NCFM

NSE's CERTIFICATION IN FINANCIAL MARKETS

Operations Risk Management Module

NATIONAL STOCK EXCHANGE OF INDIA LIMITED

Test Details:

Sr. No.	Name of Module	Fees (Rs.)	Test Duration (in minutes)	No. of Questions	Maximum Marks	Pass Marks (%)	Certificate Validity (in yrs)
	FOUNDATION						
1	Financial Markets: A Beginners' Module *	1686	120	60	100	50	5
2	Mutual Funds : A Beginners' Module	1686	120	60	100	50	5
3	Currency Derivatives: A Beginner's Module	1686	120	60	100	50	5
4	Equity Derivatives: A Beginner's Module	1686	120	60	100	50	5
5	Interest Rate Derivatives: A Beginner's Module	1686	120	60	100	50	5
6	Commercial Banking in India: A Beginner's Module	1686	120	60	100	50	5
7	FIMMDA-NSE Debt Market (Basic) Module	1686	120	60	100	60	5
8	Securities Market (Basic) Module	1686	120	60	100	60	5
	INTERMEDIATE						
1	Capital Market (Dealers) Module *	1686	105	60	100	50	5
2	Derivatives Market (Dealers) Module * [Please refer to footnote no. (i)]	1686	120	60	100	60	3
3	Investment Analysis and Portfolio Management Module	1686	120	60	100	60	5
4	Fundamental Analysis Module	1686	120	60	100	60	5
5	Options Trading Strategies Module	1686	120	60	100	60	5
6	Banking Sector Module	1686	120	60	100	60	5
7	Insurance Module	1686	120	60	100	60	5
8	Macroeconomics for Financial Markets Module	1686	120	60	100	60	5
9	NSDL–Depository Operations Module	1686	75	60	100	60 #	5
10	Commodities Market Module	2022	120	60	100	50	3
11	Surveillance in Stock Exchanges Module	1686	120	50	100	60	5
12	Corporate Governance Module	1686	90	100	100	60	5
13	Compliance Officers (Brokers) Module	1686	120	60	100	60	5
14	Compliance Officers (Corporates) Module	1686	120	60	100	60	5
15	Information Security Auditors Module (Part-1)	2528	120	90	100	60	2
	Information Security Auditors Module (Part-2)	2528	120	90	100	60	
16	Technical Analysis Module	1686	120	60	100	60	5
17	Mergers and Acquisitions Module	1686	120	60	100	60	5
18	Back Office Operations Module	1686	120	60	100	60	5
19	Wealth Management Module	1686	120	60	100	60	5
20	Project Finance Module	1686	120	60	100	60	5
21	Financial Services Foundation Module ###	1123	120	45	100	50	NA
22	NSE Certified Quality Analyst $	1686	120	60	100	50	NA
	ADVANCED						
1	Financial Markets (Advanced) Module	1686	120	60	100	60	5
2	Securities Markets (Advanced) Module	1686	120	60	100	60	5
3	Derivatives (Advanced) Module [Please refer to footnote no. (i)]	1686	120	55	100	60	5
4	Mutual Funds (Advanced) Module	1686	120	60	100	60	5
5	Options Trading (Advanced) Module	1686	120	35	100	60	5
6	FPSB India Exam 1 to 4**	2247 per exam	120	75	140	60	NA
7	Examination 5/Advanced Financial Planning **	5618	240	30	100	50	NA
8	Equity Research Module ##	1686	120	49	60	60	2
9	Issue Management Module ##	1686	120	55	70	60	2
10	Market Risk Module ##	1686	120	40	65	60	2
11	Financial Modeling Module ###	1123	120	30	100	50	NA
	NISM MODULES						
1	NISM-Series-I: Currency Derivatives Certification Examination *	1250	120	100	100	60	3
2	NISM-Series-II-A: Registrars to an Issue and Share Transfer Agents–Corporate Certification Examination	1250	120	100	100	50	3
3	NISM-Series-II-B: Registrars to an Issue and Share Transfer Agents – Mutual Fund Certification Examination	1250	120	100	100	50	3
4	NISM-Series-III-A: Securities Intermediaries Compliance (Non-Fund) Certification Examination	1250	120	100	100	60	3
5	NISM-Series-IV: Interest Rate Derivatives Certification Examination	1250	120	100	100	60	3
6	NISM-Series-V-A: Mutual Fund Distributors Certification Examination *	1250	120	100	100	50	3
7	NISM Series-V-B: Mutual Fund Foundation Certification Examination	1000	120	50	50	50	3
8	NISM-Series-V-C: Mutual Fund Distributors (Level 2) Certification Examination	1405	120	68	100	60	3
9	NISM-Series-VI: Depository Operations Certification Examination	1250	120	100	100	60	3
10	NISM Series VII: Securities Operations and Risk Management Certification Examination	1250	120	100	100	50	3
11	NISM-Series-VIII: Equity Derivatives Certification Examination	1250	120	100	100	60	3
12	NISM-Series-IX: Merchant Banking Certification Examination	1405	120	100	100	60	3
13	NISM-Series-X-A: Investment Adviser (Level 1) Certification Examination	1250	120	100	100	60	3
14	NISM-Series-XI: Equity Sales Certification Examination	1405	120	100	100	50	3
15	NISM-Series-XII:Securities Markets Foundation Certification Examination	1405	120	100	100	60	3
16	Certified Personal Financial Advisor (CPFA) Examination [Please refer to footnote no. (ii)]	4495	120	80	100	60	3

* Candidates have the option to take the tests in English, Gujarati or Hindi languages.
\# Candidates securing 80% or more marks in NSDL-Depository Operations Module ONLY will be certified as 'Trainers'.
** Following are the modules of Financial Planning Standards Board India (Certified Financial Planner Certification)
- FPSB India Exam 1 to 4 i.e. (i) Risk Analysis & Insurance Planning (ii) Retirement Planning & Employee Benefits (iii) Investment Planning and (iv) Tax Planning & Estate Planning
- Examination 5/Advanced Financial Planning
Modules of Finitiatives Learning India Pvt. Ltd. (FLIP)
Module of IMS Proschool
$ Module of SSA Business Solutions (P) Ltd.

The curriculum for each of the modules (except Modules of Financial Planning Standards Board India, Finitiatives Learning India Pvt. Ltd. and IMS Proschool) is available on our website: www.nseindia.com > Education > Certifications.

Note: (i) SEBI / NISM has specified the NISM-Series-VIII-Equity Derivatives Certification Examination as the requisite standard for associated persons functioning as approved users and sales personnel of the trading member of an equity derivatives exchange or equity derivative segment of a recognized stock exchange.
(ii) NISM Certified Personal Financial Advisor (CPFA) Examination shall be available till August 30, 2013 and thereafter shall be discontinued. If you have made payment for the Certified Personal Financial Advisor (CPFA) Examination, kindly take the examination before August 30, 2013.

Operations Risk Management Module

Background

This Workbook discusses operations risk issues and approaches to mitigate them in the banking and financial services sector.

Learning Objectives

- Understand the different types of risk that businesses are exposed to
- Appreciate various measures that are taken by companies to mitigate operations risk
- Know the process and underlying risks and their mitigation in secondary market trading
- Know the process and underlying risks and their mitigation in clearing and settlement
- Understand the role of workflow design in managing operating risk
- Get oriented to the Basel Accords and their recommendations for management of operations risk in banks

CONTENTS

Acronyms

ADB	Asian Development Bank
AfDB	African Development Bank
AMA	Advanced Measurement Approaches
ASA	Alternate Standardised Approach
BEICFs	Business Environment and Internal Control Factors
BIA	Basic Indicator Approach
BIS	Bank for International Settlements
CM	Clearing Member
CORF	Corporate Operations Risk Management Function
EAD	Exposure at Default
ED	External Data
EIB	European Investment Bank
EL	Expected Loss
EQCR	Engagement Quality Control Review
HQLA	High Quality Liquid Assets
IADB	Inter-American Development Bank
IBRD	International Bank for Re-construction & Development
ILD	Internal Loss Data
IRB	Internal-Ratings Based
KPI	Key Performance Indicators
KRI	Key Risk Indicators
LCR	Liquidity Coverage Ratio
LDA	Loss Distribution Approach
LGD	Loss Given Default
NEAT	National Exchange for Automated Trading
NSCCL	National Securities Clearing Corporation Ltd.
NSDL	National Securities Depository Ltd
NSE	National Stock Exchange
NSFR	Net Stable Funding Ratio
OECD	Organisation for Economic Co-operation & Development
OECLOB	Open Electronic Consolidated Limit Order Book
ORC	Operational Risk Categories
ORMF	Operational Risk Management Framework
ORMS	Operational Risk Measurement System
PCM	Professional Clearing Member
PD	Probability of Default
PSE	Public Sector Entities
RCSA	Risk Control Self-Assessment
RSA	Risk Self-Assessment
RTA	Registrar & Transfer Agents
SBA	Scenario Based Approaches
SCM	Self Clearing Member
SIB	Systemically Important Bank
SIGOR	Standards Implementation Group - Operational Risk Subgroup
SPE	Special Purpose Entities
TCM	Trading cum Clearing Member
TM	Trading Members
TSA	The Standardised Approach
UL	Unexpected Loss
VaR	Value at Risk

Distribution of weights of the Operations Risk Management Module Curriculum

Chapter No.	Title	Weights (%)
1	Introduction to Operations Risk	6
2	Trades in Secondary Market	13
3	Clearing & Settlement of Trades	16
4	Workflow Design	5
5	BASEL Overview	31
6	Basel II: Operational Risk	13
7	Basel: Operational Risk Principles	3
8	Basel: Audit	13
	Total	100

Note: Candidates are advised to refer to NSE's website: www.nseindia.com, click on 'Education' link and then go to 'Updates & Announcements' link, regarding revisions/ updations in NCFM modules or launch of new modules, if any.

This book has been developed for NSE by Mr. Sundar Sankaran, Director, Advantage India Consulting Pvt. Ltd. and finberry academy pvt ltd.

Chapter 1 : Introduction to Operations Risk

1.1 Risk & Uncertainty

In day to day life, 'risk' and 'uncertainty' are used inter-changeably. Economists however make a difference between the two. Frank Knight, in "Risk, Uncertainty & Profit" (Boston: Houghton Mifflin, 1921) differentiated the two as follows:

- Risks are unknown outcomes, whose odds of happening can be measured or at least learned about.
- Uncertain events are those that we do not even know how to describe.

For example, there are risks associated with investing in equities, while there are uncertainties about who will be in power after the next elections.

An alternative differentiation between the two terms is that uncertainty does not always imply something negative; risk is generally viewed as a negative – a problem.

For example, there is uncertainty about a company winning a contract. If it wins the contract, it will be a positive for the company. There is a risk that you will lose money in your investments; there is no risk that you will earn a profit in your investment. Since risk has negative implications, it needs to be managed.

1.2 The Financial Sector

The financial sector is a channel for money to flow – from savers to deposit-seeking companies, from lenders to borrowers etc. Banks, financial institutions, insurance companies, mutual funds, stock exchanges, brokers etc. constitute the financial sector.

Banks are a vehicle for savers in the economy to park their surpluses. The savers can technically ask for their money back at any time. However, in the normal course, all depositors do not ask for all their money back, at the same time. Therefore, the bank has money to lend to borrowers. The difference between the interest they earn on their loans, and the interest they pay on their deposits, is their spread.

The real economy, comprising manufacturing and service companies, too, need money flows to keep their activities going. The financial sector is an important driver of the real economy; any disruption in the financial sector can cause large scale damage to the real economy. Regulators have been trying to control the downsides to this linkage, with limited success.

Central banks [like the Reserve Bank of India (RBI) in India] closely monitor and regulate the money market in general, and banks and financial institutions (BFIs) in particular as part of their efforts to ensure macro-economic stability.

1.3 Risk Types

Businesses and governments are exposed to various kinds of risks:

- Credit Risk:

  This is the risk that a borrower's credit standing goes down or is unable to repay the lender/investor. This is the most significant risk that banks face on their loan book.

  For example, Bank B gave a loan to Borrower C. C may default in fulfilling its repayment obligations.

- Market Risk:

  This is the risk that an investment loses value in the market. This is the most significant risk that any investor in a traded asset (like equity) is exposed to.

  For example, Investor I bought shares of Company X at Rs. 50. A few days later, it reports poor financial results. Analysts expect its price to crash to Rs. 12.

- Operations Risk:

  This is the risk arising out of people or processes not working as desired.

  For instance, credit card is delivered to a party other than the card-holder or his authorised agent.

- Liquidity Risk:

  This is the risk that the business does not have the moneys to meet its normal day to day commitments, though it is not bankrupt.

  For instance, Bank B has used short term funds to lend to an infrastructure project. The moneys are locked in the project, while a freezing of the credit market prevents the Bank from making fresh borrowings to re-finance its earlier short term borrowing.

- Counter-party Risk:

  This is a risk that a transaction does not go through because the counter-party defaults; or one leg of a transaction goes through, not the other.

  Investor I bought shares of Company Y at Rs. 50 from Seller S. A few days later, the share price shoots up to Rs. 150. Technically, Investor I has made a profit of Rs. 100 per share. But in reality, S is unable to deliver the shares. In this case, if neither leg of the transaction is executed, then Investor I has an opportunity loss of Rs. 100 per share. But, if Investor I has paid Seller S Rs. 50, before the latter declares bankruptcy or runs away, then former may have to book an actual loss of the moneys paid.

- Reputation Risk:

  This is a risk to the name, goodwill, image or business standing arising out of some action or inaction. This is often very difficult to quantify and entails high level of subjectivity.

For instance, Bank B engages collection agents to recover its dues. The agents adopt inappropriate practices, which leads to a police case and wide press coverage of Bank B's business practices.

- Legal Risk:

  This is the risk that a legal position taken proves untenable.

  For example, a competitor files a case against a portfolio management company accusing the latter of using investment models and clients stolen by a former employee of the competitor.

- Systems Risk:

  This is the risk that the company or its business associates are unable to do business on account of failure of systems.

  For instance, investors are unable to transact in the market because the investment website of the broking company is down.

- Systemic Risk:

  This is a risk that failure of one party in the market leads to a domino effect of more parties failing to meet their obligations in the market.

- Model Risk:

  This is a risk that a financial model used by a party turns out to be faulty.

  For instance, a credit rating company finds a bug in the model it has been using for assessing the credit worthiness of its rating clients.

- Strategy Risk:

  This is the risk that a fundamental premise on which the business is built proves faulty or risky.

  For example, a company is formed to sell clothes that will double as phones. It finds that it is unable to deliver the product at a price that is acceptable to the market.

The above is just an illustrative list of risks that businesses are exposed to. There is an element of subjectivity in the grouping. Different schools of thoughts group them variously. For example:

- A decline in credit quality of a company causes the price of its debentures in the market to fall. Is it credit risk or market risk?
- The counter-party did not pay because it suffered losses on account of a crash in the market. Is it counter-party risk or market risk?
- A company suffers liquidity problems because of a counter-party's default. Is it liquidity risk or counter-party risk?

- The strategy may fail because of a legal challenge. Is it strategy risk or legal risk?
- Reputation of a company is affected after it lost a court case. Is it legal risk or reputation risk?

The general approach in the market is to tag the risk to the immediate cause, though it is not always possible to arrive at a consensus. The important part is to:

- Identify all the risks
- Take a call on the risk/s to accept and the risk/s to transfer to others who are better equipped to handle them.
- Ensure suitable controls over, and adequate reporting related to residual risks i.e. the risks which remain in the business
- Ensure there is adequate capital to manage the consequences of a risk fructifying.

These roles are the responsibility of Risk Management function in organisations.

The rest of the book focuses on Operations Risk, but touches on other risks that have a connection to operations.

1.4 Operations Risk

As already seen, this is the risk arising out of people or processes (or even, systems) not working as desired. The shortfall in performance is either intentional or unintentional.

- When the performance gap is unintentional, it can be called a mistake/error.

  For example, the credit officer failed to notice suspect accounting treatment of certain items that helped the borrower show profits. Based on the profitability, a loan was sanctioned.

- Intentional performance gaps can be serious cases of fraud/mal-practice.

  For example, the borrower paid the credit officer 5% of the loan amount to make sure that the loan appraisal note was falsified in a way that it complied with the bank's lending norms.

The organisation takes a hit in the case of both mistake and fraud. The only difference is that in the event of fraud, the organisation will have a strong case to proceed against the people who perpetrated the fraud to seek recovery of the losses suffered.

1.5 Operations Risk Management

The following are some of the approaches that organisations take to manage operations risk. Most of these are equally applicable to organisations that are not into banking and finance.

1.5.1 Recruitment & Training

Most mistakes and all frauds revolve around people.

Mistakes can be prevented by having a suitable recruitment policy that ensures that new recruits have the knowledge, skills and attitude required for the job. This has to be backed by effective training programs to equip the employees to deliver on expectations. Regular Training Needs Analysis of employees is required to identify critical ongoing training needs of employees while they are in service.

In the case of frauds, one or more employees may be active perpetrators doing the crime, wilful abetters assisting others in the crime or involuntary informers providing the information to fraudsters, without realising the intentions of the recipients of the information.

Organisations therefore need to be cautious in recruitments. Besides assessing candidates on their knowledge and skills, background checks and references should be an important part of the recruitment process. Apart from training, organisations should foster a culture of sharing information on need-to-know basis, so that careless sharing does not enable fraudsters.

1.5.2 Work Flow Design

Work flows should be designed in a manner where there are checks and balances within the system. Such internal checks prevent mistakes as well as fraud. For example, a system where the same person approves the voucher and signs the cheque is a risky one. Chapter 4 discusses the split of front office, middle office and back office in this regard.

1.5.3 Work Flow Documentation

The work flow for every task should not only be well designed, with internal checks, but also should be properly documented. This eliminates the possibility of anyone claiming ignorance of the process. The work flow documentation also becomes the base document for training new recruits.

1.5.4 Delegation of Authority

There has to be a written delegation of authority that states who is authorised to take what decision and upto what level. For instance, Mr. X can issue purchase orders for items A, B and C upto Rs. 50 lakh per order and Rs. 3 crore in a month.

While authority is normally delegated based on position (e.g. Senior Vice President), the authority should not flow to an individual only based on recruitment i.e. a person should not have the authority merely on account of joining the organisation as Senior Vice President. The authority should be available only to people mentioned in the List of Authorities. New recruits may be added to the list of authorities, after a cooling period that may vary with the level, and in any case it should be done after documentation checks and reference checks are completed.

1.5.5 Independent Internal Audit

Companies have an internal audit set up that reviews activities in the company on an ongoing basis. Normally, the internal audit staff are employees, though it is not unusual to have

independent outsiders (such as a CA firm other than the statutory auditor) engaged to perform the role.

Whatever the arrangement for internal audit, it should be handled by a person of stature who reports to a suitably high level person in the organisation. In large organisations, the head of internal audit has to report to the Audit Committee of the Board of Directors, and is expected have the right to report to the Board of Directors if he feels the need.

The internal audit set up would be very weak, if it comprises only of lower level employees with the head reporting to a business-head. In such a set-up, the business-head will be able to easily influence the internal audit head because of control over the latter's bonuses and career prospects.

The internal audit plan for the year too should be approved by the Audit Committee or the head of the organisation. This should cover not only review of transactions but also whether the work flow design and delegation of authority is being complied with. Instances of non-compliance should be highlighted in their reports which should go to Audit Committee or owner.

Given the criticality of the internal audit role, statutory auditors, in their report to shareholders, are required to comment on the appropriateness of the internal audit system for the size and complexity of the organisation.

1.5.6 Independent Compliance Function

In most banking and finance businesses, it is mandatory to have an independent compliance function to assess compliance with various regulations. In other businesses, if a separate compliance person is not appointed, the Company Secretary is responsible.

The Compliance-Head reports to the head of the organisation, and is obliged to inform the board of directors and regulators in case of violations of law. In any case, the Compliance-Head should not report to the head of a business or operations.

1.5.7 Independent Risk Management Function

Businesses that are active in the financial, commodity or other markets (including manufacturing companies that have an active treasury management function) should have an independent risk management function.

This function has to put together a risk tolerance policy for the company, which should be approved by the board. The policy statement might cover the kind of exposures that are permitted, the value of permitted exposure, the types of instruments permitted for the exposure, and the counter-party limits.

The risk management function should also monitor the company's activities to track the risks that are being taken as compared to the risk tolerance policy. Instances of excessive risk need to be documented and highlighted to the relevant superior authority.

1.5.8 Systems Audit

Most work flows, these days, happen through computer systems. Unlike humans, computers are programmed to keep repeating select processes. Therefore, it makes more sense to audit the system comprehensively, and then do test check of a few transactions that go through the system as a confirmation of the logic.

Systems audit has emerged as an independent profession that calls for greater knowledge of computer systems and logic than what a regular financial auditer has. This is particularly true of complex programs that may be used for automated trading or valuation of unlisted securities. Some financial auditors acquire additional qualifications to be able to competently handle systems audit. SEBI has made a systems audit compulsory for broking organisations.

