Federal Reserve System Training Program

2015 Course Catalogue

This booklet includes descriptions of Federal Reserve System examiner training programs as well as FFIEC courses and conferences.

For international distribution

The International Training and Assistance (ITA) website, which includes a link to this complete catalogue as well as our online application system, can be accessed at

www.federalreserve.gov/bankinforeg/ita/about_ita.htm

January 2015

Dear Colleagues:

I am pleased to provide you with this catalogue of supervisory and regulatory training programs the Federal Reserve System will offer in 2015. These programs, designed for and offered exclusively to supervisory staff and officials from central banks and regulatory authorities from around the globe, provide a forum for participants to exchange views and draw lessons learned from practical experience.

Given the complexities of today's financial environment, the Federal Reserve System remains steadfast in its commitment to train bank supervisors in the fundamental elements of bank examination and supervision techniques. All of our training programs are instructed by seasoned subject-matter experts within the Federal Reserve System, who share their practical experience and knowledge on the most pressing supervisory issues by incorporating case studies, exercises, and group work. The use of highly experienced instructors and practical training approaches have been the hallmarks of our international training program since its inception over twenty years ago.

The intention of most countries to adopt best practices prompted the Federal Reserve System to become a global supervisory training provider. To the more than 160 countries that have participated in our international training programs over the last two decades, thank you for being wonderful partners in our exciting investment in human capital.

Sincerely,

Sarkis D. Yoghourtdjian
Assistant Director

Table of Contents

Introduction 1

General Information 7

Schedules 17
- Schedule — Federal Reserve System 19
- Schedule — S.T.R.E.A.M./Technology Lab Federal Reserve Bank of Chicago 21
- Schedule — Federal Financial Institutions Examination Council (FFIEC) 23

Federal Reserve System Course Descriptions 25
- Advanced Credit Risk Measurement and Management Seminar 27
- Anti-Money Laundering Examination Seminar 28
- Bank Analysis and Examination School 29
- Capital Planning and Stress Testing Seminar 30
- Consolidated Supervision and Risk Integration Seminar 31
- Credit Risk Analysis School 32
- Liquidity Risk Management Seminar 33
- Market Risk Analysis Seminar 34
- Principles of Asset/Liability Management Seminar 35
- Real Estate Lending Seminar 36
- Risk Management and Internal Controls Seminar 37
- Technology Risk Supervision Seminar 38
- Joint Banque de France International Banking and Finance Institute/Federal Reserve System – "Seminar on Credit Risk Assessment and Control" 39
- Joint World Bank/International Monetary Fund/Federal Reserve Board – "Conference on Policy Challenges for the Financial Sector" 40
- Joint World Bank/International Monetary Fund/Federal Reserve System – "Seminar for Senior Bank Supervisors from Emerging Economies" 41

S.T.R.E.A.M./Technology Lab Federal Reserve Bank of Chicago Course Descriptions 43
- E-Banking/Mobile Banking 46
- Information Systems Vulnerability Management 49
- IT Supervisory Themes and Emerging Topics 52
- Network Security 55
- Operating Systems 57

Federal Financial Institutions Examination Council Course Descriptions 59
- Financial Crimes Seminar 61
- International Banking School 62
- Payment Systems Risk Conference 63

Other Agency Course Descriptions 65
- The Options Institute 67

Introduction

Introduction

It is our pleasure to provide you with this catalogue of examiner training courses the Federal Reserve System will offer in 2015. The Federal Reserve's 2015 examiner training programs will be held in training facilities at 1850 K Street NW, in Washington, D.C., as well as in the training facilities of the Federal Reserve Banks of Chicago and San Francisco. For your convenience, the catalogue also contains information on select courses offered by the Federal Financial Institutions Examination Council (FFIEC) as well as general information about registration procedures, lodging, and other relevant information. It is important that you read the information contained in this catalogue prior to submitting an application or nominating staff from your institution to these training programs. The International Training and Assistance (ITA) Section's website, which includes a link to this complete catalogue, can be accessed online at *www.federalreserve.gov/bankinforeg/ita/about_ita.htm.*

The Federal Reserve is pleased to accommodate colleagues from other bank supervisory authorities and central banks in its training programs on a space-available basis. As most classes fill up quickly, it is recommended that you submit an application or a request to enroll your staff as early as possible. We must ask that all enrollments be made at least *eight weeks* before the start date of the class.

Prior to the start of the program, every participant registered in a Federal Reserve course will receive a participant letter that provides course details along with lodging and transportation options. Many courses contain some background reading material or pre-course work, which must be completed by the participant prior to the first day of class. The nature of the required pre-course work is listed under each course description along with the estimated amount of time the participant must dedicate to complete it. Pre-course work is designed to bring each participant to a base level of knowledge, thereby enabling instructors to deliver information effectively and use class time efficiently. Registered participants can download pre-course work, the participant letter, and hotel/area information from a secure website by creating their own personalized Knowledge Central account. *Please note, English proficiency is a requirement for all courses outlined in this catalogue.*

Finally, we would like to draw your attention to the joint World Bank/International Monetary Fund/Federal Reserve System "Seminar for Senior Bank Supervisors from Emerging Economies," which is offered every October in Washington, D.C. The objectives of the seminar are to familiarize participants with the importance of bank and financial sector regulation and supervision for economic growth and development; to consider alternative regulatory and supervisory approaches and related international trends; to discuss solutions for dealing with bank insolvency and financial system distress; and to learn about the latest developments in supervision and on-site examination techniques.

Please note there are new course, feature, and service offerings in 2015 for our international participants. Among them are

- ***Joint Banque de France International Banking and Finance Institute/Federal Reserve System "Credit Risk Assessment and Control.*** We are collaborating with the Banque de France's International Banking and Finance Institute to offer a seminar designed to demonstrate a risk-focused approach to assessing and examining a financial institution's credit, market, liquidity, and operational activities. The course will highlight core elements of the examination process, such as planning, implementation, and follow-up. While presentations will be made simultaneously in French and English, this program is primarily offered for the benefit of French-speaking bank supervisory officials and staff.

Introduction

- ***The Options Institute.*** The program, which is held once a year for three days at the Chicago Board Options Exchange, will now run from 8:30 a.m. to 4:15 p.m. on Monday, 8:30 a.m. to 4 p.m. on Tuesday, and 8:30 a.m. to 2:30 p.m. on Wednesday.
- ***ITA Knowledge Central Community.*** We are pleased to partner this year with Knowledge Central, the Federal Reserve System's collaborative knowledge sharing exchange, to offer participants in our international training programs access to the *International Training and Assistance Program Community*, a professional networking and communications forum. Participants can elect to become community members by creating their own personalized Knowledge Central accounts, whereby they can maintain contact with each other, stay abreast of developments in their shared discipline, and exchange information about available training opportunities sponsored by the Federal Reserve System or its worldwide partners. In addition, Knowledge Central offers participants the ability to download training program materials, including the participant letter, directly and more efficiently from its secure, document delivery platform.

Lastly, please note that all inquiries concerning the Federal Reserve's international training and technical assistance program may be submitted to

Mr. Sarkis D. Yoghourtdjian
Assistant Director
Division of Banking Supervision and Regulation
Board of Governors of the Federal Reserve System
Washington, DC 20551

Introduction

Meet the Staff

John McCormick
Manager

Juan Melendez
Financial Analyst

Arras Korogluyan
Intern

Jose Pignano
Senior Supervisory Financial Analyst

Maribeth Seraj
Curriculum Analyst

Sheila Simms
Senior International Training and Assistance Technician

Robert Walker
Senior Supervisory Financial Analyst

General Information

General Information

Who May Attend?

Programs included in this catalogue are open to banking supervision staff from central banks and bank supervisory authorities outside the United States.

Registration Procedures

In order to attend a program, you must first complete and submit an application form online at *www.federalreserve.gov/bankinforeg/ita/courses.htm*. Click on a course from the list of courses, and on the interactive course description page, click "Apply Now" to start the application process. Once the application has been submitted, a reference number will be e-mailed to you for use in all future correspondence. Approval from your institution must be obtained prior to applying for a training program. Applications will not be processed until an official, signed letter of endorsement from an officer of your institution has been submitted. The letter may be faxed to +1-202-452-6417 or scanned and e-mailed to BSRInternationalTraining@frb.gov. Please mail the original letter on official stationery to

Mr. Sarkis D. Yoghourtdjian
Assistant Director
Division of Banking Supervision and Regulation
Board of Governors of the Federal Reserve System
20th and C Streets NW
Attention: Course Registrar, mail stop 1819
Washington, DC 20551

Security Procedures

Please note that the Federal Reserve has put in place security measures requiring each participant in a Federal Reserve program to submit his or her *date of birth*, *passport number*, and *country of passport issuance* as soon as possible. This information must be received prior to an application's approval. There will be no exceptions. **Failure to provide the necessary information will result in forfeiture of the seat.**

Tuition

There are no tuition fees for Federal Reserve or FFIEC programs outlined in this catalogue. The Options Institute Program at the Chicago Board Options Exchange (CBOE) carries a $1,075 tuition fee per participant payable to the CBOE by credit card on the first day of the program.

