

## Type of Participant Targeted

The STREAM™ “Examiner IT Bootcamp Hands-On” course is a foundational course designed for safety and soundness examiners but is applicable to others with IT exam responsibilities, and who have interests or a basic understanding of IT concepts, supervision, and risks for financial institutions.

## Prerequisites

None.

## Course Overview

The goal of this week long seminar is to provide training in IT supervision of financial institutions. It leverages content across our curriculum and adds foundational IT risk and examination material that position attendees to be able to participate in low risk IT exams.

## Course Objectives

The course presents and builds on foundational concepts including IT audit, risk frameworks, networks and operating systems, and covers applied topics of risks including system management, controls, data management, and emerging technologies. At the conclusion, participants should be able to

- Recognize and understand concepts of bank technology and architecture
- Identify business and supervision risks related to a financial institution’s IT environment
- Assess the impact of identified risks on the institution’s operations
- Discuss examination results and concerns with the financial institution’s management
- Analyze and assess the impact of the risks and exposures of existing and emerging technologies including, but not limited to: virtualization; network, security and log management solutions; “Bring Your Own Device (BYOD)”;
- cloud computing; vendor management; data loss prevention (DLP); mobile devices, payments and risks; and, social media risks.
- Make relevant control recommendations to the financial institution’s management

## Post-Course Intervention

After completing the course, the participant should be given on-the-job IT assignments that will increase the retention of the competencies presented during class. Such on-the-job assignments include:

- Completing the evaluation and identifying key risks of a non-complex financial institution’s IT environment with the assistance of a more senior IT examiner
- Preparing, or assisting in the preparation of, examination findings concerning a financial institution’s technology risks
- Conducting or participating in a discussion with bank management regarding IT examination findings and concerns

# Examiner IT Bootcamp Hands-On

## Curriculum Overview

Subject	Approx. Class Hours	Learning Objectives
Course Overview Risk Management Framework Risk Assessment	1.25	-Fundamental concepts of risk management -How to conduct & evaluate a risk assessment -Difference between risk assessment & management
IT Governance IT Audit and Exam	1.25	-Methodology, structure & approach for IT Governance -Framework for IT audits & exams
Network Concepts, Security, and Design	1.50	-Open Systems Interconnection (“OSI”) and Internet Models -Specific risks related to networks
Network Diagrams, Firewalls, and other Controls	1.25	-Elements of layered security & network devices to separate zones of risk -Firewall controls, monitoring & management
Operating Systems: Introduction, Servers, Clients and Directories	1.75	-Overview of security similarities & differences across multiple OS platforms -OS security parameters relative to Enterprise-wide Active Directory implementation -Use of Group Policy to enforce Access Controls
Virtualization	2.25	-Concepts of virtualized systems
Bring Your Own Device (“BYOD”)	0.50	-Impact of BYOD on traditional infrastructures
Security Threat Vectors Vulnerability Management Pen Testing	1.25	-Most common threat vectors impacting banks -Elements & role of a vulnerability management & penetration testing program
Security: Patch Management	1.50	-Patch management terminology, process & tools
Security Topics: Core Data Processing Change Management, Data Integrity Data Loss Prevention (“DLP”)	1.50	-Identification & classification of an organization’s information & data stream -Preventing the loss of sensitive information in a security breach -Different phases of change management & assessment of key controls
Security Information and Event Management (“SIEM”)	1.25	-Using all IT information sources to facilitate successful security monitoring -Link between log/information monitoring & incident response planning
Cloud Computing and Vendor Management	1.25	-Technical controls for managing cloud computing risks -Assessing the vendor risk matrix & cloud vendor’s security & compliance capabilities
Business Continuity Planning and Disaster Recovery	1.50	-Best practices for disaster recovery planning, testing & implementation
Mobile Topics Overview, Mobile Banking/Payments, Authentication	2.75	-Mobile payment risks & mechanisms for limiting this risk
Social Media and Risks	1.25	-Exposures & risks involved with social media applications & strategies for mitigating those risks
TOTAL	24.75	