

Federal Reserve Board of Governors

**Course Description for
Information Systems Vulnerability
Management (ISVM)—Hands-On
(S&R Technology Lab)**

Last Revised: September 2009

Information Systems Vulnerability Management (ISVM) Hands-On (S&R Technology Lab)

The Board of Governors of the Federal Reserve System is proud to offer technology-related courses developed and hosted by the S.T.R.E.A.M./Technology Lab at the Federal Reserve Bank of Chicago, Chicago, Illinois. For over nine years, the S.T.R.E.A.M./Technology Lab has pursued a unique approach to examiner technology training by combining lectures with hands-on exercises. The exercises reinforce concepts by allowing participants to input commands into software applications and observe how they work. The Technology Lab is outfitted with many applications and operating systems found in the financial industry.

Type of Participant Targeted

The Information Systems Vulnerability Management (ISVM) course is a 4-day course intended for examiners with IT examination responsibilities but who may not have had university training in information technology. At least one year of field examination experience is preferred.

Prerequisites

None required.

Course Overview

This course provides participants with a technical grounding in networking concepts and technologies that are critical to IT operations in financial institutions, including TCP/IP networking protocols and common network infrastructures and configurations. The course examines key network perimeter security tools, including firewalls and intrusion detection systems (IDS).

Course Objectives

After completing the course, the participant, at a minimum, will be able to demonstrate the following skills:

- Recognize where and how vulnerability management fits in with the bank's overall information security program and IT operations
- Identify the role a vulnerability management program has in safeguarding information and assets
- Assess the adequacy of a patch management, vulnerability scanning and assessment, and penetration testing tools and their limitations
- Evaluate the adequacy of an organization's testing program
- Recognize key elements of an incident response program
- Discuss key technology terms related to information systems vulnerability management
- Assess the key risks, controls and processes in a supervisory context, including regulatory compliance issues
- Identify what the financial institution must do to respond to new threats

Post-Course Intervention

Participants will learn the essential components that comprise a sound vulnerability management program. The bank must position vulnerability management as an integral part of the enterprise-wide information security program, network engineering and IT operations. Other key elements include: asset inventory; risk assessment; monitoring for vulnerabilities; patch management; vulnerability testing; security intelligence; incident response; forensics; and, the relationship of vulnerability management to regulatory compliance.

Overview of ISVM Curriculum

| Subject | Approximate Class Hours |
|--|-------------------------|
| General Information Security concepts | 1.0 |
| SQL Injection—Case Study | 3.0 |
| Risk Mitigation | 3.0 |
| Network mapping and vulnerability scanning—Exercise | 1.0 |
| Sources of Security Intelligence (review of CVE and Bugtraq) | 0.5 |
| Assessing the Patch Status of the Bank—Case Study | 1.0 |
| Patch Management Operations—Demonstration | 1.0 |
| Testing—Validating the Effectiveness of Patch Management | 1.0 |
| Inventory and Asset Identification—Demonstration | 0.5 |
| Update on the Latest Threat Vectors (e.g. Conficker) | 0.5 |
| Penetration Testing & Vulnerability Assessment—Case Study | 1.5 |
| Penetration Testing & Vulnerability Assessment—Demonstration | 0.5 |
| Monitoring of Network Traffic and Password Capture—Exercise | 1.0 |
| Other Monitoring and Enumeration Tools—Exercise | 1.0 |
| Incident Response | 1.0 |
| When Banks Must Notify Customers—Case Study | 1.0 |
| Incident Response Resources and Regulatory Guidance | 2.0 |
| Security Information and Event Management—Demonstration | 2.0 |
| Supervisory Concerns | 1.5 |
| Responding to New Threats—Capstone Exercise | 1.0 |
| Total Lecture & Exercise Hours | 25.00 (*) |

(*) Note: The total number of hours and topics may vary from class to class.

Learning Objectives

Examiners should be able to articulate the key elements associated with operating and managing a vulnerability management program. This starts with having an accurate inventory of all assets (servers and applications) that communicate over the network. Accuracy in this case means that consideration should be given to potential risks for each system (internal and external) and that all systems should be inventoried. It includes having an accurate risk assessment and relies on configuration management. Configuration management is critical as this requires operational discipline regardless of institution size. Finally, the financial institution must be able to articulate a risk mitigation strategy; this should be reviewed to ensure that new applications and/or systems are treated from a holistic perspective, and that controls for all systems are re-evaluated for effectiveness periodically.

By module, the following learning objectives will be accomplished:

| Module | Learning Objectives |
|---|--|
| General Information Security Concepts | <ul style="list-style-type: none"> • Foster a baseline understanding of key terms related to vulnerability management |
| SQL Injection—Case Study | <ul style="list-style-type: none"> • Identify the technical elements required for an attacker to exploit a web server • Examine the controls that must be in place to mitigate SQL injection attacks • Review the Bank’s response and identify changes that would have facilitated a quicker recovery |
| Risk Mitigation | <ul style="list-style-type: none"> • Identify why vulnerabilities are a concern to the financial institution regardless of size and complexity • Discuss vulnerability monitoring and patching • Identify the role of vulnerability assessments in the risk management process • Describe security intelligence • Evaluate vulnerability management tools |
| Patch Management | <ul style="list-style-type: none"> • Define patch management terminology • Discuss the criticality of applying patches in a timely manner • Enumerate the risks of ineffective patch management • Evaluate patch management deployment tools • Describe the patch process and demonstrate using a commercial tool |
| Penetration Testing and Vulnerability Assessment (Case Study and Demonstration) | <ul style="list-style-type: none"> • Illustrate the relationship between configuration management, change management and release management • Identify how poor configuration management practices can lead to vulnerabilities • Demonstrate how vulnerability assessment differs from penetration testing and what are the success criteria for each |
| Incident Response | <ul style="list-style-type: none"> • Define the goals and definitions of Incident Response (IR) • Describe the IR Life-Cycle, IR Planning and the IR teams and stakeholders • Evaluate customer notification requirements and other regulatory guidance |

Class Size

The optimal class size for the Information Systems Vulnerability Management course offering is approximately 25 participants. To provide sufficient variety of interaction among class participants, the minimum class size should be 10 participants.

Instructors

Information Systems Vulnerability Management courses include one or more instructor(s) from the Federal Reserve System and may also includes instructors from an external agency.