proses untuk mengakhiri kontrak dan perjanjian, mempertahankan *exit strategy* untuk pihak ketiga yang telah diprioritaskan berdasarkan risiko, dan mengakhiri hubungan jika diperlukan. Proses ini biasanya menggunakan pendekatan berbasis risiko dan mungkin melibatkan *exit plan* yang formal.

Organisasi utama 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 sama dengan pihak ketiga dapat mengurangi sebagian biaya organisasi dalam melakukan proses. Namun, hal ini dapat menimbulkan risiko operasional karena organisasi utama memiliki keterbatasan visibilitas dan wewenang atas proses pengendalian pihak ketiga. Jika pihak ketiga gagal

melaksanakan tugas sesuai kontrak, berpartisipasi dalam praktik yang tidak etis, atau mengalami gangguan bisnis, maka organisasi utama dapat menanggung dampaknya.

Organisasi utama harus mengidentifikasi, menilai, dan mengelola risiko melalui tata kelola, manajemen risiko, dan proses pengendalian yang tepat. Kategori dan contoh risiko yang terkait dengan pihak ketiga meliputi:

- Strategis, seperti kemampuan untuk mencapai misi 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.
- Etika, seperti kegagalan integritas, konflik kepentingan, suap, dan korupsi.
- Operasional, seperti keamanan fisik dan informasi, risiko orang dalam, gangguan jasa, 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 jasa 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.

Auditor internal harus mempertimbangkan setiap tahap dari daur hidup pihak ketiga ketika menilai persyaratan tata kelola, manajemen risiko, dan proses pengendalian.

Persyaratan dalam Persyaratan Topik Spesifik Pihak Ketiga dibagi menjadi tiga bagian sesuai dengan Standar 9.1 Memahami Proses Tata Kelola, Manajemen Risiko, dan Pengendalian:

- Tata Kelola - tujuan dan strategi dasar yang jelas untuk menggunakan pihak ketiga dalam mendukung tujuan, kebijakan, dan prosedur organisasi.
- Manajemen risiko - proses untuk mengidentifikasi, menganalisis, mengelola, dan memantau risiko penggunaan pihak ketiga, termasuk proses untuk mengeskalasi insiden dengan segera.
- Pengendalian - proses pengendalian yang ditetapkan oleh manajemen dan dievaluasi secara berkala untuk memitigasi risiko ketika menggunakan pihak ketiga.

Selain Persyaratan Topik Spesifik dan panduan pengguna ini, auditor internal mungkin dapat merujuk pada panduan profesional tambahan dari pihak ketiga, seperti Panduan Global IPPF dan sumber daya khusus industri.

Pertimbangan

Pertimbangan berikut ini dapat membantu auditor internal dalam menerapkan persyaratan dalam Persyaratan Topik Spesifik Pihak Ketiga. Pernyataan berhuruf di setiap bagian di bawah ini menyatakan kembali atau memparafrasa persyaratan yang sesuai dari Persyaratan Topik Spesifik. Pertimbangan yang tidak wajib ini bersifat ilustratif untuk memberikan contoh cara menilai persyaratan. Auditor internal harus menerapkan pertimbangan profesional ketika menentukan apa yang harus dimasukkan dalam penilaian mereka.

Pertimbangan Tata Kelola

Untuk menilai bagaimana proses tata kelola, termasuk pengawasan dewan, diterapkan pada tujuan pihak ketiga, auditor internal dapat meninjau bukti-bukti:

A. Pendekatan atau strategi berbasis risiko yang diformalkan dan didokumentasikan untuk menentukan apakah akan menggunakan pihak ketiga. Pendekatan ini ditinjau secara berkala dan mencakup:

- Proses yang didefinisikan dengan jelas dan terstandar untuk mengimplementasikan pendekatan tersebut, yang disetujui untuk digunakan oleh organisasi.
- Menganggarkan sumber daya berdasarkan analisis biaya-manfaat untuk menjustifikasi penugasan pihak ketiga, memastikan keselarasan strategis dan efisiensi sumber daya.
- Evaluasi manajemen atas risiko dan pengendalian, termasuk yang berhubungan dengan pihak ketiga.
- Sumber daya yang memadai untuk mengontrak, mengelola, dan memantau kinerja pihak ketiga.
- Integrasi umpan balik pemangku kepentingan ke dalam pendekatan atau strategi.

