

# PERSPEKTIF DAN PANDANGAN GLOBAL

Audit internal dan kepatuhan:  
Kejelasan dan kolaborasi  
untuk tata kelola yang lebih kuat



The Institute of  
**Internal Auditors**

## Dewan Penasihat

Nur Hayati Baharuddin, CIA, CCSA, CFSa, CGAP, CRMA –  
Member of IIA–Malaysia

Lesedi Lesetedi, CIA, QIAL –  
African Federation IIA

Karem Obeid, CIA, CCSA, CRMA –  
Member of IIA–United Arab  
Emirates

Carolyn Saint, CIA, CRMA, CPA –  
IIA–North America

Ana Cristina Zambrano Preciado,  
CIA, CCSA, CRMA –  
Member of IIA–Colombia

## Terbitan Sebelumnya

Untuk mengakses terbitan  
Perspektif dan Pandangan Global,  
kunjungi [www.theiia.org/GPI](http://www.theiia.org/GPI).

## Tanggapan Pembaca

Kirimkan pertanyaan dan saran  
via [globalperspectives@theiia.org](mailto:globalperspectives@theiia.org).

# Daftar Isi

Pendahuluan.....	1
Akuntabilitas, Tindakan, dan Asurans.....	2
Apa itu Kepatuhan? .....	2
Kepatuhan sebagai hasil .....	3
Kepatuhan sebagai kategori risiko .....	3
Kepatuhan sebagai peran atau departemen organisasi ..	3
Kepatuhan sebagai serangkaian kegiatan.....	4
Model Tiga Lini:.....	5
Kepatuhan .....	5
Menentukan tanggung jawab untuk peran dan aktivitas kepatuhan .....	5
Upaya kolektif untuk mencapai kepatuhan .....	6
Menerapkan Enam Prinsip.....	8
Fakta-Fakta Utama tentang Kepatuhan.....	17
Sepuluh hal penting untuk dicatat:.....	17
SUPLEMEN: Menyelaraskan Tanggung Jawab untuk Peran dan Aktivitas Kepatuhan.....	19

Diterjemahkan dan diselaraskan oleh volunteer IIA Indonesia:

1. Dewi Andriati, CIA, CRMA
2. I Made Suandi Putra, CIA, CRMA
3. Diana Laurencia Sidauruk
4. Fauzan Wahyuabdi Pratama, CIA, CGAP

## Ucapan Terima Kasih

IIA berterima kasih kepada anggota dan pemangku kepentingan yang berkontribusi pada makalah ini, termasuk Mark Carawan, Caroline Maurice, Vandana Siney, Karen Brady, Benito Ybarra, Mike Joyce, Stacey Schabel, Mani Sulur, Jee Kymm, Dana Lawrence, Geoff Rusnak, Paul Ricci, Senthil Kumar, Marta Budavari, Kathryn Reimann, Emily Wright, Akash Singh, Nora Ilmoni, Christine Ong, Calum Owen, Trygve Sorlie, Francis Nicholson, Jill Austin, and IIA – Australia.

## Tentang IIA

Institute of Internal Auditor (IIA) adalah advokat, pendidik, dan penyedia standar, panduan, dan sertifikasi profesi audit intern yang paling banyak dikenal. Didirikan pada tahun 1941, IIA saat ini melayani lebih dari 200.000 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](http://www.globaliia.org).

## Penafian

Perspektif dan Pandangan Global tidak mewakili pendapat pribadi kontributor atau organisasi dimana kontributor bekerja..

## Hak Cipta

Hak Cipta © 2021 oleh The Institute of Internal Auditors, Inc. Hak cipta dilindungi.

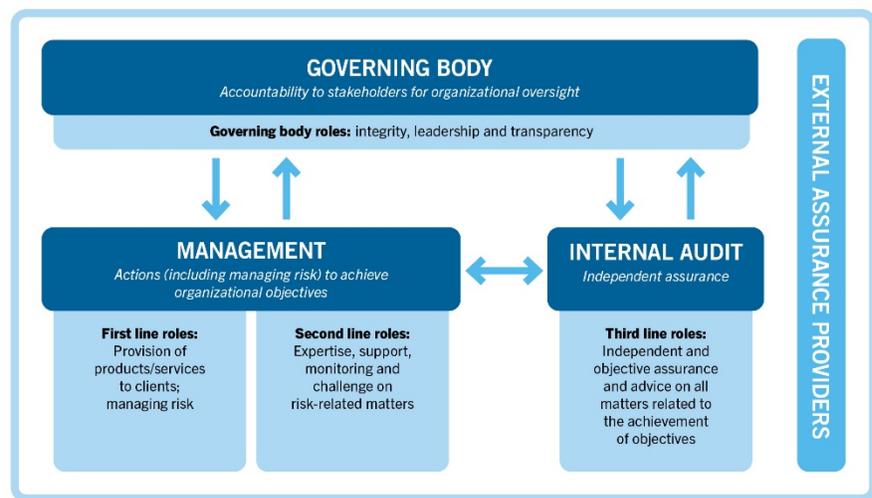
# Pendahuluan

Hubungan antara audit internal dan kepatuhan terkadang tidak jelas, sehingga menimbulkan pertanyaan penting: Dapatkah audit internal bertanggung jawab atas kepatuhan? Apakah fungsi kepatuhan bertanggung jawab atas semua kepatuhan di seluruh organisasi? Sebagai Kepala Audit Eksekutif (CAE), apakah boleh bertanggung jawab atas kepatuhan?

Makalah ini dirancang untuk membantu memperjelas kompleksitas ini dan menghindari kebingungan, kesenjangan, dan duplikasi yang tidak perlu. Yang jelas sangat penting untuk dipahami, kolaborasi sangat dianjurkan, dan independensi audit internal<sup>1</sup> pada dasarnya penting.

Ini bukan makalah tentang cara mengaudit kepatuhan. Tetapi, makalah ini berfungsi sebagai alat bagi Dewan Pengurus (*Board*), manajemen, profesional kepatuhan, dan Kepala Audit Eksekutif (*Chief Audit Executives/CAE*), dan penggunaan [Model Tiga Lini](#) untuk menjelaskan hubungan audit internal dan kepatuhan. Enam Prinsip *Model Tiga Lini* dan cara penerapan prinsip tersebut pada kepatuhan akan dibahas secara mendalam

dalam makalah ini. Pembaca harus menggunakan makalah ini untuk mengidentifikasi, memahami, mengevaluasi, dan menerapkan dengan jelas dalam struktur tata kelola — terlepas dari yurisdiksi, industri, kompleksitas, maturitas, atau ukuran — kepatuhan yang efektif dan manajemen risiko kepatuhan dalam berbagai aspeknya terkait dengan Model Tiga Lini<sup>2</sup>. Ilustrasi praktis dari pejabat-pejabat terkait risiko dan kepatuhan serta auditor internal, tentang masalah kepatuhan yang dihadapi di lapangan akan membantu penerapan praktis dari Enam Prinsip saat mengevaluasi keselarasan aktivitas kepatuhan dengan Model Tiga Lini. (Lihat halaman 8-16).



Copyright © 2020 by The Institute of Internal Auditors, Inc. All rights reserved.

<sup>1</sup> Sifat integral dari kepatuhan sebagai bagian dari tata kelola yang berkelanjutan adalah fokus utama dan tindakan kebijakan yang direkomendasikan oleh B20 Italia kepada para menteri G20 pada [B20 Italy Integrity & Compliance Policy Paper 2021](#). Secara khusus, Tindakan Kebijakan 2.1 pada hal. 11 secara khusus menyebutkan peran audit internal seperti yang dijelaskan dalam Model Tiga Lini.

<sup>2</sup> Di yurisdiksi dan industri tertentu, peran dan tanggung jawab yang terkait dengan kepatuhan dan manajemen risiko kepatuhan sangat ditentukan oleh dan menjadi subjek dari undang-undang, regulasi, kasus hukum, dan penelitian akademis yang ekstensif. Studi yang lebih rinci tersedia, dan pengguna makalah praktis ini didorong untuk berkonsultasi dengan mereka. Misalnya, lihat dari American Law Institute, *Principles of the Law, Compliance, Risk Management, and Enforcement* [No. 1](#) and *Principles of the Law, Compliance and Enforcement* [No. 2](#)

# Akuntabilitas, Tindakan, dan Asurans

Model Tiga Lini menjelaskan bagaimana akuntabilitas Badan Pengurus, tindakan oleh manajemen, dan asurans independen oleh audit internal memberikan fondasi bagi tata kelola yang efektif. Ini juga menunjukkan bagaimana Enam Prinsip membantu dalam evaluasi peran dan tanggung jawab masing-masing dalam sebuah organisasi. Penerapan elemen inti dari model dan Enam Prinsip bervariasi di setiap organisasi, tergantung dari tujuan, sumber daya, dan keadaannya. Model ini membantu organisasi mengidentifikasi struktur, proses desain, dan menetapkan tanggung jawab yang paling sesuai dalam membantu pencapaian tujuan. Ini termasuk pengelolaan risiko kepatuhan, yang merupakan tanggung jawab manajemen<sup>3</sup> tetapi dicapai melalui upaya kolaboratif.

