Lecture Note **15 to 18**

Chapter 9 : Operational Risk

Operational Risk

Introduction

The most commonly used and accepted definition of operational Risk is from Basel II which states that Operational Risk is the risk of loss resulting from inadequate or failed processes, people and systems and from external events.

This definition includes legal risk, but excludes strategic risk and reputational risk.

Why does operational risk originate?

- Inadequately defined products and services which may not be compliant to industry regulations, and/or may be exposed to risk of misspelling
- Inadequately defined policies and processes which would directly adversely impact quality of controls like checks and balances, segregation of duties as may be required
- Inadequate technology functionality, or infrastructure that exists in any technology supported environment, which organisations use in respective business operations
- Internal or external crime that takes advantage of gaps in processes for unlawful gain, i.e. fraud
- External events like terrorist attacks or natural disasters that disrupt business or cause financial losses
- Change in the environment of the industry sector (including significant regulatory changes) that impacts the operational risk profile of an organisation.

Relevance of Operational Risk

Why is operational risk relevant for accountants, auditors and management professionals?

- The Companies Act 2013 (Sections 134 and 177) lays down clear expectations from Boards of organisations in assessing the robustness of risk management framework implemented by the company.
  - Section 134 instructs that Board of Directors should include a statement on development and implementation of risk management framework for the company

- Clause (e) of Sub-section 5 of Section 134 explains the meaning of the term 'internal financial controls' as "the policies and procedures adopted by the company for ensuring the orderly and efficient conduct of its business
- Section 177 instructs that the Audit Committee shall review the risk management procedures implemented by the management.
- Schedule IV instructs that Independent Directors are required to get assurance that systems of risk management are robust and defensible.

- Paragraph 4(c) of the Standard on Auditing (SA) 315 "Identifying and Assessing the Risks of Material Misstatement Through Understanding the Entity and Its Environment" defines the term 'internal control' as "the process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, safeguarding of assets, and compliance with applicable laws and regulations. The term "controls" refers to any aspects of one or more of the components of internal control."
- Clause 49 of the Listing Agreement, indicates that disclosures are to be made to the Board of Directors on risk management, on whether the company has laid down any procedures to inform Board members about the risk assessment and mitigation procedures.
- The ICAI Guidance Note on Audit of Internal Financial Controls over Financial Reporting has several sections pertinent to the understanding of operational controls underlying in the processes
  - Assessing risks across the organisation that could lead to a material misstatement in the financial statement
  - Segregation of duties in processes
  - Addressing compliance requirements, fraud risk mitigation and implementation of meaningful control strategies
  - Assessment of Control environment, including the use of technology to automate control activities
  - Testing of Information Provided by Entity (IPE), and EUC (End Use Computation tool)
  - The auditor should test the design effectiveness of controls by determining whether the company's controls, if operated as prescribed by those authorised to perform the controls, satisfy the company's control objectives and can effectively prevent or detect frauds that could result in material misstatements in the financial statements.
  - A review of control is to be done with regard to appropriateness of the purpose of the control and its correlation to the risk/assertion
  - An assessment of the regulatory compliance framework in highly regulated industries also is part of the exercise
- Indian companies eligible to be covered under compliances of Sarbanes Oxley ("SOX") regulations have to adhere to a comprehensive framework of documentation and testing of risks and control framework
- The Internal Audit processes also establish a direct connection between risk management and audit methodology
- Operational risk forms a significant part of the ERM framework.
- Several organisations adopt standards like ISO 31000 (risk management), ISO 9000 (quality), and ISO 31000 (cyber security) for better management of risks.
- For highly regulated entities such as banking that come under RBI regulation, there are very comprehensive requirements on operational risk management.