1.5.9 Corporate Governance

Progressive companies have an active board comprising insiders and independent directors. Each director is given a role, and independent directors are given an opportunity to have discussions, independent of the insiders, on specific topics.

An audit committee of the directors, comprising of independent directors, is formed to look closely on the finances, audit and risk aspects of the organisation.

Either the same committee or a separate remuneration committee examines the remuneration policy and bonuses in the company, to be sure that it does not encourage employees to take undue risks. Similarly, it checks on the reasonableness of the compensation for the statutory auditors, internal auditors etc. For instance, compensating internal audit staff based on profits of the company can enhance the business risk profile of the company.

1.5.10 Whistle Blower Policy

The organisation should have a whistle blower policy that allows anyone to approach a responsible person to provide information about aspects of the business that may be illegal, immoral or unauthorised. The policy, at a minimum, should provide a list of people who can be approached for sharing the information, and also guarantee the anonymity and safety of the informer, and ensure that informers are not victimised.

1.5.11 Risk Management Culture

Ultimately, risk boils down to culture and value systems in the organisation. The value systems in some organisation are oriented to take risk, whatever the consequences. Such organisations back the employees, even if the risk taken is excessive and unauthorised, especially when the risky pays off in profits for the organisation. Thus, an environment is created where extreme risks are taken in the organisation.

The danger in such a care-free approach to risk is that one does not know when the risk taken can consume the capital and lead the organisation to bankruptcy.

Organisations that survive and thrive in the long term are those that accept risk with caution. They recognise risk, examine it in the context of potential returns and downsides and identify a suitably senior authority to decide on accepting the risk within limits. The caution in accepting risk might even extend to refusing to do business, where the risk is beyond the capability and balance sheet strength of the organisation.

Some of the most structured efforts to managing risk have been taken in the banking sector, through the efforts of Bank for International Settlements. Its Basel Committee on Banking Supervision has brought out various requirements that have changed the face and back-end of banking globally. The latter part of this Workbook focuses on some of the issues and principles highlighted by them that are relevant for an understanding of operations risk management.

Self-Assessment Questions

- _____ are unknown outcomes, whose odds of happening can be measured.
  - **Risks**
  - Uncertain events
  - Both the above
  - None of the above

- The most significant risk that banks face on their loan book is _____
  - Liquidity risk
  - **Credit risk**
  - Interest risk
  - Market risk

- Which of the following affects the fundamental premise on which business is built?
  - Credit Risk
  - Model Risk
  - **Strategy Risk**
  - Liquidity Risk

- Which of the following is intentional?
  - Error
  - **Malpractice**
  - Both the above
  - None of the above

- Which of the following is a critical operations risk?
  - Recruitment only through references
  - Training needs analysis by outsiders
  - **Open office policy where no passwords are used**
  - Bonuses linked to profits

- It is normal for the statutory auditor to take up the job of internal audit of the company.
  - True
  - **False**

Chapter 2 : Trades in Secondary Market

Secondary market refers to a market, where securities that are already issued by the Government or companies, are traded between buyers and sellers of those securities. The securities traded in the secondary market could be in the nature of equity, debt or derivatives.

India's premier stock exchange, National Stock Exchange (NSE) offers a Screen Based Trading System for such secondary market trades. NSE provides trading in four different segments - Wholesale Debt Market, Capital Market, Futures and Options and Currency Derivatives Segment.

Once trades are executed, their clearing and settlement is handled by the clearing house. The National Securities Clearing Corporation Ltd. (NSCCL), a wholly owned subsidiary of NSE, is responsible for clearing and settlement of trades executed in the NSE. As part of this role, NSCCL guarantees all the trades against counter-party risk. Thus, anyone who trades in the stock exchange, can be sure of the trade getting properly executed. Further, NSCCL helps in managing the risk in the market through an effective margining system.

NSCCL also undertakes settlement of transactions on other stock exchanges like, the Over the Counter Exchange of India.

NSE, along with some other institutions, promoted India's first depository, National Securities Depository Ltd (NSDL). The depository makes instantaneous electronic transfer of securities possible. Demat (Dematerialised) settlement has eliminated the bad deliveries and associated problems which were significant operating risks in previous formats of settlement of stock exchange transactions in the country.

Transactions in equity shares in the stock exchange entail change of ownership in companies. Registrar & Transfer Agents (RTAs) are often appointed to maintain the investor records for companies based on inputs from investors (for physical shares) and depository (for demat shares).

The above allocation of responsibilities and process of execution of trades has limited operations risks in the secondary market.

2.1 Trade Intermediaries

The following intermediaries are involved in trades in the secondary market:

2.1.1 Stock Broker

A stock broker is an intermediary who arranges to buy and sell securities on the behalf of clients (the buyer and the seller).

According to SEBI (Stock Brokers and Sub-Brokers) Regulations, 1992, a stockbroker is a member of a stock exchange and is required to hold a certificate of registration from SEBI in order to buy, sell or deal in securities.

2.1.2 Trading Member (TM)

Stockbrokers need to become Trading Members of NSE in order to help their clients to trade using the NSE platform. Trading members of NSE have certain benefits, such as:

- Access to a nation-wide trading facility for equities, derivatives, debt and hybrid instruments/products;
- Ability to provide a fair, efficient and transparent securities market to the investors;
- Use of state-of-the-art electronic trading systems and technology;
- Dealing with an organisation which follows strict standards for trading & settlement, at par with those available at the top international bourses, and that constantly strives to move towards a global marketplace in the securities industry.

2.1.3 Clearing Member (CM)

NSCCL handles the clearing of trades through clearing members. A trading member may choose to become a clearing member.

Self Clearing Members (SCM) clear and settle the trades executed by them only, either on their account or on account of their clients.

Trading Members cum Clearing Members (TCM) can clear and settle their own trades as well as trades of other trading members.

Professional Clearing Members (PCM) do not trade but only clear and settle trades executed by other trading members. Professional clearing membership is only applicable for the F&O Segment.

2.1.4 Authorised Persons

Trading members of the Exchange can appoint authorised persons in the Futures & Options and Currency Derivatives Segments.

Authorised persons can be individuals, registered partnership firms, bodies corporate or companies defined under the Companies Act, 1956.

An authorised person introduces clients to the trading member and receives remuneration/ commission/ compensation from the trading member and not from the clients.

The authorised person is not allowed to have any trading relationship with the clients. The trading member should issue the contract notes and bills directly to the client i.e. the authorized person should not issue contract notes, confirmation memo and/or bills in their name.

The clients introduced by the authorised person are required to deliver securities and make payments directly in the trade name of the trading member (as appearing on the SEBI registration certificate). Similarly, the trading member should deliver securities and make payments directly in the name of the clients.

2.1.5 Sub-brokers

The Trading Members of the Exchange may appoint sub-brokers to act as agents of the concerned Trading Member for assisting investors in buying, selling or dealing in securities. A sub-broker is an important intermediary between the Trading Member and the client.

A sub-broker may be an individual, a partnership firm or a corporate.

Sub-brokers are affiliated to the Trading Members, and are required to be registered with SEBI. A sub-broker is allowed to be associated with only one Trading Member of the Exchange.

The Trading Member has to ensure the settlement of all its deals, even if the deals may have originated from its sub-broker.

2.2 Screen-Based Trading System

The trading system operates on a strict price-time priority. All orders received in the system are sorted with the best priced order getting the first priority for matching i.e., the best buy orders match with the best sell order. Similar priced orders are sorted on time priority basis, i.e. the one that came in early gets priority over the later one.

Orders are matched automatically by the computer keeping the system transparent, objective and fair. Where an order does not find a match, it remains in the system and is displayed to the whole market, till a fresh order comes in to create a trade, or the earlier order is cancelled or modified.

Investors can know the fate of the orders almost as soon as they are placed with the trading members. Thus, the National Exchange for Automated Trading (NEAT) system provides an Open Electronic Consolidated Limit Order Book (OECLOB).

2.3 NEAT System

The NEAT system supports an order driven market, wherein orders match on the basis of price-time priority. All quantity fields are in units and prices are quoted in Indian Rupees.

The trading member has the facility of defining a hierarchy amongst its users of the NEAT system. This hierarchy is depicted in Figure 2.1.

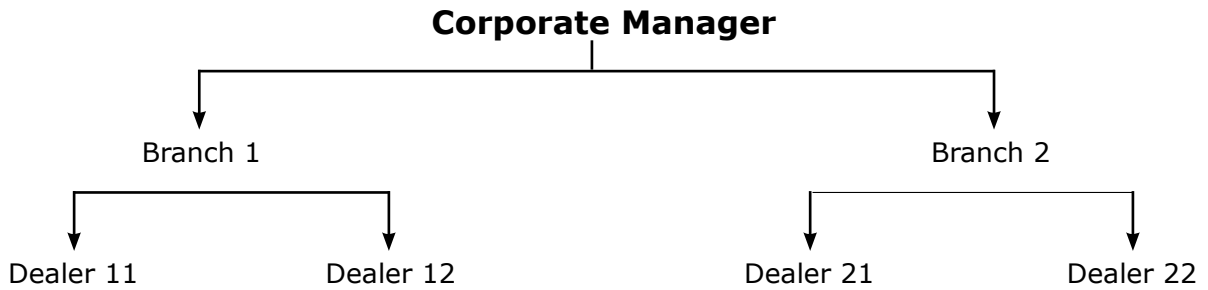

Figure 2.1: Trading System Users hierarchy

2.3.1 Corporate Manager

The corporate manager is a term assigned to a user placed at the highest level in a trading firm. Such a user receives the end-of-day reports for all branches of the trading member.

The facility to set branch order value limits and user order value limits is available to the corporate manager.

The corporate manager also has facility to set symbol wise user order quantity limit.

He can view outstanding orders and trades of all users of the trading member and can also cancel/modify outstanding orders of all users of the trading member.

2.3.2 Branch Manager

The branch manager is a term assigned to a user who is placed under the corporate manager. The branch manager receives end-of-day reports for all the dealers under that branch.

He can set user order value limit for each user of his branch. But he does not have access to information on other branches.

He can view outstanding orders and trades of all users of his branch and can also cancel/ modify outstanding order of all users of his branch.

2.3.3 Dealer

Dealers are users at the lowest level of the hierarchy. A dealer can view and perform order and trade related activities only for himself; he does not have access to information on other dealers under either the same branch or other branches.

2.4 Order Management

Order Management consists of entering orders, order modification, order cancellation and order matching.

2.4.1 Entering Orders

As and when valid orders are entered or received by the trading system, they are first numbered, time stamped and then scanned for a potential match. This means that each order has a distinctive order number and a unique time stamp on it. When any order enters the trading system, it is an active order.

An active order tries to find a match on the other side of the books. If it finds a match, a trade is generated. If it does not find a match, the order becomes a passive order and goes and sits in the order book, as per the price/time priority.

- Price priority means that if two orders are entered into the system, the order having the best price gets the higher priority. Best price for a sell order is the lowest price and for a buy order, it is the highest price.

- Time priority means if two orders having the same price is entered, the order that is entered first gets the higher priority.

2.4.2 Modifying Orders

All orders can be modified in the system till the time they are fully traded. Modification is possible only during market hours and pre-open stage. Once an order is modified, the branch order value limit for the branch gets adjusted automatically. Following is the corporate hierarchy for performing order modification functionality:

- A dealer can modify only the orders entered by him.
- A branch manager can modify his own orders or orders of any dealer under his branch.
- A corporate manager can modify his own orders or orders of all dealers and branch managers of the trading member firm.

The corporate manager/branch manager, however, cannot modify order details such that it exceeds the branch order value limit set for the day.

Order modification cannot be performed by/for a trading member who is suspended or de-activated by the Exchange for any reason.

2.4.3 Cancelling Orders

Order cancellation functionality can be performed only for orders which have not been fully or partially traded (for the untraded part of partially traded orders only) and only during market hours and in pre-open period.

2.4.4 Order Matching

The buy and sell orders are matched on Book Type, Symbol, Series, Quantity and Price.

An active buy order matches with the best passive sell order if the price of the passive sell order is less than or equal to the price of the active buy order.

Similarly, an active sell order matches with the best passive buy order if the price of the passive buy order is greater than or equal to the price of the active sell order.

2.5 Trade Management

A trade is an activity in which a buy and a sell order match with each other. Matching of two orders is done automatically by the system. Whenever a trade takes place, the system sends a trade confirmation message to each of the users involved in the trade.

The trade confirmation slip gets printed at the trader workstation of the user with a unique trade number. The system also broadcasts a message to the entire market through the ticker window displaying the details of the trade.

2.6 Risk Management in Trades

As seen above, most operations are handled by the system, thus minimising the chances of errors or malpractices.

A significant risk relates to acceptance of client in the system. SEBI has come out with various directives for its regulated intermediaries. These cover Know Your Client (KYC) norms, Anti-Money Laundering (AML), Client Due Diligence (CDD) and Combating Financing of Terrorism (CFT). It is important for intermediaries to ensure that their employees are adequately trained on the requirements. An easily accessible manual should stipulate the prevailing documentation and procedural requirements. Changes in norms should be intimated to all concerned.

Further, the intermediary needs to ensure that these requirements are being complied with. Internal audit should do test-checking on an ongoing basis. Non-compliance with the prescribed procedures needs to be dealt with firmly, to ensure that a suitable culture is embedded in the organisation.

Errors in entering orders can wreak havoc in the market. For example, a wrong price entry can give a misleading message about the security to the market as a whole.

Orders can be modified or cancelled until the trade is executed. Once the order is matched and a trade is executed, then the TM stands committed to the transaction. Mistakes in order entry can wipe out the net worth of a TM. For instance, by selling away securities at a price much below the prevailing price, or buying them at a price much above the prevailing price.

Such errors can also have a second-order impact, when automated trading systems respond to the abnormal price movement by releasing more orders into the system.

NSE sets 'price freeze' and 'quantity freeze' limits to minimise the impact of such punching errors. Orders beyond the limit are not accepted in the trading system, without an off-line confirmation from the TM.

The TM can also balance its risks by setting prudent trading limits for its Corporate Manager, Branch Managers and Dealers. Besides, it should monitor the day-end reports for any abnormalities.

Self-Assessment Questions

- Demat reduces the operations risk of bad delivery in the stock market.
  - **True**
  - False

- Which of the following do not clear trades of other TM?
  - **SCM**
  - PCM
  - TCM
  - All the above

- Authorised Persons issue contract notes for trades of clients they have introduced to a TM.
  - True
  - **False**

- Match of buy and sell orders through the NEAT system is effected without human intervention.
  - **True**
  - False

- Dealers are users at the _____ level of hierarchy in NEAT.
  - **Lowest**
  - Highest
  - Median
  - Highest for buy orders; lowest for sell orders

- Which of the following help minimise the impact of punching errors in NEAT?
  - Price freeze
  - Quantity freeze
  - **Both the above**
  - None of the above

Chapter 3 : Clearing & Settlement of Trades

While NSE provides a platform for trading to its trading members, NSCCL determines the funds/securities obligations of the trading members and ensures that trading members meet their obligations.

NSCCL becomes the legal counterparty to the net settlement obligations of every member. This principle is called `novation'. NSCCL is obligated to meet all settlement obligations, regardless of member defaults, without any discretion. Once a member fails on any obligations, NSCCL immediately cuts off trading facilities of that member and initiates the recovery process.

NSCCL protects itself through a system of ensuring capital adequacy and collecting margins.

3.1 Transaction Cycle

As illustrated in Figure 3.1, the transaction goes through following stages:

(a) A person holding assets (securities/funds), either to meet his liquidity needs or to reshuffle his holdings in response to changes in his perception about risk and return of the assets, decides to buy or sell the securities.

(b) He selects a broker and instructs him to place buy/sell order on an exchange.

(c) The order is converted to a trade as soon as it finds a matching sell/buy order.

(d) At the end of the day, various such trades are netted to determine the obligations of each Trading Member to deliver securities/funds as per the settlement schedule.

(e) Buyer (seller) delivers funds (securities) and receives securities (funds) and acquires ownership of the securities.

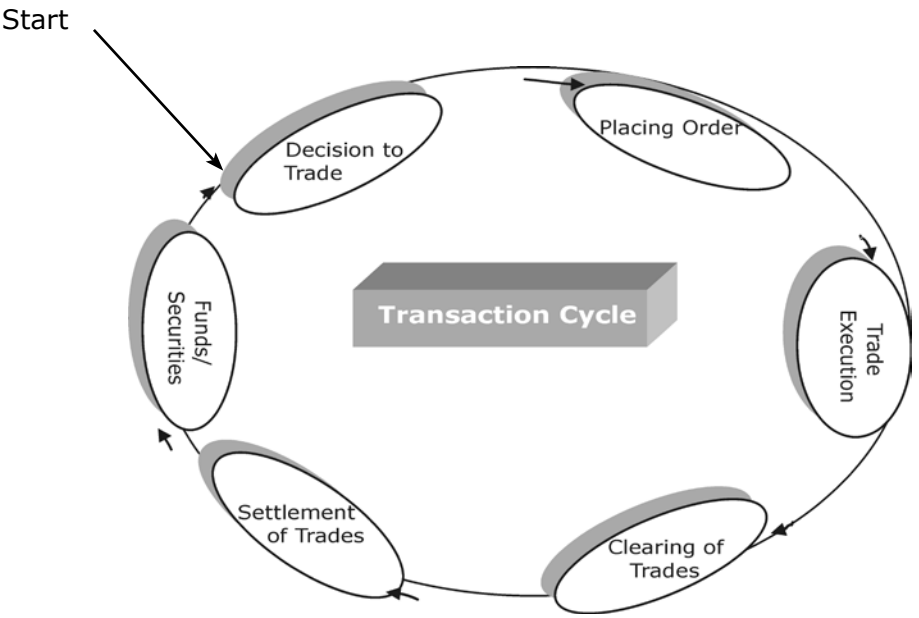

Figure 3.1: Transaction Cycle

3.2 Clearing

At the end of each trading day, concluded or locked-in trades are received from NSE by NSCCL.

The NSCCL interposes itself as a central counterparty between the two counterparties of every trade, and nets the positions so that a member has security wise net obligation to receive or deliver a security and has to either pay or receive funds. A multi-lateral netting procedure is adopted for the purpose.

On this basis, NSCCL determines the amount/securities that each counter-party owes or is due to receive on the settlement date. NSCCL electronically transfers the data to Clearing Members (CMs).

3.3 Settlement

The settlement process begins as soon as Trading Members' obligations are determined through the clearing process. The clearing banks and depositories provide the necessary interface between the custodians/clearing members (who clear for the trading members or their own transactions) for settlement of these obligations.

- Clearing Members

  They are responsible for settling the obligations of TM for whom they are responsible. The obligations are determined by the NSCCL based on trades executed by the TM.

  Clearing Members have to make available funds and/or securities in the designated accounts with clearing bank/depository participant, as the case may be, to meet their obligations on the settlement day.

  In the capital market segment, all trading members of the Exchange are required to become the Clearing Member of the Clearing Corporation.

  Self-Clearing Members (SCM) have the right to clear their own trades, but not the trades of other members. Trading-cum-Clearing Members are authorized to clear their own trades, as well as trades of other members.

  Professional clearing members (PCM) clear but do not trade. PCMs operate only in the F&O segment.

- Custodians

  Many institutional investors appoint custodians for their trades. In NSCCL, custodian is a clearing member but not a trading member. The custodian settles trades assigned by trading members.

  The custodian has documentary evidence of the title to the securities traded (ownership is with the person who owns the security).

The custodian is required to confirm whether it is going to settle a particular trade or not. If it is confirmed, the NSCCL assigns that obligation to that custodian and the custodian is required to settle it on the settlement day. If the custodian rejects the trade, the obligation is assigned back to the trading/clearing member.

- Clearing Banks

  Clearing banks are a key link between the clearing members and NSCCL for funds settlement. Every clearing member is required to open a dedicated settlement account with one of the clearing banks. Based on his obligation as determined through clearing, the clearing member makes funds available in the clearing account for the pay-in and receives funds in case of a pay-out.

- Depositories

  A depository is an entity where the securities of an investor are held in electronic form. The person who holds a demat account is a beneficiary owner. In case of a joint account, the account holders are beneficiary holders of that joint account.

  Depositories help in the settlement of the dematerialised securities. Each custodian/ clearing member is required to maintain a clearing pool account with the depositories. He is required to make available the required securities in the designated account on settlement day.

  The depository runs an electronic file to transfer the securities from accounts of the custodians/clearing member to that of NSCCL on the pay-in day.

  Similarly, as per the schedule of allocation of securities determined by the NSCCL, the depositories transfer the securities on the pay-out day from the account of the NSCCL to those of members/custodians.

The clearing corporation provides a major link between the clearing banks, clearing members and the depositories. This link ensures actual movement of funds and securities on the prescribed pay-in and pay-out day. The core processes involved in the settlement process are:

3.3.1 Pay-in of Funds and Securities

The members bring in their funds/securities to the NSCCL.

Members with securities obligations make available the required securities in designated accounts with the depositories by the prescribed pay-in time. The depositories move the securities available in the accounts of members to the account of the NSCCL.