Syarat-syarat kepatuhan dan ekspektasinya perlu dipertimbangkan oleh organisasi yang berasal dari eksternal, seperti undang-undang, aturan, dan peraturan, dan yang berasal dari internal, seperti kebijakan perusahaan, standar, prosedur, dan kode etik atau perilaku. Hal-hal tersebut mungkin secara formal dan eksplisit didefinisikan atau lebih implisit, seperti ekspektasi sosial, etika, dan budaya. Spektrum pertimbangan yang luas dan dinamis ini disebut dalam makalah ini sebagai “persyaratan dan ekspektasi.”

Pemangku kepentingan mengharapkan organisasi untuk memenuhi tujuannya dan memaksimalkan nilai secara legal dan etis. Sejalan dengan itu, organisasi melakukan investasi dalam memantau kepatuhan secara ketat di bidang-bidang utama seperti kesehatan dan keselamatan kerja; tenaga kerja; perlindungan data dan privasi; badan hukum dan hukum serta norma komersial/perdagangan; peraturan tiap sektor; standar kualitas; anti suap dan anti korupsi; perlindungan investor dan konsumen; pelaporan keuangan dan perpajakan; dan kode etik individu. Daftarnya masih banyak lagi. Kepatuhan dapat dipahami dan dilakukan dalam konteks akuntabilitas, tindakan, dan asurans, seperti yang dijelaskan dalam Model Tiga Lini, sebagai bagian dari pendekatan menyeluruh atas tata kelola yang efektif.

## Apa itu Kepatuhan?

Organisasi harus mematuhi peraturan perundang-undangan yang berlaku dan persyaratan eksternal lainnya yang merupakan prasyarat dalam menjalankan bisnis. Persyaratan kepatuhan ini mencakup berbagai hal, mulai dari hubungan karyawan hingga pembayaran pajak. Dalam industri tertentu terdapat berbagai badan pembuat aturan, pengawas, regulator, dan persyaratan yang ditetapkan, tetapi sektor lainnya memiliki lebih sedikit batasan dan aturan hukum serta peraturan eksternal. Namun demikian, sangat jarang ada organisasi baik di sektor publik atau swasta yang tidak memiliki persyaratan kepatuhan eksternal sama sekali.

Pada saat yang sama, organisasi merancang, mengembangkan, dan mengimplementasikan ekspektasi internal organisasi dalam bentuk kebijakan dan prosedur serta menetapkan standar untuk tindakan dan perilaku etis. Dalam industri tertentu, persyaratan eksternal mengharuskan organisasi untuk menetapkan dan menerapkan suatu kebijakan internal, standar, dan kode perilaku. Dengan persyaratan yang berlapis-lapis ini, konsep "kepatuhan" dalam sebuah organisasi memiliki sejumlah dimensi. Oleh karena itu, penting untuk mempertimbangkan kepatuhan dalam aspek yang luas, berkaitan, namun dapat berbeda-beda, dan

---

<sup>3</sup> Untuk tujuan makalah ini, istilah *manajemen* secara luas digunakan untuk mengidentifikasi peran yang bukan merupakan tanggung jawab badan pengurus atau audit internal.

bagaimana hal itu dibahas dalam organisasi: Sebagai hasil; Sebagai kategori risiko<sup>4</sup>; Sebagai peran organisasi, departemen, fungsi, dll<sup>5</sup>; dan sebagai rangkaian kegiatan.

Masing-masing dibahas di bawah ini.

## Kepatuhan sebagai hasil

Organisasi melakukan berbagai aktivitas untuk mematuhi peraturan perundang-undangan, aturan, kebijakan, kode, dll., atau "patuh". Mencapai persyaratan dan ekspektasi kepatuhan tertentu seringkali merupakan kondisi yang diperlukan untuk beroperasi dan mengejar tujuan strategis.

## Kepatuhan sebagai kategori risiko

Kerangka Praktik Profesional Internasional IIA mendefinisikan risiko sebagai kemungkinan bahwa suatu peristiwa akan terjadi, yang akan berdampak pada pencapaian tujuan organisasi. Dampak tersebut dapat menguntungkan atau merugikan. Oleh karena itu, ketika menilai risiko, penting untuk mempertimbangkan persyaratan dan ekspektasi kepatuhan bersama dengan kemungkinan ketidakpatuhan dan potensi dampaknya terhadap tujuan.

Ada risiko bagi organisasi yang terkait dengan kepatuhan dan ketidakpatuhan. Dampaknya mungkin dalam bentuk penghargaan atau hukuman, dalam bentuk berwujud maupun tidak berwujud. Kepatuhan dengan standar *International Organization for Standardization* (ISO), misalnya, dirancang untuk menciptakan efisiensi operasional dan keuntungan lain serta perhatian yang menguntungkan, yang diperoleh apabila mengikuti standar yang tidak diwajibkan (sukarela). Ketidakpatuhan menghilangkan keuntungan positif tersebut, dan dapat mengakibatkan kerugian secara langsung serta menimbulkan hukuman seperti pengenaan denda, pencabutan izin, sanksi, penghentian operasi, tuntutan perdata atau pidana, dan hilangnya dana atau dukungan. Selain itu, ketidakpatuhan dapat menyebabkan risiko reputasi dalam bentuk potensi ketidakpuasan pemangku kepentingan, kritik publik, atau kerusakan lainnya.

Identifikasi, pengukuran, dan penilaian risiko kepatuhan serta penentuan selera dan toleransi risiko kepatuhan membantu menentukan respons yang tepat, termasuk kebijakan, prosedur, batasan, dan pengendalian.<sup>6</sup>

## Kepatuhan sebagai peran atau departemen organisasi

Seringkali, kepatuhan juga digunakan untuk merujuk pada peran atau departemen yang dibentuk untuk memenuhi persyaratan dan ekspektasi tertentu atau memberikan pengawasan, keahlian, pemeriksaan dan tantangan, pemantauan, pengujian, atau asurans tentang hal-hal yang terkait dengan kepatuhan. Ini adalah karakteristik dari berbagai peran lini pertama atau kedua seperti yang dijelaskan dalam Model Tiga Lini.

---

<sup>4</sup> Di bawah kategori kepatuhan dalam suatu organisasi yang luas, taksonomi risiko mengidentifikasi turunan dari subkategori terkait risiko spesifik dan risiko yang berhubungan dengan undang-undang, aturan, peraturan, kebijakan, atau perilaku.

<sup>5</sup> Peran dapat diartikan mencakup risiko spesifik, seperti petugas risiko perilaku, petugas risiko perlindungan data, dll.

<sup>6</sup> *Committee of Sponsoring Organizations of the Treadway Commission* ([COSO](#)) memberikan kerangka kerja untuk manajemen risiko, dan kepemimpinan pemikiran, termasuk panduan baru tentang penerapan kerangka kerja risiko ERM untuk pengelolaan risiko kepatuhan.

Peran atau departemen ini tetap berada dalam lingkup keseluruhan dan tanggung jawab dari manajemen dan, tergantung pada karakteristik spesifik dari peran tersebut, berpotensi menawarkan dukungan spesialis dan manajemen risiko kepada mereka yang memiliki peran lini pertama dan eksekutif senior.

Bergantung pada persyaratan hukum dan peraturan serta sektor industri, ukuran, dan kompleksitas organisasi, peran seorang senior dalam fungsi kepatuhan, tergantung pada tanggung jawab spesifiknya, dapat melapor ke salah satu dari sejumlah peran yang berbeda dalam organisasi. Mereka termasuk manajemen eksekutif senior (misalnya, Chief Executive Officer, Chief Risk Officer, Chief Operating Officer, Kepala Legal atau lainnya), jalur manajemen masing-masing, dan/atau langsung ke Badan Pengurus atau subkomite yang ditunjuk. Dalam kasus tertentu, sekali lagi bergantung pada faktor-faktor yang diidentifikasi di atas dan mekanisme untuk memastikan independensi fungsi audit internal, peran atau departemen kepatuhan dapat melapor kepada Kepala Audit Eksekutif (CAE) atau individu yang mengawasi departemen kepatuhan dan departemen audit internal. Seseorang harus menerapkan Enam Prinsip yang dijelaskan dalam Model Tiga Lini untuk mengevaluasi keselarasan tanggung jawab masing-masing peran untuk memenuhi persyaratan dan ekspektasi. Seperti yang dijelaskan dalam model, tindakan mitigasi harus diambil jika penyalarsan menyebabkan potensi konflik kepentingan atau penurunan objektivitas atau independensi. Konflik potensial maupun aktual atau penurunan objektivitas juga harus dilaporkan kepada Badan Pengurus untuk pertimbangan dan tindakan yang mungkin dilakukan, termasuk pemberitahuan kepada regulator, jika berlaku.

