A Model Security Management Framework

By Thomas M. Smith, CD, CISSP

November, 2016

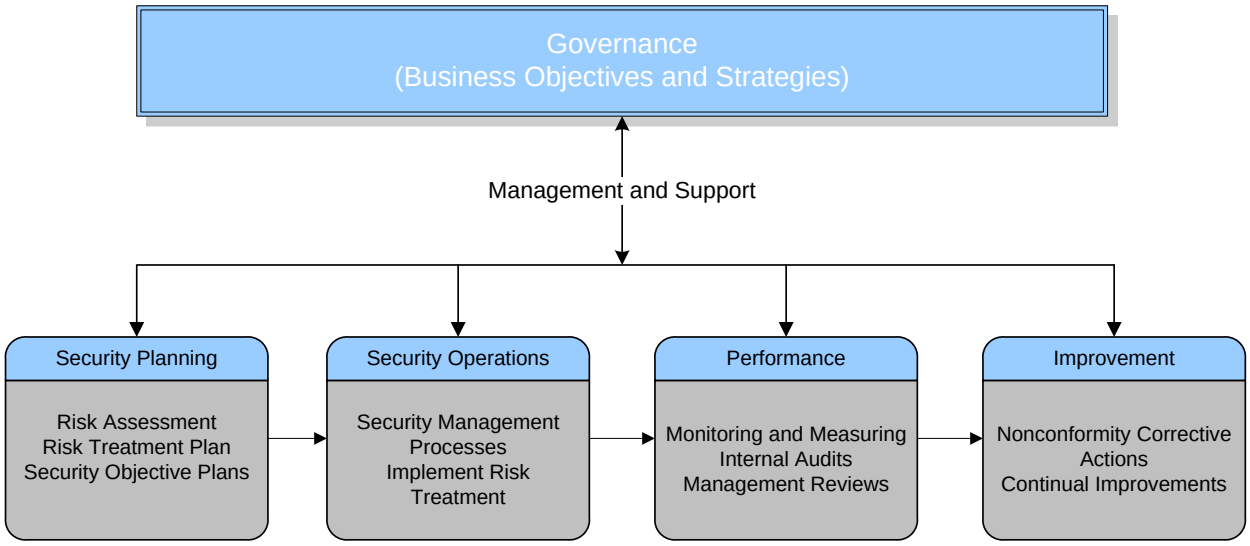
ABSTRACT

Managing information security risks is a challenge and requires an organization's resources and commitment. Responsibility for an organization rests with senior management and its governance activities. In order to ensure a successful investment is realized from security management practices, it must be acknowledged and supported at the highest levels; at governance through a sound information security management FRAMEWORK.

This paper outlines a framework that can be implemented and is ideally suited for those who are implementing the ISO 27001 standard. It provides all of the necessary components that can be developed into an organization specific ISMS implementation.

Model Overview

The following diagram provides an overview of a security management framework:



Security Governance

Governance of information security aligns information security needs and requirements with business objectives and strategies. It delivers value by ensuring that information risk is being adequately managed.

For the purposes of this framework model, governance should ensure that security activities are based on sound risk management by taking into account business, information security, and all other relevant aspects good governance.

The objectives of governance for cyber-security should include:

- *Establishing security and privacy policies*
- *Establishing and aligning security objectives with business objectives and strategy*
- *Delivering value, the organization, customers and other and to stakeholders*
- *Facilitating accountabilities*
- *Establishing compliance with external requirements (legal, regulatory or contractual)*

Security Planning

This aspect of a framework can be comprised of several traditional security management practices and evolve into more modern planning when applying a risk management approach. The following should be the minimum processes that need to be developed:

- *Security awareness requirements*
- *Incident management plan*
- *Vulnerability management process*
- *Change management*
- *Continuity planning*
- *Risk assessment*
- *Risk treatment*

Identifying Security Operations

Operational security can be the implementation of the planned security processes as well as technical security functions provided by firewall, IDS and backup and recovery operations.

- *Apply security management processes*
- *Applying IT operational procedures*
- *Implement risk treatment plans*
- *Conduct ongoing security awareness and training*

Performance Measurements

It is essential that mechanisms be put in place to determine if the planned security objectives are being achieved. It is also necessary to determine the appropriateness of the risk treatment plan in managing the initial security risks.

- *Identifying monitoring and measuring activities or performance indicators*
- *Performing security reviews, including supplier relationships*
- *Conduct internal audits and assessments*
- *Performing Management Review*

Continual Improvements

Good security management should always include mechanisms to facilitate continual improvements. In some situations, initially, planned control implementations may have

undesirable consequences and therefore need adjustments. In or instances the threat environment may change drastically and therefore the initial approach is no longer effective.

- *Identifying actions necessary to address any non-conformities*
- *Developing an action plan to implement any changes arising from the Management review process*
- *Identifying and implementing measures to improve the overall effectiveness of the program*

Summary

The success of an organization's investment in security may well depend on a robust, yet flexible, framework that allows for changing environments, new and existing business needs and adhering to any legal or regulatory requirements. The high-level guidance outlined above can formulate the basics necessary to start a security management program or improve upon existing processes and practices.

Bibliography

ISACA, COBIT 5 A Business Framework for the Governance and Management of Enterprise IT

ISO Information technology — Security techniques —Information Security Management Systems – Requirements, ISO/IEC 27001:2013

ISO Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services, ISO/IEC 27017:2015

NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014.