

## **4. Information Security Risk Management**

### **4.1 Prerequisite Knowledge**

Participants in this course should have a basic knowledge of information security management principles. There are no other prerequisites.

### **4.2 Course Objectives**

You will learn:

- Information security risk management concepts and terminology
- How to plan and organize an information security risk management program in your organization
- How to determine your organization's risk posture
- How to identify your organization's risks and build mitigation plans to address those risks
- How to use the Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) methodology
- How to implement a phased approach to addressing your organization's information security risk

### **4.3 Course Description**

This course addresses one of the key aspects of information security: risk management. Many organizations focus solely on infrastructure weaknesses and fail to establish the effect on their most important information assets. This leads to a gap between an organization's operational and information technology requirements, placing the assets at risk. Current approaches to information security risk management tend to be incomplete. The first step in managing information security risk is to understand what your risks are. Once an organization has identified its risks, it can build mitigation plans to address those risks. The Operationally Critical Threat, Asset, and Vulnerability Evaluation<sup>SM</sup> (OCTAVE<sup>SM</sup>) enables organizations to do this. The Information Security Risk Management course endeavors to give students the tools they need to implement an effective information security risk management program in their organizations. Students are taught a phased approach to information security risk management based on the OCTAVE criteria. Students will learn to build asset-based threat profiles, identify infrastructure vulnerabilities and develop security strategies and plans. At the end of this course students will have the tools necessary to conduct a risk assessment of their organization and implement mitigation strategies.

### **4.4 Course organization**

The course consists of four modules of four hours each that are taught over a two day period.

### **4.5 Course Topics**

1. Managing Information Security Risks
  - 1.1. What is information security?
  - 1.2. Information security risk evaluation
  - 1.3. An approach to information security risk evaluations

2. Principles and Attributes of Information Security Risk Evaluations
  - 2.1. Information security risk management principles
  - 2.2. Information security risk evaluation attributes
  - 2.3. Information security risk evaluation outputs
3. The OCTAVE Method
  - 3.1. Overview of the OCTAVE method
  - 3.2. Mapping attributes and outputs to the OCTAVE method
4. Preparing for OCTAVE
  - 4.1. Overview of preparation
  - 4.2. Obtain senior management sponsorship of OCTAVE
  - 4.3. Select analysis team members
  - 4.4. Select operational areas to participate in OCTAVE
  - 4.5. Select participants
  - 4.6. Coordinate logistics
5. Identifying Organizational Knowledge
  - 5.1. Overview of processes 1-3
  - 5.2. Identify assets and relative priorities
  - 5.3. Identify areas of concern
  - 5.4. Identify security requirements for most important assets
  - 5.5. Capture knowledge of current security practices and organizational vulnerabilities
6. Creating Threat Profiles
  - 6.1. Overview of process 4
  - 6.2. Before the workshop: consolidate information from processes 1 to 3
  - 6.3. Select critical assets
  - 6.4. Refine security requirements for critical assets
  - 6.5. Identify threats to critical assets
7. Identifying Key Components
  - 7.1. Overview of process 5
  - 7.2. Identify key classes of components
  - 7.3. Identify infrastructure components to examine
8. Evaluation Selected Components
  - 8.1. Overview of process 6
  - 8.2. Before the workshop: run vulnerability evaluation tools on selected infrastructure components
  - 8.3. Review technology vulnerabilities and summarize results
9. Conducting the Risk Analysis
  - 9.1. Overview of process 7
  - 9.2. Identify the impact of threats to critical assets

- 9.3. Create risk evaluation criteria
- 9.4. Evaluate the impact of threats to critical assets
- 9.5. Incorporating probability into the risk analysis
- 10. Developing a Protection Strategy – Workshop A
  - 10.1. Overview of process 8A
  - 10.2. Before the workshop: consolidate information from processes 1 to 3
  - 10.3. Review risk information
  - 10.4. Create protection strategy
  - 10.5. Create risk mitigation plans
  - 10.6. Create action list
  - 10.7. Incorporating probability into risk mitigation
- 11. Developing a Protection Strategy – Workshop B
  - 11.1. Overview of process 8B
  - 11.2. Before the workshop: prepare to meet with senior management
  - 11.3. Present risk information
  - 11.4. Review and refine protection strategy
  - 11.5. Create next steps
- 12. Variations on the OCTAVE Approach
  - 12.1. Introduction to tailoring OCTAVE
  - 12.2. The range of possibilities
  - 12.3. Tailoring the OCTAVE method
- 13. Practical Applications
  - 13.1. The small organization
  - 13.2. Very large, dispersed organizations
  - 13.3. Integrated web portal service providers
  - 13.4. Large and small organizations
  - 13.5. Other considerations
- 14. Information Security Risk Management
  - 14.1. A framework for managing information
  - 14.2. Implementing information security risk management
  - 14.3. Summary