

Security Assessments

Class 5

1

Security Assessments

- Focus on technical configuration and operational practices
- Compare existing security practices to a standard and note inadequacies
- Performed with knowledge of those being evaluated (usually)
- Does not attempt to obtain illicit access to systems
- Not restricted to flaws visible via network access

Class 5

2

Security Assessment Process Overview

- Define scope
 - Which systems?
 - Which networks?
 - Which applications?
- Define standards against which to perform the assessment
- Define methods and tools to perform assessment
- Fact finding – Collect information about security configuration
- Analysis – Determine security vulnerabilities, potential consequences, and likely countermeasures
- Delivery – Provide report to management, with recommendations for action

Class 5

3

Standard assessment methodologies

- NIST
 - Federal Government
- NSA IAM
 - Federal government
- Payment Card Industry (PCI)
 - E-commerce involving credit cards
- OSSTMM
 - Generic open-source

Class 5

4

NIST

- National Institute of Standards and Technology
- Responsible for security of non-classified Federal government information systems
- Publishes standards, guidelines, and procedures supporting this goal
- Specifically supports FISMA compliance, along with other relevant regulatory compliance

Class 5

5

Federal Information Security Management Act (FISMA)

- Formalized with the E-Government Act (Public Law 107-347)
- FISMA requires periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls at least annually
- NIST standards play a specific role here
- NIST's role in security assessment has existed long before FISMA and still extends beyond it

Class 5

6

Federal Information Security Management Act (FISMA)

- Establishes an information security framework of which assessment is a part:
 - Categorization
 - Security control selection
 - Risk assessment
 - Security planning
 - Control Implementation
 - Control assessment
 - System authorization
 - Security monitoring
- Each step is governed by applicable NIST publications.

Class 5

7

NIST

- The following documents are used for the security assessment step:
 - SP 800-53a - Guide for Assessing the Security Controls in Federal Information Systems. (Specifically required for FISMA assessments)
 - SP 800-37 - Guide for the Security Certification and Accreditation of Federal Information Systems .
 - SP 800-26 - Security Self-Assessment Guide for Information Technology Systems

Class 5

8

NIST SP 800-53a

- Framework:
 - Input, identifier of security control
 - Processing, assessment methods and objects associated with the control
 - Output, assessment procedure
- Assessment methods are generally:
 - Interview
 - Examine
 - Test

Class 5

9

NIST SP 800-53a

- *Assessment procedure catalog*, a catalog of tasks that may be incorporated into an assessment (takes up most of the document)
- Provides the link between the security control and the assessment of that control

Class 5

10

NSA IAM/IEM

- Another Federal information security assessment methodology
- Suited to both civilian and classified systems
- Three levels of assessment:
 - Level I – Assessment (IAM)
 - Level II – Evaluation (IEM)
 - Level III – “Red Team”
- Level II/III will not be covered here

Class 5

11

NSA IAM/IEM

- Specific methodology is NOT public domain
- Information Assurance Methodology (IAM) is a pure policies/procedures assessment
- Information Evaluation Methodology involves detailed technical security assessment
- Third party training required to become IAM or IEM certified
 - Offered by Security Horizons
- See <http://www.iatrp.com> for more information

Class 5

12

NSA Information Assurance Methodology (IAM)

- Pre-assessment visit
- Determine information criticality (Organization Information Criticality Matrix)
- Determine system criticality (System Criticality Matrix)
- Document existing system security environment
- Determine strengths and weaknesses in current environment
- Produce final report and de-brief client

Class 5

13

NSA IAM

- Pre-assessment visit
 - Define organization environment
 - Understand organization's mission
 - Introduce assessment process to client

Class 5

14

NSA IAM

- Determine information criticality
 - What information is critical?
 - How does the information affect the organization's mission?
 - Summarize as an Organization Information Criticality Matrix (OICM)

Class 5

15

NSA IAM

- Determine system criticality
 - What is the system's impact on identified critical information?
 - Identify boundaries
 - Identify constraints on system operation
 - Summarize as a System Criticality Matrix (SCM)

Class 5

16

NSA IAM

- Document findings
 - Information and systems environment
 - Existing security environment
 - Potential areas of improvement

Class 5

17

NSA IAM - OICM

Note: SCM is similar, with rows representing systems

	Confidentiality	Integrity	Availability
Information type 1	High	High	Medium
Information type 2	Low	Medium	Medium
Information type 3
Information type 4

Class 5

18

NSA InfoSec Evaluation Method - IEM

- A more technical, detailed security assessment
- Includes the following technical assessments
 - Port scanning
 - Service enumeration
 - Host evaluation
 - Application specific scanning
 - More...

Class 5

19

Payment Card Industry (PCI)

- Imposed by credit card processors, not by the government
- Compliance imposed on businesses that desire merchant card accounts
- Designed to enhance payment card security
- For more information:
<https://www.pcisecuritystandards.org/>

Class 5

20

PCI Reviews

- Performing PCI reviews requires specific training and certification:
 - Qualified Security Assessors (QSAs)
 - Approved Scanning Vendors (ASVs);
- Depth of review depends of nature of reviewed organization:
 - Self assessment for smaller organization
 - Scanning and audits for larger organizations

Class 5

21

PCI Core Principles

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

Class 5

22

PCI twelve compliance requirements

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

Class 5

23

PCI Applicability

- Covers any technical component involved in credit card processing
- For merchants, processing volume affects assessment requirements:
 - Level 1 - More than six million transactions annually across all channels, including e-commerce *Annual Onsite PCI Data Security Assessment and Quarterly Network Scans*
 - Level 2 - 1,000,000 - 5,999,999 transactions annually *Annual Self-Assessment and Quarterly Network Scans*
 - Level 3 - 20,000 - 1,000,000 e-commerce transactions annually *Annual Self-Assessment and Quarterly Network Scans*
 - Level 4 - Less than 20,000 e-commerce transactions annually, and all merchants across channel up to 1,000,000 VISA transactions annually *Annual Self-Assessment and Annual Network Scans*
- Service providers have similar tiered assessment levels

Class 5

24

PCI Sanctions

- Fines can be levied for failure to comply
- In extreme cases, retailer may lose their merchant account and the ability to accept credit cards
- Sanctions are non-governmental
- Sanctions are almost never publicized

Class 5

25

Open Source Security Test Methodology Manual (OSSTMM)

- Intended to be an open-source community defined security testing methodology
- Sets criteria for conducting security tests
- Goal is an objective methodology for security assessment
- More widely used in Europe than in the USA
- Version 3.0 substantially revised from prior versions

Class 5

26

Open Source Security Test Methodology Manual (OSSTMM)

- Rules of Engagement
 - Detailed description of ethical and contractual requirements for security testing
- Security Testing Methodology:
 - How do current operations work?
 - How do they differ from how management thinks they work?
 - How should they work?

Class 5

27

Open Source Security Test Methodology Manual (OSSTMM)

- Security Testing Methodology detail:
 - Regulatory phase
 - Understand scope, requirements, and constraints of review
 - Definitions phase
 - Nature of targets and their relationships
 - Information phase
 - Define information, its worth, use and controls
 - Interactive controls phase
 - Penetration and “disruption”

Class 5

28

Open Source Security Test Methodology Manual (OSSTMM)

- This phase-wise breakdown is applied for defined security “channels”
 - Human security
 - Physical security
 - Wireless
 - Data Networks
 - Telecommunications