Operational Risk Management Policy
Areas are advised to be addressed in the Policy
• Role of the Board and the Risk Management Committee of the Board in driving the

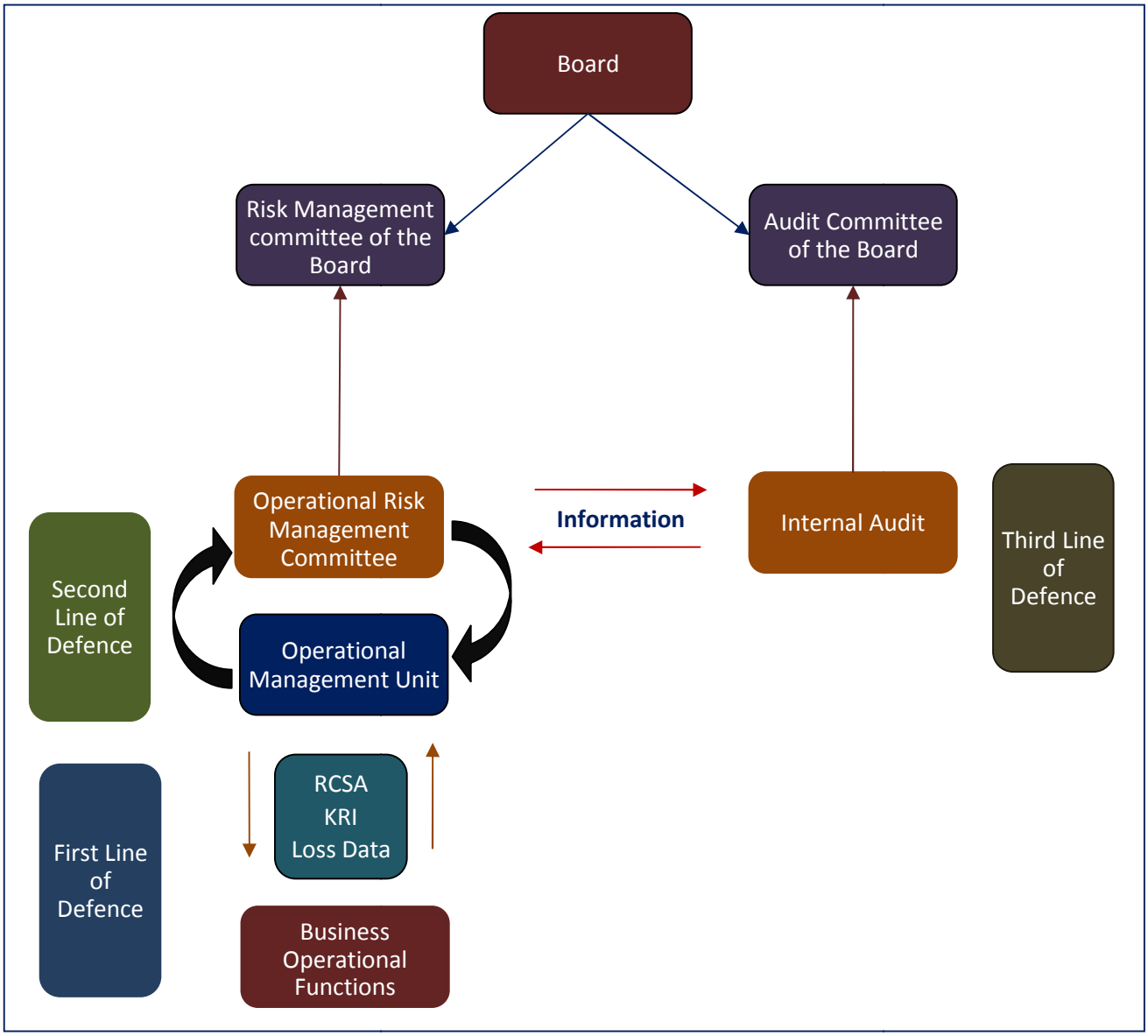
implementation of the framework

- Setting up an Operational Risk Management Committee comprising of senior management with an outline of the membership, quorum and frequency of meetings
    - The review of the Risk and Control Self Assessment (RCSA) results, Operational risk events, Loss reports, and breaches of Key Risk Indicators
    - Risk assessment of new products and services
    - Risk assessment of existing and new Technology platforms
    - Review of Cyber risk (Information security)
    - Review of Business Continuity and Disaster Recovery framework
    - Review of any regulatory development or external events that may impact the operational risk profile of the organisation
    - Management functions may highlight identified process gaps and potential issues discovered by way of routine business or reviews, and include the action being taken on them.
- The broad methodology of setting up the Risk & Control Self-Assessment library
- The constituents of the framework, like RCSAs, KRIs, Loss-Data
- Operating linkages with the other units such as those manage the policy and process documentation of the organisation, product development, internal audit, regulatory compliance unit, information security officer, business continuity plan etc.
- Capital computation methodology if applicable, needs to be described in the Policy.