General Information

Lodging Information

The Federal Reserve does not make lodging arrangements for participants attending any of our catalogue-listed programs. Therefore, participants are responsible for arranging their own lodging accommodations. For those attending the joint World Bank/International Monetary Fund/Federal Reserve “Seminar for Senior Bank Supervisors from Emerging Economies" and the “Conference on Policy Challenges for the Financial Sector” only, seminar organizers will secure blocks of rooms at select area hotels. It will be up to the participants to make their own reservations with these hotels and provide a credit card guarantee.

Pre-Course Materials

Pre-course materials will be made available after all required information, including the official endorsement letter and participant’s date of birth, passport number, and name of country issuing the passport, has been received and the application has been approved. Once approved, the participant will receive instructions on how to access the program's participant letter and pre-course materials (if any) from Knowledge Central, ITA's secure document delivery platform. Please note that participant access to Knowledge Central requires the creation of a personalized user account.

Dress Code

Business casual attire is permitted for all programs offered in this catalogue, except for the joint World Bank/International Monetary Fund/Federal Reserve programs conducted in June and October, which require business attire. Tennis shoes, T-shirts, blue jeans, and shorts should not be worn.

Attendance Policy

Participants in Federal Reserve and FFIEC training programs are expected to be in attendance at each session of the program. Please notify an ITA Section staff member of unavoidable absences. Unexplained absences from a training session will be reported to the proper authorities.

Travel and Medical Insurance

Please note that the Federal Reserve does **not** provide any insurance coverage for participants traveling to, from, or staying in the United States. Please ensure that there is adequate medical insurance coverage in place for your needs. Any medical costs incurred in the United States will be the responsibility of the participant or the participant's institution.

Cancellation Policy

To cancel participation in a Federal Reserve or FFIEC training program, please send a letter to Mr. Sarkis Yoghourtdjian at the address below. The letter must be on official stationery and signed by an officer of your institution. **If participation is not cancelled and the participant does not report to the training facility on the first day of the program, security procedures require us to notify the proper authorities, including the U.S. visa issuing agency.**

General Information

Training Facilities in Washington, D.C.

The ITA Section is pleased to welcome all participants in our Washington, D.C.-based courses to the Federal Reserve's training facility at the International Square Building complex (the complex), which is situated on an entire block between 18th and 19th Streets Northwest and between I and K Streets Northwest. Participants may enter the complex at any of its three entrances located at the corners of I and 18th Streets, I and 19th Streets, and K and 19th Streets. Participants will find a central atrium upon entering the complex. Opening onto this atrium are three separate lobbies for each of the buildings comprising the complex, designated as 1825 I Street, 1850 K Street, and 1875 K Street.

Participants should proceed to the 1850 K Street lobby, where they will be asked to show their identification to the building's concierge and sign the guest book. The concierge will direct the participants to the elevators for the Federal Reserve's training center located on the fourth floor.

International Square's lower level features a food court that offers American, Asian, Greek, Mexican, Indian, and Cuban fast food selections. The lower level also allows direct access to the subway system through the "Farragut West" metro station, serviced by the blue and orange metro lines.

Please note, smoking and the use of tobacco products are prohibited throughout the International Square complex.

Questions?

Should you have any questions, you may direct them to

Mr. Sarkis D. Yoghourtdjian
Assistant Director
Division of Banking Supervision
and Regulation, *or*

Ms. Maribeth Seraj
Curriculum Analyst

Board of Governors of the Federal Reserve System
Washington, DC 20551
Fax: +1-202-452-6417
BSRInternationalTraining@frb.gov

General Information

Hotels near the Federal Reserve's Training Center in Washington, D.C.

For your reference and information, listed below are a number of hotels within close proximity to the Federal Reserve's training center at 1850 K Street NW, Washington, D.C. You are free to make hotel reservations at these or other hotels. Since Washington, D.C. is a popular destination, *early* registration will ensure the best selection of hotel rooms and rates.

*Walking distance
**Taxi or 20–30 minute walk

*Club Quarters
839 17th Street NW
Washington, DC 20006
Tel: +1-202-463-6400
Fax: +1-202-463-6401
www.clubquarters.com

*Hotel Lombardy
2019 Pennsylvania Avenue NW
Washington, DC 20006
Tel: +1-202-828-2600
Fax: +1-202-872-0503
www.hotellombardy.com

*The Quincy Hotel
1823 L Street NW
Washington, DC 20036
Tel: +1-202-223-4320
Fax: +1-202-293-4977
www.thequincy.com

*One Washington Circle
1 Washington Circle NW
Washington, DC 20037
Tel: +1-202-872-1680
Fax: +1-202-887-4989
www.thecirclehotel.com

*AKA White House
1710 H Street NW
Washington, DC 20006
Tel: +1-202-904-2500
Fax: +1-202-904-2524
www.stayaka.com

*Hampton Inn Washington, DC/White House
1729 H Street NW
Washington, DC 20006
Tel: +1-202-296-1006
Fax: +1-202-296-1008
http://hamptoninn3.hilton.com

** Hilton Garden Inn Washington DC Downtown
815 14th Street NW
Washington, DC 20005
Tel: +1-202-783-7800
Fax: +1-202-783-7801
www.hiltongardeninn3.hilton.com

**Residence Inn Marriott
801 New Hampshire Avenue NW
Washington, DC 20037
Tel: +1-202-785-2000
Fax: +1-202-785-9485
www.marriott.com

**The Dupont Hotel
1500 New Hampshire Avenue NW
Washington, DC 20036
Tel: +1-202-483-6000
Fax: +1-202-328-3265
www.doylecollection.com

**State Plaza Hotel
2117 E Street NW
Washington, DC 20037
Tel: +1-202-861-8200
Fax: +1-202-659-8601
www.stateplaza.com

**Melrose Hotel
2430 Pennsylvania Avenue NW
Washington, DC 20037
Tel: +1-202-955-6400
Fax: +1-202-775-8489
www.melrosehoteldc.com

**Avenue Suites
2500 Pennsylvania Avenue
Washington, DC 20037
Tel: +1-202-333-8060
Fax: +1-202-338-3818
www.avenuesuites.com

**Best Western Georgetown Hotel & Suites
1121 New Hampshire Avenue NW
Washington, DC 20037
Tel: +1-202-457-0565
Fax: +1-202-331-9421
www.bestwestern.com

**The River Inn
924 25th Street NW
Washington, DC 20037
Tel: +1-202-337-7600
Fax: +1-202-337-6520
www.theriverinn.com

Hotels in Virginia

These hotels are included for consideration since they typically charge less than hotels in D.C., although a 15 or 20 minute metro ride (approximately $5.00 round trip) is necessary to arrive at the Federal Reserve's training center at 1850 K Street NW, Washington, D.C.

Best Western Rosslyn/Iwo Jima
1501 Arlington Boulevard
Arlington, VA 22209
Tel: +1-703-524-5000
Fax: +1-703-522-5484
www.bestwestern.com

Americana Hotel
1400 Jefferson Davis Highway
Arlington, VA 22202
Tel: +1-703-979-3772
Fax: +1-703-979-0547
www.americanahotel.com

Inns of Virginia Arlington
3335 Lee Highway
Arlington, VA 22207
Tel: +1-703-524-9800
Fax: +1-703-522-2167
www.innsofva.com

General Information

The Federal Reserve Bank of Chicago will host the following classes:

- **Liquidity Risk Management Seminar** — July 27–31 (see page 33)
- **Real Estate Lending Seminar, Session 1** — August 17–20 (see page 36)
- **Technology Risk Supervision Seminar** — August 17–21 (see page 38)
- **S.T.R.E.A.M./Technology Lab Courses** (see pages 21–22, 45–58)

The Federal Reserve Bank of Chicago is located at
230 South LaSalle Street, Chicago, Illinois

Hotels near the Federal Reserve Bank of Chicago

Listed below are a number of hotels within close proximity to the Federal Reserve Bank of Chicago. You are free to make hotel reservations at these or other hotels.

