itworldcanada.com

Understanding cybersecurity management for FinTech : information security governance in FinTech (Article 2) - IT World Canada

Gurdip Kaur and Arash Habibi Lashkari

10-13 minutes

Information is the key to success in the contemporary era. Just as there are two sides of a coin, there are two perspectives of a cyber-attack. On one hand, attackers seek information to take advantage of potential flaws in an organization's architecture, processes, and design; exploiting these flaws to make money. The prime targets in the organization are its information-based assets. On the other hand, organizations safeguard information to protect it from getting stolen and misused. Thereby, information can be secured by governing an information security system.

With the rising sophistication, the threats to information-based assets are much higher than in the past. With the advancement of technology, tools to gain unauthorized access have also become powerful. This increases the need to secure information as an asset.

This article uncovers information security governance in FinTech, and provides deep insights into its characteristics, principles of good governance, and an integrated security governance framework. The content in this article is based on the extensive research work behind our book titled ‘Understanding Cybersecurity Management for FinTech’ published by Springer this year.

What is information security governance?

Information security governance combines information security, and governance. Let us define these two terms separately first. Information security ensures that personal, private, confidential, and sensitive information is protected. Governance is the set of responsibilities and practices exercised by responsible individuals in an organization.

A comprehensive definition of information security governance is: *Information security governance is the practice of securing information and managing cyber risks to protect any kind of information required for effective working of the organization, in compliance with the information security policy and risk management strategy.*

Importance of securing organizational information

Information security is an important part of enterprise-level security governance. It interacts with information technology (IT) operations, IT projects, and IT governance, where IT operations are considered current state of IT and IT projects are considered future state of IT.

Figure 1 demonstrates the basic structure of information security governance in an organization. At the top-level of the enterprise exists corporate governance, which evaluates the standards and policies. It also directs the middle- and low-level management consisting of: IT governance, information security, IT operations, and IT projects. On the contrary, the bottom-up approach monitors the governance activities for the corporate governance.

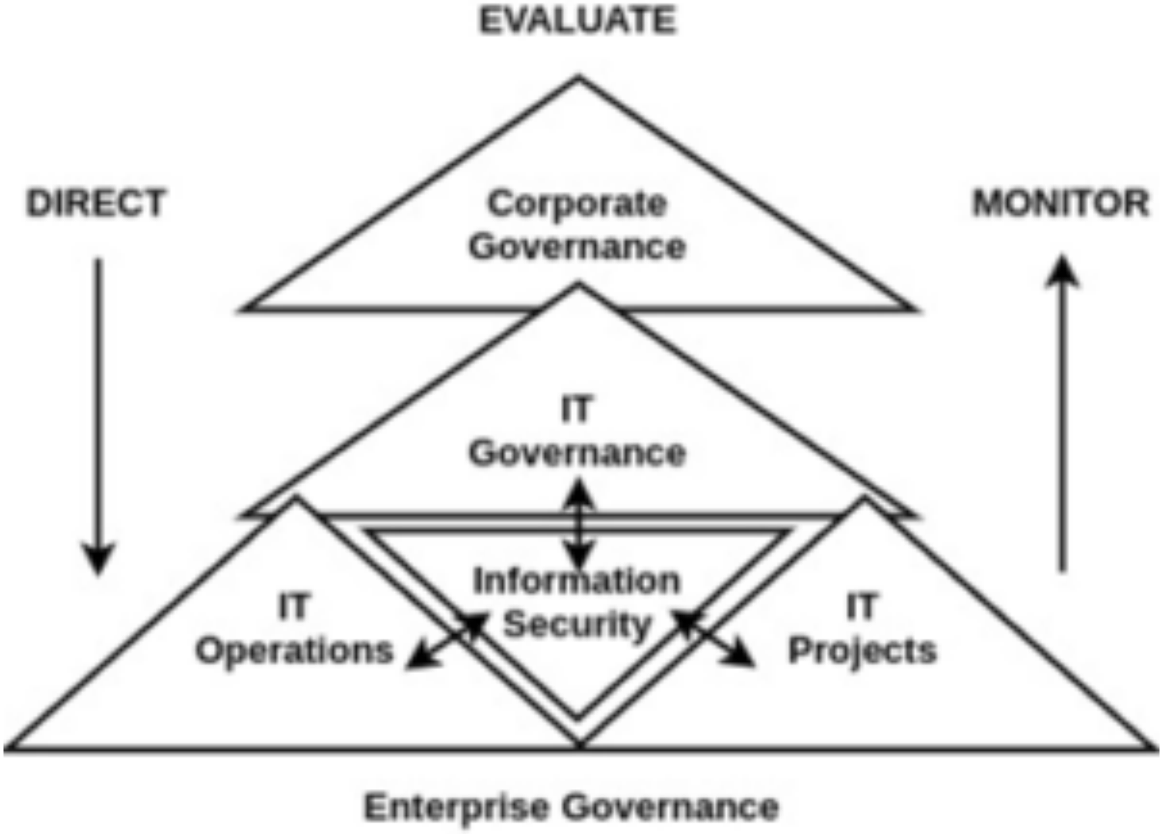

Figure 1: Information Security Governance

Overall, information security governance performs following activities:

- Promotes valuable information security practices with a clear direction from top to bottom
- Controls the risk appetite of the enterprise by considering different domains, such as legal, finance, information technology, and regulatory compliance
- Creates an overall information security activity that reflects organization’s needs and risk appetite levels

- Monitors corporate governance policies and standards for managing information security governance standards

Characteristics of effective information security governance

Effective information security governance has several characteristics, such as: involving appropriate organizational personnel, a governance framework, risk management, deliverables, and tackling changing risk levels.

1. *Appropriate organizational personnel:* Appropriate organizational personnel includes: a board of directors, executive management, business managers, and internal auditors. These personnel are involved in designing governance policies, implementing them throughout the organization, and performing internal auditing so compliance with governance standards can be validated. These individuals lead from the front to: provide an insight into the corporate culture, provide leadership, and dedicate resources; while also contributing to the implementation of information security activities, validating them, and recommending improvements.
2. *Governance framework:* A governance framework provides guidelines for the board of directors and executive management to develop an audit plan. These frameworks help the organization to operate in a structured, consistent, and effective manner – such that it can be explained easily to all stakeholders, regulatory agencies, service providers, and other parties in the business. Well planned governance frameworks can help guide future business changes and activities.