## Kepatuhan sebagai serangkaian kegiatan

Kepatuhan dapat merujuk pada proses dan pengendalian yang dirancang untuk mencapai, mendukung, memantau, mengawasi, memeriksa, menguji, menantang, atau mengonfirmasi kepatuhan. Individu yang melaksanakan langkah-langkah ini membantu memastikan organisasi dan anggotanya mematuhi persyaratan dan ekspektasi.

Kepatuhan dalam suatu organisasi dicapai melalui tindakan dan perilaku setiap orang yang bekerja untuk atau bersama organisasi, sesuai dengan peran dan senioritasnya.

Tanggung jawab untuk proses, prosedur, dan pengendalian rutin yang dirancang untuk memenuhi persyaratan dan ekspektasi tertentu pada tingkat tertentu dan dengan tingkat kepastian yang dapat diterima dapat ditempatkan di berbagai tempat dalam organisasi dan juga dapat dialihdayakan. Model Tiga Lini menetapkan bahwa elemen kunci dalam menilai keselarasan adalah mengidentifikasi hak pengambilan keputusan yang terkait dengan aktivitas kepatuhan. (Lihat peran dan aktivitas terperinci yang mencakup kepatuhan di bagian Lampiran).

# Model Tiga Lini:

## Kepatuhan

Badan Pengurus mutlak bertanggung jawab atas keseluruhan tata kelola, yang dicapai melalui tindakan dan perilaku Badan Pengurus, serta oleh manajemen dan audit internal.<sup>7</sup>

Karena setiap organisasi menetapkan tanggung jawab untuk aspek kepatuhan sesuai dengan kondisi masing-masing, tergantung pada persyaratan eksternal yang ditentukan, organisasi harus menganalisis seberapa baik peran dan tanggung jawab yang ditugaskan di seluruh organisasi selaras dengan Enam Prinsip Model Tiga Lini. Hasilnya mungkin menunjukkan bahwa beberapa tanggung jawab sama dengan peran Badan Pengurus; beberapa peran lebih ke manajemen, termasuk peran kepatuhan dan manajemen risiko; dan lainnya berperan sebagai audit internal.

Peran lini pertama termasuk menyampaikan produk dan jasa kepada klien atau pelanggan dan memberikan dukungan yang diperlukan untuk melakukannya sesuai dengan persyaratan dan ekspektasi. Peran lini kedua memberikan pengawasan dan advis spesialis, menilai risiko (terutama secara kolektif atau portofolio), dan melakukan aktivitas manajemen risiko (termasuk pemantauan, pengawasan, dan pengujian), secara kredibel menantang lini pertama. Peran audit internal lini ketiga memberikan asurans independen, termasuk asurans tentang seberapa baik lini kedua secara kredibel mendukung lini pertama. Bersamaan-sama, mereka perlu bekerja secara efektif melalui koordinasi, komunikasi, dan kolaborasi yang tepat untuk memastikan kegiatan mereka selaras dengan tepat tanpa tumpang tindih, duplikasi, dan kesenjangan yang tidak semestinya, dan tanpa konflik atau ketidaksesuaian.

Grafik yang digunakan untuk mewakili model tidak mengidentifikasi peran atau departemen kepatuhan atau peran, departemen, atau tanggung jawab lini kedua spesifik lainnya. Grafik ini menggambarkan hubungan antara peran sentral tata kelola yang berbeda dengan struktur dari organisasi.

## Menentukan tanggung jawab untuk peran dan aktivitas kepatuhan

Akuntabilitas, tindakan, dan asurans adalah unsur penting dari tata kelola. Pembentukan dan karakteristik departemen spesialis untuk manajemen risiko, kepatuhan, etika, keberlanjutan, keamanan, privasi data, penasihat hukum, pengendalian keuangan, dan sebagainya bergantung pada banyak faktor. Faktor-faktor tersebut termasuk kompleksitas organisasi, ukuran, sektor, sumber daya, regulasi, peraturan perundang-undangan dan budaya, toleransi risiko/selera risiko Badan Pengurus, dan yang terpenting termasuk tujuan dan tanggung jawab peran dalam departemen spesialis masing-masing.

---

<sup>7</sup> Struktur Badan Pengurus bervariasi menurut yurisdiksi, persyaratan peraturan, dan desain institusi individu. Ketika kami merujuk ke Badan Pengurus, kami menyertakan berbagai struktur Badan Pengurus yang ditemukan di berbagai yurisdiksi, dan industri, baik di sektor publik maupun swasta. Tanggung jawab Badan Pengurus berikut mungkin berlaku: menetapkan arah organisasi; mendefinisikan visi, misi, nilai-nilai dan selera risiko; dan menerima laporan dari manajemen tentang hasil yang direncanakan, aktual, dan diharapkan dan tentang risiko dan manajemen risiko.

Tergantung pada mandat peraturan khusus pada industri tertentu, organisasi mungkin tidak memiliki departemen kepatuhan yang ditunjuk secara terpisah. Banyak organisasi yang tidak memiliki departemen kepatuhan juga tidak memiliki individu yang jabatan atau deskripsi pekerjaannya mencakup kepatuhan.

Namun, bahkan tanpa peran atau departemen kepatuhan yang ditentukan, organisasi masih dapat memiliki tata kelola yang efektif dan mematuhi persyaratan dan ekspektasi, asalkan mereka menetapkan peran dan tanggung jawab, proporsional dengan organisasi, untuk mencapai kepatuhan terhadap persyaratan dan ekspektasi yang berlaku, dan bahwa individu mematuhi peran mereka yang ditentukan.

Biasanya, ketika organisasi tumbuh lebih besar, lebih kompleks, memiliki banyak sumber daya, atau sangat diatur regulasi, organisasi mungkin memutuskan atau diharuskan untuk menetapkan tanggung jawab dan sumber daya terpisah untuk peran individu dan departemen dalam berbagai aspek kepatuhan.

Selain itu, satu karyawan mungkin bertanggung jawab untuk lebih dari satu peran. Dalam hal ini, harus ada penilaian yang tepat tentang kompatibilitas peran ganda ini, dan definisi yang jelas tentang tanggung jawab masing-masing peran dan pengawasan serta asurans atas kinerja peran tersebut. Dalam kasus tertentu, persetujuan oleh Badan Pengurus dan regulator mungkin diperlukan.

Dengan peran ganda, mungkin ada peningkatan risiko ketidaksesuaian, konflik kepentingan, dan berkurangnya kejelasan atas akuntabilitas dan tanggung jawab. Mitigasi mungkin diperlukan untuk tetap berada dalam selera risiko, bersama dengan pelaporan ke Badan Pengurus dan regulator, jika berlaku.

## Upaya kolektif untuk mencapai kepatuhan

Bahkan jika ada peran atau departemen kepatuhan yang ditunjuk, penting untuk disadari bahwa semua aktivitas kepatuhan tidak hanya berada di satu tempat dalam struktur organisasi. Karyawan di semua tingkatan serta direktur eksekutif dan non-eksekutif diharuskan untuk berkontribusi pada upaya kepatuhan kolektif. Tanggung jawab dan akuntabilitas didistribusikan ke seluruh hierarki organisasi, peran yang ditentukan, dan struktur manajemen lini untuk mencapai kepatuhan, mengurangi risiko kepatuhan, dan memantau kepatuhan terhadap persyaratan dan ekspektasi.

Kepatuhan terhadap persyaratan dan ekspektasi eksternal dan internal sering kali ditangani oleh departemen spesialis atau individu di luar departemen kepatuhan yang ditunjuk. Peran dan tanggung jawab masing-masing mungkin lebih sempit didefinisikan oleh peraturan dalam sektor industri atau oleh individu tertentu atau serangkaian persyaratan atau ekspektasi. Contohnya dapat mencakup: kepatuhan terhadap peraturan perundang-undangan tentang sumber daya manusia (SDM) yang ditangani oleh departemen SDM, dan kepatuhan terhadap persyaratan pelaporan keuangan dan perpajakan yang ditangani oleh departemen keuangan.

Seperti yang disarankan di atas, peran dan departemen yang berbeda mungkin bertanggung jawab untuk mencapai kepatuhan serta pengawasan, pemantauan, dan pengujian aspek kepatuhan. Oleh karena itu, sangatlah penting untuk menerapkan Enam Prinsip dalam mengidentifikasi karakteristik terkait kepatuhan dari peran individu dan tanggung jawabnya.

