STUDY MATERIAL FOR B.COM BANKING & FINANCE

FINANCIAL RISK MANAGEMENT

SEMESTER – VI

ACADEMIC YEAR 2025-26

PREPARED BY

COMMERCE DEPARTMENT

INDEX

FINANCIAL RISK MANAGEMENT

Unit-I: Principles of Risk Management:

Introduction to Risk Business, specific Risks In Financial Services, External Sources Of Risk and their potential impact in a business: economic, political, competitive environment, social and market forces, technological including cyber security, shocks and natural events, external stakeholders and third parties.

UNIT- II: International Risk Regulation:

The bank for international settlements, Roles of the Bank for international settlements, Basel Regulatory Capital, international guidelines and supervisory standards established by the Basel Committee, Capital Adequacy Assessment Process (ICAAP), principles of home-host state regulation, Regulatory Risk, differences between statutory and principles-based approaches to financial regulation.

UNIT-III: Operational Risk and Credit Risk

Definitions of Operational Risk according to the Basel Committee on Banking Supervision, Basel operational risk event types. Operational Risk Framework: Identification, measurement, management and control, management information, monitoring, escalation, remediation. Operational Risk Identification, Operational Risk Assessment and Measurement, Managing operational risk. Credit Risk: Identification of credit risk: understand the key components of credit risk and how they arise. Credit risk management: techniques for measuring credit risk, credit risk management: sound practice features of an effective, credit risk management function, reporting and escalation tools of credit risk management, Basel key stages of credit risk policy development.

UNIT-IV: Market Risk & Liquidity Risk

Identification of Liquidity Risk: market, investment and operational risk. Measurement of Liquidity Risk: funding Liquidity Risk analysis: liquidity gap analysis, stress testing, expected future funding requirement.

UNIT-V: Enterprise wide risk management and risk reporting

Enterprise wide risk management (EWRM) Risk management committee, risk management department, risk based internal audit. Risk reporting: Accounting tax & Legal issues in risk management, Indian accounting standards: IAS 32 financial instrument: Presentation, IAS 39 financial instrument: Recognition & measurement, international financial reporting standards: IFRS 7 Financial instrument: Disclosure, IFRS 9 Financial instrument, financial accounting standard board statement (SFAS): FAS133 Accounting for derivative instruments and Hedging Activities, FAS 138 An Amendment to SFAS133.

UNIT - I

PRINCIPLES OF RISK MANAGEMENT

INTRODUCTION TO RISK BUSINESS:

"Risk in Business" refers to the possibility of experiencing negative outcomes or losses when engaging in business activities. When running a business, there are various uncertainties and potential hazards that can affect its operations and financial performance. These uncertainties could arise from factors such as changes in market conditions, economic fluctuations, competition, natural disasters, and regulatory changes. Understanding and managing risk is crucial for businesses to make informed decisions and protect themselves from potential harm. Businesses typically face different types of risks, including financial risk (related to investments and financing), operational risk (concerning day-to-day activities), strategic risk (associated with long-term planning), and compliance risk (related to adhering to laws and regulations).

Specific Risks in Financial Services:

1. Specific risks in financial services refer to potential threats or uncertainties that are unique to the financial industry.
2. Credit risk is the possibility of borrowers failing to repay their loans, leading to financial losses for the lender.
3. Market risk arises from the potential for financial losses due to changes in market conditions, such as interest rates, exchange rates, and stock prices.
4. Liquidity risk is the risk of not being able to meet short-term financial obligations due to a lack of liquid assets or market access.
5. Operational risk involves the risk of loss resulting from inadequate or failed internal processes, systems, people, or external events.

Risks in Financial Services:

Risk in Banking

Traditionally, risk management in banking has been related to credit risk. Banks make loans to their customers and earn an income on the interest paid on these loans. However, if that customer should default on their loan repayments, then the bank will make a loss.

Risk mitigation in banks has included understanding a customer before a loan is made, managing any issues with repayment, and putting aside provisions for any loans which may be at an increased danger of default.

Risk in Insurance

The business of insurance is one in which the insurer undertakes to provide a guarantee of compensation for a specified event such as damage to an asset, illness, or death, in return for

payment of a specified premium. However, if the premium does not cover the compensation to customers, then the insurance firm may make a loss.

Risk mitigation in insurance has included applying mathematical and statistical methods to assess risk. However, as premiums are invested in assets to allow additional income, market risk has become a part of this industry. Market risk includes the possibility of a loss or profit from a movement in the financial markets.

Risks in Funds

Investors have long invested in funds to secure a return on their investments. In turn, the fund manager provides this return without losing the funds being invested.

Risk management in funds has traditionally been around market risk, but with an increasingly complex ecosystem, operational risk is now becoming a desired skill.

Risk

Risk provides the basis for opportunity. The terms risk and exposure have subtle differences in their meaning. Risk refers to the probability of loss,

While exposure is the possibility of loss, although they are often used interchangeably. Risk arises as a result of exposure.

Exposure to financial markets affects most organizations, either directly or indirectly. When an organization has financial market exposure, there is a possibility of loss but also an opportunity for gain or profit. Financial market exposure may provide strategic or competitive benefits.

Risk is the likelihood of losses resulting from events such as changes in market prices. Events with a low probability of occurring, but that may result in a high loss, are particularly troublesome because they are often not anticipated. Put another way, risk is the probable variability of returns.

Financial Risk

Financial risk arises through countless transactions of a financial nature, including sales and purchases, investments and loans, and various other business activities. It can arise as a result of legal transactions, new projects, mergers and acquisitions, debt financing, the energy component of costs, or through the activities of management, stakeholders, competitors, foreign governments, or weather.

When financial prices change dramatically, it can increase costs, reduce revenues, or otherwise adversely impact the profitability of an organization. Financial fluctuations may make it more difficult to plan and budget, price goods and services, and allocate capital.

There are three main sources of financial risk:

1. Financial risks arising from an organization’s exposure to changes in market prices, such as interest rates, exchange rates, and commodity prices

2. Financial risks arising from the actions of, and transactions with, other organizations such as vendors, customers, and counterparties in derivatives transactions

3. Financial risks resulting from internal actions or failures of the organization, particularly people, processes, and systems

These are discussed in more detail in subsequent chapters.

Financial Risk Management

Financial risk management is a process to deal with the uncertainties resulting from financial markets. It involves assessing the financial risks facing an organization and developing management strategies consistent with internal priorities and policies. Addressing financial risks proactively may provide an organization with a competitive advantage. It also ensures that management, operational staff, stakeholders, and the board of directors are in agreement on key issues of risk.

Managing financial risk necessitates making organizational decisions about risks that are acceptable versus those that are not. The passive strategy of taking no action is the acceptance of all risks by default.

Organizations manage financial risk using a variety of strategies and products. It is important to understand how these products and strategies work to reduce risk within the context of the organization's risk tolerance and objectives.

Strategies for risk management often involve derivatives. Derivatives are traded widely among financial institutions and on organized exchanges. The value of derivatives contracts, such as futures, forwards, options, and swaps, is derived from the price of the underlying asset. Derivatives trade on interest rates, exchange rates, commodities, equity and fixed income securities, credit, and even weather.

The products and strategies used by market participants to manage financial risk are the same ones used by speculators to increase leverage and risk. Although it can be argued that widespread use of derivatives increases risk, the existence of derivatives enables those who wish to reduce risk to pass it along to those who seek risk and its associated opportunities.

The ability to estimate the likelihood of a financial loss is highly desirable. However, standard theories of probability often fail in the analysis of financial markets. Risks usually do not exist in isolation, and the interactions of several exposures may have to be considered in developing an understanding of how financial risk arises. Sometimes, these interactions are difficult to forecast, since they ultimately depend on human behaviour. The process of financial risk management is an ongoing one. Strategies need to be implemented and refined as the market and requirements change. Refinements may reflect changing expectations about market rates, changes to the business environment, or changing international political conditions, for example. In general, the process can be summarized as follows:

Identification and Evaluation of Risk

- Identify and prioritize key financial risks.
- Determine an appropriate level of risk tolerance.
- Implement risk management strategy in accordance with policy.
- Measure, report, monitor, and refine as needed.

External Sources of Risk:

1. Economic Risks

These risks stem from changes in the broader economic environment and affect a company's financial stability and growth prospects.

- **Recessions/Depressions:** Periods of economic contraction reduce consumer spending and demand for goods and services.
- **Inflation/Deflation:** High inflation increases operational costs (raw materials, labour), while deflation can lead to falling prices and reduced profit margins.
- **Interest Rate Fluctuations:** Changes in interest rates affect borrowing costs for capital expenditures and impact consumer purchasing power (e.g., mortgages, loans).
- **Exchange Rate Volatility:** For businesses operating internationally, currency fluctuations can affect the cost of imports and the profitability of exports.
- **Unemployment Rates:** High unemployment reduces the available talent pool and consumer purchasing power.

2. Political Risks

Political risks arise from government actions, policies, and stability, which can create uncertainty for businesses.

- **Changes in Laws and Regulations:** New laws regarding taxation, labour, trade, or industry standards can increase compliance costs or restrict operations.
- **Political Instability and Conflict:** Events like coups, terrorism, civil unrest, or wars can disrupt supply chains, damage property, and create an unsafe business environment.
- **Trade Barriers and Sanctions:** Tariffs, quotas, and economic sanctions imposed by governments can limit market access and increase the cost of doing business internationally.
- **Nationalization or Expropriation:** The risk of a government taking control of privately owned assets, often with little or no compensation.

3. Environmental Risks

These risks are related to the natural world, climate change, and environmental regulations, impacting operations and reputation.

- **Climate Change and Natural Disasters:** Events such as floods, droughts, hurricanes, and wildfires can cause property damage, disrupt supply chains, and displace workers.
- **Resource Scarcity:** Depletion of natural resources (e.g., water, rare earth minerals) can increase material costs and production challenges.
- **Regulatory Changes:** Stricter environmental protection laws and carbon emissions regulations may require significant investment in new technology or changes in operational practices.
- **Reputational Damage:** Failure to adhere to environmental sustainability standards can lead to boycotts and loss of consumer trust.

4. Social Risks

Social risks involve shifts in societal values, public sentiment, and demographic trends that can affect a company's relationship with its employees, customers, and communities.

- **Shifting Consumer Preferences:** Changes in what customers value (e.g., demand for ethical sourcing, healthy products) can make existing products or business models obsolete.
- **Labour Relations and Strikes:** Disputes with labour unions or employee dissatisfaction can lead to work stoppages, increased labour costs, and operational disruptions.
- **Demographic Changes:** An aging population or changes in birth rates can affect both the available workforce and the target consumer base.
- **Public Scrutiny and Activism:** Social movements and negative publicity can force changes in business practices or lead to boycotts and regulatory action.

5. Market Forces Risks

These risks stem from the competitive landscape, supply and demand dynamics, and overall market changes.

- **Competition:** New entrants, innovative products from rivals, or aggressive pricing strategies can erode market share and profitability.
- **Supply Chain Disruptions:** Events affecting key suppliers (e.g., factory fires, port strikes, geopolitical issues) can interrupt the flow of goods and raw materials.
- **Technological Disruption:** Rapid technological advances can create new business models that disrupt existing industries or render current technology obsolete.

- **Changes in Demand:** Unexpected shifts in the demand for a product or service, often driven by trends, economic shifts, or social changes, can lead to excess inventory or shortages.

Types of Business Risk:

Strategic Risk

Strategic risk arises when a business does not operate according to its business model or plan. When a company does not operate according to its business model, its strategy becomes less effective over time, and the company may struggle to reach its defined goals.

For example, imagine ABC Store is a big box store that strategically positions itself as a low-cost provider for working-class shoppers. Its main competitor is XYZ Store, which is seen as a destination for more middle-class consumers. However, if XYZ decides to undercut ABC's prices, this becomes a strategic risk for ABC.

Compliance Risk

The second form of business risk is compliance risk, sometimes known as regulatory risk. Compliance risk primarily arises in industries and sectors that are highly regulated. For example, in the wine industry, there is a three-tier system of distribution that requires wholesalers in the United States to sell wine to a retailer, which then sells it to consumers. This system prohibits wineries from selling their products directly to retail stores in some states.

However, many U.S. states do not have this type of distribution system; compliance risk arises when a brand fails to understand the individual requirements of the state in which it is operating. In this situation, a brand risks becoming noncompliant with state-specific distribution laws and may face fines or other legal action.12

Operational Risk

The third type of business risk is operational risk. This risk arises from within the corporation, especially when the day-to-day operations of a company fail to perform.

For example, in 2012, the multinational bank HSBC faced a high degree of operational risk and, as a result, incurred a large fine from the U.S. Department of Justice when its internal anti-money laundering (AML) operations team was unable to adequately stop money laundering in Mexico.3

Reputational Risk

Anytime a company's reputation is ruined, either by an event that was the result of a previous business risk or by a different occurrence, it runs the risk of losing customers and its brand loyalty suffering. The reputation of HSBC faltered in the aftermath of the fine it was levied for poor anti-money laundering practices.

Reducing Business Risk

Business risk cannot be entirely avoided because it is unpredictable. However, there are many strategies that businesses employ to cut back the impact of all types of business risk, including strategic, compliance, operational, and reputational risk.

The first step that brands typically take is to identify all sources of risk in their business plan. These aren't just external risks—they may also come from within the business itself. Taking action to cut back the risks as soon as they present themselves is key. Management should come up with a plan to deal with any identifiable risks before they become too great.

Finally, most companies adopt a risk management strategy. This can be done either before the business begins operations or after it experiences a setback. Ideally, a risk management strategy will help the company be better prepared to deal with risks as they present themselves. The plan should have tested ideas and procedures in place in case risk presents itself.

Once the management of a company has come up with a plan to deal with the risk, it's important that they take the extra step of documenting everything in case the same situation arises again. After all, business risk isn't static—it tends to repeat itself during the business cycle. By recording what led to risk the first time, as well as the processes used to mitigate it, the business can implement those strategies a second time with greater ease. This reduces the time frame in which unaddressed risk can impact the business, as well as lowering the cost of risk management.

External Economic Risk Sources and Potential Impacts

Economic Downturns/Recession

A general contraction of the economy can significantly decrease consumer spending and demand for products and services. This leads to potential revenue loss, financial strain, and in severe cases, business failure.

Inflation

Rising costs for raw materials, energy, and labor increase operational expenses and put pressure on profit margins. Businesses may have to raise prices to remain profitable, which could impact demand and market share.

Interest Rate Fluctuations

Increases in loan interest rates lead to higher borrowing costs for the business, affecting the expense of short-term and long-term debt. This limits access to capital for growth and operational needs and can increase the risk of a debt crisis if not managed properly.

Exchange Rate Volatility (Currency Risk)

Fluctuations in foreign currency exchange rates impact businesses engaged in international trade. A strong local currency makes exports more expensive and imports cheaper, potentially reducing export sales and increasing costs for imported inputs.

Changes in Demand Conditions

Shifts in consumer preferences, demographic trends, and market fads can alter demand for specific products or services. This can lead to decreased sales volumes, overstock of unwanted inventory, and the need for costly product development or strategic shifts to stay relevant.

Sudden Changes in Input Prices

Unpredictable price changes for essential raw materials or commodities (like oil or specific agricultural products) directly impact production costs and profit forecasts. Supply chains can be disrupted, requiring rapid adaptation in cost management or supplier diversification.

Changing Competitive Conditions

The entry of new competitors, innovative business models, or aggressive pricing strategies by existing rivals can erode a company's market share and competitive advantage. Businesses must constantly innovate and adapt their strategies to maintain market position.

Types of political risk:

- **Government Policy Changes:** New or altered laws and policies on issues like taxation, trade tariffs, wage levels, and environmental regulations can directly affect a company's costs, revenue, and operational framework.
- **Political Instability:** Civil unrest, protests, war, terrorism, or sudden changes in government through coups can disrupt business operations and create a volatile environment.
- **Changes in International Relations:** Shifts in a country's foreign policy can lead to new sanctions or retaliatory actions, affecting international trade and a company's ability to operate globally.
- **Regulatory Risk:** This is the risk that new or changing regulations will negatively impact a business, such as restrictions on foreign investment or new compliance requirements.

Potential impact on a business:

- **Operational Disruption:** Political instability can lead to supply chain issues, project delays, or interruptions in daily transactions.
- **Financial Losses:** Impacts can include currency devaluations, increased costs from new taxes or regulations, and even the risk of assets being seized by a government (expropriation).
- **Reputational Damage:** A business can suffer negative publicity and damage its reputation if it is perceived to be associated with controversial government actions or policies.
- **Increased Uncertainty:** Political events can create unpredictability in markets, making it harder for businesses to plan for the future and invest.

- **Negative Impact on Labour Force:** Changes in employment laws or labour disputes can affect the workforce and a business's performance levels.

Competitive Environment:

The competitive environment is an external risk where competitors' actions—such as new entrants, changing consumer preferences, or innovative technologies—can negatively impact a business by reducing market share, eroding profits, and forcing strategic changes. This risk threatens a company's stability and growth, requiring it to be agile and innovative to adapt to new market dynamics and maintain its competitive edge.

Potential impacts on a business

- **Market share and profitability:** Intense competition can lead to price wars and reduced margins, potentially causing a business to lose market share.
- **Need for innovation:** The competitive landscape forces companies to constantly innovate to differentiate their products or services and stay ahead of competitors.
- **Strategic challenges:** Emerging competitors and evolving consumer tastes present strategic challenges that can make it difficult to capture market share effectively.
- **Threat of obsolescence:** A company's products or services can become obsolete if competitors introduce disruptive new technologies or business models.
- **Reputational damage:** Negative publicity or a failure to keep up with competitors can damage a company's brand and reputation.

How to manage the risk:

- **Monitor the competition:** Proactively monitor competitor activities, market trends, and consumer preferences to anticipate potential threats.
- **Foster strategic agility:** Develop a flexible and agile strategy that allows for rapid adaptation to market changes and new competitive pressures.
- **Invest in innovation:** Allocate resources to research and development to drive innovation and create a competitive advantage.
- **Enhance customer relationships:** Focus on building strong customer relationships to foster loyalty and create a buffer against competitor actions.
- **Collaborate or acquire:** Consider strategic partnerships, collaborations, or acquisitions to gain market share, acquire new technology, or neutralize threats from competitors.

Social Forces:

Social forces encompass the values, beliefs, customs, and practices of a society, as well as demographic changes and cultural trends that shape consumer behaviour and expectations.

Changing Consumer Preferences and Behaviours: Shifts in social values, such as increased environmental awareness or demand for healthier products, can rapidly alter market demand.

- **Potential Impact:** A failure to adapt products or marketing strategies to these new preferences can lead to a significant loss of market share and revenue (e.g., the shift from gas-guzzling SUVs to hybrid cars due to environmental concerns).
- **Corporate Social Responsibility (CSR) and Ethics:** Consumers and investors increasingly hold companies accountable for their social and ethical performance, including labour practices and environmental footprints.
- **Potential Impact:** Unethical practices or a lack of social responsibility can result in boycotts, negative publicity, reputational damage, and regulatory scrutiny, all of which harm the company's financial performance and long-term viability.
- **Workplace Culture and DEI Issues:** A toxic internal culture or failure to foster diversity, equity, and inclusion (DEI) can become an external risk through social channels.
- **Potential Impact:** This can lead to high employee turnover, low morale, decreased productivity, legal battles, and a damaged reputation that hinders the ability to attract top talent and customers.
- **Demographic Shifts:** Changes in population size, age distribution, and composition affect the labour pool and market demand.
- **Potential Impact:** Businesses may need to adjust their product offerings and marketing to cater to different age groups (e.g., an aging population), or face labor shortages if they do not adapt to the needs of the modern workforce.
- **Social Unrest and Political Instability:** Broader societal issues, such as social unrest or a volatile political landscape, create an unpredictable business environment.
- **Potential Impact:** This can disrupt operations, damage infrastructure, and create policy uncertainties (e.g., changes in tax laws or trade policies) that negatively affect investment and growth prospects.

Market Forces:

Market forces relate to the dynamics of supply, demand, and competition within the marketplace.

- **Competition Conditions:** The intensity of competition is constantly changing due to globalization, new technologies, and emerging competitors.
- **Potential Impact:** New competitors with innovative business models can disrupt established markets, erode market share, and pressure a company's pricing and profit margins, forcing constant innovation to stay ahead.

- **Changes in Demand Conditions:** Fluctuations in the level and nature of demand for products or services are a primary market risk.
- **Potential Impact:** A decrease in demand can lead to overproduction, inventory waste, and reduced revenue streams, while an unexpected surge in demand may stress supply chains and operational capacity.
- **Input Price Volatility:** Sudden and significant changes in the costs of raw materials, energy, or labour.
- **Potential Impact:** This directly impacts production costs and profit margins. Companies with high dependence on foreign inputs are also vulnerable to exchange rate fluctuations, which exacerbate input cost volatility.
- **Economic Conditions:** Macroeconomic factors like inflation rates, interest rates, and overall economic growth directly influence market activity.
- **Potential Impact:** High inflation erodes purchasing power and increases business costs; rising interest rates increase borrowing costs and can curb consumer spending, leading to reduced demand during a recession or economic downturn.
- **Technological Developments:** Rapid advancements can reshape industries and disrupt traditional business models.
- **Potential Impact:** While technology offers opportunities, it also poses the risk of making a company's products, services, or production methods obsolete if they fail to invest in continuous adaptation and innovation.

External Technological Risks:

- **Disruptive Technologies:** Rapid technological advancements (like AI, automation, etc.) by competitors or the market can render a company's existing products, services, or business model obsolete if it fails to adapt, leading to a loss of market share and revenue.
- **Hardware and Software Failures (External):** Malfunctions in third-party vendor systems or widely-used software/hardware can cause widespread operational disruptions. For example, a faulty update to a third-party security software once caused thousands of businesses' systems to crash globally.
- **Third-Party Vendor Vulnerabilities:** Businesses that rely on external suppliers, contractors, or cloud service providers are exposed to risks originating from those partners' security weaknesses. A breach in a vendor's system can directly impact the client company.
- **Lack of Skilled Labour in the Market:** A shortage of skilled IT and cybersecurity professionals in the external labour market can hinder a company's ability to implement robust security measures or manage complex systems effectively.

External Cybersecurity Risks:

- **Malware and Ransomware Attacks:** Malicious software (viruses, worms, Trojans) can infiltrate systems via external sources (e.g., infected websites, email attachments). Ransomware, a prevalent type of malware, encrypts a company's data and systems, demanding payment for their release, leading to significant downtime and financial loss.
- **Phishing and Social Engineering Schemes:** External threat actors use fraudulent messages (email, text, phone calls) to trick employees into revealing sensitive information or downloading malware. These attacks exploit human psychology and are a primary entry point for major breaches.
- **Distributed Denial-of-Service (DDoS) Attacks:** Attackers can overwhelm a company's network or website with a flood of illegitimate traffic, making online services unavailable to legitimate users. This disrupts business operations and can result in significant revenue loss.
- **Zero-Day Exploits:** Hackers can exploit previously unknown software vulnerabilities for which no patch exists yet. These attacks are particularly dangerous because no immediate defines is available to the company.
- **Man-in-the-Middle (MITM) Attacks:** In unsecure networks (e.g., public Wi-Fi), an attacker can intercept communication between two parties, gaining unauthorized access to data in transit.
- **Regulatory Enforcement and Fines:** External government bodies and industry regulators impose strict data privacy and security laws (e.g., GDPR, CCPA). Failure to comply with these external mandates due to a security lapse can result in massive fines and legal action.
- **State-Sponsored Attacks:** Malicious actors backed by hostile nation-states or organized criminal groups may launch sophisticated, long-term attacks (Advanced Persistent Threats) to steal intellectual property or disrupt critical infrastructure.

