CHAPTER 9

# OPERATIONAL RISK MANAGEMENT

## LEARNING OUTCOMES

**After going through the chapter student shall be able to understand**

- Operational Risk Management
  - (a) Definition,
  - (b) Scope and
  - (c) Techniques

## 1. INTRODUCTION

### 1.1 What is Operational Risk?

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.

Basel II is the common name used to refer to the "International Convergence of Capital Measurement and Capital Standards: A Revised Framework," which was published by the Bank for International Settlements in Europe in 2004, and the framework is broadly adopted, with country level customisation as required by the countries that have been party to the accord. While this was specific only for the regulated financial institutions industry, the overall concept of operational risk remains the same irrespective of the industry.

Each and every industry, whether manufacturing, trading or in service sector, is subject to a degree of operational risk though the level of risks may differ between industry sectors,

companies, the nature of products and services offered, and the actual management control over these risks.

Operational risk is an overarching concept interrelated with several other types of risks, and cannot be viewed in isolation. The most important risks linked to operational risk are risk of non-compliance to applicable laws and regulations, risk of fraud losses due to an internal or external event that takes advantage of gaps in the processes to make an unlawful gain, risk of financial losses, risk of incorrect financial reporting, and in several organisations, reputational risk is also part of the areas touched by operational risk.

### 1.2. Why does operational risk originate?

(a) Inadequately defined products and services which may not be compliant to industry regulations, and/or may be exposed to risk of misspelling;

(b) Inadequately defined policies and processes which would directly adversely impact quality of controls like checks and balances, segregation of duties as may be required;

(c) Inadequate technology functionality, or infrastructure that exists in any technology supported environment, which organisations use in respective business operations;

(d) Internal or external crime that takes advantage of gaps in processes for unlawful gain, i.e. fraud;

(e) External events like terrorist attacks or natural disasters that disrupt business or cause financial losses;

(f) Change in the environment of the industry sector (including significant regulatory changes) that impacts the operational risk profile of an organisation.

Thus, Operational Risk Management (ORM) is primarily an exercise in mitigating potential losses, i.e. possible losses, through a well-laid out mechanism of identifying the inherent risks in a business process and reviewing / testing the efficacy of the controls related to each risk.

Additionally, an important part of ORM is also to identify and report operational risk events, including their financial impact (losses and recoveries) if any. Thus, an adequate governance framework is expected to cover both the preventive and the lag aspects of operational risks.

In coming sections, we shall also elaborate on the concepts outlined above, in terms of how policies, processes and technology failures can cause possible risks and losses.

## 2. RELEVANCE OF OPERATIONAL RISK

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

(a) 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, including identification of risks, which as per Board's opinion could threaten the very existence of 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, including adherence to company's policies, the safeguarding of its assets, the prevention and detection of frauds and errors, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information."

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.

(b) 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."

(c) 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.

(d) 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;

While the Guidance Note does not explicitly dwell on operational risk per se, the overall approach and methodologies mentioned in the Note rest on, and derive from an implied understanding of the auditor's understanding of operational risks and the mitigating controls of the organisation; for instance, the auditor is expected to have a thorough understanding of the automated and manual controls that lie in each of the processes that have a direct bearing on the financials of the organisation.

The following section on auditor's responsibility is broadly paraphrased from the Guidance Note, and it is recommended that the student read it in entirety for a holistic understanding:

- 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, to ensure timeliness, accurate and reliability of the information used in the financial control are dependent on underlying application systems that are used to generate, process, store and report the information in a manner that adequately addresses effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability;
- 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; appropriateness of control considering the nature and significance of the risk; competence of authority performing the control (especially if it is of a nature of supervisory review); frequency and consistency with which the review control is performed, including clarity of the exact steps of performance of the review control;
- An assessment of the regulatory compliance framework in highly regulated industries also is part of the exercise, and any significant weakness in internal controls related to implementing compliance requirements may result in a material weakness highlighted in the report.

(e) Moreover, 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, and these necessitate that the management personnel, consultant or auditor be highly proficient in assessing operational risk that impacts all categories of risk such as regulatory risk, financial loss risk, financial reporting risk, legal and contractual risk, fraud risk and reputational risk etc. The companies where SOX stipulations are applied, have to adhere to internationally established practices of risk management.

(f) The Internal Audit processes also establish a direct connection between risk management and audit methodology; currently most internal audit firms practice a Risk Based Audit approach, which necessitates an understanding of all risks including a comprehensive understanding of operational risks since it overarches on several other areas of risk.

(g) Operational risk forms a significant part of the ERM framework. Several organisations that are

complying to the Companies Act 2013 stipulation on implementing a risk management framework.

(h) Several organisations adopt standards like ISO 31000 (risk management), ISO 9000 (quality), and ISO 31000 (cyber security) for better management of risks. Professional managers working on these are also required to have an understanding of operational risk.

(i) For highly regulated entities such as banking that come under RBI regulation, there are very comprehensive requirements on operational risk management. Banks are also required to provide capital under regulatory norms, for which specific calculation methods are also prescribed.

Hence there is a strong convergence of audit and operational risk in current context of corporate governance responsibilities of management, Board and the role of the auditors.

# 3. OPERATIONAL RISK MANAGEMENT GOVERNANCE

As outlined in section 1, as part of the overall responsibilities of the Board of Directors, an oversight on the operational risk profile of the organisation is also included. The nature and intensity of Board oversight may differ from organisation to organisation, depending on its constitution, any specific requirements from a regulatory angle, the industry and the nature of business etc.