Likewise, members with funds obligations make available the required funds in the designated accounts with clearing banks by the prescribed pay-in time. The NSCCL sends electronic instructions to the clearing banks to debit the member’s accounts to the extent of payment obligations. The banks process these instructions, debit the accounts of the members and credit the accounts of the NSCCL.

3.3.2 Pay-out of Funds and Securities

After processing for shortages of funds/securities and arranging for movement of funds from surplus banks to deficit banks through RBI clearing, the NSCCL sends electronic instructions to the depositories/clearing banks to release pay-out of securities/funds.

The depositories and clearing banks debit the accounts of NSCCL and credit the settlement accounts of members.

Settlement is complete upon release of pay-out of funds and securities to custodians/ members.

Settlement is deemed to be complete upon declaration and release of pay-out of funds and securities. Exceptions may arise when CMs deliver less than their obligation (short delivery of securities) or if there are bad deliveries or company objections on the pay-out day.

NSCCL identifies the short deliveries and conducts a buying-in auction on the day after the pay-out day through the NSE trading system.

The delivering CM is first debited by an amount equivalent to the securities not delivered and valued at a valuation price (the closing price as announced by NSE on the day previous to the day of the valuation). If the buy-in auction price is more than the valuation price, the CM is required to make good the difference.

All shortages not bought-in are deemed closed out at the highest price between the first day of the trading period till the day of squaring off or closing price on the auction day plus 20%, whichever is higher. This amount is credited to the receiving member's account on the auction pay-out day.

The settlement process for transactions in securities in the CM segment of NSE is presented in the Figure 3.2.

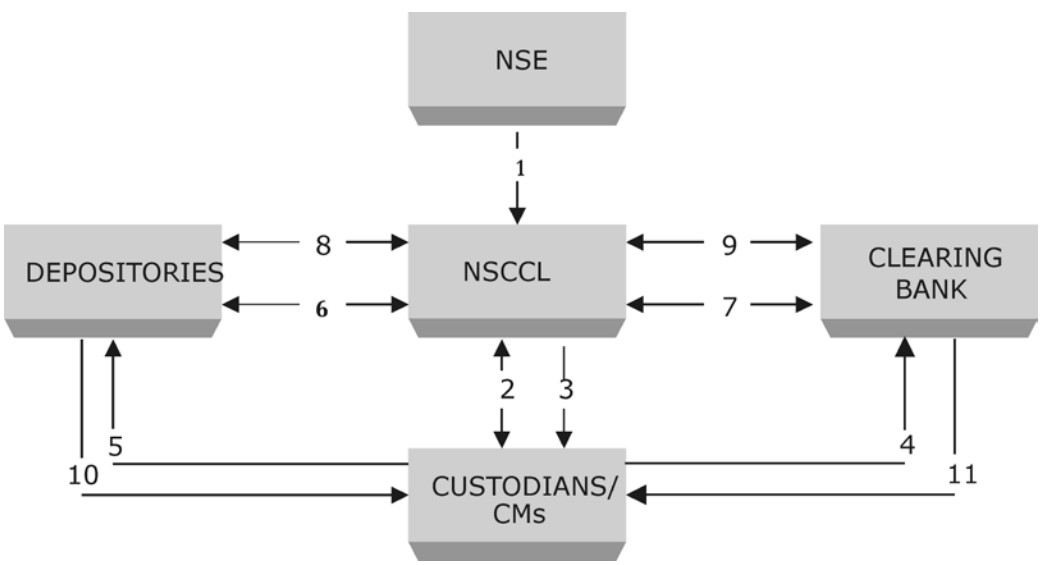

Figure 3.2: Settlement Process in CM segment of NSE

Explanation for Figure 3.2:

(1) Trade details from Exchange to NSCCL (real-time and end of day trade file).

(2) NSCCL notifies the consummated trade details to CMs/custodians who affirm back. Based on the affirmation, NSCCL applies multilateral netting and determines obligations.

(3) Download of obligation and pay-in advice of funds/securities.

(4) Instructions to clearing banks to make funds available by pay-in time.

(5) Instructions to depositories to make securities available by pay-in-time.

(6) Pay-in of securities (NSCCL advises depository to debit pool account of custodians/ CMs and credit its account and depository does it).

(7) Pay-in of funds (NSCCL advises Clearing Banks to debit account of custodians/CMs and credit its account and clearing bank does it).

(8) Pay-out of securities (NSCCL advises depository to credit pool account of custodians/ CMs and debit its account and depository does it).

(9) Pay-out of funds (NSCCL advises Clearing Banks to credit account of custodians/CMs and debit its account and clearing bank does it).

(10) Depository informs custodians/CMs through DPs.

(11) Clearing Banks inform custodians/CMs.

A fixed schedule (number of days from the Trade Date) is set for each stage in the settlement process, including post-settlement activities like handling of auctions and bad deliveries. Physical securities and dematerialised securities have different schedules.

NSCCL has introduced the facility of direct payout (i.e. direct delivery of securities) to clients' account on both the depositories. It ascertains from each clearing member, the beneficiary account details of their respective clients who are due to receive pay out of securities.

Based on the information received from members, the clearing corporation sends payout instructions to the depositories, so that the client receives the pay out of securities directly to their accounts on the pay-out day. The client receives payout to the extent of instructions received from the respective clearing members. To the extent of instruction not received, the securities are credited to the CM pool account of the member.

3.4 Settlement Risks

The risks can be broadly grouped as follows:

3.4.1 Counter-Party Risk

This arises if parties do not discharge their obligations fully, when due, or at any time thereafter. This has two components:

- Replacement Cost Risk

  This arises from the failure of one of the parties to a transaction.

  While the non-defaulting party tries to replace the original transaction at current prices, he loses the profit that has accrued on the transaction between the date of the original transaction and the date of the replacement transaction. The seller/buyer of the security loses this unrealised profit if the current price is below/above the transaction price.

  Both parties encounter this risk as prices are uncertain. This risk has been reduced by reducing time gap between transaction and settlement and by legally binding netting systems.

- Principal Risk

  This arises if a party discharges his obligations but the counterparty defaults. The seller/buyer of the security suffers this risk when he delivers/makes payment, but does not receive payment/delivery. This risk can be eliminated by delivery vs. payment mechanism (DVP), which ensures delivery only against payment.

  This risk has been reduced for investors, by having a central counterparty (NSCCL) which becomes the buyer to every seller and the seller to every buyer.

A variant of counterparty risk is liquidity risk which arises if one of the parties to transaction does not settle on the settlement date, but later. The seller/buyer, who does not receive payment/delivery when due, may have to borrow funds/securities to complete his payment/ delivery obligations.

Another variant is the third party risk which arises if the parties to a trade are permitted or required to use the services of a third party, which fails to perform. For example, the failure of a clearing bank which helps in payment can disrupt settlement. This risk is reduced by allowing parties to have accounts with multiple banks. Similarly, the users of custodial services face risk if the concerned custodian becomes insolvent, acts negligently, etc.

3.4.2 System Risk

This comprises of operational, legal and systemic risks.

The operational risk arises from possible operational failures such as errors, fraud, outages etc.

The legal risk arises if the laws or regulations do not support enforcement of settlement obligations or are uncertain.

Systemic risk arises when failure of one of the parties to discharge his obligations leads to failure by other parties. The domino effect of successive failures can cause a failure of the settlement system.

These risks have been contained by enforcement of an elaborate margining and capital adequacy standards to secure market integrity, settlement guarantee funds to provide counter-party guarantee, legal backing for settlement activities and business continuity plan, etc.

3.5 Risk Management

A sound risk management system is integral to/pre-requisite for an efficient clearing and settlement system. NSCCL ensures that trading members' obligations are commensurate with their net worth. It has put in place a comprehensive risk management system, which is constantly monitored and upgraded to pre-empt market failures.

One approach to risk-management is by ensuring capital adequacy of the members. Therefore, stringent requirements have been set for paid up capital and net worth. Besides, interest-free security deposits need to be maintained.

Margins form another key part of the risk management system. In the stock markets there is always an uncertainty in the movement of share prices. This uncertainty leads to risk which is addressed by margining system of stock markets.

Daily margins payable by the trading members in the Cash market consists of the following:

- Value at Risk (VaR) margin

  VaR is a single number, which encapsulates whole information about the risk in a portfolio. It measures potential loss from an unlikely adverse event in a normal market environment.

  For liquid securities, the VaR margins are based only on the volatility of the security while for other securities, the volatility of the market index is also used in the computation.

  It is charged on the net outstanding position (buy value-sell value) of the respective clients on the respective securities for all open settlements. There would be no netting off of positions across different settlements.

  The net position at a client level for a member is arrived at. Thereafter, it is grossed across all the clients including proprietary position to arrive at the gross open position for the member.

  The VaR margin is collected on an upfront basis by adjusting against the total liquid assets of the member at the time of trade.

- Mark to Market Margin

  Mark to market loss is calculated by marking every transaction to the closing price of the security at the end of the trading day.

  In case the security has not been traded on a particular day, the latest available closing price at the NSE is considered as the closing price.

In case the net outstanding position in any security is nil, the difference between the buy and sell values is considered as notional loss for the purpose of calculating the mark to market margin payable.

The mark to market margin (MTM) is collected from the member before the start of trading on the next day. The MTM margin is collected/adjusted from/against the cash/ cash equivalent component of the liquid net worth deposited with the Exchange.

The MTM margin is collected on the gross open position of the member. The gross open position means the gross of all net positions across all the clients of a member including its proprietary position. For this purpose, the position of a client would be netted across its various securities and the positions of all the clients of a broker would be grossed.

There is no netting off of the positions and set off against MTM profits across two rolling settlements i.e. T day and T-1 day. However, for computation of MTM profits/ losses for the day, netting or set off against MTM profits is permitted.

In case of Trade for Trade Segment (TFT segment) each trade is marked to market based on the closing price of that security. The MTM margin so collected is released on completion of pay-in of the settlement.

- Extreme Loss Margin

  The Extreme Loss Margin for any security is the higher of:

  - 5%, or
  - 1.5 times the standard deviation of daily logarithmic returns of the security price in the last six months. This computation is done at the end of each month by taking the price data on a rolling basis for the past six months and the resulting value is applicable for the next month.

The Extreme Loss Margin is collected/adjusted against the total liquid assets of the member on a real time basis.

The Extreme Loss Margin is collected on the gross open position of the member. The gross open position for this purpose means the gross of all net positions across all the clients of a member including its proprietary position.

There is no netting off of positions across different settlements. The Extreme Loss Margin collected is released on completion of pay-in of the settlement.

Upfront margin rates (VaR margin + Extreme Loss Margin) applicable for all securities in Trade for Trade- Surveillance (TFTS) is 100%.

The margins are computed at client level. A member entering an order needs to enter the client code. Based on this information, margin is computed at the client level. The margin will be payable by the trading members on upfront basis.

In case of any shortfall in margin:

- The members are not permitted to trade with immediate effect.
- Penalty is charged for margin violation. The rate depends on the number of occurrences of the default.

3.6 Investor Protection

Investors are well protected in the whole system.

- Settlement Guarantee Mechanism

  A large Settlement Guarantee Fund provides the cushion for any residual risk.

  In the event of failure of a trading member to meet settlement obligations or committing default, the Fund is utilized to the extent required for successful completion of the settlement. This has eliminated counter party risk of trading on the Exchange. The market now has full confidence that settlements will take place in time, and will be completed irrespective of possible default by isolated trading members.

  The Settlement Guarantee Fund is an important element in facilitating the settlement process. The Fund operates like a self-insurance mechanism and is funded through the contributions made by trading members, transaction charges, penalty amounts, fines etc. recovered by NSCCL.

  A part of the cash deposit and the entire security deposit of every clearing member with the Exchange has been converted into an initial contribution towards the Settlement Guarantee Fund.

  There is a provision that as and when volumes of business increase, members may be required to make additional contributions allowing the fund to grow along with the market volumes.

- Investment Protection Fund

  An Investor Protection Fund (IPF) has been set up as a trust under Bombay Public Trust Act, 1950. It is named National Stock Exchange Investor Protection Fund Trust and is administered by the Trustees.

  The purpose of IPF is to take care of investor claims which may arise out of non-settlement of obligations by trading members. The IPF is utilised to settle claims of such investors whose trading member has been declared a defaulter or expelled by the Exchange.

  Further the stock exchanges have been allowed to utilize interest income earned on IPF for Investor Protection Fund for investor education, awareness and research. The maximum amount of claim payable from the IPF to an investor is Rs. 11 lakh.

Self-Assessment Questions

- How does NSCCL protect itself against member defaults?
  - Capital adequacy requirements
  - Margins
  - **Both the above**
  - None of the above

- Custodian is a clearing member, but not trading member.
  - **True**
  - False

- Clearing banks are responsible for pay in and pay out of securities
  - True
  - **False**

- NSCCL gives consummated trade details to
  - TM
  - **CM**
  - Clearing bank
  - Depository

- Securities have to necessarily go through the pool account of the CM before they reach the demat account of client.
  - True
  - **False**

- Counter-party risk is minimised through
  - Netting
  - Reducing time gap between trade and settlement
  - **Both the above**
  - None of the above

- VaR margin for illiquid securities is calculated based on
  - Volatility of security
  - Volatility of index
  - **Both the above**
  - None of the above

Chapter 4 : Workflow Design

4.1 Front Office, Middle Office & Back Office

Chapter 1 mentioned the need for work flow design with internal checks. Chapter 2 covered Trade Management, while the previous chapter discussed Clearing & Settlement.

The normal approach in banking and finance organisations is to strengthen the internal control system by segregating the front office, middle office and back office activities, as follows:

- Front Office
  - The market interface for executing trades
  - Registers clients
  - Receives orders from clients (In the case of equities, these orders go automatically into the stock exchange trading system, subject to system checks on limits. Brokers can give their institutional clients Direct Market Access, where their orders go into the stock exchange system without any intervention by the broker).
  - Places proprietary orders in the market (actual decision to invest or sell would be taken by the investment manager)
  - Executes the orders in the market

Customer service executives and dealers are part of the front office.

- Middle Office
  - An important link between front office and back office – helps the former execute orders; helps the latter settle the transactions and account for the same
  - KYC documentation of clients is best checked by middle office, because front office has a vested interest in compromising on documentation while registering the client
  - The system checks to ensure that the client has adequate funds (or approved credit) before trading are a middle office responsibility.
  - Handles risk management especially credit and market risks of the organisation (Point to note is that risk management advice for clients will be offered by front office as a revenue generator. The front office will also place the consequent client orders, which will go through the routine middle office checks for limits)
  - Does various validations. For instance, dealers may trade based on their own models. Middle office will have its own scientific models for valuation and profit booking.

- Some institutional investors, such as Foreign Institutional Investors (FIIs) appoint custodians for their investments. When trades are done on behalf of such institutional investors, the custodian has to confirm in the system that it will settle the transaction. Accordingly, the settlement obligation goes to the custodian. This again is a back-office function.

Risk managers, surveillance staff and financial modellers are part of the middle office.

- Back Office
  - Clearing & Settlement of transactions
  - Accounting of transactions
  - Just as credit and market risk management are more of a middle office function, operating risk is more oriented to the back office.

Settlement staff and accounts personnel are part of the back office.

4.2 Risk Events

Various pro-active steps for operating risk management have been discussed. Despite the best laid plans and work flows, operating risk events do occur. The first re-active step to managing the risk is to capture the risk events.

The risk event is to be captured, even if there is no loss for the company. For example, if money is transferred to a wrong account and quickly retrieved before it is withdrawn from the wrong account, then there is no loss to the bank or the rightful claimant of the money. Yet, it is an operating risk event. The technical name for such events is "near miss". These too need to be captured as part of the risk management system.

A listing of various operating risk events is mere historical information. Proper analysis calls for grouping of these events into meaningful categories. Each such category will have a different cause and a different solution, and a different implication in terms of capital adequacy requirements. Therefore, the classification of risk event types in the data base is critical. Chapter 5 discusses the Detailed Loss Event Type Classification mentioned in Basel II.

Self-Assessment Questions

- The split of front office, middle office and back office is done to
  - Increase number of jobs in the market
  - **Enhance internal controls**
  - Reduce transaction cost
  - All the above

- _____ is the market interface for executing trades.
  - **Front office**
  - Middle office
  - Back office
  - None of the above

- Dealers are part of
  - **Front office**
  - Middle office
  - Back office
  - None of the above

- Risk management function for market risks is part of
  - Front office
  - **Middle office**
  - Back office
  - None of the above

- Valuation function is part of
  - Front office
  - **Middle office**
  - Back office
  - None of the above

- Settlement staff are part of
  - Front office
  - Middle office
  - **Back office**
  - None of the above

Chapter 5 : BASEL Overview

5.1 Bank for International Settlements (BIS)

Established on 17 May 1930, BIS is the world's oldest international financial organisation. It was created to handle the reparation payments imposed on Germany by the Treaty of Versailles following the First World War. It now focuses on co-operation among central banks and, increasingly, other agencies in pursuit of monetary and financial stability.

BIS has its head office at Basel, Switzerland and two representative offices – one, in the Hong Kong Special Administrative Region of the People's Republic of China and the other, in Mexico City.

BIS has a mission to serve central banks in their pursuit of monetary and financial stability, to foster international cooperation in those areas and to act as a bank for central banks. It pursues its mission by:

- promoting discussion and facilitating collaboration among central banks;
- supporting dialogue with other authorities that are responsible for promoting financial stability;
- conducting research on policy issues confronting central banks and financial supervisory authorities;
- acting as a prime counterparty for central banks in their financial transactions; and
- serving as an agent or trustee in connection with international financial operations.

Central banks or monetary authorities of 60 countries, including India, are members of BIS.

- The most important meetings held at the BIS are the regular meetings of Governors and senior officials of member central banks. These are held every two months in Basel, for participants to discuss the world economy and financial markets, and to exchange views on topical issues of central bank interest or concern.
- Other meetings of senior officials of the central banks are held to focus on the conduct of monetary policy, the surveillance of international financial markets and central bank governance issues.
- Besides, meetings of experts are held on monetary and financial stability issues as well as on more technical issues such as legal matters, reserve management, IT systems, internal audit and technical cooperation.

Central banks and international institutions are the customers of BIS. It does not accept money from private individuals, companies or trusts.

In a globally inter-connected world, turmoil in any part of the world has repercussions on the rest of the world. Therefore, BIS recommends policies for central banks and governments.

5.2 Basel Accords

5.2.1 Basel I

In 1988, the G-10 central bankers agreed to apply common minimum capital standards to their banking industries. This was to be achieved by end-year 1992. This International Convergence of Capital Measurement and Capital Standards, called the Basel Capital Accord, focussed almost entirely on credit risk.

As part of a standardised model, weighting factors were specified for different kinds of exposures. For example:

- 0% for
  - Cash;
  - Claims on central governments and central banks denominated in national currency and funded in that currency;
  - Other claims on Organisation for Economic Co-operation & Development (OECD) central governments and central banks;
  - Claims collateralised by cash or OECD central-government securities or guaranteed by OECD central governments.
- Countries had the discretion to specify 10% risk weight for
  - Claims on domestic public-sector entities (PSE), excluding central government, and loans guaranteed by such entities.
- 20% for
  - Claims on multilateral development banks

    [International Bank for Re-construction & Development (IBRD), Inter-American Development Bank (IADB), Asian Development Bank(ADB), African Development Bank (AfDB), European Investment Bank(EIB)] and claims guaranteed by, or collateralised by securities issued by such banks;
  - Claims on banks incorporated in the OECD and loans guaranteed by OECD incorporated banks;
  - Claims on banks incorporated in countries outside the OECD with a residual maturity of up to one year and loans with a residual maturity of up to one year guaranteed by banks incorporated in countries outside the OECD.
- 50% for
  - Loans fully secured by mortgage on residential property that is or will be occupied by the borrower or that is rented.

- 100% for
  - Claims on the private sector;
  - Claims on banks incorporated outside the OECD with a residual maturity of over one year;
  - Claims on central governments outside the OECD (unless denominated in national currency - and funded in that currency);
  - Claims on commercial companies owned by the public sector;
  - Premises
  - Plant and equipment and
  - Other fixed assets.

For example, if an exposure was US$500mn and weighting factor 10%, then the risk-weighted asset value was US$500mn X 10% i.e. US$50mn. Each bank had to maintain minimum capital of 8% of the risk-weighted asset value of its exposures.

Credit conversion factors were specified for off-balance sheet items. For example:

- 100%, for Direct credit substitutes, e.g. general guarantees of indebtedness (including standby letters of credit serving as financial guarantees for loans and securities) and acceptances (including endorsements with the character of acceptances).
- 50%, for certain transaction-related contingent items (e.g. performance bonds, bid bonds, warranties and standby letters of credit related to particular transactions).
- 20% for short-term self-liquidating trade-related contingencies (such as documentary credits collateralised by the underlying shipments).

Separate treatment was provided for interest related and exchange-rate related contingencies.