Potential Impacts on a Business:

The potential impacts of these external technology and cyber security risks are severe and multifaceted:

- **Financial Losses:** Direct costs include regulatory fines, legal fees, investigation and recovery expenses, ransom payments, and potential lawsuits.
- **Operational Disruption:** System failures and cyber-attacks can halt day-to-day operations, leading to unplanned downtime, reduced productivity, and missed business opportunities.

- **Reputational Damage and Loss of Trust:** Publicized data breaches and service disruptions can erode customer and investor confidence, damage the brand's image, and result in a decline in market value and loss of customers.
- **Loss of Intellectual Property:** The theft of trade secrets, customer data, and other sensitive information can result in a significant competitive disadvantage.

Natural Events:

Earthquakes, floods, wildfires, hurricanes, and tsunamis: These events can cause immediate and extensive physical damage to a business's facilities, equipment, and inventory.

- **Pandemics and health crises:** These can lead to labour shortages, government-mandated lockdowns, and significant shifts in consumer behaviour (e.g., a rapid shift to online shopping).
- **Climate Change:** This acts as a risk driver, increasing the frequency and intensity of extreme weather events, which in turn elevates the probability of related business disruptions.

Potential Impacts:

- **Operational Disruption:** Physical damage and infrastructure failure (e.g., damaged roads, ports, and power outages) can bring production to a standstill and impede access to markets.
- **Supply Chain Disruption:** A local disaster can create a "ripple effect" globally if key suppliers are located in the affected area (e.g., a shortage of semiconductors after the 1999 Taiwan earthquake impacted electronics manufacturers worldwide).
- **Financial Loss:** Businesses face significant financial burdens from property damage, lost sales, increased production costs (e.g., due to raw material scarcity or price instability), and potential lawsuits.
- **Labour Shortages:** Injuries, fatalities, or displacement of the workforce can disrupt the entire production schedule and delay recovery efforts.
- **Increased Uncertainty:** A drop in business confidence and increased market volatility can lead investors to postpone decisions, negatively affecting stock market returns and access to credit.

Shocks (Economic, Political, and Technological):

- **Economic Downturns/Crises:** Broader economic shifts, such as inflation, recessions, or financial meltdowns, can cause a drop in consumer spending and make accessing credit more difficult.

- **Political Instability and Regulatory Changes:** Unpredictable shifts in government policies, regulations, trade policies, or the emergence of geopolitical tensions create a volatile business environment and impact long-term planning.
- **Sudden Changes in Input Prices:** Global market dynamics or geopolitical events can cause sudden fluctuations in raw material or energy costs, directly affecting production costs and profit margins.

Potential Impacts:

- **Profitability Issues:** Economic and price shocks directly impact an organization's ability to manage costs and maintain expected profit margins.
- **Strategic Risk:** Rapid, unforeseen changes can make long-term business models irrelevant if the company cannot adapt quickly enough (e.g., the rise of e-commerce impacting traditional retail).
- **Compliance and Legal Issues:** Rapid regulatory changes can make it difficult for multinational firms to remain compliant across different jurisdictions, risking penalties and lawsuits.
- **Reduced Investor Confidence:** Political instability can damage investor confidence, leading to a decrease in foreign direct investment and potentially higher borrowing costs for the affected country and its businesses

External stakeholders

Stakeholder	Potential Risk	Impact on Business
Customers	Changing demands or dissatisfaction, boycotts due to social or environmental concerns	Reduced sales and revenue, damage to brand reputation
Regulators	New laws, enforcement actions, withdrawal of licenses	Increased costs, fines, operational restrictions, or loss of the ability to operate
Trade unions	Strikes or labor disputes	Production stoppages, supply chain disruptions, decreased employee productivity
Local community	Protests, negative publicity, or pressure to change practices	Reputational damage, potential legal challenges, and difficulty with permits or expansion

Third parties

Third Party Type	Potential Risk	Impact on Business
Suppliers	Supply chain failures, delays, or inability to meet quality standards	Production delays, increased costs, and an inability to fulfill customer orders
Service providers	Failure to perform services as contracted, security breaches, or operational failures	Disruption to core operations, data loss, financial penalties, and reputational harm
Cybersecurity vendors	Poor security practices that lead to data breaches, exposing your own company's data	Significant financial losses, legal liability, and severe damage to customer trust
Business partners	Strategic misalignment, or one partner's failure impacting the other	Inability to achieve strategic objectives, financial losses, or damage to reputation

UNIT- II

INTERNATIONAL RISK REGULATION

The bank for international settlements:

The Bank for International Settlements (BIS) is an international financial institution that serves as a bank for central banks, fostering international monetary and financial cooperation. Established in 1930 and headquartered in Basel, Switzerland, the BIS is the oldest international financial institution and provides a forum for central banks to discuss policy, produce research, and act as a prime counterparty in financial transactions.

Role:

The BIS promotes central bank cooperation, provides financial services to its members, conducts economic and monetary research, and acts as an agent for international financial operations.

Membership:

It is owned by 63 member central banks from around the world.

Operations:

The BIS does not provide services to private individuals or corporations, only to its member central banks and other international organizations.

Headquarters:

Its main office is in Basel, Switzerland, with two representative offices in Hong Kong and Mexico City.

Roles of the BIS

A bank for central banks: The BIS provides financial services to its members, such as managing reserve assets and offering short-term money market instruments. It also historically provided liquidity during financial crises.

A forum for cooperation: It facilitates dialogue and cooperation among central banks and financial regulators through meetings and committees. This helps build a common understanding of the global economy and coordinate responses to financial issues.

A centre for research: The BIS conducts and publishes research on monetary and economic topics to improve understanding of international financial markets and policies.

An agent for international agreements: It acts as an agent or trustee in the execution of international financial agreements, such as those related to European monetary cooperation.

A hub for innovation: Through initiatives like the BIS Innovation Hub, it explores new technologies like AI and blockchain to help central banks and the financial system adapt to future challenges.

Basel regulatory capital:

Capital requirements: Banks must maintain a minimum ratio of capital to risk-weighted assets, initially set at 8% in Basel I and still present in Basel III, though with significant changes to its components and the addition of new buffers.

Capital tiers: Capital is divided into tiers based on quality and loss-absorbing capacity.

Tier 1 Capital: The most permanent and highest quality capital, such as common equity.

Tier 2 Capital: Instruments with some shortcomings compared to Tier 1 capital.

Basel III reforms:

The most recent major update, Basel III, introduced several enhancements:

Stronger capital: Focuses on higher-quality forms of capital and requires banks to hold a greater amount of common equity.

Capital buffers: Add new capital buffers, such as the capital conservation buffer, to provide an extra layer of protection against losses during times of stress.

Increased deductions: Includes a wider set of deductions for certain assets like goodwill and deferred tax assets to ensure the quality of the capital base.

Risk-weighted assets: The denominator for the capital ratio. A bank's assets are assigned risk weights based on their riskiness to determine the total amount of risk-weighted assets.

Three-pillar framework: The overall structure of the accords consists of three mutually reinforcing pillars:

Pillar1: Minimum capital requirements.

Pillar2: Supervisory review of a bank's capital adequacy.

Pillar3: Market discipline through enhanced public disclosure.

Basel regulatory capital:

Capital requirements: Banks must maintain a minimum ratio of capital to risk-weighted assets, initially set at 8% in Basel I and still present in Basel III, though with significant changes to its components and the addition of new buffers.

Capital tiers: Capital is divided into tiers based on quality and loss-absorbing capacity.

Tier 1 Capital: The most permanent and highest quality capital, such as common equity.

Tier 2 Capital: Instruments with some shortcomings compared to Tier 1 capital.

Basel III reforms: The most recent major update, Basel III, introduced several enhancements:

Stronger capital: Focuses on higher-quality forms of capital and requires banks to hold a greater amount of common equity.

Capital buffers: Add new capital buffers, such as the capital conservation buffer, to provide an extra layer of protection against losses during times of stress.

Increased deductions: Includes a wider set of deductions for certain assets like goodwill and deferred tax assets to ensure the quality of the capital base.

Risk-weighted assets: The denominator for the capital ratio. A bank's assets are assigned risk weights based on their riskiness to determine the total amount of risk-weighted assets.

Three-pillar framework: The overall structure of the accords consists of three mutually reinforcing pillars:

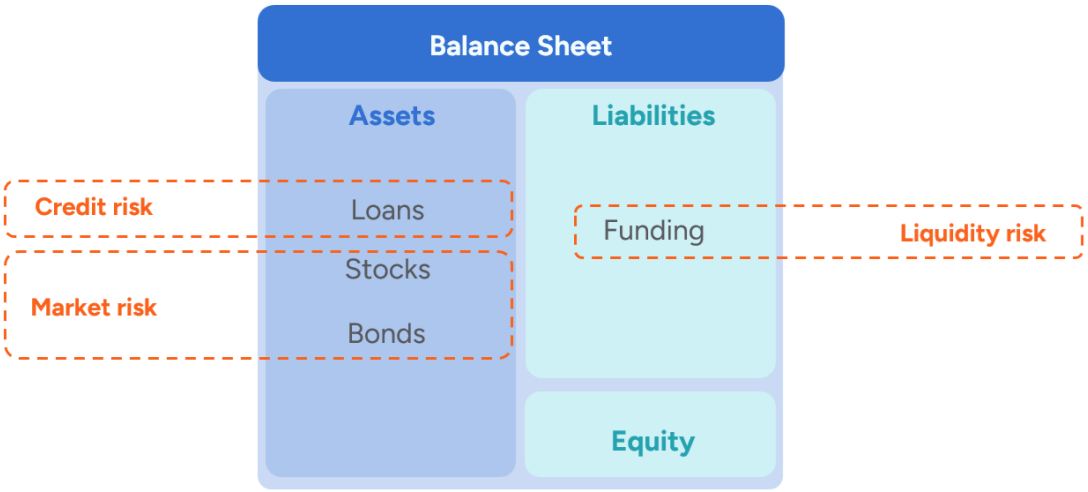
Pillar 1: Minimum capital requirements.

Pillar 2: Supervisory review of a bank's capital adequacy.

Pillar 3: Market discipline through enhanced public disclosure.

Operational Risk under the Basel Framework:

Financial risks for a bank and other financial institutions are those risks that impact the balance sheet directly.



Guideline Methods

This page includes a brief overview of the methods used to develop the fourth edition Prevention and Treatment of Pressure Ulcers/Injuries: Clinical Practice Guideline.

The fourth edition of the International PI Guideline was developed using GRADE methodology, as outlined in detail in the GRADE Handbook. The GRADE approach to guideline development is the gold standard for international guidelines. In brief, the GRADE process includes:

- Establishing clinical questions using a PICO format that focus on a comparison between two interventions (or an intervention and usual care/placebo).
- Conducting PICO searches for studies (Tiers 1, 2 and 3 evidence). The guideline project uses a broad search strategy to scope the full body of PI-related literature, and then a PICO search within that body of evidence (as well as additional PICO searches).
- Conducting risk of bias assessment for individual studies
- Performing the GRADE Certainty of Evidence evaluation
- Completing an Evidence to Decision Framework
- Reaching agreement on a recommendation
- Determining the Strength of Recommendation

Composition of Regulatory Capital:

General

Banks are required to maintain a minimum Pillar1 Capital to Risk-weighted Assets Ratio (CRAR) of 9% on an on-going basis (other than capital conservation buffer and countercyclical capital buffer etc.). The Reserve Bank will take into account the relevant risk factors and the internal capital adequacy assessments of each bank to ensure that the - 10 - capital held by a bank is commensurate with the bank's overall risk profile. This would include, among others, the effectiveness of the bank's risk management systems in identifying, assessing / measuring, monitoring and managing various risks including interest rate risk in the banking book, liquidity risk, concentration risk and residual risk. Accordingly, the Reserve Bank will consider prescribing a higher level of minimum capital ratio for each bank under the Pillar 2 framework on the basis of their respective risk profiles and their risk management systems. Further, in terms of the Pillar 2 requirements, banks are expected to operate at a level well above the minimum requirement. A bank should compute Basel III capital ratios in the following manner:

Common Equity Tier 1 capital ratio = Common Equity Tier 1 Capital /Credit Risk RWA* + Market Risk RWA + Operational Risk RWA

Elements of Regulatory Capital and the Criteria for their Inclusion in the Definition of Regulatory Capital

Components of Capital Total regulatory capital will consist of the sum of the following categories:

(a) Tier 1 Capital (going-concern capital)

(b) Common Equity Tier 1

(c) Additional Tier 1 (ii) Tier 2 Capital (gone-concern capital)

Recognition of Minority Interest (i.e. Non-Controlling Interest) and Other Capital Issued out of Consolidated Subsidiaries That is Held by Third Parties:

Under Basel III, the minority interest is recognised only in cases where there is considerable explicit or implicit assurance that the minority interest which is supporting the risks of the subsidiary would be available to absorb the losses at the consolidated level. Accordingly, the portion of minority interest which supports risks in a subsidiary that is a bank will be included in group's Common Equity Tier 1. Consequently, minority interest in the subsidiaries which are not banks will not be included in the regulatory capital of the group. In other words, the proportion of surplus capital which is attributable to the minority shareholders would be excluded from the group's Common Equity Tier 1 capital. Further, as opposed to Basel II, a need was felt to extend the minority interest treatment to other components of regulatory capital also (i.e. Additional Tier 1 capital and Tier 2 capital). Therefore, under Basel III, the minority interest in relation to other components of regulatory capital will also be recognised.

Regulatory Adjustments / Deductions:

The following paragraphs deal with the regulatory adjustments / deductions which will be applied to regulatory capital both at solo and consolidated level.

1. Goodwill and all Other Intangible Assets

i) Goodwill and all other intangible assets should be deducted from Common Equity Tier 1 capital including any goodwill included in the valuation of significant investments in the capital of banking, financial and insurance entities which are outside the scope of regulatory consolidation. In terms of AS 23 – Accounting for investments in associates, goodwill/capital reserve arising on the acquisition of an associate by an investor should be included in the carrying amount of investment in the associate but should be disclosed separately. Therefore, if the acquisition of equity interest in any associate involves payment which can be attributable to goodwill, this should be deducted from the Common Equity Tier 1 of the bank.

ii) The full amount of the intangible assets is to be deducted net of any associated deferred tax liabilities which would be extinguished if the intangible assets become impaired or derecognized under the relevant accounting standards. For this purpose, the definition of intangible assets would be in accordance with the Indian accounting standards. Operating losses in the current period and those brought forward from previous periods should also be deducted from Common Equity Tier 1 capital.

iii) Application of these rules at consolidated level would mean deduction of any goodwill and other intangible assets from the consolidated Common Equity which is attributed to the Balance Sheets of subsidiaries, in addition to deduction of goodwill and other intangible assets which pertain to the solo bank.

2. Deferred Tax Assets (DTAs)

(i) The DTAs computed as under should be deducted from Common Equity Tier 1 capital:

(a) DTA associated with accumulated losses; and

(b) The DTA (excluding DTA associated with accumulated losses), net of DTL. Where the DTL is in excess of the DTA (excluding DTA associated with accumulated losses), the excess shall neither be adjusted against item (a) nor added to Common Equity Tier 1 capital.

(ii) Application of these rules at consolidated level would mean deduction of DTAs from the consolidated Common Equity which is attributed to the subsidiaries, in addition to deduction of DTAs which pertain to the solo bank.

Cash Flow Hedge Reserve :

i. The amount of the cash flow hedge reserve which relates to the hedging of items that are not fair valued on the balance sheet (including projected cash flows) should be derecognised in the calculation of Common Equity Tier 1. This means that positive amounts should be deducted and negative amounts should be added back. This treatment specifically identifies the element of the cash flow hedge reserve that is to be derecognised for prudential purposes. It removes the element that gives rise to artificial volatility in Common Equity, as in this case the reserve only reflects one half of the picture (the fair value of the derivative, but not the changes in fair value of the hedged future cash flow).

ii. Application of these rules at consolidated level would mean derecognition of cash flow hedge reserve from the consolidated Common Equity which is attributed to the subsidiaries, in addition to derecognition of cash flow hedge reserve pertaining to the solo bank.

Scope of Application of Capital Adequacy Framework:

1. A bank shall comply with the capital adequacy ratio requirements at two levels:

(a) The consolidated (“Group”) level3 capital adequacy ratio requirements, which measure the capital adequacy of a bank based on its capital strength and risk profile after consolidating the assets and liabilities of its subsidiaries / joint ventures / associates etc. except those engaged in insurance and any non-financial activities; and

(b) The standalone (“Solo”) level capital adequacy ratio requirements, which measure the capital adequacy of a bank based on its standalone capital strength and risk profile. Accordingly, overseas operations of a bank through its branches will be covered in both the above scenarios.

2. For the purpose of these guidelines, the subsidiary is an enterprise that is controlled by another enterprise (known as the parent). Banks will follow the definition of ‘control’ as given in the applicable accounting standards.

3. Capital Adequacy at Group / Consolidated Level:

All banking and other financial subsidiaries except subsidiaries engaged in insurance and any non-financial activities (both regulated and unregulated) should be fully consolidated for the purpose of capital adequacy. This would ensure assessment of capital adequacy at the group level, taking into account the risk profile of assets and liabilities of the consolidated subsidiaries.

4 Capital Adequacy at Solo Level:

1. While assessing the capital adequacy of a bank at solo level, all regulatory adjustments indicated in paragraph 4.4 are required to be made. In addition, investments in the capital instruments of the subsidiaries, which are consolidated in the consolidated financial statements of the group, will also have to be deducted from the corresponding capital instruments issued by the bank.

2. In case of any shortfall in the regulatory capital requirements in the unconsolidated entity (e.g. insurance subsidiary), the shortfall shall be fully deducted from the Common Equity Tier 1 capital.

Capital adequacy assessment process (ICAAP):

1. Background:

The Basel capital adequacy framework rests on the following three mutually reinforcing pillars:

Pillar 1: Minimum Capital Requirements - which prescribes a risk-sensitive calculation of capital requirements that, for the first time, explicitly includes operational risk in addition to market and credit risk.

Pillar 2: Supervisory Review Process (SRP) - which envisages the establishment of suitable risk management systems in banks and their review by the supervisory authority.

Pillar 3: Market Discipline - which seeks to achieve increased transparency through expanded disclosure requirements for banks.

2. Conduct of the SREP by the RBI:

Capital helps protect individual banks from insolvency, thereby promoting safety and soundness in the overall banking system. Minimum regulatory capital requirements under Pillar 1 establish a threshold below which a sound bank's regulatory capital must not fall. Regulatory capital ratios permit some comparative analysis of capital adequacy across regulated banking entities because they are based on certain common methodology / assumptions. However, supervisors need to perform a more comprehensive assessment of capital adequacy that considers risks specific to a bank, conducting analyses that go beyond minimum regulatory capital requirements.

3. The Structural Aspects of the ICAAP:

This section outlines the broad parameters of the ICAAP that banks are required to comply with in designing and implementing their ICAAP.

Every bank to have an ICAAP Reckoning that the Basel II framework is applicable to all commercial banks (except the Local Area Banks and the Regional Rural Banks), both at the solo level (global position) as well as at the consolidated level, the ICAAP should be prepared, on a solo basis, at every tier for each banking entity within the banking group, as also at the level of the consolidated bank (i.e., a group of entities where the licensed bank is the controlling entity). This requirement would also apply to the foreign banks which have a branch presence in India and their ICAAP should cover their Indian operations only.

4. Review of the ICAAP Outcomes:

The board of directors shall, at least once a year, assess and document whether the processes relating the ICAAP implemented by the bank successfully achieve the objectives envisaged by the board. The senior management should also receive and review the reports regularly to evaluate the sensitivity of the key assumptions and to assess the validity of the bank's estimated future capital requirements. In the light of such an assessment, appropriate changes in the ICAAP should be instituted to ensure that the underlying objectives are effectively achieved.

5. ICAAP to be an Integral part of the Management and Decision-making Culture:

The ICAAP should from an integral part of the management and decision-making culture of a bank. This integration could range from using the ICAAP to internally allocate capital to various business units, to having it play a role in the individual credit decision process and pricing of products or more general business decisions such as expansion plans and budgets. The integration would also mean that ICAAP should enable the bank management to assess, on an ongoing basis, the risks that are inherent in their activities and material to the institution.

6. The Principle of Proportionality:

The implementation of ICAAP should be guided by the principle of proportionality. Though banks are encouraged to migrate to and adopt progressively sophisticated approaches in designing their ICAAP, the RBI would expect the degree of sophistication adopted in the ICAAP in regard to risk measurement and management to be commensurate with the nature, scope, scale and the degree of complexity in the bank's business operations. The following paragraphs illustratively enumerate the broad approach which could be considered by banks with varying levels of complexity in their operations, in formulating their ICAAP.

7. Regular Independent Review and Validation:

The ICAAP should be subject to regular and independent review through an internal or external audit process, separately from the SREP conducted by the RBI, to ensure that the ICAAP is comprehensive and proportionate to the nature, scope, scale and level of complexity of the

bank's activities so that it accurately reflects the major sources of risk that the bank is exposed to. A bank shall ensure appropriate and effective internal control structures, particularly in regard to the risk management processes, in order to monitor the bank's continued compliance with internal policies and procedures.

8. ICAAP to be a Forward-looking Process:

He ICAAP should be forward looking in nature, and thus, should take into account the expected / estimated future developments such as strategic plans, macro-economic factors, - 121 - etc., including the likely future constraints in the availability and use of capital. As a minimum, the management of a bank shall develop and maintain an appropriate strategy that would ensure that the bank maintains adequate capital commensurate with the nature, scope, scale, complexity and risks inherent in the bank's on-balance-sheet and off-balance sheet activities, and should demonstrate as to how the strategy dovetails with the macroeconomic factors. Thus, banks shall have an explicit, Board-approved capital plan which should spell out the institution's objectives in regard to level of capital, the time horizon for achieving those objectives, and in broad terms, the capital planning process and the allocate responsibilities for that process.

9. ICAAP to be a Risk-based Process:

The adequacy of a bank's capital is a function of its risk profile. Banks shall, therefore, set their capital targets which are consistent with their risk profile and operating environment. As a minimum, a bank shall have in place a sound ICAAP, which shall include all material risk exposures incurred by the bank. There are some types of risks (such as reputation risk and strategic risk) which are less readily quantifiable; for such risks, the focus of the ICAAP should be more on qualitative assessment, risk management and mitigation than on quantification of such risks. Banks' ICAAP document shall clearly indicate for which risks a quantitative measure is considered warranted, and for which risks a qualitative measure is considered to be the correct approach.

