INTRODUCTION

Welcome

Hello and welcome to *Inside Risk Management*!

This course follows guidelines in WCAG 2.0 Level AA Success Criteria. The elearning version of this course is designed to be accessible to people with disabilities. It adheres to standards based on guidelines originally developed by the Web Accessibility Initiative (WAI), known as the Web Content Accessibility Guidelines (WCAG). WCAG is a global set of guidelines followed around the world.

You may be eligible for Continuing Professional Education credit for this course if you are a CPA licensed in the United States. This course offers 1 CPE credit by the National Association of State Board of Accountancy (NASBA). Refer to the associated CPE information pdf for more information on the continuing education credits for this course.

Accepting risk is a fundamental part of a financial institution's business. Financial institutions cannot avoid risk entirely, and the most successful institutions are those that identify the appropriate levels of risk to assume and put the appropriate measures in place to manage that risk.

In this course, you will look at the different types of risks facing financial institutions, the techniques used to manage these risks and the current risk management challenges facing financial institutions today.

Curriculum Overview

This course is part of the *Inside Financial Services*® training curriculum and focuses on risk management within financial institutions.

The other courses in this curriculum include:

- *Introduction to Financial Services*
- *Inside Retail Banking*
- *Inside Investment Management*
- *Inside Corporate Finance*
- *Inside Transaction Banking*
- *Inside Capital Markets*
- *Inside Financial Services Regulation*
- *Making Money in Financial Services*

Course Objectives

This course is approximately 50 minutes in length and designed for professionals serving the financial services industry.

Upon completing this course, you will be able to:

- Name the risks facing financial institutions
- Identify the techniques and tools used by financial institutions to manage risks
- Recall the current risk management challenges facing financial institutions today
- Recognize important executives responsible for risk management within financial institutions

Course Structure

This program contains eight units in addition to this introduction:

- Market risk
- Credit risk
- Liquidity risk
- Operational risk
- Legal and compliance risk
- Strategic risk
- Enterprise risk management
- Important executives

Throughout the program you will see *Check Your Understanding* exercises that test your comprehension of the material presented.

INTRODUCTION

The specific risks facing a financial institution are driven by its business activities, but the primary risks in the financial services industry include:

- Market risk
- Credit risk
- Liquidity risk
- Operational risk
- Legal and compliance risk
- Strategic risk

Market Risk

Market risk is the risk that changes in market conditions will negatively impact the value of a financial institution's assets or liabilities. Market risk is a relatively broad risk, and financial institutions categorize market risks into three interrelated components:

- Trading risk
- Interest rate risk
- Currency risk

Trading Risk

Trading risk (also referred to as **investment risk** or **position risk**) is the risk that the market value of an investment (or portfolio) will drop.

The highest exposure to trading risk is found at financial institutions with large trading or investment portfolios, including investment banks and commercial banks.

To manage trading risk, financial institutions:

- Establish internal investment policies for traders and asset managers to follow
- Set exposure limits, limiting investments in specific:
  - Markets
  - Industries
  - Geographic regions
- Set stop-loss limits
  - A stop-loss limit is the maximum amount an investment can lose before the investment is liquidated
- Use derivatives to hedge their existing positions
- Use software models to measure their value at risk (VaR)
  - VaR measure the maximum amount of loss expected for an investment portfolio under specific economic and market conditions
  - For example, a portfolio might have a $1 million, one-day VaR with a 95% confidence level
  - This means the institution's model predicts the portfolio will not lose more than $1 million a day 95% of the time

Interest Rate Risk

Interest rate risk is the risk that changes in the interest rate environment will negatively impact a financial institution's profitability.

Interest rate risk impacts financial institutions in two specific ways. First, changes in interest rates have a direct impact on the value of fixed income instruments (such as bonds). As interest rates rise, the market value of fixed income instruments drop. As a result, financial institutions with large fixed income portfolios (including banks) are particularly sensitive to interest rate risk.

Interest rate risk also occurs when there is a mismatch in the duration of a financial institution's assets and liabilities, which is most pronounced in banking. For example, most banks fund long-term assets (such as loans) with short-term liabilities (primarily deposits). This exposes banks to increases in interest rates, which generally causes a bank's interest expense to rise more quickly than its interest income.