B. Kebijakan, prosedur, dan dokumentasi terkait lainnya yang digunakan untuk mendefinisikan, menilai, dan mengelola hubungan dengan pihak ketiga di sepanjang daur hidup. Kebijakan dan prosedur dapat mencakup:

- Alat bantu dan templat terstandar untuk memfasilitasi tata kelola, manajemen risiko, dan proses pengendalian utama.
- Proses untuk mengevaluasi kebijakan dan prosedur secara berkala, menentukan kecukupannya, dan memperbaruinya jika diperlukan.
- Menetapkan kriteria untuk memilih, mengontrak, mengikutsertakan, memantau, dan memberhentikan pihak ketiga.
- Identifikasi dan tinjauan berkala terhadap persyaratan peraturan yang berlaku untuk menyelaraskan dengan kebijakan dan prosedur.

- Pelaksanaan *benchmarking* dilakukan untuk mengidentifikasi dan membandingkan praktik-praktik manajemen pihak ketiga yang terkemuka.

C. Peran dan tanggung jawab yang ditetapkan yang mendukung pencapaian tujuan pihak ketiga. Bukti lebih lanjut dapat mencakup:

- Proses untuk mengevaluasi apakah nilai, etika, dan tanggung jawab sosial perusahaan pihak ketiga selaras dengan prinsip-prinsip organisasi utama. Proses tersebut harus mencakup cara mengatasi potensi konflik kepentingan atau praktik-praktik yang tidak etis dengan segera.
- Pelatihan rutin bagi personil yang mengisi peran manajemen pihak ketiga dan penilaian berkala atas kompetensi mereka.
- Sebuah proses untuk mengevaluasi apakah pelatihan telah dilaksanakan untuk menciptakan kesadaran di seluruh organisasi tentang pihak ketiga.
- Peran dan tanggung jawab diselaraskan dengan Model Tiga Lini.

D. Komunikasi dan penugasan yang tepat waktu dengan para pemangku kepentingan yang relevan di seluruh siklus hidup pihak ketiga (misalnya, dewan, manajemen senior, pengadaan, operasi, manajemen risiko, kepatuhan, hukum, teknologi informasi, keamanan informasi, sumber daya manusia, dan lain-lain), yang meliputi:

- Informasi tentang risiko pihak ketiga dan potensi kerentanan yang diketahui dalam notulen rapat, laporan, atau email.
- Pertukaran informasi tentang manajemen pihak ketiga dan promosi kolaborasi (misalnya, melalui pertemuan lintas fungsi secara berkala).

Pertimbangan Manajemen Risiko

Untuk menilai bagaimana proses manajemen risiko diterapkan pada tujuan pihak ketiga, auditor internal dapat meninjau bukti-bukti bahwa:

A. Proses manajemen risiko yang terstandar dan komprehensif untuk pengguna jasa pihak ketiga mencakup peran dan tanggung jawab yang jelas dan secara memadai menangani risiko-risiko utama yang relevan bagi organisasi:

- Proses untuk menilai dan mengelola risiko pihak ketiga termasuk bagaimana risiko utama:
  - Identifikasi dan pelaporan awal.
  - Dianalisis untuk mengevaluasi dampak terhadap kemampuan mencapai tujuan organisasi.
  - Mitigasi, termasuk rencana perbaikan untuk mengurangi risiko ke tingkat yang dapat diterima.
  - Pemantauan, termasuk deteksi dan respons terhadap peringatan dini dan rencana pelaporan berkelanjutan hingga ancaman benar-benar teratasi.
- Pemantauan dilakukan untuk memastikan kepatuhan terhadap proses dan pelaksanaan tindakan korektif untuk setiap penyimpangan, untuk mencegah terjadinya penyimpangan terhadap tujuan atau strategi jangka panjang organisasi.

