The Institute of Internal Auditors

Contents

PREVIOUS ISSUES

To access previous issues of Global Perspectives and Insights, visit www.theiia.org/GPI.

READER FEEDBACK

Send questions or comments to globalperspectives@theiia.org.

Acknowledgements

The IIA thanks the members and stakeholders who contributed to this paper, including 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.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories. The association's global headquarters are in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Disclaimer

The opinions expressed in Global Perspectives and Insights are not necessarily those of the individual contributors or of the contributors' employers.

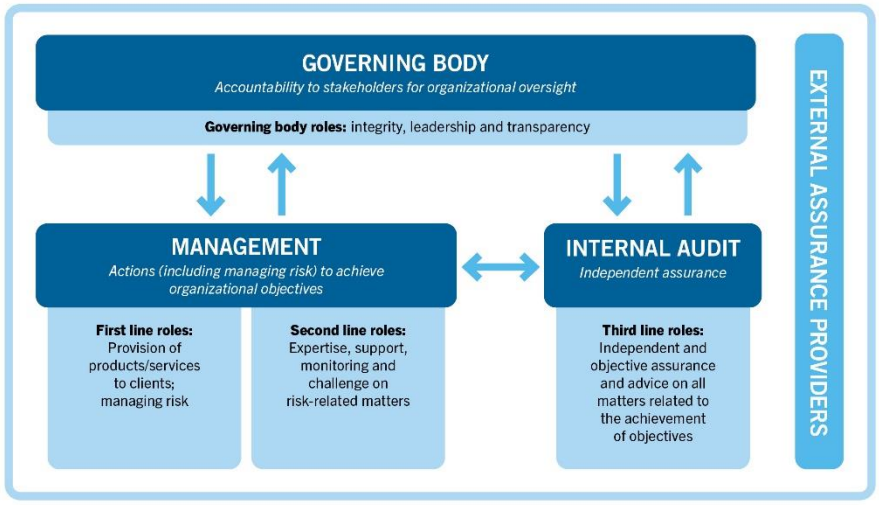
Copyright

Introduction

The relationship between internal audit and compliance is sometimes unclear, giving rise to important questions: Can internal audit have responsibility for compliance? Is a compliance function responsible for all compliance across an organization? As a chief audit executive, is it OK to be in charge of compliance?

This paper is designed to help bring clarity to these complexities and avoid confusion, gaps, and unnecessary duplication. Clear understanding is essential, collaboration is strongly encouraged, and the independence of internal audit[1] is fundamentally important.

This is *not* a paper on how to audit compliance. Instead, it serves as a tool for boards, management, compliance professionals, and chief audit executives, and uses the *Three Lines Model* as a way of explaining the relationship between internal audit and compliance. The Six Principles of the *Three Lines Model* and how they can be applied to compliance are examined in depth later in this paper.



Readers should use this paper to clearly identify, understand, evaluate, and apply within a governance structure — regardless of jurisdiction, industry, complexity, maturity or size — effective compliance and compliance risk management in its various aspects in relation to the *Three Lines Model*.[2] Practical illustrations from risk and compliance officers and internal auditors on compliance issues faced in the field will help in the practical application of the model's Six Principles when evaluating the alignment of compliance activities in accordance with the *Three Lines Model*. (See pages 8-16)

Accountability, Actions, and Assurance

The *Three Lines Model* describes how the accountability of the governing body, actions by management, and independent assurance by internal audit provide the foundation for effective governance. It also shows how the Six Principles assist in an evaluation of the respective roles and responsibilities in an organization. The application of the model's core elements and Six Principles varies for every organization, according to its goals, resources, and circumstances. The model helps

[1] The integral nature of compliance as a part of sustainable governance is a key focus and policy action recommended by B20 Italy to the G20 ministers in *B20 Italy Integrity & Compliance Policy Paper 2021*. In particular, Policy Action 2.1 on p. 11 specifically mentions the role of internal audit as described in the Three Lines Model.

[2] In certain jurisdictions and industries, roles and responsibilities related to compliance and compliance risk management are highly defined and the subject of extensive legislation, regulation, case law, and academic research. More detailed studies are available, and users of this practical paper are encouraged to consult them. For example, see from the American Law Institute, *Principles of the Law, Compliance, Risk Management, and Enforcement* No. 1 and *Principles of the Law, Compliance and Enforcement* No. 2

organizations identify structures, design processes, and assign responsibilities that best assist the achievement of objectives. This includes the management of compliance risk, which is a responsibility of management[3] but is achieved through a collaborative effort.

The range of compliance requirements and expectations an organization needs to consider comprises those externally imposed, such as laws, rules, and regulations, and internally imposed, such as policies, standards, procedures, and codes of conduct or behavior. They may be formally and explicitly defined or be more implicit, such as social, ethical, and cultural expectations. This broad, dynamic spectrum of considerations is referred to in this paper as "requirements and expectations."