Tata kelola yang efektif mendapat manfaat dari komunikasi, koordinasi, dan kolaborasi informal maupun formal, serta mendorong transparansi. Namun, jika interaksi informal dalam tata kelola dan struktur pengendalian menghindari identifikasi, eskalasi, dan mitigasi masalah kepatuhan yang sesuai, hal itu dapat

merusak efektivitas tata kelola formal dan struktur pengendalian dan mengaburkan penentuan akuntabilitas dan tanggung jawab.

Dalam menilai efektivitas model tata kelola, sangat penting untuk tidak hanya mengevaluasi struktur tata kelola formal yang dirancang dan dikembangkan untuk mencapai kepatuhan, tetapi organisasi juga perlu dievaluasi terkait jalur komunikasi informal, pengambilan keputusan, dan tindakan untuk mengidentifikasi jika, di mana, dan ketika struktur tata kelola informal melemahkan atau tidak mengindahkan jalur formal. Interaksi formal dan informal yang kuat untuk mendorong komunikasi, koordinasi dan kolaborasi didorong dalam Model Tiga Lini. Namun, struktur tata kelola informal dapat menghambat kepatuhan, menghindari pengendalian dan mengakibatkan manajemen risiko kepatuhan yang tidak efektif, dan mengaburkan kejelasan tanggung jawab dan akuntabilitas. Menerapkan Model Tiga Lini untuk mengidentifikasi peran, tanggung jawab, dan tindakan memungkinkan organisasi merancang kerangka kerja tata kelola yang efektif, termasuk mengembangkan perlindungan untuk mengurangi risiko tata kelola informal, pengambilan keputusan, dan tindakan yang dapat menyebabkan kegagalan kepatuhan.

Program kepatuhan yang efektif tidak hanya akan mendorong adopsi dan kepatuhan terhadap struktur tata kelola dan pengendalian yang formal dan terdokumentasi, tetapi juga akan menjadi elemen kunci dalam pengembangan dan pemeliharaan budaya kepatuhan dan pengendalian, memfasilitasi efektivitas Model Tiga Lini.

# Menerapkan Enam Prinsip

Model Tiga Lini mendorong pendekatan berbasis prinsip untuk menilai dan menyelaraskan peran dan tanggung jawab, dengan mempertimbangkan keadaan organisasi, termasuk persyaratan dan ekspektasi kepatuhan spesifiknya. Enam Prinsip model ini dapat digunakan untuk lebih memahami kepatuhan—sebagai hasil, sebagai kategori risiko, sebagai peran atau departemen, sebagai rangkaian kegiatan—dan kontribusinya terhadap kerangka tata kelola yang sukses. (Untuk ulasan lengkap dari Enam Prinsip, lihat [Model Tiga Lini](#)).

## Prinsip 1: Menetapkan persyaratan tata kelola

Prinsip 1 menjelaskan persyaratan minimum tata kelola yang harus ada:

- Akuntabilitas (oleh Badan Pengurus kepada pemangku kepentingan untuk kesuksesan).
- Tindakan dan penggunaan sumber daya (oleh manajemen untuk mencapai tujuan – termasuk mengelola risiko dan kepatuhan).
- Asurans dan advis (dari fungsi audit internal independen pada semua aspek untuk memungkinkan pengawasan dan transparansi yang efektif dan untuk meningkatkan kepercayaan dan perbaikan berkelanjutan).

Badan Pengurus mutlak bertanggung jawab untuk memastikan organisasi berperilaku sesuai dengan standar dan norma sosial yang diterima. Manajemen harus mengelola risiko yang terkait dengan kepatuhan dan ketidakpatuhan sesuai dengan selera yang diungkapkan oleh Badan Pengurus. Hal ini mungkin termasuk dalam menetapkan peran individu dan tim dengan fokus khusus pada aspek kepatuhan, dan dengan jelas mendefinisikan hak keputusan antara lini pertama sebagai pemilik risiko dan lini kedua dalam memberikan tantangan yang kredibel dan mendorong kesesuaian lini pertama dengan selera risiko. Audit internal memberikan asurans kepada manajemen dan Badan Pengurus tentang kecukupan dan efektivitas pengendalian untuk kepatuhan dan advis bagi perbaikan dan inovasi berkelanjutan.

## Ilustrasi Praktis dari Lapangan

**Perawatan kesehatan adalah industri yang sangat diatur, dan, dengan demikian, penyediaan dari hampir setiap layanan melibatkan kepatuhan terhadap beberapa aturan, regulasi, atau standar. Perawat, dokter, dan tenaga medis lainnya harus memastikan setiap layanan yang diberikan diberi wewenang dan didokumentasikan dengan tepat. Mereka yang memiliki tanggung jawab kepatuhan (peran individu atau departemen) dapat memberi advis kepada departemen klinis tentang persyaratan dokumentasi dan otorisasi dari prosedur yang diberikan, tetapi, pada akhirnya, pengampu lini pertama bertanggung jawab untuk menerapkan proses, mengendalikannya, dan memastikan kepatuhan terhadap persyaratan ini.**

Contoh dari industri saya adalah peringkat risiko kepatuhan teratas untuk organisasi dan persyaratan peraturan, dan penyelarasan aktivitas, pengendalian, pemantauan, dan tanggung jawab untuk mematuhi persyaratan peraturan dan sebanding dengan risiko ini. Misalnya, sebuah organisasi mungkin memiliki petugas kepatuhan anti pencucian uang, petugas privasi, petugas anti penyuapan dan korupsi, dll., sejalan dengan persyaratan peraturan, dan mungkin memiliki produk, pengungkapan, pekerjaan, keluhan, dll., tanggung jawab dan sumber daya tertentu untuk mendukung pencapaian kepatuhan dan pengelolaan area risiko utama ini. Pelaporan rutin dilakukan kepada Badan Pengurus, dan semua aktivitas dilakukan audit internal yang independen.

– Direktur Kepatuhan, Inggris Raya

Contoh yang baik dari tantangan yang dihadapi organisasi saat ini adalah dorongan untuk mengadopsi dan mematuhi standar “lingkungan, sosial dan tata kelola” atau “ESG”. Badan Pengurus bertanggung jawab untuk memastikan akuntabilitas manajemen agar organisasi berperilaku sesuai dengan strategi, standar, dan norma sosial yang ditetapkan oleh Badan Pengurus. ESG mencakup setiap bagian organisasi, setiap karyawan, pemasok, dan pelanggan, sehingga Badan Pengurus harus memastikan ada artikulasi yang jelas oleh manajemen tentang risiko ESG yang berlaku untuk organisasi, peraturan perundang-undangan eksternal, serta kebijakan internal dan prosedur, ukuran kinerja yang relevan dan data yang andal, otentik, dan dapat dibandingkan untuk mencerminkan pencapaian kepatuhan terhadap persyaratan dan ekspektasi internal tersebut. Selain itu, baik manajemen maupun Badan Pengurus akan menginginkan atau membutuhkan asuransi mengenai pencapaian tujuan kepatuhan ESG. Pemetaan tanggung jawab dan akuntabilitas yang kompleks di seluruh organisasi diperlukan untuk menangkap peran dan departemen masing-masing serta aktivitas mereka yang diperlukan untuk merangkul ESG dan menunjukkan kepatuhan.

– Direktur Kepatuhan, Amerika Serikat

## Prinsip 2: Mempertahankan pengawasan tata kelola secara memadai

Prinsip 2 mendefinisikan peran dari Badan Pengurus atas:

- Tata kelola.
- Mengawasi manajemen.
- Membangun dan mengawasi fungsi audit internal yang efektif.

Badan Pengurus mutlak bertanggung jawab atas tata kelola dan memastikan adanya struktur dan proses yang sesuai. Hal ini termasuk pengaturan untuk kepatuhan serta pengawasan terhadap peran audit internal.

Badan Pengurus harus menentukan derajat keyakinan dan menetapkan persyaratan serta ekspektasi atas kepatuhan terkait dengan tingkat paparan risiko dan potensi akibatnya yang dapat memengaruhi tujuan strategis. Dalam menentukan selera atau toleransi risiko kepatuhan, Badan Pengurus akan mengawasi pelaksanaan aktivitas manajemen dan pemenuhan tanggung jawab masing-masing peran dan departemen yang ditunjuk untuk mencapai hasil kepatuhan sesuai dengan selera dan toleransi risiko kepatuhan terkait.

Badan Pengurus harus memastikan audit internal ditempatkan dan didukung dengan sumber daya yang tepat untuk memungkinkannya memberikan asurans dan saran yang independen dan efektif atas kepatuhan. Kepala Audit Eksekutif harus akuntabel kepada Badan Pengurus, komite audit independen, atau komite setara yang ditunjuk oleh Badan Pengurus untuk mengamankan otoritas dan status independennya.