Interest rate risk is managed primarily through asset/liability management (covered later in this course).

Currency Risk

Currency risk, also referred to as **foreign exchange (or FX) risk**, is the risk that a financial institution's profitability will be negatively impacted by changes in the exchange rates between different currencies.

Currency risk is created when a financial institution:

- Issues foreign loans
- Gathers foreign deposits
- Invests in foreign securities or foreign subsidiaries
- Buys or sells currency derivatives

Financial institutions manage currency risk by:

- Limiting exposure to specific foreign currencies
- Raising local funds in the same currency as local loans
- Using currency derivatives to hedge against changes in currency rates

Challenges in Market Risk Management

Financial institutions face several challenges related to market risk management, including:

- Complying with the Fundamental Review of the Trading Book (FRTB)
- Overcoming limitations in VaR models
- Leveraging big data, high-performance computing resources, advanced mathematics and artificial intelligence to improve risk analytics
- Managing vast amounts of data

CYU #1 – Market Risk Types

Match each description to the type of market risk by choosing the appropriate risk type from the drop down menu. Then click Submit to see if you are correct.

Trading risk	The risk that the market value of an investment will drop.
Currency risk	The risk that a financial institution's profitability will be negatively impacted by changes in foreign exchange rates.
Interest rate risk	The risk that changes in interest rates will negatively impact a financial institution's profitability.

Credit Risk

Credit risk is the risk a counterparty will be unable to complete a financial transaction as promised.

Financial institutions view credit risk across three different dimensions:

- Default risk
  - Default risk is the risk that a borrower will be unable to repay a loan, resulting in a loan default
  - Default risk is the most common form of credit risk, and it is the largest risk banks face
- Issuer risk
  - Issuer risk is the risk that a bond issuer will be unable to repay its debt when its bonds mature
  - Banks, pension funds and other institutional investors which invest primarily in bonds face high levels of issuer risk
- Counterparty risk
  - Counterparty risk is the risk created when a financial institution enters certain financial contracts, such as repurchase agreements and some over-the-counter (OTC) derivatives transactions
  - In these financial contracts, the financial institution faces the risk that its counterparty to the contract will be unable to complete the transaction as promised

Managing Credit Risk

To manage credit risk, financial institutions:

- Develop written policies and procedures, which typically include:
  - Overall exposure limits for specific loan types, geographic regions and borrowers
  - Legal documentation requirements for loans
  - Internal approval levels for credit officers and credit committees
- Employ statistical modeling and analytics
  - Financial institutions use statistical models to measure and predict the probability of default associated with loan applications
  - In consumer lending, most approval decisions are driven by statistical (or scoring) models which generate individual scores for each loan applicant based on the applicant's credit history, salary and other factors
- Establish loan approval authority levels
  - While many banks have expanded scoring models to small business loans, most commercial loans are still evaluated by individual loan officers or committees with varying levels of approval authority
- Secure assets as collateral for loans (where appropriate)
- Include covenants in loan agreements which limit the use of borrowed funds and/or collateral
- Use a default management (or collections) group to work with delinquent or high-risk customers

Banks also set aside reserves on their balance sheets to absorb future credit losses. These reserves are referred to as the allowance for credit loss (in the US) or impairment (under international accounting standards).

Common terminology used in credit risk management include:

- Delinquent loans, which are loans in which payments are more than 30 days past due
- Delinquency rate, which is the percentage of delinquent loans divided by total loans at a specific point in time
- Non-performing loans, which are loans in which repayment is unlikely (typically including loans 90 or more days past due)
- Charged-off loans, which are loans that management has determined has no likelihood of repayment.
- Charge-off rate (or write-off rate), which is the percentage of loans charged off divided by the total average loans over a period of time

Challenges in Credit Risk Management

In recent years, credit losses have been relatively stable in many markets (such as the US). However, this can change quickly as economic conditions change.

Regardless of the current level of credit losses, financial institutions continue to improve credit risk management by:

- Investing in analytics and artificial intelligence
- Expanding stress test modeling to better understand the impact of adverse economic and market conditions on loan charge-offs
- Focusing more on credit portfolio management in an effort to better understand aggregate credit risk across the institution

CYU #2 – CREDIT RISK MANAGEMENT

What strategies do financial institutions use to improve credit risk management? Select the correct answer.