Stakeholders expect an organization to fulfill its purpose and maximize value legally and ethically. Accordingly, organizations invest in closely monitoring compliance in key areas such as health and safety; employment; data protection and privacy; legal entity and commercial laws and codes; sector regulations; quality standards; anti-bribery and anti-corruption; investor and consumer protection; financial reporting and taxation; and individual codes of conduct. The list goes on. Compliance can be understood and effected in the context of accountability, actions, and assurance, as described in the *Three Lines Model*, as part of an overall approach to effective governance.

What Is Compliance?

Organizations must adhere to (or comply with) applicable laws and other external requirements that are a prerequisite of doing business. These compliance requirements cover everything from employee relations to paying taxes. In certain industries there are a range of rule-setting bodies, supervisors, regulators, and defined requirements, but other sectors have fewer externally imposed legal and regulatory boundaries and constraints. Nevertheless, it is difficult to identify an organization in either the public or private sector that does not have external compliance requirements.

At the same time, organizations design, develop, and implement internal expectations in the form of policies and procedures and set standards for ethical behavior and conduct. In certain regulated industries, external requirements dictate that an organization must establish and adhere to set internal policies, standards, and behavioral codes. With this many layered network of requirements, the concept of "compliance" in an organization takes on a number of dimensions. Accordingly, it is useful to consider compliance in each of its broad, related, but distinct aspects, and how it is discussed in organizations: As an outcome; As a category of risk[4]; As an organizational role, department, function, etc.[5]; and as a set of activities.

Each of these is discussed below.

[3] For purpose of this paper, *management* is broadly used to identify roles that are not the responsibility of the governing body or internal audit.

[4] Under the broad category of compliance risk in an organization, a risk taxonomy identifies a cascade of subcategories addressing both specific risks and related risks in respect of laws, rules, regulations, policies or behaviors.

[5] Roles may be defined as covering specific risks, such as conduct risk officer, data protection risk officer, etc.

Compliance as an outcome

Organizations engage in various activities to comply with laws, rules, policies, codes, etc., or "be in compliance." Achieving certain compliance requirements and expectations is often a necessary condition to operate and pursue strategic objectives.

Compliance as a category of risk

The International Professional Practices Framework defines risk as *the possibility that an event will occur, which will impact an organization's achievement of objectives*. Those impacts may be favorable or adverse. Therefore, when assessing risk it is essential to consider compliance requirements and expectations together with the likelihood of noncompliance and its potential impact on objectives.

There are risks for organizations related to both compliance and noncompliance. Their impacts may be in the form of rewards or penalties, which may be tangible or intangible. Compliance with International Organization for Standardization (ISO) standards, for example, is designed to create operational efficiencies and other gains and the favorable attention gained from following a voluntary code. Noncompliance eliminates those positive gains, and may result directly in harm as well as incur penalties such as the imposition of fines, withdrawal of licenses, sanctions, termination of operations, civil or criminal prosecution, and loss of funding or support. Additionally, noncompliance may cause reputation risk in the form of potential stakeholder dissatisfaction, public criticism, or other damage.

The identification, measurement, and assessment of compliance risk and determination of compliance risk appetite and tolerances help determine appropriate responses, including policies, procedures, limits, and controls.[6]

Compliance as a role or organizational department

Frequently, compliance is also used to refer to a role or department established to meet particular requirements and expectations or provide oversight, expertise, check and challenge, monitoring, testing, or assurance on compliance-related matters. These are characteristic of various first or second line roles as described in the *Three Lines Model*, remaining within the overall purview and responsibilities of management and, depending on the specific characteristics of the role, potentially offering specialist support and risk management to those with first line roles and senior executives.

Subject to legal and regulatory requirements and the industry sector, size, and complexity of the organization, a senior compliance role, depending on its specific responsibilities, may report to one of a number of different roles in the organization. They include senior executive management (e.g., the chief executive officer, the chief risk officer, chief operating officer, general counsel or others), their respective management chains, and/or directly to the governing body or designated subcommittee. In certain instances, again subject to the factors identified above and a mechanism to ensure independence of the internal audit function, a compliance role or department may report to the chief audit executive (CAE) or an individual who oversees both the compliance department and the internal audit department. One should apply the Six Principles described in the *Three Lines Model* to evaluate the alignment of each role's responsibilities for compliance with requirements and expectations. As described in the model, mitigating actions should be taken if an alignment presents a potential conflict of interest or impairment in objectivity or independence. The potential or actual conflict or impairment to objectivity should also be reported to the governing body for consideration and possible actions, including notification to the regulator, where applicable.

[6] The Committee of Sponsoring Organizations of the Treadway Commission (COSO) offers frameworks for risk management, and thought leadership, including new guidance on applying the ERM risk framework to the management of compliance risks.

Compliance as a set of activities

Compliance may refer to the processes and controls designed to achieve, support, monitor, surveille, check, test, challenge, or confirm compliance. The individuals who execute these measures help ensure the organization and its members comply with requirements and expectations.

Compliance in an organization is achieved through the actions and behaviors of everyone working for or with the organization, appropriate to their role and seniority.