For banks it is mandatory to have an Operational Risk policy approved by the Board, and the RBI guidelines have clearly described roles and responsibilities of the ORM Committee, the Chief Risk Officer and other roles that are expected to engage in the implementation of the framework. For other industries where a Board approved policy may not be mandatory as per regulatory environment, it is still strongly advisable to have a comprehensive policy documenting the governance mechanism of operational risk.

## 3.1 Operational Risk Management Policy

The following areas are advised to be addressed in the Policy; the list is indicative and not comprehensive; the organisation depending on the priorities and readiness level can evolve new areas to be covered.

- 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 self-awareness of the management functions on highlighting such issues is an evolving process.

- The broad methodology of setting up the Risk & Control Self-Assessment library, the roles and responsibilities of those engaged in performing the control testing, the collation of results and review process need to be outlined in the Policy.
- The constituents of the framework, like RCSAs, KRIs, Loss-Data to be described in detail followed by a brief on roles designated to perform the necessary activities. Each of the policy stipulations is to be ideally backed up with corresponding process notes to detail the granular steps in implementation.
- 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. need to be outlined since operational risk impacts all these areas.
- Capital computation methodology if applicable, needs to be described in the Policy.

## 3.2 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. The regular updates to the Board (or the Risk Management Committee of the Board if the task is assigned to it by the Board) have to be provided by the management, covering key highlights of all the constituents.

The Operational Risk framework is effective only if imbibed at all relevant linkages who are managing the monitoring process at the departmental level. Hence it is advised that the Committee instruct and/or arrange regular trainings and awareness camps for the departmental staff, including giving them sufficient understanding of process of identifying new risks and adding them to the RCSA library from time to time, a process duly assisted and facilitated by the Operational Risk unit.

## 3.3 Lines of Defence

Basel II norms indicate the recommended governance of operational risk in an organisation by three lines of defence model. This is followed by banks in India too as part of regulatory guidance on operational risk management. However, this concept can be used by any industry with some customisation on basis of the organisational structure, the complexity of the business processes and evolving capability of the control awareness.

The ***First line of defence*** is the function/department/role that owns the process. They are supposed to have sufficient governance on the operational risks pertaining to their areas of responsibility, such as

- 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.
- Examples are, in a financial organisation, the Operations department often has a detailed set of process notes that assign control steps to designated individuals, and also a method of measuring / tracking if the controls were exercised properly.

These tracking / measuring tools could be at varying frequency, being built into a formal RCSA (Risk Control Self-Assessment) where risks and control efficiency are highlighted. This line functions closely with the Second line in a collaborative method which could be formalised in any governance process established by the ORM Committee.

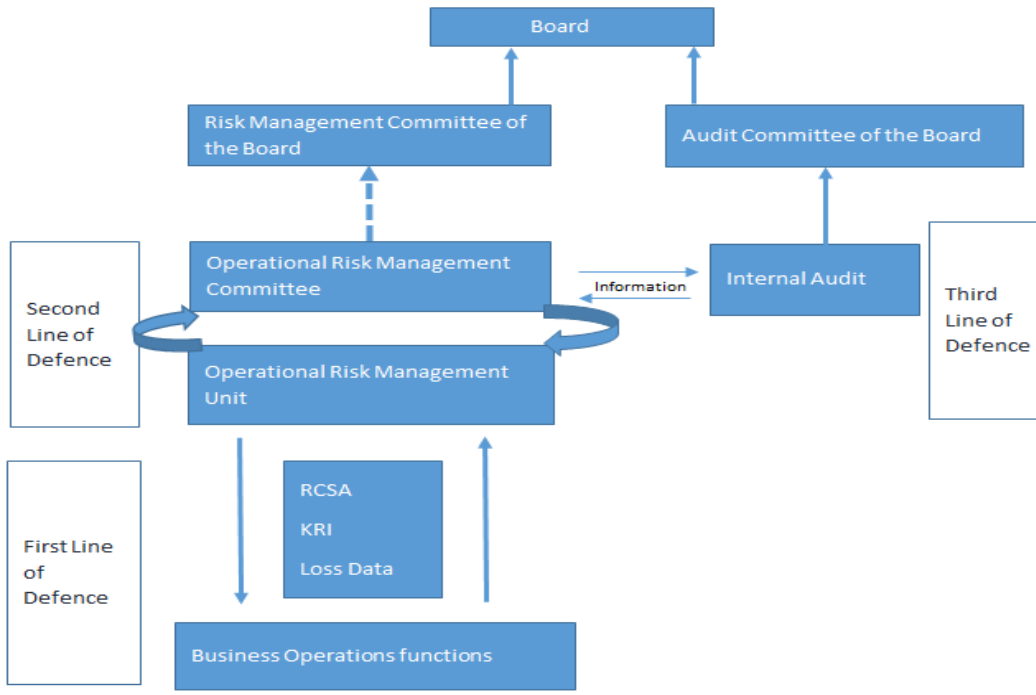
The ***Second line of defence*** is the Operational Risk department, which while being part of the management framework, sets up, oversees the operational risk management of the first line of defence. The typical roles played by the second line of defence are:

- 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. As an independent vertical, their value addition provides a better insight into the process from a holistic perspective since they are not directly involved in managing the process.
- 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. The term itself refers to an approach where the audit function identified risks and controls in a very similar fashion as the operational risk methodology, and then choose to focus their attention and deploy resources on checking the areas of choice.

All three lines of defence are expected to work in a professionally collaborative manner, respecting each other's views and concerns. ORMC of an organisation must include the Internal Audit head too, in addition to senior management, so that a holistic view of the risks and controls is obtained.