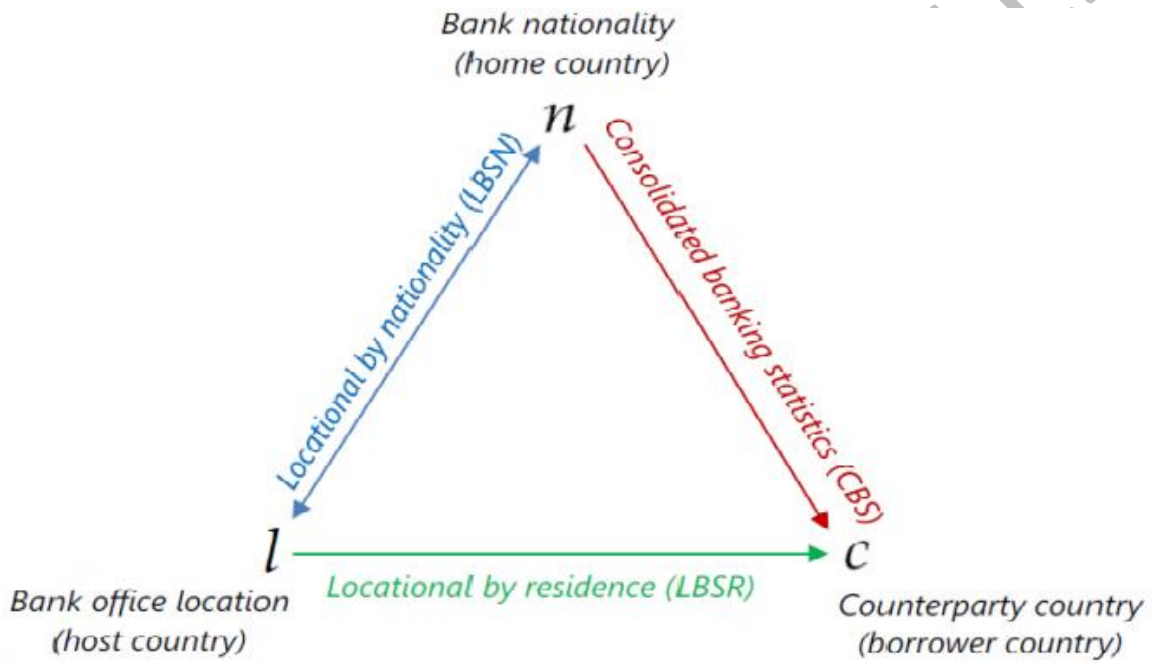
10. ICAAP to Include Stress Tests and Scenario Analyses:

As part of the ICAAP, the management of a bank shall, as a minimum, conduct relevant stress tests periodically, particularly in respect of the bank's material risk exposures, in order to evaluate the potential vulnerability of the bank to some unlikely but plausible events or movements in the market conditions that could have an adverse impact on the bank. The use of stress testing framework can provide a bank's management a better understanding of the bank's likely exposure in extreme circumstances. In this context, the attention is also invited to the RBI circular DBOD.No.BP.BC.101/21.04.103/2006-07 dated June 26, 2007 on stress testing wherein the banks were advised to put in place appropriate stress testing policies and stress test frameworks, incorporating "sensitivity tests" and "scenario tests", for the various risk factors, by September 30, 2007, on a trial / pilot basis and to operationalise formal stress testing frameworks from March 31, 2008. The banks are urged to take necessary measures for implementing an appropriate formal stress testing framework by the date specified which would also meet the stress testing requirements under the ICAAP of the banks.

Principles of home-host state regulation:

Home-host state regulation principles manage cross-border financial oversight, centering on the Home Country Control (HCC) rule (regulators oversee parent groups) and Host Country Control (HCC) safeguards (host supervisors get final say on local subsidiaries), balancing unified group supervision (home) with local stability (host), especially for banks, promoting cooperation, risk sharing, and ensuring capital adequacy across global operations, often through Basel Committee frameworks.

Geographical dimensions of global banking

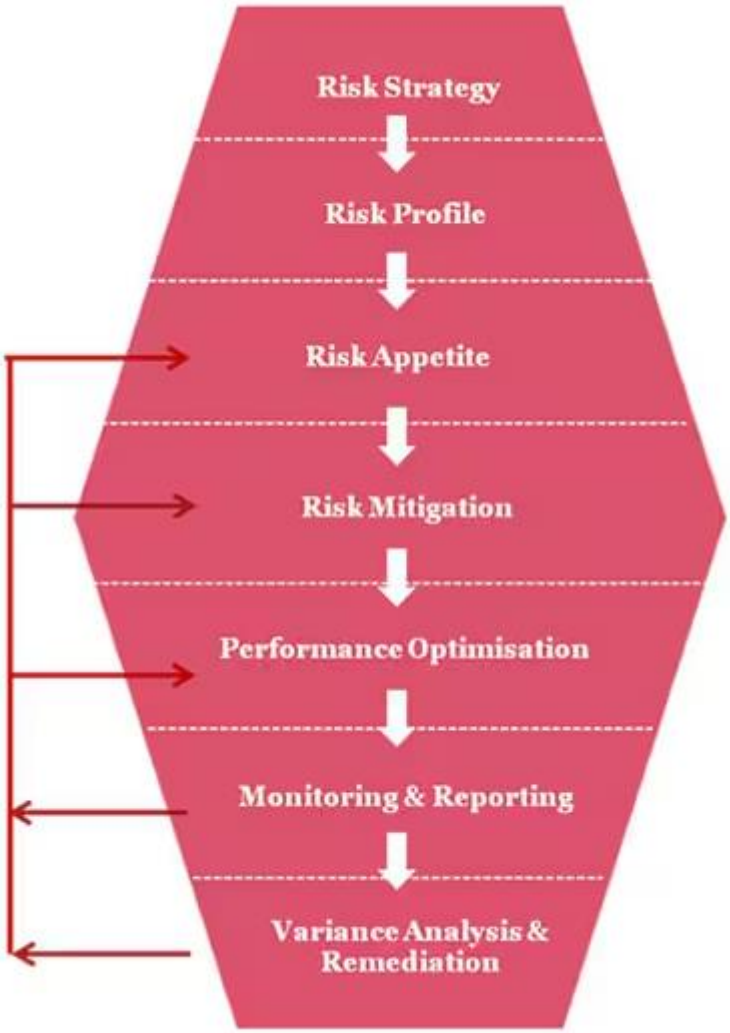


Core Principles Explained:

1. **Home Country Control (HCC):** The home country supervisor (where the parent bank is based) has primary responsibility for the solvency and liquidity of the entire international banking group.
2. **Host Country Control (HCC) Safeguards:** Host countries (where branches/subsidiaries operate) get significant powers to protect their local financial stability, often having the final say on capital requirements for local entities if home/host agreement fails.
3. **Consolidated Supervision:** International banking groups are supervised as a single entity (globally), capturing all domestic and cross-border risks, essential for Basel II/III.
4. **Cooperation & Information Sharing:** Strong communication and shared understanding between home and host supervisors are vital for effective risk management.

5. **Risk Allocation:** Clear mechanisms for allocating risks (like operational risk under Basel II) between home and host jurisdictions are needed.
6. **Subsidiarity:** While the home country leads, host supervisors retain authority for local market integrity and stability, preventing regulatory arbitrage.

Risk Framework



Regulatory Risk:

Regulatory risk is the risk that a change in regulations or legislation will affect a security, company, or industry. Companies must abide by regulations set by governing bodies that oversee their industry. Therefore, any change in regulations can cause a rippling effect across an industry.

Regulations can increase costs of operations, introduce legal and administrative hurdles, and sometimes even restrict a company from doing business.

Regulatory Risk from Regulatory Changes

Governmental and regulatory bodies often enact new regulations or update old ones. Here are some examples of regulatory changes that may affect companies or industries:

1. Tariffs and trade policies

Changes to international trade policies may affect companies that regularly export and import goods. They also affect investors that engage in foreign direct investments.

For example, conducting business in China is often restricted by trade policies. Western businesses are only allowed to operate in China through partnerships and joint ventures.

Investing in Chinese stocks is also restricted. Foreign investors have historically only been allowed to invest in 'B shares' that are denoted in USD. 'A shares', which are denoted in RMB, have typically been restricted to domestic investors. This was changed with an announcement that was made in July 2018.

In July 2018, China announced intentions to allow foreign individual investors access to a shares through domestic brokerages. In this case, the regulatory change was beneficial to individual investors.

2. Tax policy reform

Tax policy reforms can affect the bottom line for businesses and individual investors alike. Any change to income tax law directly affects the income being brought in by respective parties and may present new regulatory risk.

3. Minimum wage laws

Increases to minimum wage can be a critical source of regulatory risk, as they substantially impact businesses, especially if they hire large quantities of low-skilled labour. In particular, small businesses suffer greater losses due to their inability to access economies of scale.

4. Mandated vacation and sick days

Similar to the above examples, changes to mandated vacation or sick days affect a company's bottom line as they are required to give employees more time off.

However, the opposite can be argued. By allowing employees to have more vacation days, they will be less burnt out and more productive during days in office. Stress-related issues can also be alleviated with more vacation days.

By allowing employees more sick days, office productivity may also increase because employees keep illnesses out of the office. The effects of this topic are continually being studied.

As you can see, many of the examples above can present regulatory risks that may directly affect a company's bottom line. In some cases, the effect is not easily observable, such as with mandated vacation and sick days. Sometimes regulatory changes can benefit investors or companies.

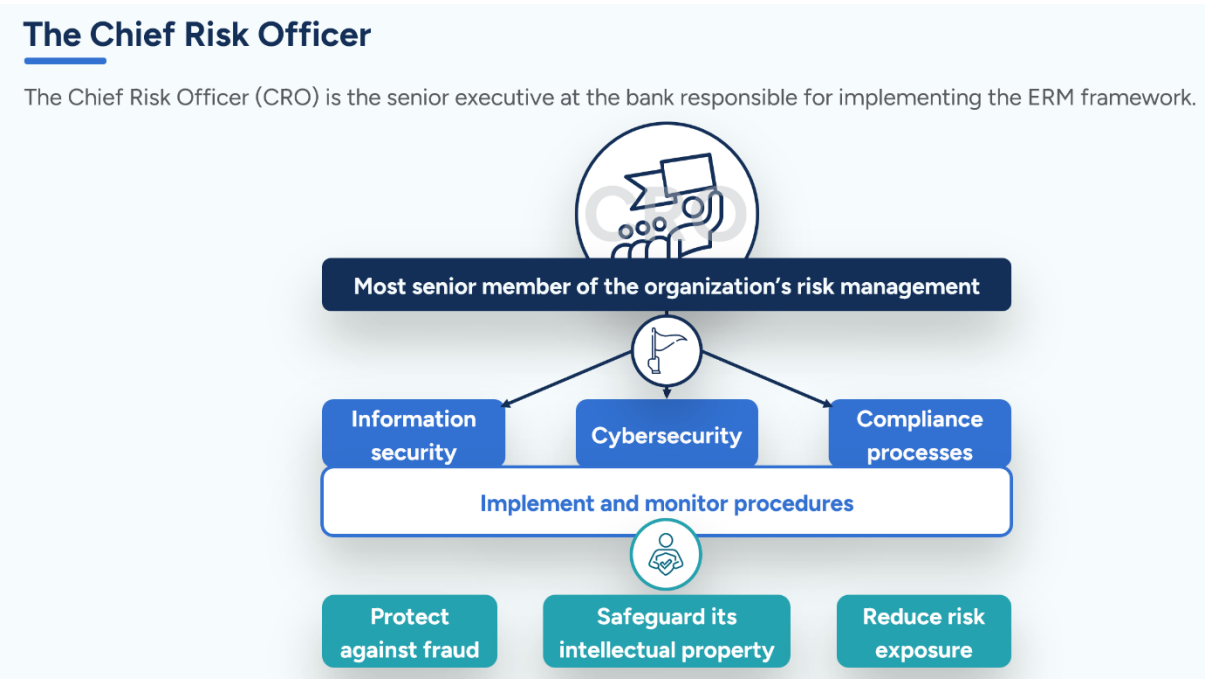
Companies may be penalized if they do not comply with regulatory changes. It is important for businesses to pay attention to and manage regulatory risk by ensuring compliance and diversification in its operating strategies.

For example, in the case of diversification, a company can protect itself from trade policy changes with any one particular country by diversifying its market into multiple countries.

Financial Regulation

Financial institutions are often subject to regulations with regard to disclosure, investment strategies, and liquidity requirements.

For example, the alternative uptick rule was a rule passed by the United States Securities and Exchange Commission (SEC) in 2010 in efforts to preserve market stability and confidence. The rule ensures that a short sale order must be entered on an uptick (where the price of a security is higher than its previously traded price). It is invoked when a stock's price drops more than 10% in one day and heavily affects how investors who take short positions invest.



Regulatory Risk Management: Value

- Ensure that our clients adopt sound corporate governance structure and practices that align with industry good practice and enable it to achieve their strategy
- Greater clarity and confidence around the regulatory risk framework and the organisation's ability to manage regulatory change.
- Understanding of both regulator expectations and business processes and challenges.
- Identification of process improvement opportunities to ensure the effective and consistent management of compliance and regulatory obligations.

Regulatory Risk Management (RRM)

Regulatory risk management (RRM) is a process of assessing and addressing the negative impact of changes in supervisory standards on a business. It's a crucial compliance strategy that helps in avoiding credibility loss and unexpected interruptions.

Businesses Need to Manage Regulatory Risk

Businesses function in an environment where regulatory standards change with time. Failure in managing regulatory risk can result in huge penalties. Managing these risks beforehand assists businesses in staying compliant, avoiding costly enforcement actions and developing trust with their clients.

Effective regulatory risk management assists businesses in staying ahead of updated regulations, adopting processes in real-time and deciding in a way that aligns with the rules and standards.

This is especially important for companies that are working in multiple jurisdictions, where even non-adherence with regional rules can create bigger problems.

In a nutshell, regulatory risk management is not just a way to evade penalties, it's a key to protecting a company's operations, reputation and long-term success.

Key Drivers of Regulatory Risks

The increase in regulatory risk depends on the combination of external and internal factors:

External Factors

Regulatory risks usually emerge when the global and national standards evolve. The Financial Action Task Force (FATF) regularly revises its recommendations, which set the direction for AML/CFT frameworks globally. For instance, at its February 2025 plenary, FATF agreed on changes to strengthen the risk-based approach guidance and monitoring updates on areas such as virtual asset risks and CDD-related guidance.

As a result, countries (including the U.S.) must consider these changes when shaping local AML rules, which in turn prompts regulators like Fin CEN to update domestic AML programmes to reflect FATF's changes.

Regulators pay close attention to new risks such as, digital payments, crypto, and high-risk entities, requiring firms to update their AML systems that can manage such risks. Companies working in multiple jurisdictions have to comply with different rules for each region, so they have to be notified every time to avoid compliance mistakes.

Internal Factors

Regulatory risks can also originate from within a company. Some of the major causes include the fragmented systems or manual workflows that are slow and error-prone, increasing the chance of omissions or regulatory breaches. Poorly defined rules and gaps in oversight can significantly contribute to risk exposure. Rapid growth or introduction of new products (e.g., digital assets) can create exposures without analyzing applicable laws and regulations that may govern such products. Furthermore, reliance on outdated data for screening and monitoring can result in serious problems, as changes to sanctions brought by new regulations are completely missed.

What are the Crucial Elements of an Effective Regulatory Risk Management (RRM)

A robust regulatory risk management (RRM) framework should include the following elements:

Governance & Internal Controls

Effective governance begins with clear board-level and senior management oversight of regulatory risk. Organizations are required to define governance structures, roles and responsibilities for compliance, monitoring and remediation. Internal risk appetite and policies should be consistently aligned with regulatory expectations to ensure the controls remain effective.

Compliance Culture

Embedding a culture of compliance across the firm is necessary in RRM. There should be an environment where employees understand regulatory risks, escalate issues and act accordingly. Ongoing Training programmes and periodic refreshers help ensure the staff remain informed, particularly when regulations change.

Monitoring, Reporting & Technology

Continuous monitoring of regulatory developments ("regulatory horizon scanning") prepares the organizations for changes in requirements. A technology-led approach is beneficial in automated screening of PEPs, adverse media, sanctions, real-time alerts, and audit-trail reporting. Data-driven risk analytics and dashboards for transparency across business lines, enabling teams to report to regulators with confidence and demonstrate the effectiveness of controls.

Scenario & Stress-Testing

Regular testing of frameworks helps firms measure the effectiveness of controls and identify potential gaps. Scenario planning for new regulations, products, and geographies prepares organizations for emerging risks. Measuring the effectiveness of controls, root-cause reviews of failures or breaches, and embedding lessons learned help in strengthening the framework.

Businesses today face an ever-increasing pressure to comply with new rules and regulations in AML (Anti-Money Laundering) compliance. To adhere to all these obligations and ensure unobstructed continuity of their business, firms require:

- A system with access to updated PEP and high-risk entity data from multiple global sources so it can help compliance team's spot risks before the risk actually arises.
- Firms must ensure that their systems offer context-driven insights that combine customer behaviour, transaction history, and regulatory data. This will help in flagging the right entities with additional context for accurate risk assessment.
- Systems must offer real-time alerts and audit-ready reports so that the compliance teams can react quickly to upcoming risks and provide regulators with necessary evidence.
- Businesses must look for a system that tracks updated regulatory developments, such as FATF recommendations, and national updates to guide internal controls and policies.
- The system must offer coverage across multiple jurisdictions to maintain uniform compliance.

Difference between GAAP and Statutory Accounting Principles

Generally Accepted Accounting Principles (GAAP) and SAPs are important in financial reporting. However, there are differences in purpose, methodology, and application. The table below outlines the principal distinctions between these two frameworks.

Aspect	GAAP (Generally Accepted Accounting Principles)	SAP (Statutory Accounting Principles)
Primary Objective	Provide a comprehensive view of a company's financial performance and position for investors and stakeholders.	They maintain regulatory oversight to ensure financial solvency and protect policyholders by focusing on the insurer's ability to meet obligations.
Users	Investors, analysts, management, creditors, and regulatory bodies.	Primarily, insurance regulators and state authorities.
Valuation of Assets	Assets are recorded at historical cost, fair value, or market value, depending on the asset class.	Assets recorded at conservative, realisable values; certain risky or illiquid assets classified as non-admitted.
Recognition of Liabilities	Liabilities recognised based on probable occurrence and estimations, often using wider assumptions.	Liabilities, especially insurance reserves, are recognised using conservative actuarial assumptions to ensure adequacy.
Focus	Earnings, profitability, and overall financial performance.	Solvency, liquidity, and ability to meet policyholder obligations.
Going Concern Assumption	Assumes the company will continue operating indefinitely.	Operates largely under a liquidation assumption to ensure assets are sufficient if the company is wound down.
Regulatory Oversight	Regulated by national accounting boards, e.g., FASB in the US.	Regulated by state insurance departments and the National Association of Insurance Commissioners (NAIC).

Based Approaches To Financial Regulation:

Statutory (Rules-Based) Approach

Definition: Prescribes specific, detailed rules for behaviour and reporting, leaving little room for interpretation (e.g., "drive under 120 km/h").

Pros: High clarity, easier compliance checks, reduced ambiguity, standardizes reporting for comparability (e.g., U.S. GAAP).

Cons: Can be rigid, complex to update with new tech, encourages "box-ticking," allows firms to exploit loopholes for favourable (but potentially misleading) reports.

Best For: Environments needing strong deterrence and standardization where specific actions are easily defined.

Principles-Based Approach

Definition: Sets broad objectives and guidelines, requiring judgment to apply them contextually (e.g., "drive responsibly").

Pros: Flexible, adaptable to new situations, promotes better judgment, fosters relevant information (e.g., IFRS).

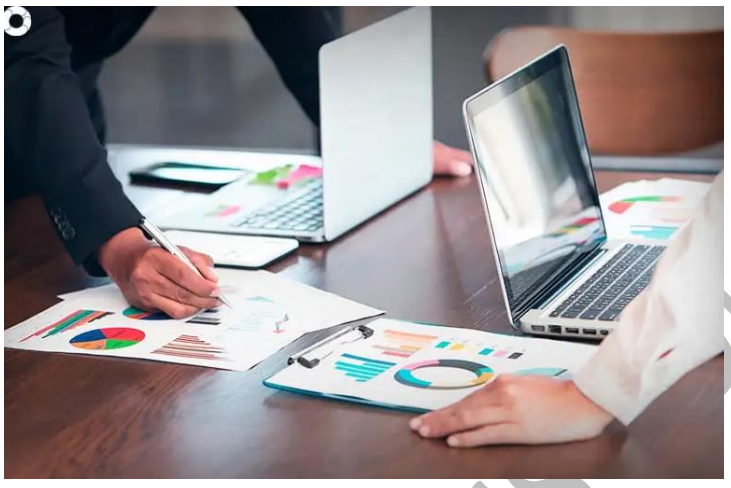
Cons: Relies heavily on professional judgment, leading to potential subjectivity, inconsistent application, and opportunities for manipulation.

Best For: Dynamic environments where rules can't keep pace, promoting true economic substance over form.

UNIT - III

OPERATIONAL RISK AND CREADIT RISK

Measurement of Operational Risk:



In this article, we explain the different approaches to measuring operational risk in an organization. See what they are!

According to the Basel Committee, there are three ways to measure operational risk: the basic indicator approach (BIA), the standard approach (SA) and the advanced measurement approach (AMA). Here we explain each of them.

1. Basic indicator approach for measuring operational risk

The basic indicator approach is much simpler than the other techniques for measuring operational and is therefore recommended for small financial entities whose operations are not very complex.

This method calculates the operational risk for the entire organization and then assigns the result to the operational lines. The basic indicator is measured as a percentage of gross income over that of the preceding three years.

There are several reasons why this indicator is calculated through gross income. Firstly, it is verifiable. Secondly, because it is immediately available and also because it is a counter-cyclical measure that helps to reliably measure the size of activities.

2. Standard approach to measuring operational risk (SA)

According to this method for measuring operating risk, banks' activities are divided into eight lines of business: corporate finance, sales and trading, retail banking, commercial banking, payments and settlements, agency services, asset management and retail brokerage.

Within each line of business, gross revenue serves as an indicator to measure the scale of commercial operations and, therefore, to calculate the possible exposure to operational risk in each line.

It is calculated by taking the three-year average of the sum of the regulatory capital charges for each operating line in each year.

To use the standard approach, a bank must meet certain requirements:

- Both the board of directors and senior management must be involved in overseeing the operational risk management framework.
- It must have a solid operational risk management system that is implemented throughout the company.
- It must have sufficient resources to use this approach in the main lines of business, as well as in the areas of control and auditing.