Operational Risk Management Committee (ORMC)
The ORMC must conduct its business basis a Charter / Terms of Reference and the proceedings and discussions are advised to be documented for future reference and follow-up on agreed actionables.

Lines of Defence
Basel II norms indicate the recommended governance of operational risk in an organisation by three lines of defence model.
• The **First line of defence** is the function/department/role that owns the process
▪ Set up required policies govern the area of work ▪ Establish process notes, control-steps in the process notes, and methods to measure the efficacy of the controls ▪ Perform the self-assessments and monitoring of risk indicators, etc. ▪ In a financial organisation, the Operations department often has a detailed set of process notes that assign control steps to designated individuals
• The **Second line of defence** is the Operational Risk department, which while being part of the management framework, sets up, oversees the operational risk management of the first line of defence.
▪ Working with the process owners (first line of defence) to set up the risk and control matrix. ▪ Advise / recommend the method and frequency of testing of controls to the first line of defence, thereby setting up a self-assessment process based on the RCM. ▪ Perform risk assessment of new products, services and processes, especially in instances where new technology is being deployed. ▪ Review and publish results of the RCSAs and risk assessments, and any exception reports / Key risk indicators set up in the framework. ▪ Convene, and report to the ORMC, and report to the Board / Risk Committee of the Board as well with the necessary updates.
• The **Third line of defence** is Internal Audit; it is independent of management control and reports to the Audit Committee of the Board.

- An effective internal audit would highlight issues and potential gaps in processes, which were missed by the first two lines of defence as well.
- Checking on efficacy of controls that mitigate operational risk, is a key deliverable of Internal Audit.
- Over last few decades, internal audit has evolved into a concept of Risk Based Auditing.



Effective policy framework

Entity level policies: Depending on nature of the industry and applicable regulations, it is necessary for an organisation to have certain high-level policies that are applicable to the organisation, irrespective of lines of businesses or departments.

Line of business / Departmental policies: Depending on nature of the business an organisation is engaged in each business activity or department may need suitable Policies to govern and direct its functioning.

Process notes / Standard Operating Procedures (SOP)
Process notes are detailed instructions that address the specific responsibilities given in the policy documents; process notes detail the roles and responsibilities of each department / responsible person in executing a process/ transaction; it is expected that process notes have fair granularity, on how exactly a process is executed, including the controls to be exercised.

RISK IDENTIFICATION AND RISK-TYPES
RCM = Risk and Control Matrix.
RCSA = Risk & Control Self-Assessment
Inherent Risk : RCSA is built on identification of all risks that could lead to an operational risk event. This is built on an inherent risk concept. Inherent risks mean the risk as it stands assuming there is no control to mitigate it. In creating a risk register, the process, the sub-process, and the inherent risk is described.

Risk Type

Regulatory risk
When the risk of a failure may lead to a violation of the regulatory requirements that the organisation is supposed to comply with, the risk is termed as regulatory risk.

Financial risk
Risk of possible financial loss to the organisation.

Financial reporting
Risk of misstatement of financials due to a failure, is termed risk of financial reporting.

Legal risk
Risk of the organisation being at a risk of facing lawsuits, litigation, or a risk of inadequate legal enforceability.

Reputation risk
Risk of the organisation's reputation in public view is a key concern in current age of an active and engaged media and social media.

Fraud risk:
Fraud risk is basically one that can lead to an unlawful gain by an internal employee or an external person / entity by exploiting a gap in a process that fails to catch the deliberately created scenarios by the perpetuator of the fraud

External risk
External risk are essentially those on which the organisation has no control, like terrorist attacks, natural disasters etc

Risk Grading / Rating	
Impact /Severity	Impact category has to be ascribed to each risk. Impact category may fall under one or more heads
Probability / Frequency	Probability, simply put, is the chance of the transaction / process going wrong due to a failure.