Responsibility for routine processes, procedures, and controls designed to satisfy specific requirements and expectations to a given level and with an acceptable degree of certainty may sit in various places within the organization and may also be outsourced. The *Three Lines Model* establishes that a key element in assessing alignment is identifying the decisioning rights related to compliance activities. (See the detailed roles and activities that comprise compliance in the Annex section.)

The Three Lines Model:

Compliance

The governing body is ultimately accountable for governance, which is achieved through the body's actions and behaviors, as well as by management and internal audit.[7]

As each organization assigns responsibilities for the aspects of compliance according to their own circumstances, subject to any prescribed external requirements, it must analyze how well the specific roles and responsibilities assigned across the organization align with the Six Principles of the *Three Lines Model*. The assessment may show that some responsibilities align to governing body roles; some to management, including compliance and risk management, roles; and others to internal audit roles.

First line roles include providing products and services to clients or customers and providing the support needed to do so in compliance with requirements and expectations. Second line roles provide specialist oversight and advice, assess risk (particularly on a collective or portfolio basis), and perform risk management activities (including monitoring, surveillance, and testing), credibly challenging the first line. The third line internal audit role provides independent assurance, including assurance on how well the second line credibly challenges the first line. Together, they need to work effectively through appropriate coordination, communication, and collaboration to ensure their activities are appropriately aligned without undue overlap, duplication, and gaps, and without conflict or incompatibility.

The graphic used to represent the model does not identify a compliance role or department nor other specific second line roles, departments, or responsibilities. It depicts relationships between the central roles of governance as opposed to a prescribed organizational structure.

Determining responsibility for compliance roles and activities

Accountability, actions, and assurance are the essential ingredients of governance. The establishment and characteristics of specialist departments for risk management, compliance, ethics, sustainability, security, data privacy, legal counsel, financial control, and so on are contingent on many factors. They include organizational complexity, size, sector, resources, regulation, legislation and culture, risk tolerance/appetite of the governing body, and, importantly, the objectives and responsibilities of the roles within the respective specialist department.

Subject to specific regulatory mandates in certain industries, organizations may not have a separate designated compliance department. Many do not, nor may they have individuals whose titles or job descriptions include compliance.

However, even without a designated compliance role or department, organizations can still have effective governance and comply with requirements and expectations, provided that they assign roles and responsibilities, proportionate to the organization, to achieve compliance with the applicable requirements and expectations, and that individuals adhere to their defined roles.

Typically, as organizations grow larger, more complex, resource rich, or heavily regulated, they may decide or be required to assign separate responsibilities and resources to individual roles and departments for various aspects of compliance.

[7] Structures for governing bodies vary by jurisdiction, regulatory requirements, and individual institution design. When we refer to governing bodies, we include the wide range of governing body structures found in various jurisdictions, and industries, and both in the public and private sectors. The following responsibilities of the governing body may apply: setting direction of the organization; defining vision, mission, values and risk appetite; and receiving reports from management on planned, actual, and expected outcomes and on risk and risk management.

Additionally, one employee may be responsible for more than one role. In this case, there should be an appropriate assessment of the compatibility of these multiple roles, and a clear definition of each role's responsibilities and of the oversight and assurance on the performance of those roles. In certain instances, approval by the governing body and the regulator may be required.

With multiple roles, there may be increased risk of incompatibility, conflict of interest, and diminished clarity on accountability and responsibility. Mitigation may be required to remain within risk appetite, along with reporting to the governing body and regulator, where applicable.

A collective effort to achieve compliance

Even where there is a designated compliance role or department, it is important to recognize that all compliance activities do not reside in just one place within an organization's structure. Employees at all levels as well as executive and nonexecutive directors are required to contribute to the collective compliance effort. Responsibility and accountability are distributed throughout an organization's hierarchy, defined roles, and line management structure to achieve compliance, mitigate compliance risks, and monitor compliance with requirements and expectations.

Compliance with external and internal requirements and expectations is often handled by specialist departments or individuals outside of a designated compliance department. Their respective roles and responsibilities may be more narrowly defined by industry sector regulations or by a specific individual or set of requirements or expectations. Examples may include: compliance with human resources (HR) legislation and regulations handled by the HR department, and compliance with financial reporting and taxation requirements handled by the finance department.

As suggested above, different roles and departments may be responsible for achieving compliance as well as oversight, monitoring, and testing of aspects of compliance. As a result, it is clearly important to apply the Six Principles in identifying the compliance related characteristics of an individual role and its responsibilities.

Effective governance benefits from informal as well as formal communication, coordination, and collaboration and promotes transparency. However, if informal interactions in governance and control structures circumvent the appropriate identification, escalation, and mitigation of compliance issues, it can undermine the effectiveness of the formal governance and control structures and blur the determination of accountability and responsibility.

In assessing the effectiveness of a governance model, it is essential not only to evaluate the formal governance structure designed and developed to achieve compliance, but also to probe the organization for informal lines of communication, decision-making, and action to identify if, where, and when the informal governance structure undermines or frustrates the formal one. Strong formal and informal interactions to promote communication, coordination and collaboration are encouraged in the Three Lines Model. However, an informal governance structure can block compliance, circumvent controls and result in ineffective compliance risk management, and obscure clarity of responsibility and accountability. Applying the *Three Lines Model* to identify roles, responsibilities, and actions allows organizations to design an effective governance framework, including developing safeguards to mitigate the risks of the informal governance, decision-making, and action that can lead to compliance failures.