## **Ilustrasi Praktis dari Lapangan**

**Badan Pengurus yang efektif mampu melakukan perubahan dan memiliki suara di seluruh organisasi. Kadang-kadang eskalasi dan pelaporan dibuat sebagai hal yang biasa, namun hal ini tergantung pada seberapa mutakhir Badan Pengurus dan kualitas informasi mampu memberikan pengawasan dan arahan yang efektif dan terkini daripada berdasarkan retrospektif data historis. Audit internal harus memvalidasi apakah Badan Pengurus memperoleh visibilitas yang jelas tentang risiko yang dikelola untuk mengantisipasi, memberikan pengawasan, dan memberikan arahan tentang risiko tersebut. Kepatuhan memainkan peran lini kedua yang penting dalam menantang manajemen tentang kepatuhan dan efektivitas pengendalian dan memberikan wawasan kepada Badan Pengurus mengenai efektivitas manajemen risiko kepatuhan sesuai selera risiko.**

– Pegawai Kepatuhan, Singapura

**Dalam perawatan kesehatan dan banyak sektor lainnya, departemen kepatuhan mungkin memiliki tanggung jawab sehari-hari untuk elemen tertentu dari program kepatuhan, termasuk pelatihan dan pendidikan, pemantauan *hotline*, penyebaran kode etik, melakukan pemeriksaan latar belakang, dan sebagainya. Beberapa dari kegiatan ini adalah tentang mencapai kepatuhan, beberapa mungkin tentang menetapkan kebijakan, memantau, atau melaporkan efektivitas kepatuhan kepada manajemen senior dan Badan Pengurus. Departemen audit internal tidak dapat menawarkan asurans independen tentang efektivitas program kepatuhan jika departemen kepatuhan melapor kepada CAE. Namun demikian, dalam kasus seperti itu, pihak ketiga yang independen dapat dilibatkan untuk menawarkan asurans kepada badan pengurus.**

– Kepala Kepatuhan dan Audit Internal, Amerika Serikat

**Badan pengurus seharusnya berusaha untuk memastikan risiko kepatuhan dinilai/dipertimbangkan secara menyeluruh dalam rencana audit dari fungsi internal audit, memahami cakupan audit internal multi-tahun di seluruh risiko regulasi utama dan area yang menjadi fokus regulator, dan meninjau hasil laporan/kegiatan terkait kepatuhan.**

– Kepala Audit Eksekutif, United Kingdom

**Badan pengurus menetapkan *tone* untuk manajemen risiko kepatuhan, baik untuk manajemen maupun audit internal. Agar badan pengurus efektif dalam pengawasan kepatuhannya, harus ada pemeriksaan yang cukup, teratur, dan sering atas informasi kuantitatif dan kualitatif yang sesuai mengenai keadaan kepatuhan, yang disediakan oleh manajemen dan audit internal. Badan pengurus harus menetapkan agenda tetap berbagai aktivitas manajemen risiko kepatuhan untuk menangani manajemen risiko kepatuhan yang berwawasan ke depan dan**

**bukan hanya berfokus pada peristiwa pelanggaran, penyimpangan, dan perbaikan pada masa lalu.**

– Kepala Kantor Kepatuhan, United Kingdom

## Prinsip 3: Mendefinisikan peran manajemen pada lini pertama dan kedua

Prinsip 3 menjelaskan peran manajemen (pada peran lini pertama dan kedua yang dapat tergabung maupun terpisah bergantung pada sumber daya, tujuan, regulasi, dan sebagainya).

Peran lini pertama dan kedua merupakan peran manajemen. Peran tersebut mencerminkan tanggung jawab lini pertama untuk menyediakan produk dan layanan kepada klien dan lini kedua untuk menyediakan keahlian dalam melakukan pengawasan, penilaian risiko (khususnya secara kolektif maupun portofolio), dan melaksanakan aktivitas manajemen risiko untuk menguji lini pertama secara kredibel.

Departemen yang terpisah, misalnya departemen kepatuhan atau kepala departemen (atau pada organisasi yang lebih kecil dan kompleks sebagai individu) dapat bentuk atau ditunjuk dengan lini pelaporan kepada Badan Pengurus baik secara langsung maupun melalui Komite Badan Pengurus. Pimpinan departemen atau individu tersebut juga memiliki pelaporan bersama kepada CEO atau orang lain yang ditunjuk oleh manajemen. Lini pelaporan atau akuntabilitas kepada Badan Pengurus ini tampak menciptakan suatu independensi yang lebih besar bagi Kepala Departemen Kepatuhan atau individu tersebut. Namun demikian, aspek kunci dari independensi adalah tidak adanya tanggung jawab untuk pengambilan keputusan. Biasanya, seorang individu yang mempunyai peran kepatuhan mempunyai tanggung jawab pengambilan keputusan manajemen (dari penerimaan pelanggan, memberikan pengecualian kebijakan, persetujuan produk baru, dan sebagainya). Oleh karena itu, jalur pelaporan ke Badan Pengurus atau Komite Badan Pengurus tidak menciptakan independensi sejati untuk departemen, kepala departemen, atau individu. Audit internal dan Kepala Audit Eksekutif, memiliki independensi dari manajemen dalam lini pelaporan mereka, serta tidak memiliki tanggung jawab pengambilan keputusan operasional manajemen sehingga memberikan tingkat independensi tambahan.

Dengan demikian, karakteristik peran masing-masing lini dapat diartikulasikan sebagai berikut:

- Peran lini pertama: Patuh terhadap hukum, peraturan, kode perilaku, kebijakan organisasi, dan sebagainya dalam menyediakan produk dan layanan. Kepatuhan tetap menjadi tanggung jawab manajemen.
- Peran lini kedua: peran fungsi kepatuhan baik individu maupun departemen membangun kerangka kerja, melaksanakan pengawasan, memberikan saran, pemantauan dan pengamatan, melakukan pengujian, menguji manajemen, dan secara umum dapat memegang pengambilan keputusan operasional manajemen dan memiliki kekuasaan sebagai pemilik risiko (misalnya dapat mencakup melakukan keputusan untuk penerimaan pelanggan atau klien, persetujuan produk atau layanan baru, persetujuan transaksi, persetujuan terhadap pelampauan batas, pengecualian kebijakan, dan sebagainya).
- Peran lini ketiga: audit internal memberikan asurans independen atas kepatuhan, efektivitas upaya manajemen untuk mencapai kepatuhan, dan pekerjaan dari peran atau departemen kepatuhan untuk memantau dan memberikan pengawasan dan pengendalian manajemen risiko kepatuhan.

Audit internal tidak bertanggung jawab dalam pengambilan keputusan manajemen, serta melapor secara independen kepada Badan Pengurus.

Dengan menggunakan Model Tiga Lini, sebuah organisasi dapat mencapai kepatuhan terhadap persyaratan dan ekspektasi, serta berkontribusi pada tata kelola yang efektif dan berkelanjutan, serta memerangi praktik ilegal dan korupsi. Kepatuhan harus didasarkan pada transparansi dengan penetapan standar yang sesuai dalam suatu organisasi. Selain itu, bagi pemangku kepentingan eksternal (termasuk pemegang saham, badan pemerintah, regulator dan bursa, pemasok, dan rantai pasokan) program kepatuhan yang efektif yang mendorong transparansi akan menanamkan kepercayaan pada organisasi.

## **Ilustrasi Praktis dari Lapangan**

**Peran lini pertama dan kedua harus bekerja sama secara efektif untuk mengidentifikasi, mengelola, dan memantau mitigasi risiko kepatuhan organisasi. Seharusnya, tidak ada ketergantungan pada audit internal untuk memantau, menguji, dan menemukan sesuatu. Ini harus dilakukan dan dimiliki oleh peran lini pertama dan kedua.**

– Kepala Kantor Administrasi, Amerika Serikat

**Peran kepatuhan harus mendukung bisnis dan memastikan bahwa proses dan pengendalian selaras secara jelas. Ada berbagai contoh peran kepatuhan sebagai lini kedua memberikan nasihat kepada bisnis. Indikator kinerja utama dan indikator risiko utama akan mendukung bisnis untuk mengidentifikasi dan mengelola risiko untuk efektivitas pengendalian.**

– Kepala Kantor Kepatuhan, Meksiko

**Banyak industri tunduk pada segudang peraturan yang kompleks. Departemen kepatuhan menawarkan keahlian dan sarannya tentang persyaratan peraturan atau perubahan peraturan terbaru dalam departemen tertentu. Misalnya, dalam bisnis perawatan kesehatan, manajemen berbagai departemen klinis bertanggung jawab untuk merancang dan menerapkan pengendalian yang diperlukan untuk memastikan kepatuhan. Karena keahlian mereka, departemen kepatuhan idealnya ditempatkan untuk menilai kepatuhan terhadap persyaratan tersebut.**