4. Advanced measurement approach (AMA)

Out of the three approaches to measuring operational risk, this is the most sophisticated method. With the AMA model, banks can create their own empirical model to quantify the capital required for operational risk.

An AMA framework should include the use of four quantitative elements for its development: internal loss data, external data, scenario and business environment analysis, or internal control factors.

Among the AMA models, there are three different types of methodologies: internal measurement approach (IMA), loss distribution approach (LDA) and scorecards.

At Pirani, the advanced measurement approach (AMA) is the one we use to estimate operational risk capital based on the loss distribution approach (LDA). This approach allows us to establish continuous improvement systems, predict expected losses for the organization over a period of time, define loss indicators and thresholds, and create scenarios to simulate catastrophic events.

Operational Risk:

Operational risk refers to the risk of losses resulting from errors or inefficiencies in a business's everyday operations. It's a type of unsystematic risk, meaning it's specific to a particular business or industry. This is opposed to systemic risks in overarching political or economic processes.

Operational Risk Framework:

The operational risk framework includes five dimensions:

- People
- Processes

- Systems
- External Events
- Intentional Fraud

We'll now briefly describe how each of these relate to operational risks.

People

Operational risk related to people typically comes down to problems of either quality or quantity. In terms of quality, a company may not have staff members with the appropriate skill sets to solve specific challenges, for example. In terms of quantity, for comparison, a company may get caught with not enough employees on duty to handle high-volume business periods.

This problem is largely handled by hiring or activating more employees. However, that comes with further complications: selecting appropriate candidates, training them properly, enticing them to stay with the company, and so on.

Processes

Every business has processes: sequences of tasks that must be followed in order for the company's operations to run correctly. Operations risk tends to happen here when companies don't refine their processes or don't fully document what must be done for them.

This can happen if a company experiences high turnover. For example, new employees keep coming in who aren't totally familiar with how things should be done at the company.

Systems

Systems refers to the software and hardware a company uses to help manage its operations. Operation risk can happen here because these systems are improperly configured, out of date, or not designed to handle what a company needs them to do. Risk can also be related to a business's systems not being as efficient as one or more of its competitors.

External Events

Risk to a company's operations can also come from outside the company itself. Sometimes it's simply related to the nature of business, such as partnered businesses not fulfilling their contractual obligations. Other times, it can be related to things like environmental factors, such as storms or other inclement weather that can prove to be obstacles for a company's logistics.

Intentional Fraud

This is sometimes called operating risk related to legal and regulatory compliance. It's about deficiencies in processes and systems that leave them vulnerable to being exploited for criminal activities.

These threats often come from outside a company, such as cybercriminals taking advantage of bugs or other loopholes in the company's system security. However, they can also come from inside a company, such as employees conspiring to steal money by taking advantage of a lack of internal process controls.

Types of Operational Risk:

1. Shady business practices:

Companies that engage in misleading advertising, selling defective products (knowingly or not), or ignoring regulatory business requirements (such as doing anti-competitive things like price-fixing) have a higher degree of operational risk.

2. Technological failures:

Businesses that rely heavily on computer systems to automate their processes face increased operational risk of a software error or hardware damage causing the system to function improperly – or even shut down.

3. Adverse environmental conditions:

Depending on what industry a business is in and where it's located, things like inclement weather or natural disasters can pose an operational risk to the company's logistics or physical infrastructure.

4. Lack of workplace safety:

Failing to address incidents or hazards that threaten employees' physical or mental health constitutes operational risk. It may cause high employee turnover, and even penalties from regulatory agencies.

5. Faulty process execution:

Human errors in data entry, accounting, and other everyday business tasks create operational risk. They can cause a company to miss meeting its obligations, or mislead managers into choosing ineffective business strategies.

6. External fraud:

Companies with insufficient cybersecurity, identity verification/authorization, and fraud detection incur operational risks. They are vulnerable to clients abusing them to launder money, hackers looking to steal sensitive information, and other types of fraudsters.

7. Internal fraud:

A lack of internal process controls can create operational risks for internal fraud. Employees may conspire to embezzle funds, or senior management officials may abuse their positions to misappropriate assets or use privileged information to gain unfair advantages.

Operational Risk Management:

1. Identify Current Risks and Anticipate Future Ones

The first step in managing operational risk is to brainstorm everything that could reasonably go wrong with a business, based on what industry it's in and how it specifically operates. This should involve employees from every level of the organization in order to cover all the different dimensions of operational risk.

It should also consider what risks may present themselves down the road, due to both changing external circumstances and possible business moves the company might make. If these risks do come up, the company will already have an idea of whether it will want to try to avoid or mitigate them, or else just accept them.

2. Assess and Prioritize Risks

The next step is to do an operational risk assessment. This involves a company conducting a data-driven evaluation of factors such as:

- How likely each identified risk is to cause a problem
- How soon each risk is expected to cause a problem
- How severe each of these problems is likely to be
- The potential upsides of accepting certain kinds of risks

Based on these estimations, a company can make a series of decisions regarding its risk management strategy. These include:

- Which order to address risks in
- Which level of the business should address a certain risk
- Whether to accept, mitigate, or avoid a particular risk

3. Put Risk Mitigation Measures into Action

Once a company has prioritized which risks to act on and which actions to take, it needs to actually start putting the controls in place. Some risks may be able to be avoided entirely, while others may have to be simply reduced to levels that the company can tolerate.

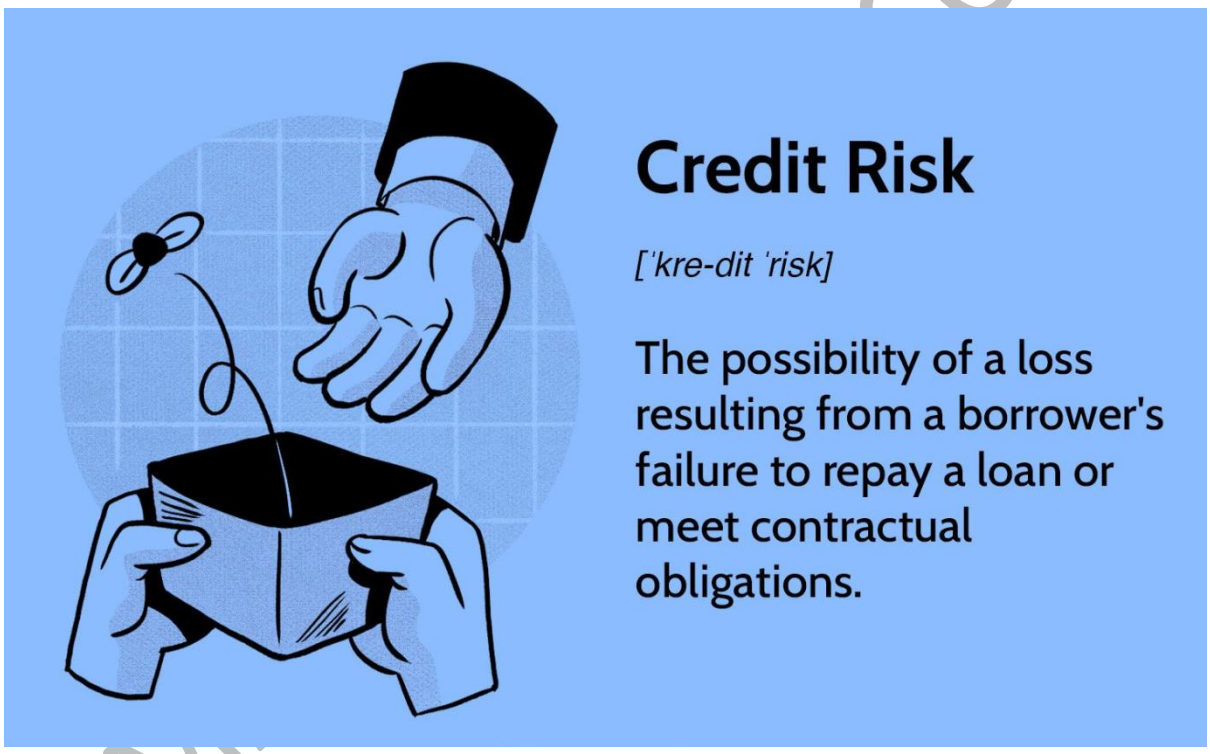
Another strategy is to delegate responsibility for risks to outside parties, such as insurance companies. And some risks may simply be accepted because their costs are far outweighed by their benefits.

4. Monitor and Report on Ongoing Risk Management Efforts

Operational risk management is an ongoing process. So it's essential to monitor both risks and the controls on them continually. In some cases, risks may need tighter controls. In other cases, risk controls may be too costly and need to be relaxed for a better risk-reward balance. This is especially true because the amount of threat that certain types of risks represent for a business can increase or decrease, based on changing circumstances.

Credit Risk:

Credit risk is the potential for a lender or investor to lose money because a borrower fails to repay a loan or meet other financial obligations, encompassing defaults, late payments, or downgrades, and is assessed by analyzing credit history, income, and capacity to repay to determine the probability of default, influencing interest rates and lending terms. It's a core concern for banks, companies, and investors in all lending activities, from personal loans to corporate bonds.



Credit Risk

Credit risk is the chance that a borrower might not fulfill their loan repayment or other contractual commitments, causing a financial loss to the lender. This risk is inherent in all lending activities and can arise from various factors, including economic downturns, poor credit history, or inadequate collateral.

Credit Risk Definition

In the context of financial institutions, credit risk is defined as the potential that a borrower or counterparty will fail to meet their obligations in accordance with agreed terms. It includes the

risk of missing payments on principal or interest, as well as the risk that the borrower's creditworthiness deteriorates.

Credit Risk Management Matters:

Proper management of credit risk is essential for safeguarding the financial stability of lending institutions. By proactively identifying and mitigating potential credit losses, institutions can ensure stable earnings, preserve capital, and maintain investor confidence. Moreover, robust credit risk management practices contribute to the overall stability of the financial system by preventing the accumulation of non-performing assets and minimizing systemic risk.

Components of Credit Risk Management:

1. Credit Risk Assessment

Credit risk assessment involves evaluating the likelihood that a borrower will be unable to fulfill their debt repayments. This process includes analyzing the borrower's credit history, financial statements, cash flow projections, and collateral quality. Tools such as credit scoring models and the Altman Z-score are commonly used to quantify credit risk.

2. Credit Risk Measurement

Quantifying credit risk is essential for determining the potential loss exposure. Key metrics include:

Probability of Default (PD): This probability refers to the chance of default occurring within a certain period.

Loss Given Default (LGD): The anticipated loss percentage on the outstanding amount if the borrower defaults.

Exposure at Default (EAD): The entire sum exposed to risk at the point of default.

These metrics are integral to calculating the Expected Loss (EL) and informing risk-based pricing and capital allocation decisions.

3. Credit Risk Monitoring

Ongoing monitoring of credit exposures ensures that changes in a borrower's financial condition are promptly identified. This includes regular reviews of credit ratings, financial statements, and compliance with covenants. Identifying signs of declining credit quality early allows for prompt action to minimize losses.

4. Credit Risk Control

Implementing controls to mitigate credit risk is crucial. Strategies include setting credit limits, requiring collateral, and incorporating covenants into loan agreements. Moreover, spreading credit exposure across different industries, regions, and types of borrowers helps reduce the risk of over-concentration.

5. Credit Risk Mitigation Techniques

To further manage credit risk, institutions employ various mitigation techniques:

Collateralization: Securing loans with assets that can be liquidated in case of default.

Guarantees: Obtaining third-party assurances to cover potential losses.

Credit Derivatives: Using instruments like credit default swaps to transfer risk.

Credit Insurance: Securing insurance coverage can also protect against potential credit losses.

6. Credit Risk Management in Banks

Banks face unique challenges in credit risk management due to their role in financial intermediation. They must comply with regulatory requirements, such as Basel III, which mandates capital adequacy and risk management standards. Banks also utilize internal rating systems and stress testing to assess and manage credit risk effectively.

7. Commercial Credit Risk Management

In the commercial lending space, credit risk management focuses on evaluating the financial health of businesses. This process involves studying market conditions, business models, and key financial indicators. Commercial lenders often require detailed business plans and financial projections to assess creditworthiness.

8. Corporate Credit Risk Management

Corporate credit risk management involves assessing the creditworthiness of large corporations. This process includes analyzing complex financial structures, market positions, and operational risks. Corporations may also engage in credit risk management by monitoring their own credit ratings and managing counterparty exposures.

9. Credit Risk Management System

A credit risk management system encompasses the policies, procedures, and technologies used to manage credit risk. Key components include:

Credit Policies: Documented guidelines for credit approval and monitoring.

Risk Rating Systems: Structures designed to evaluate the risk levels associated with borrowers.

Loan Review Processes: Regular evaluations of loan performance and compliance.

Reporting Mechanisms: Tools for tracking and reporting credit risk metrics.

10. Credit Risk Management Software

Advancements in technology have led to the development of sophisticated credit risk management software. These tools facilitate:

Automated Credit Scoring: Utilizing algorithms to assess creditworthiness.

Portfolio Monitoring: Monitoring credit exposures and risk concentrations in real time.

Regulatory Compliance: Ensuring adherence to reporting and capital adequacy requirements.

Predictive Analytics: Forecasting potential defaults and losses.

Credit and Risk Management in Banking:

In the banking sector, credit and risk management are intertwined disciplines. Banks must balance the pursuit of profitable lending opportunities with the imperative to manage risk exposures. This involves integrating credit risk management into the broader enterprise risk management framework, aligning risk appetite with strategic objectives, and fostering a risk-aware culture.

Challenges in Credit Risk Management:

Despite advancements in methodologies and technologies, credit risk management faces several challenges:

Economic Volatility: Fluctuations in economic conditions can impact borrower creditworthiness.

Regulatory Compliance: Staying compliant with changing regulations demands ongoing adjustments.

Data Quality: Accurate and timely data is essential for effective risk assessment.

Model Risk: Reliance on quantitative models necessitates validation and oversight.

Cyber security Threats: Protecting sensitive credit data from breaches is paramount.

Best Practices in Credit Risk Management:

To navigate these challenges, institutions should adopt best practices:

Robust Credit Policies: Establish clear guidelines for credit approval and monitoring.

Comprehensive Risk Assessment: Incorporate both quantitative and qualitative analyses.

Regular Stress Testing: Evaluate the impact of adverse scenarios on credit portfolios.

Continuous Monitoring: Implement systems for real-time tracking of credit exposures.

Skilled Personnel: Invest in training and retaining experienced credit risk professionals.

Emagia Enhances Credit Risk Management:

Emagia offers advanced solutions to streamline and enhance credit risk management processes. By leveraging artificial intelligence and machine learning, Emagia's platform provides:

Automated Credit Assessments: Accelerating decision-making with AI-driven analytics.

Real-Time Monitoring: Offering up-to-date insights into credit exposures.

Predictive Modelling: Forecasting potential defaults and optimizing risk mitigation strategies.

Integrated Workflows: Facilitating seamless collaboration across credit, collections, and finance teams.

By integrating Emagia's solutions, institutions can enhance the accuracy, efficiency, and responsiveness of their credit risk management practices.

Credit Risk Influences Interest Rates:

Creditors may decline a loan to a borrower they perceive as too risky.

For instance, applicants with high credit ratings and steady income are seen as low risk and usually get low-interest rates. In contrast, an applicant with a poor credit history may have to work with a subprime lender to get financing.

The best way for a high-risk borrower to get lower interest rates is to improve their credit score. If you have poor credit, consider working with a credit repair company.

Similarly, bond issuers with less-than-perfect ratings offer higher interest rates than those with perfect credit ratings. The issuers with lower credit ratings use high returns to entice investors to assume the risk associated with their offerings.

Banks can manage credit risk with several strategies. They can set specific standards for lending, including requiring a certain credit score from borrowers. Then, they can regularly monitor their loan portfolios, assess any changes in borrowers' creditworthiness, and make any adjustments.

The five Cs of credit include capacity, capital, conditions, character, and collateral. These are the factors that lenders can analyze about a borrower to help reduce credit risk. Performing an analysis based on these factors can help a lender predict the likelihood that a borrower will default on a loan.

Each lender will measure the five Cs of credit (capacity, capital, conditions, character, and collateral) differently. Generally, lenders emphasize a potential creditor's capacity, or the amount of income they have relative to the debt they are carrying.

5 C's of Credit Work

1. Character in 5 Cs of Credit

Character refers to the borrower's commitment to uphold their obligation to meet the payments per the lending agreement, irrespective of unforeseen events.

The assessment of a borrower's character is a bit of a subjective measure, since it is closely tied to integrity and reputation.

Oftentimes, a borrower's financial state can unexpectedly undergo a sudden change, such as a reduction in income from a job loss or unanticipated medical bills. The lender needs assurance

that the borrower will still continue to abide by the lending agreement and meet the required payments on time.

The track record of the borrower tends to be the most insightful data set for lenders to diligence, which can be evaluated via the credit history and credit score of the borrower.

Historical proof of the borrower repaying loans and fulfilling their obligations without irresponsible behaviour—i.e. the absence of "red flags" such as late payments and past defaults—are perceived positively by lenders.

If the borrower has worked with the lender in the past, then the existing relationship can also be influential in the lender's decisions, as well as make the application process quicker.

For example, a private equity firm that has worked with a lender in the past and has built a strong reputation over the years is far more likely to be trusted by the lender for future financing arrangements.

2. Capacity in 5 Cs of Credit

Capacity is the ability of the borrower to generate sufficient income to repay the new loan, with consideration also given to existing debt obligations.

The methods of measuring capacity are thus more objective, where the items considered are generally quantitative, such as the borrower's monthly income.

For instance, the debt to income ratio is a relevant credit metric that compares the borrower's monthly debt payments to their pre-tax monthly income. While the target DTI differs by lender, most prefer a DTI around 35% or less to approve the applicant.

Debt to Income Ratio (DTI) = Total Monthly Debt ÷ Gross Monthly Income

The capacity of a borrower can be improved by an increased salary, an additional source of income, and/or the reduction of existing debt.

The lender must also ensure the borrower's job security and stream of income is stable, which can be confirmed by the employer and the proof of consistent wages (i.e. the borrower is a long-term employee at the company, as opposed to a recent hire).

The reduction of debt is straightforward, since it entails the borrower using discretionary cash to reduce existing debt. In addition, another method is to refinance debt with more favourable terms, e.g. to reduce the monthly payments on an existing loan.

3. Capital in 5 Cs of Credit

Capital encompasses the overall financial position of the borrower, such as the initial capital contribution and the value of the borrower's savings and assets (i.e. net worth).

One example is the size of the down payment on a mortgage loan, where a greater down payment results in a lower interest rate and more favourable terms.

A larger-sized down payment is proof to the lender about the seriousness of the borrower to repay the entire loan at maturity and service all interest payments. A larger capital contribution indicates to the lender that liquidity is not a concern, given that it is a form of upfront payment.

Other than the capital contribution to the loan, capital also refers to the analysis of the past financial state of the borrower.

The lender will evaluate how stable the borrower's financial health has progressed over time.

For corporate borrowers, risks such as cyclicality and the ability to withstand an economic contraction are considered here, whereas the risks more applicable to consumers include job security and substantial changes in discretionary income.

4. Collateral in 5 Cs of Credit

Collateral can be pledged by the borrower to secure a loan and receive more favourable terms.

The collateral-backed loan, or "secured loan", provides the lender with more assurance because the downside risk is reduced.

In the event of default—the worst case scenario —the lien on the collateral means that the lender has a legal claim on the pledged asset of the borrower and can seize it.

The lender is thereby likely to recover the original loan principal, even if the matter becomes more complicated from the borrower filing for bankruptcy protection, as the Court must then first prioritize the claims held by secured lenders.

For example, two of the most common consumer loans are mortgages and auto loans, wherein the collateral consists of the purchased property (i.e. the house and the car, respectively).

5. Conditions in 5 Cs of Credit

Conditions describe the contextual details of the borrower and the current credit environment in which the loan application is considered.

For instance, the specifics behind the requested loan amount and how the borrower intends to use the proceeds from the loan can influence the lender's decision.

If the borrower needs the funds to start a new business at a time when the economy is at risk of entering a global recession and the proposed business operates in a high-risk industry with secular headwinds, the likelihood of the application being accepted is lower.

The conditions can consist of internal factors including the purpose of the borrowing, or external factors outside the control of the borrower, such as the prevailing interest rates, current economic conditions (or outlook), geopolitical risks, and pending regulatory risks that could negatively impact the borrower.

Credit Risk Identification and Assessment:

1 Credit Risk Identification:

Identifying credit risk is the first step in credit risk management. The identification of credit risk focuses on detecting potential risks in financial transactions such as loans and leases. Banks should adopt various process and tools such as checklists, early warning signals, to identify credit risk prevalent in the bank.

The bank should undertake following techniques for identification of credit risk:

a) Efficient Management Information System (MIS): Banks should have an MIS in place to ensure that exposures approaching risk limits are brought to the attention of senior management. The bank's information system should be able to aggregate credit exposures to individual borrowers and counterparties and report on exceptions to credit risk limits in a meaningful and timely basis.

b) Continuous review: The bank should monitor the borrower's profile to understand his/her financial stability, regularity in repayments, defaulting nature. Banks may design detailed checklists including source of income, financial position of the borrower, CIBIL score, willingness of borrower to default, etc. Banks should establish a mechanism of independent, ongoing review of credit risk management framework to assess the credit administration process, the accuracy of credit rating including adequacy of provisions for losses, and overall quality of credit portfolio. All facilities should be subjected to risk review at least quarterly. More frequent review should be conducted for new accounts where bank may not be familiar with the obligor, and for classified or adverse rated accounts that have higher probability of default.

c) Root Cause Analysis: Another effective risk identification technique is finding the root cause indicating why an event occurred. This provides information about what triggered a loss and where the bank was vulnerable. The business departments shall undertake such exercise through an operational audit exercise. The findings of such analysis may be internalised in case of new loans.

d) SWOT analysis: Assessing the strengths, weaknesses, opportunities and threats involved with the loan/investment shall be undertaken at the time of approval of loans/investments.

e) Early Warning Signals: The banks shall put in place a system of early warning signals to identify risks.

f) Stress testing: Stress tests are a risk identification technique which help identify downgrade risk, concentration risk, depletion in collateral, etc. The banks should undertake stress tests on credit risk to assess the impact of increasing NPA, concentration risk, etc., on capital adequacy and profitability.

2 Credit Risk Assessment and Approval:

Credit appraisal or credit assessment is undertaken by banks at the time of lending in order to address certain signals and undertake precautions when a new sanction is imposed, or an existing

client's facilities are renewed. The credit assessment process includes determining eligibility for credit, quantum of credit/investment, credit delivery as well as terms and conditions of credit.

The details of credit assessment shall be covered in the respective loan policy taking into consideration the broad factors indicated in this policy. Credit assessment process should, at a minimum, cover the factors specified in Annexure IV.