An effective compliance program will not only drive the adoption of and adherence to a formal, documented governance and control structure, it also will be a key element in the development and maintenance of a culture of compliance and control, facilitating the effectiveness of the *Three Lines Model*.

Applying the Six Principles

The Three Lines Model encourages a principles-based approach to assessing and aligning roles and responsibilities, taking into consideration an organization's circumstances, including its specific compliance requirements and expectations. The model's Six Principles can be used to better understand compliance—as an outcome, as a category of risk, as a role or department, as a set of activities — and its contribution to a successful governance framework. (For the full language of the Six Principles, see the *Three Lines Model*.)

Principle 1: Establish governance requirements

Principle 1 describes the minimum requirements of governance to be:

- Accountability (by the governing body to stakeholders for success).
- Actions and application of resources (by management to achieve goals – includes managing risk and compliance).
- Assurance and advice (from an independent internal audit function on all aspects to enable effective oversight and transparency and to promote confidence and continuous improvement).

The governing body is ultimately accountable for ensuring the organization behaves in accordance with accepted standards and societal norms. Management must manage risk associated with compliance and noncompliance according to the appetite expressed by the governing body. This may include establishing individual roles and teams with a specific focus on aspects of compliance, and clearly defining decision rights between the first line owning the risks and the second line in providing credible challenge and driving first line conformance with risk appetite. Internal audit provides assurance to management and the governing body on the adequacy and effectiveness of controls for compliance and advice for continuous improvement and innovation.

Practical Illustrations from the Field

Healthcare is a highly regulated industry, and, as such, the provision of almost every service involves compliance with some rule, regulation, or standard. Nurses, doctors, and other clinicians must ensure every service provided is appropriately authorized and documented. Those with compliance responsibilities (individual roles or a department) may advise the clinical departments on the documentation and authorization requirements of a given procedure, but, ultimately, the first line caregivers are responsible for implementing the processes, controls and ensuring compliance with these requirements.

– Head of Compliance and Internal Audit, United States

An example from my industry is the ranking of top compliance risks for the organization and regulatory requirements, and the alignment of activities, controls, monitoring, and responsibilities to comply with regulatory requirements and in proportion to these risks. For example, an organization may have an anti-money laundering compliance officer, privacy officer, anti-bribery and corruption officer, etc., in line with regulatory requirements, and may have product, disclosure, employment, complaints, etc., responsibilities and specified resources to support achieving compliance and management of these key risk areas. Regular reporting is made to the governing body, and all the activities are subject to independent internal audit.

– Chief Compliance Officer, United Kingdom

A good example of the challenges facing organizations today is the drive to adopt and embrace "environmental, social and governance" or "ESG" standards. The governing body is responsible for holding management accountable for the organization to behave in accordance with the strategy, standards, and societal norms set by the governing body. ESG embraces every corner of the organization, and every employee, supplier, and customer, so the governing body must ensure there is a clear articulation by management of the ESG risks applicable to the organization, the external laws and regulations, and the internal policies and procedures, the relevant performance measures and reliable, authentic, comparable data to reflect achievement of compliance with those internal requirements and expectations. Moreover, both management and the governing body will want or need assurance regarding the achievement of the ESG compliance objectives. A complex mapping of responsibilities and accountabilities across the organization is required to capture the respective roles and departments and their activities required to embrace ESG and demonstrate compliance.

– Chief Compliance Officer, United States

Principle 2: Maintain adequate governance oversight

Principle 2 defines the roles of the governing body for:

- Governance.
- Overseeing management.
- Establishing and overseeing an effective internal audit function.

The governing body is ultimately responsible for governance and ensures there are appropriate structures and processes in place. This includes arrangements for compliance as well as oversight of the role of internal audit.

The governing body must determine the degree of confidence it has and requires over compliance with requirements and expectations related to the level of exposure to risk and the potential to impact strategic objectives. In determining its compliance risk appetite or tolerance, the governing body will oversee management's execution of activities and fulfilment of the respective responsibilities of designated roles and departments to achieve compliance outcomes in accordance with the compliance risk appetite and related tolerances.

The governing body should ensure internal audit is suitably positioned and resourced to enable it to deliver independent and effective assurance and advice on compliance. The CAE must be accountable to the governing body, an independent audit committee, or equivalent designated committee of the governing body to secure its authority and independent status.

Practical Illustrations from the Field

An effective governing body is able to enact change and have a voice across the organization. Sometimes escalations and reporting are made as a matter of course, but it depends on how up-to-date the governing body is, and the quality of the information, to provide effective oversight and direction in the 'now' rather than retrospectively based on historic data. Internal audit should validate whether the governing body is obtaining clear visibility on risks being managed in order to anticipate, provide oversight, and give direction regarding those risks. Compliance plays an important second line role in challenging management on compliance and control effectiveness and providing the governing body with insight regarding the effectiveness of compliance risk management within risk appetite.

