FEATURE

Roles of Three Lines of Defense for Information Security and Governance

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2sLKf4m

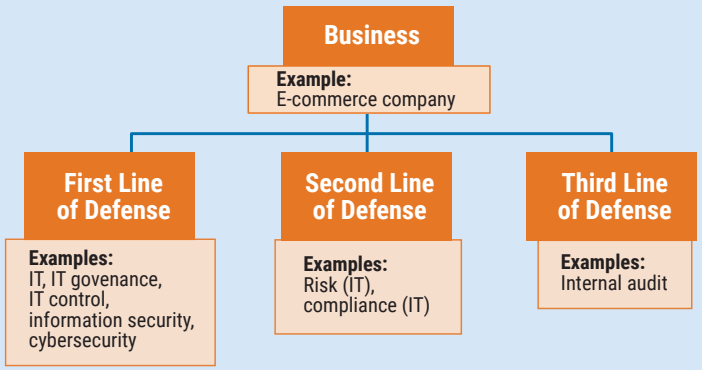
Disponible également en français
www.isaca.org/currentissue

While the three lines of defense covering assurance, governance, risk, compliance, information security and cybersecurity functions can all be working in one way or another on information security and governance, one can examine the objectives, roles and activities of these functions to explore ways to optimize outputs. Optimized outputs means the combined outputs of the various parties working on information security are maximized, which allows resources to be better deployed with increased productivity by reducing duplication.

Roles and Responsibilities of Various Functions

Organizations aim to achieve their objectives while managing risk within their risk appetites. A good governance structure for managing risk is to establish three lines of defense. Briefly, the first line of defense is the function that owns and manages risk. Within the first line of defense, businesses can set up control functions (e.g., IT control, which reports to the IT department) to facilitate the management of risk. The second line of defense is the independent control function (e.g., IT risk, IT compliance) that oversees risk and monitors the first-line-of-defense controls. It can challenge the effectiveness of controls and management of risk across the organization. The third line of defense is internal audit, which provides independent assurance. **Figure 1** provides examples of the functions under the three lines of defense.

Figure 1—Three Lines of Defense



Various business functions aim to ensure organizations are managing risk within their risk appetites. In particular, IT governance provides the consistency, processes, standards and repeatability needed for effective IT operations while monitoring the budget and compliance with regulatory and/or organization requirements. IT risk management must function as part of the enterprise risk management framework and address various types of risk and the challenges and opportunities the risk presents. It helps focus IT governance, security and privacy investments in the areas most critical to the achievement of organizational objectives. Information security aims to protect data and information systems from inappropriate access, manipulation, modification and destruction, thus ensuring systems/data confidentiality, integrity and availability. Cybersecurity, which includes technology, processes, policies and people, focuses on using business drivers to guide security activities while ensuring that cybersecurity risk factors are included in the organization's risk management processes.[1]

The assurance function is internal audit, whose mission can be defined to enhance and protect organizational value by providing risk-based and objective assurance to evaluate the effectiveness of governance, risk management and control processes.[2]

Amelia Ho, CISA, CISM, CA, CFE, CIA, CISSP, FRM, PMP
Is a senior vice president with Citibank and has more than 20 years of experience in the financial services industry in a number of internal audit, risk management and compliance roles. She has contributed to ISACA as an article author and expert reviewer of ISACA publications. She is the recipient of the 2013 Ted Keys Honorable Mention Award for her article "Emerging Risk Audits" in *Internal Auditor* published by The Institute of Internal Auditors.

Organization Structure of Various Functions

Different teams can be organized in various ways, as shown in **figures 2** and **3**. **Figure 2** illustrates how the IT risk, information security and cybersecurity teams can be organized in a hierarchical way. Under this organizational structure, there is less chance that their tasks/activities are duplicated because cybersecurity is within information security, which means the latter is fully aware of the former's activities and role. **Figure 3**, on the other hand, is an example of IT risk, information security and cybersecurity teams organized in a flat structure, as counterparts of each other. With this kind of organizational structure, there is a higher chance that their activities will overlap because the different teams may not be aware of what each other is doing. For instance, the information security team can be reviewing information security settings and controls over all operating systems, whereas the cybersecurity team can be reviewing web server settings and controls that may cover the same server. Another example may be information security being responsible for disaster recovery planning or service level management, while the cybersecurity team is responsible for addressing denial-of-service (DoS) risk; whereas, disaster recovery and service level management are controls to address DoS risk.

