

**Federal Reserve Board of Governors**

**Course Description for  
IT Supervisory Themes and  
Emerging Topics  
(S&R Technology Lab)**

**Last Revised: June 2009**

---

## IT Supervisory Themes and Emerging Topics (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 IT Supervisory Themes and Emerging Topics (STET) course is a 4 day class. The class is suitable both for newer examiners looking for some introduction to various IT topics, and experienced examiners who have encountered these issues and could benefit from further collaboration with other examiners.

### Prerequisites

None.

### Course Overview

This course is designed to highlight emerging topics in information technology in a condensed and discussion –oriented format. Topics include: Virtualization and risks, wireless 802.11n, Voice over IP, IT Governance, Remote Deposit Capture, vendor management / Outsourcing, BCP/Pandemic Preparedness, and capacity management. The class modules are dynamically developed based on evolving IT operational risks and new found IT exam issues. Therefore each class may have different focused areas based on latest IT trends. This course offers 28 continuing professional educational credits (CPE) through NASBA.

## Course Objectives

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

- Demonstrate basic understanding of learned IT technology
- Identify strengths and weaknesses of various technologies
- Perform fundamental system administration and audit operations
- Evaluate and report efficiency of various security controls to protect technology operations

## 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 technology operations.

## Overview of IT Supervision Themes and Emerging Topics Curriculum

Subject	Approximate Class Hours
Vendor management / Outsourcing	3.0
Strong authentication	1.0
IT regulation/ red flags	1.0
Top IT supervisory themes	1.0
IT governance frameworks	2.0
Remote deposit capture	2.0
Portable device risk	1.0
Virtualization and virtualization risk	5.0
Capacity management	2.0
Wireless 802.11n	3.0
Voice over IP	3.0
BCP/Pandemic Plan	2.0- 4.0
Web application security	2.0
<b>Total Lecture &amp; Exercise Hours</b>	<b>28.00 *</b>

*\* Note: The topics may vary from class to class.*

## Learning Objectives

Participants develop a solid understanding of various technologies and identify security strengths and weaknesses in the technology implementations. Furthermore participants evaluate the technology and its security measurement by reviewing, auditing, reporting and recommending proper security controls.

**By module, the following learning objectives will be accomplished:**

Module	Learning Objectives
Vendor management / Outsourcing	<ul style="list-style-type: none"> <li>Identify most regularly outsourced IT services</li> <li>Review and discuss key components of an outsourcing contract</li> <li>Examine top 10 outsourcing questions</li> </ul>
Strong authentication	<ul style="list-style-type: none"> <li>Understand the reason for strong authentication</li> <li>Explain SR05-19 and SR06-13 requirements on strong authentication</li> <li>Review challenges that regulators and banks face for the compliance exam</li> </ul>
IT regulation/ red flags	<ul style="list-style-type: none"> <li>Define Red Flag, FACT act and top 7 red flag requirements</li> <li>Clarify responsibilities of red flag requirements</li> </ul>
Top IT supervisory themes	<ul style="list-style-type: none"> <li>Survey IT supervisory themes workgroup and list top IT supervisory themes and emerging topics during 2009</li> </ul>
IT governance frameworks	<ul style="list-style-type: none"> <li>Explicate why the IT governance is necessary for a financial institution</li> <li>Discuss major frameworks on IT governance, such as ITIL, COBIT, ITSM, ISO standards</li> </ul>
Remote deposit capture	<ul style="list-style-type: none"> <li>Illustrate Remote deposit capture landscape</li> <li>Identify related risks and controls to manage the risks</li> <li>Evaluate relevant red flags requirements</li> </ul>
Portable device risk	<ul style="list-style-type: none"> <li>Assess various information risks</li> <li>Identify risk controls to protect sensitive information</li> </ul>
Virtualization and virtualization risk	<ul style="list-style-type: none"> <li>Explain virtualization and its trends</li> <li>Specify virtualization risks and risk controls</li> </ul>
Capacity management	<ul style="list-style-type: none"> <li>List capacity management best practices</li> <li>Explain capacity survey and capacity management</li> </ul>
Wireless 802.11n	<ul style="list-style-type: none"> <li>Review and Discuss 802.11n WLAN standard</li> <li>Identify WLAN risks and controls</li> </ul>
Voice over IP( VoIP)	<ul style="list-style-type: none"> <li>Detail voice over IP system components</li> <li>Discover various risk areas in a VoIP system</li> <li>Recommend VoIP reviews and exams</li> </ul>
BCP/Pandemic Plan	<ul style="list-style-type: none"> <li>Show structure of FFIEC BCP booklet</li> <li>Lesson learned from pandemic events</li> <li>Use examiner guide for supervision of BCP</li> </ul>
Web application security	<ul style="list-style-type: none"> <li>Display web application is on top IT vulnerability list</li> <li>Describe how a cross site attack can occur without end user's notice</li> </ul>

## **Class Size**

The optimal class size for the IT Supervisory Themes and Emerging Topics course offerings is approximately 20 participants. To provide sufficient variety of interaction among class participants, the minimum class size should be 10 participants.

## **Instructors**

The IT Supervisory Themes and Emerging Topics course is conducted and supported by a group of professionals, including senior IT examiners, information security specialists, technology architects and program managers from the Federal Reserve System, FFIEC agencies, state banking supervision department and consultant firms. This course may require 4 or more instructors.