For an effective Operational Risk Management Framework, the following focus areas are recommended; though they fall outside the direct management of the Operational Risk

department, these are prime drivers of operational risk, and hence frequently either the cause of higher operational risks and/or its remedial measure.

## 3.4 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. These are typically owned at the highest levels of management and set the tone at the top. Examples are Code of Conduct for employees, Whistleblower policy, Expense Delegation Policy, Procurement Policy, Information Security Policy etc.
- **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. Inadequate definition of the policy statement and responsibilities thereof are often a cause of operational risk events. Examples are Credit policy in a lending institution, product specific policies in a manufacturing industry, Human Resources policies, and Operational policies. Policies often include a "standard" too, which outlines the specific deliverables and a minimum expected level of performance in it. In some organisations, the Standards could be maintained outside the Policy documentation, nevertheless, it is an advisable item to have in overall governance process.

Policies have to be made in a manner that they are compliant all existing applicable laws and regulations, and enable the organisation meet the business objective.

## 3.5 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. In an advanced operational risk management environment, the process notes tend to be very articulate and define the processes granularly and leave no scope for ambiguity or misinterpretation by those responsible for execution.

Taking the same example as in policies, in a lending institution, a credit process note would detail the exact steps that an organisation is to follow, in lending money to a customer and all the checks and controls expected to be done in the process. A manufacturing process manual may describe in detail aspects like the factory specifications, technology used in the process or the sub-process, the assembly line, the specific departmental, and individual roles and technical tasks, output, productivity and the quality expected.

# 4. RISK IDENTIFICATION AND RISK-TYPES

## 4.1 Definition of RCM and RCSA

The acronym RCM stands for Risk and Control Matrix. To understand the Risk and Control concepts we need to understand the various terms that are commonly used in assessing them, as is elucidated in this section.

The acronym RCSA stands for Risk & Control Self-Assessment; when a test step is tagged to each of the controls and the management function performs that test, the exercise is known as a Risk and Control Self-Assessment.

This is the basic platform on which an ORM framework is built. It has these critical constituents: Risk, Control, Risk grading, Control Owner

## 4.2 Description of the 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. To arrive at the inherent risk, one may use judgement of the impact category that a failure in the particular process/sub-process can lead to. For example, in a finance lending business, an error in data entry of a bank account of a customer, can lead to a disbursement going to the wrong account and hence cause financial loss to the organisation. Or, in case of an inadequate check on KYC of customer before approving a loan facility, it is possible that a regulatory violation is committed, leading to regulatory risk.

This exercise is a comprehensive one and can take an organisation a few months or years to effectively document all identified inherent risks, and at any point in time, there would always be some new learnings to modify and enhance the list.

The Risk description is then followed by an assessment of the impact that a failure can have. Some failures will have a minor impact on the organisation while some may cause a higher level of impact. It is up to each organisation what it considers major and medium and any intermediate grading it may have in between these two, basis the risk appetite of the management and shareholders.

Example of a major impact are regulatory licence suspension, or a class action legal indemnity that can throw all or most of the financial profits in jeopardy; a financial loss due to excess payment or short recoveries of dues, that can wash away the projected revenues; loss of life of employees or significant part of physical assets;

Example of minor impact are violation of regulation but not likely to invite penal action by regulator; financial loss up to a small portion of the projected revenues to an extent that can be easily absorbed; litigation losses on individual cases that can be easily absorbed without significant

impact to the revenues, injury to employees or loss or property that can be recuperated with a small expense or effort.

Broadly, **risk types** that often overlap or are caused by operational failures, used commonly are:

(a) **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. An inter-related term, often used in conjunction with regulatory risk, is statutory risk. Statutory risk refers to violation of applicable law. Essentially, in common parlance they often refer to the same group of potential risk, though, most organisations use the word statutory risk to refer to violation of law, and regulatory risk to refer to violation of norms issued by the specific regulator they fall under. KYC-AML is a common example of being a statutory and regulatory risk (since Prevention of Money Laundering is an Act), and since all regulated industries have norms on KYC, it is commonly tagged as regulatory risk.

(b) **Financial risk:** Risk of possible financial loss to the organisation.

(c) **Financial reporting:** Risk of misstatement of financials due to a failure, is termed risk of financial reporting. This may be linked to financial risk in some specific risks, but not always. For example, an excess payment made to a vendor may qualify for being categorised as financial loss, but if it is accounted for properly it may not lead to risk of financial reporting. Some organisations choose to include a description of financial assertions in the RCSAs, so as to indicate the nature of impact a failure may have on the financial reporting from an audit perspective.

(d) **Legal risk:** Risk of the organisation being at a risk of facing lawsuits, litigation, or a risk of inadequate legal enforceability. Often, contractual risk is clubbed with legal risk, since lack of due diligence in contractual agreements is inter-related to legal risks, given the chance of disputes between parties, or the incapability to enforce terms of the agreement due to a poorly defined contract.

(e) **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. The related aspects like a lower credit rating for the organisation, higher borrowing costs, reduction in credit terms extended to organisation, fall in share price leading to overall market capitalisation fall, and disruption due to vendors/suppliers/service providers refusing to do business due to reputational risk are all real risks that a business faces. Quite often, a failed operational transaction leading to a customer dispute/complaint may lead to an enhanced reputation risk.

(f) **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; Examples are falsifying identity for taking a loan, or raising an inflated bill, deliberate excess payment to a customer / vendor etc. With the enhancement of COSO framework to ensure highest degree of accuracy and completeness in financial statements, fraud risk in financial reporting assumes greatest

importance. Operational control failures, such as those that allow an employee to deliberately tamper data (on systems or manually) leading to financial misstatement is a typical fraud risk, linked to operational risk (poorly designed process of reporting of data).

