ABA RISK MANAGEMENT

Register Now!

A $10.00 shipping, recordkeeping and administrative fee will be added to all self-paced enrollments.

Course Descriptions Below

Course Name	Tuition
Certificate in Fraud Prevention	**$795**
Introduction to Fraud Management	
Establishing a Fraud Prevention Program	
Types of Fraud and Prevention Strategies	
Operating a Fraud Prevention Program	
Maintaining a Compliant Fraud Prevention Program	
Certificate in Operational Risk Management Bundle	**$1595**
Cybersecurity Management	$275
Elements of an Operational Risk Management Program	$275
Fraud and Criminal Threats	$275
Incident Management and Resilience	$275
Operational Risk Model Management	$275
Oversight and Management of Operational Risk	$275
Payments and Settlements	$275
Physical Security	$275
Regulatory Exam Management	$275
Risk Control and Self Assessment	$275
Vendor Risk Management	$275

Course Descriptions

Certificate in Fraud Prevention

Fraud management professionals face an increased burden to detect and prevent fraud losses against customers and their institution. The ABA Certificate in Fraud Prevention fills a training gap within many institutions and helps both new and experienced financial crimes professionals establish and maintain a fraud management program with sufficient internal and external controls. It provides in-depth training on the applicable U.S. laws and regulations governing fraud and an overview of the various types of criminal behavior commonly used against banks.
The ABA Certificate in Fraud Prevention is an excellent refresher for experienced financial crimes professionals who wish to take the Certified Fraud and AML Professional (CAFP) exam, and may be required for those individuals with less than five years' experience in the field.

You must complete the following courses:

- **Introduction to Fraud Management:** An overview of fraud-related regulations, the key pillars of a fraud prevention program and what makes the program successful or unsuccessful
- **Establishing a Fraud Prevention Program:** A discussion of the components required to start a fraud prevention program, including elements of fraud reporting and what considerations to take regarding risk management
- **Types of Fraud and Prevention Strategies:** An explanation of ACH transactions and a financial institution's related responsibility, including wire fraud, card fraud, ATM fraud, mortgage fraud, as well as the associated risks and challenges
- **Operating a Fraud Prevention Program:** A description of how fraud operations are designed and maintained, including trend anaylsis, defect analysis, and the components of fraud response and recovery opportunities
- **Maintaining a Compliant Fraud Prevention Program:** An overview of the laws and regulations that affect fraud prevention programs, and training and education that relate to fraud strategy

The estimated time to complete these 5 courses is approximately 5 hrs and 20min.

Elements of an Operational Risk Management Program

Highlights the benefits of a strong operational risk program and identifies the key components banks should include, regardless of size or location. Provides an introduction to key definitions, types of risks, key risk indicators, monitoring and controlling risks, and identifying emerging trends.

After completing this course, students will be able to:

- Explain the importance of an operational risk management program
- Describe the categories of risks faced by banks
- Identify the key components of an operational risk management framework

- Describe in general the processes used by banks at each of these lifecycle stages:
  - Risk Identification
  - Risk Assessment
  - Risk Reporting
  - Risk Monitoring

Cybersecurity Management

An understanding of the risks associated with technology and its importance to the bank's operations and its management. Learn what to consider regarding the protection of technology, systems and data from inappropriate modification or destruction.

After completing this course, students will be able to:

- Learn how technology used by banks influences cybersecurity risk
- Describe the regulatory environment for cybersecurity, including GLBA requirements and financial regulatory guidance
- Identify risk stressors that affect the level of cyber risk
- Review the three key activities included in an effective cyber risk management program

Fraud and Criminal Threats

Explains how fraud and other criminal threats affect consumers and financial institutions. Describes considerations when assessing the organization's strength in each pillar of a well-built financial crimes program, and key components of an effective program's operations.

After completing this course, students will be able to:

- Describe the importance of an effective financial crimes program and the risks associated with financial crimes
- Identify the elements of an effective financial crimes program
- Explain the basic four pillars of an effective program and the key aspects of each
- Describe the day-to-day and ongoing operational components of a financial crimes program
- Identify common crimes committed against institutions and effective counter measures

Incident Management and Resilience

Provides an overview of the risk considerations related to an organization's ability to plan for and recover from events that could have negative effects on its ability to continue offering products and services. Also includes a perspective on the current regulatory expectations.