*Walking distance
**Taxi or 20–30 minute walk

*Club Quarters Central Loop
111 West Adams Street
Chicago, IL 60603
Tel: +1-312-601-3525
Fax: +1-312-601-3300
www.centralloophotel.com

*Palmer House – A Hilton Hotel
17 East Monroe Street
Chicago, IL 60603
Tel: +1-312-726-7500
Fax: +1-312-917-1707
www.palmerhousehiltonhotel.com

*The Silversmith Hotel
10 South Wabash Avenue
Chicago, IL 60603
Tel: +1-312-372-7696
Fax: +1-312-372-7320
www.silversmithchicagohotel.com

*Club Quarters Wacker at Michigan
75 East Wacker Drive
Chicago, IL 60601
Tel: +1-312-357-6400
Fax: +1-312-357-9900
www.clubquarters.com

**Wyndham Grand Chicago Riverfront
71 East Wacker Drive
Chicago, IL 60601
Tel: +1-312-346-7100
Fax: +1-312-346-4549
www.wyndhamgrandchicagoriverfront.com

**Swissôtel
323 East Wacker Drive
Chicago, IL 60601
Tel: +1-312-565-0565
Fax: +1-312-565-0540
www.swissotel.com

**Residence Inn Chicago
201 East Walton Place
Chicago, IL 60611
Tel: +1-312-943-9800
Fax: +1-312-943-8579
www.marriott.com

**Sofitel Chicago
20 East Chestnut Street
Chicago, IL 60611
Tel: +1-312-324-4000
Fax: +1-312-324-4026
www.sofitel.com

General Information

The Federal Reserve Bank of San Francisco will host the following classes:

- **Capital Planning and Stress Testing Seminar** — October 5–9 (see page 30)
- **Real Estate Lending Seminar, Session 2** — November 2–5 (see page 36)

The Federal Reserve Bank of San Francisco is located at
101 Market Street, San Francisco, California

Hotels near the Federal Reserve Bank of San Francisco

Listed below are a number of hotels within close proximity to the Federal Reserve Bank of San Francisco. You are free to make hotel reservations at these or other hotels.

*Walking distance
**Taxi /public transportation or 20–30 minute walk

*Hyatt Regency
5 Embarcadero Center
San Francisco, CA 94111
Tel: +1-415-788-1234
Fax: +1-415-398-2567
www.sanfranciscoregency.hyatt.com

*Harbor Court Hotel
165 Steuart Street
San Francisco, CA 94105
Tel: +1-415-882-1300
Fax: +1-415-882-1313
www.harborcourthotel.com

*Hilton San Francisco Financial District
750 Kearny Street
San Francisco, CA 94108
Tel: +1-415-433-6600
Fax: +1-415-765-7891
www.sanfranciscohiltonhotel.com

*Hotel Abri
127 Ellis Street
San Francisco, CA 94102
Tel: +1-415-392-8800
Fax: +1-415-398-2650
www.hotelabrisf.com

*Club Quarters
424 Clay Street
San Francisco, CA 94111
Tel: +1-415-392-7400
Fax: +1-415-392-7300
www.clubquarters.com

**Hotel Nikko
222 Mason Street
San Francisco, CA 94102
Tel: +1-415-394-1111
Fax: +1-415-394-1106
www.hotelnikkosf.com

**San Francisco Marriott Marquis
780 Mission Street
San Francisco, CA 94103
Tel: +1-415-896-1600
Fax: +1-415-486-8101
www.marriott.com

**The Prescott Hotel
545 Post Street
San Francisco, CA 94102
Tel: +1-415-563-0303
Fax: +1-415-563-6831
www.prescotthotel.com

General Information

Duration of Programs

Federal Reserve System Courses

Advanced Credit Risk Measurement and Management Seminar	1 week
Anti-Money Laundering Examination Seminar	1 week
Bank Analysis and Examination School	1 week
Capital Planning and Stress Testing Seminar	1 week
Consolidated Supervision and Risk Integration Seminar	1 week
Credit Risk Analysis School	1 week
Liquidity Risk Management Seminar	1 week
Market Risk Analysis Seminar	1 week
Principles of Asset/Liability Management Seminar	1 week
Real Estate Lending Seminar	4 days
Risk Management and Internal Controls Seminar	1 week
Technology Risk Supervision Seminar	1 week
Joint Banque de France International Banking and Finance Institute/Federal Reserve System – "Seminar on Credit Risk Assessment and Control"	1 week
Joint World Bank/International Monetary Fund/Federal Reserve Board – "Conference on Policy Challenges for the Financial Sector"	3 days
Joint World Bank/International Monetary Fund/Federal Reserve System – "Seminar for Senior Bank Supervisors from Emerging Economies"	2 weeks

S.T.R.E.A.M./Technology Lab - Federal Reserve Bank of Chicago Courses

E-Banking/Mobile Banking	1 week
Information Systems Vulnerability Management	1 week
IT Supervisory Themes and Emerging Topics	1 week
Network Security	1 week
Operating Systems	1 week

Federal Financial Institutions Examination Council (FFIEC) Courses

Financial Crimes Seminar	3½ days
International Banking School	1 week
Payment Systems Risk Conference	3½ days

Other Agency Courses

The Options Institute	(CBOE)	3 days

Schedules

Schedule — Federal Reserve System

Program	From	To
IT Supervisory Themes and Emerging Topics, Session 1 (Chicago, IL)	April 27	May 1
Payment Systems Risk Conference, Session 1(Arlington, VA)	May 4	May 7
Anti-Money Laundering Examination Seminar (Washington, DC)	May 4	May 8
IS Vulnerability Management, Session 1 (Chicago, IL)	June 1	June 5
Joint World Bank/International Monetary Fund/Federal Reserve Board "Conference on Policy Challenges for the Financial Sector" (Washington, DC)[1]	June 3	June 5
Advanced Credit Risk Measurement and Management Seminar (Washington, DC)	June 15	June 19
Credit Risk Analysis Seminar (Washington, DC)	June 22	June 26
E-Banking/Mobile Banking (Chicago, IL)	June 22	June 26
Bank Analysis and Examination Seminar (Washington, DC)	July 20	July 24
Network Security (Chicago, IL)	July 20	July 24
Liquidity Risk Management Seminar (Chicago, IL)	July 27	July 31
Consolidated Supervision and Risk Integration Seminar (Washington, DC)	August 10	August 14
Real Estate Lending Seminar, Session 1 (Chicago, IL)	August 17	August 20
Technology Risk Supervision Seminar (Chicago, IL)	August 17	August 21
Financial Crimes Seminar, Session 1 (Arlington, VA)	August 24	August 27
Risk Management and Internal Controls Seminar (Washington, DC)	August 24	August 28
IT Supervisory Themes and Emerging Topics, Session 2 (Chicago, IL)	August 24	August 28
The Options Institute (Chicago, IL)	September 14	September 16
Principles of Asset/Liability Management Seminar (Washington, DC)	September 14	September 18
Joint Banque de France International Banking and Finance Institute/Federal Reserve System "Seminar on Credit Risk Assessment and Control" (Paris, France)	September 14	September 18
Operating Systems (Chicago, IL)	September 14	September 18
Market Risk Analysis Seminar (Washington, DC)	September 21	September 25
Capital Planning and Stress Testing Seminar (San Francisco, CA)	October 5	October 9
Payment Systems Risk Conference, Session 2 (Arlington, VA)	October 19	October 22
Joint International Monetary Fund/World Bank/Federal Reserve System "Seminar for Senior Bank Supervisors from Emerging Economies" (Washington, DC)	October 19	October 30
Financial Crimes Seminar, Session 2 (Arlington, VA)	October 26	October 29
IS Vulnerability Management, Session 2 (Chicago, IL)	October 26	October 30

Schedule — Federal Reserve System

Program	From	To
International Banking School (Arlington, VA)	October 26	October 30
Real Estate Lending Seminar, Session 2 (San Francisco, CA)	November 2	November 5

Note: Schools and programs denoted in bold text are designed for and offered exclusively to participants from other central banks and supervisory authorities.

[1] Participation in this conference is by invitation only.

Schedule — S.T.R.E.A.M./Technology Lab Federal Reserve Bank of Chicago

Program	From	To
IT Supervisory Themes and Emerging Topics		
Session 1	April 27	May 1
Session 2	August 24	August 28
E-Banking/Mobile Banking	June 22	June 26
Information Systems Vulnerability Management		
Session 1	June 1	June 5
Session 2	October 26	October 30
Network Security	July 20	July 24
Operating Systems	September 14	September 18

Note: All S.T.R.E.A.M./Technology Lab courses are held at the
Federal Reserve Bank of Chicago, 230 South LaSalle Street, Chicago, Illinois.

Hotels near the Federal Reserve Bank of Chicago

Listed below are a number of hotels within close proximity to the Federal Reserve Bank of Chicago. You are free to make hotel reservations at these or other hotels.