(g) **External risk:** External risk are essentially those on which the organisation has no control, like terrorist attacks, natural disasters etc. But these are real risks and the losses of loss of employee lives or damage to physical assets incurred on these events do fall under operational losses.

## 4.3 Risk Grading / Rating

Table of examples below indicate an assessment of impact into high, medium and low. These are purely indicative and a hypothetical example; each organisation has to create this grid basis a mix of qualitative and quantitative parameters and keep improving upon it with ongoing learnings with reference to the risk appetite.

A purely illustrative table is given below, containing hypothetical thresholds.

A lot of it is subjective to the perception of the organisation and basis the risk appetite of each operational risk framework. These are only examples, and parameters are to be set by the ORMC and evolved.

| *Parameter* | *High* | *Medium* | *Low* |
|---|---|---|---|
| Financial loss | Over 10 lacs (due to any event falling under any Loss category) | 5 to 10 lacs (due to any event falling under any Loss category) | Below 5 lacs (due to any event falling under any Loss category) |
| Regulatory violation | Design level error, over 1% violation in key regulatory compliance;<br>May lead to regulatory reprimand / license suspension / penalty etc. | Transaction level errors, above 0.2% and below 1% of transactions ;<br>May lead to regulatory reprimand/ penalty | Below 0.2% of transactions<br>Minor violations, but overall the process design is in place |
| Statutory violation | Design level error, leading to serious non-compliance of applicable laws, may lead to penalties, reprimand, withdrawal of licence etc. | Transaction level errors, not leading to serious penalty / withdrawal of licence etc., but may lead to issues with statutory authorities | Minor transgressions, not leading to statutory penalty etc.<br>Overall process being in place, only transactional errors occur. |
| Financial reporting error | Significant error that may lead to material misstatement of financial information and/or material | Minor error but overall could lead to a misstatement in financials and an adverse comment from | Minor error in financial reporting, leading to a material misstatement or a qualified statement |

| | | | |
|---|---|---|---|
| | misstatement of financial information and/or qualified statement from auditors.<br>May be impacting regulatory reporting and impact on investor and lender relationships;<br>Fraudulent misstatements | auditors;<br>May lead to external adverse impact on investor / lender relationships. | from auditors. |
| Reputational loss | Reputational risk event inviting regulatory and media attention,<br>Significant Investor and lender impact<br>Attrition of employees due to reputational loss | Reputation risk event inviting moderate media attention, but no significant impact on investor / lender relationship or regulatory aspects. | Minor event with short term impact only. |
| Cyber risk | Loss of data of more than 1% of accounts /<br>Failure of firewall vulnerability control of over a defined threshold that could threaten entire network | Minor loss of data /<br>Failure of firewall vulnerability control to limited impact on network, or limited to some part of it | Minor issues not amounting to any significant impact on network security |
| Fraud risk | Fraud in financial statement leading to misstatement;<br>Significant fraud in core business process of organisation with a fraud loss of over 10 lacs,<br>May invite media, regulatory ire, legal suits, law enforcement action etc. on company/officials. | Fraud impacting financial statement but not material misstatement;<br>Fraud in peripheral processes of an organisation not its core business process;<br>Will not invite regulatory or law enforcement / legal action on company/ officials<br>Impact of less than 10 lacs loss | Transactional events of fraud with negligible impact on the overall financial statements;<br>Events not impacting regulatory, investor, or law enforcement / legal aspects |

- **Impact /Severity:** Impact category has to be ascribed to each risk. Impact category may fall under one or more heads; for example, a fraud risk may also result in financial loss; or a regulatory violation may lead to a reputational risk; or, wrong product configuration sold to a customer and inability to service it, may lead to regulatory, reputational and financial losses in combination; thus, it is possible to tag multiple heads of impact as well as use only the primary impact category, that is a flexible judgement of the organisation.
- **Probability / Frequency:** Probability, simply put, is the chance of the transaction / process going wrong due to a failure. Probability of failures are often expressed in percentage terms of the total volume of transactions in a process if it is a high volume transaction process; in processes where the universe of transactions is of lower volumes or of lower frequency, a qualitative judgement on probability is often required to be taken. Probability can be arrived at in high-volume processes by analysing past data on failures in the process. It is important to note that this is often a subjective assessment in instances where no past data is available.

This brings us to a very important concept of bucketing the risk profile of the processes into four basic categories:

- High Impact – High Probability
- High Impact- Low Probability
- Low Impact – High Probability
- Low Impact – Low Probability

While the first and third categories tend to get sufficient attention by management, the high impact low probability often skips the management decision purely because these incidents are either not foreseen at all in reality or even if they are, they are so rare but with severe impact that putting a risk mitigation plan for them is very difficult. However, wherever possible the management must consider them on an evolving basis.

While it is easier for an operational risk practitioner to work on four buckets, it is often enhanced by introducing an additional factor of Medium Probability and Medium Impact, depending on the organisation's view on risk grading.

## 4.4 Residual risk and Rating/Grading

Identified inherent risks in processes, are expected to be mitigated by using suitably designed controls. In any organisation that has a view on managing operational risks, all or most of the identified risks in a process would be controlled through a process that reduces, or eliminates the risk of a failure taking place in that process.

Residual risk is thus the remaining risk in a process assuming the control designed is operating properly. Thus, all companies strive to have a low level of residual risk.

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. We shall study more about the concept of controls in the subsequent section.

## 5. UNDERSTANDING OF CONTROLS

Controls are activities that are intended to prevent the inherent risk from materialising into a real failure of the process / transaction. These activities are designed keeping in mind the overall process objective, the inherent risks in the process, and the impact of the risk if the failure were to materialise in reality. Given that this concept applies to all industries we have attempted to broadly categorise the types of controls into the following.

