COMPONENTS OF INFORMATION SECURITY FRAMEWORK

A simple understanding of Information security framework components and their importance

By Madireddy Venkat

BE, MBA, CISA, CISM

A framework represents a concept or set of concepts. An information security framework is a conceptual representation of information security management. The information security framework should define the educational, technical, operational, managerial and administrative components of the information security program. The framework should also define the organizational units and the leadership responsible for each component, the objective of each component and the interfaces and information flow among the components.

In this paper we will try to understand the information security management framework from the functional component perspective, and by understanding we can ensure that every aspect is represented and accordingly given security consideration.

Technical components: Majority of the IT components require information security. To provide information security most of these IT components must be protected with security controls based on the risk identified with these technical components, risks from configuration, maintenance and operation. For majority of these IT systems IT is not the owner, they are only the “custodians”. Every technology component must have an owner. Responsibility and accountability must be clearly established for maintaining all IT systems according to the security policies and also for treating risks to acceptable levels. The information security function must ensure policy compliance and maintain risk to acceptable levels to achieve the information security objectives.

Operational components: Operational components of information security are those administrative activities in the organization that are performed on a day-to-day basis. These include Standard Operation procedures (SoPs), security practices in business operations, maintenance of security technologies. Since most of these components fall outside the information security function it is important for the information security manager to work with the other functions/department such as IT and business units and support them to provide operational security needs and have oversight. Some of the operational components where support is needed are: System patch processes, configuration management, change management, release management processes. For each of these operational components of information security the information security management must work with the owner and document the information necessary for the management of these functions. The information that need to be documented should be execution roles, inputs, process steps, escalation procedures, metrics, success criteria, and approval and review process. information security manager should ensure procedures for log maintenance, issue escalation, and continuous risk assessment is developed, and maintained. Roles and responsibilities documentation should be updated for all these operational components as new tasks may be designed for these operational components.

Management components: Management components include continuous communication with all business units to get feedback that can be helpful to information security management in ensuring

effectiveness and ensure alignment with organization objectives. Information security manager is also responsible for key management components like Information security program execution, monitoring of initiatives, development of standards and policy reviews Making adjustments to policies and standards should be driven by the continuous analysis of threats to assets, risks and the impact on the organization, therefore the information security manager must be flexible in making adjustments to the policies and standards during the beginning stages of the security program. There should be senior management oversight to ensure fulfilment of the requirements that are consistent with the strategy and the oversight can be in the form of review the effectiveness of program, review the KPIs, and any issues impacting the achievement of objectives and any modification to technical or operational components.

Administrative components: As Information security function matures and grows the dependence on finance, human resources also increases, therefore the information security manager must ensure that the human resources and finance and other functions are also effective. The information security manager must ensure that financial policies are adhered to, and also update the finance function regularly about the budget requirements of information security. The information security manager must develop a good working relationship with finance and must comply with all financial procedures and policies.

The information security manager must consider the time and activities needed for human resource function like recruitment, hiring, time tracking, employee education and termination management as the information security program staffing requirements grow. The Information security manager must build rapport with human resources and work closely and adhere to the procedures of the HR function. It is very common for information security manager to be under pressure to short cut information security or divert resources from operations to projects. The information security manager must make the management understand the risk of moving an initiative without full diligence.

Educational components: The information security manager must collaborate and work with human resources and all business units to identify the information security training needs. Employee orientation and induction training must include information security risks and policies. Other policies such as acceptable use policy and disciplinary policies must be administered by the HR function. Policies and procedures specific to employee role must be administered by business unt. Metrics designed to monitor employee training should be designed, tracked and communicated to senior management.