Figure 2—Hierarchical Organization Structure

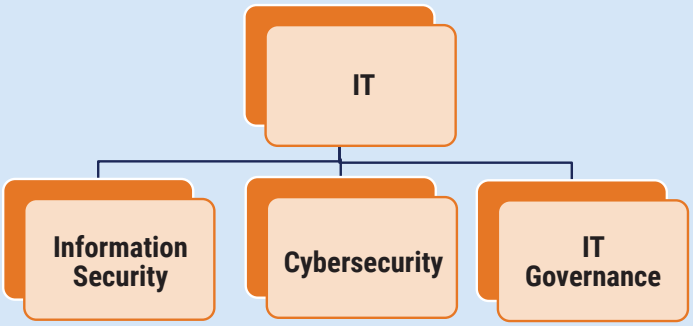
Activities of Various Functions and/or Three Lines of Defense

To achieve the organization's ultimate goal of managing risk (e.g., information and technology risk) within its risk appetite, various business functions and/or the three lines of defense have to perform activities such as information gathering, risk assessment, reviews, analysis, reporting and monitoring of risk that may be common among the three lines. One way to find out these commonalities is through frequent communication, which facilitates information sharing. To facilitate communication and discussion of risk within an organization, different business functions can use the same set of risk categories and taxonomy.

Sharing of Inputs

Various business functions working on IT risk can share useful internal information such as source information (e.g., transaction data), risk information (e.g., trends or statistics such as web application availability percentage) and internal loss data (e.g., IT security incidents including details and/or nature of incidents). Through the sharing of

Figure 3—Flat Organization Structure



internal information, business functions can fulfill their duties by conducting respective analysis, risk assessment and monitoring, and control review planning (e.g., compliance or audit planning).

Also, information can be shared within the industry through an external loss database, just as ORX stores loss data for the banking and insurance industry. Through the sharing of external risk information, various business functions can be better informed on how to detect and prevent similar risk. For example, in 2016, there was an unauthorized money transfer request through Bangladesh Bank,[3] detected by one of the routing banks that flagged the transaction for further review solely because of the misspelled word "fandation," which resulted in the transfer being stopped.

> "THROUGH THE SHARING OF EXTERNAL RISK INFORMATION, VARIOUS BUSINESS FUNCTIONS CAN BE BETTER INFORMED ON HOW TO DETECT AND PREVENT SIMILAR RISK."

Information can also be shared within a country. For instance, Cyber Security Information Sharing Partnership (CiSP)[4] of the United Kingdom is a joint industry/government initiative set up to exchange cyberthreat information in real time in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK organizations. Information can also be shared among countries. For instance, there is intercountry sharing such as the Asia Pacific Computer Emergency Response Team (APCERT) to encourage and support cooperation among national CERTs in the Asia Pacific (APAC) region. APCERT maintains a trusted network of computer security experts in the APAC region to improve the region's awareness and competency in relation to computer security incidents.[5]

Sharing of Processing

Besides sharing of inputs, processing can also be shared. Different functions may be using tools to develop monitoring measures for preventive and/or detective purposes. Sharing these tools can reduce duplication of work among various teams. For instance, either the first or second line of defense may be adopting regtech (an application of technology to ensure compliance with the latest requirements from regulators and/or the company) or using machine learning to detect distributed DoS (DDoS) attacks based on detection of similar past patterns of DDoS. Tools developed by the first line can be used by the second line and vice versa. Internal audit can develop automated scripts to perform testing or continuous auditing (e.g., use of bots to go to service providers' websites to check whether the latest system patches or virus signatures are used by the organization), which can also be used by the first or second line of defense for continuous monitoring purposes.

Sharing of Outputs

Results of reviews conducted by one party can be shared. For instance, the first line of defense can conduct a self-check of adherence to the Hong Kong regulators' (Hong Kong Monetary Association) e-banking guidelines for compliance management; the second line of defense can use this self-check for regulatory reporting.

Another example is the governance function. The second and third lines of defense can use the first line's exception reporting and/or third-party (e.g., regulator or external auditor) control review results for identification of systemic issues. The third line can also use the first or second line's control review results for assessing the effectiveness of the first and second lines of defense.

Work of the Assurance Function

While the reviews performed by the assurance function can be similar to those conducted by the first or second lines of defense, only the internal audit department or external service providers can provide the required assurance because they are functionally independent from the business and have reporting lines and a mandate that differs from those of the first and second lines of defense. Hence, audit teams need to conduct certain work to evaluate the effectiveness of governance, risk management and control processes.