There are several different, but closely related or similar categorisations used in different kinds of control framework, organisations, but mostly they would fall under these categories, thus this is an indicative list and is subject to evolution.

(a) **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. For example, in a financial lending institution, a department may process an application along with the customer documents, and carry out a verification at the end of the process within the department, before passing the file to the other department for further processing that relies on the accuracy of the earlier department's processing.

(b) **Reconciliations:** Refers to a control where an output of a process step is reconciled against other known, established sources of information. For example, before publishing a report, the responsible person may use the primary data, and reconcile it with other existing sources from multiple systems / departments before finalising it.

(c) **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. For example, in a finance lending organisation, the process of sourcing an application is owned by Sales department, while the credit process is completely segregated into the Risk department, and further, the entire operational process of checking the accuracy and completeness of the processed application documentation may lie with Operations who would actually set up the account and make the disbursement.

(d) **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. Original critical documents, legal agreements etc. are also stored safely in safe keeping vaults. In certain cases, organisations may further add a control of authorisation thereby creating a process where an individual holding a key has to operate it first, and additionally the manager would use a different key in his position and open the vault to be accessed.

(e) **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. Sometimes this is also classified as Authorisation if the authorisation is given by an authority superior to the one originating the transaction. Often, where the primary control is MIS (Management Information System) such review based controls fall under supervisory control category.

(f) **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. This control type is effective only when the process has achieved a stability and scale that only deviations are reviewed by authorities. For example, reporting of error rate in an operational process is an exception trigger. Or, reporting of a high balance in a suspense account beyond the usual acceptable levels can be an exceptional report item.

(g) **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. For example, there are several organisations use automated or semi-automated credit decision tools in a financial lending process. However, as per selected parameters, a credit officer may be designated to review the system based processing and approve it as well.

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.

(i) **Preventive controls** are those which attempt to prevent the inherent risk from materialising into a failure.

(ii) **Detective controls** are built in to analyse the process / transactions post-facto and throw up issues and exceptions. Preventive control in a transaction intensive process may be verification and authorisation; a detective control may be MIS on errors that falls under supervisory review.

For example, two people being required to count cash before making a cash payment, is a common preventive control. If there is a cash reconciliation process at end of day, that detects whether the correct amounts of cash was paid out, it is termed detective control.

(iii) **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.

(iv) **Automated controls** are dependent on a predefined system check, it is called an automated control. For example credit application data is fed into an automated system and data supporting the process is done by a system, giving the recommended investment decision and/or next steps in processing as the output. For example, a complex credit decision involving several parameters and input data, if done manually, is subject to error if done manually; using a system would be an optimal control and hence an automated control is set

up. There may be controls that are partly automated and use manual steps to synergize / verify data from automated controls, these are termed hybrid controls. A MIS process that uses automated data, and involves manual collation from different sources and checked manually by a verifier is a hybrid control.

## 6. RISK CONTROL SELF-ASSESSMENT (RCSA)

A Risk Control Self Assessment (RCSA) activity is to be done through an objective, quantitative review. Some assessment checks may involve sampling, some may involve specific affirmative / negative answers, or some other test Steps. It is imperative to define the test step of each check in each row item of the RCSA so that objectivity is maintained in the exercise irrespective of the person conducting the activity. If the check involves sampling, it is ideally recommended to follow an established standard or practice; for example, the ICAI guidelines on sampling logic used in audits can be used. The residual risk rating is important to derive after the test results are populated on each check, thereby indicating to the management any areas requiring attention.

**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* |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | |

Additional information may include, financial assertion impact (if any), the name of system used (if any), Sample description of test done etc.

## 7. TECHNOLOGY RISK

As we saw in the very fundamental definition of operational risk, a key constituent is 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.

All organisations nowadays use some kind of systems, technology platforms depending on the nature of business. For large complex business processes, there would be several systems, either in isolation or interrelated with each other, working to deliver the business outputs required.

From an auditor's perspective or the operational risk professional perspective, the main issues that can surface from technology risk are:

**(a) Unscheduled system downtime** or a system malfunctioning due to which a business process is disrupted, due to which the necessary work output suffers a setback. This could result in financial loss, loss of opportunity of business, customer issues and loss of raw material. For

example, a system failure in a financial lending organisation may lead to critical customer commitments like disbursements not happening due to which customer may suffer losses; or inability to post incoming payments on account leading to liquidity issues; or inability to service a customer account leading to customer attrition. Organisations have backup servers, systems, databases, and disaster recovery procedures to ensure work disruption is minimized in such circumstances. The operational risk manager is expected to have an overview of the specific facilities available to the technology department, to service the organisation's critical needs at such times of failure.

**(b) 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. Organisations either build their own systems or buy them from specialised service providers, and customise them. In either case, depending on the nature of transactions required to be processed, a very detailed business requirement document is required to be given to the technology department by the business user groups. Often, either due to incapability or poor co-ordination between the business user groups, the requirement document does not capture the entire detailing and the extremely granular details that are required by the technical teams doing the coding, customisation or the deployment. The result is a poorly executed system that causes errors in processing, which may have financial, regulatory, fraud risks, depending on kind of error in the system.