*Walking distance
**Taxi or 20–30 minute walk

*Club Quarters Central Loop
111 West Adams Street
Chicago, IL 60603
Tel: +1-312-601-3525
Fax: +1-312-601-3300
www.centralloophotel.com

*Palmer House – A Hilton Hotel
17 East Monroe Street
Chicago, IL 60603
Tel: +1-312-726-7500
Fax: +1-312-917-1707
www3.hilton.com

*The Silversmith Hotel
10 South Wabash Avenue
Chicago, IL 60603
Tel: +1-312-372-7696
Fax: +1-312-372-7320
www.silversmithchicagohotel.com

*Club Quarters Wacker at Michigan
75 East Wacker Drive
Chicago, IL 60601
Tel: +1-312-357-6400
Fax: +1-312-357-9900
www.clubquarters.com

Schedule — S.T.R.E.A.M./Technology Lab Federal Reserve Bank of Chicago

**Wyndham Grand Chicago Riverfront
71 East Wacker Drive
Chicago, IL 60601
Tel: +1-312-346-7100
Fax: +1-312-346-4549
www.wyndhamgrandchicagoriverfront.com

**Swissôtel
323 East Wacker Drive
Chicago, IL 60601
Tel: +1-312-565-0565
Fax: +1-312-565-0540
www.swissotel.com

**Residence Inn Chicago
201 East Walton Place
Chicago, IL 60611
Tel: +1-312-943-9800
Fax: +1-312-943-8579
www.marriott.com

**Sofitel Chicago
20 East Chestnut Street
Chicago, IL 60611
Tel: +1-312-324-4000
Fax: +1-312-324-4026
www.sofitel.com

Schedule — Federal Financial Institutions Examination Council (FFIEC)

Program	From	To
Financial Crimes Seminar		
Session 1	August 24	August 27
Session 2	October 26	October 29
International Banking School	October 26	October 30
Payment Systems Risk Conference		
Session 1	May 4	May 7
Session 2	October 19	October 22

Note: All FFIEC courses are held at the
L. William Seidman Center at 3501 Fairfax Drive, Arlington, Virginia (a suburb of Washington, DC).

Hotels near the FFIEC's training facility in Arlington, Virginia

Listed below are a number of hotels within close proximity to the L. William Seidman Center in Arlington, Virginia. You are free to make hotel reservations at these or other hotels.

*Walking distance
**Taxi or 20–30 minute walk
***Taxi or public transportation

Seidman Center Student Residence
1001 North Monroe Street
Arlington, VA 22226
Tel: +1-703-516-4630
Fax: +1-703-516-5476

*Hilton Arlington
950 North Stafford Street
Arlington, VA 22203
Tel: +1-703-528-6000
Fax: +1-703-812-5127
www.hilton.com

**Holiday Inn Arlington
4610 North Fairfax Drive
Arlington, VA 22203
Tel: +1-703-243-9800
Fax: +1-703-527-2677
www.holidayinn.com

**The Virginian Suites
1500 Arlington Boulevard
Arlington, VA 22209
Tel: +1-703-522-9600
Fax: +1-703-842-9279
www.virginiansuites.com

**Best Western Rosslyn/Iwo Jima
1501 Arlington Boulevard
Arlington, VA 22209
Tel: +1-703-524-5000
Fax: +1-703-522-5484
www.bestwestern.com

***The Americana Hotel
1400 Jefferson Davis Highway
Arlington, VA 22202
Tel: +1-703-979-3772
Fax: +1-703-979-0547
www.americanahotel.com

Federal Reserve System Course Descriptions

Federal Reserve System
Course Descriptions

Advanced Credit Risk Measurement and Management Seminar

Type of Participant Targeted

The Advanced Credit Risk Measurement and Management Seminar is a course designed for individuals with five or more years of experience with credit risk management. The purpose of the seminar is to provide participants with an overview of advanced credit risk measurement and management techniques from an internal management and supervisory perspective. The seminar provides supervisors with an introduction to the management and examination techniques used to evaluate the effectiveness of advanced risk measurement and management systems.

Prerequisites

None.

Course Overview

This one-week seminar consists of a series of lectures and group exercises intended to provide participants with an overview of the advanced risk measurement and management systems banks employ to monitor credit risk. Lectures will address the estimation and calculation of the inputs into advanced credit risk measurement systems such as probability of default and loss-given default, portfolio management techniques, and the governance necessary to employ these advanced systems. Lectures will also focus on basic methods supervisors can employ to understand and evaluate the effectiveness of banks' implementation of these advanced credit risk management systems. Group work will take the form of a case study and give participants an opportunity to practice and reinforce the techniques discussed during the lectures.

Course Objectives

At the end of the seminar, participants should have an understanding of the following

- The fundamental building blocks an institution must have in place before it begins developing more advanced models and techniques
- What type and quality of data a bank needs to have
- What each of the advanced credit risk metrics are and how they are derived
- Basics of how to examine a bank's models
- Fundamentals of modern portfolio theory and its practical implementation
- Basic portfolio management exam techniques
- What to expect from a board of directors
- What to expect from a senior management team
- The roles of internal and external audit and the role of loan review, including how to examine these functions
- How advanced credit metrics can be used

Anti-Money Laundering Examination Seminar

Type of Participant Targeted

This program is for financial institution supervisors with more than six months of financial institution examination experience and an interest in learning techniques for targeted anti-money laundering and counter-terrorist financing examinations.

Prerequisites

None.

Course Overview

This course is designed to provide banking supervision staff with an understanding of the importance of reviewing the operational, legal, and reputational risks associated with money laundering and terrorist financing and their impact on the overall bank rating assessment. The course provides examiners with guidance on proper customer identification and due diligence procedures, counter-terrorist financing, and suspicious activity reporting. There are also presentations and discussions on assessing the money laundering risks associated with high-risk areas like foreign correspondent banking, wire transfers, private banking and prepaid cards, and other emerging payment systems. This course will also provide an overview of the USA PATRIOT Act, the general U.S. AML/CFT regulatory framework, and the FATF recommendations; it will present the U.S. experience and regulatory perspective on these topics. Case studies will be utilized to highlight and analyze key money laundering and terrorist financing risks in a bank's high-risk business areas.

Course Objectives

Upon completion of this 4½-day seminar, the participant will, at a minimum, have

- A working knowledge of anti-money laundering and counter-terrorist financing terminology
- An overall understanding of the key risks associated with money laundering and the impact on the bank's overall risk management
- A familiarity with examination procedures utilized to review high-risk areas, as well as the bank's internally published anti-money laundering program and procedures
- An understanding of the roles of the risk manager and compliance officer within the environment of the bank
- An ability to apply anti-money laundering examination concepts consistently among different-sized banks

Bank Analysis and Examination School

Type of Participant Targeted

The Bank Analysis and Examination School is designed for individuals with approximately 12 to 18 months of relevant experience. Attendees are typically involved in risk-focused supervision, risk management processes, bank examination, loan classification, and surveillance.

Prerequisites

None.

Course Overview

This is an intensive course based on risk management and analytical concepts that apply to all areas of supervision: examinations, inspections, surveillance, and applications. The program emphasizes risk-focused examination and its products as well as common analytical and supervisory themes and techniques.

Course Objectives

Upon completion of this one-week course, the participant will, at a minimum, be able to

- Discuss and apply risk-focused examination techniques to a bank
- Analyze the financial condition of a bank using the Uniform Bank Performance Report (UBPR)
- Use information from a bank examination report and a UBPR to prepare and present an analysis of a bank's condition
- Understand the CAMELS bank rating system
- Provide an introductory analysis and classification of a loan
- Understand various regulatory and financial topics, including principles of internal controls, information systems, and supervisory strategies

Capital Planning and Stress Testing Seminar

Type of Participant Targeted

The Capital Planning and Stress Testing Seminar is designed for safety and soundness bank supervisors. The curriculum is designed to provide the examination skills necessary for a comprehensive understanding of the capital planning process and capital adequacy. The course also focuses heavily on the mechanics of a robust stress testing process and its role in gauging the resiliency of the organization's capital. Many concepts discussed in the seminar apply to Basel II Pillar 2 assessments as well.

Prerequisites

None.

Course Overview

This course will provide an in-depth exposure to a capital planning process, overall capital adequacy, and the ability to sustain capital in various stressed environments. The goal of this course is to provide a foundation to effectively assess an organization's capital adequacy relative to its overall risk and its plan for maintaining appropriate capital levels. This theoretical foundation will be enhanced with a detailed case study that allows participants to apply their knowledge to reviewing the capital planning process, assessing an organization's risk through stress testing, and analyzing measures of ensuring that capital supports the level of risk.

Course Objectives

Upon completion of this one-week training program, the participant will, at a minimum, be able to

- Identify an organization's risk profile, material portfolios, and operating strategy
- Assess the quality of the organization's capital plan
- Develop supervisory perspectives regarding the quality of capital monitoring
- Develop an understanding of stress testing methodologies
- Understand corporate governance expectations for capital stress testing
- Understand key concepts in the analysis for Basel II Pillar 2 assessments

Consolidated Supervision and Risk Integration Seminar

Type of Participant Targeted

The Consolidated Supervision and Risk Integration Seminar is designed for participants who are familiar with risk-focused supervision and have five or more years of supervision and regulation experience. The curriculum provides a conceptual framework and practical examples of supervisory tools and techniques that help a supervisory team "roll-up" various risk exposures and evaluate a banking organization on a consolidated basis. The seminar provides supervisors with (1) practical bank examination techniques to evaluate enterprise-risk management and (2) exposure to analyzing the financial strength of a consolidated organization.