- Komite manajemen risiko atau kelompok lain memberikan pengawasan langsung terhadap pihak ketiga dan masukan kepada dewan. Komite ini memiliki tujuan yang jelas dan mengadakan pertemuan secara teratur. Bukti dapat berupa notulen rapat.

B. Risiko yang terkait dengan pihak ketiga di seluruh siklus hidup diidentifikasi dan dinilai secara teratur. Asesmen risiko memberi peringkat dan memprioritaskan pihak ketiga. Tanggapan terhadap risiko diurutkan dan diprioritaskan.

- Organisasi utama mempertimbangkan faktor-faktor seperti ukuran, kematangan, dan jumlah pihak ketiga yang terlibat ketika mengembangkan asesmen risiko pihak ketiga.
- Asesmen risiko didokumentasikan dan mengidentifikasi risiko inheren dan risiko residual.
- Organisasi mengikuti proses *due diligence* untuk meninjau dan memperbarui asesmen risiko.
- Kriteria dibuat untuk menentukan peringkat dan memprioritaskan pihak ketiga berdasarkan risiko. Contoh kriteria tersebut meliputi:
  - Jasa yang diberikan sangat penting bagi operasi organisasi.
  - Nilai finansial dari pengaturan tersebut adalah material.
  - Hubungannya baru, terjalin dengan cepat, dan/atau durasinya lama.
  - Beberapa pihak eksternal terlibat.
  - Pihak ketiga berencana untuk mensubkontrakkan sebagian atau seluruh pekerjaan.
- Organisasi mematuhi praktik asesmen risiko yang diterima secara luas, termasuk bahwa asesmen risiko dilakukan sedini mungkin, biasanya ketika proposal dianalisis selama tahap seleksi, dan sebelum onboarding.
- Vendor mengisi kuesioner untuk menentukan peringkat dan prioritas risiko mereka berdasarkan risiko yang melekat. Organisasi memastikan bahwa kuesioner diisi oleh personil yang relevan dan ditinjau untuk memastikan keakuratannya.
- Organisasi memperoleh masukan secara berkala mengenai manajemen risiko pihak ketiga dari bidang-bidang fungsional, seperti teknologi informasi, pengadaan, manajemen risiko perusahaan, sumber daya manusia, hukum, kepatuhan, operasional, akuntansi dan keuangan.

C. Tanggapan terhadap risiko, seperti mitigasi, penerimaan, eliminasi, dan berbagi, diidentifikasi dan disesuaikan dengan peringkat risiko.

- Tanggapan terhadap risiko didokumentasikan dan mencakup pertimbangan lingkungan pengendalian pihak ketiga.
- Dokumentasi bahwa tanggapan terhadap risiko yang melebihi toleransi risiko organisasi utama ditinjau kesesuaiannya, terutama ketika risiko tersebut diterima. Tanggapan-tanggapan tersebut termasuk yang membahas potensi konflik kepentingan dengan pihak ketiga.

D. Proses untuk mengelola dan meningkatkan risiko pihak ketiga, termasuk bagaimana tingkat ancaman atau risiko dievaluasi, ditetapkan, dan diprioritaskan. Reviu dapat termasuk melakukan identifikasi:

- Definisi dan penjelasan tingkat risiko organisasi - seperti tinggi, sedang, dan rendah - dan prosedur eskalasi untuk setiap kategori risiko.
- Daftar pihak ketiga yang diprioritaskan berdasarkan risiko yang teridentifikasi dan status mitigasi dari setiap kejadian risiko.
- Persyaratan hukum, peraturan, dan kepatuhan yang berlaku.
- Dampak risiko, baik finansial maupun non-finansial (misalnya, reputasi).
- Proses untuk mengomunikasikan risiko pihak ketiga kepada manajemen dan karyawan, termasuk pelaporan profil risiko secara berkala kepada dewan (atau badan lain yang sesuai). Komunikasi harus mencakup pembaruan tentang perbaikan masalah apa pun yang dicatat dengan pihak ketiga yang diprioritaskan.
- Proses untuk menilai kembali peringkat dan prioritas ketika selera risiko dan tingkat toleransi risiko organisasi utama berubah.

