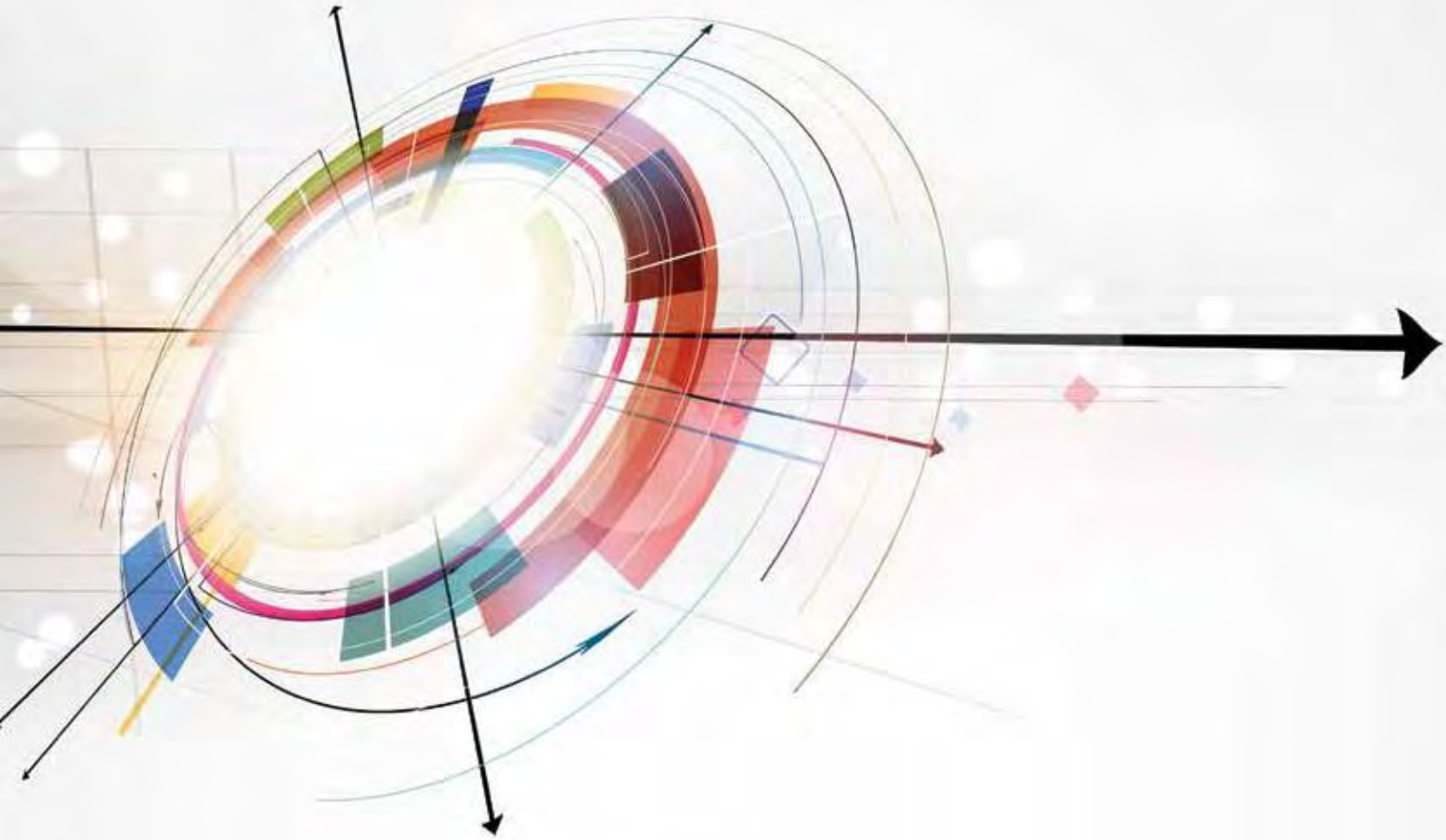

GLOBAL PERSPECTIVES AND INSIGHTS

2018 Global Risk Report

Risiko-risiko puncak yang dihadapi oleh Chief Audit Executive

(saduran dari: Top Risks Faced by Chief Audit Executives)

The Institute of Internal Auditors

Isu Sebelumnya

Untuk mengkases isu Global Perspectives and Insights sebelumnya, kunjungi www.theiia.org/gpi.

Komentar dan Tanggapan

Kirimkan pertanyaan dan tanggapan kepada: globalperspectives@theiia.org.

Daftar Isi

Pendahuluan

Menyongsong tahun baru 2018, tahun dengan proyeksi prospek ekonomi yang sehat dan munculnya sesuatu yang baru di bidang hukum , peraturan, opini, ide, teknologi, dan risiko. Lingkungan bisnis saat ini sangat berbeda dari sebelumnya; lebih kompleks dan lebih terhubung. Organisasitidak saja menghadapi risiko baru yang belum diketahui, tetapi juga peluang baru yang belum tersentuh. Mempertimbangkan di tahun mendatang adanya peluang baru dan sejumlah tantangan dan risiko potensial - beberapa di antaranya adalah kondisi yang diharapkan dan beberapa di antaranya mungkin hanya berlaku di tahun 2018- Rencana audit harus dilihat sebagai kerangka kerja yang dapat berubah megikuti terjadinya suatu peristiwa, termasuk yang bersifat menggangu (*disruptive)*.

Mengacu kepada pandangan organisasinya secara menyeluruh, audit internal membantu organisasi mencapai tujuannya dengan membawa pendekatan yang sistematis dan disiplin untuk mengevaluasi dan meningkatkan efektivitas proses manajemen risiko, kontrol, dan tata kelola. Regulator dan komite audit ingin dan membutuhkan jaminan bahwa upaya manajemen risiko memadai untuk mengatasi ancaman yang ditimbulkan oleh pesaing yang tangguh, teknologi yang berkembang, tren pasar yang berubah, dan perkembangan peraturan. *(lihat Internal Audit Future Trends: Emerging Trends and High-impact Areas of Focus).*

Karena adanya kebutuhan bagi fungsi audit internal untuk memberikan lebih banyak nilai tambah dan dukungan strategis untuk semua industri, auditor perlu memastikan bahwa pekerjaan mereka selaras dengan semua risiko signifikan, terutama risiko strategis dan operasional. Audit internal harus responsif dan dapat beradaptasi dengan lingkungan risiko yang dinamis.

Risiko berubah-rencana audit yang telah dipersiapkan secara matang seharusnya fleksibel dan dapat berubah mengikuti potensi munculnya risiko baru di setiap tingkat organisasi. Makalah ini membahas lima risiko puncak (untuk audit internal atau organisasi) yang dihadapi oleh *chief audit executives* (CAEs), seperti yang diidentifikasi oleh afiliasi dari IIA Global. Risiko-risiko ini adalah: Management Talenta, Analisa Data, Siber, Regulasi, dan Respon atas gangguan (disrupsi).

Manajemen Talenta

Manajemen talenta secara konsisten menjadi perhatian utama CAE dan para profesional audit internal. Selama beberapa tahun terakhir, CAE merasa prihatin untuk mendapatkan kandidat auditor dengan keterampilan yang diperlukan untuk mengisi peran baru serta mampu mengatasi risiko baru yang ada. Secara nyata, ada kumpulan kandidat dengan keterbatasan keterampilanyang dibutuhkan untuk memenuhi kebutuhan audit internal yang berkembang. Selain itu, ada tantangan untuk menyelaraskan lingkungan kerja dengan atribut unik dari angkatan kerja milenium, yang memiliki harapan dan dukungan yang lebih besar dan berbeda, lingkungan kerja yang spesifik dalam

pikiran, dan preferensi untuk jadwal kerja yang lebih fleksibel. (lihat 4 Strategies for Bridging the Internal Audit Talent Gap).