- Expand stress test modeling
- Employ VaR models
- Comply with FRTB
- Set exposure limits on investments

LIQUIDITY RISK

The simple definition of liquidity risk is the risk of a financial institution not having cash available to meet its obligations, such as funding customer deposit withdrawals.

However, today's definition is a slightly more sophisticated one in which liquidity risk management is defined as "ensuring an institution can meet its contractual obligations and fund growth and business operations through unconstrained access to funding at reasonable market rates."

To manage liquidity risk, financial institutions:

- Hold a percentage of their assets in highly liquid investment securities
    - These securities provide an institution with interest income but can be sold quickly to raise cash if needed
- Use analytics to project their cash flow needs
- Gather deposits to ensure a stable source of funding
- Maintain direct relationships with other financial institutions to raise wholesale funding when needed
- Liquefy assets through loan sales and asset securitizations, if needed

- Perform contingency planning and stress testing to monitor the need for funding in abnormal market conditions

Liquidity risk is an important part of a financial institution's asset/liability management.

Asset/Liability Management

Asset/liability management (ALM) is the proactive management of both sides of a financial institution's balance sheet. ALM involves setting goals for how the institution's balance sheet should look, including setting targets for different types of assets and liabilities.

The ALM function is a balancing act, weighing the exposure to various risks against potential returns. The ALM function is responsible for ensuring the financial institution:

- Gathers sufficient funds to support the institution's business activities
- Allocates these funds to assets with appropriate returns to maximize net interest income
- Maintains appropriate levels of interest rate and liquidity risk

ALM strategy and balance sheet goals are set by a financial institution's Asset/Liability Committee (ALCO). ALCO is composed of senior executives and meets on a regular basis to review positions and adjust strategy as conditions change.

This ALM strategy is then executed by the institution's internal Corporate Treasury group, which has the day-to-day responsibility for ensuring appropriate asset/liability management.

To execute ALM, the Corporate Treasury group:

- Leverages simulation models to analyze the institution's exposure to changes in interest rates
- Uses funds transfer pricing to remove interest rate risk from individual business units and centralize it in the Corporate Treasury group
- Works with business units to set growth and pricing initiatives to ensure the institution is attracting the right types of assets and liabilities needed to meet the institution's ALM goals
- Buys and sells investment securities
- Buys and sells derivatives (such as interest rate swaps)

Challenges in Liquidity Risk Management

Liquidity risk is receiving more attention from financial institutions (and regulators) since the global financial crisis when several financial institutions failed (or almost failed) because of their inability to raise enough funds to meet their current liabilities.

As a result, Basel III guidelines require banks to meet minimum requirements for the:

- Liquidity coverage ratio (LCR)

- Net stable funding ratio (NSFR)

In response to these new ratios (and prudent liquidity risk management), banks are:

- Relying more on deposits as a source of funding
- Maintaining more liquid investment portfolios
- Increasing their use of liquidity risk modeling and stress testing

CYU #3 – Challenges based on Risk

Match the current challenges associated with the risk type by choosing the appropriate risk from the drop down menu. Then click Submit to see if you are correct.

Operational risk	A growing prevalence of cyberattacks is increasing this risk.
Credit risk	Financial institutions in certain markets are struggling to manage this risk as non-performing loans continue to rise.
Liquidity risk	Financial institutions are relying more on deposits as a source of funding to meet new requirements related to managing this risk.

Operational Risk

Operational risk is the risk of direct or indirect financial losses caused by a breakdown in a financial institution's operations. Operational risk encompasses a wide variety of risks, including:

- Legal and compliance risk (covered later in this course)
- Information security and cybersecurity (covered later in this course)
- Fraud risk (covered later in this course)
- Reputational risk, which is the risk of financial losses arising from an adverse perception of a financial institution by customers, investors and/or other stakeholders

Operational risk is created by factors such as:

- Inadequate internal controls, policies or procedures

- Systems failures or network outages
- Internal and external fraud
- Human error
- External events, such as natural catastrophes or terrorist attacks

Some examples of operational risk include:

- Transferring funds into the wrong account because of a data entry error
- Allowing a hacker to access customer information
- Lacking the ability to process customer transactions because a network is damaged by an earthquake
- Failing to prevent illegal sales practices

Poor operational risk management can result in:

- Increased expenses associated with the high costs of resolving errors
- Higher fraud losses
- Lower customer retention resulting from poor customer service
- Regulatory sanctions

Operational risk is receiving more attention now than it has in the past, driven by:

- Several highly public examples of operational risk failures in recent years
- Greater scrutiny by regulators
- Increasing reliance on technology across the financial services industry
- A growing use of outsourcing and third parties

Managing Operational Risk

Traditional operational risk management includes:

- Establishing detailed operating procedures and policies
- Monitoring internal activity through an institution's Compliance and Internal Audit groups
- Creating disaster recovery and business continuity plans
- Using insurance to mitigate losses

In recent years, financial institutions have begun to enhance the sophistication of their operational risk management. This is driven by the increased focus on operational risk and the desire to elevate operational risk management to a "science" or "discipline" (much as financial institutions treat credit, market and liquidity risk management today).

This increased sophistication includes:

- Establishing internal governance for managing operational risk
- Building internal loss event databases to track and analyze operational risk exposures

- Developing operational risk analytics
- Integrating operational risk management into day-to-day business activities

Information Security

Information security is an important part of operational risk management. The goal of information security (also referred to as data security) is to protect information held by a financial institution, ranging from sensitive customer information (such as account numbers and personally identifiable information) to the institution's intellectual property related to products and strategies.

Financial institutions face many threats to their information security, including:

- The theft of physical assets, such as data tapes and employee laptops
- Internal threats, ranging from:
    - Staff who intentionally steal customer financial records or trade secrets to…
    - …Careless employees who unintentionally send unencrypted, sensitive customer information through emails or text messages
- External threats, including hacking attempts in which criminals attempt to access internal systems and information
- Inadequate customer protection
    - Criminals often focus their external attacks on the weakest link… customers
    - Common methods for attacking customers include phishing attacks in which criminals masquerade as actual financial institutions to trick customers into providing sensitive information
    - Criminals also use malware such as spyware, trojans and botnets to collect and transmit account details, passwords and other sensitive customer information
    - Once criminals capture this data, they use it to perform identity fraud

Cybersecurity

Cybersecurity overlaps with information security. Cybersecurity includes protecting information a financial institution holds in electronic form (which is also part of information security).

In addition, cybersecurity also includes defending a financial institution from other types of cyberattacks that are not designed to steal internal information. Rather, these attacks are designed to damage or disrupt a financial institution's operations.

Common types of these cyberattacks include:

- Distributed denial of service (DDoS) attacks in which attackers attempt to saturate an institution's website or systems with external communications requests, making it impossible for the institution to respond to legitimate traffic in a timely manner
- Ransomware attacks in which malicious software infiltrates a financial institution's computer networks and then encrypts and denies access to data until a ransom is paid

To improve information security and cybersecurity, financial institutions are:

- Establishing Chief Security Officers to oversee information security and cybersecurity efforts
- Developing security standards for external partners, suppliers and vendors
- Improving user authentication systems, including the use of multi-factor authentication and biometrics
- Investing in a wide array of related technology and services, including predictive analytics, artificial intelligence , identity and access management as well as network and endpoint security

Fraud Risk

Financial institutions face several different types of fraud, including:

- Application fraud
- Payments fraud
- Card fraud

Application fraud (also known as **loan application fraud**) involves fraudsters deliberately providing false information to receive a loan they would not otherwise receive. Financial institutions manage application fraud by ensuring appropriate account opening processes are in place. Information security is also an important tool in preventing application fraud, since application fraud is often linked to identity theft.

Payments fraud involves criminals attempting to illegally transfer funds through various payment channels, including card payments and wire transfers. Since these activities are also used for money laundering, payments fraud prevention and anti-money laundering efforts are closely linked.