– Compliance Officer, Singapore

In healthcare and many other sectors, a compliance department may have day-to-day responsibility for certain elements of the compliance program, including training and education, hotline monitoring, promulgating a code of ethics, performing background checks, etc. Some of these activities are about achieving compliance, some may be about setting policies, monitoring, or reporting on the effectiveness of compliance to senior management and the governing body. The internal audit department cannot offer independent assurance on the effectiveness of the compliance program if the compliance department reports to the CAE. However, in such cases, an independent third party can be engaged to offer assurance to the governing body.

– Head of Compliance and Internal Audit, United States

The governing body should seek to ensure compliance risks are thoroughly assessed/considered in internal audit's audit plan, understand internal audit's multi-year coverage across key regulatory risks and regulator focus areas, and review results of compliance related reports/activities.

– Chief Audit Executive, United Kingdom

The governing body sets the tone for compliance risk management to both management and internal audit. For the governing body to be effective in its oversight of compliance, there must be ample, regular, and frequent examination of appropriate quantitative and qualitative information regarding the state of compliance, provided by both management and internal audit. The governing body should establish as standing agenda items the range of compliance risk management activities to address forward-looking compliance risk management, and not merely backward-looking event-driven focus on violations, breaches, and remediation.

– Chief Compliance Officer, United Kingdom

Principle 3: Define management roles over the first and second line

Principle 3 describes management roles (both first and second line roles that may be blended or separated depending on resources, goals, regulation, etc.).

First and second line roles constitute management. They reflect the responsibilities of the first line to provide the products and services to clients, and the second line to provide specialist oversight, assess risk (particularly on a collective or portfolio basis), and perform risk management activities, credibly challenging the first line.

Separate departments, such as a compliance department, may be established, or the head of the department or, in smaller and less complex organizations an individual, may be appointed with reporting lines to the governing body either directly or via a committee of the governing body. The head of the department or the individual may also have joint reporting to the CEO or a designee within management. This reporting line or accountability to the governing body may appear to establish greater independence for the head of the compliance department or individual. However, a key aspect of independence is the absence of decision-making responsibilities. Typically, an individual in a compliance role does retain a degree of management decision-making responsibility, from customer acceptance, granting policy exceptions, new product approval, and so forth. Accordingly, a reporting line to a governing body or a committee of the governing body does not create for such a department, department head, or individual true independence. Internal audit and the CAE, in addition to the

independence from management in their reporting lines, also have no management operational decision-making responsibilities, which provides an additional degree of independence.

Accordingly, the characteristics of roles across the lines may be articulated as follows:

- First line roles: achieving compliance with laws, regulations, behavior codes, organizational policies, etc., in providing products and services. Compliance remains the responsibility of management.
- Second line roles: individual compliance roles and departments establish frameworks, perform oversight, provide advice, monitoring and surveillance, undertake testing, challenge management, and generally may hold management operational decision-making, risk-owning powers (e.g., may include customer or client acceptance, new product or service approval, transaction approval, limit excess approval, policy exceptions, and so forth).
- Third line roles: internal audit provides independent assurance on compliance, the effectiveness of management's efforts to achieve compliance, and the work of the compliance role or department to monitor and provide compliance risk management oversight and control, but not vice versa. Internal audit has no management decision-making responsibilities and reports independently to the governing body.

Using the *Three Lines Model*, an organization can achieve compliance with requirements and expectations, as well as contribute to effective and sustainable governance and combat illegality and corruption. Compliance must be founded on transparency, setting a suitable standard within an organization. Additionally, for external stakeholders, including shareholders, governmental bodies, regulatory agencies and exchanges, suppliers, and the supply chain, an effective compliance program that promotes transparency instills confidence in an organization.

Practical Illustrations from the Field

First and second line roles should be working together effectively to identify, manage, and monitor mitigation of the organization's compliance risks. There should not be reliance on internal audit to monitor, test, and find things. This should be done and owned by the first and second line roles.

– Chief Administrative Officer, United States

A compliance role should support the business, making sure that processes and controls are clearly aligned. There are various instances in which a compliance role as a second line provides advice to the business. Key performance indicators and key risk indicators will support the business to identify and manage risks for control effectiveness.

– Chief Compliance Officer, Mexico

Many industries are subject to a myriad of complex regulations. The compliance department offers its expertise and advice on the regulatory requirements or recent regulatory changes within any given department. For example, in healthcare, management of the various clinical departments is responsible for designing and implementing the controls necessary to ensure compliance. Because of their expertise, the compliance department is ideally situated to assess compliance with these requirements.

– Chief Compliance Officer, United States

A key challenge, but one which is managed well in larger firms, is the ownership and obligations of compliance requirements and expectations and how these are executed by those in compliance roles or compliance departments. This requires a very clear risk management and control framework that has clear lines of accountability and roles and

responsibilities with effective escalation routes through robust governance. Without this, compliance oversight is blurry and difficult to execute on.

