Challenges in the Instruction of Risk Management

TREO Talk Paper

Michael E. Whitman, Ph.D., CISM, CISSP
Kennesaw State University
mwhitman@kennesaw.edu

Abstract

This paper provides an overview of the challenges associated with delivering instruction on the assessment and treatment or risk in the organization. Challenges addressed include selecting a risk management methodology and choosing an application to provide students with essential skills needed for success in industry. Details on methodologies and applications will be provided during the talk.

The cornerstone of any information security or cybersecurity program is the instruction of risk management (RM) theory and providing students with useful skills in demand by employers. Risk management is the formal program of identifying, assessing and treating risk to information assets in the organization. It is through the process of RM that the organization determines whether additional controls or safeguards are needed. In the instruction of RM, selecting the optimal approach is as much a matter of personal preference as professional experience.

There are several widely used methodologies providing structure suitable to RM instruction. While each approach varies, most include identifying and assessing the value of information assets, assessing current levels of risk, comparing levels of risk to the organization’s risk appetite, and selecting among strategies to accept, avoid, mitigate, or transfer risk until the residual risk falls with the organization’s specifications. Suitable RM methodologies for instruction include:

- NIST Risk Management Framework (RMF) – NIST provides no-cost publications to guide public and private sector organizations in the use of their RM framework, most notably SP 800-37, Rev. 1.
- ISACA COBIT 5 for Risk – developed for and promoted by the professional security organization responsible for the CISM and CISA certifications, and part of the Control Objectives for IT (COBIT).
- OCTAVE series – available through Carnegie Melon University’s Software Engineering Institute, the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology, defines three RM methodologies including OCTAVE-Allegro focused on risk assessment.
- Microsoft’s MOF Risk Management Discipline – the RM approach employed and promoted by Microsoft as the Microsoft Operations Framework (MOF) geared toward operations management.
- Information Risk Assessment Methodology 2 (IRAM2) – promoted by, and available to members of, the British Information Security Forum, this methodology has limited information available.

Once a suitable RM methodology is selected, comes selecting an application to support instruction and learning. Many of the aforementioned methodologies can be implemented in a pen-and-paper exercise based on fictional case organization. Of particular note is the availability of commercial applications at no charge to instructors in public universities and colleges – such as Clearwater Compliance’s Information Risk Management. Such applications provide increased depth of instruction and skills valued by employers.

References

Links to the aforementioned RM methodologies and applications will be provided in the TREO talk.