Card fraud is an important subset of payments fraud. There are several different forms of card fraud:

- **Card-present fraud** involves either a counterfeit or stolen card physically presented at the point-of-sale
- **Card-not-present fraud** involves fraud in which a merchant does not review the physical card (such as buying goods over the internet by providing a credit card number)
- **Merchant fraud** involves fraud at the merchant, such as an employee stealing credit card numbers

To manage fraud risk, financial institutions are:

- Leveraging predictive analytics, artificial intelligence and natural language processing to improve fraud analytics
- Implementing more advanced user authentication schemes that require multi-factor authentication and biometrics
- Centralizing fraud operations across product lines

- Increasing security requirements for merchants and payment processors

Legal and Compliance Risk

Legal and compliance risk is the risk that:

- A financial institution does not comply with an existing law, regulation or contract
- Changes in laws or regulations will make an existing activity of a financial institution illegal or non-compliant

Legal and compliance risk (also referred to as **regulatory risk**) exposes financial institutions to:

- Fines, penalties and punitive damages from regulators
- Monetary settlements with regulators, customers, investors and others
- Reputational risk

Legal and compliance risk has increased in recent years as industry regulators and lawmakers have increased regulation of the financial services industry.

Political risk is related to legal and compliance risk.

Strategic Risk

Strategic risk refers to risks that affect or are created by a financial institution's strategy or business model. Examples of strategic risk include:

- Industry disruption created by:
  - Changes in technology such as big data, artificial intelligence, blockchain and voice computing
  - New competitors, such as fintech firms and large consumer technology companies
- Pandemics, such as Covid-19
- Geopolitical risks, such as:
  - Changes in political leadership
  - Armed conflicts
  - Terrorism
- Economic changes
- Merger and acquisition activity

- Regulatory changes

To manage strategic risk, financial institutions are increasingly integrating strategic risk analysis into their business strategy and planning processes.

ENTERPRISE RISK MANAGEMENT

Enterprise risk management (ERM) is the coordinated management of multiple risks across a financial institution.

Historically, financial institutions have had different internal groups responsible for each type of risk. These groups have used different definitions of risk, control procedures and analytical models based on different assumptions and underlying data sets.

To remove the inaccuracies and inefficiencies associated with this approach, financial institutions are turning to ERM to:

- Standardize risk management by:
  - Creating common views of how risk is defined, assessed and managed
  - Building risk calculations based on a consistent, enterprise-wide risk data set
  - Improving collaboration between internal risk groups
- Identify overall exposure across multiple risks
- Understand and manage the correlation between different types of risk
- Lower the operational costs associated with risk management
- Comply with regulations related to risk-based capital and stress testing

To improve enterprise risk management, financial institutions are:

- Expanding the authority of Chief Risk Officers
- Standardizing risk management within specific risk types
- Integrating market, credit and liquidity risk management
- Improving data management

CYU #5 – ERM DEFINITION

What strategy are financial institutions using to enhance enterprise risk management? Select the correct answer.

- Improving data management
- Shifting authority away from Chief Risk Officers
- Increasing operational costs

- Creating risk approaches based on lines of business

Important Executives

In this section, we will take a look at the important executives and internal groups responsible for risk management within a financial institution.

Global Risk Committee

The Global Risk Committee has overall responsibility for a financial institution's market risk management. In some institutions, this Committee also has responsibility for operational risk management and/or enterprise risk management.

This committee is composed of members of the Board of Directors and/or senior risk management executives, and the committee reports directly to the Board. The Chief Risk Officer often serves as the chairperson for the Global Risk Committee.

Chief Risk Officer

The Chief Risk Officer (CRO) is responsible for a financial institution's day-to-day market risk management. In some institutions, the Chief Risk Officer also has responsibility for credit risk management, operational risk management and/or other areas of risk management.

The Chief Risk Officer heads the Risk Management department. Most Chief Risk Officers are growing in influence within their organizations as financial institutions look to improve risk governance and standardize risk management. In some financial institutions, the CRO is considered a peer of the CEO and CFO as the most important senior executives.

Asset/Liability Committee

The Asset/Liability Committee (ALCO) is responsible for developing an institution's asset/liability management strategy and policies.

This committee is composed of members of the Board of Directors and senior executives within the financial institution, and it meets on a regular basis to review the institution’s positions and adjust strategy as conditions change.

Corporate Treasurer

The primary responsibility of a financial institution's Corporate Treasurer is the day-to-day execution of the asset/liability management strategy set by ALCO.