– Chief Compliance Officer, United Kingdom

Compliance is the responsibility of everyone. In highly regulated industries, such as healthcare, this responsibility embraces every caregiver and can include compliance with authorization and documentation requirements for any given procedure. If the compliance department develops the policies, processes, and controls over specific processes or procedures, or has routine responsibility for the procedure, it would not be able to offer objective assurance. However, advising and consulting on the regulatory requirements associated with a process or procedure would not necessarily impair the compliance department's objectivity.

– Head of Compliance and Internal Audit, United States

Principle 4: Define the role of the third line

Principle 4 describes internal audit's role as the provider of independent assurance and advice.

The *Three Lines Model* amplifies the critical need for assurance on the adequacy and effectiveness of risk responses, including controls, as a fundamental component of governance. The risk responses and controls include those in respect of achieving, monitoring, and providing oversight of compliance and compliance risk management. This is achieved through the competent application of systematic and disciplined processes, expertise, and insight by internal audit, as the organization's sole provider of assurance that is independent from management.

Effective coordination and collaboration between compliance roles and internal audit roles can be achieved to the benefit of an organization without impairing the effectiveness of each in fulfilling their distinct roles.

As a result of the various roles and accountabilities across an organization, there can be other sources of assurance that in the aggregate, could provide a comprehensive, composite perspective on an organization. However, it is important to analyze and evaluate specific roles and their alignment according to the *Three Lines Model* to assess the quality and objectivity of such assurance.

Internal audit maintains accountability to the governing body and independence from the responsibilities of management. This is critical to understanding assurance roles and the distinct position of internal audit within the governance structure. If the independence of the internal audit activity and the objectivity of internal auditors are threatened, the CAE must report this to the governing body for corrective actions.

Internal auditors, in assessing the effectiveness of compliance roles and departments, should be open to communication, coordination, and collaboration in order to achieve effective application of the *Three Lines Model* and promote a culture of compliance and control.

Practical Illustrations from the Field

A key item to look out for when assessing the management of compliance risk is the effectiveness of the activities being performed in mitigating issues. A solid risk assessment of specific compliance risk items and alignment of activities in proportion to those risks is important. Otherwise, a lot of activity could be going on without the benefit of safeguarding the organization from the risks of noncompliance.

– Chief Audit Executive, South Africa

A particular challenge for internal auditors is the incorporation into their audit work and reporting of the explicit identification of instances of noncompliance: violations of laws and regulations, breaches of policies, standards, and codes of conduct. To deliver such assurance requires access to appropriately skilled resources to effectively assess and report on achieving the desired compliance outcome.

– Chief Audit Executive, United Kingdom

Principle 5: Maintain third line independence

Principle 5 describes the importance of internal audit independence.

Internal audit as the third line has several characteristics that help to define its independence. These include an independent functional reporting line to the governing body or a governing body committee, and, importantly, independence from management decision-making.

Risk management functions (including compliance risk management functions), while often having a functional reporting line to the governing body or a governing body committee, typically also have within their respective roles management decision-making responsibilities, particularly with respect to taking, managing, mitigating, controlling, and reporting risk, including compliance risk.

The second line can maintain its responsibility to provide effective and credible challenge of the first line. However, the independence of internal audit from management decision-making is a significant differentiator between the third line role and the roles of the second and first line, as detailed above in Principle 3.

Practical Illustrations from the Field

For internal audit not to be conflicted, internal auditors must not have designed or executed controls or participated in management decision-making; their focus is observation, testing, and evaluation to determine if key risks are identified and controlled as intended. They must have no bias or preconceived expectations.

– Chief Audit Executive, Australia

Internal audit's key stakeholder is the governing body, and internal audit's organizational independence allows it to report unfiltered results and recommendations. There is no expectation or need to ensure that the control mechanisms and those executing them are seen in a favorable light. Internal audit has ultimate accountability to report the truth.

– Chief Audit and Compliance Officer, United States

Compliance second line roles define policies, advise businesses regarding control design, advise and review business risk appetites, and provide assurance. Compliance individuals or departments may have responsibilities assigned to execute operational functions on behalf of the first line. In such cases, the compliance individual or department is not fully independent of the first line. Internal audit is the only fully independent activity due to its independence from the management decision-making of the first and second line.

– Head of Enterprise Risk and Internal Audit, United States

Principle 6: Create and protect value through collaboration

Principle 6 describes the importance of ensuring coordination and collaboration among all these roles.

Effective governance not only requires appropriate assignment of responsibilities but also strong alignment of activities through coordination, collaboration, and communication. Governing bodies rely on reports from management, internal audit, and others to exercise oversight and give direction to management to achieve objectives, manage risk, and create value. Governing body roles, together with first, second, and third line roles, collectively contribute to the creation and protection of value when they are aligned with each other and with the prioritized interests of stakeholders. Accordingly, clear communication of compliance responsibilities across the organization, decisioning rights, reporting obligations, risk appetite, common taxonomies, well-defined assessment entities or units, performance and risk reporting against requirements and expectations, and testing and assurance programs all serve to improve coordination and collaboration.