Pertimbangan Pengendalian

Untuk menilai bagaimana proses pengendalian diterapkan pada hubungan dengan pihak ketiga, auditor internal dapat meninjau bukti-bukti bahwa:

A. Proses *due diligence* yang kuat untuk mencari dan memilih pihak ketiga tersedia dengan kasus bisnis yang didokumentasikan dan disetujui atau dokumentasi terkait lainnya yang menjelaskan dan membenarkan kebutuhan dan sifat hubungan dengan pihak ketiga.
   - Kasus bisnis juga dapat:
     - Mengatasi risiko terhadap kemampuan pihak ketiga untuk memenuhi harapan dan potensi dampaknya terhadap organisasi.
     - Meliputi analisis biaya-manfaat yang terperinci.
   - Proses pengadaan yang telah ditetapkan - seperti penawaran kompetitif, permintaan proposal, dan pengadaan tunggal - diikuti. Proses tersebut meliputi:
     - Kriteria untuk aspek-aspek penting, seperti meninjau protokol keamanan siber, verifikasi detail bank, melakukan pemeriksaan latar belakang keuangan, dan meneliti struktur organisasi pihak ketiga, catatan kriminal dan hukum, catatan mengemudi, kegiatan politik, dan hubungan dengan kegiatan kriminal.
     - Kriteria seleksi yang terdefinisi dengan baik termasuk untuk menilai kinerja masa lalu, referensi, reputasi, dan biaya kontrak.
     - *Due diligence* untuk memastikan seleksi vendor yang tepat, seperti membentuk tim lintas fungsi untuk meninjau proposal. Untuk memitigasi risiko bias, pengendalian untuk tim reviu mencakup prosedur untuk pembentukan tim dan persyaratan untuk pengungkapan potensi konflik kepentingan.
     - *Due diligence* dalam menilai lingkungan pengendalian pihak ketiga; misalnya, melakukan kunjungan lapangan atau meninjau lingkungan pengendalian pihak ketiga:
       - Laporan Pengendalian Sistem dan Organisasi (SOC).
       - Stabilitas keuangan.

- Anggaran dasar atau sertifikat reputasi yang baik.
- Transparansi dalam pengambilan keputusan oleh manajemen dan pemangku kepentingan.
- Struktur organisasi.
- Stabilitas operasional.
- Protokol keamanan siber.
- Kepatuhan terhadap hukum, peraturan, dan standar yang relevan.
- Etis.
- Riwayat dengan organisasi utama.
- Reputasi.

  - Bukti bahwa vendor atau kontraktor potensial hanya maju ke tahap kontrak dalam daur hidup setelah proses *due diligence* yang relevan dilakukan dan hasilnya telah dianalisis.

B. Kebijakan dan prosedur kontrak ditetapkan dan diikuti.

- Kontrak ditulis dengan istilah yang tidak ambigu.
- Risiko-risiko utama dipertimbangkan selama tahap penyusunan kontrak, dan klausul-klausul yang relevan disertakan. Masalah yang memerlukan penyelesaian dikomunikasikan dengan pihak ketiga selama tahap ini.
- Elemen-elemen penting dari kontrak ditentukan berdasarkan kebijakan dan prosedur kontrak organisasi dan tingkat prioritas pihak ketiga. Elemen-elemennya dapat meliputi:
  - Perjanjian kerahasiaan (privasi).
  - Klausul penghentian dan parameter yang ditentukan untuk akses data.
  - Persyaratan keamanan siber, termasuk persyaratan untuk mengakses dan berbagi semua data dan melaporkan insiden atau pelanggaran dalam periode tertentu.
  - Persyaratan untuk pemberitahuan pelanggaran yang memengaruhi data organisasi utama.
  - Proses standar untuk memverifikasi identifikasi pihak ketiga, termasuk nama lengkap, alamat, lokasi fisik, dan situs web. Praktik standarnya adalah dengan menggunakan ceklis selama proses identifikasi dan meninjau keakuratan informasi.
  - Perjanjian tingkat jasa yang didefinisikan dengan jelas, yang menetapkan hasil yang diharapkan dan hak, kewajiban, hukuman, penghargaan, dan tanggung jawab masing-masing pihak, termasuk tanggung jawab untuk membayar biaya tenaga kerja (termasuk subkontraktor hilir).
  - Klausul hak untuk mengaudit yang mencakup subkontraktor hilir, atau persyaratan untuk bukti bahwa penyedia jaminan independen yang bereputasi baik telah mengaudit para pihak. Tanpa klausul hak untuk mengaudit, kemampuan fungsi audit internal untuk memperoleh atau memberikan asurans mungkin terbatas.