Very important concept of bucketing the risk profile of the processes into four basic categories		
High Impact	High Probability	sufficient attention by management
High Impact	Low Probability	skips the management decision
Low Impact	High Probability	sufficient attention by management
Low Impact	Low Probability	

Residual risk and Rating/Grading
Identified inherent risks in processes, are expected to be mitigated by using suitably designed controls. *Higher the control effectiveness, the lower the residual risk.* *Lower the control effectiveness, the residual risk would be same or similar to level of inherent risk.*

Understanding of Controls	
Controls are activities that are intended to prevent the inherent risk from materialising into a real failure of the process / transaction.	
Verification	Refers to a control where a control step necessitates the transaction is verified by either the same individual or a different individual before it is completed.
Reconciliations	Refers to a control where an output of a process step is reconciled against other known, established sources of information.
Segregation of duties	Refers to a control where part of the transaction is executed across two segregated departments / functions / verticals thereby eliminating the risk of the originating department to carry out the entire transaction on its own.
Physical control	Refers to a control type where physical custody of an asset is the control. For example, cash and blank cheque books are stored in a vault or safe to prevent misuse.
Supervisory control	Refers to a control where the primary transaction / process is executed at a particular level in an organisation, but before finalising it, the supervisor is required to review it and accord an approval.
Exception triggers	Refers to a control where a system, or a responsible individual, throws up regular reports of transactions which are deviant from the accepted, established process. These reports are expected to be actioned upon by designated individuals.
Authorisation/ approval	Refers to a control step where, after a processing of a transaction basis built in controls is almost complete, a final authority reviews it and approves it.
Other Classification	
Classification of controls is also required to be classified in two more ways, considering whether the control is exercise manually or is built into an automated system; and if the control is intended to prevent a potential failure in the process, or detect a failure if it has happened.	
Preventive controls	are those which attempt to prevent the inherent risk from materialising into a failure.
Detective controls	are built in to analyse the process / transactions post-facto and throw up issues and exceptions.
Manual controls	are those which are exercised by a designated role in a manual fashion. For example, a verification of customer documents in a credit application, done manually, is a manual control.
Automated controls	are dependent on a predefined system check, it is called an automated control.

RISK CONTROL SELF-ASSESSMENT (RCSA)

A Risk Control Self Assessment (RCSA) activity is to be done through an objective, quantitative review.

RCSA: indicative details

Process	Sub-process	Inherent risk description	Probability rating	Impact rating	Risk type	Control description	Control type	Control owner	Control Test steps	Test results	Residual risk rating

TECHNOLOGY RISK	
In the current environment of increasing automation in business processes, and evolved technology platforms for accounting, the operational risk practitioner and the auditor must both understand the exact nuances of technology risk in any organisation.	
Main issues	
Unscheduled system downtime	A system malfunctioning due to which a business process is disrupted, due to which the necessary work output suffers a setback.
System failure pertaining to incorrect programming	This is by far the most common cause of operational risk events in an organisation, since each system can only function in the manner it is set up.
Master maintenance	Master configuration is in itself a key risk that technology users face, since the linkages between products or service programs as defined by the business users can be ambiguous, or at times contradictory instructions go to the technology team resulting in erroneous set up of Masters.
User access control	This is by far the most key control in driving controls in an automated controls environment.
Accounting systems	From an audit and accounting perspective, the most intensive focus area is the technology platform that is used for accounting. There are obvious operational risks of misstatements in financial reporting if the accounting software is not configured properly.
Change management	It is a key area of Information Technology General Controls (ITGC). It simply means that any change to the systems can cause a risk of incorrect change being developed or deployed.
Migration risk	It is a subset of change management ITGC to the extent that the controls over an end-to-end migration from one system to another, can bring upon significant operational risk if not carried out perfectly.
Technology outsourcing risk	In many organisations the technology platform, or the servicing / maintenance of the platform is outsourced. Outsourcing while has its inherent efficiency benefits comes with operational risks of running a system through a service provider that has no or little understanding of the actual business process the system supports in the organisation; such relationships of principal and service provider have to be carefully defined both contractually as well as from an operational perspective otherwise the seamless functioning of the systems can be disrupted.

