CEP Magazine - October 2020
Building an IT compliance center of excellence

By Anushree M. Bag, PMP, MS EE

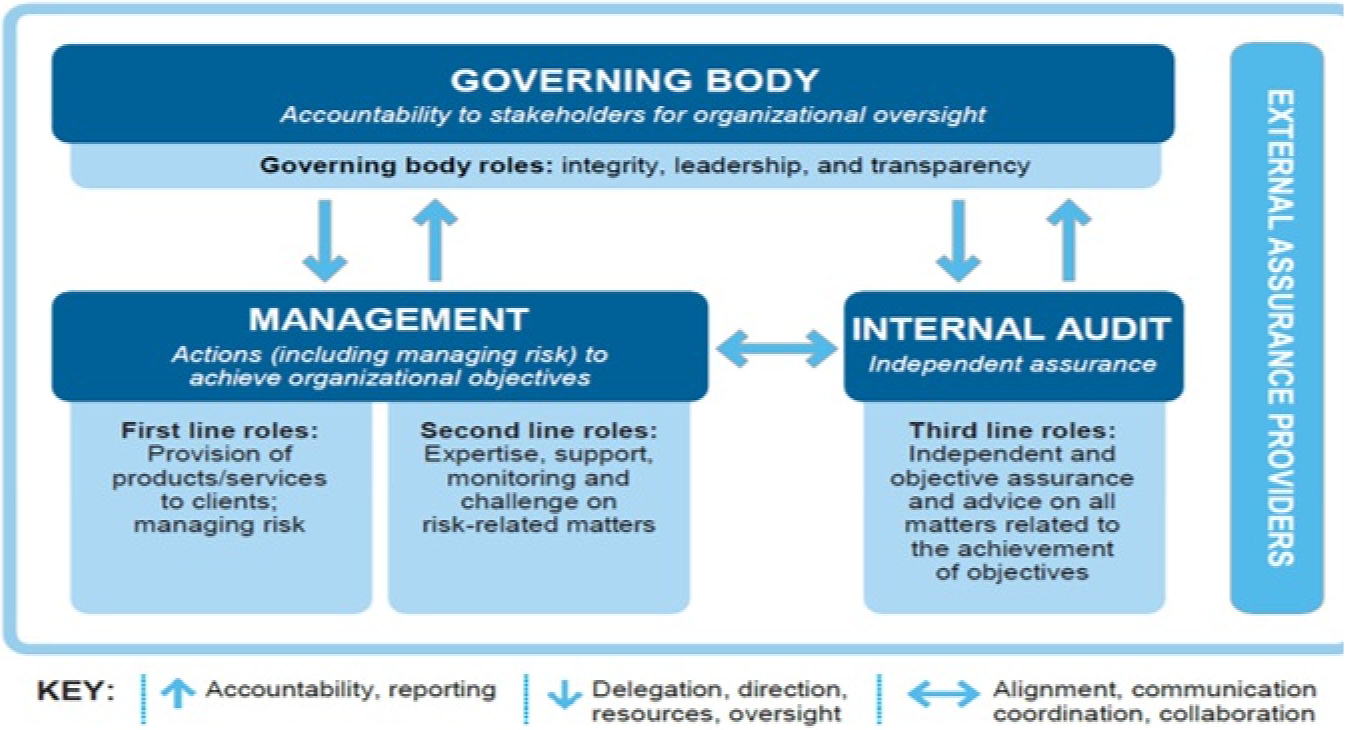
Anushree M. Bag (abag@iot.in.gov) is Executive Director of Risk and Compliance for the Indiana Office of Technology in Indianapolis, Indiana, USA.

In today’s business world, where known unknowns and unknown unknowns are becoming increasingly prevalent, organizations are being challenged to adopt a business-focused, technology-driven agile mindset. As the business landscape becomes more global, complex, and fast moving, it is critical for organizations to anticipate, identify, and respond to emerging information technology (IT) security and privacy risks quickly and effectively to stay ahead of the game. This article explores the role that an IT compliance center of excellence (CCoE) plays in developing a structured, disciplined approach to managing IT risks.