Practical Illustrations from the Field

An illustration of coordination and collaboration is, for example, data privacy. Compliance, or in certain organizations compliance in collaboration with the legal department, identifies the regulatory requirements, communicates them to the organization, and ensures appropriate processes and controls are implemented. The business teams (operations, IT, information security, etc.) implement the activities, including monitoring, escalation, and reporting of information as required. The information security team and compliance teams monitor key risk areas to ensure the business teams are following procedures and monitoring and reporting appropriately. Internal audit assesses the framework for managing relevant risks, including compliance risk, and related processes and controls undertaken by the business teams while auditing those areas.

– Chief Compliance Officer, United Kingdom

ESG is a great example of coordination and collaboration across the organization to achieve compliance with requirements and expectations. The first, second, and third line roles must work together, within their respective roles and with the oversight of the governing body, to achieve their desired ESG outcomes. Those with various responsibilities for compliance will work with others in the organization to achieve the organization's ESG objectives:

- **The governing body sets the strategy and risk appetite and provides the tone for culture and behavior.**
- **Management Integrates ESG requirements and expectations into the organization's governance and operations.**
  - **Provides advice, framework, and requirements on the content, design, and implementation of appropriate structures, systems, and processes for strategic and operational planning, goal setting, data collection, decision-making, and reporting related to ESG.**
  - **Assesses the risks associated with achieving compliance with ESG external requirements and standards, as well as internal policies and targets.**

        - **Develops standards, frameworks, principles, or models that should be adopted for measuring, monitoring, and reporting impacts on achieving ESG outcomes.**
        - **Evaluates the accuracy and consistency of data and methodologies used to collect data utilized in sustainability and ESG reporting.**
        - **Establishes measurements and evaluation processes; definition of materiality and listing of relevant indicators (KPIs); introduction of reporting methods, guidelines and tools (both internal and external).**
    - **Internal audit provides independent assurance to the governing body on the above activities and management's achievement of the ESG objectives, as well as to management reporting conformance with requirements and expectations.**

– Chief Compliance Officer, United Kingdom

Key Facts about Compliance

Ten important takeaways to note:

1. There may not be a dedicated resource, department, manager, etc., for compliance. Not all organizations are able or need to assign resources in this way. It is often as organizations become more complex, highly or specifically regulated, larger, subject to greater scrutiny, begin to operate in rapidly changing environments (regulatory, commercial, etc.), and start to address similar factors that they decide individuals, teams, systems, and/or other resources need to be assigned to aspects of compliance as a division of labor and formal component of organizational design. Such resources may be external in some organizations; for example, through outsourcing of certain compliance monitoring or subject-matter expertise.

2. In applying the Six Principles of the *Three Lines Model* to evaluate compliance-related roles, it is useful to consider the outcomes for which the role is responsible:

- Achieving compliance with laws, regulations, contracts, policies, procedures, codes of conduct, or other requirements in the provision of products and services.
- Providing specialist oversight; assessing risk (particularly on a collective or portfolio basis) and performing risk management activities; and credibly challenging the first line to promote and achieve compliance across the organization in accordance with applicable conduct codes or standards, requirements, and expectations.
- Providing an assessment on the adequacy and effectiveness of the compliance program.
- Providing expert challenge on the effectiveness of the compliance program and its components across the organization.

3. A single compliance role or department within an organization may not cover all compliance-related matters for that organization[8]. In such instances, the organization should clearly document the scope of the compliance role(s) or department(s) as well as which roles have responsibility for other requirements and expectations. This is as important for smaller organizations -- where an individual may be assigned multiple responsibilities and roles and some responsibilities may be outsourced -- as it is for larger organizations, where there may be multiple roles or departments charged with various compliance activities.

4. A compliance role or head of a compliance department may, in practice and subject to legal and regulatory requirements, report to one of a number of different roles in an organization, including: senior executive management (e.g., the CEO, the chief risk officer, chief operating officer, general counsel or others) and/or the governing body or committee thereof. In some instances, compliance, while part of management, may report to the CAE. The suitability of the reporting line may be determined in part by assessing responsibilities in accordance with the *Three Lines Model* and respective legal and regulatory requirements.

5. A compliance role or head of a compliance department may have a reporting line or reporting accountability to one or more board committees or chair of one or more board committees. However, this does not equate to independence from management and does not replace the need for independent assurance provided by internal audit.

[8] Ethics, sustainability, financial reporting, data privacy, human resources, and legal obligations, as examples, may have their own internal and/or external resource to achieve compliance or provide additional oversight and risk management for specific components of compliance. For example, the evolution of environmental, social, and governance (ESG) is seeing a range of new roles, responsibilities, activities, and departments within various organizations, focused on compliance with the wide-ranging aspects of ESG.

6. Individual compliance roles and compliance departments may include responsibilities including, but not limited to: compliance risk management broadly, monitoring, testing, analysis, assessment, advice, assurance, policy setting, development and implementation of systems and controls, management decisions, oversight, and training.