Credit Risk Measurement:

The bank should employ measurement techniques that are appropriate to the complexity and level of the risks involved in their activities, based on robust data and periodic verification of results. The measurement of credit risk considers the specific nature of the credit, its contractual and financial conditions (maturity, interest rate, etc.), existence of collateral or guarantees and the potential for default based on the internal risk rating. It is important to ensure that risk measurement is performed on a consistent and bank-wide basis, based on inherent credit risk and residual impact. The banks may employ following techniques for measurement of credit risk:

1. Credit Rating Framework:

Prior to sanctioning a credit facility to any client/obligator, the risk level should be measured as per internal risk assessment model. The internal credit rating framework assigns a number/alphabet/symbol as a primary summary indicator of risks associated with a credit exposure. The internal credit rating framework may be mapped with credit rating from external credit rating agencies.

Risk rating models are required to be technically reviewed on a regular basis to ensure accuracy and validity of the models. An indicative credit rating framework is given in Annexure V.

2. Risk based Pricing:

Banks should assess the risk/return relationship in any credit as well as the overall profitability of the account relationship. Credits should be priced in such a way as to cover all the embedded costs and compensate the bank for the risks incurred. In evaluating whether, and on what terms, to grant credit, banks need to assess the risks against expected return, factoring in, to the greatest extent possible, price and non-price (e.g., collateral, restrictive covenants, etc.) terms. In evaluating risk, banks should also assess likely downside scenarios and their possible impact on borrowers or counterparties. A common problem among banks is the tendency of not pricing a credit or overall relationship properly and thus not receiving adequate compensation for the risks incurred.

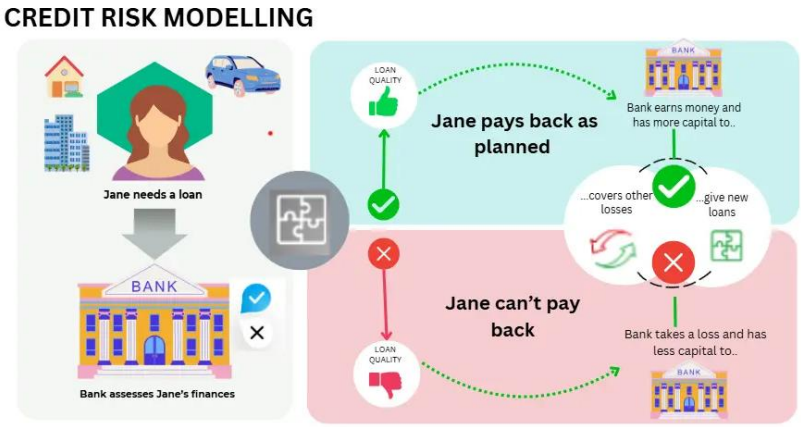
In present scenario, banks may assign a risk premium that it may charge against each risk grade.

3. Risk-Adjusted Returns / Capital:

a. **Return On Risk-Adjusted Capital:** RORAC considers the risk of unexpected loss by allocating capital and is used to evaluate projects involving a high-risk element relative to the capital required.

b. **Risk-Adjusted Return on Capital:** RAROC is a risk-based profitability framework for analyzing risk-adjusted financial performance and providing a consistent view of profitability across businesses. RAROC adjusts both return and allocated capital for the risks associated and is a ratio of profitability used to compare alternative investments based on risks involved at the business unit level.

Credit Risk Modelling Techniques:



Counterparty credit risk is commonly defined as the possibility that the counterparty, or the other party to a certain financial transaction, will be unable to fulfill his contractual obligations. This type of risk is usually common in products like derivatives, securities lending and foreign exchange whereby both contract parties rely on the counterpart to deliver his side of the bargain. Counterparty credit risk is a major problem in the financial market since in the case of default, one party suffers financial losses.

In financial markets, counterpart credit risk is significant since it affects the stability as well as the confidence of the participants in the market. Banks, investment banks, trading companies, and clearinghouses are a few examples of financial institutions that conduct numerous transactions daily. When counterparties fail to fulfill their contractual obligations, it triggers chain effects, instantly resulting in a lack of liquidity, loss of capital, and possibly, and systemic failures. It is crucial to mitigate this risk to avoid drastic fluctuations in the market and maintain its stability.

In addition to the actual credit loss, there are other risks when a counterparty is unable to meet its obligations. This outcome can result in legal actions, negative word of mouth and contractual constraints in the market. Also, a default can create a snowball effect, most especially if the entities defaulting are related in one way or the other through various financial derivatives. This was evident in the 2008 financial crisis where counterparty risks caused the world to be hit hard with an economic collapse and that urged institutions to embrace efficient measures to manage such risks.

For the management of counterparty credit risk, credit risk analysis and therefore, credit risk modelling is crucial. Nested, a low code/no code platform that offers modern, best-in-class rules based engine and workflow orchestration functionality allow businesses to set up efficient risk

management solutions. Through the use of Nested, organizations can be able to fully manage the credit risks without having to invest in technical knowledge to do so, thus enhancing security from counterparty risk.

Sound Practice Features of Effective Credit Risk Management

The Basel Committee on Banking Supervision and industry experts identify several key features:

1. Establishing an Appropriate Credit Risk Environment (Governance)

Board and Senior Management Oversight: The board of directors is responsible for approving the bank's credit risk strategy and significant policies, which should align with its risk tolerance and capital plans. Senior management is tasked with implementing these policies and ensuring effective procedures are in place.

Clear Roles and Accountability: The organizational structure should clearly delineate roles and responsibilities, ensuring separation between the credit origination/business function (front office) and the independent risk management and internal audit functions (middle and back office).

Risk Culture and Ethics: Remuneration policies should align with the long-term credit risk strategy and not encourage excessive short-term profit-seeking at the expense of sound risk practices. A strong risk-aware culture across the organization is essential.

2. Operating Under a Sound Credit-Granting Process

Well-Defined Criteria: Credit-granting criteria must be sound and clearly defined, including target markets, risk acceptance criteria, and a thorough understanding of the borrower's capacity and character.

The assessment process should be forward-looking and use methodologies like the 5 Cs of Credit (Character, Capacity, Capital, Collateral, and Conditions) to evaluate a borrower's ability and willingness to repay.

Approval Authority Structure: A structured approval process with appropriate limits for lending officers, and dual or committee approval for large exposures, ensures consistency and accountability.

Robust Documentation: All loan agreements and documentation must be clear, legally sound, and comprehensive, outlining terms, conditions, collateral, and covenants.

3. Maintaining an Appropriate Credit Administration, Measurement, and Monitoring Process

Risk Rating Framework: Banks should use a transparent internal risk rating system to assess the risk of individual credits and the overall portfolio. These ratings should be reviewed periodically and validated by an independent function.

Ongoing Monitoring and Early Warning: Continuous monitoring of borrower performance and market conditions is crucial. Early warning signal systems should be in place to detect deteriorating credit quality promptly, allowing for timely corrective action.

Portfolio Management and Diversification: Active management of the loan portfolio involves diversifying exposure across industries, geographies, and borrowers to avoid undue concentration risks.

Risk-Based Pricing: Credits should be priced to cover all embedded costs and adequately compensate the bank for the risks incurred, reflecting the borrower's risk profile.

4. Ensuring Adequate Controls over Credit Risk

Effective Loan Review Mechanism: An independent loan review function should regularly assess the quality of the credit portfolio, the accuracy of risk ratings, and compliance with policies and procedures.

Stress Testing and Scenario Analysis: Regular stress testing and scenario analysis should be conducted to assess the impact of potential economic downturns or market movements on the portfolio and capital adequacy. Results should inform limit setting and contingency planning.

Remedial Action and Problem Loan Management: A clear system for early remedial action on deteriorating credits and established workout procedures for nonperforming assets (NPAs) helps minimize losses and maximize recoveries.

Technology Integration: Leveraging advanced analytics, AI, and automation can enhance speed, accuracy, and scalability in risk assessment, monitoring, and reporting.

Credit Risk Management Function:

1. Strong Governance Framework

Develop a solid governance framework that clearly defines organizational structures, roles, and responsibilities related to credit risk management. This ensures accountability and facilitates effective decision-making within the organization.

2. Continuous Data Evaluation

Constantly evaluate and validate your data sources to ensure that the information being used for risk modeling is accurate and relevant. This involves regularly assessing the quality of the data and the methodologies employed in model development.

3. Consistent Model Validation

Validate your credit risk scorecard models consistently to ensure they remain effective over time. This involves applying rigorous statistical tests and back-testing against historical data to assess predictive accuracy and effectiveness in risk evaluation.

4. Proactive Monitoring

Implement proactive monitoring of your risk models. This includes continuously tracking performance indicators and adjusting the models as necessary in response to emerging trends, regulatory changes, or shifting market conditions.

5. Leverage Dynamic Data

Utilize dynamic data to enhance decision-making processes. By integrating real-time information such as economic indicators and behavioral data, organizations can make more informed credit decisions and anticipate potential risks more accurately.

6. Comprehensive Framework Development

Create a credit risk management framework that assists in identifying, monitoring, measuring, and controlling risks when extending credit. An effective framework facilitates systematic assessments and supports strategic decision-making regarding credit approvals.

7. Continuous Risk Assessment

Adopt a continuous, proactive approach to risk assessment. This involves regularly identifying potential risks, evaluating their impact, and strategically implementing measures to safeguard against potential losses.

By adhering to these best practices, organizations can develop a credit risk management model that not only minimizes potential losses but also promotes sustainable lending practices. This comprehensive approach fosters resilience and flexibility in the face of evolving economic realities.

Reporting Tools:

Risk Reporting and Dashboards: These provide a centralized, real-time view of the credit portfolio's health using visuals like charts and heat maps. This helps decision-makers quickly understand key risk indicators (KRIs), exposure, and emerging trends.

Credit Risk Management Software: Specialized platforms (like those offered by Moody's Analytics, SAS Risk Management, and High Radius) aggregate data from various sources, perform analyses, and generate comprehensive reports for management and regulatory bodies.

Business Intelligence (BI) Tools: These tools enhance reporting by delivering actionable insights and supporting automated regulatory reporting, which is crucial for meeting compliance requirements efficiently.

Management Information Systems (MIS) Reports: Lenders may require borrowers to submit periodic financial statements and pre-determined reports, which are then integrated into internal MIS for ongoing monitoring and assessment.

Escalation Tools:

Early Warning Systems (EWS): These systems are perhaps the most critical escalation tool. They use data analytics to detect early signs of potential problems (e.g., changes in payment behavior, deteriorating financial ratios, or macroeconomic shifts) before they become significant issues.

Real-time Risk Alerts: Integrated within risk management software, these alerts automatically notify relevant teams (e.g., collections) when a customer's credit risk profile changes or predefined thresholds/limits are exceeded.

Credit Risk Limits and Thresholds: Clearly defined limits for individual borrowers, sectors, or the entire portfolio act as triggers. Breaching a limit automatically initiates an escalation process, which may involve tightening credit terms or reducing exposure.

Formalized Review Processes: The escalation framework is often built into regular credit review processes. If a review identifies heightened risk, the account is escalated to a higher level of management or a specialized risk committee for intervention and strategy adjustment.

Defined Workflows: Automated and transparent workflows within software platforms ensure that when a risk is identified, it is automatically routed to the appropriate person or department for action, ensuring accountability and timely response.

Basel Key Stages of Credit Risk Policy Development:

Establishing a Suitable Credit Risk Environment: This foundational stage involves the board of directors and senior management defining the institution's overall credit risk strategy and tolerance. It includes:

Approving and regularly reviewing the credit risk strategy and significant policies.

Ensuring the strategy reflects the bank's risk tolerance, expected returns, market conditions, and forward-looking information.

Establishing an effective internal control system.

Operating Under a Sound Credit-Granting Process: This stage focuses on the actual process of extending credit and ensuring that exposures are well-understood and managed from the outset. Key elements include:

Conducting comprehensive due diligence and obtaining sufficient documentation to assess a borrower's risk profile.

Employing a sound credit assessment framework (such as the 5 Cs of credit: Character, Capacity, Capital, Collateral, and Conditions).

Putting in place a system for the ongoing administration and proper maintenance of credit files and relevant financial information.

Maintaining an Appropriate Credit Administration, Measurement, and Monitoring Process: Once credit is granted, this stage involves continuous oversight to manage the risk over time. This includes:

Implementing systems for the ongoing measurement and monitoring of credit risk-bearing portfolios.

Using robust methodologies for assessing and measuring credit risk, which may involve internal models or standardized approaches (as per Basel II/III Pillars 1 and 2).

Ensuring an independent system for the ongoing evaluation of credit risk management processes, with clear reporting lines to senior management and the board.

Ensuring Adequate Controls over Credit Risk: The final stage is about implementing effective internal controls and mitigation techniques to manage potential losses. This involves:

Developing and using a comprehensive credit risk mitigation strategy (e.g., collateral, guarantees, and credit derivatives).

Establishing limits and escalation procedures for managing counterparty credit risk (CCR).

Promptly addressing problem loans and ensuring appropriate provisioning and reserves are maintained in accordance with applicable accounting standards.

UNIT – IV

Market Risk and Liquidity Risk

Identification of Liquidity Risk; Market, Investment and Operational Risk, Measurement of Liquidity Risk; funding Liquidity risk analysis: Liquidity gap analysis, stress testing, expected future funding requirement.

Liquidity Risk

Liquidity risk is the risk that a business will not have enough liquid assets to meet its short-term financial obligations as they come due. It occurs when there is a mismatch between the timing of cash inflows and outflows, leading to challenges in covering immediate needs such as payroll, supplier payments, or debt obligations. In extreme cases, liquidity risk can escalate into insolvency if the business cannot access the cash required to sustain operations.

This risk matters because cash flow is the foundation of a business's financial health. Poor liquidity management can lead to operational disruptions, strained relationships with stakeholders, and a loss of financial flexibility. Furthermore, businesses facing liquidity constraints often incur higher financing costs, as they may be forced to seek expensive short-term loans or sell assets under unfavourable terms. Effective liquidity risk management is critical to maintaining stability and ensuring that financial resources are available to navigate both routine demands and unexpected challenges.

Sources of Liquidity Risk

To put it simply, liquidity risk is the risk that a business will not have sufficient cash to meet its financial commitments in a timely manner. Without proper cash flow management and sound liquidity risk management, a business will face a liquidity crisis and ultimately become insolvent.

As businesses go about the process of measuring and managing liquidity risk, they need to be on alert for common sources of that risk. Those sources include:

1. Lack of Cash Flow Management

Cash flow management gives a business good visibility into potential liquidity challenges and opportunities. Cash is king, and cash flow is the bloodline of all businesses. Without proper management of cash flow, a business will increase its exposure to unnecessary liquidity risks. Moreover, a business without healthy and well-managed cash flow will face an uphill battle to remain profitable, secure favourable financing terms, attract potential inventors and be viable in the long run.

2. Inability to Obtain Financing

A history of late debt repayment and/or non-compliance with loan covenant requirements may translate into additional challenges when attempting to secure financing. Therefore, it is imperative that businesses have good capital structure management, match debt maturity

profiles to assets, and maintain a good relationship and regular communication with lenders. The inability to obtain funding at all or to obtain it at competitive rates and acceptable terms increases liquidity risk.

3. Unexpected Economic Disruption

At the start of 2020, the stock market was at an all-time high, and few people expected the world would be so hard hit by COVID-19. The adverse economic impact of this global pandemic was swift and relentless. Lockdowns created an unexpected economic disruption, and many businesses saw sales dwindle to a catastrophically low level and liquidity risk drastically increase.

4. Unplanned Capital Expenditures

Having proper fixed asset management is extremely important, particularly for a business that operates in a capital-intensive industry such as energy, telecommunications or transportation.

A capital-intensive business is often highly leveraged with a high fixed to variable costs ratio. For businesses like these, a single unplanned capital expenditure, such as a new purchase or major equipment repairs, may exacerbate existing budget constraints. This, in turn, further increases operating leverage and heightens liquidity risk.

5. Profit Crisis

A business in a profit crisis will not only see a decline in its profitability margins but also a decline in its top-line revenue. Consequently, to combat negative profitability margins and remain in operation, it will need to start dipping into cash reserves. Failure to stop a continuous cash burn will eventually deplete cash reserves, with the business inevitably facing a liquidity crisis. Developing a detailed cash flow forecast is a critical step in identifying potential shortfalls and creating a plan for recovery.

Types of Market Risk

The different types of market risk are shown below:

Market liquidity risk – this is the risk that the level of market activity might decrease and in certain cases cease making an asset illiquid to trade. This may mean a bank may not be able to transact business or execute trades in an orderly manner

Interest rate risk – this is exposure to instruments whose values change due to changes in interest rates

FX risk – FX or currency risk is the exposure to holdings and future cash flows that are not denominated in USD (or local currency of the investment bank)

Issuer credit risk – there is risk associated with the value of an asset when the credit rating associated with the issuer changes

Equity market risk – equity market risk changes in the value of an instrument linked to the ownership interest in a companyThis includes shares, ADRs, convertible bonds, equity options, equity TRS, equity futures etc.

Commodity risk – commodity risk changes in value of futures, forwards, swaps and options linked to the value of commodities such as oil, metals etc

Model risk – model risk is risk of adverse consequences arising from decisions based on incorrect or misused models

Measuring Market Risk

Measuring the market risk, or uncertainty surrounding an asset's potential performance can be done using several techniques.

Risk Measurement Techniques

Value at Risk (VaR)

Value at Risk is a widely used measure that estimates the potential loss that could occur to an asset over a specific time horizon, given a certain confidence level. It provides an estimate of the maximum loss that an investment or portfolio may experience under normal market conditions.

The three common methods for computing Value at Risk (VaR) are:

Historical simulation: this approach calculates VaR by using historical data. It involves ordering historical returns or price changes, selecting a confidence level, and identifying the loss value at the specified quantile.

Parametric VaR: this method assumes that the distribution of returns follows a specific statistical distribution, often the normal distribution. It estimates the mean and standard deviation of returns and uses these parameters to calculate VaR at the desired confidence level.

Monte Carlo simulation: this technique employs random sampling to generate numerous possible future scenarios for asset returns. Monte Carlo Simulation can handle complex portfolios and capture nonlinear relationships, but it can be computationally intensive and requires careful calibration of input parameters.

Risk Management Strategies

There are several ways to mitigate market risk within a portfolio. These can be undertaken at the time of the initial purchase or instigated at any point when market conditions or an investors' risk appetite has changed.

1. Hedging: taking offsetting positions to mitigate market risk exposure
2. Diversification: spreading investments across different asset classes, sectors, and geographies to reduce overall market risk

3. Risk Limits and Policies: establishing appropriate risk limits and policies to manage market risk exposure effectively

A combination of these practises is typically used within financial institutions to manage market risk. Risk limits and policies should be updated to maintain regulatory requirements. Management may also deem it appropriate to establish limits and policies which are go beyond the minimal regulatory requirements.

Investment risk

Investment risk can be defined simply as the risk that the actual return on an investment will be lower than the investor's expectations. Many investors are able to assess investment track records and investment models to decide if the potential rewards are worth the perceived risks in an investment. This type of risk is also readily measurable using various statistical measures, including:

- Alpha, the excess return of an investment relative to the return of the benchmark
- Beta, the measure of a volatility relative to the overall market
- R-squared, the measure that represents the percentage of an asset's movement that can be explained by movements in the benchmark
- Standard deviation, the measure of the dispersion of data from its mean
- Sharpe ratio, which describes how much excess return is generated for extra volatility of holding an asset

Investment risk:

All investments involve risks including possible loss of principal. The following are some general risks associated with various asset classes mentioned on this website. This is not an all-inclusive list. Each specific investment approach and product will have its own specific risks and risks will vary.

Alternatives risks — Alternative investments tend to use leverage, which can serve to magnify potential losses. Additionally, they can be subject to increased illiquidity, volatility and counterparty risks, among other risks.

Asset/Mortgage-backed securities risk — Mortgage-related and asset-backed securities are subject to prepayment risk, which is the possibility that the principal of the loans underlying the securities may prepay differently than anticipated at purchase. Because of prepayment risk, the duration of mortgage-related and asset-backed securities may be difficult to predict.

Below investment grade risks — Lower-rated securities have a significantly greater risk of default in payments of interest and/or principal than the risk of default for investment-grade securities. The secondary market for lower-rated securities is typically much less liquid than the market for

investment-grade securities, frequently with significantly more volatile prices and larger spreads between bid and asked price in trading.

Capital risk — Investment markets are subject to economic, regulatory, market sentiment, and political risks. All investors should consider the risks that may impact their capital, before investing. The value of your investment may become worth more or less than at the time of the original investment.

Commodities risk — Exposure to the commodities markets may be more volatile than investments in traditional equity or fixed income securities. The value of commodity-linked derivative instruments may be affected by changes in overall market movements, commodity index volatility, interest-rate changes, or events affecting a particular commodity or industry.

Common stock risk — Common stock are subject to many factors, including economic conditions, government regulations, market sentiment, local and international political events, and environmental and technological issues as well as the profitability and viability of the individual company. Equity security prices may decline as a result of adverse changes in these factors, and there is no assurance that a portfolio manager will be able to predict these changes. Some equity markets are more volatile than others and may present higher risks of loss. Common stock represents an equity or ownership interest in an issuer.

Concentration risk — Concentration of investments in a relatively small number of securities, sectors or industries, or geographical regions may significantly affect performance.

Credit risk — The value of fixed income security may decline, or the issuer or guarantor of that security may fail to pay interest or principal when due, as a result of adverse changes to the issuer's or guarantor's financial status and/or business. In general, lower-rated securities carry a greater degree of credit risk than higher-rated securities.

Currency risk — Investments in currencies, currency derivatives, or similar instruments, as well as in securities that are denominated in foreign currency, are subject to the risk that the value of a particular currency will change in relation to one or more other currencies.

Emerging markets risks — Investments in emerging and frontier countries may present risks such as changes in currency exchange rates; less liquid markets and less available information; less government supervision of exchanges, brokers and issuers; increased social, economic and political uncertainty; and greater price volatility. These risks are likely significantly greater relative to developed markets.

Equity market risks — Equity markets are subject to many factors, including economic conditions, government regulations, market sentiment, local and international political events, and environmental and technological issues.

Fixed income securities market risks — Fixed income securities markets are subject to many factors, including economic conditions, government regulations, market sentiment, and local and international political events. In addition, the market value of fixed income securities will fluctuate in response to changes in interest rates, currency values, and the creditworthiness of the issuer.

Foreign and emerging markets risk — Investments in foreign markets may present risks not typically associated with domestic markets. These risks may include changes in currency exchange rates; less-liquid markets and less available information; less government supervision of exchanges, brokers, and issuers; increased social, economic, and political uncertainty; and greater price volatility. These risks may be greater in emerging markets, which may also entail different risks from developed markets.

Hedging risk — Any hedging strategy using derivatives may not achieve a perfect hedge.

Interest-rate risk — Generally, the value of fixed income securities will change inversely with changes in interest rates. The risk that changes in interest rates will adversely affect investments will be greater for longer-term fixed income securities than for shorter-term fixed income securities.