For example, taking an example of a lending institution that processes loan applications on a particular Loan Originating System and a Loan Management System the following scenarios indicate how errors of programming can cause severe operational risk failures:

- Processing fees or interest not being charged correctly to the loan account correctly, resulting in financial loss and / or customer disputes;
- Hands-off between different control owners may be compromised if the system workflow is not properly defined on the system; for example, an application that requires specific fraud risk checks on documents supplied by customer, may totally bypass the required check and go from sales to credit department, thus exposing the organisation to fraud risk. Or, an application may get processed with incorrect customer data, credit bureau information basis the credit parameters set in the system. The coding of acquisition scorecards in the financial lending industry is a typical example of a very sensitive area where technology risk is the cause of operational risk.

Taking an example from manufacturing,

- A software error in parameterizing the right quantity of one raw material to flow into an automated assembly line may result in a completely wasted production output thereby causing an operational loss;
- Another industry-agnostic example is wrong master maintenance of taxation rates in any business charging its customers can lead to a non-compliance in taxation requirements.

**(c) Master maintenance:** All systems, besides the basic coding, need a set of Masters which are user-defined parameters that enable the processing of the data. 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.

**(d) User access control:** This is by far the most key control in driving controls in an automated controls environment. For example, in a lending institution, a credit officer if allowed to process operational activities beyond his job role may result in compromise of the segregation of duties that the process is designed with; or, if an user may have a higher level of access to changing customer data by one modification, while the process may require an authorisation which was bypassed due to inadequate user access control maintenance. User access control requires the user profiles to be set up properly upfront in the initial basic programming, followed by correct assignment of user profiles upon employee requests as per their permissible authorities basis their job role. Organisations are required to delete or modify user IDs once employees move out from their roles or the organisation itself.

**(e) 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. In complex organisations with several types of transactions that have a financial impact are performed in various systems, the feed in from other production systems (i.e. outside of the main accounting system) are very important to check for accuracy since they are used in financial reporting. The feeds, if manual have their own risk of incorrect manual processing; in automated feed process also, there are risks of incorrect data inflows that could lead to financial misstatements. In lending institutions, the loan management systems are different from the main accounting system; a huge amount of data, at various frequencies, flows into the accounting system. The linkage of the source system to the correct GLs in accounting system, and appropriate reconciliations, the exception reports, analysis and ongoing supervisory reviews can prevent the data from being inconsistent in final reporting. Any regular exceptions in the data in two systems, need to be analysed to find out the root cause of the technological reason, and any incorrect programming. Examples are the data of customers like interest due, principal outstanding, overdue amounts etc. which flow from loan management systems to accounting systems.

**(f) Change management** 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. This can be a result of multiple causes:

- Change being carried out without approvals of authorised roles,
- Change being wrongly conceived by the user groups, without adequate analysis of pros and cons for the change, and getting deployed by the technology unit under approvals

- Change, though conceived correctly and communicated correctly under adequate approvals to the technology team, is wrongly executed
- The preventive control around all these issues, is to ensure only authorised roles, whether internal or external, have access to making changes in the system; these changes have to be approved by all the departments that the change impacts so that the impact of change is well understood before approvals are accorded; and, a proper user acceptance testing is conceived and conducted before deploying the change. Often the design of the User Acceptance Testing (UAT) script is found defective, and sufficient combinations of test data is not put through the system resulting in some functionalities not being adequately tested.
- A database of such changes, such as audit trail reports have to be judiciously maintained as to what changes were carried out, including the issue tracker related to the changes. This helps track back any changes, to ensure that appropriate change management control and review was exercised.

**(g) Migration risk** 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. A significantly high effort is required to ideate before the deployment as to the exact manner of migration; migration has to cover:

- Data, both dynamic and static
- Functionality mapping from old to new system, and any changes to be adequately familiarised within user groups
- Exception reports that could help track any incorrect migration points
- User acceptance test scripts to be intelligent enough to enable the usage of the new system after adequate granular review
- An emergency roll back plan in case some significant unpredictable issue comes up in migration deployment.
- An auditor or operational risk manager is required to carry out a review of the data integrity and the functionality of the systems that have an impact on the financials of the organisation. This risk is not only restricted to financial reporting, but any risk that could jeopardise the business process, including regulatory, financial and other risks.

**(h) 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.

## 8. 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.

They are actually interrelated concepts. For example, in a manufacturing process, a half yearly RCSA check may be built on checking for number of batches failed in quality check; however a KRI may be a better method being a lead indicator, where batch failure numbers are reviewed every week rather than at longer intervals. Conversely, if a KRI exists for a process, an RCSA can be built using the KRI.

In an evolved internal control framework, there would be a robust KRI monitoring process.

In initial stage of an operational risk management implementation, when either a KRI or RCSA is not possible due to paucity of objective data or capability to analyse it, an organisation can use Scenario analysis as a surrogate mode. In a scenario analysis, the risk scenarios are described and a subjective assessment of the risk materialising is described, using whatever available data and reviews are possible to collate. Over time, this method has been gradually overshadowed by more objective methods like KRI monitoring (which is based on MIS), and RCSA (which is based on actual testing and/or uses the KRI as a base).

## 9. 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, an alternative mode of management of priorities, technology solutions, and business processes is undertaken.

Business Continuity is now an integral part of Operational Risk Management. Any of the risks we enumerated above, can be triggered as part of an overall disruption that is caused by any or a combination of the following reasons:

(a) Natural disaster affecting services of either technology solutions and/or the business process itself; to elaborate, a situation to invoke BCP may exist in a case of natural disaster like flood, where staff of a company are unable to go to office; or, it may be a combination of situation where the technology solutions of the company that is required for daily functioning of the organisation is also not working;

(b) Civic infrastructural failures like essential services of electricity or transport being brought down due to terrorist attacks or natural disasters;

(c) Keyman risk due to death or incapacitation of key decision makers in a company leading to chaos in management of the company;

(d) Failure of one department or function to do their assigned tasks in a case of disruption may cause the entire process to delivery of the organisation;

(e) In current business scenario, several organisations concentrate their operational activities in one major operational hub; these organisations are at a higher BCP risk than the ones with operations in several hubs if they are geared to support each other in a moment of crisis.