- Organisasi utama memiliki akses ke laporan penilaian pengendalian dari auditor independen; misalnya, laporan keuangan, kepatuhan, dan keamanan data, seperti laporan *International Standard on Assurance Engagements* atau SOC.
    - Jika mengandalkan hasil kerja penyedia jaminan eksternal pihak ketiga, dokumen-dokumen ditinjau untuk memastikan keandalannya.
    - Laporan SOC digunakan untuk mengidentifikasi risiko yang tidak memadai dan proses manajemen perubahan.
- Kebijakan dan prosedur membahas komponen apa pun yang penting bagi organisasi atau jenis kontrak tertentu:
    - Klausul lingkungan dan keberlanjutan.
    - Protokol pelaporan pelanggaran.
    - Persyaratan untuk penilaian ukuran kinerja.
    - Menguji rencana keberlanjutan bisnis untuk pihak ketiga.
    - Penggunaan kecerdasan buatan dalam penyampaian jasa.
    - Identifikasi, pengungkapan, persyaratan, dan ruang lingkup yang jelas untuk setiap pekerjaan yang disubkontrakkan.
    - Proses manajemen perubahan, yang menguraikan cara menangani perubahan pada ruang lingkup, persyaratan, atau persyaratan operasional (seperti perubahan teknologi atau pembaruan peraturan) selama masa kontrak.
    - Batasan jumlah pesanan perubahan atau jumlah yang dapat ditagihkan.
- Kebijakan dan prosedur mengharuskan penerimaan formal atas produk akhir sebelum pembayaran dilakukan atau retensi dilepaskan.
- Pihak ketiga diwajibkan untuk membagikan kebijakan etika atau kode etik mereka dan/atau mematuhi kebijakan organisasi utama.
- Jika pihak ketiga yang memberikan kontrak, organisasi utama telah melakukan tinjauan hukum, dan risiko-risiko utama telah dipahami dan didukung oleh strategi mitigasi risiko yang sesuai.

C. Kontrak atau perjanjian yang telah selesai ditinjau dan disetujui oleh pemangku kepentingan yang tepat, termasuk bagian hukum dan kepatuhan, disimpan dengan aman, dan ditugaskan kepada manajer atau administrator kontrak untuk bertanggung jawab.

- Kontrak atau dokumen resmi lainnya yang menandakan hubungan alih daya dan kewajiban pihak ketiga, serta bukti tinjauan hukum dan kepatuhan yang diperlukan.

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

- Proses untuk menambahkan kontrak atau perjanjian pihak ketiga yang baru ke dalam daftar atau sistem.
- Proses untuk memasukkan pihak ketiga yang potensial ke dalam sistem vendor dan menghapusnya jika kontrak tidak disetujui.

- Proses untuk menghapus kontrak atau perjanjian pihak ketiga dari daftar atau sistem.
- Sistem pelacakan untuk mendokumentasikan masalah dengan kontraktor atau vendor tertentu sebagai referensi di masa mendatang.
- Proses peninjauan untuk menentukan apakah populasi pihak ketiga akurat dan lengkap.