Pada tahun 2015, merekrut dan mempertahankan talenta adalah prioritas utama atau penting bagi lebih dari 40 persen dari responden yang menanggapi survey IIA global, lebih dari separuh responden tersebut menghubungkan kesenjangan pengetahuan dengan keterbatasan jumlah auditor terampil

"Jika audit internal harus dipersiapkan untuk masa depan, salah satu dari lima keharusan yang harus ditangani adalah ketangkasan. Kita harus cukup tangkas untuk mengenali dan mengatasi risiko yang muncul dan menilai risiko secara terus-menerus, kemudian menyesuaikan cakupan audit kita. Dan, kita harus cukup tangkas untuk mengenali celah dalam kemampuan kita dan menutupnya dengan cepat. Sukses di masa depan akan datang bagi departemen audit internal yang memiliki dinamika strategi manajemen bakat."

Richard Chambers,
IIA President and CEO

Sekali lagi pada tahun 2017, sebagai tanggapan atas survei IIA Audit Executive Center® (AEC®), terdapat mayoritas yang jelas (79 persen) dari hampir 200 CAE mengidentifikasi manajemen talenta sebagai risiko paling penting / sangat penting bagi profesi audit internal. Menurut KPMG, talenta - atau ketiadaannya - dianggap oleh dewan direksi sebagai risiko perusahaan. Ketika organisasi menjadi global, tenaga kerja yang mendukung mereka terus berkembang, itulah sebabnya mengapa manajemen talenta sangat penting. Dampak potensial dan implikasi dari kekurangan bakat global diantaranya ketidakmampuan untuk mempertahankan keterampilan kepemimpinan, karena tidak ada lagi saluran yang sehat dari pemimpin masa depan, dan pelaksanaan strategi bisnis diragukan karena kandidat tidak mampu mengambil peran penting. Organisasi menemukan bahwa mereka tidak mampu melatih dan membimbing generasi baru atau mempertahankan talenta atau memiliki keahlian khusus, hal ini menyebabkan hilangnya modal intelektual dan keunggulan kompetitif. Lebih lanjut, dan terus-menerus, populasi yang memasuki usia pensiun memicu kelangkaan keterampilan *(lihat Boardroom Questions: Talent Management...or Talent Risk?)*

Untuk menambah pentingnya hal ini, karena risiko yang muncul - seperti analisa data, manajemen pihak ketiga, *cybersecurity*, keberlanjutan, unsur politik dan ketidakpastian lainnya - organisasi mengharapkan sesuatu yang lebih dari auditor internal mereka. Saat ini sudah tidak relevan lagi kondisi dimana fokus audit internal terbatas pada tugas dan minat berbasis keuangan dan kepatuhan tradisional.

Walaupun audit internal tidak terlibat langsung dalam urusan sumber daya manusia, audit internal harus menilai seberapa baik manajemen menangani risiko-risiko yang ada. Organisasi saat ini membutuhkan, dan mengharapkan auditor internal untuk mengambil pendekatan yang lebih holistik untuk audit, termasuk pengawasan risiko dan penciptaan nilai yang terintegrasi. Karena itu, pencarian bakat, keterampilan, dan kekuatan audit internal menjadi sangat kompetitif.

Tanpa keterampilan yang memadai, audit internal rentan terhadap kesalahan dan kelalaian, atau tidak melakukan audit dengan sepenuhnya, risiko spesifik dan non-tradisional, seperti teknologi, geopolitik, ekonomi, pelaporan perusahaan yang berkembang, budaya, serta peraturan domestik dan global. Menurut *Society for Human Resource Management*, kemampuan audit internal untuk berevolusi melampaui keahlian keuangan tradisional, operasional, dan TI umum, dan fokus pada gambaran yang lebih besar menjadi sangat penting.

Kegiatan audit internal yang dengan serius memperluas kompetensinya dan melakukan pekerjaannya berdasarkan pemahaman yang lebih komprehensif

dari profil risiko organisasi akan lebih siap untuk melayani organisasi. Bagian dari persiapan itu adalah membawa orang dengan kemampuan berpikir kritis dan ketajaman bisnis yang tajam, dipasangkan dengan keahlian di bidang tertentu atau dengan pengetahuan khusus industri. Risiko nontradisional yang muncul akan mempengaruhi lingkup kerja audit; oleh karena itu, audit internal harus mencapai dan memperluas luas dan kedalaman keterampilannya.

Sangat penting bahwa CAE memimpin auditor untuk memperluas pengalaman dan keterampilan mereka, dan mempertimbangkan "risiko baru" yang timbul dalam menilai dan melaksanakan rencana audit. Namun jangan salah pengertian, pelatihan audit tradisional tetap relevan, dan akan selalu relevan; tetapi pendidikan berkelanjutan dan eksposur, kemampuan beradaptasi, ketrampilan non teknis yang baik, dan pengetahuan proses dan operasi sangat penting untuk menavigasi dunia bisnis baru.

Kemampuan untuk mengelola semua talenta sangat penting bagi keberhasilan audit internal, dan dapat membawa manfaat jangka panjang - melampaui kekurangan staf yang mengisi kekurangan staf. Untuk mengoptimalkan upaya pengelolaan talenta, CAE dan manajemen senior harus mengembangkan pendekatan yang dipikirkan secara matang dan dikembangkan dengan baik untuk membantu merestrukturisasi dan meningkatkan tenaga kerja mereka. Untuk efektifitas, membangun, melibatkan, dan mempertahankan kegiatan audit internal terbaik yang memungkikann dalam menghadapi risiko baru, CAE harus mengembangkan strategi yang mencakup mengukur apa yang dibutuhkan dari anggota staf mereka yang ada, apa yang dibutuhkan dari penambahan yang diantisipasi untuk staf mereka , dan, sama pentingnya, apa yang perlu dilihat dan didengar anggota staf dari para pemimpin mereka untuk tumbuh dan berhasil.

Strategi manajemen talenta yang baik tergantung pada kombinasi beberapa pendekatan. CAE tidak akan dapat menemukan jalan keluar dari kekurangan bakat. Ada pasokan singkat atas kandidat dengan keterampilan yang dibutuhkan untuk mengatasi risiko masa depan - termasuk mereka yang memiliki keterampilan dalam ilmu data, pemikiran inovatif, pemikiran analitis / kritis, komunikasi, dan lain-lain. Strategi yang efektif didalamnya juga termasuk memahami keterampilan dan atribut apa yang diperlukan, dan upaya berkelanjutan untuk memperoleh, mengembangkan, dan mempertahankan talenta terbaik.

Fokus Audit

IIA Standard 1210: Kecakapan

Auditor internal harus memiliki pengetahuan, keterampilan, dan kompetensi lain yang dibutuhkan dalam melaksanakan tugas dan tanggung jawabnya.
Aktivitas audit internal,secara Kolektif harus memiliki atau memperoleh pengetahuan, keterampilan, dan kompetensi lain yang dibutuhkan untuk me laksanakan tanggung jawabnya

IIA Standard 1230: Pengembangan Profesional Berkelanjutan

Auditor internal harus senantiasa meningkatkan pengetahuan, keterampilan dan kompetensi
lainnya melalui pengembangan profesional berkelanjutan.

Tujuan

- Kompetensi secara kolektif dari auditor internal yang muncul karena risiko yang menyebabkan penetapan lingkup audit internal.
- CAE, komite audit, dan manajemen eksekutif memiliki pemahaman yang kuat tentang keterampilan yang dibutuhkan untuk mendukung tujuan organisasi, dan total biaya staf audit internal.
- Audit internal telah menerapkan proses manajemen kinerja yang konsisten.
- Pemimpin audit internal memiliki kemampuan untuk melatih, membimbing, dan melibatkan generasi baru atau pendatang baru dalam profesi audit internal.
- Rencana karir formal tersedia untuk semua staf audit internal.
- Audit internal telah membuat program untuk mengikutsertakan karyawan baru dan secara berkelanjutan mendidik semua orang tentang budaya organisasi, selera risiko, dan arah strategis.

Langkah Penerapan

- Tinjau kembali penilaian risiko dan rencana audit. Identifikasi keterampilan yang dibutuhkan untuk melaksanakan rencana tersebut. Lakukan analisis kesenjangan (gap analysis) antara keterampilan yang ada dan keterampilan yang dibutuhkan saat ini. Kembangkan strategi untuk mengisi kesenjangan yang ada.
- Rancang atau Restrukturisasi ulasan kinerja untuk menyertakan kompetensi kerja spesifik, sasaran yang dapat ditindaklanjuti yang sejalan dengan rencana strategis organisasi, dan struktur gaji untuk profesional khusus seperti analis data.