The starting point: The Three Lines Model

The Institute of Internal Auditors’ (IIA) Three Lines Model (Figure 1) is a straightforward and effective way to help enterprises coordinate the IT security risk and compliance management duties through a systematic approach. It helps to assure the success of governance, risk management, and compliance (GRC) initiatives, regardless of the size and complexity of the enterprise. The Three Lines Model is distributed between various functionalities of an organization and distinguishes the functionality among three groups: (1) functions that manage and own the risks, (2) functions that oversee risks, and (3) functions that provide independent advice.

Figure 1: IIA’s Three Lines Model


GOVERNING BODY
Accountability to stakeholders for organizational oversight
Governing body roles: integrity, leadership, and transparency
MANAGEMENT
Actions (including managing risk) to achieve organizational objectives
First line roles: Provision of products/services to clients; managing risk
Second line roles: Expertise, support, monitoring and challenge on risk-related matters
INTERNAL AUDIT
Independent assurance
Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives
EXTERNAL ASSURANCE PROVIDERS
KEY:
Accountability, reporting
Delegation, direction, resources, oversight
Alignment, communication coordination, collaboration

Source: The IIA's Three Lines Model. Copyright © 2020 The Institute of Internal Auditors, Inc. All rights reserved. The IIA's full article can be found at: https://bit.ly/34hZGWh.

The IT compliance center of excellence

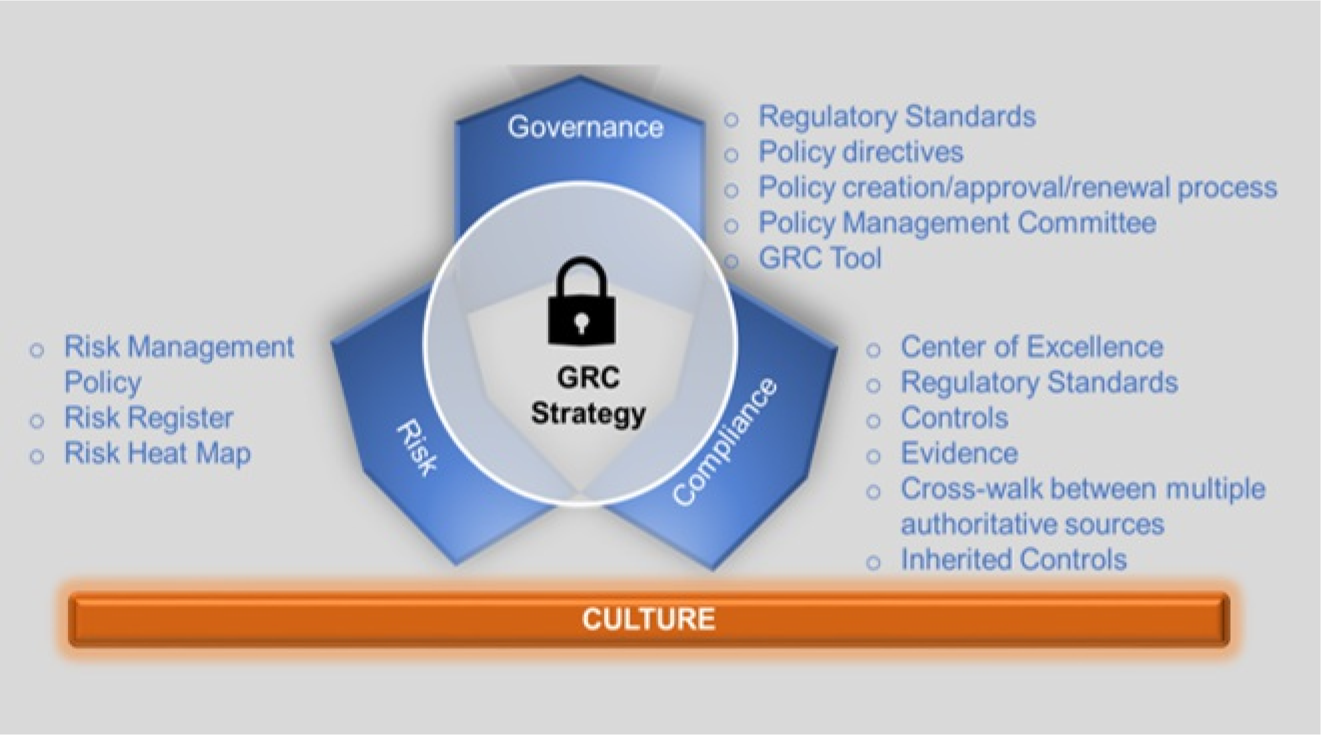
The CCoE is a second-line role, with a focus on expertise and support related to compliance with laws and regulations for IT privacy and security. The CCoE has two primary overarching objectives: (1) establishing a GRC strategy (Figure 2), which should be aligned with the organization's strategy, goals, and mission; and (2) influencing, promoting, and advancing a risk- and compliance-aware culture in the organization. Over time, the CCoE should become a team of specialists who would collaborate to develop and promote compliance best practices across the various business units of the organization.

