A Standard Technique for Assessing Security Risks

Using the ISO Risk Management Standard ISO 27005

By Thomas M. Smith, CD, CISSP

May, 2016

ABSTRACT

In todays threat environment, any organization is susceptible to security risks arising from the plethora a of threats, some real and some not so real. In any case, an organization would do well to perform risk assessment with a view to understanding the business impacts to the organization. An organization should also take into account risks associated with privacy, legal and regulatory, as well as contractual obligations.

This paper sets out the basic components of a risk assessment that can be adopted to perform a general high level security risk assessment using the guidance provided in the International Organization for Standardization (ISO) I 27005 Information Security Risk Management Standard.

Introduction

Any business should recognize that there are both risks and rewards in developing business opportunities and delivering services to clients. Certain risks are considered acceptable as long as they are adequately managed. Risk management is a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, acting on and communicating risk issues that may adversely affect business opportunities and services.

Information security means the preservation of confidentiality integrity and availability of information and therefore an information security risk assessment focuses on adverse events that could affect the preservation of these values. In order to dertmine the actual values an assessment is necessary using a systematic approach.

The processes outlined in the ISO 27005 Standard provides such a systematic approach by establishing processes such as:

- *Context of the organization and its tolerance for risks*
- *Asset identification and valuation process*
- *Threat assessment*
- *Vulnerability analysis*
- *Risk analysis*
- *Risk treatment*

By applying the Standard's processes and techniques a good risk assessment can be produced.

Risk Assessment components

Using the ISO Standard as a guide, the following risk assessment components can be undertaking using the noted application guidance:

Establishing the business context	• *Identify the purpose, business, missions, values and strategies of this organization. Identify any constraints affecting the organization such as contractual obligations, legal and regulatory requirements and environmental factors as well as any technical constraints* • *Document the information including a description of the scope for the assessment and the issues constraints noted.* • *Management's tolerance for risk should be identified and*

	quantified where possible along with any existing enterprise level risk processes.
Asset Identification and valuation	• *Make a list of critical business assets that are within the scope, including information, systems. Services, and other assets of importance* • *Provide a valuation of the assets based on their importance and the business impacts arising from a loss of compromise of these assets.*
Threat Assessment	• *Identify threats taking into account of the external environment where the organization is established and operates, internal threats such as deliberate or accident activities by employees, contractors or others* • *Use a rating schema to rate the threat levels and take into account any impacts that may arise*
Vulnerability Analysis	• *Identify all of the existing security controls that are in place* • *Assess the effectiveness of these controls taking into account how well they are implemented, understood and general effectiveness* • *Identify technical, procedural and other vulnerabilities.* • *Produce a list of vulnerabilities* • *Rate the vulnerabilities while taking account of the safeguard effectiveness and the assets that may be exposed or threat exploited* • *Produce a list of rated vulnerabilities*
Risk Analysis	• *Calculate the risk levels using the business impacts, the asset values, threat levels and vulnerabilities ratings* • *Provide a prioritized rated list of security risks*
Risk treatment	• *Develop a risk treatment plan that documents all of the identified risks including the safeguards or controls that already mitigate the risks* • *Identify any additional controls or improvements to existing ones* • *Assign responsivities for implementation as well as timelines* • *Obtain management approval*

The outputs from each of the steps provided above can be assembled into an over risk assessment report that should have management's approval.

Summary

Using the basic concepts outlined above and applying some of the evaluation guidance and metrics provided in the ISO standard will serve well for a good risk assessment.

Bibliography

BSI, Risk Management, Risk Assessment, BSI 31010. 2010

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

ISO, Information Technology Security Techniques — Information Security Risk Management, (BS ISO/IEC 27005:2015),

Software Engineering Institute, CMMI® for Services, Version 1.3