Fokus Audit

IIA Standard 1220: Prinsip Kecermatan Profesional

Auditor internal harus menggunakan kecermatan dan keahlian sebagaimana diharapkan dari seorang auditor internal yang cukup hati-hati (reasonably prudent) dan kompeten. Cermat secara profesional tidak berarti tidak akan terjadi kekeliruan.

1220.A2 – Dalam menerapkan kecermatan profesional, auditor internal harus mempertimbangkan penggunaan sarana audit berbantuan teknologi dan teknik analisis data lainnya.

- Bimbing dan latih keterampilan staf yang ada, yang memberi sedikit gangguan dan mengintegrasikan pengetahuan perusahaan yang sudah ada dengan keterampilan yang dibutuhkan.
- Terus-menerus dapatkan keterampilan baru di pasar. Carilah kandidat dengan latar belakang yang berbeda, bukan hanya mereka yang memiliki gelar keuangan dan akuntansi. Pertimbangkan penyedia layanan pihak ketiga sebagai sumber daya untuk mendapatkan keterampilan yang dibutuhkan dengan cepat untuk mengatasi risiko yang kompleks dan khusus.
- Tetapkan program transfer pengetahuan dan orientasi yang efektif.

Analisis Data

Analisis data adalah proses mengumpulkan dan menganalisis data, dan kemudian menggunakan hasilnya untuk membuat keputusan yang lebih baik *(Internal Auditing, 4th edition, 11-2,* Internal Audit Foundation, 2017*)*. Organisasi menghasilkan simpanan data yang tumbuh signifikan dari kegiatan operasional mereka, yang menghadirkan dua tantangan utama untuk audit internal. Yang pertama adalah bagaimana membantu dewan direksi dan manajemen memahami bagaimana data dikumpulkan, dikelola, dilindungi, dan dimanfaatkan. Yang kedua adalah bagaimana mengeksploitasi data yang berkembang dari perspektif audit internal dalam menerapkan alat analisis untuk proses audit yang ada, dan mengotomatisasi audit rutin dan berfokus pada bidang risiko yang muncul. *(lihat Risk in Focus: Hot Topics for Internal Audit 2018).*

Pada dasarnya, *data analytic* memecah volume data, dan membangunnya kembali dalam bentukpotongan yang lebih kecil, memberikan kesempatan untuk mengekstrak makna dan pemahaman dari data. Dengan informasi itu, audit internal dapat menganalisis total risiko populasi dan korelasi potensial, memberikan wawasan dan pandangan ke depan, dan melaporkan isu-isu yang menjadi perhatian para pemangku kepentingan dan tertarik untuk mengikutinya. Mengelola *data analytic*, dan risiko yang terkait dengannya, bisa menjadi sesuatu yang membingungkan. Menghasilkan wawasan yang berarti dari data itu - dan mengubah pengetahuan menjadi tindakan - adalah, kadang-kadang, lebih mudah dikatakan daripada dilakukan. Agar analitik data menjadi efektif, orang yang tepat, format, proses, dan teknologi harus ada.

Dengan lebih banyak data daripada sebelumnya, manajemen dan dewan direksi harus menyadari bahwa sejumlah besar data akan memaparkan organisasi pada risiko finansial dan nonfinansial terkait data tersebut. Beberapa area risiko tersebut harus ditangani dalam semua inisiatif analisis data *(lihat Understanding and Managing the Risks of Analytics)*:

- **Risiko Kualitas Data dan Informasi** - Pengambil keputusan membutuhkan data yang mengkomunikasikan dan mempromosikan pemahaman yang kompleks. Harus ada definisi yang jelas dan standar kualitas untuk semua data dan informasi.
- **Risiko Kepatuhan Data dan Informasi** - Kegagalan untuk memenuhi persyaratan agen resmi dan diakui (biasanya terkait dengan negara bagian,

federal, atau internasional) dapat menyebabkan hasil yang merugikan seperti sanksi finansial, pekerjaan tambahan, atau tanggung jawab pribadi.

- **Risiko Tata Kelola Data dan Informasi** - Data dan informasi harus dikontrol secara hati-hati melalui penggunaan prinsip dan proses manajemen risiko pada tingkat yang sesuai untuk memastikan privasi, keamanan, kualitas, dan auditabilitas.
- **Penggunaan Analisis Risiko yang Tidak Tepat atau Prematur** – Analsis data tidak akan membantu ketika tidak ada waktu untuk mengumpulkan, memproses, dan menafsirkan data; ketika tidak ada riwayat atau preseden yang terkait dengan keputusan atau ketika data historis menyesatkan; atau ketika variabel kunci tidak dapat diukur atau memiliki tingkat ketidakpastian yang tinggi.
- **Risiko Dampak Kontra Budaya** - Memaksakan inisiatif analisis data dalam budaya organisasi yang tidak berorientasi data dapat menimbulkan risiko signifikan bagi para pemimpin; inisiatif analisis data harus mencakup penilaian terhadap sistem pengambilan keputusan organisasi dan tingkat di mana budaya organisasi berorientasi pada data.
- **Risiko Etika Data** - Inisiatif analisis data harus selaras dengan nilai inti organisasi, pengambilan keputusan, dan perilaku. Kontrol harus dilakukan untuk memastikan pengumpulan dan penggunaan data dilakukan dengan etis.

Audit internal harus selalu menyadari bahaya yang dihadapi organisasi dengan proyek data besar, terutama dalam situasi di mana staf tidak memiliki keterampilan. Permintaan analisis data sedang meningkat, dan segera - jika belum - akan menjadi bagian integral dari setiap organisasi. Meskipun penting bagi organisasi untuk berpartisipasi dalam proyek *Big-data* agar tetap kompetitif dan tidak tertinggal, ada risiko yang perlu dipertimbangkan:

- Keamanan data.
- Privasi data.
- Biaya.
- Data tidak dapat diandalkan, tidak valid, tidak cukup, atau tidak relevan.
- Proses analisis yang tidak andal, tidak valid, tidak cukup, atau tidak relevan.

Teknologi mengubah dunia yang kita tinggali dengan kecepatan tinggi, dan konsekuensi dari kecepatan perubahan itu membuat frustrasi, jika kita tidak dipersiapkan dengan benar. Teknologi menghasilkan jumlah data yang jauh lebih besar, dan audit internal dapat menggunakannya untuk mengevaluasi risiko secara lebih menyeluruh, meningkatkan penyampaian hasil audit, dan berpotensi meningkatkan tingkat asurans yang diberikan.

Hasil dari studi kasus yang baru-baru ini dilakukan menunjukkan bahwa manfaat utama dari analisis data untuk audit internal termasuk peningkatan efisiensi, peningkatan efektivitas, peningkatan jaminan, fokus yang lebih besar pada risiko strategis, cakupan audit yang lebih besar, dan penghematan yang signifikan dalam hal waktu dan uang dalam jangka panjang . Namun, untuk mendapatkan manfaat ini, audit internal harus menilai seberapa baik program analitik data melayani tujuan menyeluruh dan kegiatan yang diinginkan.

Analisis data sangat penting untuk perangkat alat audit internal, karena dapat memberikan wawasan yang terpendam jauh di dalam data serta memungkinkan pengujian yang lebih efisien dan efektif. Banyak tim audit internal belum mengadopsi teknologi analitik data yang lebih canggih; mereka masih mengandalkan terutama pada alat dan aplikasi berbasis *spreadsheet*. Dukungan komite audit sangat penting. Audit internal harus memastikan komite audit dididik tentang pentingnya analitik data *(lihat Data Analytics: Is it Time to Take the First Step?).*

Untuk membangun atau meningkatkan program analitik data, CAE harus terlibat dalam diskusi dengan para pemangku kepentingan mengenai hasil yang diinginkan, mendefinisikan tujuan analitik dan menentukan kompetensi dan teknologi apa yang diperlukan.

