An Overview of COBIT® 5 for Information Security

By Thomas M. Smith, CD, CISSP

November, 2016

ABSTRACT

Information security is best achieved using a recognized set of industry best practices while applying a risk-based approach to the selection and implementation of the controls. There are several good industry best practices that can be adopted, modified and/or implemented "as is" with some efforts. In all cases, an organization should make every effort to adopt a set of practices and implement the controls provided therein based on its tolerance for risks and adhering to any legal, regulatory or contractual requirements.

This paper highlights the main aspects of the COBIT® *5 For Information Security* and implementation considerations to assist with the selection and application of the requirements set out therein.

Introduction

Organizations should be aware that the COBIT 5® for Information Security, as a best practice, relies upon the implementation of an overall IT management framework provided by COBIT5®. Implementation of the COBIT5® framework would require additional acceptance and detailed planning; however, the security practices themselves are still manageable without the actual framework, COBIT5® conformance notwithstanding.

In addition, factors such as the financial costs should be considered prior to advancing to implementation. The financial costs to implement best practices associated with COBIT 5® for Information Security are likely to be the same as that for other best practices such as the ISO/IEC 2700; however, this does not include addressing the additional costs associated with implementing COBIT 5® for IT management (i.e. the COBIT 5® framework).

In any case the main aspects of the COBIT 5®provide governance and management support. Understanding that governance means: [1]

"Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives."

And management means:[2]

"Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives."

With these in mind, an organization can consider selection and implementation issues such as:

- *Legal and regulatory requirements*
- *Contractual or customer requirements and expectations*
- *Policy requirements*
- *Risks to be mitigated*
- *Maintenance and support capabilities*
- *Financial costs*

Governance and management controls

[1] ISACA® (2012). COBIT 5, *A Business Framework for the Governance and Management of Enterprise IT*, Pg.31.
[2] Ibid.

COBIT 5® provides specific controls for security governance and management. The Governance domain practices of Evaluate, Direct and Monitor (EDM) are comprised of several processes:

- *Governance Framework (EDM01)*
- *Benefits Delivery (EDM02)*
- *Risk Optimization (EDM03)*
- *Resource Optimization (EDMI04*
- *Stakeholder Transparency (EDM05)*

In addition to these governance controls, there are also supporting management controls grouped as:

- *Align, Plan and Organise (APO)*
- *Build, Acquire and Implement (BAI)*
- *Deliver, Service and Support (DSS)*
- *Monitor, Evaluate and Assess (MEA)*

Information Security Controls

The COBIT 5® provides a good selection of controls in key areas and these include:

- *Manage risk*
- *Manage security services*
- *Ensure resource optimization*
- *Manage human resources*
- *Manage strategy*
- *Manage enterprise architecture*
- *Manage relationships*
- *Manage service agreements*
- *Manage programs and projects*
- *Manage requirements definition*
- *Manage solutions identification and build*
- *Manage availability and capacity*
- *Manage changes*
- *Manage change acceptance and transitioning*
- *Manage organizational change enablement*
- *Manage knowledge*
- *Manage assets*
- *Manage configuration*
- *Manage operations*
- *Manage service requests and incidents*
- *Manage problems*
- *Manage continuity*
- *Manage quality*
- *Manage security*
- *Ensure benefits delivery*
- *Manage business process controls*
- *Monitor, evaluate and assess performance and conformance*
- *Monitor, evaluate and assess the system of internal control*
- *Monitor, evaluate and assess compliance with external requirements*

The COBIT 5® For Information Security documentation also provides additional implementation guidance on how these controls can be implemented.

Summary

The COBIT 5® For Information Security provides a comprehensive set of security controls that address many if not all of any organization's security needs. In addition, it provides good governance and management guidance that will serve well for maintaining and improving security management.

Bibliography

Educase, Center for Applied Research, Information Security Governance, Volume 2008, August 19, 2008

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

COBIT® 5 For Information Security, ISACA®

COBIT® 5, Implementation, 2012

Software Engineering Institute, CMMI® for Services, Version 1.3