Prerequisites

This seminar does not have a pre-course assignment. However, participants are strongly encouraged to familiarize themselves with the case study materials prior to the seminar.

Course Overview

This 4½-day seminar is an interactive workshop that includes lectures, discussion sessions, and small group case study work to provide participants with an overview of consolidated supervision analysis. Lectures will address the accounting concepts associated with business consolidation and the review of enterprise-risk management of important risk categories. Group work will take the form of a case study and give participants an opportunity to practice and reinforce the techniques discussed during the lectures. The curriculum recognizes that each participant arrives with unique risk-focused supervision experiences and examination skills. The seminar is intended to build on these experiences and skills to integrate various risk exposures into a consolidated assessment of a large banking organization. Participants will benefit by learning from the application of "real world" experience to a stylized case study.

Course Objectives

Upon completion of this 4½-day seminar, the participant will, at a minimum, be able to

- Recognize and analyze desirable corporate governance and risk control functions
- Recognize risk identification and reporting mechanisms, and build an organization-wide risk assessment
- Incorporate stress testing results plus capital and liquidity adequacy and planning procedures into an organization-wide risk assessment
- Integrate risk assessments of individual risk disciplines into a consolidated risk assessment of a large banking organization

Credit Risk Analysis School

Type of Participant Targeted

The Credit Risk Analysis School is a course designed for individuals with one to three years of supervision and regulation experience. The curriculum provides an introductory learning experience designed to provide a basic set of credit analysis and examination skills that are applicable to the asset quality review function. The typical student will (1) have bank examination experience, (2) have been introduced to loan analysis, and (3) have participated in the examination of loan portfolios during the examinations or inspections of several financial institutions.

Prerequisites

The pre-course assignments consist of a self-instruction module, reading assignments, and an accounting quiz. The pre-course assignments will take approximately 40 hours to complete. The accounting quiz is collected on the first day of class and counts towards the final course grade.

Course Overview

This one-week school is composed of a workshop on basic financial statement analysis and cash flow analysis, loan underwriting case studies, and loan grading exercises. Homework assignments will take approximately eight hours.

The curriculum recognizes that, while the fundamentals of extending credit are similar for all types of lending activities, their application may differ to meet the needs of specific credit transactions. This course gives the participants a systematic strategy for analyzing credits. Participants will benefit by learning analytical skills and applying those skills to actual loan case studies. It is expected that significant additional on-the-job training, experience, and academic opportunities will be necessary to develop a graduate of the Credit Risk Analysis School into a fully competent loan examiner.

Course Objectives

Upon completion of this one-week course, the participant will, at a minimum, be able to

- Identify and analyze the borrowing causes for a loan and determine the proper loan structure and pricing for the risk
- Analyze both business and personal income statements and balance sheets for strengths and weaknesses, and cash flow for loan repayment ability
- Analyze loan documentation for content, completeness, and efficiency
- Analyze the credit risks in personal and business loans of moderate complexity
- Classify loans according to regulatory classification definitions
- Identify the factors to consider when managing a problem loan

Liquidity Risk Management Seminar

Type of Participant Targeted

The Liquidity Risk Management Seminar is designed to prepare market and liquidity risk bank examiners to assess and evaluate the liquidity risk management practices of financial institutions.

Prerequisites

Participants should have a general understanding of the background of liquidity risk. Participants are also strongly encouraged to review the pre-course material.

Course Overview

This one-week seminar will provide an in-depth exposure to liquidity-risk management concepts and methodologies, such as cash flow modeling, stress testing, and international regulatory requirements. The topics covered will enable participants to identify and assess liquidity-risk issues present at most financial institutions, including funding vulnerabilities, asset liquidity value, roll-over risk, funding liquidity risk, market-based liquidity risk, intraday liquidity risk, and contingent liquidity risk. This program will include case study work to illustrate and reinforce the concepts presented in the lectures.

Course Objectives

This program is designed to familiarize the participants with the current issues in liquidity-risk management, including

- Commercial Bank Liquidity Risk Management
  —Collateral management
  —Liquidity cash flow modeling
  —Contingency funding plans
  —Stress testing
  —Intraday liquidity risk
  —Liquidity transfer pricing
  —Stability characteristics of deposits and wholesale liabilities
  —Liquidity risk arising from off-balance sheet activities
  —Liquidity issues related to repurchase agreements, covered bonds, and securitization
- Liquidity Risk in Nonbank Financial Market Intermediaries
  —Potential impact on commercial banks
  —Potential impacts on financial markets

In addition, the course will address the ramifications of new developments in supervision and regulation, such as

- Liquidity requirements contained in the Dodd-Frank Wall Street Reform and Consumer Protection Act, with a focus on requirements for foreign banking entities operating in the United States
- Basel III: standards for liquidity risk management and quantitative liquidity measures (the LCR and NSFR)

Market Risk Analysis Seminar

Type of Participant Targeted

The Market Risk Analysis Seminar (MRAS) is a course designed for individuals with one to three years of supervision and regulation experience. The curriculum is designed to provide the basic set of examination skills needed to understand and provide supervisory oversight of market risk inherent in a financial institution's trading book and overall balance sheet. The typical participant will have experience with (1) bank examinations, (2) the analysis of financial institutions, and (3) the examination of investment portfolios and treasury activities during the examination or inspection of financial institutions.

Prerequisites

Participants should be familiar with financial derivatives (futures, forwards, swaps, and options) and financial mathematics, including bond duration. They should also have a basic understanding of trading activities. Participants will receive a pre-seminar reading assignment, "Review of Basic Math and Financial Concepts," to determine their familiarity with the concepts covered. In addition, they will receive background papers on related topics as supplementary review materials.

Course Overview

MRAS provides an overview of market risk management with respect to both the trading portfolio and overall balance sheet. The course also covers related topics including counterparty credit risk and liquidity risk management. MRAS introduces market risk metrics, such as value-at-risk (VaR), earnings at risk, and economic value of equity, and illustrates a proper risk-management framework, including policies, limits, and internal controls. The course is a combination of lectures on technical risk management topics and short case studies that apply the concepts studied. Fully qualified participants will not require any pre-course study, although background papers on various subjects are provided if participants wish to review basic concepts.

Course Objectives

At the end of this one-week seminar, the participant will, at a minimum, be able to

- Describe the elements of sound internal controls and risk management systems for a bank's trading book and banking book
- Discuss investment and derivative products and understand the components of market risk that can be controlled through the use of on- and off-balance-sheet instruments
- Describe market organization, regulation, and emerging issues in the derivatives market
- Discuss the significance of credit risk management for trading activities
- Describe the VaR method as it relates to trading activities and portfolio management
- Discuss the tools commonly employed to identify, measure, monitor, and control balance sheet market risk and liquidity risk
- Discuss the incentives for securitization, the major types of securitized assets, and the risks and regulatory considerations when a bank begins securitization activities
- Describe the basic accounting concepts and methods for derivative instruments from an international accounting standards perspective

Principles of Asset/Liability Management Seminar

Type of Participant Targeted

The Principles of Asset/Liability Management (PALM) Seminar is designed for safety and soundness bank examiners. It should be taken in examiners' careers when they begin to assess and evaluate asset/liability management (ALM) activities and the market-risk sensitivity of financial institutions as a part of their routine job function.

Prerequisites

Participants should have a general understanding of intermediate financial concepts—similar to that achieved in junior or senior level economics and finance classes. This background should include familiarity with futures, forwards, swaps, and options; duration; and intermediate balance sheet analysis. Participants are encouraged to check their proficiency by reviewing the background papers provided as pre-course supplementary course materials.

Course Overview

PALM provides an in-depth exposure to ALM, concepts, and methodologies as they apply to a financial institution's banking book—non-trading assets and liabilities. (Trading assets are addressed in a companion class, the Market Risk Analysis Seminar.) The materials covered in PALM will enable participants to identify and draw conclusions about interest rate, investment, and liquidity-risk issues they will encounter while examining financial institutions. The course contains a case study based on an intermediate-sized U.S. commercial bank. The case study is used to illustrate and reinforce the balance sheet ALM concepts presented in the lectures. This 4½-day course has no pre-course work, although background papers on various subjects are provided.

