Guide for Conducting Risk Assessments: Information Security

By Yigal Rechtman

Although *Guide for Conducting Risk Assessments: Information Security* is not a book that one can purchase in a store, it reads just like one (Special Publication 800-30, Revision I, National Institute of Standards and Technology [NIST], September 2012, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf). It is well organized and contains a wide range of risk-related concepts that can be helpful to C-suite executives, accountants, auditors, and compliance officers. Risk assessment is found in many aspects of the profession, from managing risk in business and industry; to assessing risk in financial audits and other attestation engagements; to compliance and monitoring requirements, such as those under the Health Information Portability and Accountability Act (HIPAA). According to Thompson.com, "while the [HIPAA] rule does not specifically require compliance with NIST standards, the U.S. Department of Health and Human Services has referenced them frequently in this and other contexts" (David Slaughter, "NIST Issues Updated Risk Assessment Guidance," Thompson, http://prodadmin1.tmg.atex.cniweb.net:8080/preview/www/2.3305/2.3443/1.111564).

Guide for Conducting Risk Assessments: Information Security is a standalone publication that contains only three chapters. Twelve supplementary appendixes provide additional information. The first chapter discusses the guide's purpose, target audience, and organization. The second contains a fundamental discussion of core concepts. The third guides the reader—using advanced language—on how to implement a risk assessment process.

Core Concepts

The aforementioned discussion in the second chapter is very detailed. First, the authors frame the risk management process as a triangle with three points: assessment, response, and monitoring. Although these are not new concepts in risk assessment, the publication provides some useful analysis on the various types of risks. For example, risk is defined as a measurement based on impact and its intersection with the likelihood of an adverse occurrence. The risk assessment approach could be quantitative, qualitative, or semiqualitative.

Threats are classified as being intentional, accidental, structural, natural, or man-made disasters. The discussion of threats—as with other terms that are introduced and analyzed—gives helpful examples. For example, an intentional threat could come in a form of a cyber-attack; a structural threat could be the failure of a hardware or software control.

The second chapter continues with a detailed examination of threat shifting, vulnerabilities, likelihood, impact, risk, aggregation of risks, and uncertainty. The publication describes threat shifting as the response of an adversary to controls that are in place (p. 9). For example, if an intentional threat agent encounters a safeguard, it might select a new target, a new approach, or a new time to attack, thus shifting the initial threat to a different threat. When discussing a weighted risk factor known as the likelihood of occurrence, the publication states that it is based on an adversary's intent, capability, and targeting (p. 10).

The chapter concludes with an analysis of approaches for assessing risk; this builds the foundation to the third chapter, which addresses implementation. Overall, the discussion in the second chapter is rather detailed; although its language is somewhat conceptual, its ideas are broken down into small segments, making it an enjoyable and understandable read.

The Application of Risk Assessment

The third chapter discusses the applications of risk assessment. It begins by classifying risk response and monitoring into three tiers: the organization level (tier 1), the business process level (tier 2), and the information system level (tier 3). The publication then delves into some detail about what is important for each tier. For example, it states that "Tier 1 risk assessment may address ... specific types of threats directed at organizations that may be different from other organizations and how those threats affect policy decisions" (p. 18); however, it suggests that that "more realistic and meaningful risk assessments are based on ... multiple mission/business lines (i.e., derived primarily from Tier 2 activities)" (p. 18).

In addition, this chapter describes the implementation process, starting with the selection of a risk management framework; the identification of threats, the likelihood of occurrence, and the magnitude of impact; and the determination of risk. This implementation process is multidimensional, with regular communication of the results at each step and a detailed analysis at each tier. The chapter's discussion of the implementation process is a rather high-level one; however, it contains constant references to the appendixes, which are hands-on. For example, when the identification of threats is discussed, the publication refers the reader to Appendix D, "Threat Sources," which details threats, such as individuals (e.g., outsider, insider, trusted insider, and privileged insider) or environmental disasters (e.g., floods, earthquakes, or hurricanes).

Additional Material

The 12 appendixes include a wealth of ideas and information well suited for a scoring approach, under which each threat and response receive a score and can be acted upon (threat) or implemented (response) based upon the organization's appetite for risk and available resources. Appendixes include lists of threat sources and events, vulnerabilities, and likelihood and impact. There are also appendixes for glossary, references, and acronyms. The appendixes conclude with an outline of a risk report and a breakdown of tasks to create a full risk-assessment process.

A Benefit for CPAs

Although this guide is not a book, this governmental publication is well worth reading. It reads succinctly, is broken down into manageable pieces, and is actionable. In addition, for all its value and benefit, it is free to download. Auditors, managers in business and industry, and compliance officers can all benefit from the publication. ❑

Yigal Rechtman, CPA, CFE, CITP, CISM, *practices in Brooklyn, N.Y.*