Information Security Management System (ISMS) Implementation: Examining Roles and Responsibilities

"Security is everyone's responsibility".

Everyone have roles and responsibilities for maintaining security in organization. The management, technical people, employees, vendors and contractors have different roles in developing and implementing an effective security process. For this article, we will look at the roles and responsibilities of management, Information Security Department and users in implementing and maintaining information security management system (ISMS) in organization.

Management's responsibilities

Management's responsibility goes beyond the basics of support. They must set the tone for the entire program. It is not enough just to bless the program. Management must own up to the program by becoming a part of the process.

Management is responsible for overseeing the development, implementation, and maintenance of ISMS. This includes defining the information security objectives of the organization, allocating an amount of money to be invested in information security, and ensuring the compliancy and enforcement of implementation.

Management has specific goals for the organization, and sometimes technical people are not in the position to understand these nuances. Both groups should understand that security is not something that can be wrapped in a package and bought off the shelf. It should be a goal that both parties strive to maintain. One of the ways to bridge the divide is by setting up an Information Security Management Committee. It is the responsibility of management to form this committee that will be responsible for reviewing changes in the business and determining how ISMS implementation should support those changes. To make this committee success, it is good to distribute the responsibilities throughout the organization depending on the institution's size, complexity, culture, nature of operations, and other factors. The distribution of duties should ensure an appropriate segregation of duties between individuals or organizational groups.

Management should also ensure integration of security controls throughout the organization by performing the following:

- Ensure the security process is governed by organizational policies and practices that are consistently applied,
- Require that information with similar criticality and sensitivity characteristics be protected consistently regardless of where in the organization it resides,

- Enforce compliance with the security program in a balanced and consistent manner across the organization, and

- Coordinate information security with physical security.

Information Security Department Responsibilities

The Information Security Department is responsible and accountable for security administration. At a minimum, they should directly manage or oversee risk assessment, development of policies, standards, and procedures, testing, and security reporting processes. Security officers should have the authority to respond to a security event by ordering emergency actions to protect the organization from an imminent loss of information or value. They should have sufficient knowledge, background, and training, as well as an organizational position, to enable them to perform their assigned tasks.

User Responsibilities

Users should know, understand, and be held accountable for fulfilling their security responsibilities. The means of ensuring users understanding and/or recognition of their responsibilities varies. User security awareness training is one of the most common means available to achieve recognition of responsibility and computing asset worth. Some organizations require personnel to sign an agreement that includes the protection of computing assets as a condition of employment, while others sign agreements as a condition of allowing their connection to the organizations network.

One way to ensure that every current and future user knows that security is part of his job function is to make it part of each job description. Spelling out the security function or expectations within the job description demonstrates the commitment to information security, as well as emphasizes that it is part of the job. After it is made part of the job description, it becomes something that can be considered in performance evaluations.

Conclusion

Information security is the responsibility of everyone in the organization. Management support is crucial for a successful ISMS implementation. Along with its support is a responsibility to the ongoing maintenance of this program. To have a successful ISMS implementation; management, Information Security Department and users must have a good understanding of their roles and responsibilities and be willing to take actions.