Two forms of capital were defined in the Accord:

- Core Capital which was the equity capital and reserves disclosed in the published accounts. Non-cumulative perpetual preferred stock was included, but not, cumulative perpetual preferred stock. Core Capital is commonly referred to as 'Tier 1 Capital'
- Supplementary Capital i.e. Tier 2 capital comprised undisclosed reserves, revaluation reserves, general loss provisions, hybrid debt capital instruments and subordinated term debt.

  Conditions were attached to inclusion of each of these items as Tier 2 capital.

  The total Tier 2 capital was permitted for the capital adequacy calculations upto the value of Tier 1 capital.

  Subordinated term debt was permitted upto 50% of Tier 1 capital.

Goodwill and investment in non-consolidated subsidiaries involved in banking and financial services business was subtracted from capital for the purpose of capital adequacy calculations.

In 1996, modifications were made to address market risk better.

5.2.2 Basel II

In 2004, the G-10 central bankers agreed to a revised framework, based on the experience. It made greater use of assessments of risk provided by banks' internal systems as inputs to capital calculation. However, detailed set of minimum requirements were designed to ensure the integrity of these internal risk assessments.

Basel II also provided a range of options for determining the capital requirements for credit risk and operational risk to allow banks and supervisors (i.e. the central banks) to select approaches that were most appropriate for their operations and their financial market infrastructure.

BIS wanted the framework to be applied on a consolidated basis to internationally active banks. It was to be applied on a fully consolidated basis, to any holding company that was the parent entity within a banking group to ensure that it captured the risk of the whole banking group. It applied to all internationally active banks at every tier within a banking group, also on a fully consolidated basis. Further, to ensure adequate protection of depositors, supervisors had to check capital adequacy of banks on stand-alone basis too.

Basel II focused on three important risks:

- **Credit Risk**

  This is the risk that a party to whom money has been given is unable to repay as per the terms of the arrangement.

  Banks were given a choice between two broad methodologies for calculating their capital requirements for credit risk.

  - Standardised Approach based on external credit rating
  - Internal Ratings-based (IRB) Approach

  Risk weight of 150% or higher were provided in the following cases:

  - Claims on sovereigns, PSEs, banks, and securities firms rated below B-
  - Claims on corporates rated below BB-
  - Past due loans
  - Securitisation tranches rated between BB+ and BB- were to be risk weighted at 350%.

IRB approach relies on bank's own internal estimates of risk components in determining the capital requirement for a given exposure. The risk components include measures of the

probability of default (PD), loss given default (LGD), the exposure at default (EAD), and effective maturity (M).

IRB approach is based on measures of unexpected losses (UL) and expected losses (EL). The risk-weight functions produced capital requirements for the UL portion. EL was treated separately.

Under the IRB approach, banks categorise banking-book exposures into broad classes of assets with different underlying risk characteristics. The classes of assets are (a) corporate, (b) sovereign, (c) bank, (d) retail, and(e) equity.

Within the corporate asset class, five sub-classes of specialised lending are separately identified viz. project finance, object finance, commodities finance, income-producing real estate, and high-volatility commercial real estate.

Within the retail asset class, three sub-classes are separately identified viz. (a) exposures secured by residential properties(b) qualifying revolving retail exposures and (c) all other retail exposures.

In order to be eligible for the IRB approach, banks must meet the disclosure requirements set out in Pillar 3 (discussed in a subsequent section).

- **Market Risk**

  Market risk is defined as the risk of losses in on and off-balance-sheet positions arising from movements in market prices. The following risks are covered here:

  - Risks pertaining to interest rate related instruments and equities in the trading book;
  - Foreign exchange risk and commodities risk throughout the bank.

  A trading book consists of positions in financial instruments and commodities held either with trading intent or in order to hedge other elements of the trading book.

  To be eligible for trading book capital treatment, financial instruments must either be free of any restrictive covenants on their tradability or able to be hedged completely. In addition, positions should be frequently and accurately valued, and the portfolio should be actively managed.

  A financial instrument is any contract that gives rise to both a financial asset of one entity and a financial liability or equity instrument of another entity. Financial instruments include both, primary financial instruments (or cash instruments) and derivative financial instruments.

  A financial asset is any asset that is cash, the right to receive cash or another financial asset; or the contractual right to exchange financial assets on potentially favourable terms, or an equity instrument.

A financial liability is the contractual obligation to deliver cash or another financial asset or to exchange financial liabilities under conditions that are potentially unfavourable.

Positions held with trading intent are those held intentionally for short-term resale and/ or with the intent of benefiting from actual or expected short-term price movements or to lock in arbitrage profits, and may include for example proprietary positions, positions arising from client servicing (e.g. matched principal broking) and market making.

Banks must have clearly defined policies and procedures for determining which exposures to include in, and to exclude from, the trading book for purposes of calculating their regulatory capital, to ensure compliance with the criteria for trading book and taking into account the bank's risk management capabilities and practices.

Compliance with these policies and procedures must be fully documented and subject to periodic internal audit.

These policies and procedures should, at a minimum, address the general considerations listed below.

- The activities the bank considers to be trading and as constituting part of the trading book for regulatory capital purposes;
- The extent to which an exposure can be marked-to-market daily by reference to an active, liquid two-way market;
- For exposures that are marked-to-model, the extent to which the bank can:
    - Identify the material risks of the exposure;
    - Hedge the material risks of the exposure and the extent to which hedging instruments would have an active, liquid two-way market;
    - Derive reliable estimates for the key assumptions and parameters used in the model.
- The extent to which the bank can and is required to generate valuations for the exposure that can be validated externally in a consistent manner;
- The extent to which legal restrictions or other operational requirements would impede the bank's ability to effect an immediate liquidation of the exposure;
- The extent to which the bank is required to, and can, actively risk manage the exposure within its trading operations; and
- The extent to which the bank may transfer risk or exposures between the banking and the trading books and criteria for such transfers.

The basic requirements for positions eligible to receive trading book capital treatment are as follows:

- Clearly documented trading strategy for the position/instrument or portfolios, approved by senior management (which would include expected holding horizon).
- Clearly defined policies and procedures for the active management of the position, which must include:
    - positions are managed on a trading desk;
    - position limits are set and monitored for appropriateness;
    - dealers have the autonomy to enter into/manage the position within agreed limits and according to the agreed strategy;
    - positions are marked to market at least daily and when marking to model the parameters must be assessed on a daily basis;
    - positions are reported to senior management as an integral part of the institution's risk management process; and
    - positions are actively monitored with reference to market information sources (assessment should be made of the market liquidity or the ability to hedge positions or the portfolio risk profiles). This would include assessing the quality and availability of market inputs to the valuation process, level of market turnover, sizes of positions traded in the market, etc.
- Clearly defined policy and procedures to monitor the positions against the bank's trading strategy including the monitoring of turnover and stale positions in the bank's trading book.

Prudent valuation practices should include the following:

- Systems & Controls

  Banks must establish and maintain adequate systems and controls sufficient to give management and supervisors the confidence that their valuation estimates are prudent and reliable. These systems must be integrated with other risk management systems within the organisation (such as credit analysis). Such systems must include:

    - Documented policies and procedures for the process of valuation. This includes clearly defined responsibilities of the various areas involved in the determination of the valuation, sources of market information and review of their appropriateness, frequency of independent valuation, timing of closing prices, procedures for adjusting valuations, end of the month and ad-hoc verification procedures; and

- Clear and independent (i.e. independent of front office) reporting lines for the department accountable for the valuation process. The reporting line should ultimately be to a main board executive director.

- Valuation Methodologies

  - Marking to Market

    Marking-to-market is at least the daily valuation of positions at readily available close out prices that are sourced independently. Examples of readily available close out prices include exchange prices, screen prices, or quotes from several independent reputable brokers.

    Banks must mark-to-market as much as possible. The more prudent side of bid/offer must be used unless the institution is a significant market maker in a particular position type and it can close out at mid-market.

  - Marking to Model

    Where marking-to-market is not possible, banks may mark-to-model, where this can be demonstrated to be prudent.

    Marking-to-model is defined as any valuation which has to

    be benchmarked, extrapolated or otherwise calculated from a market input. When marking to model, an extra degree of conservatism is appropriate. Supervisory authorities will consider the following in assessing whether a mark-to-model valuation is prudent:

    - Senior management should be aware of the elements of the trading book which are subject to mark to model and should understand the materiality of the uncertainty this creates in the reporting of the risk/ performance of the business.

    - Market inputs should be sourced, to the extent possible, in line with market prices. The appropriateness of the market inputs for the particular position being valued should be reviewed regularly.

    - Where available, generally accepted valuation methodologies for particular products should be used as far as possible.

    - Where the model is developed by the institution itself, it should be based on appropriate assumptions, which have been assessed and challenged by suitably qualified parties independent of the development process. The model should be developed or approved independently of the front office. It should be independently tested. This includes validating the mathematics, the assumptions and the software implementation.

- There should be formal change control procedures in place and a secure copy of the model should be held and periodically used to check valuations.
- Risk management should be aware of the weaknesses of the models used and how best to reflect those in the valuation output.
- The model should be subject to periodic review to determine the accuracy of its performance (e.g. assessing continued appropriateness of the assumptions, analysis of P&L versus risk factors, comparison of actual close out values to model outputs).
- Valuation adjustments should be made as appropriate, for example, to cover the uncertainty of the model valuation.

Independent price verification is distinct from daily mark-to-market. It is the process by which market prices or model inputs are regularly verified for accuracy.

While daily marking-to-market may be performed by dealers, verification of market prices or model inputs should be performed by a unit independent of the dealing room, at least monthly (or, depending on the nature of the market/trading activity, more frequently). It need not be performed as frequently as daily mark-to-market, since the objective, i.e. independent, marking of positions, should reveal any error or bias in pricing, which should result in the elimination of inaccurate daily marks.

Independent price verification entails a higher standard of accuracy in that the market prices or model inputs are used to determine profit and loss figures, whereas daily marks are used primarily for management reporting in between reporting dates. For independent price verification, where pricing sources are more subjective, e.g. only one available broker quote, prudent measures such as valuation adjustments may be appropriate.

Banks have a choice between two methodologies to measure the market risk:

- Measure the risks in a standardised manner, using the measurement frameworks prescribed by the Basel Committee for Banking Supervision.
- Use risk measures derived from the bank's own internal risk management models, subject to seven sets of conditions, namely:
  - certain general criteria concerning the adequacy of the risk management system;
  - qualitative standards for internal oversight of the use of models, notably by management;
  - guidelines for specifying an appropriate set of market risk factors (i.e. the market rates and prices that affect the value of banks' positions);

- quantitative standards setting out the use of common minimum statistical parameters for measuring risk;
- guidelines for stress testing;
- validation procedures for external oversight of the use of models;
- rules for banks which use a mixture of models and the standardised approach.

- **Operational Risk**

Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Legal risk is covered by the definition, but it excludes strategic and reputational risk.

Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.

Basel II discusses three methods for calculating operational risk capital charges in a continuum of increasing sophistication and risk sensitivity:

- The Basic Indicator Approach (BIA);
- The Standardised Approach (TSA); and
- Advanced Measurement Approaches (AMA).

Banks are encouraged to move along the spectrum of available approaches as they develop more sophisticated operational risk measurement systems and practices.

The topic is discussed in greater detail in Chapter 6.

Basel II provided for risk-mitigation through three pillars:

- **Pillar 1: Minimum Capital Requirements**

This was the approach taken in the Basel Capital Accord (Basel I). The components of capital were fine-tuned as part of Basel II.

Banks were permitted a third tier of Capital (Tier 3). This comprised short-term subordinated debt for the sole purpose of meeting a proportion of the capital requirements for market risks. It is not available for any capital requirement arising in respect of credit and counterparty risk in both trading and banking books.

Tier 3 capital is limited to 250% of a bank's Tier 1 capital that is required to support market risks. This means that a minimum of about (100 ÷ (100+250)) i.e. 28½% of market risks needs to be supported by Tier 1 capital that is not required to support risks in the remainder of the book.

Tier 2 elements may be substituted for Tier 3 up to the same limit of 250%. This is subject to eligible Tier 2 capital not exceeding total Tier 1 capital, and long-term subordinated debt not exceeding 50% of Tier 1 capital (as already discussed in Basel I).

For short-term subordinated debt to be eligible as Tier 3 capital, it needs, if circumstances demand, to be capable of becoming part of a bank's permanent capital and thus be available to absorb losses in the event of insolvency. It must, therefore, at a minimum:

- be unsecured, subordinated and fully paid up;
- have an original maturity of at least two years;
- not be repayable before the agreed repayment date unless the supervisory authority agrees;
- be subject to a lock-in clause which stipulates that neither interest nor principal may be paid (even at maturity) if such payment means that the bank falls below or remains below its minimum capital requirement.

- **Pillar 2: Supervisory Review Process**

The supervisory review process is intended not only to ensure that banks have adequate capital to support all the risks in their business, but also to encourage banks to develop and use better risk management techniques in monitoring and managing their risks.

Bank management needs to develop an internal capital assessment process and set capital targets that are commensurate with the bank's risk profile and control environment. They are responsible for ensuring that the bank has adequate capital to support its risks beyond the core minimum requirements.

However, increased capital should not be viewed as the only option for addressing increased risks confronting the bank. Other means for addressing risk, such as strengthening risk management, applying internal limits, strengthening the level of provisions and reserves, and improving internal controls, must also be considered. Capital should not be regarded as a substitute for addressing fundamentally inadequate control or risk management processes.

Pillar 2 has to specifically address the following areas:

- Risks considered under Pillar 1 that are not fully captured by the Pillar 1 process (e.g. credit concentration risk);
- Those factors not taken into account by the Pillar 1 process (e.g. interest rate risk in the banking book, business and strategic risk); and
- Factors external to the bank (e.g. business cycle effects).

Pillar 2 should also assess compliance with the minimum standards and disclosure requirements of the more advanced methods in Pillar 1, in particular the IRB framework for credit risk and the AMA for operational risk. Supervisors must ensure that these requirements are being met, both as qualifying criteria and on a continuing basis.

The Supervisory Review is governed by four basic principles:

- Banks should have a process for assessing their overall capital adequacy in relation to their risk profile and a strategy for maintaining their capital levels.
- The internal capital targets should be well founded and the targets have to be consistent with their overall risk profile and current operating environment.

  In assessing capital adequacy, bank management needs to be mindful of the particular stage of the business cycle in which the bank is operating.

  Rigorous, forward-looking stress testing that identifies possible events or changes in market conditions that could adversely impact the bank should be performed. The features of such a rigorous process are:

  - Board and senior management oversight;
  - Sound capital assessment;
  - Comprehensive assessment of risks;
  - Monitoring and reporting; and
  - Internal control review
- Supervisors should review and evaluate banks' internal capital adequacy assessments and strategies, as well as their ability to monitor and ensure their compliance with regulatory capital ratios. Supervisors should take appropriate supervisory action if they are not satisfied with the result of this process.
- Supervisors should expect banks to operate above the minimum regulatory capital ratios and should have the ability to require banks to hold capital in excess of the minimum.
- Supervisors should seek to intervene at an early stage to prevent capital from falling below the minimum levels required to support the risk characteristics of a particular bank and should require rapid remedial action if capital is not maintained or restored.

  Supervisors should consider a range of options if they are concerned that a bank is not meeting the requirements. This would include intensifying the

monitoring of the bank, restricting the payment of dividends, requiring the bank to prepare and implement a satisfactory capital adequacy restoration plan, and requiring the bank to raise additional capital immediately. Supervisors should have the discretion to use the tools best suited to the circumstances of the bank and its operating environment.

- **Pillar 3: Market Discipline**

This complements the minimum capital requirements (Pillar 1) and the supervisory review process (Pillar 2). The objective is to encourage market discipline by developing a set of disclosure requirements which will allow market participants to assess key pieces of information on the scope of application, capital, risk exposures, risk assessment processes, and hence the capital adequacy of the institution.

The banks' disclosures should be consistent with how senior management and the board of directors assess and manage the risks of the bank.

A bank should decide which disclosures are relevant for it based on the materiality concept. Information would be regarded as material if its omission or mis-statement could change or influence the assessment or decision of a user relying on that information for the purpose of making economic decisions. This definition is consistent with International Accounting Standards and with many national accounting frameworks.

The disclosures set out in Pillar 3 should be made on a semi-annual basis, subject to the following exceptions:

- Qualitative disclosures that provide a general summary of a bank's risk management objectives and policies, reporting system and definitions may be published on an annual basis.
- In recognition of the increased risk sensitivity of the Framework and the general trend towards more frequent reporting in capital markets, large internationally active banks and other significant banks (and their significant bank subsidiaries) must disclose their Tier 1 and total capital adequacy ratios, and their components, on a quarterly basis.
- Furthermore, if information on risk exposure or other items is prone to rapid change, then banks should also disclose information on a quarterly basis.
- In all cases, banks should publish material information as soon as practicable and not later than deadlines set by like requirements in national laws.

  In exceptional cases, disclosure of certain items of information required by Pillar 3 may prejudice seriously the position of the bank by making public,

information that is either proprietary or confidential in nature. In such cases, a bank need not disclose those specific items, but must disclose more general information about the subject matter of the requirement, together with the fact that, and the reason why, the specific items of information have not been disclosed. This limited exemption is not intended to conflict with the disclosure requirements under the accounting standards.

5.2.3 BASEL III

"Basel III" is a comprehensive set of reform measures, developed by the Basel Committee on Banking Supervision, to strengthen the regulation, supervision and risk management of the banking sector. These seek to:

- improve the banking sector's ability to absorb shocks arising from financial and economic stress, whatever the source;
- improve risk management and governance;
- strengthen banks' transparency and disclosures.

The reforms target:

- Bank-level, or micro-prudential, regulation, which will help raise the resilience of individual banking institutions to periods of stress.
- Macro-prudential, system wide risks that can build up across the banking sector as well as the pro-cyclical amplification of these risks over time.

These two approaches to supervision are complementary as greater resilience at the individual bank level reduces the risk of system wide shocks.

BASEL III draws on the learning from the global crisis starting 2007. The crisis highlighted that banks' risk exposures should be backed by a high quality capital base. Credit losses and write-downs come out of retained earnings, which is part of banks' tangible common equity base.

Accordingly, the predominant form of Tier 1 capital must be common shares and retained earnings. This standard is reinforced through a set of principles that also can be tailored to the context of non-joint stock companies to ensure they hold comparable levels of high quality Tier 1 capital.

Deductions from capital and prudential filters have been harmonised internationally and generally applied at the level of common equity or its equivalent in the case of non-joint stock companies.

The remainder of the Tier 1 capital base must be comprised of instruments that are subordinated, have fully discretionary non-cumulative dividends or coupons and have neither a maturity date nor an incentive to redeem.

Innovative hybrid capital instruments with an incentive to redeem through features such as step-up clauses, currently limited to 15% of the Tier 1 capital base, will be phased out.

In addition, Tier 2 capital instruments will be harmonised and so-called Tier 3 capital instruments, which were only available to cover market risks, eliminated.

Finally, to improve market discipline, the transparency of the capital base will be improved, with all elements of capital required to be disclosed along with a detailed reconciliation to the reported accounts.

The framework introduces measures to strengthen the capital requirements for counterparty credit exposures arising from banks' derivatives, repo and securities financing activities. These reforms will raise the capital buffers backing these exposures, reduce pro-cyclicality and provide additional incentives to move OTC derivative contracts to central counter parties, thus helping reduce systemic risk across the financial system. They also provide incentives to strengthen the risk management of counterparty credit exposures.

It also mitigates the reliance on external ratings of the Basel II framework. The measures include requirements for banks to perform their own internal assessments of externally rated securitisation exposures.

The recent global crisis was characterised by build-up of excessive on - and off - balance sheet leverage in the banking system. The Committee therefore is introducing a leverage ratio requirement that is intended to achieve the following objectives:

- Constrain leverage in the banking sector, thus helping to mitigate the risk of the destabilising de leveraging processes which can damage the financial system and the economy; and
- Introduce additional safeguards against model risk and measurement error by supplementing the risk-based measure with a simple, transparent, independent measure of risk.

The 2007 crisis also featured the pro-cyclical amplification of financial shocks throughout the banking system, financial markets and the broader economy. Basel III has introduced a number of measures to make banks more resilient to such pro-cyclical dynamics. These measures will help ensure that the banking sector serves as a shock absorber, instead of a transmitter of risk to the financial system and broader economy.

The leverage ratio is calculated in a comparable manner across jurisdictions, adjusting for any differences in accounting standards. The Committee has designed the leverage ratio to be a credible supplementary measure to the risk-based requirement with a view to migrating to a Pillar 1 treatment based on appropriate review and calibration.

The objective of the Liquidity Coverage Ratio (LCR) is to promote the short-term resilience of the liquidity risk profile of banks. It does this by ensuring that banks have an adequate stock of unencumbered high-quality liquid assets (HQLA) that can be converted easily and

immediately in private markets into cash to meet their liquidity needs for a 30 calendar day liquidity stress scenario.

The LCR will improve the banking sector's ability to absorb shocks arising from financial and economic stress, whatever the source, thus reducing the risk of spill-over from the financial sector to the real economy.

LCR is to be assessed in each significant currency, in order to monitor and manage the overall level and trend of currency exposure at a bank.