E. Proses onboarding yang terdokumentasi dibuat dan diikuti untuk memungkinkan pihak ketiga memenuhi persyaratan kontrak atau perjanjian. Reviu mungkin termasuk memverifikasi apakah:

- Prosedur onboarding terstandar untuk memastikan semua dokumentasi, pelatihan, dan reviu kepatuhan yang diperlukan telah diselesaikan.
- Sistem dan proses pihak ketiga dapat berintegrasi secara mulus dengan teknologi organisasi utama.
- Sistem bersama kompatibel dan aman. Bukti dapat mencakup pengendalian entitas pengguna yang saling melengkapi sebagai bagian dari pelaporan SOC.
- Organisasi utama menilai rencana keberlangsungan bisnis pihak ketiga, yang memastikan jasa terus berlanjut selama keadaan darurat. Rencana kontingensi disertakan untuk mengatasi potensi gangguan.

F. Proses untuk memantau kinerja vendor yang sedang berlangsung sehubungan dengan tujuan kontrak atau perjanjian, termasuk evaluasi indikator kinerja utama.

- Proses pemantauan menginformasikan asesmen risiko pihak ketiga, dan kelemahan pengendalian yang teridentifikasi ditinjau, dieskalasi, dan ditangani sesuai kebutuhan.
- Laporan atau pengamatan proses, teknologi, dan alat yang dibuat untuk mengelola pemantauan secara *real time*.
- Proses untuk memastikan pembayaran dilakukan sesuai dengan ketentuan kontrak atau perjanjian, seperti memenuhi jadwal proyek, pencapaian, dan persyaratan komunikasi. Pembayaran dilakukan hanya kepada kontraktor yang disetujui yang telah menyelesaikan tahap onboarding dan masuk ke dalam sistem pembayaran vendor. Ketika hasil kerja ditentukan dalam kontrak, pembayaran akhir hanya dilakukan setelah hasil kerja diverifikasi.
- Pemantauan untuk mengendalikan biaya yang terkait dengan perjanjian pihak ketiga untuk memastikan nilai dan menentukan laba atas investasi. Hasil analisis biaya-manfaat digunakan untuk menegosiasikan ulang kontrak.
- Proses untuk menilai penalti atas ketidakpatuhan terhadap perjanjian tingkat jasa dalam kontrak atau perjanjian. Denda dihitung dan dibebankan pada saat terjadi.
- Peringkat berbasis risiko dari pihak ketiga yang diprioritaskan dievaluasi kembali secara berkala, ketika ada perubahan pada perjanjian, dan ketika kontrak mendekati masa berlaku atau perpanjangan otomatis.
- Peninjauan pihak ketiga yang diprioritaskan, seperti tinjauan bisnis di lokasi atau triwulanan, untuk memvalidasi pengendalian dan integritas operasional.
- Bukti pemantauan tambahan yang sedang berlangsung dapat mencakup:

- Analisis stabilitas keuangan pihak ketiga.
- Penilaian atas pengaduan terhadap pihak ketiga.
- Tinjauan manajemen atas laporan auditor independen seperti *International Standard on Assurance Engagements*, *Statements on Standards for Attestation Engagements*, pelaporan keuangan, audit, kepatuhan, dan keamanan data yang disediakan oleh pihak ketiga; sertifikasi ISO.
- Tinjauan manajemen atas uji ketahanan bisnis yang dilakukan oleh pihak ketiga, termasuk isu-isu signifikan yang teridentifikasi.
- Ketentuan dan pembatasan penggunaan pihak subkontrak atau pihak hilir.
- Evaluasi nilai, budaya, dan perilaku etis pihak ketiga.
- Tanggapan terhadap pertanyaan media.
- Evaluasi protokol privasi dan keamanan siber untuk melindungi penyimpanan dan transfer data dan informasi utama organisasi, termasuk penggunaan teknologi canggih seperti kecerdasan buatan.
- Identifikasi organisasi terhadap peluang untuk peningkatan kinerja yang berkelanjutan dan memenuhi tujuan kontrak atau perjanjian.
- Peninjauan terhadap pemisahan tugas.

G. Protokol untuk memulai tindakan korektif atas insiden yang teridentifikasi ketika pihak ketiga gagal memenuhi persyaratan kontrak atau perjanjian, atau jika tindakan pihak ketiga meningkatkan risiko bagi organisasi utama.