KEY RISK INDICATORS AND SCENARIO ANALYSIS
As an organisation evolves from an elementary level of operational risk management to the next level, there is a need to monitor certain areas on continuous basis, by way of regular reports and exception triggers. While an RCSA hinges on the self-assessment at a point in time, the Key Risk Indicator (KRI) concept is more focused on continuous monitoring.

BUSINESS CONTINUITY PLAN
Business continuity refers to a concept that encompasses technology and business process framework that ensures that in times of unscheduled disruption of the routine process.
Any of the risks can be triggered as part of an overall disruption that is caused by any or a combination of the following reasons
• Natural disaster • Civic infrastructural failures

- Keyman risk due to death or incapacitation of key decision makers
- Failure of one department or function
- Concentrate operational activities in one major operational hub

Business Impact Analysis (BIA)
This refers to the impact that a business disruption has on all activities in an organisation; this is the base line from which an organisation can build its BCP.
Impact: Critical, Important, Routine;
Cover following aspects:

- Minimum % that the process must continue to run in BCP scenario (say 10 %, 50 % etc. of original volume / workload),
- Minimum resourcing required to carry it out,
- Maximum permissible time to allow a task to be not performed (Recovery Time)
- Category of impact due to disruption (customer impact, regulatory impact, financial loss or risk to employee health and life),
- Deriving the criticality from these parameters (including consideration for normal days and month-ends),
- Minimum technological and infrastructural requirements in the BCP site.
- This exercise will lead to decisions on which processes / activities need to be covered under BCP on priority, and which can be scoped out (and for how long).

Functional Recovery Plan (FRP)
Once the BIA is approved at management level, a detailed plan as to alternate functioning of the selected processes / sub-processes has to be made. This by far is the most challenging phase since it involves alternative resources, staffing, infrastructure and maybe technology systems as well. Depending on the complexity and nature of services provided by an organisation, each organisation must decide the steps to be taken
A FRP is a very detailed document that would list the following at a minimum

- Site in which the process would be carried out
- This needs to be documented and circulated
- The names and contacts of all key members in each process need to be listed and available to all others involved in FRP
- The FRP is useful and practical only if tested regularly,

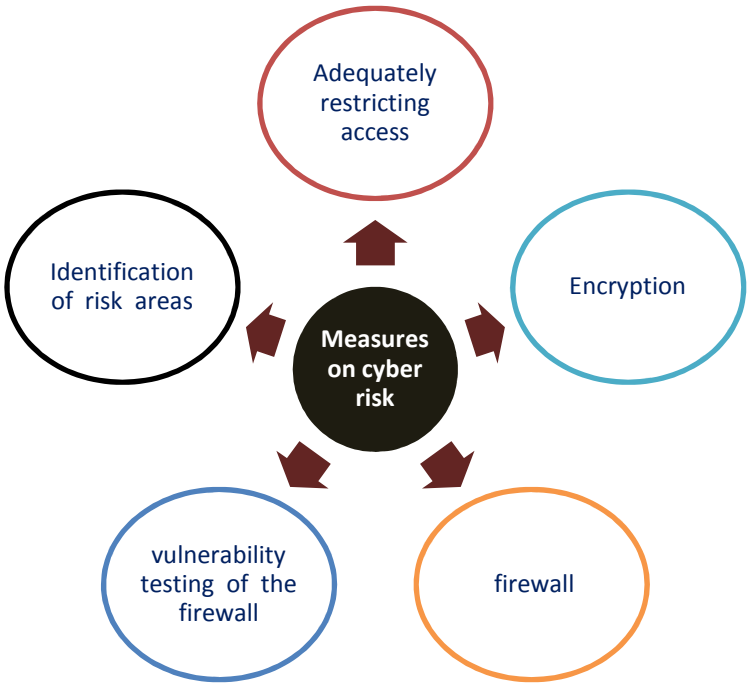
Outsourcing Risk
Hiring of an outsourced vendor/service provider must cover the following aspects:

- Clearly defined objective of outsourcing; this has to be brought into the scope of work;
- Contractual documentation to be adequate to ensure the service provider does only what is assigned and to the standard mutually agreed to by all parties involved;
- Legal indemnities to the organisation to be assessed while hiring a service provider;
- In agreements where the client and the service provider are in different states or in different countries, the respective countries' or states' laws have to be complied with;
- The BCP of the service provider has to be reviewed.
- The operational risk assessment covering regulatory risks, financial risk, financial reporting risk and other risks as delivery to end customers of the client in case the service provider fails to deliver for whatever reason.
- If technology or its disaster recovery itself is outsourced, all the attention is required to ensure the business operations work as designed and agreed.