The minimum requirement of LCR is set at 60% by 1 January 2015; it will rise in equal annual steps to reach 100% on1 January 2019.

The framework also seeks to promote resilience over a longer time horizon by creating additional incentives for banks to fund their activities with more stable sources of funding on an ongoing basis. The Net Stable Funding Ratio (NSFR) aims to limit over-reliance on short-term wholesale funding during times of buoyant market liquidity and encourage better assessment of liquidity risk across all on- and off-balance sheet items.

The NSFR supplements the LCR and has a time horizon of one year. It has been developed to provide a sustainable maturity structure of assets and liabilities.

5.3 Detailed Loss Event Type Classification

As discussed in the previous chapter, loss events need to be classified for meaningful analysis. Basel II provides a framework for such a classification. The following are a few examples:

Event-Type Category (Level 1)	**Definition**	**Categories (Level 2)**	**Activity Examples (Level 3)**
Internal Fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involves at least one internal party	Unauthorised Activity	Transactions not reported (intentional)
			Transaction type unauthorised (w/ monetary loss)
			Mismarking of position (intentional)
		Theft & Fraud	Fraud/credit fraud/ worthless deposits Theft/extortion/ embezzlement/robbery Misappropriation of assets Malicious destruction of assets

Event-Type Category (Level 1)	**Definition**	**Categories (Level 2)**	**Activity Examples (Level 3)**
			Forgery Smuggling Account take-over/ impersonation/etc. Tax non-compliance/ evasion (wilful) Bribes/kickbacks Insider trading (not on firm's account)
External Fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party	Theft and Fraud	Theft/Robbery Forgery
		Systems Security	Hacking damage Theft of information (w/monetary loss)
Clients, Products & Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a	Suitability, Disclosure & Fiduciary	Fiduciary breaches/ guideline violations Suitability/disclosure issues (KYC, etc.) Retail customer disclosure violations Breach of privacy Aggressive sales Account churning Misuse of confidential information Lender liability
	product	Improper Business or Market Practices	Anti-trust Improper trade/market practices Market manipulation Insider trading (on firm's account) Unlicensed activity Money laundering

Event-Type Category (Level 1)	**Definition**	**Categories (Level 2)**	**Activity Examples (Level 3)**
		Product Flaws	Product defects (unauthorised, etc.) Model errors
		Selection, Sponsorship & Exposure	Failure to investigate client per guidelines Exceeding client exposure limits
		Advisory Activities	Disputes over performance of advisory activities
Business disruption and system failures	Losses arising from disruption of business or system failures	Systems	Hardware Software Telecommunications Utility outage/ disruptions

Self-Assessment Questions

- BIS accepts money from
  - Private individuals
  - Public Limited Companies
  - Trusts
  - **None of the above**

- The standardised model in Basel I provided for a weighting factor of _____ for claims on multilateral development banks.
  - 0%
  - **20%**
  - 50%
  - 100%

- IRB approach was introduced in
  - Basel I
  - Basel II
  - **Basel III**
  - None of the above

- Which of the following market risks are covered in Basel II?
  - Interest-related instruments in trading book
  - Foreign exchange risk throughout bank
  - Commodities risk throughout bank
  - **All the above**

- NSFR in Basel III, assesses bank liquidity over _____
  - 30 calendar days
  - 1 quarter
  - 6 months
  - **1 year**

- Wilful tax non-compliance is categorised as internal fraud in Basel III.
  - **True**
  - False

Chapter 6 : Basel II: Operational Risk

6.1 The Three Methods

As seen earlier, Basel II discusses three methods for calculating operational risk capital charges in a continuum of increasing sophistication and risk sensitivity:

- The Basic Indicator Approach (BIA);
- The Standardised Approach (TSA); and
- Advanced Measurement Approaches (AMA).

Banks are encouraged to move along the spectrum of available approaches as they develop more sophisticated operational risk measurement systems and practices.

Internationally active banks and banks with significant operational risk exposures (for example, specialised processing banks) are expected to use an approach that is more sophisticated than the BIA and that is appropriate for the risk profile of the institution.

A bank is permitted to use the BIA or TSA for some parts of its operations and an AMA for others provided certain minimum criteria are met.

A bank is not allowed to choose to revert to a simpler approach, once it has been approved for a more advanced approach, without supervisory approval. However, if a supervisor determines that a bank using a more advanced approach no longer meets the qualifying criteria for this approach, it may require the bank to revert to a simpler approach for some or all of its operations, until it meets the conditions specified by the supervisor for returning to a more advanced approach.

6.1.1 Basic Indicator Approach

Banks using the BIA must hold capital for operational risk equal to the average over the previous three years of a fixed percentage ("alpha") of positive annual gross income.

Figures for any year in which annual gross income is negative or zero, should be excluded from both the numerator and denominator, when calculating the average. The charge may be expressed as follows:

$K_{BIA} = [\Sigma(GI_{1....n} X \alpha]/n$

Where,

K_{BIA} is the capital charge under BIA

GI is annual gross income, where positive over the previous three years

n is the number of previous years in which GI is positive

α was set at 15% by the committee.

Gross income = Net interest income +Net non-interest income.

The numbers should-

(i) be gross of any provisions (e.g. for unpaid interest);

(ii) be gross of operating expenses, including fees paid to outsourcing service providers;

(iii) exclude realised profits/losses from the sale of securities in the banking book;

(iv) exclude extraordinary or irregular items as well as income derived from insurance; and

(v) exclude fees received by banks that provide out sourcing services.

6.1.2 The Standardised Approach

In this approach, the banks' activities are divided into eight business lines:

- corporate finance,
- trading & sales,
- retail banking,
- commercial banking,
- payment & settlement,
- agency services,
- asset management, and
- retail brokerage.

Within each business line, gross income is a broad indicator that serves as a proxy for the scale of business operations and thus the likely scale of operational risk exposure within each of these business lines.

The capital charge for each business line is calculated by multiplying gross income by a factor ("beta") assigned to that business line. Beta serves as a proxy for the industry-wide relationship between the operational risk loss experience for a given business line and the aggregate level of gross income for that business line.

Thus, in TSA gross income is measured for each business line, not the whole institution.

The total capital charge is calculated as the three-year average of the simple summation of the regulatory capital charges across each of the business lines in each year.

In any given year, negative capital charges (resulting from negative gross income) in any business line may offset positive capital charges in other business lines without limit. However, where the aggregate capital charge across all business lines within a

given year is negative, then the input to the numerator for that year will be zero. The total capital charge may be expressed as follows:

$K_{TSA} = [\Sigma_{Years\ 1\text{-}3}\ Max\ \{\Sigma(GI_{1....8}\ X\ \beta_{1....8}),0\}]/3$

Where,

K_{TSA} is the capital charge under the Standardised Approach

$GI_{1....8}$ is the gross income in a year for each of the 8 business lines

$\beta_{1....8}$ is the Beta factor set by the committee, as follows:

- corporate finance (β_1) 18%
- trading & sales (β_2) 18%
- retail banking (β_3) 12%
- commercial banking (β_4) 15%
- payment &settlement (β_5) 18%
- agency services (β_6) 15%
- asset management (β_7) 12%
- retail brokerage (β_8) 12%

There is also an Alternate Standardised Approach (ASA), where the operational risk capital charge/methodology is the same as for the Standardised Approach except for two business lines — retail banking and commercial banking. For these business lines, loans and advances — multiplied by a fixed factor 'm' — replaces gross income as the exposure indicator. The betas for retail and commercial banking are the same as in the Standardised Approach.

The ASA operational risk capital charge for retail banking (the same basic formula is applicable for commercial banking) can be expressed as:

$K_{RB} = \beta_{RB}\ X\ m\ X\ LA_{RB}$

Where,

$K_{RB}$is the capital charge for the retail banking business line,

β_{RB} is the beta for the retail banking business line,

LA_{RB} is total outstanding retail loans and advances (non-risk weighted and gross of provisions), averaged over the past three years.

The committee set the value of 'm' as 0.035

Under the ASA, banks may aggregate retail and commercial banking (if they wish to) using a beta of 15%.

Similarly, banks which are unable to disaggregate their gross income into the other six business lines can aggregate the total gross income for these six business lines using a beta of 18%.

The qualifying criteria for adopting TSA are as follows:

- Its board of directors and senior management, as appropriate, are actively involved in the oversight of the operational risk management framework;
- It has an operational risk management system that is conceptually sound and is implemented with integrity; and
- It has sufficient resources in the use of the approach in the major business lines as well as the control and audit areas.
- The bank must develop specific policies and have documented criteria for mapping gross income for current business lines and activities into the standardised framework. The criteria must be reviewed and adjusted for new or changing business activities as appropriate.

Internationally active banks need to meet the following additional criteria:

- The bank must have an operational risk management system with clear responsibilities assigned to an operational risk management function. This function has to be responsible for:
    - developing strategies to identify, assess, monitor and control/mitigate operational risk;
    - codifying firm-level policies and procedures concerning operational risk management and controls;
    - design and implementation of the firm's operational risk assessment methodology; and
    - design and implementation of a risk-reporting system for operational risk.
- As part of the bank's internal operational risk assessment system, the bank must systematically track relevant operational risk data including material losses by business line. The system must be closely integrated into the risk management processes of the bank. Its output must be an integral part of the process of monitoring and controlling the banks operational risk profile.

  For instance, this information must play a prominent role in risk reporting, management reporting, and risk analysis.

  The bank must have techniques for creating incentives to improve the management of operational risk throughout the firm.

- There must be regular reporting of operational risk exposures, including material operational losses, to business unit management, senior management, and to the board of directors.

  The bank must have procedures for taking appropriate action according to the information within the management reports.

- The bank's operational risk management system must be well documented. The bank must have a routine in place for ensuring compliance with a documented set of internal policies, controls and procedures concerning the operational risk management system, which must include policies for the treatment of non-compliance issues.

- The bank's operational risk management processes and assessment system must be subject to validation and regular independent review. These reviews must include both the activities of the business units and of the operational risk management function.

- The bank's operational risk assessment system (including the internal validation processes) must be subject to regular review by external auditors and/or supervisors.

6.1.3 Advanced Measurement Approaches

Under the AMA, the regulatory capital requirement is the risk measure generated by the bank's internal operational risk measurement system using specified quantitative and qualitative criteria.

- In order to use AMA, the bank must be able to satisfy its supervisor that:
  - Its board of directors and senior management, as appropriate, are actively involved in the oversight of the operational risk management framework;
  - It has an operational risk management system that is conceptually sound and is implemented with integrity; and
  - It has sufficient resources in the use of the approach in the major business lines as well as the control and audit areas.

The bank's internal measurement system must reasonably estimate unexpected losses based on the combined use of internal and relevant external loss data, scenario analysis and bank-specific business environment and internal control factors.

The bank's measurement system must also be capable of supporting an allocation of economic capital for operational risk across business lines in a manner that creates incentives to improve business line operational risk management.

- In order to use AMA, the bank must also be able to satisfy its supervisor on the following qualitative criteria
  - The bank has an independent operational risk management function that is responsible for the design and implementation of the bank's operational risk management framework. This function has to be responsible for:
    - developing strategies to identify, assess, monitor and control/mitigate operational risk;
    - codifying firm-level policies and procedures concerning operational risk management and controls;
    - design and implementation of the firm's operational risk assessment methodology; and
    - design and implementation of a risk-reporting system for operational risk.
  - The bank's internal operational risk measurement system must be closely integrated into the day-to-day risk management processes of the bank. Its output must be an integral part of the process of monitoring and controlling the bank's operational risk profile.

    For instance, this information must play a prominent role in risk reporting, management reporting, internal capital allocation, and risk analysis.

    The bank must have techniques for allocating operational risk capital to major business lines and for creating incentives to improve the management of operational risk throughout the firm.

    There must be regular reporting of operational risk exposures and loss experience to business unit management, senior management, and to the board of directors.

    The bank must have procedures for taking appropriate action according to the information within the management reports.
  - The bank's operational risk management system must be well documented. The bank must have a routine in place for ensuring compliance with a documented set of internal policies, controls and procedures concerning the operational risk management system, which must include policies for the treatment of non-compliance issues.
  - Internal and/or external auditors must perform regular reviews of the operational risk management processes and measurement systems. This review must include both the activities of the business units and of the independent operational risk management function.

- The validation of the operational risk measurement system by external auditors and/or supervisory authorities must include the following:
  - Verifying that the internal validation processes are operating in a satisfactory manner; and
  - Making sure that data flows and processes associated with the risk measurement system are transparent and accessible.

    In particular, it is necessary that auditors and supervisory authorities are in a position to have easy access, whenever they judge it necessary and under appropriate procedures, to the system's specifications and parameters.

- Besides, in order to use AMA, the bank must be able to satisfy its supervisor on the following quantitative criteria:

- AMA Soundness Standard

  The committee did not prescribe any approach or distributional assumptions used to generate the operational risk measure for regulatory capital purposes. However, a bank had to demonstrate that its approach captured potentially severe 'tail' loss events.

  Whatever the approach used, a bank had to demonstrate that its operational risk measure met a soundness standard comparable to that of the internal ratings-based approach for credit risk,(i.e. comparable to a one year holding period and a 99.9th percentile confidence interval).

  The bank had to maintain rigorous procedures for operational risk model development and independent model validation.

- Detailed Criteria
  - The bank had to calculate its regulatory capital requirement as the sum of expected loss (EL) and unexpected loss (UL). In order to base the minimum regulatory capital requirement on UL alone, the bank had to demonstrate to the satisfaction of its national supervisor that it has measured and accounted for its EL exposure.
  - The bank's risk measurement system had to be sufficiently 'granular' to capture the major drivers of operational risk affecting the shape of the tail of the loss estimates.
  - Risk measures for different operational risk estimates had to be added for purposes of calculating the regulatory minimum capital requirement.

    However, the bank could use internally determined correlations in operational risk losses across individual operational risk estimates, provided it could demonstrate to the satisfaction of the national supervisor

that its systems for determining correlations were sound, implemented with integrity, and take into account the uncertainty surrounding any such correlation estimates (particularly in periods of stress). The bank had to validate its correlation assumptions using appropriate quantitative and qualitative techniques.

- Any operational risk measurement system requires certain key features to meet the supervisory soundness standard. These elements must include the use of internal data, relevant external data, scenario analysis and factors reflecting the business environment and internal control systems (elaborated later in this Chapter).
- A bank needed to have a credible, transparent, well-documented and verifiable approach for weighting these fundamental elements in its overall operational risk measurement system.

  For example, there may be cases where estimates of the99.9th percentile confidence interval based primarily on internal and external loss event data would be unreliable for business lines with a heavy-tailed loss distribution and a small number of observed losses. In such cases, scenario analysis, and business environment and control factors, may play a more dominant role in the risk measurement system.

  Conversely, operational loss event data may play a more dominant role in the risk measurement system for business lines where estimates of the 99.9th percentile confidence interval based primarily on such data are deemed reliable.

  In all cases, the bank's approach for weighting the four fundamental elements had to be internally consistent and avoid the double counting of qualitative assessments or risk mitigants already recognised in other elements of the framework.

- Internal Data
  - The tracking of internal loss event data is an essential prerequisite to the development and functioning of a credible operational risk measurement system.

    Internal loss data is crucial for tying a bank's risk estimates to its actual loss experience. This can be achieved in a number of ways, including using internal loss data as the foundation of empirical risk estimates, as a means of validating the inputs and outputs of the bank's risk measurement system, or as the link between loss experience and risk management and control decisions.

- Internal loss data is most relevant when it is clearly linked to a bank's current business activities, technological processes and risk management procedures. Therefore, a bank must have documented procedures for assessing the on-going relevance of historical loss data, including those situations in which judgement overrides, scaling, or other adjustments may be used, to what extent they may be used and who is authorised to make such decisions.
- Internally generated operational risk measures used for regulatory capital purposes must be based on a minimum five-year observation period of internal loss data, whether the internal loss data is used directly to build the loss measure or to validate it. When the bank first moves to the AMA, a three-year historical data window is acceptable.
- A bank's internal loss collection processes must meet the following standards:
    - Bank must be able to map its historical internal loss data into the relevant level 1 supervisory categories and to provide these data to supervisors upon request.

      It must have documented, objective criteria for allocating losses to the specified business lines and event types. However, it is left to the bank to decide the extent to which it applies these categorisations in its internal operational risk measurement system.
    - A bank's internal loss data must be comprehensive in that it captures all material activities and exposures from all appropriate sub-systems and geographic locations.

      A bank must be able to justify that any excluded activities or exposures, both individually and in combination, would not have a material impact on the overall risk estimates.

      A bank must have an appropriate de minimis gross loss threshold for internal loss data collection, for example €10,000. The appropriate threshold may vary somewhat between banks, and within a bank across business lines and/or event types. However, particular thresholds should be broadly consistent with those used by peer banks.
    - Besides gross loss amounts, a bank should collect information about the date of the event, any recoveries of gross loss amounts, as well as some descriptive information about the drivers or causes of the loss event. The level of detail of any descriptive information should be commensurate with the size of the gross loss amount.

- Bank must develop specific criteria for assigning loss data arising from an event in a centralised function (e.g. an information technology department) or an activity that spans more than one business line, as well as from related events over time.
- Operational risk losses that are related to credit risk and have historically been included in banks' credit risk databases (e.g. collateral management failures) continue to be treated as credit risk for the purposes of calculating minimum regulatory capital. Therefore, such losses are not subject to the operational risk capital charge.

  However, for the purposes of internal operational risk management, banks must identify all material operational risk losses consistent with the scope of the definition of operational risk, including those related to credit risk. Such material operational risk-related credit risk losses should be flagged separately within a bank's internal operational risk database. The materiality of these losses may vary between banks, and within a bank across business line sand/or event types. Materiality thresholds should be broadly consistent with those used by peer banks.
- Operational risk losses that are related to market risk are treated as operational risk for the purposes of calculating minimum regulatory capital.

- External Data

  Bank's operational risk measurement system must use relevant external data (either public data and/or pooled industry data), especially when there is reason to believe that the bank is exposed to infrequent, yet potentially severe, losses.

  These external data should include data on actual loss amounts, information on the scale of business operations where the event occurred, information on the causes and circumstances of the loss events, or other information that would help in assessing the relevance of the loss event for other banks.

  A bank must have a systematic process for determining the situations for which external data must be used and the methodologies used to incorporate the data (e.g. scaling, qualitative adjustments, or informing the development of improved scenario analysis). The conditions and practices for external data use must be regularly reviewed, documented, and subject to periodic independent review.

- Scenario Analysis

  A bank must use scenario analysis of expert opinion in conjunction with external data to evaluate its exposure to high-severity events. This approach draws on the knowledge of experienced business managers and risk management experts to derive reasoned assessments of plausible severe losses.

  For instance, these expert assessments could be expressed as parameters of an assumed statistical loss distribution. In addition, scenario analysis should be used to assess the impact of deviations from the correlation assumption sembedded in the bank's operational risk measurement framework, in particular, to evaluate potential losses arising from multiple simultaneous operational risk loss events.

  Over time, such assessments need to be validated and re-assessed through comparison to actual loss experience to ensure their reasonableness.

- Business Environment & Internal Control Factors (BEICF)

  In addition to using loss data, whether actual or scenario-based, a bank's firm-wide risk assessment methodology must capture key business environment and internal control factors that can change its operational risk profile.

  These factors will make a bank's risk assessments more forward-looking, more directly reflect the quality of the bank's control and operating environments, help align capital assessments with risk management objectives, and recognise both improvements and deterioration in operational risk profiles in a more immediate fashion.

  To qualify for regulatory capital purposes, the use of these factors in a bank's risk measurement framework must meet the following standards:

  - The choice of each factor needs to be justified as a meaningful driver of risk, based on experience and involving the expert judgment of the affected business areas. Whenever possible, the factors should be translatable into quantitative measures that lend themselves to verification.
  - The sensitivity of a bank's risk estimates to changes in the factors and the relative weighting of the various factors need to be well reasoned. In addition to capturing changes in risk due to improvements in risk controls, the framework must also capture potential increases in risk due to greater complexity of activities or increased business volume.
  - The framework and each instance of its application, including the supporting rationale for any adjustments to empirical estimates, must be documented and subject to independent review within the bank and by supervisors.

- Over time, the process and the outcomes need to be validated through comparison to actual internal loss experience, relevant external data, and appropriate adjustments made.

- Risk Mitigation

Under the AMA, a bank is allowed to recognise the risk mitigating impact of insurance in the measures of operational risk used for regulatory minimum capital requirements.