GRC strategy

Businesses need to manage policies; demonstrate compliance; and identify, analyze, and manage risks while ensuring that trust and assurance are maintained within a complex IT infrastructure. A GRC tool serves as a platform for aggregation and consolidation of GRC information across the business.

The term "GRC" was spawned from the need for better internal control and governance in enterprises, determined by the U.S. Sarbanes-Oxley Act in 2002. Over time, GRC evolved to become associated with compliance-driven initiatives designed to improve corporate governance and internal control.

Figure 2: The GRC strategy



Governance

IT governance is a formal framework that shows senior management that IT investments support business objectives. The National Institute of Information Security's Security and Privacy Controls for Federal Information Systems and Organizations[1] is the premier regulatory document for all IT security and privacy controls. It provides a catalog of security and privacy controls for all federal information systems and organizations, except those related to national security. The first step to implementing governance is to establish policies with a documented process and roles and responsibilities for creation, review, and oversight.

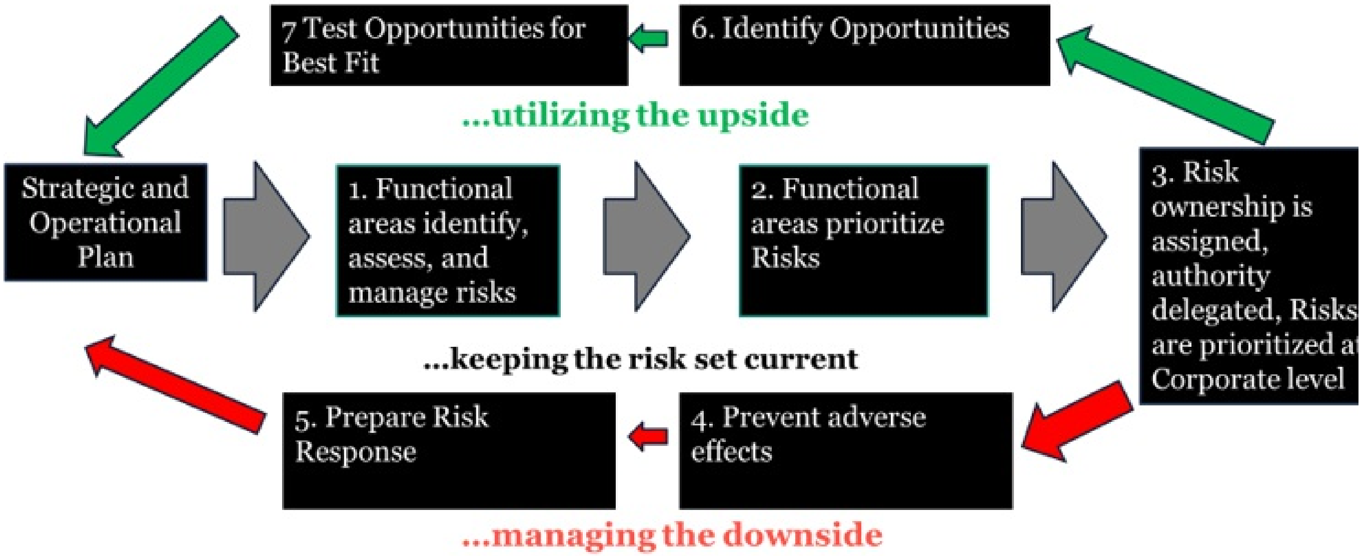
Policies

- Develop policies that capture processes and procedures that the organization has established to meet each National Institute of Information Security control across the 18 control families.[2]
    - Policy examples: access control, acceptable use of information technology resources, change management, data classification and categorization, disaster recovery, information security training and awareness, laptop security, secure file transfer, records retention schedule, remote access, vulnerability management
- Ensure that each policy has defined controls for future demonstrations of operational compliance with the policy.
- Ensure that each policy has defined roles and responsibilities.
- Establish a cadence for review of existing policies, such as annual.
- Develop a process to capture evidence that policies are being followed.

Committee

- Establish committee membership with people who have authority and expertise to oversee and approve the development of IT privacy and security policies.
- Establish a process for development of new policies and revision of existing policies.
- Establish roles and responsibilities, such a policy owner, executive sponsor, and steering committee.
- Develop a workflow for the approval and review processes.

Figure 3: Risk management plan


7 Test Opportunities for Best Fit
6. Identify Opportunities
...utilizing the upside
Strategic and Operational Plan
1. Functional areas identify, assess, and manage risks