Salah satu hambatan utama untuk membangun program *data analytic* yang efisien - dan risiko yang konstan untuk audit internal - adalah staf terampil yang kurang memadai untuk menangani data dalam jumlah besar. Karena kurangnya dalam spesialisasi ini, program analitik audit internal menjadi kurang optimal – bukan karena program itu sendiri, melainkan karena tidak digunakan secara maksimal. Seperti halnya inisiatif bisnis baru, proyek data besar melibatkan unsur risiko. Jika keahlian untuk mengelola data dalam jumlah besar itu hilang, maka akan meningkatkan elemen risiko menjadi lebih banyak lagi.

Tujuan

- Audit internal memiliki pemahaman yang mendalam tentang analitik data dan teknologi, dan bagaimana teknologi canggih dapat meningkatkan efektifitas dan efisiensi audit internal.
- Audit internal mengevaluasi seberapa baik manajemen merespons risiko baru yang diperkenalkan dari penggunaan analitik data yang diperluas.
- Audit internal memanfaatkan kemampuan berkelanjutan dari program analitik data untuk memberikan manfaat lengkap bagi organisasi (misalnya, validasi dan pemantauan skema dan perilaku berisiko tinggi, evaluasi dan keakuratan proses penilaian risiko khusus untuk organisasi, dan sebagainya).
- Audit internal memanfaatkan teknologi untuk identifikasi anomali dan pola risiko kecurangan secara dini, dan mengkomunikasikan temuan-temuan kunci tersebut.
- Audit internal memanfaatkan teknologi untuk meningkatkan cakupan risiko organisasi secara keseluruhan pada jam kerja dan biaya tenaga kerja yang lebih rendah.

Sebagian diadaptasi dari: First Steps in Building a Data Analytics Program for Your Internal Audit Team

Langkah Penerapan

- Tentukan hasil terbaik apa dari analisis terhadap tujuan audit internal, dengan memutuskan kebutuhan dasar dan spesifik untuk program analisis data.

- Memahami manfaat yang dapat diberikan oleh program analitik kepada organisasi dan audit internal dalam hal inovasi dan peluang. Mengidentifikasi keterampilan yang diperlukan untuk melaksanakan program secara optimal dan mewujudkan manfaatnya.
- Pertimbangkan analitik data sebagai komponen bisnis yang penting, dan sesuaikan keterlibatan audit untuk menerima pendekatan kualitas berkelanjutan terbaik untuk mengelola seluruh kerangka kerja kepatuhan dan kontrol organisasi.
- Terlibat dengan manajemen pada aturan spesifik, poin data, kode, dan asumsi dalam program yang secara akurat mendeteksi penyimpangan atau pola penipuan.

Siber

Apakah berupa serangan gencar tanpa henti terhadap pelanggaran informasi suatu organisasi atau akun pencurian identitas pribadi yang tidak pernah berakhir, penjahat dunia maya - canggih dan didanai dengan baik - adalah lawan yang tangguh. Interdependensi membuat dunia yang kompleks dan penuh risiko, diminati oleh penjahat cyber. Teknik yang mereka gunakan terus berkembang dan berevolusi; sedemikian sering, dan sudah menjadi urusan yang rutin bagi mereka.

Menjalankan rencana pertahanan terhadap serangan siber, dan memastikan bahwa rencana itu berjalan efektif, adalah pekerjaan 24 jam; yang menjadi masalah bukan bagaimana serangan akan terjadi tetapi kapan akan terjadi. Ada perbedaan besar antara kesadaran risiko siber dan kesiapan risiko siber. Semua sadar akan risikonya; kita dihadapkan dengan kebenaran setiap hari. Kesiapsiagaan, bagaimanapun, termasuk kemampuan untuk menggagalkan upaya serangan sepenuhnya, atau menahan serangan dan memulihkan dengan relatif sedikit atau tidak ada kerusakan. Suatu organisasi dikatakan memiliki ketahanan siber jika mereka harus mampu menahan, bereaksi, dan pulih dari serangan siber – atau sering kita kenal dengan istilah *cyber-resilient*.

Karena kepedulian terhadap isu-isu siber (misalnya: Peretasan / penyusupan, spear fishing, spionase ekonomi, dll.) telah meningkat, para pemangku kepentingan membutuhkan visibilitas yang lebih besar ke dalam program manajemen risiko *cybersecurity* dari organisasi mereka, dan dewan direksi menginginkan tinjauan independen, obyektif, dan komprehensif dari audit internal terhadap risiko siber dan program siber. Oleh karena itu, audit internal juga harus memiliki pengetahuan tentang risiko yang mungkin, dan memainkan peran penting dalam ketahanan siber.

Sayangnya, risiko *cybersecurity* tidak terbatas pada ancaman eksternal; ancaman potensial dapat dihasilkan dari tindakan karyawan atau mitra bisnis. Oleh karena itu, komponen penting dari ketahanan siber adalah manajemen yang tepat dan efektif dari budaya organisasi, serta evaluasi risikonya. Ketika mempertimbangkan budaya, dewan direksi juga termasuk mempertimbangkan budaya risiko, karena itu adalah dasar dari semua keputusan, perilaku, dan pengambilan risiko di dalam seluruh organisasi. Audit internal dapat mengaudit

budaya risiko dalam audit operasional dan keuangan standar dengan mengumpulkan data dan melakukan tinjauan informal.

Memimpin perubahan, audit internal dapat memperkuat pemahaman manajemen tentang efektivitas kontrol keamanan siber di semua area, bahkan pada tingkat di mana budaya organisasi memengaruhi persyaratan, proses, dan kemampuan. Budaya mendorong produktivitas, nilai, sikap, dan praktik dalam suatu organisasi, dan dibentuk dan dipelihara oleh banyak faktor yang berbeda; oleh karena itu, audit internal dapat menilai budaya untuk risiko dengan cara yang sama seperti menilai area lain dari suatu organisasi *(lihat Internal Audit Future Trends)*.

Audit internal dapat memaksimalkan nilainya dengan memahami cara mengevaluasi budaya, dan mendidik manajemen tentang pentingnya hal tersebut.

Untuk mengatasi risiko yang terkait dengan siber, termasuk budaya, penting bagi tim kepemimpinan untuk mengembangkan langkah-langkah pencegahan, menerapkannya dengan program pelatihan dan kesadaran, dan kemudian memastikan bahwa mereka terus ditunjukkan dalam perilaku. Oleh karena itu, karyawan, vendor, mitra, dan kontraktor harus dilatih dan dibuat untuk memahami apa yang diharapkan dari mereka berkaitan dengan langkah-langkah keamanan siber dan protokol.

Strategi penilaian risiko audit internal harus dikembangkan dengan mempertimbangkan semua risiko khusus untuk *cybersecurity*, dan memastikan kepatuhan dengan kebijakan dan kontrol internal. Audit internal perlu mengembangkan pendekatan audit yang sesuai untuk memenuhi kebutuhan organisasi dan pemangku kepentingannya di semua bidang di mana isu-isu siber. Untuk meningkatkan efektifitas, hal tersebut membutuhkan implementasi - pada aktivitas minimum - kontrol, lingkungan pengendalian, penilaian risiko, komunikasi, dan pemantauan, serta kerangka kerja untuk menilai tindakan *cybersecurity* *(lihat Risk in Focus: Hot Topics for Internal Audit 2018).*

Sebagai pertahanan lini ketiga, audit internal harus bekerja dengan manajemen dan dewan direksi ketika mereka mengembangkan strategi dan kebijakan keamanan siber untuk meningkatkan kemampuan organisasi untuk mengidentifikasi dan mengurangi risiko *cybersecurity*; memanfaatkan hubungan dengan komite audit dan dewan komisaris, untuk memastikan bahwa mereka tetap terlibat; dan pastikan bahwa risiko *cybersecurity* secara resmi terintegrasi dalam rencana audit, dengan keterampilan yang diperlukan (*inhouse* atau melalui cosourcing) untuk melaksanakan rencana tersebut. Muncul teknologi dan tren mempengaruhi profil risiko sosio-keamanan organisasi; oleh karena itu, audit internal juga harus mengikuti perkembangan teknologi baru dan mengevaluasi tingkat kerentanan organisasi, dan kegiatan risikonya terhadap rencana *cybersecurity* yang diinginkan.