Issuer-specific risk — A security issued by a particular issuer may be impacted by factors that are unique to that issuer and thus may cause that security's return to differ from that of the market.

Leverage risk — Use of leverage exposes the portfolio to a higher degree of additional risk, including (i) greater losses from investments than would otherwise have been the case had leverage not been used to make the investments, (ii) margin calls that may force premature liquidations of investment positions.

Operational risk

The ratios described above are all built on certain assumptions, including that volatility equal's risk. These ratios all derive risk measures based on quantitative factors; however, they do not consider qualitative factors, including the investment manager's internal controls, design and implementation of its systems, and oversight of its employees. This is operational risk.

Human error makes operational risk unpredictable. Many investors may assume that human errors are prevented by the managers' systems and controls, but that is not always the case. Consider the following situations:

- You hire Manager A to manage a large cap equity portfolio, and instead, Manager A finds better opportunities in the small caps and rationalizes investing your portfolio in small caps in the interest of earning you a better return. This guideline violation results in your portfolio being overweighted in small caps and minimizes your exposure to large caps.
- Manager B was recently examined by the Securities and Exchange Commission (SEC) and the SEC concluded that Manager B's compliance program was wholly inadequate.

- Manager C has a trader with inappropriate access rights to override controls in the compliance system. The trader executes trades that are in violation of the investment guidelines and conceals these through the inappropriate access rights so these securities are not identified as investment guideline violations.

These examples are real. While some of these risks may be identified in the risk measures described previously, many go undetected until disaster strikes and losses pile up.

Types of operational risk:

The types of risks involved in various business practices can be broadly categorized. Here are 5 categories commonly used to break out different types of risk.

1. Process risk

These risks are related to the efficiency and effectiveness of internal processes. For example, errors or delays in processing transactions, inadequate procedures for handling customer complaints, supply chain breakdowns or failures in internal controls.

To avoid process risks, organizations can improve workflows by introducing automation powered by artificial intelligence (AI) to reduce the chances of slowdowns, outages and shortages. Documentation of processes can also help senior management to see where improvements can be made.

2. People risk

This encompasses risks associated with employees, such as a deficiency in human resources, or any kind of human error, fraud or misconduct. Examples include:

- unauthorized trading by employees (internal fraud)
- vendor breach of contract (external fraud)
- errors in data entry
- workplace accidents
- Failure to comply with regulatory requirements due to lack of training.

To mitigate people risks, companies take steps to bring a sufficient quantity of highly skilled, well-trained and ethical people and arrange them within the organization in such a way as to facilitate successful collaborations in an environment characterized by workplace safety.

3. Systems risk

Sometimes called “technology risk,” this refers to risks stemming from the use of technology and systems within an organization. Risk events might include bugs, system failures, cyberattacks or other cybersecurity failures, data breaches or inadequate IT infrastructure.

Systems can break down or be compromised in innumerable ways, and it's up to chief technology officers (CTOs), chief information officers (CIOs), chief data officers (CDOs), and IT managers to help ensure that systems are safe, secure and running smoothly.

4. Financial risk

Financial risk encompasses the risk of financial loss from financial decision-making, such as insufficient cash flow to meet operational needs, bad investments or the risk of partners failing to fulfill their financial obligations to the organization.

5. Strategic risk

This is a catch-all term used to describe any business risk resulting from strategic initiatives. Mergers and acquisitions, new product offerings and branding changes, all of these business decisions involve some element of risk.

Operational Risk Management:

Operational Risk Management (ORM) is a systematic, comprehensive framework for identifying, assessing, and controlling risks that could impair an organization's ability to achieve its objectives.

Unlike traditional risk management approaches that focus primarily on financial or market risks, ORM addresses the full spectrum of operational vulnerabilities that organizations face in their daily activities.

The Evolution of Operational Risk Management

The concept of operational risk management has evolved significantly over the past decades.

Initially focused primarily on preventing fraud and ensuring basic operational continuity, modern ORM has transformed into a sophisticated discipline that leverages advanced technologies and data analytics.

Historical Development:

1990s: Early focus on basic operational controls and fraud prevention

2000s: Introduction of Basel II framework and formal ORM requirements

2010s: Integration of technology and data-driven approaches

Present: Emergence of AI-powered risk analytics and predictive modeling

Today's operational risk management model incorporates:

Advanced Analytics: Machine learning algorithms for risk prediction

Real-time Monitoring: Continuous assessment of risk indicators

Integrated Frameworks: Holistic approach to risk management

Automated Controls: Technology-enabled risk mitigation

The regulatory industry has also shaped ORM's evolution, with frameworks like Basel III and various industry-specific regulations requiring organizations to maintain robust operational risk management programs.

These regulatory influences have led to standardized approaches while allowing flexibility for organization-specific adaptations.

The Operational Risk Management Framework

A robust operational risk management framework serves as the foundation for effectively managing and mitigating operational risks across an organization.

This structured approach ensures consistency in risk identification, assessment, and control while enabling organizations to maintain regulatory compliance and optimize business performance.

Operational Risk Management Framework

Components of Operational Risk Management (ORM)

The operational risk management framework consists of several interconnected components that work together to create a comprehensive risk management solution:

Governance Structure

- Board oversight and senior management commitment
- Clear roles and responsibilities
- Risk committees and reporting lines
- Independent risk management function

Policies and Procedures

- Documented risk management policies
- Standard operating procedures
- Control documentation
- Escalation protocols

Risk Assessment Methodology

- Risk identification techniques
- Risk scoring and prioritization methods
- Impact and likelihood assessment

- Risk appetite and tolerance levels

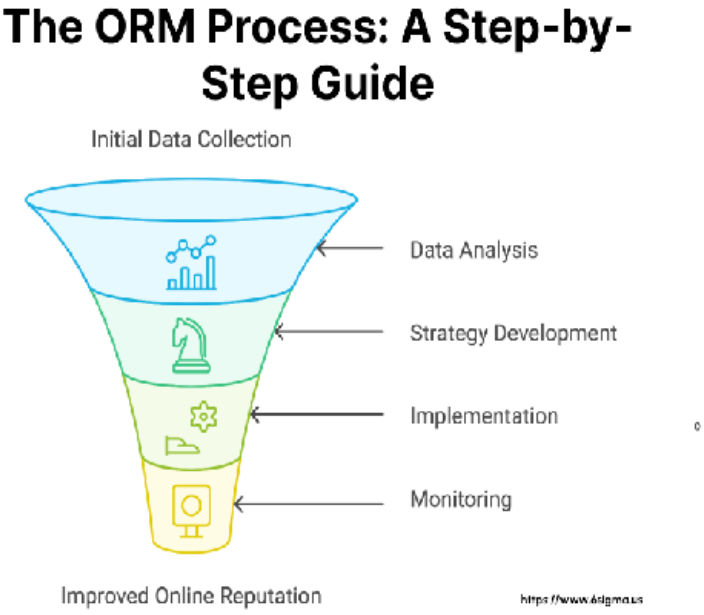
Reporting Mechanisms

- Regular risk reporting schedules
- Key Risk Indicators (KRIs)
- Dashboard development
- Stakeholder communication protocols

The Operational Risk Management (ORM) Process: A Step-by-Step Guide

The operational risk management process follows a structured approach that enables organizations to systematically identify, assess, mitigate, and monitor risks.

This comprehensive guide breaks down each step of the process, providing practical insights and implementation strategies.



Measurement of Liquidity Risk:

Liquidity Ratios:

Liquidity ratios, such as the liquidity coverage ratio (LCR) and the net stable funding ratio (NSFR), are key metrics for measuring liquidity risk. LCR assesses the bank's ability to meet short-term liquidity needs, while NSFR focuses on the stability of funding sources.

Cash Flow Projections:

Banks use cash flow projections to estimate future cash inflows and outflows. This helps in quantifying potential liquidity gaps and managing liquidity risk effectively.

Scenario Analysis:

Scenario analysis involves modeling various market conditions and assessing their impact on liquidity. Banks analyze different scenarios to determine the potential severity of liquidity risk.

Measuring Liquidity Risk

Liquidity ratios, such as the current ratio and quick ratio, can be used as an indicator of a company's funding liquidity risk. The current ratio, the most common ratio used to measure such a risk, is shown below:

$$\text{Current Ratio} = \frac{\text{Current Assets}}{\text{Current Liabilities}}$$

Where:

- **Current Assets** are assets that are expected to be converted into cash within a year.
- **Current Liabilities** are liabilities that are expected to be due within a year.

Additional ratios, such as the interest coverage ratio, debt to gross cash flows, quick ratio, etc., should be used to provide a better picture of a company's funding liquidity risk.

What is Funding Liquidity Risk?

Funding liquidity risk refers to the risk that a company will not be able to meet its short-term financial obligations when due. In other words, funding liquidity risk is the risk that a company will not be able to settle its current outstanding bills.

Understanding Liquidity

Liquidity is defined as the ability to meet immediate and short-term obligations (within a year). As such, funding liquidity risk is the risk that a company is unable to meet its immediate and short-term obligations in a timely manner.

This risk is a major concern for cyclical companies where operating cash flows and debt obligation due dates might not match up perfectly. For example, a company may experience a season of strong performance followed by a season of weak performance. During the period of slowdown, the company may be exposed to funding liquidity risk if the obligations due during that time are greater than the operating cash flows generated. This can be illustrated below:

Period	Q1 2020	Q2 2020	Q3 2020	Q4 2020
Operating Cash Flows	$3 million	$3 million	$0.5 million	$0.5 million
Debt Obligations Due	$2 million	$2 million	$2 million	$2 million
Funding Liquidity Risk?	Unlikely	Unlikely	Likely	Likely

In Q3 2020 and Q4 2020, the company may not be able to generate enough cash flows (assuming that they do not keep a cash reserve) to satisfy its debt obligations.

When a company incurs a funding liquidity risk, it faces the potential of having to liquidate capital assets (or other operating assets) at a price lower than the market price to satisfy its debt obligations. Selling operating assets could result in severe repercussions on the future revenue generation capabilities of the company.

Liquidity gap:

Liquidity gap is a term used in several types of financial situations to describe a discrepancy or mismatch in the supply or demand for a security or the maturity dates of securities. Banks deal with liquidity risks and potential liquidity gaps to the extent that they need to make sure they have enough cash on hand at all times to meet requests for funds.

Understanding a Liquidity Gap:

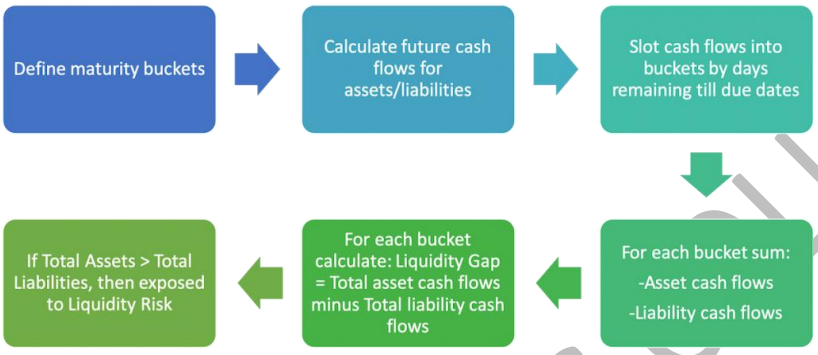
A firm might also experience a liquidity gap when they don't have enough cash on hand to meet operational needs and have assets and liabilities maturing at different times. Liquidity gaps can also occur in the markets when there is an insufficient number of investors to take the opposite side of a trade, and people who are looking to sell their securities are unable to do so.

For banks, the liquidity gap can change over the course of a day as deposits and withdrawals are made. This means that the liquidity gap is more of a quick snapshot of a firm's risk, rather than a figure that can be worked over for a long period of time. To compare periods of time, banks calculate the marginal gap, which is the difference between gaps of different periods.

During the early months of the global financial crisis, some bond and structured product investors found they could not sell their investments. There was a liquidity gap in that there weren't parties that were willing to take the other side of the trade and purchase the securities at depressed prices. This lack of liquidity caused markets in some securities to dry up for several weeks.

Liquidity gap Analysis:

Asset Liability Management (ALM) includes effective Liquidity Management. One way of assessing a bank's exposure to liquidity risk is to consider the gaps that exist between its assets and liabilities for pre-defined time buckets, and then calculate the cost incurred to close out those gaps. We describe the Cost-to-Close Liquidity Gap methodology in the post below.



How to calculate Liquidity Gap:

Assets represent outflows of cash whereas liabilities represent inflows of cash. When assets exceed liabilities there is a deficit of funds which could expose the financial institution to liquidity risk. To fill the gap (net cash outflow) and remain liquid the bank will seek funding from the market.

Let us take a simple example to illustrate this situation. Today, Alan deposits an amount of USD 300 with Bank Big for a period of 3 months. Bank Big then lends this USD 300 to Clint for 6 months. Let us assume that there are no further transactions. Bank Big's liquidity gap report as of today will look as follows:

For the time bucket 'Up to 3 months', there is a negative liquidity gap, where liabilities exceed assets. This represents an excess of funds. Bank Big has a net cash inflow, therefore, it has no exposure to liquidity risk.

However in the next time bucket, Bank Big has a positive liquidity gap. This indicates that Bank Big has liquidity risk exposure. It is deficient in funds due to cash outflows exceeding cash inflows during this period. In order to compensate for this lack of liquidity the bank would need to fund the gap from the market either by decreasing its assets e.g. by selling off assets and/ or increasing its liabilities e.g. by borrowing from the market.

One measure of liquidity risk is the cost to close gap analysis. This analysis assumes that we do this by filling the positive gaps by borrowing from the market. The first step in this analysis is the definition of time buckets. Let us assume that the following time buckets have been defined:

- Up to 1 month (0.83 years)

- 1 month -3 months (0.25 years)
- 3 months – 6 months (0.50 years)
- 6 months – 9 months (0.75 years)
- 9 months -12 months (1 year)
- 3 years (3 years)
- 5 years (5 years)

The figures in brackets represent the upper bounds of the time intervals expressed in years. They are used in calculating the cost to close measure as explained later.

After this, we group all of the bank's assets and liabilities into these time buckets according to the receipt or payment day of the cash flow, i.e. we consider the assets or liability's maturity or due date as opposed to its re-pricing date. This involves first calculating each future cash flow/ instalment going forward for each individual asset/ liability and then slotting each of these amounts into the relevant time buckets depending on when their expected payment or received dates. The same process, depending on the extent of the analysis, also applies to off-balance sheet items and non-funded exposures.

After slotting each individual asset and liability future cash flow into the appropriate bucket, we sum the asset values for each bucket first across each asset category (e.g. advances) and second across the asset portfolio. In the same manner, we sum the liabilities values for each bucket first across each asset category (e.g. deposits) and second across the liability portfolio.

We then calculate the difference between the total assets and liabilities for each time bucket. This difference represents the liquidity gap. A negative difference i.e. liabilities exceed assets indicate an excess of funds and could potentially be a source of interest rate risk to the bank as interest revenues (from the investment of these excess funds) could be adversely affected by movements in the interest rates. A positive difference, i.e. assets exceed liabilities indicates deficient funds which are a source of liquidity risk for the bank as the bank has a net cash outflow for that time bucket.

In this post, we reviewed a measure for assessing a bank's liquidity risk, namely the Cost-to-Close Liquidity Gap technique. In the following post, we will present a simple example illustrating this methodology.

Stress Testing:

Stress Testing Applications in Various Industries:

Stress testing is used in many industries to check the strength and reliability of systems and products. In engineering and manufacturing, stress testing finds out the limits of materials and components. This involves putting materials under high pressure, temperature, or mechanical strain to find breaking points and ensure they meet safety standards.

Software stress testing involves pushing applications to their limits by simulating high traffic, processing large amounts of data, or running the software for extended periods to identify potential failure points. This type of testing helps developers ensure that applications can handle real-world demands such as high user loads during peak usage times without crashing or slowing down.

In healthcare, stress testing can take on a more literal meaning. Medical stress tests, such as those used in cardiology, involve placing the human body under physical stress to monitor how the heart and other systems respond. This type of testing is used to diagnose diseases. By monitoring the body's response to stress, healthcare providers can make informed decisions about patient care and treatment plans.

Financial Institutions Use Stress Testing:

Asset management companies use stress testing to identify portfolio risk and set hedging strategies to prevent losses. Specifically, their portfolio managers use internal proprietary stress-testing programs to evaluate how well the assets they manage might weather certain market occurrences and external events.

Asset and liability matching stress tests are widely used, too, by companies that want to ensure they have the proper internal controls and procedures in place. Retirement and insurance

portfolios are also frequently stress-tested to ensure that cash flow, payout levels, and other measures are well aligned.

Exploring Different Stress Testing Techniques:

Stress testing involves running simulations to identify hidden vulnerabilities. The literature about business strategy and corporate governance identifies several approaches to these exercises. Among the most popular are stylized scenarios, hypotheticals, and historical scenarios.

Historical Stress Testing:

In a historical scenario, the business—or asset class, portfolio, or individual investment—is run through a simulation based on a previous crisis. Examples of historical crises include the stock market crash of October 1987, the Asian crisis of 1997, and the tech bubble that burst in 1999-2000.

Hypothetical Stress Testing:

A hypothetical stress test is generally more specific, often focusing on how a particular company might weather a particular crisis. For example, a firm in California might stress-test against a hypothetical earthquake or an oil company might do so against the outbreak of war in the Middle East.

Stylized scenarios are a little more scientific in the sense that only one or a few test variables are adjusted at once. For example, the stress test might involve the Dow Jones index losing 10% of its value in a week.

Simulated Stress Testing:

As for the methodology for stress tests, Monte Carlo simulation is one of the most widely known. This type of stress testing can be used for modeling probabilities of various outcomes given specific variables. Factors considered in the Monte Carlo simulation, for example, often include various economic variables.

Expected Future Funding Requirements:

Determining future funding needs involves a systematic approach to financial planning, usually covering the next three to five years.

Project Sales and Revenue: Start by forecasting future income from all sources. Base these projections on market research, industry trends, and historical data if available, making them realistic rather than overly optimistic.

Estimate Expenses: Detail all anticipated operating expenses, including salaries, rent, marketing, raw materials, and any one-time costs like new equipment or legal fees. Include a contingency buffer for unexpected challenges.

Create Financial Statements: Use your sales and expense data to prepare key financial documents:

Cash Flow Projections: This critical document forecasts the timing of cash inflows and outflows on a monthly basis for the first year, then quarterly or annually after that. It helps identify potential cash shortfalls and ensures liquidity for daily operations.

Income (Profit and Loss) Statement: This projects revenue, costs, and expenses over a period to show anticipated profitability.

Balance Sheet Projections: This estimates the future financial position, including assets, liabilities, and equity.

Identify Milestones and Growth Needs: Align funding requirements with specific business milestones, such as launching a new product, entering a new market, or a major recruitment drive. The funding request should specify how the capital will be used to drive growth.

Calculate the Funding Gap: Compare your projected internal cash flow and existing resources to the total capital needed to reach your milestones. The difference is your expected future funding requirement.

Outline the Funding Plan: Specify the nature of the funding needed (e.g., short-term loan, equity investment, and grant) and the intended sources (e.g., banks, venture capitalists, government schemes). This plan builds confidence with potential investors or lenders by demonstrating a clear strategic vision.

UNIT – V

Enterprise Wide Risk Management and Risk Reporting

What Does ERM Mean?

Enterprise risk management (ERM) is a business process that involves the identification of potential risks and proactively taking steps to prevent them from happening — or minimize the effects of risks on the business in case they do happen.

Business risks come in many different forms, and the ERM process is essentially an ongoing process with methods that address the potential events that represent risks to the accomplishments of a business.

Enterprise risk management will often comprise holistic and strategic plans that take into account every part of an enterprise. Rather than approach potential business risks within an organization separately in each individual department, ERM takes a holistic approach to addressing risks from the management level and includes every part of the enterprise.

Being a risk-based approach to managing a business, ERM focuses on all forms of business risks, including financial, economic, legal compliance, security and fraud, operational, competitive reputational and publicity, strategic, etc. This ensures that the capital, earnings, assets, and interests of the business stakeholders, including owners, investors, employees, customers, are protected.

ENTERPRISE WIDE RISK MANAGEMENT

Introduction:

Achievement of business and financial objectives is of paramount importance for a Bank or a Financial Services Organisation. The Top Managements of Banks and Financial Services Organisations are always under pressure to perform and to achieve their business targets. When periodical reviews are undertaken, related questions surface. Some such questions could be "What sort of roadblocks they can face on their way to achievement of their business goals? What are the risk-factors faced by the organisation? To what extent, can these risk-factors impact the achievement of the business objectives? How can these risk factors be mitigated? How to regularly control and monitor the risk-factors? " etc.

Enterprise-Wide Risk Management (EWRM) provides an answer to such questions. We can define EWRM as a continuous and structured process of identifying all external and internal risk-factors; assessing their impact on the achievement of the organisation's business and financial targets; prioritising the risk-factors; exploring alternatives for mitigating the risks; and controlling and monitoring such risks.

Thus, we may say that EWRM encompasses the entire gamut of the organisation's operations and is not limited to a single event or circumstance impacting the organisation's functioning. It is a dynamic process involving people at all levels, covers every aspect of the organisation's resources and operations and takes a holistic picture of the entire organisation for the purpose of risk management.

Implementation of Enterprise Wide Risk Management:

EWRM involves listing the objectives of the organisation; identifying the risk-factors that could adversely impact the achievement of each of the objectives; assessing the impact of the risk-factors on the achievement of each of the objectives; finding alternatives for mitigating the risk-factors and take steps to control and monitor the risk-factors on a regular basis..

Let us illustrate the enterprise wide risk management by taking the example of a Bank which has an objective to achieve an increase of 25% in its market share of deposits in 2017-18. The Bank has identified one of the risk-factors that could have an adverse impact on its projected growth is shortage of a well-trained marketing team at its branches. The Top Management of the Bank realises that if it does not have a well-trained team in place, it would at best achieve a deposit growth of 10%, which is almost the same as the previous year's deposit growth. This shows that "untrained marketing team" is a major risk-factor. There could be other risk-factors too, like competition from other Banks, competition from mutual funds, reduction in interest rates and lack of brand awareness.

Now let us explore a few risk-mitigating options for "untrained marketing team".

The options could be:

- Train the existing marketing team
- Hire well-trained personnel from the market
- Use a mix of the two

For each of the above available choices, the Bank shall have to carry out a cost-benefit analysis before deciding on a particular course of action.

The implementation of EWRM therefore, involves the following steps:

1. Evaluation of the existing risk management systems involving

   a. Review of the internal environment with a view to assess the risk philosophy and risk culture

   b. Review of the process of setting objectives

   c. Assessment of the existing mechanism of identifying risk-factors that can affect achievement of the desired objectives

   d. Evaluation of the existing process of assessing risks

   e. Assessment of the process of responding to identified risks

   f. Evaluation of the adequacy of existing control processes

   g. Assessment of the adequacy of existing management information system (MIS)

   h. Review of the process of monitoring risks

2. Formulation of a road map for the implementation plan that seeks to bridge the gaps in risk management practices vis-à-vis EWRM.