There are various reviews that can be conducted by audit teams. If the audit teams conduct re-performance, it is not economical because it duplicates efforts by re-performing a control such as checking extracting sampled emails to identify any unencrypted customers' personally identifiable information (PII) or independently checking the accuracy of processing by the company's application. Even if the audit team re-performs a control, such as application control, for the first year, audit can nonetheless reduce the extensive control re-performance work in a subsequent year (hence saving time and effort while achieving the desired assurance) by performing other tests such as change management controls or a check of the last date of change to see if any change has been applied since the last audit, when the re-performance test was conducted to confirm accurate processing of the company's application.

"THE AUDIT FUNCTION'S APPROACH TO, AND AMOUNT OF, CONTINUOUS AUDITING DEPENDS ON THE EXTENT TO WHICH MANAGEMENT HAS IMPLEMENTED CONTINUOUS MONITORING6 AND ITS EFFECTIVENESS."

Audit can also perform continuous auditing to provide assurance on a more timely basis, based on a bigger data population being tested. However, the scope of continuous auditing can potentially be reduced if management has implemented similar and effective continuous monitoring. There is an inverse relationship between the adequacy of management's monitoring and risk management activities and the extent to which auditors must perform detailed testing of controls and assessment of risk. The audit function's approach to, and amount of, continuous auditing depends on the extent to which management has implemented continuous monitoring[6] and its effectiveness.

Economic Allocation of Resources

If a business function lacks the resources to perform the required tasks, it can consider obtaining the resources internally. For instance, IT's Sarbanes-Oxley Act (SOX) testing can be conducted by internal resources such as the internal audit/compliance/risk team, depending on which team has the required resources, as all functions meet the requirements for performing SOX testing.

For regulator-mandated reviews that require an independent party to conduct, an organization can

Enjoying this article?

- Learn more about, discuss and collaborate on information security management in the Knowledge Center. *www.isaca.org/information-security-management*

choose internal resources with adequate skills for fulfilling the requirement because internal resources are usually less costly than external resources. If internal resources do not have the requisite skills/tools (e.g., penetration tests or ethical hacking) and cannot provide the required assurance, then external resources should be hired, irrespective of the relatively higher costs involved.

Conclusion

When examining the roles and objectives of the three lines of defense covering assurance, governance, risk, compliance, information security and cybersecurity, there can be common or overlapped activities. A hierarchical organization structure can reduce the chance of duplicated tasks/activities among functions or teams because each team is more aware of the role and activities of the other teams within the hierarchical structure. Another way to optimize outputs and save resources and costs for the organization is to share inputs, processing and outputs of various business functions and teams (including output of industrywide and countrywide public or nonprofit organizations), which can be used to streamline each function's activities.

The assurance function, however, can be delivered only by independent parties such as the internal audit team and external providers. Internal resources would be less costly than external resources, but the former may not have the required resources to conduct certain tasks. For these cases, external service providers may be required despite the relatively higher costs involved to ensure the required assurance is provided.

Author's Note

Opinions expressed in this article are the author's and do not necessarily represent the views of Citibank.

Endnotes

1 Lainhart, J W.; Z. Fu; C. Ballister; "Holistic IT Governance, Risk Management, Security and Privacy: Needed for Effective Implementation and Continuous Improvement," *ISACA® Journal,* vol. 5, 2016, *https://www.isaca.org/Journal/archives/Pages/default.aspx*

2 The Institute of Internal Auditors, "Supplemental Guidance, Model Internal Audit Activity Charter," 2017, *https://iia.no/wp-content/uploads/2017/04/2017-SG-Model-Internal-Audit-Activity-Charter.pdf*

3 Schwartz, M.; "Bangladesh Bank Hackers Steal $100 Million," Bank Info Security, 10 March 2016, *https://www.bankinfosecurity.com/bangladesh-bank-hacers-steal-100-million-a-8958*

4 National Cyber Security Centre, Cyber Security Information Sharing Partnership, 20 March 2018, *https://www.ncsc.gov.uk/cisp*

5 Asia Pacific Computer Emergency Response Team, *https://www.apcert.org*

6 Coderre, D.; "Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment," The Institute of Internal Auditors, 2005, *https://www.iia.nl/SiteFiles/IIA_Ieden/Praktijkgidsen/GTAG3.pdf*