"Direktur tidak perlu menjadi teknolog untuk memainkan peran yang efektif dalam pengawasan risiko siber - tetapi setiap anggota dewan direksi dapat mengambil kesempatan untuk meningkatkan efektivitas praktik pengawasan siber"

NACD Director's Handbook on Cyber-Risk Oversight, National Association of Corporate Directors (NACD), 2017

Sumber: The Value of Visibility: Cybersecurity risk management examination

Tujuan

- Organisasi memiliki budaya ketahanan siber.

- Audit internal memberikan kontribusi terhadap komponen-komponen kunci yang penting untuk pemeriksaan dan kesiapan *cybersecurity*:
  - Perlindungan dan Deteksi: Audit internal memberikan pendekatan holistik untuk mengidentifikasi di mana suatu organisasi rentan, dan menggabungkan analitik data dalam bidang tanggung jawabnya, yang akan memberi peringatan bahwa ada sesuatu yang salah.
  - Kelangsungan Bisnis: Audit internal memberikan saran, melibatkan manajemen karena mereka berencana untuk menangani dan mengatasi skenario risiko yang dapat berdampak pada operasi yang sedang berlangsung, termasuk serangan dunia maya, bencana alam, atau suksesi.
  - Manajemen Krisis / Komunikasi: Audit internal membantu perencanaan manajemen krisis dan kesiapan komunikasi dengan menyediakan pemeriksaan jaminan untuk keefektifan dan ketepatan waktu, dan melakukan analisis dan kritik terhadap rencana yang telah dilaksanakan.
  - Perbaikan Berkesinambungan: Audit internal menambah nilai dengan memberikan wawasan, dan meningkatkan strategi dan protokol untuk menjadi lebih baik untuk persiapan menghadapi serangan siber.

Langkah Penerapan

- Menilai budaya organisasi berkaitan dengan ketahanan siber.
- Lakukan penilaian risiko model keamanan dan proses *cybersecurity* dan buat rekomendasi untuk perbaikan.
- Lakukan pengujian penetrasi data dengan IT dan kontraktor pihak ketiga untuk menilai kemampuan pihak ketiga untuk mematuhi protokol yang ditetapkan.
- Melakukan analisis kesenjangan (gap analysis) ketahanan siber, merekomendasikan remediasi, dan menindaklanjuti kegiatan remediasi.
- Mempengaruhi budaya dengan menekankan pemantauan dan respons *cybersecurity* sebagai prioritas utama.
- Pastikan bahwa rencana kesinambungan bisnis diuji secara berkala dan tindakan korektif diambil untuk setiap kekurangan yang diidentifikasi.
- Menerapkan dan mendorong budaya siber yang kuat dan budaya risiko di seluruh organisasi, yang, seiring waktu, akan mempengaruhi dan meningkatkan langkah-langkah keamanan siber dan protokol/kesepakatan yang diterapkan.

Fokus Audit

IIA Standard 2130: Pengendalian

Aktivitas audit internal harus membantu organisasi memelihara pengendalian yang efektif dengan cara mengevaluasi efisiensi dan efektivitasnya serta mendorong pengembangan berkelanjutan.

2130.A1 – Aktivitas audit internal harus mengevaluasi kecukupan dan efektivitas pengendalian dalam merespon risiko dalam proses tata kelola (governance),operasi, dan sistem informasi organisasi, yang mencakup:

- Pencapaian tujuan strategis organisasi;
- Reliabilitas dan integritas informasi keuangan dan operasi;
- Efektivitas dan efisiensi operasi dan program;
- Pengamanan aset; dan
- Ketaatan terhadap hukum, peraturan, kebijakan, prosedur dan perjanjian kontrak

Regulasi

Secara global, organisasi menghadapi persyaratan peraturan baru atau yang dimodifikasi, yang dirancang untuk melindungi konsumen atau kepentingan publik. Peraturan yang paling penting berfokus pada risiko dan kontrol keuangan, privasi data dan keamanan, dan mereka memengaruhi organisasi di semua industri.

Cryptocurrencies

Menurut CNBC, *cryptocurrency* dapat menembus angka triliun dolar dalam hal nilai, menyusul aksi jual baru-baru ini di seluruh koin digital. Nilai Bitcoin mudah berubah: Pada awal 2018, harga berfluktuasi antara $ 6.000 dan $ 10.000. Thomas Glucksmann, kepala pengembangan bisnis Asia-Pasifik di Bursa Cryptocurrency Gatecoin, menyatakan, "Meningkatnya pengakuan regulasi pertukaran *cryptocurrency*, serta masuknya modal institusional, dan perkembangan teknologi utama akan berkontribusi terhadap pulihnya pasar dan mendorong harga *cryptocurrency* ke level tertinggi baru tahun ini. Tidak ada alasan mengapa kami tidak bisa melihat Bitcoin terdorong menjadi senilai $ 50.000 hingga Desember (2018)."

Selain itu, tidak adanya aturan yang jelas dari regulator global, menyulitkan organisasi keuangan untuk menetapkan peraturannya sendiri. Beberapa orang menganggap *cryptocurrency* sebagai komoditas, sementara yang lainnya mengatakan bahwa beberapa *cryptocurrency* mungkin adalah sekuritas, tetapi tidak menentukan *cryptocurrency* yang mana. Regulator global telah cemas terhadap volatilitas eksplosif atas nilai Bitcoin dan mata uang digital lainnya baru-baru ini, serta kemungkinan penerapan peraturan yang tegas (lihat Compliance Officers Sweat as Cryptocurrency Trades Go Mainstream).

"GDPR dan implikasinya semakin menonjol. Dari perspektif asurans, awalnya komite audit akan meminta kami untuk menilai program tersebut untuk kemudian kami mengembangkan program kami sendiri secara berkelanjutan dalam memastikan bahwa bisnis memiliki proses yang tepat sehingga dapat tetap memenuhi ketentuan."

CAE dari grup perbankan multinasional

Sumber: Risk in Focus: Hot Topics For Internal Audit 2018

Regulasi Perlindungan Data Global

Sejumlah pemerintah sedang menerapkan peningkatan regulasi atas privasi data. Dua pemerintah yang dapat dijadikan contoh adalah Uni Eropa (UE) dan Cina.

Setelah empat tahun persiapan dan perdebatan, Peraturan Perlindungan Data Umum (GDPR) Uni Eropa, yang menggantikan Petunjuk Perlindungan Data 95/46 / EC, telah disetujui oleh Parlemen Eropa pada bulan April 2016. GDPR mulai berlaku efektif pada bulan Mei 2018, di saat tahun demi tahun, pelanggaran atas data terbukti semakin besar, semakin mengganggu, dan semakin mahal. Pelanggaran atas data meningkat secara signifikan pada tahun 2017 yang melebihi peningkatan dari 2015 hingga 2016 sebesar 40 persen. (Untuk detail tambahan, lihat "Pelanggaran Data 2017," pada halaman berikutnya.)

Meskipun banyak perusahaan memiliki kebijakan privasi yang konsisten dengan Petunjuk yang berlaku sebelumnya, GDPR baru ini berisi sejumlah perlindungan baru untuk data UE, dan berjanji untuk mengenakan denda atau memberi hukuman kepada pengendali dan pengolah data atas ketidakpatuhan mereka saat peraturan baru ini telah berlaku. Sederhananya, setiap organisasi (lokal atau internasional) yang melakukan bisnis di Eropa atau menangani data pribadi warga Uni Eropa harus mematuhi aturan yang baru.