The recognition of insurance mitigation is limited to 20% of the total operational risk capital charge calculated under the AMA. Such risk mitigation is permitted only if the following conditions are fulfilled:

- The insurance provider has a minimum claims paying ability rating of A (or equivalent).
- The insurance policy must have an initial term of no less than one year. For policies with a residual term of less than one year, the bank must make appropriate haircuts reflecting the declining residual term of the policy, up to a full 100% haircut for policies with a residual term of 90 days or less.
- The insurance policy has a minimum notice period for cancellation of 90 days.
- The insurance policy has no exclusions or limitations triggered by supervisory actions or, in the case of a failed bank, that preclude the bank, receiver or liquidator from recovering for damages suffered or expenses incurred by the bank, except in respect of events occurring after the initiation of receivership or liquidation proceedings in respect of the bank. However, the insurance policy may exclude any fine, penalty, or punitive damages resulting from supervisory actions.
- The risk mitigation calculations must reflect the bank's insurance coverage in a manner that is transparent in its relationship to, and consistent with, the actual likelihood and impact of loss used in the bank's overall determination of its operational risk capital.
- The insurance is provided by a third-party entity. In the case of insurance through captives and affiliates, the exposure has to be laid off to an independent third-party entity, for example through re-insurance, which meets the eligibility criteria.
- The framework for recognising insurance is well reasoned and documented.
- The bank has to disclose a description of its use of insurance for the purpose of mitigating operational risk.

The AMA is to be approved by the regulator.

The AMA provides for a well-reasoned estimate of diversification benefits at the group-wide level or at the banking subsidiary level.

Banks adopting the AMA are also required to calculate their capital requirement using the 1988 Accord and make certain adjustments for determining the applicable capital charge.

6.2 Mix of Three Methods

A bank is permitted to use an AMA for some parts of its operations and the BIA or TSA for the balance (partial use), provided that the following conditions are met:

- All operational risks of the bank's global, consolidated operations are captured;
- All of the bank's operations that are covered by the AMA meet the qualitative criteria for using an AMA, while those parts of its operations that are using one of the simpler approaches meet the qualifying criteria for that approach;
- On the date of implementation of an AMA, a significant part of the bank's operational risks are captured by the AMA; and
- The bank provides its supervisor with a plan specifying the timetable to which it intends to roll out the AMA across all but an immaterial part of its operations. The plan should be driven by the practicality and feasibility of moving to the AMA over time, and not for other reasons.

Bank may determine which parts of its operations will use an AMA on the basis of business line, legal structure, geography, or other internally determined basis.

6.3 SIGOR (June 2011)

The Basel Committee's Standards Implementation Group, through its Operational Risk Subgroup (SIGOR), has focused on the practical challenges associated with the development, implementation and maintenance of an operational risk management and measurement framework that meets the requirements of Basel II, especially as regards AMA.

The Committee has been publishing papers providing current information on the operational risk data and practices of institutions implementing Basel II. For instance, it was found that banks commonly use the Poisson distribution for estimating frequency. However, there are significant differences in the way banks model severity, including the choice of severity distribution.

The governance structure adopted by many banks relies on three lines of defence – business line management, independent corporate operational risk management function (CORF), and independent review.

6.3.1 Risk Appetite & Risk Tolerance

A bank's board of directors should approve and review a clear statement of operational risk appetite and tolerance.

- "Risk appetite" is a high level determination of how much risk a firm is willing to accept taking into account the risk/return attributes; it is often taken as a forward looking view of risk acceptance.
- "Risk tolerance" is a more specific determination of the level of variation a bank is willing to accept around business objectives that is often considered to be the amount of risk a bank is prepared to accept.

Risk appetite and tolerance statements should:

- account for all relevant risks, including the bank's current financial situation and strategic direction;
- encapsulate various risk tolerance and/or threshold levels; and
- detail how the board of directors will monitor and manage adherence to the risk appetite and tolerance statement.

The board of directors and senior management performance assessment should reflect and measure adherence to the risk appetite and tolerance statement. This should be applied and monitored across all business entities.

6.3.2 ORMF & ORMS: Verification & Validation

The Basel II Framework requires banks to develop an ORMF. This consists of a bank's:

- Risk organisational and governance structure;
- Policies, procedures and processes;
- Systems used by a bank in identifying, measuring, monitoring, controlling and mitigating operational risk; and
- Operational risk measurement system (ORMS).

  A bank's ORMS consists of the systems and data used to measure operational risk in order to estimate the operational risk capital charge. The ORMS must be closely integrated into the day-to-day risk management processes of the bank.

The ORMS should be validated and ORMF should be verified for their effectiveness using quantitative and qualitative approaches. The review should be conducted by independent internal or external auditors and/or other independent parties. It should be consistent with the materiality and complexity of the risk being managed.

Verification ensures that the ORMF, including the ORMS, is well-designed, implemented effectively and operates in a satisfactory manner, consistent with the bank's policies and procedures, and fulfils regulatory requirements.

Validation is more explicit and quantitative; it ensures that the ORMS's processes and data flows are credible, transparent, well-documented and verifiable.

Verification and validation are fundamental components of the AMA. They consist of inspection, observation, inquiry and confirmation (testing), computation and analytical exercises.

Individuals performing the assessments should be competent and appropriately trained. They should be independent, meaning they cannot influence the development, implementation and operation of the AMA framework. Further, they may not be part of the corporate operational risk function.

Verification activities should ensure:

- Policies, processes, procedures and systems that comprise the bank's ORMF, including the ORMS, are conceptually sound, transparent and documented;
- Business unit activities, the independent corporate operational risk management function and operational risk management governance committees and structures are effective and appropriate;
- ORMF inputs and outputs are accurate, complete, credible, relevant, authorised and accessible;
- Risk monitoring and management of the accuracy and soundness of all significant processes and systems are effective;
- Appropriate remediation is undertaken if deficiencies are identified;
- Outcome analysis is incorporated into bank processes, as appropriate, and is effective (outcome analysis includes comparisons of data elements such as a comparison of BEICFs with actual loss experience, or a comparison of scenario results with internal loss data and external data);
- Validation processes are satisfactory. The verification function should ensure that validation of AMA models is completed in accordance with the bank's model validation policy;
- Tests of operational risk management controls determine whether they are designed to prevent or detect and correct material deviations from or non-compliance with the policies, procedures and processes and operate effectively throughout the period being reviewed;
- Every significant activity and division, subsidiary or other component of the bank is included; and
- There is a periodic independent review of the AMA framework.

Validation should:

- Have a broad scope, evaluating all relevant items of the ORMS, such as
    - Distributional assumptions

- Correlation assumptions
- Documentation
- The four elements of the AMA
- Qualitative aspects (including the internal controls, use test, reporting, role of senior management and organisational aspects)
- Technological environment relating to the computational processes; and
- Procedures for the approval and use of new and modified estimation models or methodologies (such procedures should seek explicit opinion from the validation function in the approval process);

- Evaluate the bank's processes for escalating issues identified during validation reviews to ensure that:
  - Escalation processes are sufficiently comprehensive;
  - All significant ORMS concerns are appropriately considered and acted upon by senior management; and
  - All significant ORMS concerns are escalated to appropriate governance committees;
- Evaluate the conceptual soundness – including benchmarking and outcome analysis – of the ORMS and of the modelling output;
- Reflect policies and procedures to ensure that model validation efforts are consistent with board and senior management expectations.
- Assess whether policies and procedures are sufficiently comprehensive to address critical elements of the validation process. These include independent review; clearly defined responsibilities for model development and validation; model documentation; validation procedures and frequency; and audit oversight; and
- Confirm that the relationship between the model's inputs and outputs are stable and that the techniques underlying the model are transparent and intuitive.

Verification activities may be carried out by qualified external parties and/or internal or external audit, if independent of the processes and systems being reviewed. Validation should generally be carried out internally by qualified validation resources. Both activities can be outsourced. However, the board and senior management are responsible for ensuring that the outsourced activities are done consistently with the overall verification and validation plan.

A bank should have a broad strategic plan that governs the verification and validation of its ORMF and ORMS. The plan should be approved by the appropriate audit or operational risk committee and should incorporate all relevant business units. The plans should ensure that the bank's ORMF and ORMS are independently reviewed. In addition, the bank should

develop more detailed annual plans which state the purpose and tasks to be carried out during upcoming years.

The nature, timing and extent of work performed each year should provide a sufficient indication as to whether the bank's ORMF and ORMS:

- Function appropriately
- Are consistent with bank policies and
- Are free of material weaknesses.

The frequency with which policies, processes and systems within the bank's AMA framework is reviewed should be based on risk and significance.

Results from verification and validation work should be documented and distributed to appropriate business line management, internal audit, the corporate operational risk management function and appropriate risk committees. Bank staff ultimately responsible for the validated units, should have access to and an understanding of these results. Internal audit should evaluate management's response to significant findings.

Results of verification and validation reviews (including senior management's attestation) should be summarised and reported annually (or periodically, as appropriate) to the bank's board of directors, or a committee thereof, for approval.

A bank's strategic and business planning processes should consider its operational risk profile, including outputs from the ORMS. Potential material changes to the operational risk profile resulting from strategic and business planning change should be appropriately reviewed, considered, reported and monitored.

While banks have flexibility on the risk management and risk measurement practices adopted, a bank's operational risk strategy should reflect the nature and source of the bank's operational risks for all Operational Risk Measurement System (ORMS) elements. There has to be regular review of predictive elements against experience. The operational risk strategy should be current and reflect material changes to the internal and external environment.

Risk reporting should provide a clear understanding of the key operational risks, the related drivers and the effectiveness of the internal controls. The internal reporting framework should include regular reporting of relevant information at all levels of the bank, be transparent, responsive to changes, appropriate and support the proactive management of operational risk.

6.3.3 Embeddedness

The level to which the broader Operational Risk Management Framework(ORMF) processes and practices are embedded at all organisational levels across a bank is referred to as "embeddedness". A bank should have sustainable and embedded ORMFs and policies that are used in its risk management decision-making practices. There has to be clear evidence of the

integration and linkage between the measurement and management processes of the ORMF through the entire institution.

- The strategic and business planning processes should consider a bank's operational risk profile, including the outputs of the ORMS.
- A bank's board should endorse a clear statement of appetite and tolerance for operational risk and the bank should have adequate processes in place to monitor identified controls, ensuring that they are appropriate to mitigate the identified risks to the desired residual level and operating effectively.
- The business entity/unit management must be able to clearly demonstrate how the ORMF is implemented within the business entity/unit, including how specific procedures and processes have been used to facilitate implementation, validation and verification of the ORMF elements, and integration into the decision-making processes.
- A bank's operational risk profile should reflect both the internal and external environment. Risk reporting should provide a clear understanding of the key operational risks, the related drivers, and the effectiveness of risk management.
- The internal reporting framework should include regular reporting of relevant information at all levels of the bank. The internal reporting framework should be transparent, responsive to changes, appropriate, and support the proactive management of operational risk.
- Performance management criteria in relation to ORMS elements and outputs should be established.

6.3.4 Operational Risk Data

Operational risk data in a bank falls into four categories:

- Internal loss data (ILD)

  These are to be used in the ORMS to assist in the estimation of loss frequencies, to inform the severity distribution(s) to the extent possible and to serve as an input into scenario analysis.

- External data (ED)

  This is to be used in the estimation of loss severity as such data contain valuable information to inform the tail of the loss distribution(s). ED is also an essential input into scenario analysis.

  Banks may choose to source ED from a public database, from a consortium where members submit their loss information, or from other means such as collecting relevant ED themselves.

- Scenario data

  A robust scenario analysis framework is an important part of the ORMF in order to produce reliable scenario outputs which form part of the input into the AMA model.

  The scenario process is qualitative - the output from a scenario process necessarily contains significant uncertainties. This uncertainty, together with the uncertainty from the other elements, should be reflected in the output of the model producing a range for the capital estimate. Quantifying the uncertainty arising from scenario biases poses significant challenge and is an area requiring further research.

- Data related to a bank's business environment

  Incorporating BEICFs directly into the capital model poses challenges given the subjectivity and structure of BEICF tools. These are widely used as an indirect input into the quantification framework and as an ex-post adjustment to model output.

  A bank should provide a clearly articulated rationale for its modelling choices and assumptions and conduct sufficient research and analysis that support these decisions.

AMA operational risk data is used for various purposes, including risk quantification, risk management, accounting and other forms of reporting. Some data are suitable for more than one application. A bank should develop data policies and procedures for ensuring consistency. For example, there should be guidelines around perimeter of application, minimum observation period, reference date, de minimis modelling thresholds, and data treatment.

An operational risk loss can only arise from an operational risk event. Whether or not it has an impact on the financial statement, operational risk loss events should be included in the operational risk loss database. They may be used for purposes such as management or measurement.

6.3.5 Gross Loss & Net Loss

A gross loss is a loss before recoveries of any type. Net loss is the loss after taking into account the impact of recovery. A recovery is an independent event, related to the original loss event. Funds or economic benefits flow from a third party at a point of time that is independent of the original loss event. For an operational risk event, a bank should be able to identify gross loss, recoveries and any insurance recoveries.

An AMA bank should have robust processes to collect operational risk losses based on clear and consistent definitions of "gross loss" and "recoveries". A bank may use "gross loss amount" or "gross loss amount after all recoveries (except insurance)" as input for its AMA models.

The bank should demonstrate to its relevant supervisors that its choice is appropriate and should not use losses net of insurance recoveries as an input for AMA models. This is because BASEL II framework allows a maximum 20% capital reduction for insurance mitigation.

Internal loss collection thresholds should be based on statistical evidence showing that losses below the threshold have an immaterial impact on capital. The bank should be aware of the impact of the threshold on the capital.

The bank should define and justify the threshold for each operational risk class. Different thresholds may be used for data collection and monitoring. These should be reasonable and should not omit operational loss event data that are material for operational risk exposure and for effective risk management. The choice of threshold for modelling should not adversely impact the credibility and accuracy of the operational risk measures.

Gross loss computations should include the following:

- Direct charges (including impairments) to the statement on comprehensive income and write-downs due to operational risk events.
- Costs incurred as a consequence of the event that should include external expenses with a direct link to the operational risk event (e.g. legal expenses directly related to the event and fees paid to advisors, attorneys or suppliers) and costs of repair or replacement, to restore the position that was prevailing before the operational risk event.
- Provisions ("reserves");
- Pending losses that stem from operational risk events with a definitive financial impact, which are temporarily booked in transitory and/or suspense accounts and are not yet reflected in the statement of comprehensive income.

Gross loss computations should exclude the following:

- Costs of general maintenance contracts on property, plant or equipment;
- Internal or external expenditures to enhance the business after the operational risk event: upgrades, improvements, risk assessment initiatives and enhancements;
- Insurance premiums.

The inclusion or exclusion of the following items depends on their nature and materiality.

- Timing losses - These are defined as the negative economic impacts booked in an accounting period, due to operational risk events impacting the cash flows or financial statements of previous accounting periods.

  Timing impacts typically relate to the occurrence of operational risk events that result in the temporary distortion ofan institution's financial accounts (e.g. revenue overstatement, accounting errors and mark-to-market errors).

  While these events do not represent a true financial impact on the institution (net impact over time is zero), if the error continues across two or more accounting periods, it may represent a material misrepresentation of the institution's financial statements.

Material "timing losses" due to operational risk events that span two or more accounting periods should be included, i.e. full amount that includes make-up payments as well as penalties and interest, in the scope of operational risk loss when they give rise to legal events.

- Rapidly recovered loss events – These are operational risk events that lead to losses recognised in financial statements that are recovered over a short period. For instance, a large internal loss is rapidly recovered when a bank transfers money to a wrong party but recovers all or part of the loss soon thereafter. A bank may consider this to be a gross loss and a recovery. However, when the recovery is made rapidly, the bank may consider that only the loss net of the rapid recovery constitutes an actual loss. When the rapid recovery is full, the event is considered to be a "near miss".

Gross loss may be measured as follows:

- Mark-to-market

  The economic impact of an operational risk loss is usually the same as the accounting impact when an operational risk loss affects assets or accounts treated on a mark-to-market basis. In such cases, the gross loss amount is the loss or adjustment as recognised in the comprehensive statement of income.

- Replacement cost

  The economic impact of an operational risk loss usually differs from the accounting impact when losses affect assets or accounts that are not maintained on a mark-to-market basis such as property, plant, equipment or intangible assets. The gross loss amount is the replacement cost of the item.

6.3.6 Dates

Several reference dates can be captured for any individual operational loss. For example, date of occurrence, date of discovery, date of contingent liability, date of accounting (first financial impact), and date of settlement.

The collection of numerous dates is not an issue from an operational risk management perspective, as each reference date potentially offers different information on the characteristics of each loss. However, concern is that AMA banks could select a reference date for quantification that results in the omission of large internal losses, which can have a significant impact on the bank's operational risk capital charge at a given point in time, and over time. Therefore, supervisors are encouraging convergence of practice in how losses are treated and recorded as operational risk loss events.

An AMA bank may use any of the reference dates (occurrence date, discovery date, contingent liability date or accounting date) for building its calculation dataset, and for meeting minimum observation period requirements, as long as material loss data is not omitted.

When collecting data, banks typically gather information from at least three reference dates: occurrence date, discovery date and accounting date. The discovery date or accounting date are the most prudent choices for developing a bank's dataset for the quantification of the operational risk capital requirements related to that event. However, institutions may use occurrence date for building the calculation dataset if the institution has not constrained or limited the observation period of five years.

Banks do group a number of losses and treat the group as a single loss for recording, management or modelling purposes.

- Losses caused by a common operational loss event should be grouped and entered into the loss calculation dataset as a single loss, unless a bank chooses to model causality or dependence among those losses in a different manner.
- A bank that groups small losses with no causal relations for data collection and registration purposes should generally exclude them from their calculation dataset. When they do include them in their calculation dataset, they should demonstrate that the use of this type of grouped losses does not materially distort the capital calculation.

Differences in models (for instance, different correlation estimates, or different distribution assumptions) affect the AMA methodology and therefore the capital calculations. Therefore, the critical features of a bank's AMA model should be supported by quantitative and qualitative analysis and appropriately reflect the operational risk profile of the bank.

Due to the nature and diversity of operational risk across an institution, a bank should define its operational risk categories (ORC). A bank's risk measurement system and capital charge calculation is greatly influenced by the number of ORCs used within the model. A bank's choice of ORCs should reflect the unique nature of its business model and risk profile.

A bank should have a policy on when a loss or an event recorded in the internal (or external) loss event database is also to be included in the calculation dataset. Exceptions to the policy should be limited.

6.3.7 Distributions

The bank should follow a well specified, documented and traceable process for the selection, update and review of probability distributions and the estimate of its parameters. This process should lead to consistent and clear choices and be mainly finalised to properly capture the risk profile in the tail.

The techniques to determine the aggregated loss distributions should ensure adequate levels of precision and stability of the risk measures. The risk measures should be monotonic, reasonable and be supplemented with information on their level of accuracy.

The technicalities of AMA models predominantly based on scenario analysis (Scenario Based Approaches, or SBA) differ from those of AMA models predominantly based on loss data

(loss distribution approach, or LDA). The identification of distributions in the SBA and LDA processes should be more consistent with each other.

Many observed SBA models do not apply statistical inference to raw scenario data. The curves are predetermined and the scenario data are used only to estimate the parameters of those distributions. Under such a process, the scenario data risks being distorted by an inappropriate choice of distribution. A bank should thus ensure that the loss distribution(s) chosen to model scenario analysis estimates adequately represent(s) its risk profile.

Dependence assumptions, too, affect the capital. They should be conservative and supported by empirical data and expert judgement. The degree of conservatism should increase, as the rigor of the dependence model and reliability of capital estimates decrease.

A bank should perform sensitivity analyses and stress testing (e.g. different parameter values, different correlation models) on the effect of alternative dependence assumptions on its operational risk capital estimate.

Self-Assessment Questions

- As per Basel II, BIA is suitable for which of the following?
  - International Active Banks
  - Banks with significant operating risk
  - Both the above
  - **None of the above**

- A bank had gross income of Rs.100 crore, Rs. 140 crore and –Rs. 60 crore in the previous 3 years? What would be the capital charge as per BIA?
  - **Rs. 18 crore**
  - Rs. 9 crore
  - Rs. 24 crore
  - Rs. 12 crore

- Under ASA, gross income is not used for determining operating capital charge in the case of
  - Retail banking
  - Commercial banking
  - **Both the above**
  - None of the above

- Under AMA, operational risk losses that are related to market risk are treated as operational risk for the purposes of calculating minimum regulatory capital.
  - **True**
  - False

- Insurance mitigation is limited to ___ of the total operational risk capital charge calculated under the AMA.
  - 0%
  - 5%
  - 10%
  - **20%**

- Which of the following is commonly used as indirect input in risk quantification frameworks?
  - **BEICF**
  - Internal Loss Data
  - External Data
  - Scenario Data

Chapter 7 : Basel: Operational Risk Principles

7.1 Background

Operational risk is inherent in all banking products, activities, processes and systems, and the effective management of operational risk has always been a fundamental element of a bank's risk management programme. As a result, sound operational risk management is a reflection of the effectiveness of the board and senior management in administering its portfolio of products, activities, processes, and systems.

Risk management generally encompasses the process of identifying risks to the bank, measuring exposures to those risks (where possible), ensuring that an effective capital planning and monitoring programme is in place, monitoring risk exposures and corresponding capital needs on an ongoing basis, taking steps to control or mitigate risk exposures and reporting to senior management and the board on the bank's risk exposures and capital positions.

Internal controls are typically embedded in a bank's day-to-day business and are designed to ensure, to the extent possible, that bank activities are efficient and effective, information is reliable, timely and complete and the bank is compliant with applicable laws and regulation.