Course Objectives

This program is designed to give participants a broad overview of the basic principles of ALM, including

- Interest-rate risk
- Investment portfolio management
- Liquidity risk
- Balance sheet hedging
- ALM model risk management

The class will also provide participants with a basic understanding of

- How financial markets determine interest rates
- How changes in interest rates can affect the risk posture and profitability of financial institutions
- What tools are available to measure interest-rate risk and liquidity risk
- Why and how institutions use certain products to manage their interest-rate risk and liquidity risk

Real Estate Lending Seminar

Type of Participant Targeted

Real Estate Lending (REL) is a seminar designed for participants whose typical job assignments involve the credit-quality evaluation of loan portfolios. The typical participant will have some exposure to real estate credits, along with three to five years of regulatory experience.

Prerequisites

Participants should have completed the *Credit Risk Analysis School* and preferably be commissioned safety and soundness examiners or have equivalent experience with other regulatory agencies or banking departments. There is a required pre-course reading assignment and a suggested reading assignment that each requires approximately three hours to complete.

Course Overview

REL is designed to provide a systematic approach to analyzing real estate acquisition, development, and construction lending facilities. This course reviews various types of real estate projects and the unique risks associated with each. Topics to be addressed include real estate underwriting standards, developer cash flow analysis, appraisals and appraisal policy guidelines, financing different types of real estate, real estate-related accounting issues, problem real estate loan management, classification standards and issues, and local economic conditions affecting real estate lending. REL is an interactive seminar, where participants are encouraged to share relevant experiences and contribute to classroom discussions and case studies.

Course Objectives

Upon completion of this 4-day seminar, the participant will, at a minimum, be able to

- Evaluate the most important risks inherent in common types of real estate projects
- Determine critical due diligence requirements for various real estate loans, including environmental audits, project feasibility studies, plan and budget reviews, and other relevant documentation
- Differentiate the valuation methods and analyze the key elements of a real estate valuation, as well as determine whether the appraisal reports meet applicable requirements
- Analyze the likely adequacy of real estate loan repayment sources, including those related to the borrower, project, and guarantor
- Assess real estate loan policies to determine if they comply with relevant policy statements and guidelines

Risk Management and Internal Controls Seminar

Type of Participant Targeted

This program is for all examiners with more than six months of field examination experience.

Prerequisites

None.

Course Overview

The course is designed to provide examiners with an understanding of the importance of internal controls and risk management in banks, and how the review of internal controls and risk management fits into the overall bank rating assessment. The course is also intended to give examiners guidance on assessing the risk management and internal control environment in key functions such as credit administration and investments, including trading operations, deposits, and payment systems risk.

Course Objectives

Upon completion of this 4½-day seminar, the participant will have

- Gained an overall understanding of key risk management and internal control concepts
- Understood the role of internal and external audits and the internal control environment in a bank
- Become familiar with the role of information technology in banking institutions and the general risk factors and control areas
- Developed examination skills for assessing the risk management and internal control environment of banks in such areas as lending function management and operating areas (funds transfer, trading and investments, trade finance/letters of credit, etc.), resulting in the assignment of an internal control rating
- Developed the ability to apply risk management and internal control examination concepts consistently among banks

Technology Risk Supervision Seminar

Type of Participant Targeted

The Technology Risk Supervision Seminar is an intermediate-level course designed primarily for information technology (IT) examiners. The seminar is also appropriate for safety and soundness examiners who are exposed to IT-related issues during examinations and who have a basic understanding of IT concepts, supervision, and risks for financial institutions.

Prerequisites

None.

Course Overview

The goal of this 4½-day seminar is to provide training in IT supervision of financial institutions.

Course Objectives

The course builds on foundational concepts of 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 more advanced 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; 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 Technology Risk Supervision Seminar, 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

Joint Banque de France International Banking and Finance Institute/Federal Reserve System – "Seminar on Credit Risk Assessment and Control"

Type of Participant Targeted

This program, to be held in Paris jointly with the Banque de France International Banking and Finance Institute (IBFI), is designed for supervisory officials and staff from French speaking countries who have more than three years of relevant field experience and have participated in on-site or off-site examinations of banks. The lectures will be conducted simultaneously in English and French.

Course Overview

This course will cover the definition of credit risk, the Basel rules for credit risk, credit risk management (including risk-adjusted return on capital and portfolio management), credit risk off-site and on-site control, rating systems, stress testing, and implementation by banks and validation of advanced systems.

Course Objectives

This 5-day seminar is designed to

- Broaden participants' knowledge of credit risk management
- Give a practical view of credit risk management through case studies
- Detail the process for identifying and measuring critical risk areas
- Familiarize participants with examination techniques
- Enable participants to develop a final risk profile and identify appropriate supervision tools

Contact for Further Information and Registration

Mr. Jean-Luc Quemard: e-mail: jean-luc.quemard@banque-france.fr

Ms. Chantal Gadroy: e-mail: chantal.gadroy@banque-france.fr

Joint World Bank/International Monetary Fund/Federal Reserve Board – "Conference on Policy Challenges for the Financial Sector"

Type of Participant Targeted

This 3-day program is designed for senior level officials from around the world who hold key positions in the financial sector. These officials generally are governors, deputy governors, heads, or deputy heads of banking supervisory authorities, or high-level staff involved in, or capable of influencing, policy formulation as it concerns the supervision and regulation of banks in their respective countries. Participation in this program is by invitation only.

Program Overview

The program aims to provide policymakers a forum for identifying, developing, and challenging responses to strategy and policy issues. It explores current policy issues, disseminates research in the financial sector, and creates awareness of financial sector issues discussed in international forums.

Presentations serve as a setting for extensive discussions and exchanges of experiences among the participants. Debates will encompass major economic, legal, and institutional strategies and policies that are necessary to ensure that appropriate regulatory and prudential safeguards are in place to support sound and sustainable economic growth.

Joint World Bank/International Monetary Fund/Federal Reserve System – "Seminar for Senior Bank Supervisors from Emerging Economies"

Type of Participant Targeted

This seminar is designed for senior bank supervisors from emerging economies. These supervisors generally are directors of bank supervision, deputy heads of supervision, or high-level staff involved in, or capable of influencing, policy formulation as it concerns the supervision and regulation of banks in their respective countries.

Program Background

In response to the financial crisis, central banks and bank regulators around the world have developed new measures to ensure financial stability by allowing them to identify and appropriately address systemic risks to their financial systems. Regulatory and supervisory processes have been restructured in many countries to deliver a more assertive, risk-based approach to bank supervision. Additionally there is a greater focus on macro-prudential analysis to identify the risks and stresses to the economy and the financial system, including the harm that large, interconnected and highly leveraged institutions could inflict on the financial system and economy if they fail. The supervisory focus is to try to ensure that institutions are better capitalized, more liquid, and better managed than before. To accomplish this goal, a forward looking approach is taken to assess whether, on the balance of risks, there are vulnerabilities in the institution's business models, capital and liquidity positions, governance, risk management, and controls that cast into doubt the institution's financial soundness.

Program Objectives

The objectives of the seminar are

- To familiarize participants with the supervisory problems faced by emerging economies and the constraints such problems pose to economic growth and development
- To discuss alternative solutions for dealing with banking insolvency and financial system distress through deposit insurance schemes and bank restructuring
- To upgrade the technical skills of bank supervisors

At the conclusion of this seminar, participants will, at a minimum, be able to

- Improve supervision and examination capabilities
- Understand the implications of a financial crisis and the alternatives for restructuring banks
- Gain a better understanding of regulations affecting banking institutions and achieve a greater awareness of major regulatory and supervisory topics being discussed at the international level

Joint World Bank/International Monetary Fund/Federal Reserve System – "Seminar for Senior Bank Supervisors from Emerging Economies"

Program Overview

Strong and effective bank supervision and prudential regulation are cornerstones of a healthy financial system. Agencies, such as the World Bank, the International Monetary Fund, and the Federal Reserve System, have strengthened bank supervision and prudential regulations by enacting changes based on experiences realized during different economic conditions. Traditionally, in most countries, highly specialized bank supervision and examination skills have been learned on the job, with only the largest, most developed countries having the resources to establish training departments and courses. Training, to the extent that it has been conducted in emerging economies, has been narrow in focus.

This seminar will attempt to overcome some of these shortcomings by bringing together a group of participants from a wide variety of countries. The program will focus on discussions of the principal policy issues facing bank supervisors in developing countries today. It will establish the linkages between financial system health and macroeconomic performance and the World Bank's general framework for financial sector reform. From these broader issues, the seminar will move to discussions concerning the causes of financial system distress and possible solutions, including problem bank resolution and bank restructuring.

World Bank and IMF staff, and a distinguished group of experts from the U.S. bank supervisory agencies, major international accounting firms, and elsewhere, will lead the discussions. Class participation and interaction will be encouraged.