- Protokol untuk meningkatkan insiden berdasarkan tingkat keparahan insiden dan prioritas pihak ketiga.
- Tinjauan pasca insiden, termasuk analisis akar masalah.

H. Proses untuk memberikan peringatan untuk kontrak dan perjanjian yang mendekati berakhirnya masa berlaku atau perpanjangan otomatis. Proses perpanjangan otomatis termasuk peninjauan:

- Kinerja pihak ketiga.
- Ketentuan kontrak atau perjanjian dan segala adendumnya.
- Faktor-faktor risiko.

I. Rencana *offboarding* yang diformalkan diimplementasikan dan diikuti untuk memastikan persyaratan kontrak yang melibatkan waktu dan ekspektasi ditangani secara memadai, termasuk untuk subkontraktor hilir.

- Ceklis atau wawancara dengan pemangku kepentingan utama untuk memastikan langkah-langkah keamanan berjalan efektif.
- Informasi atau data organisasi yang berada di tangan pihak ketiga telah dikembalikan atau dimusnahkan.
- Akses pihak ketiga ke data, sistem, atau fasilitas organisasi telah dicabut.

- Aset utama organisasi, seperti perangkat, lisensi perangkat lunak, kekayaan intelektual, dan dokumentasi, telah dikembalikan.
- Ketika pihak ketiga diberhentikan karena suatu alasan, keadaan atau risiko yang meringankan akan diidentifikasi dan dieskalasi kepada manajemen senior dan/atau dewan.
- Ketika kontrak pihak ketiga yang diprioritaskan diakhiri, pihak tersebut diganti berdasarkan asesmen risiko yang sama, kecuali jika kontrak tersebut telah selesai atau tidak lagi diperlukan.

Lampiran A. Contoh Aplikasi Praktis

Contoh-contoh berikut ini menjelaskan skenario di mana Persyaratan Topik Spesifik Pihak Ketiga dapat diterapkan:

Contoh 1: Penugasan audit internal pada rencana audit internal mencakup jasa atau output yang saat ini disediakan oleh pihak ketiga.

Ketika fungsi audit internal menyelesaikan proses perencanaan berbasis risiko dan memasukkan satu atau beberapa penugasan dalam rencana audit internal atas jasa atau output yang saat ini disediakan oleh pihak ketiga berdasarkan kontrak atau perjanjian, maka Persyaratan Topik Spesifik wajib diterapkan.

Tidak semua persyaratan dalam Persyaratan Topik Spesifik dapat diterapkan dalam setiap penugasan. Ketika auditor internal menerapkan pertimbangan profesional dan menentukan bahwa satu atau beberapa persyaratan dari Persyaratan Topik Spesifik Pihak Ketiga 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 persyaratan tertentu bisa jadi karena fungsi audit internal telah menetapkan bahwa ketergantungan organisasi pada pihak ketiga untuk jasa yang sangat penting adalah rendah, atau karena hubungan yang terjalin adalah hubungan yang sudah mapan dengan dampak keuangan yang rendah.

Contoh 2: Risiko pihak ketiga diidentifikasi selama penugasan asurans atas topik selain dari pihak ketiga atau manajemen kontrak.

Auditor internal dapat mengidentifikasi risiko pihak ketiga yang signifikan ketika menilai proses yang pada awalnya tidak ditentukan terkait dengan pihak ketiga atau manajemen kontrak. Sebagai contoh, ketika merencanakan penugasan untuk menilai penyimpanan data, auditor internal mengetahui bahwa jasa *cloud* diselenggarakan melalui pihak ketiga. Selama wawancara dengan manajemen pihak ketiga yang menyediakan jasa, auditor internal mengidentifikasi risiko keamanan siber yang terkait dengan pihak ketiga tersebut.