Common examples of critical disruption in business process are:

- Raw material in process being lost or spoilt due to one of the processes being disrupted due to system, people or process failure, i.e. operational reasons;
- Contractual financial obligations such as repayment of loans, or vendor payments, salaries,
- Payment of taxes;
- Inability to disbursement of loans that causes customer dissatisfaction;
- In an ITES company, the principal (i.e. the main organisation that hires an ITES company) may have complete disruption of their services to their customers in case of failure in the ITES service provider's services;
- In fact in highly developed economies, the risk of customer's dissatisfaction, the highest form of which takes class lawsuits, is high in case of large scale business process failures;

Hence a Business Continuity Plan ("BCP") is required to be adopted.

BCP is now an evolved, objective framework and involves a large section of the organisation, including the operational risk management framework.

Now we shall discuss the key constituents of a BCP one by one.

## 9.1 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.

All departments of the organisation are required to list all their processes (including sub-processes) and grade them in order of priority. This is a difficult task, since most organisations like to believe all their processes are critical; but in reality, with limited resources in a disruption situation, the best that can be done are the most important activities; hence parameters of prioritisation are to be fixed; these could be as follows:

**Impact:** Critical, Important, Routine; the classification into each of these could be done on the basis of some objective parameters such as whether it affects regulatory violations, or can cause financial loss, or loss to lives or property; for instance, in a lending institution, a process that does

due diligence on customer identity and address (KYC checks) may be very critical and indispensable without which a sanction cannot happen since it is a regulatory risk; or a case where a secondary check on the sanction is dispensed with in given sanctions, where a financial loss can happen. These are carefully evaluated parameters that the management has to consider and take a decision on what processes to keep running in disruption situation and what to stop.

Also, what is considered as important but not critical for a department, may be critical for another department; for instance, treasury may feel making payment to external lenders as most critical while making payments to operations or finance departments for making disbursements to loan customers or vendors as not critical; however, the operations or finance departments may be severely inconvenienced if the money to service their obligations is not made available in a disruptive situation. Thus, a categorisation of Impact is done with collaborative approach of all departments that a process impacts.

In summary,

A BIA must ideally 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).

## 9.2 Functional Recovery Plan (FRP)

Here, 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;

For example: an operations intensive company may decide to use an alternative, smaller hub to process all key transactions; a customer service centric company may have an alternative customer service centre if the main one is down due to disruption;

Roles identified as key in running a FRP in execution, are required to have formal backups in case they cannot move locations or carry out the required operation from their base location or site. Companies resort to several tech savvy solutions such as work-from-home facilitated by remote logging in to systems, webinars, video conference, telephonic conference bridges, and use of secured-data-storage such as cloud.

An FRP has to consider the key elements involved in the alternate plan; whether it is movement of goods, or movements of information, or paper-based files; any plan is successful only if the practical constraints of the Plan are clearly elucidated, thereby objectively listing the conditions in which the FRP would function, and when it cannot.

A FRP is a very detailed document that would list the following at a minimum:

- Site in which the process would be carried out (called the Alternate Site), the role/s who would carry it out, the back-up to the roles if the primary one is unable to perform in disruptive circumstances; the minimum resources such as telephones, internet, printers or access to intranet, internal systems etc. as an indicative list.
- This needs to be documented and circulated, and reiterated to each employee and/or service provider who is involved in the FRP. Operational risk managers are required to oversee whether the framework is composite and integrated sufficiently to ensure the framework is real and practically implementable, not a drawing board theory document.
- The names and contacts of all key members in each process need to be listed and available to all others involved in FRP , in a domain other than the primary office domain so that the communication lines are not disrupted when it is required to invoke a FRP. This communication plan is commonly known as a Call Tree.
- The FRP is useful and practical only if tested regularly, maybe at predefined periodic intervals, as well as unannounced situations to mirror a real disruption. This is the critical stage where theory is tested in practice, and the ensuring failures and successes have to be documented to improve the Plan in future. An organisation has to ensure this is a recurring process to be able to give confidence to investors/promoters/owners, management, and customers that the FRP is practical and genuinely addresses the critical tasks.

In an effective BCP, the concern on outsourced activities need to be addressed too; in current scenario where several organisations use outsourced vendors, the vendor's BCP has to reviewed periodically to ensure the whole process works. In fact the choice of a vendor should ideally cover the BCP aspects too.

An auditor / consultant working on internal controls or an operational risk manager needs to review the efficacy of the organisation's BCP, in context of the services it provides. For example, even a small scale audit firm may need a BCP to ensure its services to the clients are not disrupted. In

large complex manufacturing organisations the BCP needs to be a major framework that co-ordinates the interrelationships of various business units, locations, business processes etc.

It is highly advisable to have a formal decision making committee of management functions to oversee the entire chain of activities from formation of BCP policy, Business Impact Analysis, Functional Recovery Plan and to review Test results.

## 10. OUTSOURCING RISK

There are several specific aspects that need to be looked into 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.

It is advisable for an operational risk manager to have an oversight of different department's adherence to the management of their respective outsourcing risks, and have it covered in their respective RCMs.

## 11. CYBER RISK AND INFORMATION SECURITY CONTROLS

Cyber risk is a vast and complex technical subject by itself; however we shall outline some of the key points that is relevant from an operational risk perspective. Information Security and Cyber risk by themselves are studied under specialised courses as CISA by those aspiring for professional certification in information security management domain.