ERM COMMITTEES:

Institutions with enterprise risk management (ERM) programs often use an ERM committee to collaboratively manage the process. The committee is comprised of key leaders from across the institution who regularly come together to advance the enterprise-wide risk management process. This cross-collaboration helps ensure a coordinated and visible approach to managing risks, making it likelier that risk management stays an institutional priority and not a marginalized side project. Leaders overseeing your institution's ERM program can use this guide and tool to establish and scope your ERM committee's responsibilities. Also, leaders can use this tool to identify strategies for involving others in your institution's risk management efforts without compromising your committee's size.

1. Select A Chairperson to Lead ERM Efforts:

Committees need a clear owner to champion ERM efforts and hold leaders accountable. Often an ERM committee chairperson oversees progress, maintains and updates key documents and reports, and manages any ERM technologies or processes. This leader likely will be your liaison to the senior administration and board.

In some cases, an institution may have a leader in mind for this role. When senior leaders are looking to identify a new ERM committee chair:

- Base your decision on a leader's skills, experience, and interest in risk management, not on a person's title or position at your institution.
- Ensure the leader has experience overseeing cross-functional efforts and moving strategic projects forward.
- Consider leaders with the ability to clearly communicate with the board and senior administration.

2. Identify Your ERM Committee Members:

All institutions are different, and your committee should reflect those differences. When forming a committee, important considerations include:

- Positional authority of members
- Departments of your institution that need representation
- Specific subject matter expertise, experience, or personality of leaders who participate.

Composition of Committee:

The Committee consists of members appointed by the positions listed below (for a maximum of three years); and ex-officio members. The committee makeup will take into account a multi campus model, principles of Equity, Diversity and Inclusion (EDI), Indigenization, and Academic and Administrative functions. There will be one vote per member. The committee shall consist of:

i. Vice-President (Administration, Finance and Advancement) (Chair)

ii. One member as appointed by the Provost and Vice-President (Academic)

iii. One member as appointed by the Vice-President (Grenfell Campus)

iv. One member as appointed by the Vice-President (Marine Institute)

v. One member as appointed by the Vice-President (Research)

vi. One member as appointed by the Vice-President (Indigenous)

vii. An Academic Dean as appointed by the Provost and Vice-President (Academic)

viii. Associate Vice President – Facilities Management

ix. Associate Vice President – People and Culture

x. Associate Vice President (Academic) Students Enterprise Risk Management Committee

xi. Chief Information Officer.

xii. Chief Financial Officer.

xiii. Chief Operating Officer – Faculty of Medicine.

xiv. University Registrar.

xv. Executive Director – Marketing and Communications

xvi. Manager, Enterprise Risk Additional resources may attend and provide advice or guidance such as The Office of the General Counsel, The Office of Internal Audit, or other units as deemed necessary by the committee.

Committee Responsibilities:

The ERM Committee oversees the University's ERM framework, as per the Enterprise Risk Management policy.

The ERM Committee responsibilities include but are not limited to:

- Assist in the maturation of risk culture throughout all of Memorial University.
- Provide recommendations to PEC on the ERM Framework.
- Monitor the University Risk Profiles(s) and report (each semester) to PEC on changing and/or emerging risks.
- Develop and provide guidance on University Risk Appetite and Tolerance in relation to the ERM Framework and identified Risks.
- Examine business processes where risk assessments are/or should be conducted on a regular basis, and provide recommendations on where risks assessments can be integrated (budget, briefing notes);

- Receive an annual review of ERM governing documents and training materials and provide feedback.

RISK MANAGEMENT DEPARTMENT:

The Risk Management Department of NABARD was set up on June 2, 2014 to function as the Nodal Department to handle all types of risks in NABARD, including:

- Credit Risk
- Market Risk
- Operational Risk
- Compliance Risk
- IT Risk/Security

Core functions of the Department

- Placement of a sound risk management framework in the Bank;
- Formulation and revision of the 'Enterprise Risk Management Policy' and other critical risk management related policies of NABARD;
- Identification and diagnosis of Credit Risks in NABARD through introduction of proper policies, systems, standard operating procedures, risk rating tools/models, stress testing, exposure limits, and forecast mechanisms;
- Management of Market Risks within acceptable level;
- Execution of functions relating to Operational Risk and Compliance Risk in NABARD;
- Coordination with the Government of India, the Reserve Bank of India, and rating agencies on risk-related matters;
- Apprising the Top management and Risk Management Committee of the Board regarding the status of enterprise level risks, the risk mitigation systems in place, etc;
- Framing policies and frameworks for compliance of BASEL III guidelines;

Broad Achievements

- Comprehensive 'Enterprise Risk Management Policy' put in place;
- Enterprise Risk Management framework implemented through ERMS software as a risk monitoring system;
- ICAAP policy and stress testing policy to ensure compliance with BASEL III guidelines;
- Regular ALCO (Asset Liability Committee) Meetings addressing Market Risk related issues conducted;

- Internal Risk Rating Models introduced for various clients and reviewed periodically;
- RCSA framework implemented through development of software to capture Operational Risk events;
- Introduction of guidelines relating to non-performing asset (NPA) management, client-specific exposure norms and guidelines for debarring of NGOs/other agencies by NABARD;
- Major Operational Risks and incidents identified and risk mitigation systems put in place;
- Risk vetting of the policies of NABARD;
- Comprehensive Enterprise wide Business Continuity Management Plan put in place;
- Implementation of Compliance Risk monitoring system;
- Creating Risk awareness culture across the organisation;
- Capacity building of NABARD staff through regular interaction with stakeholders;

RISK BASED INTERNAL AUDIT:

A risk-based audit approach starts with a risk universe as the basis for the audit plan. In a risk-based audit approach, the goal of the project is to address management's highest-priority risks. Many audit departments think they are risk-based, but their audit plans are generally built from an audit universe consisting of departments, functions, or processes. A true risk-based audit approach starts with an assessment of management's top risks and business objectives. All of the audits on the plan are designed to address those risks and provide insights back to senior management.

Risk-based audit plans rely on establishing the organization's risk appetite, defining inherent risks facing the organization, and focusing on high-risk business processes. An organization may opt to undergo a formal risk assessment, ideally at least once each year. Many common risk management frameworks require companies to perform regular risk assessments as a best practice. Once risk identification has taken place, evaluations performed for each line item generate mitigation plans for each potential risk exposure, allowing the business to address those risk areas. In applying a risk-based approach to auditing, organizations seek to mitigate key risks and implement risk management processes and controls to protect the business from internal and external risks.

Risk Based Internal Audit Planning:

The Internal Auditor needs to plan the audit to be performed, well before the commencement of the audit. It should include the scope of the audit, personnel and time required.

Audit plan is a bird's eye-view, as it provides full information regarding the areas of work to be performed, delegation of work among the personnel.

It needs to be comprehensive and definitive to ensure that non-value-added activities are eliminated.

It should be formulated in a cost and within a stipulated time. Internal auditor should, in consultation with those responsible for governance, including the audit committee, develop a each internal audit engagement to help him conduct the efficient and timely manner.

The internal audit plan, which should be approved by the audit committee, should be based on risk assessment as well as on issues hi audit committee and senior management.

The risk assessment should be of a continuous nature to identify not only risks, but also emerging risks.

The internal auditor should work plan by aligning it with the objectives and risks of concentrate on those issues where assurance is sought.

Benefits of Risk-Based Audit (RBA)

1. Auditor can easily justify the work carried out by him with complete details & reason. No oversight or negligence can be alleged on the auditor and it is a systematic approach which saves time & efforts.

2. It eliminates over auditing or under auditing and helps auditor to identify & prove the high-risk/low risk areas. Audit report should be prepared for highlighting the irregularities as per the risk involved.

3. improves the understanding of critical areas, thus preventive & corrective action can be suggested by the internal auditor.

4. RBA improves understanding of vulnerability & leads to better decision-making.

Disadvantages of Risk-Based Audit:

It is proved to generate an excessive number of false alarms which may overwhelming impact on management thereby diluting their focus. Lack of contextual information in the alerts may generate complexities & lack of differentiation between actual threat & false alarms. It may also be expensive & not suitable for small units. Uncertain in standards. Disruption in smooth functioning.

Risk based audit may highlight a problem without any bearing on finding a solution, for example, there are leakages in revenue is high risk due to lack of data analysis in trend & pattern of recovery. However, way to recovery may be totally elusive unless payment processes are rectified.

Types of Risks in Accounting

1. Operational Risks

Operational risks stem from everyday business processes, such as inaccurate financial reporting or data mismanagement. Inefficient workflows, lack of process documentation, and outdated

technology can increase these risks. For example, delayed payments could damage client relationships and lead to compliance issues if you fail to automate payroll processing.

2. Financial Risks

Financial risks involve cash flow issues, poor credit management, and bad investment decisions. Your firm may face insolvency, reduced profitability, or financial instability without proper risk management. For instance, neglecting to assess a client's creditworthiness could result in bad debt write-offs, straining your firm's cash flow.

3. Compliance Risks

Failure to comply with regulations, tax codes, and industry standards can put your firm at risk. Common compliance issues include incorrect tax filings, non-adherence to GAAP, and missed regulatory deadlines. Non-compliance can lead to hefty fines, audits, or even the suspension of your firm's license.

4. Cyber security Risks

Cyber threats like data breaches, phishing scams, and ransom ware attacks can jeopardize your firm's sensitive financial data. For example, if cybercriminals infiltrate your systems, they could lock crucial client records, forcing you to pay a ransom or risk losing valuable data. In 2024, the average cost of data breaches was estimated to be $4.88m. Implementing robust cyber security measures is essential to protecting your firm and clients.

5. File Sharing Risks

Improper file-sharing practices can expose confidential client data to unauthorized access, cyber threats, or accidental leaks. Using unsecured email attachments, public cloud storage, or outdated file-sharing methods increases the likelihood of data breaches and regulatory violations. For example, sending financial statements via unencrypted email makes them vulnerable to interception by hackers. To mitigate this risk, firms should use secure accounting file-sharing solutions with access controls, encryption, and audit trails to ensure data security and compliance.

Benefits of Proactive Risk Management in Accounting

A well-executed risk management strategy strengthens your firm's operations, minimizes financial risks, and enhances client confidence. By identifying potential threats early and implementing preventive measures, you create a stable and secure foundation for long-term success.

Reduced Financial Exposure

Proactively identifying and mitigating risks helps prevent costly errors, fraud, and financial setbacks that could impact your firm's profitability. For example, catching discrepancies in financial reports early can prevent regulatory fines or client disputes. By implementing strong internal controls and audit procedures, you can safeguard your firm against losses and ensure long-term financial stability.

Better Decision-Making

A data-driven risk management approach provides valuable insights that help you make well-informed financial and business decisions. By continuously assessing risks related to cash flow, compliance, and cybersecurity, you can proactively adjust strategies to avoid potential pitfalls. Access to real-time risk analytics allows you to forecast trends, allocate resources more effectively, and develop strategic plans with greater confidence.

Stronger Client Relationships

Clients rely on accounting firms to protect their sensitive financial data, maintain compliance, and ensure the accuracy of financial reports. A firm that prioritizes risk management demonstrates reliability, professionalism, and a commitment to safeguarding client interests. By implementing rigorous security protocols and compliance measures, you build trust.

COMPONENTS OF TAX RISK MANAGEMENT

1. Identification of Tax Risks

Organizations must identify potential tax risks within their operations and transactions. Regulatory Changes: Modifications in tax legislation or interpretations that affect tax liabilities and compliance obligations. Tax implications related to international operations, such as transfer pricing, withholding taxes, and indirect taxes. The use of intricate organizational structures or financial transactions that may attract scrutiny from tax authorities. Risks stemming from accounting practices, like improper documentation or inadequate record-keeping.

2. Assessment of Tax Risks

After identifying risks, organizations need to assess the likelihood and potential impact of each risk. Estimating the potential financial repercussions of non-compliance or tax errors. Evaluating the probability that a tax risk could materialize based on internal and external factors.

3. Mitigation Strategies

Following the assessment, organizations should formulate strategies to mitigate identified risks. Strengthening Compliance Processes: Establishing robust tax compliance practices, including regular audits, internal controls, and meticulous record-keeping. Training and Education: Providing ongoing training for staff on tax regulations, compliance requirements, and best practices. Consulting tax professionals for guidance on complex tax issues and to ensure compliance with evolving laws. Creating clear tax policies that outline the procedures for tax reporting, compliance, and risk management within the organization.

4. Monitoring and Reporting

Continuous monitoring of tax risks is essential for adapting to changes in the regulatory environment. Businesses should regularly review and update their tax risk management strategies. Conducting regular evaluations of tax positions, compliance status, and risk

assessments. Ensuring that tax risks are consistently reported to senior management and the board, fostering a culture of accountability regarding tax compliance.

5. Crisis Management

In the event of a tax dispute or investigation, organizations should have a crisis management plan in place. Consult tax lawyers or advisors to navigate disputes and negotiate with tax authorities. Establish communication protocols for internal and external stakeholders, addressing potential reputational issues.

LEGAL RISK MANAGEMENT:

Legal risk management is a crucial aspect of running a business, yet it is often overlooked or not given the attention it deserves. Businesses face various legal risks, ranging from contract disputes to regulatory compliance issues, and managing these risks effectively can make the difference between success and failure. In this blog, we will explore the concept of risk management, its importance in the business landscape, and strategies businesses can implement to mitigate risks. Whether you are a small business owner or a corporate executive, understanding risk management is essential for protecting your business and ensuring its long-term success. So, let's dive in and explore the world of risk management.

The Role of Legal Risk in Business Strategy

Legal risk plays a pivotal role in the formulation of business strategy and the overall risk management framework. Integrating legal risk management into the business strategy allows companies to identify, assess, and mitigate risks effectively, minimizing the potential negative consequences.

Managing risks is essential in contract management, as the breach of contract can result in legal disputes, financial implications, and damaged business relationships. By understanding the risks associated with contracts, businesses can take proactive steps to prevent breaches and resolve any potential issues before they escalate.

Additionally, risk management is crucial in regulatory compliance. Businesses must navigate complex regulatory environments to ensure compliance with laws and regulations. Failing to do so can result in significant financial penalties, legal consequences, and reputational damage.

Incorporating risk management into the business strategy allows companies to develop robust compliance programs, identify regulatory risks, and implement appropriate risk mitigation strategies.

Moreover, legal risk management should be considered in the context of entity management, as risks can arise from the structure and operations of the business entity itself. Understanding the risks associated with the business's structure, such as liability and governance issues, enables the business to take necessary precautions and make informed decisions to protect its interests.

Types of Legal Risk

Understanding the different types of legal risks is the first step toward managing them effectively.

1. Regulatory Risk

This involves non-compliance with laws and regulations issued by governments, regulators, or industry bodies. It can also include adapting to legislative changes that impact operational policies.

2. Contractual Risk

Contractual risks arise when organizations fail to honor terms in agreements. Common causes include unclear contract language, mismanagement of clauses, and failure to meet obligations.

3. Extra contractual Risk

These risks occur outside the scope of formal agreements. For example:

Intellectual property violations by third parties.

Claims against the organization for consumer harm caused by products or services.

4. Compliance Risk

Similar to regulatory risks, compliance risks extend to internal policies and practices. Failing to follow internal protocols can lead to operational inefficiencies and reputational harm.

5. Litigation or Dispute Risk

Litigation risks involve legal disputes with customers, suppliers, or employees. Common scenarios include:

- Customer dissatisfaction with products or services.
- Employment disputes, such as wrongful termination claims.

6. Constitutional and Extinction Risks

These risks occur during significant business events:

- Constitutional Risks: Issues during company formation or mergers.

- Extinction Risks: Legal challenges during bankruptcy or liquidation.

Each of these risks underscores the necessity of incorporating governance, risk, and compliance (GRC) principles into organizational frameworks to proactively address vulnerabilities.

INDIAN ACCOUNTING STANDARDS (IND AS):

Objectives, Applicability, & List Indian Accounting Standards (IND AS) are a set of financial reporting standards harmonized with the International Financial Reporting Standards (IFRS) to enhance global accessibility and transparency for Indian companies. As Indian businesses expand their global reach, the convergence of local reporting practices with international standards has become essential. By adopting IND AS, companies in India improve the reliability of their financial statements, facilitating informed decision-making. These standards, issued by the Institute of Chartered Accountants of India (ICAI), ensure that Indian businesses comply with international norms, fostering trust and credibility in the global market. This article provides complete information on Indian Accounting Standards (IND AS).

Indian Accounting Standards (Ind AS) are IFRS-converged standards issued by the Central Government of India. They are developed under the supervision of the Accounting Standards Board (ASB) of the Institute of Chartered Accountants of India (ICAI) and in consultation with the National Financial Reporting Authority (NFRA). These standards are mandatory for certain Indian companies, ensuring their financial statements align with global practices. The ASB, established in 1977, oversees the formulation and implementation of Ind AS, making them the primary accounting standards adopted by companies in India. Objectives of Indian Accounting Standards The Indian Accounting Standards (IND AS) were introduced in India with the primary objective of aligning Indian accounting practices with international standards.

Objectives of Indian Accounting Standards:

Uniformity and Consistency: IND AS aims to establish a consistent framework for accounting practices across various industries and sectors in India. This uniformity ensures that financial statements are prepared using a common set of principles and methods, making them more comparable and understandable.

International Convergence: One of the primary goals of IND AS is to converge Indian accounting standards with International Financial Reporting Standards (IFRS). This convergence facilitates international trade, investment, and cross-border transactions.

Transparency and Accountability: IND AS promotes transparency in financial reporting by requiring companies to disclose relevant information about their financial performance, position, and cash flows. This transparency enhances accountability and helps stakeholders make informed decisions.

Reliability and Credibility: IND AS ensures that financial information is reliable and credible by providing a framework for the preparation of financial statements that reflect the economic substance of transactions and events. This enhances the credibility of financial reporting in India.

Investor Protection: IND AS aims to protect investors by providing them with reliable and comparable financial information. This helps investors make informed decisions about their investments.

Facilitation of Cross-Border Transactions: Convergence with IFRS facilitates cross-border transactions and investments by reducing the complexities associated with reconciling financial statements prepared under different accounting standards.

IAS 32:

IAS 32 outlines the accounting requirements for the presentation of financial instruments, particularly as to the classification of such instruments into financial assets, financial liabilities and equity instruments. The standard also provide guidance on the classification of related interest, dividends and gains/losses, and when financial assets and financial liabilities can be offset. IAS 32 was reissued in December 2003 and applies to annual periods beginning on or after 1 January 2005.

IAS 32 FINANCIAL INSTRUMENT:

A contract that gives rise to a financial asset of one entity and a financial liability or equity instrument of another entity.

Financial asset:

- cash
- an equity instrument of another entity
- a contractual right
- to receive cash or another financial asset from another entity; or
- to exchange financial assets or financial liabilities with another entity under conditions that are potentially favourable to the entity; or
- a contract that will or may be settled in the entity's own equity instruments and is:
- a non-derivative for which the entity is or may be obliged to receive a variable number of the entity's own equity instruments
- a derivative that will or may be settled other than by the exchange of a fixed amount of cash or another financial asset for a fixed number of the entity's own equity instruments. For this purpose the entity's own equity instruments do not include instruments that are themselves contracts for the future receipt or delivery of the entity's own equity instruments
- put table instruments classified as equity or certain liabilities arising on liquidation classified by IAS 32 as equity instruments

Financial liability:

- to deliver cash or another financial asset to another entity; or
- to exchange financial assets or financial liabilities with another entity under conditions that are potentially unfavourable to the entity; or
- a contract that will or may be settled in the entity's own equity instruments and is
- a non-derivative for which the entity is or may be obliged to deliver a variable number of the entity's own equity instruments or
- a derivative that will or may be settled other than by the exchange of a fixed amount of cash or another financial asset for a fixed number of the entity's own equity instruments. For this purpose the entity's own equity instruments do not include: instruments that are themselves contracts for the future receipt or delivery of the entity's own equity instruments; put table instruments classified as equity or certain liabilities arising on liquidation classified by IAS 32 as equity instruments

Fair value:

The amount for which an asset could be exchanged, or a liability settled, between knowledgeable, willing parties in an arm's length transaction.

The definition of financial instrument used in IAS 32 is the same as that in IAS 39.

Puttable instrument: a financial instrument that gives the holder the right to put the instrument back to the issuer for cash or another financial asset or is automatically put back to the issuer on occurrence of an uncertain future event or the death or retirement of the instrument holder.

Classification as liability or equity

The fundamental principle of IAS 32 is that a financial instrument should be classified as either a financial liability or an equity instrument according to the substance of the contract, not its legal form, and the definitions of financial liability and equity instrument. Two exceptions from this principle are certain put table instruments meeting specific criteria and certain obligations arising on liquidation (see below). The entity must make the decision at the time the instrument is initially recognised. The classification is not subsequently changed based on changed circumstances. [IAS 32.15]

A financial instrument is an equity instrument only if (a) the instrument includes no contractual obligation to deliver cash or another financial asset to another entity and (b) if the instrument will or may be settled in the issuer's own equity instruments, it is either:

- a non-derivative that includes no contractual obligation for the issuer to deliver a variable number of its own equity instruments; or

- A derivative that will be settled only by the issuer exchanging a fixed amount of cash or another financial asset for a fixed number of its own equity instruments. [IAS 32.16]

Illustration – preference shares

If an entity issues preference (preferred) shares that pay a fixed rate of dividend and that have a mandatory redemption feature at a future date, the substance is that they are a contractual obligation to deliver cash and, therefore, should be recognised as a liability. [IAS 32.18(a)] In contrast, preference shares that do not have a fixed maturity, and where the issuer does not have a contractual obligation to make any payment are equity. In this example even though both instruments are legally termed preference shares they have different contractual terms and one is a financial liability while the other is equity.

Illustration – issuance of fixed monetary amount of equity instruments

A contractual right or obligation to receive or deliver a number of its own shares or other equity instruments that varies so that the fair value of the entity's own equity instruments to be received or delivered equals the fixed monetary amount of the contractual right or obligation is a financial liability. [IAS 32.20]

Illustration – one party has a choice over how an instrument is settled

When a derivative financial instrument gives one party a choice over how it is settled (for instance, the issuer or the holder can choose settlement net in cash or by exchanging shares for cash), it is a financial asset or a financial liability unless all of the settlement alternatives would result in it being an equity instrument. [IAS 32.26]

Contingent settlement provisions

If, as a result of contingent settlement provisions, the issuer does not have an unconditional right to avoid settlement by delivery of cash or other financial instrument (or otherwise to settle in a way that it would be a financial liability) the instrument is a financial liability of the issuer, unless:

- the contingent settlement provision is not genuine or
- the issuer can only be required to settle the obligation in the event of the issuer's liquidation or
- the instrument has all the features and meets the conditions of IAS 32.16A and 16B for puttable instruments

IAS 39 FINANCIAL INSTRUMENTS:

IAS 39 was superseded by IFRS 9 subject to:

- the accounting policy choice about whether or not to continue applying the hedge accounting requirements in IAS 39 in accordance with paragraph 7.2.21 or paragraph 6.1.3 of IFRS 9; and

- the temporary exemption in paragraph 20A of IFRS 4 that provides a temporary exemption to some insurers from applying IFRS 9 until they apply IFRS 17.