2. Functional areas prioritize Risks
3. Risk ownership is assigned, authority delegated, Risks are prioritized a Corporate level
...keeping the risk set current
5. Prepare Risk Response
4. Prevent adverse effects
...managing the downside

Risk

The current IT ecosystem includes an interconnected network of appliances—workstations, servers, network devices, switches, firewalls, databases—that all need to work together to ensure the smooth delivery of products and services. Every piece of the network introduces some risk, and the more effectively that IT organizations can understand and manage these risks (Figure 3), the better their resilience will be. Risks can have both downsides and upsides. A risk management plan should include:

- Risk identification,
- Risk analysis and prioritization,
- Risk treatment,
- Risk monitoring, and
- Risk control.

The selection of risk treatment strategies should be based on a multitude of factors. These include the magnitude and frequency of the risk, should it actually materialize. The magnitude is a function of the criticality or sensitivity of the resource. Risk management options include:

- **Treat**: Where rational consideration is made for taking the risk, but mitigation strategies are put in place, and the risk is actively monitored.
- **Tolerate**: A conscious strategy of accepting risks where the reward outweighs the risk.
- **Transfer**: A control strategy that involves contractual shifting a risk from one party to another, such as through purchase of an insurance policy.
- **Termination**: An approach taken to avoid taking the risk, since it is higher than the established risk appetite and risk tolerance of the organization.

Every organization has some level of investment in IT, and with every new technology comes new security and privacy risks. While it is imperative that we take risks in order to grow, we need to be diligent about managing both the upsides and downsides of those risks. The CCoE should provide guidance to organizational leadership to create a risk appetite (the level of risk that an organization is prepared to accept in pursuit of its objectives), a risk tolerance (the degree of variance from the organization's risk appetite that the organization is willing to tolerate), and a formal risk management plan, all of which should be embedded in the organization's strategic and operational processes.

The CCoE should also work with organizational leadership to establish its risk appetite and risk tolerance. Risk appetite is a description of the desired level of risk that an entity will take in pursuit of its mission, while risk tolerance reflects the acceptable variation in outcomes related to specific performance measures linked to objectives that the entity seeks to achieve.