CYBER RISK AND INFORMATION SECURITY CONTROLS

Cyber risk term broadly refers to the risks an organisation / individual is exposed to, due to a situation where its data, or network systems, or its transactions are disrupted, compromised or damaged/destroyed by an intrusive access from an external entity.

Scenarios



OPERATIONAL LOSS DATA MANAGEMENT

Some very common scenarios are elaborated in the description of three levels of activity examples in Basel norms itself. ***(ICAI Study Mat 9.28)***

Identification

- Regular reconciliations or other internal control checks
- RCSA process
- Customer complaint
- Vendor complaint/ dispute
- Regulatory inspection / audit / reviews
- Concurrent / management audits
- Internal and/or Statutory audits that identify an issue that uncovers operational loss events

Quantification	It may have a direct financial loss impact or not having an immediate direct financial impact. It is necessary to enumerate all Operational risk events.
Reporting	**A report to the ORMC**

Date of incident	Date of reporting	Event description including root causes	Financial loss	Event category	Recovery if any	Action taken	Event closed / further action due

Corrective action	Any event has to be correlated with the respective RCSA to evaluate whether it was covered in the RCSA. If yes, then assess the sampling or test frequency adequacy. If not covered, it needs to be included in future.

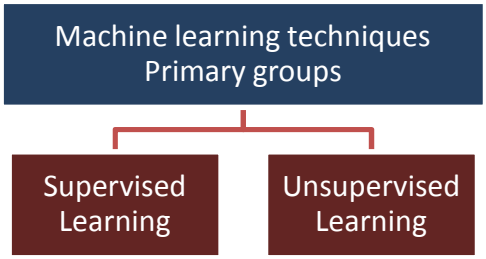
Business Analytics and Artificial Intelligence

The increasing penetration of information technology in everyday life has meant that global data size has increased in exponential terms in velocity, variety, and volume.

Machine Learning

A standard software code is characterized by explicit rules that a computer is supposed to perform. In case, there is a change in the data / situation, a programmer needs to change these explicit rules.

Machine learning uses an inductive approach to form a representation of the world based on the data it sees. It is able to tweak and improve its representation as new data arrive



Analytics – Risk Management Applications	Risk management faces new demands and challenges. In response to the crisis, regulators are requiring more detailed data and increasingly sophisticated reports.
Artificial Intelligence	Artificial Intelligence is the science that makes intelligent machines especially computer programs. It is a way of making a computer in a similar manner the intelligent humans think. It has been dominant in many fields such as • Gaming • Natural Language Processing • Expert Systems • Vision Systems

Distributed Ledger Technology

Distributed Ledger Technology (DLT) is the generic name of advanced technologies that allow nodes in a decentralized information technology network to securely propose validate and record state changes (or updates) to a synchronised ledger that is distributed across the network's nodes.

Benefits

- Significant reduction in operational complexity
- Major increase in processing speeds and consequent asset availability
- Higher operating efficiency due to lowered reconciliation requirements
- Transparency and immutability in transaction record keeping
- Network security and safety due to distributed architecture
- Overall reduction in credit and operational risk

INSURANCE

Insurance is used by organisations to mitigate operational risks that can be insured.

- Insurance coverage is commonly available for risks arising out of fire
- other losses due to terrorist attacks, natural disasters etc can also be covered
- Recently a new concept of Cyber risk insurance has also come up, and there are companies offering cover against the risk of damages due to lawsuits / compensation on account of being a victim of cyber-attack, due to which data of customers, vendors or any other counter- party can be leaked to an unauthorised, malevolent entity.