– Kepala Staf Kepatuhan, Amerika Serikat

**Tantangan utama, namun salah satu yang dikelola dengan baik di perusahaan yang lebih besar, adalah kepemilikan dan kewajiban persyaratan dan ekspektasi kepatuhan dan bagaimana hal ini dijalankan oleh mereka yang memiliki peran kepatuhan atau departemen kepatuhan. Hal ini membutuhkan kerangka kerja manajemen dan pengendalian risiko yang sangat jelas yang memiliki garis akuntabilitas dan peran serta tanggung jawab yang jelas dengan rute eskalasi yang efektif melalui tata kelola yang kuat. Tanpa ini, pengawasan kepatuhan menjadi kabur dan sulit untuk dijalankan.**

– Kepala Kantor Kepatuhan, United Kingdom

**Kepatuhan merupakan tanggung jawab semua orang. Dalam industri yang diatur ketat, seperti bisnis perawatan kesehatan, tanggung jawab ini mencakup setiap pengasuh dan dapat mencakup kepatuhan terhadap persyaratan otorisasi dan dokumentasi untuk setiap prosedur**

yang diberikan. Jika departemen kepatuhan mengembangkan kebijakan, proses, dan pengendalian atas proses atau prosedur tertentu, atau memiliki tanggung jawab rutin untuk prosedur tersebut, departemen tersebut tidak akan dapat menawarkan asurans yang objektif. Namun demikian, memberikan nasihat dan konsultasi tentang persyaratan peraturan yang terkait dengan proses atau prosedur tidak serta merta merusak objektivitas departemen kepatuhan.

– Kepala Unit Kepatuhan dan Audit Internal, Amerika Serikat

## Prinsip 4: Mendefinisikan peran lini ketiga

Prinsip 4 menjelaskan peran audit internal sebagai penyedia asurans dan saran independen.

Model Tiga Lini menyelaraskan kebutuhan kritical akan asurans terhadap kecukupan dan efektivitas respon risiko, termasuk pengendalian, sebagai komponen fundamental tata kelola. Respon terhadap risiko dan pengendalian termasuk penerimaan, pemantauan, dan penyediaan pengawasan terhadap kepatuhan dan manajemen risiko kepatuhan. Hal ini tercapai melalui penetapan yang kompeten akan suatu proses, keahlian, dan wawasan yang sistematis dan disiplin oleh audit internal sebagai satu-satunya penyedia asurans pada organisasi yang independen dari manajemen.

Koordinasi dan kolaborasi antara peran kepatuhan dan audit internal dapat diraih sehingga memberikan manfaat bagi organisasi tanpa menurunkan efektivitas masing-masing peran tersebut secara terpisah.

Sebagai hasil dari berbagai peran dan akuntabilitas sepanjang lini organisasi, terdapat sumber asurans lain yang secara agregat mampu menyediakan perspektif yang komprehensif dan komposit pada suatu organisasi. Walau demikian, penting untuk menganalisis dan mengevaluasi peran spesifik tersebut dan keselarasannya berdasarkan Model Tiga Lini untuk menilai kualitas dan objektivitas asurans semacam itu.

Audit internal mempertahankan akuntabilitas kepada Badan Pengurus dan independen dari tanggung jawab manajemen. Hal ini kritical untuk memahami peran asurans dan posisi yang berbeda dari suatu audit internal dalam struktur tata kelola. Jika independensi aktivitas audit internal dan objektivitas auditor internal terancam, Kepala Audit Eksekutif harus melaporkannya kepada Badan Pengurus untuk diambil tindakan koreksi.

Auditor internal dalam menilai efektivitas dari peran dan departemen kepatuhan seharusnya terbuka untuk berkomunikasi, berkoordinasi, dan berkolaborasi untuk mencapai penerapan efektif dari suatu Model Tiga Lini dan mendorong budaya kepatuhan dan pengendalian.

## Ilustrasi Praktis dari Lapangan

**Hal kunci untuk dilihat ketika menilai risiko kepatuhan manajemen adalah efektivitas suatu aktivitas yang dilaksanakan untuk memitigasi suatu isu. Penilaian risiko yang kuat terhadap butir risiko kepatuhan spesifik dan keselarasan aktivitas terhadap proporsi risiko tersebut adalah penting. Kebalikannya, banyak aktivitas yang dapat dijalankan tanpa memberikan manfaat berupa pengamanan terhadap organisasi dari risiko ketidakpatuhan.**

– Kepala Audit Eksekutif, Afrika Selatan

**Tantangan khusus bagi auditor internal adalah penyatuan hal-hal berikut ke dalam pekerjaan audit mereka dan pelaporan atas suatu identifikasi eksplisit dari ketidakpatuhan: pelanggaran peraturan hukum dan regulasi, pelanggaran kebijakan, standar, dan aturan perilaku. Untuk memberikan asurans tersebut memerlukan sumber daya terampil agar secara efektif dapat menilai dan melaporkan pencapaian hasil kepatuhan yang diharapkan.**

– Kepala Audit Eksekutif, United Kingdom.

## Prinsip 5: Mempertahankan independensi lini ketiga

Prinsip 5 mendeskripsikan pentingnya independensi audit internal.

Internal audit sebagai lini ketiga memiliki beberapa karakteristik yang dapat membantu untuk mendefinisikan independensinya. Hal ini meliputi lini pelaporan fungsional yang independen kepada Badan Pengurus atau Komite Badan Pengurus, dan yang terpenting adalah independen terhadap pengambilan keputusan manajemen.

Fungsi manajemen risiko (termasuk fungsi manajemen risiko kepatuhan), yang biasanya sering memiliki lini pelaporan fungsional kepada Badan Pengurus atau Komite Badan Pengurus, umumnya juga memiliki peran tanggung jawab pengambilan keputusan manajemen, misalnya terkait dengan pengambilan, pengelolaan, mitigasi, pengendalian, dan pelaporan risiko, termasuk risiko kepatuhan.

Lini kedua dapat mempertahankan tanggung jawabnya untuk menyediakan pengujian yang efektif dan kredibel kepada lini pertama. Namun demikian, independensi audit internal dari pengambilan keputusan manajemen merupakan pembeda yang signifikan antara peran lini ketiga dengan peran lini kedua dan pertama, sebagaimana diuraikan pada Prinsip 3 di atas.

## Ilustrasi Praktis dari Lapangan

**Bagi audit internal, agar tidak berkonflik, auditor internal harus didesain untuk tidak menjalankan pengendalian atau berpartisipasi dalam pengambilan keputusan manajemen; fokus audit internal adalah pengamatan, pengujian, dan pengevaluasian untuk menentukan apakah risiko kunci telah diidentifikasi dan dikendalikan sesuai tujuan. Mereka harus memiliki ekspektasi yang tidak bias atau berupa dugaan.**

– Kepala Audit Eksekutif, Australia

**Pemangku kepentingan utama dari audit internal adalah Badan Pengurus dan independensi auditor internal memungkinkannya untuk melaporkan hasil dan rekomendasi tanpa tersaring. Tidak ada ekspektasi atau kebutuhan untuk memastikan bahwa mekanisme pengendalian dan mereka yang melaksanakan pengendalian tersebut tampak dalam kondisi yang diharapkan. Audit internal memiliki akuntabilitas untuk melaporkan sejujurnya.**

– Kepala Audit dan Staf Kepatuhan, Amerika Serikat.

**Lini kedua kepatuhan berperan mendefinisikan kebijakan, menyarankan kepada bisnis terkait dengan desain pengendalian, dan menyediakan asurans. Individu atau departemen kepatuhan**

dapat memiliki tugas tanggung jawab untuk melaksanakan fungsi operasional atas nama lini pertama. Dalam kasus seperti ini, individu atau departemen kepatuhan tidak sepenuhnya independen terhadap lini pertama. Audit internal adalah satu-satunya aktivitas independen penuh karena independensinya dari pengambilan keputusan manajemen oleh lini pertama dan kedua.

– Kepala Risiko dan Audit Internal, Amerika Serikat.

## Prinsip 6: Menciptakan dan melindungi nilai melalui kolaborasi

Prinsip 6 menjelaskan pentingnya memastikan koordinasi dan kolaborasi antara seluruh peran tersebut.