Compliance

Organizations that deal with personally identifiable information or federal tax information are subject to regulatory IT compliance, such as Security and Privacy Controls for Federal Information Systems and Organizations and more. A CCoE facilitates an organization's response to IT regulatory standards by facilitating the following functions:

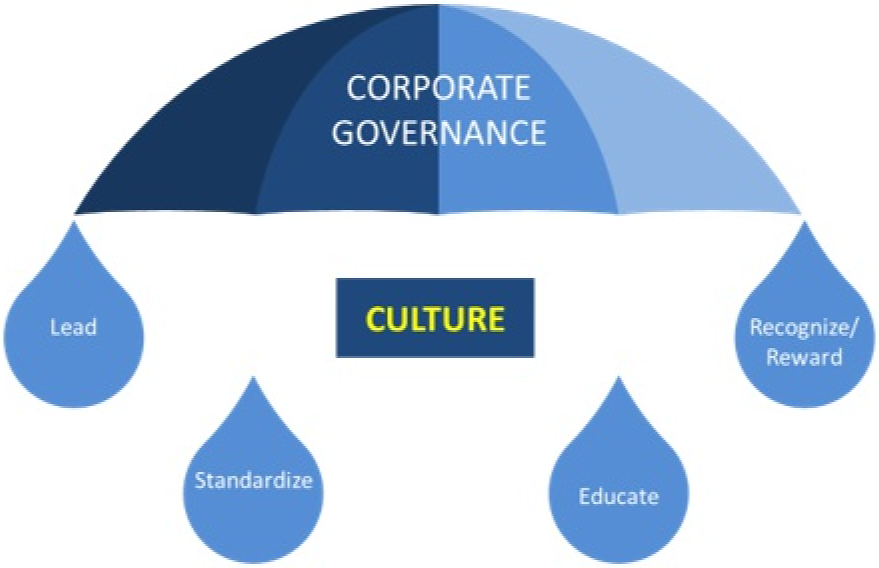
- Establishing IT privacy and security controls to meet the regulatory standards.
- Selecting and implementing a GRC tool to use as a system of record for all GRC activities.
- Documenting how the organization is responding to the baseline regulatory requirement.
- Conducting a crosswalk (i.e., identifying associations) between the baseline requirements and other authoritative sources (the Internal Revenue Service's Tax Information Security Guidelines For Federal, State and Local Agencies;[3] the Centers for Medicare & Medicaid Services' Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges;[4] FedRAMP's guidance documents;[5] etc.) and document the relationship. Note if there is a full or partial match.
    - A full match is when the baseline regulatory requirement fully matches another authoritative source's regulatory requirement. A partial match is when the baseline regulatory requirement partially matches another authoritative source's regulatory requirement.
    - For the full matches, the controls applied to meet the baseline requirements can be inherited from the other authoritative sources. For the partial matches, additional actions need to be documented to meet the differential requirements of the authoritative source that are not covered by the baseline regulatory requirement.

Culture

An essential but often silent aspect of GRC is culture. GRC increases compliance effectiveness, enhances risk management, and results in better governance, but it needs the right organizational culture to thrive.

Should a culture of compliance be grown or enforced? Enforcement may yield quick results, but it usually only works under supervision and monitoring, and it does not change behavior. Over time, people who are forced to behave in a certain way may fall back to the same wrong choices once they are no longer being monitored. Culture takes more time to produce results, but it results in compliance being embedded into the fabric of organizational performance. To do this effectively, it is recommended that the following actions be taken (Figure 4):

Figure 4: Corporate governance framework



- **Lead**: Leaders of organizations should contribute to the GRC culture by setting the example—lead from the front. When leaders adopt a GRC culture, others follow the example.
- **Standardize**: Establishing a standard framework with standard terminologies and best practices is critical to driving a successful adoption of the GRC framework. When the standard framework is simple and easy to follow, employees are more likely to embrace it, and leaders are better able to review performance and make good decisions.
- **Educate**: It is imperative that employees appreciate and value the GRC directives in place, so employees need to be educated on becoming cognizant of how they can contribute to the firm's success by adopting a GRC strategy. The organizational culture needs to be conducive to understanding and appreciating the benefits of a disciplined GRC approach.
- **Recognize/reward**: GRC practices should not be seen as something that gets in the way of doing a job but rather something that is a valuable part of the job. To ensure that GRC is embraced, it should be embedded within performance objectives. Additionally, where applicable, creating recognition and/or financial incentives, such as spot bonuses, may promote the adoption of a robust GRC culture. Efforts should be made to highlight and recognize GRC successes, as they may motivate others to adopt GRC as well, thereby improving the overall organizational GRC culture.