Setelah risiko yang relevan diidentifikasi, auditor internal harus meninjau Persyaratan Topik Spesifik Pihak Ketiga dan Persyaratan Topik Spesifik Keamanan Siber dan menentukan persyaratan mana yang berlaku. Auditor dapat mengecualikan proses tata kelola pihak ketiga atau proses manajemen risiko pihak ketiga dalam ruang lingkup penugasan dan berfokus pada pengendalian pihak ketiga atas jasa yang diaudit. Penilaian profesional yang sama ini berlaku untuk penerapan Persyaratan Topik Spesifik Keamanan Siber. Auditor harus mendokumentasikan dalam kertas kerja penugasan alasan untuk mengecualikan persyaratan dari Persyaratan Topik Spesifik Pihak Ketiga atau Persyaratan Topik Spesifik Keamanan Siber dan menyimpan dokumentasi tersebut.

Contoh 3: Penugasan pihak ketiga yang semula tidak termasuk dalam rencana audit internal diperlukan.

Suatu masalah muncul di dalam organisasi yang melibatkan pihak ketiga yang diprioritaskan yang memerlukan perhatian segera dari fungsi audit internal. Permasalahan melibatkan kegagalan pengendalian. Chief audit executive harus berkomunikasi dengan dewan mengenai prioritas ulang rencana audit dan sumber daya fungsi audit internal untuk mengakomodasi kebutuhan. Auditor harus terlibat dengan manajemen yang terkena dampak untuk mengembangkan tujuan penugasan untuk mengevaluasi situasi dan membuat rekomendasi untuk mencegah kejadian di masa depan. Chief audit executive harus meninjau Persyaratan Topik Spesifik untuk menentukan ruang lingkup penugasan, menentukan persyaratan mana yang berlaku, dan mendokumentasikan setiap pengecualian.

Lampiran B. Alat Dokumentasi Opsional

Auditor internal diharapkan untuk menggunakan pertimbangan profesional dalam menentukan penerapan persyaratan berdasarkan asesmen risiko dan mendokumentasikan pengecualian persyaratan tertentu secara tepat. Persyaratan Topik Spesifik dapat didokumentasikan dalam rencana audit internal atau dalam kertas kerja penugasan berdasarkan pertimbangan profesional auditor. Satu atau beberapa penugasan audit internal dapat memenuhi persyaratan tersebut. Sebagai tambahan, tidak semua persyaratan dapat diterapkan. Formulir yang dapat dicetak di bawah ini menyediakan satu opsi untuk mendokumentasikan kesesuaian dengan Persyaratan Topik Spesifik Pihak Ketiga, tetapi penggunaannya tidak wajib.

Tata Kelola Pihak Ketiga

Persyaratan	Cakupan yang Dieksekusi atau Alasan Pengecualian	Referensi Dokumentasi
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 jasa.		
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.		

Persyaratan	Cakupan yang Dieksekusi atau Alasan Pengecualian	Referensi Dokumentasi
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 Pihak Ketiga

Persyaratan	Cakupan yang Dieksekusi atau Alasan Pengecualian	Referensi Dokumentasi
A. Proses untuk manajemen risiko pihak ketiga dan jasa 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.		

Persyaratan	Cakupan yang Dieksekusi atau Alasan Pengecualian	Referensi Dokumentasi
B. Risiko yang terkait dengan pihak ketiga di seluruh daur hidup diidentifikasi dan dinilai secara teratur. Asesmen 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. Asesmen 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 tersedia 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 meningkat, maka tersedia 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 Pihak Ketiga

Persyaratan	Cakupan yang Dieksekusi atau Alasan Pengecualian	Referensi Dokumentasi
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.		

Persyaratan	Cakupan yang Dieksekusi atau Alasan Pengecualian	Referensi Dokumentasi
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 onboarding 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.		

Persyaratan	Cakupan yang Dieksekusi atau Alasan Pengecualian	Referensi Dokumentasi
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.

Sangkalan

IIA menerbitkan dokumen ini untuk tujuan informasi dan pendidikan. Materi ini tidak dimaksudkan untuk memberikan jawaban yang pasti untuk keadaan individu tertentu dan dengan demikian hanya dimaksudkan untuk digunakan sebagai panduan. IIA merekomendasikan untuk mencari advis ahli independen yang berkaitan langsung dengan situasi tertentu. IIA tidak bertanggung jawab atas siapa pun yang hanya mengandalkan materi ini.

Hak Cipta

September 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