Tata kelola yang efektif tidak hanya mensyaratkan penugasan tanggung jawab secara tepat tetapi juga keselarasan yang kuat antar aktivitas melalui koordinasi, kolaborasi, dan komunikasi. Badan Pengurus mengandalkan laporan manajemen, audit internal, dan lainnya untuk menjalankan pengawasan dan memberikan arahan kepada manajemen untuk mencapai tujuan, mengelola risiko, dan menciptakan nilai. Peran Badan Pengurus, bersama dengan peran lini pertama, kedua, dan ketiga, secara kolektif berkontribusi pada penciptaan dan perlindungan nilai ketika mereka saling selaras satu sama lain dan dengan memprioritaskan kepentingan pemangku kepentingan. Sejalan dengan itu, komunikasi yang jelas atas tanggung jawab kepatuhan pada satu organisasi, hak pengambilan keputusan, selera risiko, taksonomi umum, penilaian entitas atau unit yang didefinisikan secara jelas, pelaporan kinerja dan risiko terhadap persyaratan dan ekspektasi, dan program pengujian dan asuransi, seluruhnya dilaksanakan untuk meningkatkan koordinasi dan kolaborasi.

## Ilustrasi Praktis dari Lapangan

Suatu ilustrasi koordinasi dan kolaborasi sebagai contoh adalah privasi data. Kepatuhan, atau dalam organisasi tertentu berkolaborasi dengan departemen hukum, mengidentifikasi persyaratan regulasi, mengomunikasikannya kepada organisasi, dan memastikan proses dan pengendalian yang tepat telah dilaksanakan. Tim bisnis (operasi, TI, keamanan informasi, dsb) mengimplementasikan aktivitas, termasuk pemantauan, eskalasi, dan pelaporan informasi yang dibutuhkan. Tim keamanan informasi dan tim kepatuhan memantau area risiko kunci untuk memastikan tim bisnis telah mengikuti prosedur dan melakukan pemantauan dan pelaporan secara tepat. Audit internal menilai kerangka kerja untuk mengelola risiko yang relevan, termasuk risiko kepatuhan, dan proses dan pengendalian terkait yang dilaksanakan oleh tim bisnis ketika mengaudit area-area tersebut.

– Kepala Kantor Kepatuhan, United Kingdom

ESG merupakan satu contoh yang sangat bagus tentang koordinasi dan kolaborasi di dalam organisasi untuk mencapai kepatuhan terhadap persyaratan dan ekspektasi. Peran lini pertama, kedua, dan ketiga harus bekerja bersama (dalam perannya masing-masing dan dalam pengawasan Badan Pengurus) untuk mencapai hasil ESG yang diharapkan. Mereka dengan berbagai tanggung jawab kepatuhan akan bekerja dengan yang lainnya di dalam organisasi untuk mencapai tujuan ESG organisasi:

- **Badan Pengurus menentukan strategi dan selera risiko dan penyiapan ritme untuk budaya dan perilaku.**

- **Manajemen mengintegrasikan persyaratan dan ekspektasi ESG ke dalam tata kelola dan operasi organisasi.**
  - **Menyediakan saran, kerangka kerja, dan persyaratan muatan, desain, dan implementasi struktur, sistem, dan proses yang tepat untuk perencanaan strategis dan operasional, penetapan tujuan, pengumpulan data, pengambilan keputusan, dan pelaporan terkait ESG.**
  - **Menilai risiko yang berkaitan dengan pencapaian kepatuhan dengan persyaratan dan standar ESG, termasuk kebijakan dan target internal.**
  - **Mengembangkan standar, kerangka kerja, prinsip, atau model yang perlu diadopsi untuk mengukur, memantau, dan melaporkan dampak terhadap pencapaian hasil ESG.**
  - **Mengevaluasi akurasi dan konsistensi data dan metodologi yang digunakan untuk mengumpulkan data yang digunakan untuk pelaporan berkelanjutan dan ESG.**
  - **Membangun proses pengukuran dan evaluasi; pendefinisian materialitas dan daftar indikator kinerja yang relevan (KPI); mengenalkan metode, pedoman, dan alat-alat pelaporan (internal dan eksternal).**
- **Audit internal menyediakan asurans independen kepada Badan Pengurus atas aktivitas tersebut di atas dan pencapaian manajemen terhadap tujuan ESG, termasuk kepatuhan pelaporan manajemen dengan persyaratan dan ekspektasi.**

– Kepala Kantor Kepatuhan, United Kingdom

# Fakta-Fakta Utama tentang Kepatuhan

## Sepuluh hal penting untuk dicatat:

1. Mungkin saja tidak ada sumber daya, departemen, manajer, dan lainnya yang didedikasikan khusus untuk kepatuhan. Tidak seluruh organisasi mampu atau perlu mengalokasikan sumber daya. Seringkali ketika organisasi menjadi lebih kompleks, teregulasi secara ketat atau spesifik, lebih besar, menjadi subjek pengaturan ketat, mulai untuk beroperasi di dalam lingkungan yang berubah secara cepat (regulasi, komersial, dsb), dan untuk mengatasi faktor yang sama tersebut, mereka menentukan individu, tim, sistem, dan/atau sumber daya lain yang diperlukan untuk ditugaskan pada aspek kepatuhan sebagai sebuah divisi kerja dan komponen formal dalam suatu desain organisasi. Sumber daya tersebut mungkin bisa eksternal organisasi, misalnya melalui alih daya terhadap suatu kegiatan pemantauan kepatuhan tertentu atau keahlian pada hal pokok tertentu.
2. Untuk menerapkan Enam Prinsip Model Tiga Lini untuk mengevaluasi peran terkait kepatuhan, akan bermanfaat untuk mempertimbangkan hasil dari peran tersebut dalam melaksanakan tanggung jawab berikut:
  - Mencapai kepatuhan terhadap undang-undang, regulasi, kontrak, kebijakan, prosedur, kode perilaku, atau persyaratan lain berkaitan dengan produk atau layanan;
  - Menyediakan pengawasan khusus, menilai risiko (utamanya berbasis kolektif atau portofolio dan melaksanakan aktivitas manajemen risiko, serta secara kredibel menguji lini pertama untuk mendorong dan mencapai kepatuhan di dalam organisasi secara keseluruhan sesuai dengan kode perilaku yang berlaku atau standar, persyaratan, dan ekspektasi.
  - Menyediakan suatu penilaian terhadap kecukupan dan efektivitas program kepatuhan.
  - Menyediakan ahli untuk menguji efektivitas program kepatuhan dan komponen-komponennya di dalam organisasi secara keseluruhan.
3. Peran kepatuhan baik secara individu atau departemen dalam suatu organisasi mungkin tidak dapat mencakup seluruh hal tentang kepatuhan untuk organisasi itu<sup>8</sup>. Dalam kondisi ini, organisasi hendaknya mendokumentasikan secara jelas cakupan dari peran atau departemen kepatuhan, termasuk peran yang bertanggung jawab terhadap persyaratan dan ekspektasi lain. Hal ini penting untuk organisasi yang lebih kecil, dimana satu individu dapat ditugaskan untuk berbagai tanggung jawab dan peran dan beberapa tanggung jawab mungkin dialihdayakan, dan juga untuk organisasi yang lebih besar, yang terdapat berbagai peran atau departemen ditugaskan dengan beragam aktivitas kepatuhan.
4. Suatu peran kepatuhan atau Kepala Departemen Kepatuhan, baik secara praktik maupun sebagai subjek hukum dan syarat regulasi, dapat melaporkan kepada satu dari berbagai peran berbeda di dalam organisasi, termasuk: manajemen eksekutif senior (misal direktur eksekutif, direktur risiko, direktur operasional, kepala bagian umum, atau lainnya), dan/atau kepada Badan Pengurus atau Komite. Dalam

---

<sup>8</sup> Etika, keberlangsungan, pelaporan keuangan, privasi data, sumber daya manusia, dan kewajiban hukum, sebagai contoh, dapat memiliki sumber daya internal/eksternal masing-masing untuk mencapai kepatuhan atau menyediakan pengawasan dan manajemen risiko tambahan untuk komponen spesifik dari suatu kepatuhan. Contohnya, evolusi lingkungan, sosial, dan tata kelola (environmental, social, and governance (ESG)) dipandang sebagai suatu jangkauan peran baru, tanggung jawab, aktivitas, dan departemen di dalam beragam organisasi, berfokus pada kepatuhan terhadap aspek ESG yang luas.

beberapa kondisi, kepatuhan sebagai bagian dari manajemen, dapat melaporkan kepada Kepala Audit Eksekutif. Ketepatan lini pelaporan dapat ditentukan dengan menilai tanggung jawab sesuai Model Tiga Lini dan persyaratan hukum dan regulasi yang terkait.