Untuk pelanggaran yang paling merusak karena ketidakpatuhan terhadap ketentuan-ketentuan utama, regulator berwewenang untuk memungut denda hingga sebesar € 20 juta atau 4 persen dari omset tahunan global perusahaan pada tahun sebelumnya. Terdapat pendekatan berjenjang terhadap denda (misalnya, perusahaan dapat didenda 2 persen karena tidak memiliki catatan sesuai ketentuan [Pasal 28], tidak memberi tahu otoritas pengawas dan subjek pemilik data tentang adanya pelanggaran, atau tidak melakukan penilaian dampak atas pelanggaran). Penting untuk dicatat bahwa aturan ini berlaku untuk pihak pengendali dan pengolah - yang berarti bahwa server *cloud* tidak akan dikecualikan dari penerapan GDPR. Contoh lain yang termasuk dalam kategori ini adalah ketidakpatuhan terhadap prinsip-prinsip inti pemrosesan data pribadi, pelanggaran hak-hak subyek pemilik data, dan transfer data pribadi ke negara ketiga atau organisasi internasional yang tidak menjamin tingkat perlindungan data yang memadai. (lihat The EU General Data Protection Regulation).

Pelanggaran atas Data 2017		
Bulan	**Organisasi**	**Pelanggaran / Pembobolan**
8 Januari 2017	E-Sports Entertainment Association (ESEA)	1.503.707 catatan ditambahkan ke database dan rekaman yang bocor termasuk informasi pribadi.
2 Februari 2017	ISO Xbox 360 dan ISO PSP	1,2 juta pengguna Xbox 360 ISO dan 1,3 juta PSP ISO terpengaruh;informasi pribadi dicuri.
15 Maret 2017	Dun & Bradstreet	Lebih dari 33 juta kontak perusahaan dibagikan di web, termasuk Departemen Pertahanan AS dan Layanan Pos AS; informasi pribadi bocor.
6 April 2017	FAFSA: Alat Pengambilan Data IRS	Hingga 100.000 pembayar pajak / pelajar mungkin memiliki informasi pribadi yang dicuri.
10 Mei 2017	Pusat Rumah Sakit Bronx Lebanon	Setidaknya 7.000 pasien antara 2014 dan 2017 mungkin memiliki informasi pribadi yang sangat dibahayakan, termasuk kecanduan, diagnosis kesehatan mental dan medis, status HIV, dan laporan adanya seranga.
20 Juni 2017	Deep Root Analytics	Sekitar 198 juta warga Amerika terkena dampak, saat Deep Root Analytics, yang disewa oleh *Republican National Committee* , menyimpan informasi pribadi di server cloud tanpa perlindungan kata sandi, diekspos selama lebih dari dua minggu.
13 Juli 2017	Verizon	14 juta informasi pelanggan terpapar karena catatan disimpan di server yang tidak aman; data yang diperoleh adalah file *log* (catatan), yang dihasilkan ketika pelanggan menghubungi Verizon melalui telepon.
30 Agustus 2017	Online Spambot	711 juta alamat email dan kata sandi diambil dari server yang tidak diamankan.
7 September 2017	Equifax	143 juta pelanggan mungkin terpengaruh karena peretas mengeksploitasi titik lemah dalam perangkat lunak situs web; informasi pribadi terpapar, termasuk nomor jaminan sosial dan nomor kartu kredit.
12 Oktober 2017	Hotel Hyatt	Akses tidak sah ke informasi pembayaran untuk kartu debit dan kredit, termasuk nomor kartu kredit, kode verifikasi internal, dan nama pemegang kartu yang digunakan (digesek) di 41 hotel di 11 negara.
21 November 2017	Uber	Informasi pribadi dari 57 juta pengemudi dan pelanggan yang terpapar, termasuk nama, alamat email, dan nomor telepon.
10 Desember 2017	TIO Networks (PayPal)	Lebih dari 1,6 juta identitas pelanggan dibahayakan, termasuk informasi rekening bank, informasi kartu pembayaran, kata sandi, nama pengguna, dan nomor jaminan sosial.

Diadaptasi dari: 2017 Data Breaches – The Worst So Far

Fokus Audit

IIA Standard 2120: Manajemen Risiko

Kegiatan audit internal harus mengevaluasi efektivitas dan berkontribusi pada peningkatan proses manajemen risiko.

2120.A1 - Kegiatan audit internal harus mengevaluasi eksposur risiko yang berkaitan dengan tata kelola organisasi, operasi, dan sistem informasi terkait:

- Pencapaian tujuan strategis organisasi.
- Keandalan dan integritas informasi keuangan dan operasional.
- Efektivitas dan efisiensi operasi dan program.
- Pengamanan aset.
- Kepatuhan dengan hukum, peraturan, kebijakan, prosedur, dan kontrak.

Bahkan definisi dan ketentuan "persetujuan" sangat dibatasi. Sebelumnya, pengendali data diizinkan untuk berpegangan pada persetujuan implisit dan persetujuan "opt-out" dalam beberapa keadaan. Pada 25 Mei 2018, GDPR memperkuat persyaratan untuk persetujuan, dan perusahaan tidak akan lagi dapat menggunakan syarat dan ketentuan yang tidak terbaca panjang yang dipenuhi bahasa hukum, karena permintaan persetujuan harus diberikan dalam bentuk yang mudah diakses, dengan tujuan untuk mengijinkan pengolahan data yang melekat atas persetujuan itu. Persetujuan harus jelas dan dapat dibedakan dari hal-hal lain dan disediakan dalam bahasa yang jelas dan sederhana. Membatalkan persetujuan yang telah diberikan harus sama mudahnya dengan memberikannya. Selanjutnya, setelah persetujuan ditarik, subyek data memiliki hak untuk menghapus data pribadi mereka dan tidak lagi digunakan untuk pemrosesan (lihat The Top 10 Operational Impacts of the EU's General Data Protection Regulation).

GDPR akan secara signifikan mempengaruhi upaya *cybersecurity* Jerman. Pada bulan Mei 2017 badan legislatif mengadopsi versi revisi dari Undang-undang Perlindungan Data Federal, yang akan berlaku bersamaan dengan EU GDPR pada 25 Mei 2018. Dikenal dengan undang-undang perlindungan data nasional yang kuat, dengan denda hingga € 300.000, Jerman adalah sekarang bergerak menuju standar *cybersecurity* yang ketat dan menetapkan tanggung jawab kepada penyedia layanan dan operator infrastruktur penting untuk melindungi pengguna dan mengamankan informasi *cyber.* Undang-undang baru itu berisi 85 ketentuan, beberapa di antaranya mengacu pada EU GDPR. Operator infrastruktur penting harus menerapkan pengamanan organisasi dan teknis yang tepat dan langkah-langkah lain yang diperlukan sesuai dengan keadaan terkini dalam waktu dua tahun setelah berlakunya undang-undang sekunder yang menetapkan kerangka pengaman tersebut. Selain itu, operator infrastruktur penting harus secara teratur membuktikan bahwa mereka memenuhi persyaratan keamanan, dan memberitahu *Bundesamt für Sicherheit in der Informationstechnik* (BSI) segera atas setiap gangguan signifikan dari ketersediaan, integritas, keaslian, dan kerahasiaan sistem TI mereka, komponen, dan proses, yang dapat mengakibatkan atau telah mengakibatkan kegagalan atau kerusakan fungsi infrastruktur penting yang dioperasikan oleh mereka (lihat What You Need to Know About Germany's Cybersecurity Law).

Meskipun China telah memiliki undang-undang, aturan, dan peraturan yang ketat terkait dengan keamanan informasi, China memperkenalkan undang-undang menyeluruh yang menjembatani kesenjangan antara keamanan *cyber* dan perlindungan data (berlaku mulai Juni 2017), yang menggabungkan ketentuan GDPR UE. Dalam banyak hal, Hukum *Cyber Security* Republik Rakyat Cina (HCS) sesuai dengan GDPR (lihat Risk in Focus: Hot Topics For Internal Audit 2018). HCS membuat amandemen yang lebih memperhatikan perlindungan informasi pribadi dan privasi individu, dan menstandardisasi pengumpulan dan penggunaan informasi pribadi. Misalnya, sebelumnya perusahaan asing dapat memindahkan informasi keluar China, namun sekarang, undang-undang menetapkan bahwa data sensitif harus disimpan di dalam negeri, dan ada hukuman yang kuat atas pelanggaran hukum, termasuk penangguhan kegiatan bisnis. Denda dapat mencapai RMB1.000.000. (Untuk detail tambahan, lihat "Amandemen untuk HCS," halaman berikutnya.)