After completing this course, students will be able to:

- Identify the scope of an Incident Management and Resilience program
- Explain the current regulatory environment
- Describe roles and responsibilities across the organization
- How to assess and prioritize risks
- How to develop and test a continuity plan

Operational Risk Model Management

Covers the importance of building and maintaining a strong risk model management framework and the principles of model development. Explains conducting the model validation and how to validate results. Explores types of model controls, maintaining appropriate change controls and how documentation supports an effective model risk framework.

After completing this course, students will be able to:

- Describe the guidance available on model risk management and the role of the board in model risk policy and oversight
- Describe the types of models that are covered under model risk management guidance
- Identify areas of a financial institution where models are typically found and information that should be included in an inventory of models
- Recognize the factors that should be considered when assessing model risk
- Describe the principles of model development and training that should be provided prior to model implementation

Oversight and Management of Operational Risk

Explains the principal roles for board of directors and senior leaders when establishing an operational risk governance program. Identifies the importance of effective challege by the board, risk culture and appetite, three lines of defense, and methods for measuring operational losses, and definition of economic capital. Covers the criteria for key risk indicator (KRI) selection.

After completing this course, students will be able to:

- Describe the principles of effective operational risk governance and the roles of the board and senior management in overseeing operational risk programs
- Identify the elements of an effective operational risk governance program
- Describe the three lines of defense approach and its role in establishing effective management and oversigh of operational risk across the organization

- Identify the methods used in measuring operational risk
- Describe criteria for key risk indicator (KRI) selection and best practices in monitoring and reporting operational risk

Payments and Settlements

Covers specific areas of payment and settlement risk management and effecitvely managing common types of issues. Addresses common challenges with exception items, closed accounts, restricted accounts, reclamations, garnishments, and seizure orders. Describes areas found to be of higher risk while managing payment returns involving various mobile channels, ACH, wires and others.

After completing this course, students will be able to:

- Identify common risks in payments and settlements
- Describe payments and settlement risk controls and available resources
- Describe common settlement issues and how to manage them
- Explain guidelines for managing payment returns

Physical Security

Explores elements of physical security planning and components for an effective physical security plan to improve the bank's prevention and detection strategy. Addresses cameras, lighting, access control, security design, and vendor risk. Covers areas to review when developing a plan for insider fraud and other manmade threats, like bank robberies.

After completing this course, students will be able to:

- Explain the care of duty owed to customers and employees
- Identify the key components of physical security
- Describe the role of the security plan and resources available to assist with establishing an emergency operations plan (EOP)
- Identify issues to consider when planning for threats

Regulatory Exam Management

Focuses on the regulatory examination process and keys for administering the exam process to ensure success. Describes the role and examination approach for different regulatory agencies, establishing responsibilities for bank employees and reducing the impact on bank operations. Covers responding to unfavorable exam results, appeals process and viewing the relationship as a partnership.

After completing this course, students will be able to:

- Explain bank and regulatory objectives for examinations
- Identify the tools used by regulatory agencies to execute the supervisory process
- Describe fundamental components of exam management from the regulatory perspective
- Describe fundamental components of exam management from the bank perspective
- Identify leading practices for exam management

Risk and Control Self Assessment

Explains the risk and control self assessment (RCSA) process and its role in a bank's risk culture. Convers establishing the primary objectives of the RCSA process, identifying risks and appropriate control environment, determining relative priorities, and the overall purpose and benefits of an RCSA.

After completing this course, students will be able to:

- Define operational risk, identify control frameworks, and describe the purpose and benefits of conducting a risk and control self-assessment (RCSA)
- Identify considerations for effective implementation of the RCSA
- Describe approaches for assessing and prioritizing risks
- Describe methods for managing and controlling risks
- Identify techniques and resources to gather data, perform the RCSA, and monitor and report results

Vendor Risk Management

An overview of the risk considerations associated with the selection, engagement, oversight and termination of vendors by a bank, and a perspective on the current regulatory expectations.

After completing this course, students will be able to:

- Know why financial institutions use third parties and the typical services provided
- Understand typical risk areas and the regulatory content
- Outline the methodology for risk categorization
- Describe the stages in the vendor relationship life cycle
- Identify documentation and record keeping requirements