

Federal Reserve Board of Governors

**Course Description for
Operating Systems Hands-On
(S&R Technology Lab)**

Last Revised: November 2009

Operating Systems 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 hands-on exercises with lectures. Learning materials are based on applicable FFIEC Examination Handbooks and other examiner guides. The hands-on exercises reinforce concepts by allowing participants to interact with various vendor software applications, operating systems, and security appliances widely used in the financial industry and observing how they work. Each participant has a PC at their disposal in the state-of-the-art facility which supports teleconferencing, audio/video recordings, and interactive participant response systems.

Type of Participant Targeted

The Operating Systems 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.

Course Overview

This course focuses on the security capabilities and limitations of computer operating systems (OS). OS under the review include network OS, virtual machines, the Microsoft OS family (including Windows 2003 & 2008 servers, Vista and Windows 7), the UNIX/Linux operating system family, and IBM's AS/OS/400. Hands-on exercises use virtualized or native environments. Class activities include reviewing security parameters and permissions on various platforms.

Course Objectives

Upon completion of this course, the participant, at a minimum, will be able to demonstrate the following skills:

- Describe the typical uses of different operating systems in the enterprise and how they interact with other components of an organization's core IT infrastructure
- Perform fundamental system administration and audit operations
- Reference U.S. supervisory agency examination work programs
- Perform user administration, access control, auditing, and reporting on various operating systems

Post-Course Intervention

Participants should be provided with opportunities that allow them to identify security capabilities and limitations associated with computer operating systems within a financial institution. They should review security measurements and recommend proper security controls to protect various OS assets.

Overview of Operating Systems Curriculum

Subject	Class Hours
OS history and legacy OS	3.5
Network operating systems	3.0
Virtualization	4.5
Vista & Windows 7	3.0
Windows security and controls	5.5
Windows server (Win2003/2008)	3.0
Unix/Linux OS	3.5
IBM/OS 400	2.0
Summary	1.0
Total Lecture & Exercise Hours	29.00

Note: The length of each module may vary from class to class due to class discussion.
*28 Continuing Professional Education (CPE) Credits may be earned.

Learning Objectives

Participants build up a solid understanding of various operating systems functions, features, and their associated security risks through lectures and hands-on exercises. Furthermore participants evaluate the OS and its security measurement by reviewing, auditing, reporting and recommending proper security controls.

By module, the participant, at a minimum, will able to do the following:

Module	Learning Objectives
DOS, OS/2 and Thin Client	<ul style="list-style-type: none">• Identify the basics of operating systems• Enumerate the role operating systems play in information technology• Test the functionalities and characteristics of different operating systems
Unix/Linux	<ul style="list-style-type: none">• Explain features of Unix and Linux• Identify security strengths and weaknesses• Audit Unix and Linux
Windows Security and Controls	<ul style="list-style-type: none">• Explain Windows security concepts• Examine Windows elements, including Windows administrative tools, file systems, process management, registry management, performance monitoring, Microsoft Management Console, active directory, user management, group and share, group policy and account policy, audit and various Window services• Examine Windows security controls, such as device hardening, security template and encryption of file system
Virtual Machine	<ul style="list-style-type: none">• Gain basic understanding of virtual machine solutions• Explain features in virtualization player• Review virtualization vendors
Vista and Windows 7	<ul style="list-style-type: none">• Describe new options and features in Vista and Windows 7• Explain new security applications• Consider migration impacts
Windows Servers	<ul style="list-style-type: none">• Review features in the latest Microsoft server 2008• Identify new security controls and improvement in user interface
IBM OS 400	<ul style="list-style-type: none">• Inspect IBM OS and servers• Explain the management functions, such as log on, screen and operation navigation and print• Examine system security values, password, user profiles and group membership
Network Operating Systems	<ul style="list-style-type: none">• Explain features of network router, switch and firewall• List usages of network devices• Perform user creation, OS administration, maintenance and audit

Class Size

The optimal class size for the Operating Systems course offerings is approximately 20 participants. To provide sufficient variety of interaction among class participants, the minimum class size should be 10 participants.

Instructors

Operating Systems courses include one or more instructor(s) from the Federal Reserve System and may also include additional instructors from an external agency or consultant firm.