Common industry practice for sound operational risk governance often relies on three lines of defence –

- Business line management,
- An independent corporate operational risk management function (CORF), and
- An independent review.

Depending on the bank's nature, size and complexity, and the risk profile of a bank's activities, the degree of formality of how these three lines of defence are implemented will vary. In all cases, however, a bank's operational risk governance function should be fully integrated into the bank's overall risk management governance structure.

The degree of independence of the CORF will differ among banks.

- For small banks, independence may be achieved through separation of duties and independent review of processes and functions.
- In larger banks, the CORF will have a reporting structure independent of the risk generating business lines and will be responsible for the design, maintenance and ongoing development of the operational risk framework within the bank. This function may include the operational risk measurement and reporting processes, risk committees and responsibility for board reporting.

A key function of the CORF is to challenge the business lines' inputs to, and outputs from, the bank's risk management, risk measurement and reporting systems. The CORF should have a sufficient number of personnel skilled in the management of operational risk to effectively address its many responsibilities.

A strong risk culture and good communication among the three lines of defence are important characteristics of good operational risk governance.

Internal audit coverage should include opining on the overall appropriateness and adequacy of the Framework and the associated governance processes across the bank.

Internal audit should not simply be testing for compliance with board approved policies and procedures, but should also be evaluating whether the Framework meets organisational needs and supervisory expectations. For example, while internal audit should not be setting specific risk appetite or tolerance, it should review the robustness of the process of how these limits are set and why and how they are adjusted in response to changing circumstances.

The Basel Committee has laid down the following principles for operational risk management:

7.2 The Principles

- Principle 1:

  The board of directors should take the lead in establishing a strong risk management culture. The board of directors and senior management should establish a corporate culture that is guided by strong risk management and that supports and provides appropriate standards and incentives for professional and responsible behaviour. In this regard, it is the responsibility of the board of directors to ensure that a strong operational risk management culture exists throughout the whole organisation.

- Principle 2:

  Banks should develop, implement and maintain a Framework that is fully integrated into the bank's overall risk management processes. The Framework for operational risk management chosen by an individual bank will depend on a range of factors, including its nature, size, complexity and risk profile

  Framework documentation should clearly:

  - identify the governance structures used to manage operational risk, including reporting lines and accountabilities;
  - describe the risk assessment tools and how they are used;
  - describe the bank's accepted operational risk appetite and tolerance, as well as thresholds or limits for inherent and residual risk, and approved risk mitigation strategies and instruments;
  - describe the bank's approach to establishing and monitoring thresholds or limits for inherent and residual risk exposure;
  - establish risk reporting and Management Information Systems (MIS);
  - provide for a common taxonomy of operational risk terms to ensure consistency of risk identification, exposure rating and risk management objectives;

- provide for appropriate independent review and assessment of operational risk; and
- require the policies to be reviewed whenever a material change in the operational risk profile of the bank occurs, and revised as appropriate.

- Principle 3:

  The board of directors should establish, approve and periodically review the Framework. The board of directors should oversee senior management to ensure that the policies, processes and systems are implemented effectively at all decision levels.

- Principle 4:

  The board of directors should approve and review a risk appetite and tolerance statement for operational risk that articulates the nature, types, and levels of operational risk that the bank is willing to assume.

- Principle 5:

  Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well defined, transparent and consistent lines of responsibility.

  Senior management is responsible for consistently implementing and maintaining throughout the organisation policies, processes and systems for managing operational risk in all of the bank's material products, activities, processes and systems consistent with the risk appetite and tolerance.

- Principle 6:

  Senior management should ensure the identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood.

  Examples of tools that may be used for identifying and assessing operational risk include:

  - Audit Findings:

    While audit findings primarily focus on control weaknesses and vulnerabilities, they can also provide insight into inherent risk due to internal or external factors.

  - Internal Loss Data Collection and Analysis:

    Internal operational loss data provides meaningful information for assessing a bank's exposure to operational risk and the effectiveness of internal controls. Analysis of loss events can provide insight into the causes of large losses and information on whether control failures are isolated or systematic.

    Banks may also find it useful to capture and monitor operational risk contributions to credit and market risk related losses in order to obtain a more complete view of their operational risk exposure;

- External Data Collection and Analysis:

  External data elements consist of gross operational loss amounts, dates, recoveries, and relevant causal information for operational loss events occurring at organisations other than the bank.

  External loss data can be compared with internal loss data, or used to explore possible weaknesses in the control environment or consider previously unidentified risk exposures;

- Risk Assessments:

  In a risk assessment, often referred to as a Risk Self Assessment (RSA), a bank assesses the processes underlying its operations against a library of potential threats and vulnerabilities and considers their potential impact.

  A similar approach, Risk Control Self Assessments (RCSA), typically evaluates inherent risk (the risk before controls are considered), the effectiveness of the control environment, and residual risk (the risk exposure after controls are considered).

  Scorecards build on RCSAs by weighting residual risks to provide a means of translating the RCSA output into metrics that give a relative ranking of the control environment;

- Business Process Mapping:

  Business process mappings identify the key steps in business processes, activities and organisational functions. They also identify the key risk points in the overall business process. Process maps can reveal individual risks, risk interdependencies, and areas of control or risk management weakness. They also can help prioritise subsequent management action;

- Risk and Performance Indicators:

  Risk and performance indicators are risk metrics and/or statistics that provide insight into a bank's risk exposure. Risk indicators, often referred to as Key Risk Indicators (KRIs), are used to monitor the main drivers of exposure associated with key risks.

  Performance indicators, often referred to as Key Performance Indicators (KPIs), provide insight into the status of operational processes, which may in turn provide insight into operational weaknesses, failures, and potential loss.

  Risk and performance indicators are often paired with escalation triggers to warn when risk levels approach or exceed thresholds or limits and prompt mitigation plans;

- Scenario Analysis:

  Scenario analysis is a process of obtaining expert opinion of business line and risk managers to identify potential operational risk events and assess their potential outcome.

  Scenario analysis is an effective tool to consider potential sources of significant operational risk and the need for additional risk management controls or mitigation solutions.

  Given the subjectivity of the scenario process, a robust governance framework is essential to ensure the integrity and consistency of the process;

- Measurement:

  Larger banks may find it useful to quantify their exposure to operational risk by using the output of the risk assessment tools as inputs into a model that estimates operational risk exposure. The results of the model can be used in an economic capital process and can be allocated to business lines to link risk and return; and

- Comparative Analysis:

  Comparative analysis consists of comparing the results of the various assessment tools to provide a more comprehensive view of the bank's operational risk profile. For example,

  - Comparison of the frequency and severity of internal data with RCSAs can help the bank determine whether self-assessment processes are functioning effectively.
  - Scenario data can be compared to internal and external data to gain a better understanding of the severity of the bank's exposure to potential risk events.

- Principle 7:

  Senior management should ensure that there is an approval process for all new products, activities, processes and systems that fully assesses operational risk.

  In general, a bank's operational risk exposure is increased when a bank engages in new activities or develops new products; enters unfamiliar markets; implements new business processes or technology systems; and/or engages in businesses that are geographically distant from the head office. Moreover, the level of risk may escalate when new products activities, processes, or systems transition from an introductory level to a level that represents material sources of revenue or business-critical operations.

A bank should ensure that its risk management control infrastructure is appropriate at inception and that it keeps pace with the rate of growth of, or changes to, products activities, processes and systems.

A bank should have policies and procedures that address the process for review and approval of new products, activities, processes and systems. The review and approval process should consider:

- inherent risks in the new product, service, or activity;
- changes to the bank's operational risk profile and appetite and tolerance, including the risk of existing products or activities;
- the necessary controls, risk management processes, and risk mitigation strategies;
- the residual risk;
- changes to relevant risk thresholds or limits; and
- the procedures and metrics to measure, monitor, and manage the risk of the new product or activity.

The approval process should also include ensuring that appropriate investment has been made for human resources and technology infrastructure before new products are introduced.

The implementation of new products, activities, processes and systems should be monitored in order to identify any material differences to the expected operational risk profile, and to manage any unexpected risks.

- Principle 8:

Senior management should implement a process to regularly monitor operational risk profiles and material exposures to losses. Appropriate reporting mechanisms should be in place at the board, senior management, and business line levels that support proactive management of operational risk.

Reporting should be timely and a bank should be able to produce reports in both normal and stressed market conditions. The frequency of reporting should reflect the risks involved and the pace and nature of changes in the operating environment.

Operational risk reports should include:

- breaches of the bank's risk appetite and tolerance statement, as well as thresholds or limits;
- details of recent significant internal operational risk events and losses; and
- relevant external events and any potential impact on the bank and operational risk capital.

- Principle 9:

  Banks should have a strong control environment that utilises policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies.

  The use of technology related products, activities, processes and delivery channels exposes a bank to strategic, operational, and reputational risks and the possibility of material financial loss. Consequently, a bank should have an integrated approach to identifying, measuring, monitoring and managing technology risks. Sound technology risk management uses the same precepts as operational risk management and includes:

  - governance and oversight controls that ensure technology, including outsourcing arrangements, is aligned with and supportive of the bank's business objectives;
  - policies and procedures that facilitate identification and assessment of risk;
  - establishment of a risk appetite and tolerance statement as well as performance expectations to assist in controlling and managing risk;
  - implementation of an effective control environment and the use of risk transfer strategies that mitigate risk; and
  - monitoring processes that test for compliance with policy thresholds or limits.

  Management should ensure the bank has a sound technology infrastructure that meets current and long-term business requirements by providing sufficient capacity for normal activity levels as well as peaks during periods of market stress; ensuring data and system integrity, security, and availability; and supporting integrated and comprehensive risk management.

  Mergers and acquisitions resulting in fragmented and disconnected infrastructure, cost-cutting measures or inadequate investment can undermine a bank's ability to aggregate and analyse information across risk dimensions or the consolidated enterprise, manage and report risk on a business line or legal entity basis, or oversee and manage risk in periods of high growth.

  Management should make appropriate capital investment or otherwise provide for a robust infrastructure at all times, particularly before mergers are consummated, high growth strategies are initiated, or new products are introduced.

  Outsourcing is the use of a third party – either an affiliate within a corporate group or an unaffiliated external entity – to perform activities on behalf of the bank. Outsourcing can involve transaction processing or business processes.

While outsourcing can help manage costs, provide expertise, expand product offerings, and improve services, it also introduces risks that management should address. The board and senior management are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective risk management policies and practices are in place to manage the risk in outsourcing activities.

Outsourcing policies and risk management activities should encompass:

- procedures for determining whether and how activities can be outsourced;
- processes for conducting due diligence in the selection of potential service providers;
- sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights;
- programmes for managing and monitoring the risks associated with the outsourcing arrangement, including the financial condition of the service provider;
- establishment of an effective control environment at the bank and the service provider;
- development of viable contingency plans; and
- execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between the outsourcing provider and the bank.

In those circumstances where internal controls do not adequately address risk and exiting the risk is not a reasonable option, management can complement controls by seeking to transfer the risk to another party such as through insurance.

The board of directors should determine the maximum loss exposure the bank is willing and has the financial capacity to assume, and should perform an annual review of the bank's risk and insurance management programme. While the specific insurance or risk transfer needs of a bank should be determined on an individual basis, many jurisdictions have regulatory requirements that must be considered.

Because risk transfer is an imperfect substitute for sound controls and risk management programmes, banks should view risk transfer tools as complementary to, rather than a replacement for, thorough internal operational risk control. Having mechanisms in place to quickly identify, recognise and rectify distinct operational risk errors can greatly reduce exposures.

Careful consideration also needs to be given to the extent to which risk mitigation tools such as insurance truly reduce risk, transfer the risk to another business sector or area, or create a new risk (e.g. counterparty risk).

- Principle 10:

  Banks should have business resiliency and continuity plans in place to ensure an ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

  Banks are exposed to disruptive events, some of which may be severe and result in an inability to fulfil some or all of their business obligations. Incidents that damage or render inaccessible the bank's facilities, telecommunication or information technology infrastructures, or a pandemic event that affects human resources, can result in significant financial losses to the bank, as well as broader disruptions to the financial system.

  To provide resiliency against such risk, a bank should establish business continuity plans commensurate with the nature, size and complexity of their operations. Such plans should take into account different types of likely or plausible scenarios to which the bank may be vulnerable.

  Continuity management should incorporate business impact analysis, recovery strategies, testing, training and awareness programmes, and communication and crisis management programmes.

  A bank should identify critical business operations, key internal and external dependencies, and appropriate resilience levels.

  Plausible disruptive scenarios should be assessed for their financial, operational and reputational impact, and the resulting risk assessment should be the foundation for recovery priorities and objectives.

  Continuity plans should establish contingency strategies, recovery and resumption procedures, and communication plans for informing management, employees, regulatory authorities, customer, suppliers, and – where appropriate – civil authorities.

  A bank should periodically review its continuity plans to ensure contingency strategies remain consistent with current operations, risks and threats, resiliency requirements, and recovery priorities.

  Training and awareness programmes should be implemented to ensure that staff can effectively execute contingency plans. Plans should be tested periodically to ensure that recovery and resumption objectives and timeframes can be met. Where possible, a bank should participate in disaster recovery and business continuity testing with key service providers. Results of formal testing activity should be reported to management and the board.

- Principle 11:

  A bank's public disclosures should allow stakeholders to assess its approach to operational risk management.

Self-Assessment Questions

- Internal audit is responsible for setting the risk tolerance of the organisation.
  - True
  - **False**

- Operational Risk Management Framework of a bank depends on
  - Size of business
  - Nature of business
  - Complexity of business
  - **All the above**

- Which of the following are used in risk assessments?
  - RSA
  - RCSA
  - Scorecard
  - **All the above**

- According to the Basel Committee's Operating Risk Management Principles, appropriate investment has to be made for human resources and technology infrastructure, before new products are introduced.
  - **True**
  - False

- Operational risk reports should include o details of recent significant internal operational risk events and losses, but not breaches of risk tolerance.
  - True
  - **False**

- Risk transfer tools should be viewed as complementary to, rather than a replacement for, thorough internal operational risk control.
  - **True**
  - False

Chapter 8 : Basel: Audit

8.1 External Audit

Banks play an important role in financial stability. Therefore, the market needs to have confidence in the external audit of banks' financial statements. Global banks that are Systemically Important Banks (SIB) are especially important. Failure of one can drag other banks in the system.

The Basel Committee's consultative paper on the subject covers the following:

- all banks, including those within a banking group;
- holding companies whose subsidiaries are predominantly banks; and
- holding companies subject to prudential supervision whose subsidiaries are predominantly banks.

Implementation of the principles should be proportionate to the size, complexity, structure, economic significance and risk profile of the bank and the group (if any) to which it belongs.

An external auditor performs audit of a bank's financial statements with a view to obtain reasonable assurance about whether the financial statements as a whole are free from material mis-statements, whether due to fraud or error, and are prepared, in all material respects, in accordance with an applicable financial reporting framework.

External audit help identify weaknesses in internal controls relating to financial reporting at a bank. This helps supervisory efforts in this area and contributes to a safe and sound banking system. The audit, however, does not relieve management or those charged with governance of their responsibilities.

Audit quality includes delivering an appropriate, independent professional opinion on the financial statements, in compliance with internationally accepted auditing standards.

The Audit Committee is responsible for supervising the external auditor. Regular and effective engagement and communication between them contribute to audit quality. The two have a mutual interest in building and maintaining an effective relationship, which fosters regular communication of useful information.

The bank may have Board of Directors and Audit Committee. If the external auditor finds it necessary, he can report to both authorities.

Similarly, the banking supervisory authority and the relevant audit oversight body share a strong mutual interest in ensuring quality independent audits. Regular and effective dialogue between them at a national level can assist in identifying and dealing with key issues in relation to the conduct of bank audits. Supervisors are in a unique position to identify audit quality issues at both the industry and individual bank audit level.

The consultative document lays down the following principles for external audit:

- Principle 1:

  The external auditor of a bank should have banking industry knowledge and competence sufficient to respond appropriately to the risks of material misstatement in the bank's financial statements and to properly meet any additional regulatory requirements that may be part of the statutory audit.

  At times, more specialised knowledge may be required to support the audit engagement team. These may relate to a field other than accounting or auditing. For example, valuation of complex financial instruments, commercial property valuations and evaluation of highly complex IT environments, particularly in areas subject to significant risks of material mis-statement.

  The external auditor should assess the competence, capabilities and objectivity of the experts the external auditor may use for the purpose.

- Principle 2:

  The external auditor of a bank should be objective and independent in fact and appearance with respect to the bank, consistent with the more stringent requirements applicable to public interest entities in internationally accepted ethical standards.

  Independence should be observed not only in the context of the bank that is being audited but also with respect to the bank's related entities.

- Principle 3:

  The external auditor should exercise professional scepticism when planning and performing the audit of a bank, having due regard to the specific challenges in auditing a bank.

  Professional scepticism is an attitude that includes a questioning mind, being alert to conditions which may indicate possible misstatement due to error or fraud, and a critical assessment of evidence. This is particularly important when auditing areas that:

  - Involve significant management estimates and judgments because these are more prone to management bias;
  - Involve significant non-recurring or unusual transactions; or
  - Are more susceptible to fraud and errors being perpetuated due to weak internal controls.

  Specific areas include impairment calculations, fair value measurements and going concern assessments, including assessments of solvency and liquidity, and complex transactions structured to achieve a particular accounting treatment and/or regulatory outcome by the management that the audit engagement partner finds suspicious.

Where a bank consistently utilises valuations that are at the high or low end of a range of acceptable valuations or when there are other indications of possible management bias, the external auditor should consider this in the overall risk assessment of the bank and should inform those charged with governance, where appropriate.

Audit documentation should describe how, why and what conclusions were reached by the external auditor.

- Principle 4:

  Audit firms undertaking bank audits should comply with the more stringent requirements on quality control applicable to listed entities in internationally accepted quality control standards, having due regard to the complexity of a bank audit.

  The audit of a bank should be subject to an engagement quality control review (EQCR) performed internally by the audit firm prior to the issuance of the audit opinion. The engagement quality control reviewer should have the appropriate knowledge and competence to review bank audits. The reviewer should exercise professional scepticism in assessing the quality of audit evidence and whether the auditor's judgments are appropriate.

  Any significant discussions between the engagement quality control reviewer and the audit engagement team, particularly in areas where views may have differed and as to how conclusions were reached, should be fully documented in the audit working papers.

- Principle 5:

  The external auditor of a bank should identify and assess the risks of material misstatement in the bank's financial statements, considering the complexities of banking activities and the need for banks to have a strong control environment.

  Internal control components are the control environment, risk assessment process, information and communication systems and processes, control activities and monitoring of controls.

  A robust internal control environment is critical to the strength of a bank's governance system and its ability to manage risk. Therefore, the external auditor should:

  - assess the "tone at the top", i.e. whether management, with the involvement of those charged with governance, is promoting a robust control environment;
  - determine whether the control environment extends to all types of operations and service offerings and encompasses all subsidiaries and branches of the banking group;
  - understand the bank's approach to outsourcing/off shoring of business activities and functions and assess how internal control over these activities is maintained; and

- obtain an adequate understanding of the organisation of key control functions within the bank and its subsidiaries. At a minimum, key control functions include the internal audit, risk management, compliance and other monitoring functions.

Compensation arrangements at a bank may be a good indicator of the culture within the organisation because they can influence the behaviour of the bank's personnel and the quality of corporate governance.

While identifying and assessing risks of material mis-statement and assessing controls, the external auditor should take account of the following factors:

- The knowledge and competence of those in charge of financial reporting and of other control functions having an impact on financial reporting;
- The nature of hedging strategies employed by the bank which, if complex, improperly structured or inadequately monitored, can have accounting and solvency implications;
- The use of complex financial instruments involving significant estimates of fair value;
- The provision of custodial services to retail and/or institutional clients and the procedures in place to avoid co-mingling of client and proprietary assets;
- The volume of transactions by type of activity and/or presence of significant non-routine transactions;
- The use and monitoring of internal accounts;
- The structure and complexity of IT systems for conducting business and for facilitating efficient business and financial reporting, as they may lead to increased risk of fraud or error, particularly where there is potential for individual override of the control system or the potential for fraudulent transactions to go undetected due to the sophistication and complexity of the IT systems;
- The number, scope and geographical dispersion of subsidiaries and the necessity for complex consolidation procedures;
- The existence of significant transactions with related parties; and
- The use of off-balance sheet financing arrangements, such as special purpose entities (SPEs) and other complex structures.

The internal control of a bank must be robust and reliable in order to cope with stressed environments. Significant deficiencies in internal control which have been identified by the external auditor should be communicated in writing to those charged with governance and senior management.

Other deficiencies in internal control should be communicated to the senior management at an appropriate level of responsibility on a timely basis.

Further, the external auditor should communicate in writing all matters that are likely to be significant to the responsibilities of those charged with governance in overseeing the strategic direction of the entity or the entity's obligations.