The seminar will also focus on skills development. Speakers from the Federal Reserve System, the World Bank, the IMF, the Bank for International Settlements, the Toronto Centre, and the Financial Stability Institute, among others, will discuss many aspects of supervisory and regulatory best practices, including implementation of road maps and challenges. Other topics may include loan portfolio management, credit risk, classification of assets, bank analysis, foreign exchange risk, market risk, interest-rate risk, the CAMELS rating system, risk-focused examination techniques, and internal and external auditing. The topics will be presented using a combination of lectures, class discussions, case studies, group exercises, and class presentations. Once again, class participation and interaction will be encouraged as an effective means of sharing ideas and learning. This seminar will continue the process of providing technical assistance to emerging economies.

S.T.R.E.A.M./Technology Lab
Federal Reserve Bank of Chicago
Course Descriptions

S.T.R.E.A.M./Technology Lab
Federal Reserve Bank of Chicago
Course Descriptions

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. Since 1999, 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 interact with software applications and systems as well as observe how they work. The Technology Lab is outfitted with many applications and operating systems found in the financial industry.

A selection of these 4½-day courses is being offered to international participants. The targeted participant is an examiner responsible for technology risk supervision, but who may not have had university training in information technology.

E-Banking/Mobile Banking

Type of Participant Targeted

E-Banking/Mobile Banking is a five-day course intended for examiners with IT examination responsibilities but with little or no university training in information technology. At least one year of field examination experience is preferred.

Prerequisites

None.

Course Overview

This course provides participants with a detailed understanding of the technologies and risks fundamental to electronic banking (e-banking) and mobile banking. Topics include technology and mobile financial service overview, common security threats and vulnerabilities, device authentication techniques, and web application testing. Hands-on demonstrations and exercises encompass web site authenticity evaluation, vulnerability testing, and a Structured Query Language (SQL) injection vulnerability demonstration. Mitigating controls such as web-application testing, mobile device testing, and the Federal Financial Institutions Examination Council's (FFIEC) strong authentication guidance are also covered.

Course Objectives

After completing the course, the participant, at a minimum, will be able to

- Describe fundamental concepts behind modern e-banking/mobile banking technologies
- Perform a risk assessment of an existing e-banking/mobile banking solution
- Test controls in an e-banking/mobile banking environment
- Recommend possible solutions/procedures to enhance e-banking/mobile banking security controls
- Assess the vendor management program to identify required controls that meet financial institution policies and standards

Post-Course Intervention

Participants will learn the technology essentials contributing to internet and mobile banking risks, and will be able to apply that knowledge in the context of common threats. Participants will contrast the risks for serviced and turnkey e-banking platforms, as well as for established and emerging technologies. Case-based demonstrations and exercises will provide context for examination activities.

Learning Objectives

Participants should be able to identify risks associated with the three tiers (presentation, business, and database logic) commonly used to describe the technical implementation of an e-banking/mobile banking website. Participants will also be able to identify the risks associated with various web server technologies. Hands-on exercises will provide participants with an understanding of the SQL as well as

the tiers that can be compromised by attackers. Participants will understand the various technical solution enablers used to support policies and procedures for risk mitigation of associated vulnerabilities and exploits. Finally, the participant will understand the importance of web-application testing methodology and tools.

By module, the following learning objectives will be accomplished:

Module	Learning Objectives
Introduction to E-Banking/Mobile Banking	• Gain a basic understanding of key terms related to e-banking/mobile banking
Mobile Financial Services Overview	• Provide overview of various mobile services (e.g., mobile banking, mobile payment, and alternative transaction channels)
Identifying and Analyzing Risk	• Understand the risk associated with e-banking/mobile banking solutions • Provide a methodology to assess the risks associated with an e-banking/mobile banking solution
E-Banking/Mobile Banking Key Components	• Define e-banking/mobile banking • Describe e-banking/mobile banking infrastructure and components.
Implementing E-Banking/ Mobile Banking	• Introduce web applications • Illustrate e-banking/mobile banking implementation modes
Gathering information	• Identify the means by which attackers can acquire the technical characteristics of a website
Web Search	• Identify the extent of publicly available information that can be found on the Internet regarding financial institutions • Describe ways to limit the amount of information that is publicly available
Web Server	• Introduce IIS Web Server • Introduce Apache Web Server
Web Authentication/Mobile Device authentication	• Illustrate web authentication methods • Describe current mobile device authentication technologies

E-Banking/Mobile Banking

Module	Learning Objectives
Vulnerabilities	• Demonstrate common vulnerabilities in the web server and applications • Illustrate social engineering exploits (e.g., Phishing)
Banking Case Study Overview	• Hands-on lab using a mockup of a financial institution
Common Web Vulnerabilities	• Hands-on lab designed to demonstrate common web vulnerabilities and exploits
Using SQL	• Demonstrate the Structured Query Language • Review key commands used to add, change, or modify data in the database
SQL Injection	• Understand the technical operation and describe how SQL can be used to compromise a host • Review common configuration errors
Web Application Testing	• Review current tools that are designed to automate the detection of vulnerabilities
Vulnerability Testing	• Identify other means of testing web applications
Guidelines on Risks and Managing Risks	• Review the FFIEC guidance on Strong Authentication • Review guidance from other agencies regarding the Gramm-Leach-Bliley Act, and legal and data privacy issues
Vendor Management	• Describe vendor selection and evaluation via due diligence • Outline performance monitoring for e-banking/mobile banking third-party solution providers • Assess vendor incident response and management program
Examination Issues	• Describe common issues related to e-banking/mobile banking
E-Banking/Mobile Banking Trend Watch	• Maintain awareness of e-banking/mobile banking emerging trends • Anticipate future directions of e-banking/mobile banking

Instructors

This course is developed and supported by a group of instructors with extensive examination experience and expertise in banking technologies. Instructors come from across the Federal Reserve System as well as other regulatory agencies and industry.

Information Systems Vulnerability Management

Type of Participant Targeted

The Information Systems Vulnerability Management course is a one-week 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 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.

Course Objectives

After completing the course, the participant, at a minimum, will be able to

- 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 of 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.

Information Systems Vulnerability Management

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	• Foster a baseline understanding of key terms related to vulnerability management
SQL Injection—Case Study	• 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	• 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	• 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

Information Systems Vulnerability Management

Module	Learning Objectives
Penetration Testing and Vulnerability Assessment (Case Study and Demonstration)	• 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	• 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

Instructors

This course is developed and supported by a group of instructors with extensive examination experience and expertise in banking technologies. Instructors come from across the Federal Reserve System as well as other regulatory agencies and industry.

IT Supervisory Themes and Emerging Topics

Type of Participant Targeted

IT Supervisory Themes and Emerging Topics (ITSTET) is a one-week course. The course 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 overview, virtualization work program, cloud computing, cloud computing vendor management, social media risks and controls, mobile banking and risk assessment, "bring your own device (BYOD)," the Federal Reserve's supervisory guidance letter #11-9 concerning authentication in an internet banking environment, and data leak prevention. The class modules are dynamically developed based on evolving IT operational risks and newfound IT exam issues. Therefore, each class may have different focus areas based on latest IT trends.

Course Objectives

Upon completion of this course, the participant, at a minimum, will be able to

- Demonstrate a basic understanding of 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.

Learning Objectives

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

IT Supervisory Themes and Emerging Topics

By module, the following learning objectives will be accomplished:

Module	Learning Objectives
Supervisory Control and Data Acquisition (SCADA) and the Internet of Things (IoT).	• Explain the basic concepts of SCADA and IoT • Identify the risks associated with SCADA and IoT • Recommend the necessary policies, procedures, and controls to mitigate the risks
Virtual Currencies	• Explain the basic transaction flows of virtual currencies • Identify the risks associated with virtual currencies • Identify regulatory and examiner touchpoints
Virtualization Overview	• Explain the basic concept of virtualization • Identify the advantages of server virtualization
Virtualization Work Program	• Explain how to use virtualization work program to conduct virtualization exam • Evaluate the controls and processes in the virtual environment
Cloud Computing	• Explain cloud computing concept • Illustrate various deployment models • Identify security and compliance risks • Evaluate controls to mitigate the risks
Cloud Computing Vendor Management	• Identify the necessary management process and technical controls in the cloud • Review the vendor risk matrix • Assess cloud vendor's security and compliance capabilities
Social Media Risks and Controls	• Understand the social media applications in various forms • List the exposures and risks regarding information security • Recommend the necessary policies, procedures and controls to mitigate the risks
Social Media Hands-on Labs	• Explain the social channels such as Twitter • Illustrate Internet search with privacy protection • Evaluate the management of social media channels
Mobile Banking Risks and Controls	• Review and discuss mobile banking technology • Identify risks and controls
Mobile Banking Case Study–Risk Assessment	• Explain critical areas impacted by mobile banking • Identify financial risks and operational risks associated with mobile banking • Evaluate controls to mitigate the risks

(continued on next page)

Table—*continued*

Module	Learning Objectives
SR 11-9 Authentication in an Internet Banking Environment	• Review the guidelines • Evaluate multi-layer authentication implementations
Bring Your Own Device	• Understand the benefits and risks of BYOD • Recommend the necessary policies, procedures and controls to mitigate the risks

Instructors

This course is developed and supported by a group of instructors with extensive examination experience and expertise in banking technologies. Instructors come from across the Federal Reserve System as well as other regulatory agencies and industry.