7. Compliance roles and departments may also include responsibilities that are closely or directly related to providing products and services. This would require a clear documentation of the responsibilities, authority, and accountability in the role (for example, the ability to prevent noncompliance in providing the product or service by forbidding a transaction or vetoing a management decision).

8. First and second line roles should be separated. Members of the first line should own the risk they take, while those in the second line should establish and oversee the frameworks and standards to assist the first line in managing the risks they own, while providing credible challenge to the first line's decisions and activities. In practice, depending on jurisdictional or industry requirements, and the organization's size, complexity, and other factors, there may be blended roles. In that case, an assessment of those roles' compatibility must be undertaken and any related risks mitigated. This may require adjustments of the composition of the roles to effectively mitigate the risks from an incompatible set of activities within a role. Responsibility for managing risk remains a part of first line roles and within the scope of management.

9. Regardless of how organizations structure their resources devoted to compliance obligations, management maintains the responsibility for ensuring the organization meets its requirements and expectations within the risk appetite parameters set by the governing body.

10. An essential responsibility of the second line compliance role is the assessment of the effectiveness of the organization's compliance program and efforts required to achieve the organization's compliance requirements and expectations.

ANNEX: Aligning Responsibility for Compliance Roles and Activities

Compliance activities are an essential component of an organization's governance, risk management, and internal control activities. Responsibility for the actions needed to achieve, support, check, and confirm compliance, and the execution of those responsibilities, may be assigned to various parts of the organization. Those responsible for compliance activities need to define the expected outcomes that constitute compliance and define appropriate measures to demonstrate achievement of those outcomes.

The activities that comprise compliance may include, but are not limited to, the following:

- Identify relevant external laws, rules, regulations and internal policies, standards, procedures, and codes of conduct and acceptable behavior consistent with organizational objectives.
- Determine appropriate risk measurement for compliance and noncompliance with relevant external laws, rules, regulations and internal policies, standards, procedures, and codes of conduct and acceptable behavior consistent with organizational objectives.
- Perform risk assessment for compliance with relevant external laws, rules, regulations and internal policies, standards, and procedures, including future and emerging risks, and codes of conduct and acceptable behavior consistent with organizational objectives.
- Design, develop, and implement processes and controls to achieve compliance with relevant external laws, rules, regulations and internal policies, standards, procedures, and codes of conduct and acceptable behavior consistent with organizational objectives.
- Perform, maintain, and manage processes and controls to achieve compliance with external laws, rules, regulations and internal policies, standards, procedures, and codes of conduct and acceptable behavior consistent with organizational objectives.
- Evaluate, test, and monitor, compliance with relevant external laws, rules, regulations and internal policies, standards, procedures, and codes of conduct and acceptable behavior consistent with organizational objectives.
- Provide credible challenge to management in respect of compliance risk.
- Manage and mitigate compliance risk.
- Determine instances of compliance or noncompliance.
- Inform and escalate instances of noncompliance.
- Report compliance or noncompliance in accordance with external and internal requirements.
- Foster a culture conducive to compliance.
- Raise awareness through communication, training, promotion, and education.
- Consult and advise on aspects of compliance.
- Establish and maintain an ethics or whistleblowing program.
- Develop and provide compliance training, education, and awareness.
- Perform the regulatory liaison responsibilities between regulatory agencies and the organization.

- Establish and maintain relationships with professional organizations and industry bodies to identify relevant standards, codes, or guidelines by which the organization and its respective activities should or may choose to adhere, as well as facilitating the gathering and reporting of benchmark information.
- Establish and maintain liaison relationships with industry infrastructure organizations which may establish and require conformance with requirements or expectations for infrastructure users and counterparties.

It is important that the responsibilities, and the desired outcomes, of each role are clear. Some of these roles and activities are incompatible with other roles, such as transaction approval, customer acceptance, or other business risk decision-making within third-line responsibilities, as detailed in the *Three Lines Model*. Where internal audit is asked to assume such roles, key safeguards are needed, including the consent of the governing body or audit committee, the use of a third party to provide independent assurance in affected areas, and, where appropriate, regulatory approval.

Likewise, even with the best intentions to achieve the outcome of providing products and services to clients in compliance, an organization must be vigilant to identify roles, the responsibilities of which are designed both to achieve compliance in providing the product or service, and to provide the oversight and broader compliance risk management. The basic principles of segregation of duties and independence apply, as does the expectation to mitigate the risks arising when incompatible activities in roles are identified.

Similarly, at times there is a temptation by those in oversight roles, when identifying gaps or deficiencies in the risk management and control activities underpinning the provision of products or services, to expand their own scope beyond oversight into execution. The inverse can be true, as well, where the first line can place too much reliance on those roles providing oversight or with risk management responsibilities. This undermines the benefits of objective oversight. In such cases it is incumbent on the oversight role to identify, escalate, and monitor the gap or deficiency, and management's remediation. These elements should be aligned and documented in accordance with established governance roles and responsibilities.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Disclaimer

Copyright

January 2022

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101