IAS 39 establishes principles for recognising and measuring financial assets, financial liabilities and some contracts to buy or sell non-financial items. It also prescribes principles for derecognising financial instruments and for hedge accounting. The presentation and the disclosure of financial instruments are the subjects of IAS 32 and IFRS 7 respectively.

Recognition and Derecognition

A financial instrument is recognised in the financial statements when the entity becomes a party to the financial instrument contract. An entity removes a financial liability from its statement of financial position when its obligation is extinguished. An entity removes a financial asset from its statement of financial position when its contractual rights to the asset's cash flows expire; when it has transferred the asset and substantially all the risks and rewards of ownership; or when it has transferred the asset, and has retained some substantial risks and rewards of ownership, but the other party may sell the asset. The risks and rewards retained are recognised as an asset.

MEASUREMENT

A financial asset or financial liability is measured initially at fair value. Subsequent measurement depends on the category of financial instrument. Some categories are measured at amortised cost, and some at fair value. In limited circumstances other measurement bases apply, for example, certain financial guarantee contracts.

The following are measured at amortised cost:

- held to maturity investments—non-derivative financial assets that the entity has the positive intention and ability to hold to maturity;
- loans and receivables—non-derivative financial assets with fixed or determinable payments that are not quoted in an active market; and
- Financial liabilities that are not carried at fair value through profit or loss or otherwise required to be measured in accordance with another measurement basis.

The following are measured at fair value:

- Financial assets and financial liabilities held for trading—this category includes derivatives not designated as hedging instruments and financial assets and financial liabilities that the entity has designated for measurement at fair value. All changes in fair value are reported in profit or loss.
- Available for sale financial assets—all financial assets that do not fall within one of the other categories. These are measured at fair value. Unrealised changes in fair value are reported in other comprehensive income. Realised changes in fair value (from sale or impairment) are reported in profit or loss at the time of realisation.

IAS 39 sets out the conditions where special hedge accounting is permitted, and the procedures for doing hedge accounting.

IFRS 7 FINANCIAL INSTRUMENTS:

Disclosures (IFRS 7 or the Standard) in addition to discussing the main differences compared to the existing disclosure requirements for financial instruments. A comprehensive comparison between IFRS 7 and existing disclosure requirements is presented as an Appendix to this publication.

IFRS 7 incorporates the disclosures relating to financial instruments contained in IAS 32 Financial Instruments: Disclosure and Presentation1 and replaces IAS 30 Disclosures in the Financial Statements of Banks and Similar Financial Institutions, so that all financial instruments disclosures are located in a single Standard for all types of entities. The disclosure requirements contained in IFRS 7 are less prescriptive than those in IAS 30 for banks and there are no longer any bank-specific disclosure requirements.

All the disclosures required by IFRS 7, except for the risk disclosures, must be part of the financial statements with minimum disclosure requirements subject to the materiality requirements of IAS 1 Presentation of Financial Statements. The qualitative and quantitative risk disclosures required by IFRS 7 may be provided in the financial statements or incorporated by reference from the financial statements to another statement (eg, the management commentary or a risk report).

IFRS 7 introduces:

- Requirements for enhanced balance sheet and income statement disclosure 'by category' (eg, whether the instrument is available-for-sale or held-to-maturity)
- Information about any provisions against impaired assets
- Additional disclosure relating to the fair value of collateral and other credit enhancements used to manage credit risk
- Market risk sensitivity analyses.

Scope:

IFRS 7 applies to all risks arising from all financial instruments, including those instruments that are not recognised on-balance sheet. Consistent with IAS 30 and IAS 32, there is no scope exemption for subsidiaries or, as yet, for small- and medium-sized entities, but the IASB has agreed to consider this issue in its project on financial reporting for small- and medium-sized entities.

The application to subsidiaries may present a challenge to entities that are members of a consolidated group as they often manage risk on a consolidated basis. Furthermore, the requirement to provide the disclosure for each entity may provide limited value to users of

financial statements (compared to the cost of compilation) when the information is already disclosed at the group level.

IFRS 7 disclosures must be presented based on the accounting policies used for the financial statements prepared in accordance with IFRS, including consolidation adjustments. It is possible that the internal information made available to management for risk management purposes is not prepared using such accounting policies, in which case it will need to be amended. A good example is when hedging transactions are economically effective but do not qualify for hedge accounting.

Balance Sheet:

IFRS 7, as with IAS 32, does not prescribe the location of the required balance sheet disclosures. An entity is permitted to present the required disclosures either on the face of the balance sheet or in the notes to the financial statements. When the Standard requires disclosure by class of financial instrument, the entity shall group instruments in classes that are appropriate to the nature of the information disclosed and the characteristics of the instruments.

IFRS 7 requires additional detail in the disclosures for each category of financial instruments such as financial assets held at fair value through profit or loss or available-for-sale. In contrast, IAS 32 only requires separate disclosure of financial instruments carried at fair value through profit or loss, although the level of detail required by IFRS 7 is not as prescriptive as the requirements of IAS 30. The required core balance sheet disclosures for each category of financial assets and financial liabilities in IFRS 7 are similar to those in IAS 32 and include the carrying amount and related fair value, along with the amount and reason for any reclassifications between categories.

IFRS 9 - Financial Instruments:

IFRS 9 specifies how an entity should classify and measure financial assets, financial liabilities, and some contracts to buy or sell non-financial items. It addresses the accounting in three main topics: classification and measurement of financial instruments, impairment and hedge accounting.

IFRS 9 also requires an entity to recognize a financial asset or liability in its statement of financial position when it becomes party to the contractual provisions of the instrument (fair value plus or minus):

- measurement with a different mixture of amortized cost and fair value;
- impairment model, which consideration of macroeconomics and forecasts;
- Hedge accounting linking with risk management.

Failing to use IFRS 9 adequately could lead to profit warnings, delays in lodging financial statements, qualified audit reports and even a loss of investor confidence and sharp falls in share price.

Finally, IFRS 9 changes amounts reported in financial statements with knock on effects on bonuses or earn-outs, finance charges where interest rate margins are linked to key ratios, and breaches of bank covenants.

Statement of Financial Accounting Standard (SFAS)

Home » CMA Glossary Term » Financial Statements and Reporting » Statement of Financial Accounting Standard (SFAS)

The Statement of Financial Accounting Standard (SFAS) refers to a set of authoritative guidelines issued by the Financial Accounting Standards Board (FASB) to standardize financial accounting and reporting practices. SFAS meaning encompasses the principles and rules that govern the preparation of financial statements, ensuring consistency and transparency. These standards are integral to the development of Generally Accepted Accounting Principles (GAAP) in the United States.

FAS 133 accounting for derivative instruments and hedging activities:

After nearly becoming effective for fiscal years beginning after June 15, 1999, Financial Accounting Standard No. 133, "Accounting for derivative instruments and hedging activities" (FAS133) has been delayed once again. First out for comment in 1996, the Financial Accounting Standards Board's (FASB's) draft version was met by strong objections from end users, banks, dealers, industry groups, exchanges, and several regulatory agencies. Congress even stepped into the debate by introducing legislation to delay or bar the proposed accounting standard. The comment process produced numerous suggestions, many of which were incorporated. In the end, the FASB appeared to have moved significantly closer to its goals of increased financial statement transparency, consistency, and comparability. In the final hour, however, at the request of many banks and corporate end users, the FASB postponed the effective date for another year.

In this Chicago Fed Letter, we describe the most notable aspects of FAS133, outline industry objections, and explore some of the possible short- and long-term effects on banks and the derivatives industry of implementing the standard.

Features of the Standard:

The FASB's ultimate objective is fair value accounting; that is, reporting all financial assets and liabilities at fair value on the financial statements. FAS133 is an interim step in this direction. Greater transparency for derivatives is the FASB's intermediate focus. Derivatives currently appear predominantly in the footnotes of corporate annual reports and supplemental schedules of quarterly bank regulatory reports. However, the amount and format of information varies from firm to firm, except in the structured bank regulatory reports. Even in the case of trading derivatives, which are reported in some manner on the balance sheet, several different treatments have evolved based on limited guidelines issued by the FASB for futures and foreign currency contracts.1 Therefore, the FASB identified a need for increased consistency and comparability for the benefit of investors, counterparties, and regulators.

FAS133 fundamentally changes the accounting treatment for derivatives. The new standard requires all derivatives to be recorded at fair or current market value as assets or liabilities on the balance sheet. Subsequent gains and losses on these instruments must be reflected on the income statement as they occur. The only exception to this treatment applies to derivatives used for certain types of qualified hedges. Allowable hedges fall into two categories: fair value hedges and cash flow hedges. Foreign currency hedges are classified and treated similarly.

Fair value hedges protect against a change in the market value of existing assets, liabilities, or firm commitments. FAS133 requires that gains and losses on both the hedged item and the derivative hedge be recognized in current period earnings. This requires market value accounting of the hedged item.

Cash flow hedges protect against the variability in the cash flows associated with assets, liabilities, and forecasted transactions. For this category of hedges, the standard allows gains and losses on the derivative to be deferred in comprehensive income until the corresponding cash flow or forecasted transaction affects earnings. This applies only to the "effective" portion of the hedge; that is, the change in value of the derivative that exactly tracks the change in value of the cash flow being hedged. The difference is referred to as the "ineffective" portion and must be recognized in earnings.

FAS133 requires extensive disclosure requirements. Firms must show that a hedge is and will continue to be effective. The statement also requires certain derivatives embedded in other financial contracts to be bifurcated and treated in the same manner as other derivative contracts. FAS133 precludes common practices such as cross hedging using derivatives on similar but not identical underlying assets—for example, Treasury bond futures to hedge a mortgage portfolio. Furthermore, except for a few cases, hedging must be done for individual assets or liabilities. Hedging treatment for portfolio risks is severely restricted. Portfolio or other unqualified hedging may still be done for purely economic reasons, of course, but may result in increased volatility of reported earnings.

These narrow restrictions on hedge requirements will mean that many derivatives positions will not qualify as hedges under the standard. Gains and losses on these derivatives must be run through the income statement or the positions must be restructured to qualify. All these measures mean that the new accounting procedures will be more labour intensive and that, given the preclusion of portfolio hedging, may require a greater number of individual contracts.

Objections—timing and volatility:

Prior to the latest delay in implementation, some of the strongest objections to the standard concerned the timing of implementation. For most derivatives users, FAS133 was to be effective at the start of the new millennium. The timeframe in which to make the necessary accounting, risk-management, and valuation systems changes would have coincided with the recent resource commitments and expenditures on year 2000 preparedness, a deadline that could not be delayed. Petitioners to the FASB strongly objected to the standard's effective date, citing the number of

implementation issues still unresolved by the FASB, the lack of time remaining to educate staff on the complex new standard, and the internal freezes on computing systems mandated by many firms. Only the last of these objections was cited by the FASB in its decision to delay implementation of the standard.

Aside from timing issues, the most significant concern of derivatives users is that FAS133 will increase reported earnings volatility. Volatility may increase for two distinct reasons. First, fewer derivatives will qualify for hedge treatment. These derivative gains and losses will now be reflected in current income. However, changes in the value of the hedged item, for instance a bank's loan portfolio, may continue to be carried at book value because there is no generally accepted accounting procedure for marking these to market (or model). Second, even for qualifying hedges, the ineffective portion must be recognized in current income, potentially causing volatility on the income statement.

Why should firms care about accounting induced earnings volatility?

Management may fear that investors and analysts will not be able to disentangle the effects of the accounting change and so may conclude that the economic risk of the firm has changed. However, there is little evidence that analysts and investors are misled by accounting conventions. On the contrary, research suggests that analysts and investors are able to incorporate both book and fair value data for securities into their bank valuations.2 Thus, they should be able to incorporate the accounting changes into their valuations and see through the increased volatility.

Another reason that managers may care about increased volatility is based on personal rather than firm concerns. Demarzo and Duffie (1995) find that managers may incorporate private interests such as career and future wage considerations when determining the optimal hedge strategy for the firm.3 Because managers' compensation is frequently tied to reported earnings, increased volatility may affect managers' compensation and reputation. This may also have a real impact on managers' hedging decisions.

Short-term effects of FAS133:

There are several one-time costs associated with the implementation of FAS133. Most notable is the cost of revising accounting, risk-management, and valuation systems. Meanwhile, the FASB has not yet resolved many of the implementation details. This in turn is impeding the progress of firms trying to implement the standard and reprogram their systems.

Another potential short-term effect of FAS133 is a temporary increase in derivatives activity prior to implementation. Hedging firms will have an incentive to terminate their existing hedge positions in order to take advantage of current treatment that allows them to amortize the gain or loss over the life of the hedged item. After the new standard takes effect, some of these firms will enter into new derivative contracts. In this way, firms can minimize their current income recognition. This strategy is likely to lead to a one-time flurry of derivatives activity. Firms will also have the incentive to replace unqualified hedges with derivatives contracts that are more

customized and of the types favored by the new standard. Other firms may find the new standard too costly to implement and simply terminate their old derivative contracts without replacing them. Those firms choosing to remain unhedged will be taking on greater economic risk.

Long-term effects of FAS133

Ongoing costs associated with the standard include its extensive disclosure requirements. These include documentation of the hedge relationship, the risk-management strategy, and the risk-management objective. The perceived need to use over-the-counter (OTC) derivatives to obtain customization required for qualified hedge treatment will result in higher transactions costs, including fees paid to derivatives intermediaries.

Over the longer horizon, if the stricter hedge accounting rules and changed management incentives lead to less hedging, corporate risk may increase. Because of the need to match derivative positions to individual hedged items to meet requirements for "effective" hedges, FAS133 may also exacerbate the ongoing shift from exchange-traded derivative products to OTC derivative products. As of December 31, 1998, only 13% of banks' derivatives were exchange-traded.4 Customized OTC products are more costly and less liquid than exchange-traded instruments. During a financial crisis, it may be more difficult to liquidate or dynamically manage these positions. As exemplified in the recent collapse and recapitalization of Long-Term Capital Management, highly illiquid positions can raise systemic risk issues.

Higher costs associated with customized hedges is good news for derivatives dealers only if the volume of derivatives usage by end users does not fall off markedly as a result of these and other increased costs. There is nothing in the standard that is good news for the derivatives exchanges.

Bank regulatory capital requirements may also be affected. Under current risk-based capital guidelines, banks must hold capital equivalent to 8% of their risk-weighted assets to be considered adequately capitalized. The Federal Financial Institutions Examination Council, a consortium of bank regulators, has issued guidelines to minimize the effects of FAS133 on regulatory capital. However, the new treatment will ultimately affect reported assets and earnings, which in turn will affect banks' leverage and risk-based capital ratios, although it is unclear whether these will increase or decrease.

The possible magnitude of these effects can be judged by examining the output of the banks' regulatory report, known as the "Report of condition and income," or Call Report. Among other data, this report collects quarterly information on the notional and fair value of all derivatives and breaks these numbers down into contracts used for trading purposes and contracts used for hedging purposes. Table 1 highlights some interesting statistics. Most strikingly, nearly 96% of derivatives held by all banks are in their trading accounts. Derivatives held for trading purposes are already accounted for on the balance sheet at fair value, with gains and losses reflected on the income statement. Therefore, for banks at least, the new standard will affect only the small percentage of derivative positions that are used for risk-management purposes. As of December 31, 1998, the 447 commercial banks and trust companies with derivatives positions reported a

gross positive fair value of $17 billion for derivatives used as hedges.5 Under the FASB's new proposal, this amount would be recorded on the balance sheet as assets. The increase in assets that would result from the new treatment for all 447 banks represents a minuscule 0.004% of assets.

FAS 138 an Amendment to SFAS 133:

Normal Purchases and Normal Sales Exception

In their normal course of business, companies that consume or produce commodities often enter contracts to physically deliver nonfinancial assets, such as electricity, natural gas, oil, aluminium, wheat, or corn. Although these physical contracts are typically settled by the delivery of the commodity, they often include cash settlement provisions in case one party does not deliver or accept delivery of the goods, although these provisions are not intended as derivatives. Historically, the accounting principles for executory contracts applied to physical contracts.

FASB decided contracts that permit but do not require settlement by delivery of a commodity are often used interchangeably with other derivatives and present similar risks; therefore, they should be considered derivatives. As a result, the "normal purchases and normal sales" exception in paragraph 10(b) of SFAS 133 did not apply to these commodities contracts because they could be settled at net or liquidated through a market mechanism that would facilitate net settlement. Normal purchases and sales provide commodities that the reporting entity would use or sell in a reasonable period of time during the normal course of business.

In response to concerns that SFAS 133 inappropriately classified such physical contracts as derivatives, SFAS 138 amends paragraph 10(b) by expanding the normal purchases and normal sales exception to contracts that contain net settlement provisions if it is probable (at inception and throughout the term of the individual contract) that the contract will not settle at net and will result in physical delivery. The entity must document this conclusion. While this amendment will affect many forward contracts, exchange-traded futures that require periodic cash settlements do not qualify for the exception.

Interest Rate

SFAS 138 sought to reduce the implementation confusion caused by the definition of interest rate risk used in SFAS 133. The new standard combines all components of risk into interest rate risk and credit risk, and broadens the concept of interest rate risk to include the interest rate benchmarked in the hedged item's index, including the popular LIBOR (London interbank offer rate) hedging rate that, strictly speaking, also captures risk movements beyond the risk-free rate. In the SFAS 138 amendments, credit risk consists of all elements of interest rate risk other than the benchmark interest rate.

Under certain conditions, SFAS 133 allows interest rate swaps to use a shortcut method that assumes no ineffectiveness. The shortcut method does not apply, however, to a hedging strategy that designates the benchmark interest rate as the hedged risk when the hedged item is stated at

a different index, such as the prime rate. The basis difference between those indices would affect the assessment and measurement of hedge ineffectiveness and possibly force more items into quarterly hedge effectiveness testing.

SFAS 138 has broadened the scope of qualifying hedges. It allows companies to hedge interest rates with available derivative products based on LIBOR. Hedge effectiveness will increase because changes in credit spreads will not be considered a source of ineffectiveness if hedging with a benchmark interest rate. It has also complicated the accounting, however, forcing more frequent effectiveness testing.

Hedging of Foreign Currency– Denominated Items

One important provision of SFAS 138 is that it allows joint hedging of interest rate risk and foreign exchange (FX) risk in one compound hedge. SFAS 138 widens the net of qualified FX hedges to include the following:

- Foreign currency-denominated (FCD) assets or liabilities can be hedged in fair value or cash flow hedges. However, cash flow hedges of recognized FCD assets or liabilities are permitted only when all the variability in the hedged items' functional currency equivalent cash flows is reduced to zero.
- Unrecognized FCD firm commitments can be hedged in fair value or cash flow hedges.

Prior to SFAS 138, hedge accounting for foreign currency risk exposures was limited to fair value hedges of unrecognized FCD firm commitments, cash flow hedges of forecasted FCD transactions, and net investments in FCD foreign operations.

Example. FCD items (e.g., a fixed-rate bond in deutsche marks) are subject to two underlying risks: fair value risk in terms of changes in German interest rates, and changes in the FX rates (between the deutsche mark and the U.S. dollar). Before SFAS 138, the debtor would first hedge the interest rate risk by locking in the combined value of the bond and swap at a fixed amount in marks with a swap in which variable interest was received and fixed interest was paid. Then another derivative contract, such as a forward contract to hedge against the possible fall of the mark against the dollar, would hedge the combined FCD value for FX risk. Under SFAS 133, the FCD debt was premeasured (via the income statement) based on the prevailing spot rate of exchange and the derivative was marked to market (also via the income statement). However, these two adjustments rarely match, creating unintended earnings volatility.

Under the SFAS 138 amendments, it is now possible to acquire a single compound derivative to hedge the joint fair value risk of interest rate and FX movements. One such derivative is a cross-currency interest swap, which would receive a fixed interest rate in foreign currency and pay a variable interest rate in domestic currency. SFAS 138 permits these recognized FCD assets and liabilities to be designated as the hedged items in fair value or cash flow hedges.

Intercompany Exposures

Multinational corporations enter into many transactions with FX risk exposure. A centralized treasury center that assesses corporate-wide FX exposure and hedges the net exposure with a single derivative offers significant cost savings over subsidiaries acquiring their own third-party hedges.

Example. A German subsidiary forecasts sales of DM 5 million from a Japanese purchaser in the next three months, and a Japanese subsidiary expects to purchase DM 3 million worth of inventory from a German supplier in the same period. The net exposure would be a long position of DM 2 million and the parent company could hedge its risk by selling a forward contract or buying a put option for DM 2 million.

SFAS 133 discouraged hedge accounting by treasury centers because it required individual members of a consolidated group to enter individual offsetting derivative contracts with third parties, which nullifies the cost savings benefits. The SFAS 138 amendments allow certain intercompany derivatives that are offset by unrelated third-party contracts to be designated as the hedging instrument in cash flow hedges of foreign currency risk in the consolidated financial statements.

Amendments to DIG Guidance

SFAS 138 also amends related interpretations issued by the Derivatives Implementation Group (DIG).

Issue G3: Discontinuation of a cash flow hedge. SFAS 138 amends the accounting for discontinued cash flow hedges by requiring that the net derivative gain or loss from a discontinued cash flow hedge be reported in accumulated other comprehensive income, unless it is probable that the forecasted transaction will not occur by the end of the originally specified time period or within an additional two months.

Issue H1: Hedging at the operating unit level. SFAS 138 extends the functional currency concept of SFAS 52 to foreign currency fair value hedges and to hedges of the net investment in a foreign operation, in addition to foreign currency cash flow hedges. It also requires that the hedged transaction be denominated in a currency other than the hedging unit's functional currency.

Issue H2: Requirement that the unit with the exposure must be a party to the hedge. The SFAS 138 amendments ensure that the functional currency concept of SFAS 52 is applied to determine whether hedge accounting is appropriate for consolidated financial statements. One of two conditions must be satisfied in order to use hedge accounting:

- The operating unit with the FX exposure must be party to the hedging instrument; or
- Another member of the consolidated group is party to the hedge; this party has the same functional currency as the operating unit, and there are no intervening subsidiaries with a different functional currency.

Example. A second-tier subsidiary (B) whose functional currency is the U.S. dollar has a French franc exposure. A parent company could designate a dollar-franc derivative as a hedge of a first-tier subsidiary's (A) exposure, provided that A's functional currency is also the dollar.

However, if A's functional currency is the Japanese yen, the consolidated parent company could not designate its dollar-franc derivative as a hedge of B's exposure. In this case, the financial statements of B are first translated into yen before the yen-denominated financial statements of A are translated into dollars for consolidation. As a result, there is no direct FX exposure, because A has a different functional currency than B's functional currency. Furthermore, there is no direct exposure to the consolidated parent company.