Network Security

Type of Participant Targeted

The Network Security course is a one-week 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 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/prevention systems (IDS/IPS).

Course Objectives

After completing the course, the participant, at a minimum, will be able to

- Explore, map, and analyze realistic TCP/IP networks using a variety of diagnostic software tools
- Examine the role of access controls within an networked environment
- Explore the different firewall types and architectures that exist in a simulated e-banking setting
- Identify the different IDS products currently available, determine the limitations of these products, and understand the controls needed for maintaining an IDS infrastructure
- Discuss examination procedures outlined in the IT Examination Handbook produced by the FFIEC
- Conduct hands-on lab work utilizing commonly available network tools

Post-Course Intervention

Participants will learn the essential components of a network. For each technical element (e.g., firewalls and intrusion detection systems), appropriate controls will be reviewed.

Learning Objectives

Examiners should be able to articulate the key risk elements associated with operating and managing a production network. Good network security starts with an accurate risk assessment. 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. Change management is critical as is ensuring that hosts are hardened according to corporate guidelines. Remote access also needs to be managed to include some form of monitoring and logging. 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.

Network Security

By module, the following learning objectives will be accomplished:

Module	Learning Objectives
Network Attack Vectors	• Identify and understand the technical implications of the latest network attack vectors • Assess effectiveness of alternative mitigation techniques
Perimeter Defense: Firewalls	• Evaluate and assess appropriate implementation of firewall controls relative to the complexity of a given network • Use network configuration and sound design of firewall architecture through multiple filter points, active firewall monitoring and management, and integrated security monitoring
Network Diagramming	• Review the elements of layered security and understand how network devices are used to separate zones of risk
Protocols	• Illustrate the OSI model by following a packet from encapsulation on one computer to de-encapsulation on another • Examine the various protocol characteristics and evaluate the risk associated with using protocols in a production environment
IDS/IPS Systems	• Distinguish between alert and block versus alert and pass strategies • Identify sound practices associated with current state-of-the-art intrusion detection and prevention system devices

Instructors

This course is developed and supported by a group of instructors with extensive examination experience and expertise in banking technologies. Instructors come from across the Federal Reserve System as well as other regulatory agencies and industry.

Operating Systems

Type of Participant Targeted

The Operating Systems course is a one-week 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), including network OS, virtual machines, mobile device operating systems, the Microsoft OS family (including Windows 2008/2012 server, Windows 7, and Windows 8), 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

- 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 OS within a financial institution. They should review security measurements and recommend proper security controls to protect various OS assets.

Learning Objectives

Participants build up a solid understanding of various OS 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.

Operating Systems

By module, the following learning objectives will be accomplished:

Module	Learning Objectives
Operating Systems Overview	• 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	• Explain features of Unix and Linux • Identify security strengths and weaknesses • Audit Unix and Linux
Windows Security and Controls	• 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	• Gain basic understanding of virtual machine solutions • Explain features in virtualization player • Review virtualization vendors
Windows 7 and 8	• Describe new options and features in Windows 7 and 8 • Explain new security applications • Consider migration impacts
Windows Servers	• Review features in the latest Microsoft server 2008/2012 • Identify new security controls and improvement in user interface
IBM OS/400	• 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	• Explain features of network router, switch, and firewall • Understand roles of network devices and access control lists • Understand user creation, OS administration, maintenance, and audit

Instructors

This course is developed and supported by a group of instructors with extensive examination experience and expertise in banking technologies. Instructors come from across the Federal Reserve System as well as other regulatory agencies and industry.

Federal Financial Institutions Examination Council Course Descriptions

Financial Crimes Seminar

Type of Participant Targeted

The Financial Crimes Seminar is offered to commissioned safety and soundness examiners.

Prerequisites

None.

Course Overview

The Financial Crimes Seminar provides commissioned examiners with a higher level of knowledge of fraudulent schemes and insider abuses. The seminar is designed to provide insight and information on a variety of current and emerging financial crime-related topics. Presenters may include staff from the U.S. Federal Bureau of Investigation, the Securities and Exchange Commission, the Financial Crimes Enforcement Network, the Department of Justice, and various regulatory agencies. Industry specialists, accountants, and attorneys may also serve as presenters.

Topics vary from year to year based on feedback from prior participants, regulatory changes, and discussions with an interagency development group.

Course Objectives

Upon completion of this 3½-day seminar, the seminar participants should have a heightened awareness of

- Current financial crimes impacting financial institutions
- Red flags of mortgage fraud
- Potential insider abuse
- Interviewing techniques
- Examiner insights to uncovering fraud
- Current trends in cyber crimes and payment systems risk
- Fidelity Bond coverage

International Banking School

Type of Participant Targeted

The International Banking School is a specialized course not intended for all bank examiners. Rather, it is designed for examiners who have supervisory responsibilities for regional or multinational banks that are actively engaged in international banking activities and for U.S. branches and agencies of foreign banks. This course is considered inappropriate for those who do not have international supervisory responsibilities.

Prerequisites

Examiners who have limited international banking knowledge are required to complete the FFIEC *Basic International Banking Self-Study* course prior to attending this course. This prerequisite may be waived if the participant can demonstrate significant international experience.

Course Objectives

At the completion of the of the 4½-day course course, a participant will be able to

- Identify key global organizations and their influence on international banking
- Identify current key regulatory and market issues in examining and supervising financial holding companies and banks with international banking activities
- Analyze the major forces driving structural changes in international financial markets and the impact of these changes on the banking community
- Define country macroeconomic and financial risks and identify how they materialize at financial institutions
- Evaluate the role of global rating agencies and their impact on banks' capital adequacy and their capital markets transactions
- Discuss major components of Basel II and III, and their influence on international financial markets
- Identify significant issues in emerging markets and compare and contrast key countries with international banking activities
- Analyze the various types of foreign exchange (FX) spot and derivatives transactions and their risks
- Discuss mechanics of and trends in global loan, debt, and equity issuance underwriting
- Analyze trade finance activities and their risks

Payment Systems Risk Conference

Type of Participant Targeted

The Payment Systems Risk Conference is intended for commissioned or equivalent tenured field examiners who need a better understanding of the risks associated with payment systems.

Prerequisites

None.

Course Overview

The Payment Systems Risk Conference offers an overview of wholesale and retail payment systems and identifies associated risks. The conference provides examiners with knowledge that may be incorporated into the supervisory process. The conference also includes insight into emerging payment processes and technology and their impact on the financial industry. Topics vary from year to year and are selected based on the feedback from prior participants, regulatory changes, and suggestions from an interagency subject matter expert development group.

Course Objectives

After attending this 3½-day conference, participants will be able to

- Identify current and emerging risks to payment systems and the impact on the financial industry
- Apply regulatory guidance and industry standards on the assessment and management of retail and wholesale payment systems risk to the supervisory process

Other Agency Course Descriptions

The Options Institute

Length

Three days. This course will be held from 8:30 a.m. to 4:15 p.m. on Monday, 8:30 a.m. to 4 p.m. on Tuesday, and 8:30 a.m. to 2:30 p.m. on Wednesday.

Cost

The cost is $1,075 per attendee. All participants taking this program are expected to make payment directly to the Chicago Board Options Exchange (CBOE) with a credit card upon arrival.

Location

The Options Institute is located within CBOE on LaSalle and Van Buren Streets, in Chicago, Illinois.

Instructors

The faculty consists of traders and members of the financial and academic communities.

Course Objectives

The Options Institute is the educational unit within CBOE that offers a 3-day seminar on how to use options for risk management. The seminar explains the role of options in modern portfolio management. The curriculum combines lectures, discussions, strategy workshops, and trading floor experience.

Day 1: The first day of the program covers essential options concepts, options pricing theory, and options mechanics. In addition, the role of the Options Clearing Corporation is discussed. Also, options strategies for risk management are discussed as well as the role of market makers.

Day 2: During the second day, the program covers futures pricing and hedging strategies. Also, index options and foreign currency options are discussed. Participants are introduced to options strategies under simulated market conditions.

Day 3: The final day covers regulatory structure and managing risk using interest rate derivatives, as well as a visit to the trading floor. Participants view the trading floor from inside the trading pit and have the opportunity to ask questions of brokers on the trading floor.

Board of Governors of the Federal Reserve System
www.federalreserve.gov
0115

@FederalReserve

Flickr.com/FederalReserve

YouTube.com/FedReserveBoard