5. Suatu peran kepatuhan atau kepala departemen kepatuhan dapat memiliki lini pelaporan atau akuntabilitas pelaporan kepada satu atau lebih Komite Pengurus atau pimpinan dari satu atau lebih Komite Pengurus. Namun demikian, hal ini tidak sama dengan independensi dari manajemen dan tidak menggantikan kebutuhan asuransi independen yang disediakan oleh audit internal.
6. Peran kepatuhan individual dan departemen kepatuhan dapat termasuk tanggung jawab yang meliputi, namun tidak terbatas pada: manajemen risiko kepatuhan secara luas, pemantauan, pengujian, analisis, penilaian, saran, asuransi, penetapan kebijakan, pengembangan dan penerapan sistem dan pengendalian, keputusan manajemen, pengawasan, dan pelatihan.
7. Peran dan departemen kepatuhan dapat memuat tanggung jawab yang erat atau langsung berkaitan dengan penyediaan produk atau layanan. Hal ini akan memerlukan dokumentasi yang jelas tentang tanggung jawab, kewenangan, dan akuntabilitas dalam peran tersebut (contohnya kemampuan untuk mencegah ketidakpatuhan dalam penyediaan produk atau layanan dengan menolak transaksi atau keputusan manajemen).
8. Lini pertama dan kedua sebaiknya dipisahkan. Anggota lini pertama seharusnya adalah pemilik risiko yang mereka ambil, sementara lini kedua seharusnya menciptakan dan mengawasi kerangka kerja dan standar untuk membantu lini pertama dalam mengelola risiko mereka sendiri, termasuk menguji keputusan dan aktivitas lini pertama. Dalam praktiknya, tergantung dengan persyaratan yurisdiksi atau industri, dan ukuran, kompleksitas, dan faktor lain organisasi, mungkin terdapat peran yang tercampur. Dalam kasus ini, penilaian terhadap kesesuaian peran tersebut harus dilakukan dan risiko lain yang terkait perlu dimitigasi. Hal ini mungkin memerlukan penyesuaian terhadap komposisi dari peran-peran tersebut agar secara efektif memitigasi risiko dari satu rangkaian aktivitas yang tidak sesuai dengan suatu peran. Tanggung jawab untuk mengelola risiko tetap menjadi bagian dari lini pertama dan dalam lingkup manajemen.
9. Terlepas dari bagaimana manajemen mengatur struktur sumber daya mereka untuk melaksanakan kewajiban kepatuhan, manajemen bertanggung jawab untuk memastikan organisasi memenuhi persyaratan dan ekspektasi sesuai parameter selera risiko yang ditetapkan oleh Badan Pengurus.
10. Salah satu tanggung jawab penting dari kepatuhan lini kedua adalah penilaian terhadap efektivitas program kepatuhan dan upaya yang diperlukan untuk mencapai persyaratan dan ekspektasi kepatuhan.

# SUPLEMEN: Menyelaraskan Tanggung Jawab untuk Peran dan Aktivitas Kepatuhan

Aktivitas kepatuhan merupakan komponen penting dari tata kelola, manajemen risiko, dan aktivitas pengendalian internal organisasi. Tanggung jawab atas tindakan yang diperlukan untuk mencapai, mendukung, mengecek, dan mengkonfirmasi kepatuhan, dan pelaksanaan tanggung jawab tersebut, dapat ditugaskan kepada berbagai bagian dari organisasi. Mereka yang bertanggung jawab atas kepatuhan perlu untuk mendefinisikan ekspektasi hasil yang berhubungan kepatuhan dan mendefinisikan pengukuran yang tepat untuk mendemonstrasikan pencapaian keluaran tersebut.

Aktivitas yang memuat kepatuhan dapat termasuk, namun tidak terbatas pada:

- Mengidentifikasi peraturan perundang-undangan eksternal yang relevan, aturan, regulasi dan kebijakan internal, standar, prosedur, dan kode perilaku, dan perilaku yang dapat diterima konsisten dengan tujuan organisasi.
- Menentukan pengukuran risiko yang tepat untuk kepatuhan dan non kepatuhan sesuai peraturan perundang-undangan eksternal yang relevan, aturan, regulasi dan kebijakan internal, standar, prosedur, dan kode perilaku, dan perilaku yang dapat diterima konsisten dengan tujuan organisasi.
- Menilai risiko kepatuhan atas peraturan perundang-undangan eksternal yang relevan, aturan, regulasi dan kebijakan internal, standar, prosedur, dan kode perilaku, dan perilaku yang dapat diterima konsisten dengan tujuan organisasi.
- Mendesain, mengembangkan, dan mengimplementasikan proses dan pengendalian untuk mencapai kepatuhan dengan peraturan perundang-undangan eksternal yang relevan, aturan, regulasi dan kebijakan internal, standar, prosedur, dan kode perilaku, dan perilaku yang dapat diterima konsisten dengan tujuan organisasi.
- Melaksanakan, mempertahankan, dan mengelola proses dan pengendalian untuk mencapai kepatuhan dengan peraturan perundang-undangan eksternal yang relevan, aturan, regulasi dan kebijakan internal, standar, prosedur, dan kode perilaku, dan perilaku yang dapat diterima konsisten dengan tujuan organisasi.
- Mengevaluasi, menguji, dan memantau kepatuhan dengan peraturan perundang-undangan eksternal yang relevan, aturan, regulasi dan kebijakan internal, standar, prosedur, dan kode perilaku, dan perilaku yang dapat diterima konsisten dengan tujuan organisasi.
- Menyediakan tantangan yang kredibel kepada manajemen berkaitan dengan risiko kepatuhan.
- Mengelola dan memitigasi risiko kepatuhan.
- Menentukan hal terkait kepatuhan dan ketidakpatuhan.

- Menginformasikan dan mengeskalasi hal terkait ketidakpatuhan.
- Melaporkan kepatuhan atau ketidakpatuhan sesuai dengan persyaratan eksternal dan internal.
- Mendorong budaya yang kondusif untuk kepatuhan.
- Meningkatkan kesadaran melalui komunikasi, pelatihan, promosi, dan edukasi.
- Memberikan konsultasi dan saran terhadap aspek kepatuhan.
- Membangun dan mempertahankan etika atau program pelaporan pelanggaran (*whistleblowing*)
- Membangun dan menyediakan pelatihan, edukasi, dan kesadaran tentang kepatuhan.
- Menjalankan hubungan terkait tanggung jawab regulasi antara badan regulasi dengan organisasi.
- Membangun dan mempertahankan hubungan dengan organisasi profesional dan kelompok industri untuk mengidentifikasi standar, aturan, atau pedoman yang relevan di mana organisasi dan aktivitas terkaitnya seharusnya patuh atau dapat memilih untuk patuh, termasuk memfasilitasi pemerolehan dan pelaporan informasi yang menjadi acuan.
- Membangun dan mempertahankan hubungan dengan infrastruktur industri yang melibatkan organisasi dan yang memerlukan kepatuhan dengan persyaratan atau ekspektasi untuk pengguna infrastruktur dan pihak terkait.

Penting bahwa tanggung jawab dan hasil yang diharapkan memiliki peran yang jelas. Beberapa peran dan aktivitas ini tidak kompatibel dengan peran lain, seperti persetujuan transaksi, penerimaan pelanggan, atau pengambilan keputusan risiko bisnis lain di dalam tanggung jawab lini ketiga, sebagaimana dirinci pada Model Tiga Lini. Ketika audit internal diminta untuk melaksanakan peran tersebut, pengamanan diperlukan, termasuk perhatian dari Badan Pengurus atau Komite Audit, penggunaan pihak ketiga untuk menyediakan asuransi independen pada area terdampak, dan persetujuan regulasi jika diperlukan.

Demikian juga, bahkan dengan niat terbaik untuk mencapai hasil dari penyediaan produk dan layanan kepada klien sesuai kepatuhan, organisasi harus waspada dalam mengidentifikasi peran dan tanggung jawab yang dirancang baik untuk mencapai kepatuhan dalam menyediakan produk atau layanan, dan untuk menyediakan pengawasan serta manajemen risiko kepatuhan yang lebih luas. Prinsip dasar pemisahan tugas dan independensi berlaku, seperti halnya harapan untuk mengurangi risiko yang timbul ketika aktivitas yang tidak sesuai dalam peran diidentifikasi.

Demikian pula, terkadang ada keinginan dari mereka yang memiliki peran pengawasan, ketika melakukan identifikasi kesenjangan atau kekurangan dalam kegiatan manajemen risiko dan pengendalian yang mendasari penyediaan produk atau layanan, mereka memperluas cakupan mereka sendiri di luar pengawasan dan masuk ke dalam ranah pelaksanaan. Kebalikannya juga dapat terjadi, lini pertama dapat terlalu bergantung pada peran-peran pengawasan atau dengan tanggung jawab manajemen risiko. Ini merusak manfaat dari pengawasan objektif. Dalam kasus seperti itu, peran pengawasan harus mengidentifikasi, meningkatkan, dan memantau kesenjangan atau kekurangan, dan perbaikan manajemen. Elemen-elemen ini harus diselaraskan dan didokumentasikan sesuai dengan peran dan tanggung jawab tata kelola yang telah ditetapkan.



The Institute of  
**Internal Auditors**

[theiia.org](http://theiia.org)