The work of internal auditors can help external auditors assess the quality of the internal control processes and identify risks. The external auditor should engage with, and seek information on key internal audit findings from, the internal auditors. This may provide valuable input into the external auditor's understanding of the entity and its environment and aid in identifying and assessing risks of material misstatement.

The external auditor's observations on and, where relevant, evaluation of a bank's internal audit function are of particular interest to the audit committee and the bank's supervisor given the role an effective internal audit function plays in maintaining a robust control environment in a bank.

- Principle 6:

  The external auditor of a bank should respond appropriately to the significant risks of material mis-statement in the bank's financial statements. The following is an illustrative list of areas where material mis-statement is possible.

  - Loan loss provisioning
  - Financial instruments measured at fair value
  - Liabilities including contingent liabilities arising from non-compliance with laws and regulations, and contractual breaches
  - Disclosures
  - Going concern assessment

    There should be equal emphasis on the evaluation of liquidity and solvency of the bank for the period over which the going concern assumption has been assessed.

- Securitisation – SPEs

- Principle 7:

  The audit committee should have a robust process for approving, or recommending for approval, the appointment, reappointment, removal and remuneration of the external auditor.

  The audit committee has the primary responsibility for approving, or recommending to the board of directors for approval, the appointment, reappointment, removal and remuneration of the external auditor. In doing so, the audit committee should

determine appropriate criteria for selecting the external auditor and regularly assess the knowledge, competence and independence of the external auditor and effectiveness of the external audit.

If the board of directors does not accept the audit committee's recommendation, it should include in the annual report, and in any papers relating to the appointment/ reappointment/dismissal of the external auditor, a statement explaining the audit committee's recommendation and the reasons why the board of directors has taken a different position.

The audit committee should also satisfy itself that the level of the audit fees is commensurate with the scope of work undertaken.

Where fee reductions are offered and accepted, the audit committee should seek assurance that these reductions do not imply an inappropriate increase in the materiality level to be applied by the external auditor, or a narrowing of the external auditor's proposed scope of the audit, or a reduction in the attention which will be given to each business component and the significant audit risks identified.

If the external auditor resigns or communicates an intention to resign, the audit committee should follow up on the reasons/explanations giving rise to such resignation and consider whether the audit committee needs to take any action in response to those reasons.

- Principle 8:

  The audit committee should monitor and assess the independence of the external auditor.

  The assessment should also involve a consideration of all relationships between the bank and the audit firm (including the provision of non-audit services) and any safeguards established by the external auditor.

  Audit committees should understand the audit firm's policy on rotation of members of the audit engagement team and the audit firm's compliance with any jurisdictional or other local regulatory requirements in this regard.

  Audit committees should understand the audit firm's policy on rotation of members of the audit engagement team and the audit firm's compliance with any jurisdictional or other local regulatory requirements in this regard.

- Principle 9:

  The audit committee should monitor and assess the effectiveness of the external audit.

  At the start of each audit, the audit committee should consider whether the audit approach is appropriate, including considerations on the audit scope, the level of

materiality, areas of focus and whether planned audit procedures address the areas of significant risk for the bank.

- Principle 10:

  The audit committee should have effective communication with the external auditor to enable the audit committee to carry out its oversight responsibilities and to enhance the quality of the audit.

  The audit committee should have the right and authority to meet regularly – in the absence of executive management – with the external auditor.

- Principle 11:

  The audit committee should require the external auditor to report to it on all relevant matters to enable the audit committee to carry out its oversight responsibilities.

  The audit committee should request that the external auditor report to it in writing on other significant matters, including the following:

  - Key areas of significant risk of material misstatement in the financial statements, in particular on critical accounting estimates or areas of measurement uncertainty (e.g. loan loss provisioning and valuation uncertainties), including potential valuation bias and consequential effects on earnings, compensation structures and regulatory ratios.
  - Areas of significant management and auditor judgment, including judgments pertaining to the recognition, de-recognition, measurement or disclosure of relevant items within the financial statements and, where relevant, judgments about material uncertainties that may cast doubt on an entity's ability to continue as a going concern (including consideration of liquidity/funding issues of the entity).
  - Outsourcing of key external audit work (e.g. with respect to audits of subsidiaries) to another audit firm or use of external experts to assist with the external audit.
  - Significant internal control deficiencies identified in the course of the statutory audit.
  - Matters that are likely to be significant to the responsibilities of those charged with governance in overseeing the strategic direction of the entity or the entity's obligations related to accountability.
  - Areas of financial statement disclosures, for the bank itself and relative to its peers, which the auditor believes could be improved, including the results of discussions with management.

- Principle 12:

  The supervisor and the external auditor should have an effective relationship that includes appropriate communication channels for the exchange of information relevant to carrying out their respective statutory responsibilities.

  When communicating with management and/or those charged with governance of the bank, both the supervisor and the external auditor should consider communicating matters that may also be of mutual interest to each other in writing so that they form part of the bank's records to which the other party should have access.

- Principle 13:

  The external auditor should report to the supervisor matters that are likely to be of material significance to the functions of the supervisor.

  External auditors who make any disclosure in good faith to the supervisor cannot be held liable for breach of a duty of confidentiality. The following are examples of such matters:

  - Information that indicates the bank's failure to fulfil one of the requirements for a banking licence;
  - A serious conflict within the bank's decision-making bodies or the unexpected departure of a manager in a key function;
  - Information that may indicate a material breach of laws and regulations or the bank's articles of association, charter or by-laws;
  - Material adverse changes in the risks of the bank's business and possible risks going forward; and
  - A refusal to certify the financial statements or the expression of reservations in the audit report (other than a clean opinion) by the external auditor

  It is also usual practice for the external auditor to notify the supervisor of the external auditor's intent to resign or the bank's removal of the external auditor from office.

- Principle 14:

  There should be open, timely and regular communication between the banking supervisory authority, the audit firm and the accounting profession as a whole on key risks and systemic issues as well as a continuous exchange of views on appropriate accounting techniques and auditing issues.

- Principle 15:

  There should be regular and effective dialogue between the banking supervisory authority and the relevant audit oversight body.

  Meetings between the banking supervisory authority and the audit oversight body should take place as frequently as deemed necessary to enable them to inform each

other of topics or issues of mutual concern or interest arising from the performance of their duties that could be of relevance to the other authority, subject to relevant legal constraints.

- Principle 16:

  The banking supervisory authority and the audit oversight body should observe appropriate confidentiality requirements when sharing information.

8.2 Audit Committee

Audit Committee is a specialised committee established by the board, the mandate, scope and working procedures for which are set out in a charter or other instrument. it prepares the work of, and reports to the board of directors in specific areas for which it has designated responsibility. The board of directors assumes final responsibility.

The Basel Committee recommends that for large and internationally active banks, an audit committee or equivalent should be mandatory. The responsibilities of the audit committee are as follows:

- Financial Reporting including disclosures:
  - monitoring the financial reporting process and its output;
  - overseeing the establishment of accounting policies and practices by the bank and reviewing the significant qualitative aspects of the bank's accounting practices, including accounting estimates and financial statement disclosures;
  - monitoring the integrity of the bank's financial statements and any formal announcements relating to the bank's financial performance;
  - reviewing significant financial reporting judgments contained in the financial statements; and
  - reviewing arrangements by which staff of the bank may confidentially raise concerns about possible improprieties in matters of financial reporting.
- Internal control
  - ensuring that senior management establishes and maintains an adequate and effective internal control system and processes. The system and processes should be designed to provide assurance in areas including reporting (financial, operational, risk), monitoring compliance with laws, regulations and internal policies, efficiency and effectiveness of operations and safeguarding of assets.
- Internal audit
  - monitoring and reviewing the effectiveness of the bank's internal audit function;

- approving the internal audit plan, scope and budget;
- reviewing and discussing internal audit reports;
- ensuring that the internal audit function maintains open communication with senior management, external auditors, the supervisory authority, and the audit committee;
- reviewing discoveries of fraud and violations of laws and regulations as raised by the head of the internal audit function;
- approving the audit charter and the code of ethics of the internal audit function;
- approving, or recommending to the board for its approval, the annual remuneration of the internal audit function as a whole, including performance awards;
- assessing the performance of the head of the internal audit function; and,
- approving, or recommending to the board for its approval, the appointment, re-appointment or removal of the head of the internal audit function and the key internal auditors.

- The statutory or external auditor
  - Appointment, reappointment, dismissal and remuneration
  - approving a set of appropriate objective criteria for approving the statutory auditor or external audit firm of the bank;
  - approving, or recommending to the board or shareholders for their approval, the appointment, re-appointment and removal of the statutory auditor or external audit firm;
  - approving the remuneration and terms of engagement of the statutory auditor or external audit firm.
- Compliance with relevant ethical requirements, in particular independence and objectivity
  - reviewing and monitoring the independence of the statutory auditor or external audit firm, and in particular the provision of additional services to the bank, including the related safeguards that have been applied to eliminate identified threats to independence or reduce them to an acceptable level;
  - reviewing and monitoring the statutory auditor’s objectivity and the effectiveness of the audit process;

- developing and implementing a policy on the engagement of the statutory auditor or external audit firm for the supply of non-audit services, taking into account relevant ethical guidelines on the provision of non-audit services by the external audit firm; and,
- Approving the total fees charged for the audit of the financial statements and for non-audit services provided by the external audit firm and external audit network firms to the entity and its components controlled by the entity.

- The statutory audit or external audit
  - overseeing the statutory audit of the annual and consolidated accounts;
  - discussing with the statutory auditor or external audit firm key matters arising from the statutory audit or external audit, and in particular any identified material weaknesses in internal control in relation to the financial reporting process; and,
  - discussing the written representations the statutory auditor or external audit firm is requesting from senior management and, where appropriate, those charged with governance;
- Remedial actions
  - ensuring that senior management is taking necessary corrective actions to address the findings and recommendations of internal auditors and external auditors in a timely manner;
  - addressing control weaknesses, non-compliance with policies, laws and regulations and other problems identified by internal auditors and external auditors; and
  - ensuring that deficiencies identified by supervisory authorities related to the internal audit function are remedied within an appropriate time frame and that progress of necessary corrective actions are reported to the board of directors.

8.3 Internal Audit

According to the Basel Committee on Banking Supervision, banks should have an internal audit function with sufficient authority, stature, independence, resources and access to the board of directors. Independent, competent and qualified internal auditors are vital to sound corporate governance.

The internal audit function is an important element of the overall internal control environment. The work of internal auditors can help external auditors assess the quality of the internal control processes and identify risks.

Banking supervisors must be satisfied as to the effectiveness of a bank's internal audit function that policies and practices are followed and that management takes appropriate and timely corrective action in response to internal control weaknesses identified by internal auditors. The internal audit function helps reduce the risk of loss and reputational damage to the bank.

The Basel committee has laid down the following principles for the internal audit function:

- Principle 1:

  An effective internal audit function provides independent assurance to the board of directors and senior management on the quality and effectiveness of a bank's internal control, risk management and governance systems and processes, thereby helping the board and senior management protect their organisation and its reputation.

- Principle 2:

  The bank's internal audit function must be independent of the audited activities, which requires the internal audit function to have sufficient standing and authority within the bank, thereby enabling internal auditors to carry out their assignments with objectivity.

- Principle 3:

  Professional competence, including the knowledge and experience of each internal auditor and of internal auditors collectively, is essential to the effectiveness of the bank's internal audit function.

- Principle 4:

  Internal auditors must act with integrity.

- Principle 5:

  Each bank should have an internal audit charter that articulates the purpose, standing and authority of the internal audit function within the bank in a manner that promotes an effective internal audit function as described in Principle 1.

  The charter should at least establish the following:

  - The internal audit function's standing within the bank, its authority, its responsibilities and its relations with other control functions in a manner that promotes the effectiveness of the function as described in Principle 1 of this guidance;
  - The purpose and scope of the internal audit function;
  - The key features of the internal audit function;
  - The obligation of the internal auditors to communicate the results of their engagements and a description of how and to whom this should be done (reporting line);

- The criteria for when and how the internal audit function may outsource some of its engagements to external experts;
- The terms and conditions according to which the internal audit function can be called upon to provide consulting or advisory services or to carry out other special tasks;
- The responsibility and accountability of the head of internal audit;
- A requirement to comply with sound internal auditing standards;
- Procedures for the coordination of the internal audit function with the statutory or external auditor.

- Principle 6:

  Every activity (including outsourced activities) and every entity of the bank should fall within the overall scope of the internal audit function.

  The scope of internal audit activities should include the examination and evaluation of the effectiveness of the internal control, risk management and governance systems and processes of the entire bank, including the organisation's outsourced activities and its subsidiaries and branches.

  The internal audit function should independently evaluate the:

  - Effectiveness and efficiency of internal control, risk management and governance systems in the context of both current and potential future risks;
  - Reliability, effectiveness and integrity of management information systems and processes (including relevance, accuracy, completeness, availability, confidentiality and comprehensiveness of data);
  - Monitoring of compliance with laws and regulations, including any requirements from supervisors; and
  - Safeguarding of assets.

- Principle 7:

  The scope of the internal audit function's activities should ensure adequate coverage of matters of regulatory interest within the audit plan.

  The following aspects of risk management should be covered in the plan:

  - the organisation and mandates of the risk management function including market, credit, liquidity, interest rate, operational, and legal risks;
  - evaluation of risk appetite, escalation and reporting of issues and decisions taken by the risk management function;
  - the adequacy of risk management systems and processes for identifying, measuring, assessing, controlling, responding to, and reporting on all the risks resulting from the bank's activities;

- the integrity of the risk management information systems, including the accuracy, reliability and completeness of the data used; and
- approval and maintenance of risk models including verification of the consistency, timeliness, independence and reliability of data sources used in such models.

When the risk management function has not informed the board of directors about the existence of a significant divergence of views between senior management and the risk management function regarding the level of risk faced by the bank, the head of internal audit should inform the board about this divergence.

Internal audit should review management's process for stress testing its capital levels, taking into account the frequency of such exercises, their purpose (e.g., internal monitoring vs. regulator imposed), the reasonableness of scenarios and the underlying assumptions employed, and the reliability of the processes used.

Additionally, the bank's systems and processes for measuring and monitoring its liquidity positions in relation to its risk profile, external environment, and minimum regulatory requirements, should fall within the audit universe.

The scope of the activities of the compliance function should be subject to periodic review by the internal audit function.

Compliance laws, rules and standards include primary legislation, rules and standards issued by legislators and supervisors, market conventions, codes of practice promoted by industry associations, and internal codes of conduct applicable to the staff members of the bank.

The audit of the compliance function should include an assessment of how effectively it fulfils its responsibilities.

Internal audit should devote sufficient resources to evaluate the valuation control environment, availability and reliability of information or evidence used in the valuation process and the reliability of estimated fair values. This is achieved through reviewing the independent price verification processes and testing valuations of significant transactions.

Internal audit should also include in its scope:

- The organisation and mandate of the finance function;
- The adequacy and integrity of underlying financial data and finance systems and processes for completely identifying, capturing, measuring and reporting key data such as profit or loss, valuations of financial instruments and impairment allowances;
- The approval and maintenance of pricing models including verification of the consistency, timeliness, independence and reliability of data sources used in such models;

- Controls in place to prevent and detect trading irregularities;
- Balance sheet controls including key reconciliations performed and actions taken (e.g. adjustments).

- Principle 8:

  Each bank should have a permanent internal audit function, which should be structured consistent with Principle 14 when the bank is within a banking group or holding company.

- Principle 9:

  The bank's board of directors has the ultimate responsibility for ensuring that senior management establishes and maintains an adequate, effective and efficient internal control system and, accordingly, the board should support the internal audit function in discharging its duties effectively.

- Principle 10:

  The audit committee, or its equivalent, should oversee the bank's internal audit function.

- Principle 11:

  The head of the internal audit department should be responsible for ensuring that the department complies with sound internal auditing standards and with a relevant code of ethics.

- Principle 12:

  The internal audit function should be accountable to the board, or its audit committee, on all matters related to the performance of its mandate as described in the internal audit charter.

- Principle 13:

  The internal audit function should independently assess the effectiveness and efficiency of the internal control, risk management and governance systems and processes created by the business units and support functions and provide assurance on these systems and processes.

  The relationship between a bank's business units, the support functions and the internal audit function can be explained using the three lines of defence model.

  - The business units are the first line of defence. They undertake risks within assigned limits of risk exposure and are responsible and accountable for identifying, assessing and controlling the risks of their business. Their approach is transaction-based and ongoing.

- The second line of defence includes the support functions, such as risk management, compliance, legal, human resources, finance, operations, and technology. Each of these functions, in close relationship with the business units, ensures that risks in the business units have been appropriately identified and managed.

  The business support functions work closely to help define strategy, implement bank policies and procedures, and collect information to create a bank-wide view of risks.

  Their approach is risk-based and ongoing or periodic.

- The third line of defence is the internal audit function that independently assesses the effectiveness of the processes created in the first and second lines of defence and provides assurance on these processes.

  Their approach is risk-based and periodic.

- Principle 14:

To facilitate a consistent approach to internal audit across all the banks within a banking organisation, the board of directors of each bank within a banking group or holding company structure should ensure that either:

- the bank has its own internal audit function, which should be accountable to the bank's board and should report to the banking group or holding company's head of internal audit; or

- the banking group or holding company's internal audit function performs internal audit activities of sufficient scope at the bank to enable the board to satisfy its fiduciary and legal responsibilities.

- Principle 15:

Regardless of whether internal audit activities are outsourced, the board of directors remains ultimately responsible for the internal audit function.

The head of internal audit should ensure that outsourcing suppliers comply with the principles of the bank's internal audit charter.

To preserve independence, it is important to ensure that the supplier has not been previously engaged in a consulting engagement in the same area within the bank unless a reasonably long "cooling-off" period has elapsed. Subsequently, those experts who participated in an internal audit engagement should not provide consulting services to a function of the bank they recently audited.

Additionally, as a sound practice, banks should not outsource internal audit activities to their own external audit firm.

- Principle 16:

  Supervisors should have regular communication with the bank's internal auditors to

  - discuss the risk areas identified by both parties,
  - understand the risk mitigation measures taken by the bank, and
  - understand weaknesses identified and monitor the bank's responses to these weaknesses.

  The board of directors and senior management are responsible for establishing the bank's strategy and business models. However, changes therein may have consequences for the bank's internal control, risk management and governance systems and processes.

  Although internal audit does not set the bank's policies and should not interfere in its business decisions, it can be in a position to influence them by challenging management. Both the internal audit function and banking supervisors have an interest in the following:

  - Processes for objective setting and strategic decision making; and,
  - Quality and substance of management and governance structure and processes.

- Principle 17:

  Bank supervisors should regularly assess whether the internal audit function has sufficient standing and authority within the bank and operates according to sound principles.

- Principle 18:

  Supervisors should formally report all weaknesses they identify in the internal audit function to the board of directors and require timely remedial actions.

- Principle 19:

  The supervisory authority should consider the impact of its assessment of the internal audit function on its evaluation of the bank's risk profile and on its own supervisory work.

- Principle 20:

  The supervisory authority should be prepared to take informal or formal supervisory actions requiring the board and senior management to remedy any identified deficiencies related to the internal audit function within a specified timeframe and to provide the supervisor with periodic written progress reports.

Self-Assessment Questions

- Basel Committee's consultative paper on external audit covers standalone banks and banks that are holding companies, but not holding companies with significant bank subsidiaries.
  - True
  - **False**

- Which of the following are expectations of external audit of a bank's financial statements?
  - Reasonable assurance that the statements are free from material mis-statements
  - Statements prepared, in all material respects, in accordance with an applicable financial reporting framework
  - **Both the above**
  - None of the above

- External audit of financial statements ensures that management does not worry about internal controls.
  - True
  - **False**

- If valuations are consistently at low end of valuation range, then external auditor need not worry about management bias.
  - True
  - **False**

- EQCR stands for
  - Equivalent Quality Control Review
  - **Engagement Quality Control Review**
  - Equivalent Credit Risk
  - Environmental Quality Control Review

- Audit Committee in Banks is appointed by
  - **Board of Directors**
  - Shareholders
  - Reserve Bank of India
  - Institute of Chartered Accountants of India

- A bank's second line of defence against operating risk is
  - Statutory auditor
  - **Support functions**
  - Business head
  - Internal audit

References

Bank for International Settlements (www.bis.org)

Global Association of Risk Professionals (www.garp.org)

External Audit of Banks (Consultative Document), Basel Committee on Banking Supervision, March 2013

The Internal Audit Function in Banks, Basel Committee on Banking Supervision, June 2012

Core Principles for Effective Bank Supervision, Basel Committee on Banking Supervision, September 2012

International Convergence of Capital Measurement & Capital Standards, Basel Committee on Banking Supervision, July 1988

International Convergence of Capital Measurement & Capital Standards, Basel Committee on Banking Supervision, June 2006

Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems, Basel Committee on Banking Supervision, December 2010 (rev June 2011)

Basel III: The Liquidity Coverage Ratio and Liquidity Risk Monitoring Tools, Basel Committee on Banking Supervision, January 2013

Principles for Sound Management of Operational Risk, Basel Committee on Banking Supervision, June 2011

Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches, Basel Committee on Banking Supervision, June 2011