Amandemen untuk HCS

Pasal	Versi akhir	Amandemen Signifikan
31	Mengenai perlindungan keamanan *cyber*, negara menekankan perlindungan infrastruktur informasi penting dalam ***komunikasi publik dan layanan informasi, energi, keuangan, transportasi, konservasi air, layanan publik dan e-governance*** , serta infrastruktur informasi penting lainnya yang dapat menyebabkan kerusakan serius terhadap keamanan nasional, ekonomi nasional dan kepentingan publik jika hancur, fungsionalitas hilang, atau data bocor.	Artikel ini menjelaskan industri dan sektor di mana perlindungan infrastruktur informasi kritis akan diberikan prioritas.
43	Individu memiliki hak untuk meminta operator jaringan untuk memperbaiki kesalahan dalam informasi pribadi yang dikumpulkan atau disimpan oleh mereka. ***Operator jaringan harus mengambil langkah-langkah untuk menghapus atau memperbaiki kesalahan.***	Artikel ini memberi warga hak yang lebih besar untuk melindungi informasi pribadi mereka, dan meningkatkan kewajiban operator jaringan untuk memperbaiki kesalahan secara tepat waktu.
46	Individu atau organisasi ***bertanggung jawab atas penggunaan jaringan mereka*** , dan tidak boleh membuat situs web atau grup komunikasi untuk tujuan penipuan atau kegiatan ilegal lainnya.	Artikel ini menekankan bahwa individu dan organisasi memikul tanggung jawab untuk penggunaan jaringan mereka.
76 (5)	"Informasi pribadi" mengacu pada semua jenis informasi, dicatat secara elektronik atau melalui cara lain, yang dapat menentukan identitas orang natural secara mandiri atau dalam kombinasi dengan informasi lain, termasuk, tetapi tidak terbatas pada, nama ***orang natural*** , tanggal lahir, nomor identifikasi, informasi biometrik pribadi, alamat, dan nomor telepon.	Artikel ini memperluas cakupan perlindungan informasi pribadi dari "warga negara" ke "orang-orang natural".
63	Orang yang melanggar Pasal 27 undang-undang dan terlibat dalam kegiatan yang membahayakan *cybersecurity* dapat ditahan selama 5 hingga 15 hari dan dapat didenda ***RMB100.000 – RMB1.000.000*** , tergantung pada tingkat keparahan kasus tersebut.	Hukuman maksimum karena melanggar Undang-Undang Keamanan Siber telah ditingkatkan menjadi RMB1.000.000.

Sumber: Overview of China's Cybersecurity Law

Tapi HCS juga memiliki pihak oposisi. Seperti dilansir The New York Times pada Mei 2017, "sebuah koalisi kelompok lobi bisnis yang mewakili perusahaan Eropa, Amerika, dan Asia meminta China untuk menunda penerapan hukum, sementara Kamar Dagang Uni Eropa di China meminta waktu tambahan untuk memungkinkan perusahaan untuk mematuhi karena 'kewajiban kepatuhan yang substansial. "

Melakukan bisnis di Uni Eropa, Cina, atau sejumlah negara lain dengan peraturan yang semakin meningkat mengenai privasi data, organisasi merasakan dampaknya. Dewan mendorong peningkatan kerangka kerja tata kelola dalam organisasi mereka, dan dewan didorong oleh regulator, investor, dan pemangku kepentingan lainnya yang meminta pertanggungjawaban mereka atas efektivitas proses mereka secara keseluruhan (lihat Of Corporate Governance, Risk Management, and Internal Audit). Peraturan baru meningkatkan biaya dan memberi tekanan pada organisasi dengan menambahkan kompleksitas manajemen risiko, pengendalian, dan proses tata kelola organisasi.

Ketika tekanan pada Dewan meningkat, tekanan juga dilakukan pada audit internal. Organisasi melihat audit internal dengan harapan besar. Mereka mengakui perlunya audit internal untuk memberikan saran dan asurans ketika

Fokus Audit

IIA Standard 2210: Tujuan Penugasan

Tujuan harus ditetapkan untuk setiap penugasan.

2210.A3 - Kriteria yang memadai diperlukan untuk mengevaluasi tata kelola, manajemen risiko, dan pengendalian. Auditor internal harus memastikan sejauh mana manajemen dan / atau Dewan telah menetapkan kriteria yang memadai dalam menentukan apakah tujuan dan sasaran telah tercapai.Jika memadai, auditor internal harus menggunakan kriteria tersebut dalam evaluasi mereka. Jika tidak memadai, auditor internal harus mengidentifikasi kriteria evaluasi yang tepat melalui diskusi dengan manajemen dan / atau Dewan.

IIA Standard 2050: Koordinasi dan Kebergantungan

Chief Audit Executive harus berbagi informasi, mengkoordinasikan kegiatan, dan mempertimbangkan untuk bergantung pada pekerjaan dari penyedia layanan asurans eksternal dan internal serta layanan konsultansi lainnya untuk memastikan cakupan yang memadai dan meminimalkan duplikasi upaya.

mereka mengalihkan kekuatan disruptif menjadi peluang, sementara pada saat yang sama tetap mematuhi perubahan konstan dalam peraturan (lihat KPMG Internal Audit: Top 10 Key Risks in 2016).

Kunci untuk bertahan dari kekuatan disruptif adalah pencapaian tata kelola, manajemen risiko, kepatuhan terhadap peraturan, dan keseimbangan kinerja. Dengan memenuhi tantangan ini, organisasi dapat melindungi dan meningkatkan nilai bisnis dan mendorong efisiensi operasional.

Tujuan

- Klarifikasi atas *risk appetite* saat mengevaluasi proyek dan strategi.
- Kesadaran seluruh organisasi dari peraturan nasional dan internasional saat ini.
- Menetapkan langkah-langkah untuk mematuhi peraturan nasional dan internasional saat ini.
- Adanya koordinasi penyedia jasa asurans internal dan eksternal.

Tindakan

- Memahami kerangka kerja kepatuhan dan standar asurans internasional.
- Melakukan inventarisasi atas badan regulator yang ada dan ketentuannya.
- Menilai pendekatan organisasi dalam mengelola kegiatan kepatuhan globalnya, termasuk integrasi organisasi yang baru saja diakuisisi.
- Mengevaluasi tanggapan organisasi terhadap kondisi-kondisi penting atas ketidakpatuhan.
- Meninjau program pelatihan kepatuhan, dan evaluasi kelayakan untuk masing-masing peran.
- Berkoordinasi dengan penyedia asurans internal dan eksternal untuk memastikan cakupan yang memadai dan meminimalkan duplikasi upaya.
- Membangun komunikasi yang disesuaikan dengan kepentingan dan prioritas organisasi untuk mendorong budaya kepatuhan.
- Evaluasi pembagian tanggung jawab organisasi demi kepatuhan terhadap regulasi.

Merespon Gangguan (Disrupsi)

Hari baru - lonceng baru, peluit baru. Teknologi saat ini selalu berubah; perubahan itu lebih cepat, lebih kuat, lebih besar (atau lebih kecil); perubahan teknologi mencapai lebih jauh dan lebih intens. Hal ini belum pernah terjadi sebelumnya. Setiap hari auditor internal dihadapkan pada peluang baru dalam memberikan wawasan dan pandangan ke depan kepada para pemangku kepentingan, namun auditor mungkin saja belum mengembangkan keterampilan terkait dengan inovasi seperti pemikiran kritis dan kreativitas. Akibatnya, tanpa inovasi, auditor tidak mampu menangani hal-hal yang belum diperkirakan serta rentan terhadap kepuasan diri. Auditor internal harus menyesuaikan metodologi mereka untuk memanfaatkan teknologi - untuk menjadi lincah dan proaktif, serta dengan cepat mengubah arah seiring dengan inovasi inovasi.