In addition, the Corporate Treasurer is also responsible for:

- Managing the institution's cash flow
- Raising debt by issuing bonds and/or securitizing assets
- Hedging interest rate risk and currency risk
- Allocating capital to internal groups
- Setting internal transfer prices

The Corporate Treasurer usually reports to the institution's Chief Financial Officer.

Credit Risk Committee

The Credit Risk Committee (or Credit Committee) has overall responsibility for an institution's credit risk management, including approving policies and procedures and setting loan approval authority levels.

This committee is composed of members of the Board of Directors and/or senior executives from various business units, and it reports directly to the Board of Directors. This committee is headed by the Chief Credit Officer.

Chief Credit Officer

The Chief Credit Officer is responsible for the financial institution's day-to-day credit risk management.

In many financial institutions, there is a single Chief Credit Officer who heads the Credit Risk Committee and the Credit Department. In other financial institutions there are Chief Credit Officers within each line of business, and these Chief Credit Officers report to the Chief Risk Officer.

SVP, Operational Risk Management

Most financial institutions have established Operational Risk executives responsible for improving operational risk management.

However, operational risk management is an evolving discipline within financial institutions, so the reporting lines can vary:

- In some institutions, this executive is considered the Chief Operational Risk Officer (CORO) and reports to a Board-level Operational Risk Committee
- In other institutions, this executive reports to the Chief Risk Officer

Chief Security Officer

Most large financial institutions have a Chief Security Officer or Chief Information Security Officer responsible for the institution's information and cybersecurity.

The reporting lines for CSOs vary:

- In some institutions, the CSO reports to the Chief Information Officer or Chief Technology Officer
- In some institutions, the CSO reports to the Chief Risk Officer
- Given the increased focus on information and cybersecurity, CSOs in some institutions report directly to the CEO and/or Board of Directors (elevating them to a peer of the CIO)

CYU #6 – ALCO

Who has primary responsibility for developing a financial institution's asset/liability management strategy and policies? Select the best answer.

- Asset/Liability Committee **[correct]**
- Chief Risk Officer
- Credit Risk Committee
- Corporate Treasurer

FINAL TEST

To successfully complete this course, you must score at least 70% on the test. There are 10 questions in total. When you have answered all the questions in the test, submit it to info@goto-psi.com and it will be graded. Good luck!

Question #1

Which executive committee is responsible for a financial institution's market risk management? Select the best answer.

Global Risk Committee

Asset/Liability Committee

Credit Risk Committee

Corporate Governance Committee

Question #2

What software model measures the maximum amount of loss expected for an investment portfolio under specific economic and market conditions? Select the best answer.

Variable risk (VaR) models

Value at risk (VaR) models

Mark to market (m2m) models

Measure to market (m2M) models

Question #3

Which financial institution is likely to have the highest amount of trading risk? Select the best answer.

Clearing agent

Finance company

Investment bank

Reinsurance company

Question #4

Which risk is often the responsibility of a financial institution's Chief Risk Officer? Select the best answer.

Legal and compliance risk

Trading risk

Liquidity risk

Interest rate risk

Question #5

What are some of the challenges facing financial institutions today as they manage information security threats? Select all that apply.

Hacking attempts

Inadequate customer protection

Staff stealing consumer records

Establishing operating policies

Question #6

What is the risk that a financial institution does not comply with an existing law or regulation? Select the correct answer.

Enterprise risk

Information risk

Legal and compliance risk

Strategic risk

Question #7

Which risk is defined as the risk that a counterparty will be unable to complete a financial transaction as promised? Select the best answer.

Operational risk

Market risk

Liquidity risk

Credit risk

Question #8

Which tool is used to manage liquidity risk within a financial institution? Select the correct answer.

Network security software

ALM simulation models

Credit derivatives

Insurance policies

Question #9

Which are some of the challenges related to the management of market risk? Select all that apply.

Reducing stress test modeling

Complying with the Fundamental Review of the Trading Book

Employing VaR models

Managing vast amounts of data

Question #10

Which activity is typically the responsibility of the Corporate Treasurer? Select the best answer.

Managing the institution's market risk

Improving operational risk management

Hedging interest rate risk and currency risk

Managing the institution's day-to-day credit risk