Inovasi, seperti teknologi baru, menawarkan peluang besar pada audit internal dalam melaksanakan penugasan audit, dalam banyak contoh, inovasi disertai dengan risiko, ancaman, dan disrupsi baru, yang menuntut perhatian audit internal. Misalnya, alih-alih (secara tradisional) hanya berfokus pada risiko, auditor internal saat ini harus dapat dengan cepat mengidentifikasi kemungkinan disrupsi dan menentukan mana yang memerlukan perhatian langsung atau tambahan.

Salah satu alasan utama organisasi harus berinovasi adalah untuk memisahkan diri dari kompetisi - dan audit internal dapat memimpin upaya tersebut. Menurut Pulse of Internal Audit Amerika Utara 2018, inovasi memberikan dua pilihan kepada audit internal yaitu: menyempurnakan kemampuannya dalam mengisi peran yang semakin penting dalam suatu organisasi, atau mempertahankan praktik masa lalu dan membawanya ke masa depan. Yang kedua hamper menjamin kegagalan di masa depan; oleh karena itu, audit internal harus terbuka terhadap ide-ide kreatif (atau bahkan radikal), serta siap dan bersedia untuk berfokus pada manajemen risiko terkait yang efektif.

Akan ada berbagai tantangan. Manajemen bisa saja tidak nyaman membayangkan akan melakukan sesuatu secara berbeda; anggaran mungkin dibatasi oleh lingkungan bisnis, dan kandidat yang tersedia mungkin kurang memadai saat dibutuhkan keterampilan tertentu. Tetapi kabar baiknya adalah audit internal tidak sendirian. Audit internal dapat belajar dari unit bisnis lain, organisasi, atau aktivitas audit internal lain yang telah mengembangkan teknik khusus untuk mengelola proses inovasi.

Inovasi - saat dihadapi dengan benar - sangat berharga untuk audit internal dan seluruh organisasi:

- Biaya dapat dikurangi.
- Nilai dapat ditingkatkan.
- Pertumbuhan dan peningkatan kinerja dapat direalisasikan.
- Produk dan layanan dapat diluncurkan lebih cepat.
- Pengalaman dan kepuasan pelanggan dapat ditingkatkan.
- Fleksibilitas dan kelincahan organisasi menjadi diperkuat.
- Kepuasan para pemangku kepentingan semakin meningkat.

Inovasi tidak hanya mengarahkan pada praktik audit yang lebih baik dan lebih efisien, namun inovasi juga secara langsung dapat mendukung kelincahan auditor dengan memungkinkan respons yang lebih cepat, lebih cerdas, dan lebih terfokus terhadap disrupsi (lihat 2018 North American Pulse of Internal Audit: The Internal Audit Transformation Imperative). Ketua IIA dari Dewan Amerika Utara, Shannon Urban, mendorong inovasi dalam audit internal karena sangat penting bagi pertumbuhan internal audit dan diperlukan dalam memenuhi kebutuhan pemangku kepentingan yang selalu berubah. Hal ini mungkin sedikit tidak mengenakan dan membuat frustrasi, namun hal ini sedang berlangsung, serta menuntut komitmen dan keberanian. Inovasi juga bisa sangat bermanfaat. Jika audit internal ingin memahami pemangku kepentingannya, dan melayani mereka dengan baik di masa depan, berinovasi adalah satu-satunya pilihan (lihat The Innovative Internal Auditor).

"Saya sangat percaya bahwa audit internal memiliki peran penting untuk dimainkan dalam mencapai keberhasilan organisasi kami. Tetapi saya juga percaya bahwa untuk dapat melakukan tugas itu, kami perlu menyegarkan kembali komitmen kami terhadap inovasi dalam audit internal. Inovasi harus menjadi inti dari audit internal jika ingin mengikuti perkembangan organisasi kita sendiri dan seterusnya."

Shannon Urban, Ketua
Dewan IIA Amerika Utara
(2017 – 2018)

Sumber: Internal Auditor

Tujuan

- Audit internal menyadari perubahan dalam lingkungan bisnis.
- Audit internal bertujuan untuk mengembangkan budaya inovasi, serta memperkuat kemampuan dan kinerja.
- Audit internal bertujuan untuk menerapkan praktik terbaik dan upaya perbaikan melalui inovasi.
- Audit internal berusaha untuk lebih efisien melalui inovasi.

Tindakan

- Merancang dan mengimplementasikan ide-ide baru, membuat inovasi menjadi landasan inti atas praktik audit internal.
- Mengambil peran pemimpin, mengantisipasi gangguan bisnis, memantau perubahan pada lingkungan, dan menawarkan respon yang lebih komprehensif.
- Membangun dan berinvestasi dalam hubungan. Tetap terhubung dengan lingkungan bisnis dan menyadari inovasi yang terjadi.
- Mengklarifikasi lanskap risiko yang sedang berkembang dengan menentukan gangguan mana yang memerlukan perhatian tambahan.
- Memberikan wawasan dan sudut pandang seputar risiko yang muncul atas peristiwa disruptif.
- Mendapatkan kandidat dengan kompetensi yang tepat untuk secara cepat dan tegas menanggapi risiko baru maupun yang sedang berkembang.
- Berkolaborasi dengan fungsi manajemen risiko dan kepatuhan lainnya.

Pemikiran Penutup

Risiko yang disoroti dalam laporan ini - diidentifikasi sebagai bidang perhatian utama oleh afiliasi global IIA - tidak mewakili semua risiko yang dihadapi organisasi atau audit internal. Selain bidang-bidang ini, afiliasi global IIA juga mengidentifikasi risiko yang melekat pada komite audit, anggaran, *lines of defences*, dan strategi – setiap area penting dari tata kelola organisasi yang perlu dipahami dan diperiksa. Risiko membuka pintu kegagalan dalam pencapaian misi organisasi dan tujuan strategis, dan mengancam nilai organisasi secara keseluruhan. Oleh karena itu, tanggung jawab audit internal - sebagai penasihat tepercaya untuk membantu manajemen risiko, pengendalian, dan proses tata kelola organisasi - membutuhkan pertimbangan semua peluang adanya risiko dan membuat rekomendasi yang tepat.

Di seluruh dunia, organisasi bergantung pada audit internal, dan penilaiannya. Agar tetap relevan dan diakui sebagai penasihat terpercaya, audit internal memiliki kewajiban untuk memperhatikan risiko terhadap pencapaian tujuannya, serta tujuan organisasi. Karena itu, audit internal harus berfokus pada hasil dan berkomitmen untuk meningkatkan kemampuannya demi kepentingan organisasi secara keseluruhan. Hal ini membutuhkan kemampuan dalam mengatasi tantangan dan rintangan, termasuk kemampuan berpikir kritis; tetap independen dan obyektif; tetap gesit; berfokus pada kepemimpinan terhadap pengelolaan risiko – baik nyata maupun khayalan; menavigasi "waktu" dengan berfungsi sebagai konsultan saat diperlukan; memberikan jasa asurans apabila diperlukan; dan memahami interdependensi seluruh sistem, proses, regulasi, dan operasi.

Afiliasi IIA Global

Afiliasi IIA merupakan pilar-pilar bangunan IIA. IIA bermitra dengan Afiliasi IIA di lebih dari 170 negara dan wilayah untuk memenuhi misinya dalam memajukan profesi audit internal dan melayani lebih dari 190.000 anggota secara global. Afiliasi IIA berfungsi sebagai perwakilan eksklusif IIA yang secara kolektif membawa suara profesi audit internal yang mempromosikan standar etika dan praktik profesional yang tinggi di komunitas audit internal mereka.

Tentang IIA

Institute of Internal Auditor (IIA) adalah advokat, pendidik, dan penyedia standar, panduan, dan sertifikasi profesi audit internal yang paling banyak dikenal. Didirikan pada tahun 1941, IIA saat ini melayani lebih dari 190.000 anggota dari lebih dari 170 negara dan teritori. Kantor pusat global IIA berada di Lake Mary, Florida, AS. Untuk informasi lebih lanjut, kunjungi www.globaliia.org.

Disclaimer

Pendapat yang diungkapkan dalam Perspektif dan Pandangan Global belum tentu merupakan kontribusi masing-masing kontributor atau pemberi kontribusi.

Hak Cipta

The Institute of
Internal Auditors

globaliia.org