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.

This broadly covers scenarios like this, for example:

- Confidential data of customers' demographics, personal financials, collaterals, bank account data etc. stolen from a lending institution's database by an external entity having made unauthorised access to the system of the organisation; this can cause customer disputes, class lawsuits, breach of confidentiality law, and loss of business.
- Trade secret software programs, like acquisition scorecards or manufacturing formulae, stolen from the systems of an institution and causing significant loss of competitive business; this is also covered in a broad term called Intellectual Property risk. This is a result of corporate espionage, or simply, an employee quitting a job with a view to take up a career in a competitor organisation may take away account data or other information that may help his unlawful benefits.
- Malevolent attack on system of an institution that can lead to complete or partial data loss, of customers, accounts and of past financial transactions; this can lead to serious regulatory violation, financial reporting issues, and /or financial losses;
- Ransomware can lock or encrypt the entire data on an individual or entity's computer systems and thereby completely ruin the business; the retrieval of such data may not be possible or would come at significantly high cost and at compromised quality; ransomware originators demand money, often through illegal channels for release of such data.
- The financial transactions that an organisation performs outside its own network can also be compromised due to cyber risk; organisations involved in e-commerce where a large chain of activities is performed on internet, and, since multiple parties are connected with each other and a compromise on one entity's network may lead to issues for anyone in the entire chain. A lot of customer data, credit card numbers, bank account numbers, details of the goods and services being transacted, all are being transmitted over the internet. An increasingly digitized business environment does put all parties involved in such transactions, at a higher risk.
- An entity intending to create fraudulent transactions and benefit financially may send emails to individuals or organisations, pretending to be from an organisation that the other one is already engaged with; this happens on an email that looks identical to the ones from the actual organisation, and it may ask for money to be transferred to a bank account.
- Phishing is a very common fraud technique, whereby there is a link sent to the targeted victim and upon clicking it, the intruder gets access to the victim's computer system/s; and, in cases, if asked for personal data of credit card, passwords etc. on such dubious links, the victim may also incur immediate financial losses because the link is a malevolent one and the perpetuator of the fraud gets access to credit card details or bank account detail of the victim.

*Mitigation of such risks is done through the following measures:*

An organisation, depending on its nature of business, complexity of business operations, and the kind of system network/s used, need to take adequate measures on cyber risk.

The key aspects in consideration are:

- Identification of risk areas: whether it is own or outsourced network, internet, individual computers, mobile devices etc. Prioritization of resources and effort can be managed accordingly.
- Adequately restricting access to systems is the common way to prevent cyber risk; this is done by password protection at various levels, from common user to administrator level.
- Encryption solutions on individual computers is also done in a manner that if lost, the unauthorised entity cannot download the data into an external storage device.
- There are several technology solutions that create an adequate firewall of the organisation's systems to protect them from hacking from outside.
- A regular vulnerability testing of the firewall and periodic review to upgrade it is one of the main tasks of the information security manager. Detection of a test-attack is very important part of the preventive mechanism; an attacker may attempt to cause a minor violation to test the organisation's network security before causing a major incident.
- A response strategy to a cyber-attack incident is also important as part of risk management. The measures to prevent or mitigate customer disputes, legal indemnities, assess and minimize the financial impact of a cyber-attack, and governance over decision making and investments to restore the system functionalities to its secure state, are all important considerations. The root cause of these incidents and the impact have to be adequately documented.

Examples in recent times are the ransomware attacks (for example WannaCry Ransomware) that led to several reputed organisations both in public and private services to be adversely impacted.

It is highly advisable to maintain adequate documentation on technical standards followed and aspired to be followed by the organisation, and that is driven by policy and senior management governance. For example, the RBI has issued information security and IT governance related circular that enables the organisations regulated by it, to follow adequate security measures and to ensure that the highest level of attention from the Board level is also accorded to information security.

Different sets of employees depending on whether they are users / custodians of data or are part of governance of the systems network need different kind of awareness and training to maintain information security. It is recommended that the senior management is guided by a professional Chief Information Security Officer (or a role that carries these responsibilities) in carrying out these responsibilities.

It is recommended to have an internal audit scoped for technology and information security by teams that have technology assessment competence.

Most organisations do have a Code of Conduct that has a significant section on confidentiality and protection of data, broadly covering information security aspects. This is further enabled by mandatory training by the employees depending on their roles and exposure.

## 12. OPERATIONAL LOSS DATA MANAGEMENT

While an effective operational risk management framework drives to bring preventive measures as elucidated above, there is every possibility that some loss events do occur in an organisation. It is imperative to identify the losses as and when they happen, quantify them (both in financial and non-financial terms), and assess their short term and long term impact. This is normally followed by an assessment of the controls of the specific process / sub-process in which the event occurred.

Basel II has already indicated a comprehensive list of operational loss event categories. While these were introduced for financial organisations, they are, with minor customisations, equally valid for all organisations measuring operational loss data with an objective methodology. A slightly modified description from the one in Basel II norms is presented in table below:

Identification of an operational loss event is the primary challenge an organisation faces, because a loss may occur and its discovery may takes place after a long time. Some very common scenarios are elaborated in the description of three levels of activity examples in Basel norms itself. A slightly modified extract is thus:

| *Event type Category (Level 1)* | *Description* | *Categories (Level 2)* | *Activity examples (Level 3)* |
|---|---|---|---|
| Internal fraud | Losses due to intentional fraud, misappropriation of property, violate law or company rules, by an internal party/in collusion with an internal party | Unauthorised activity | Unauthorised transaction with monetary loss;<br>Transaction not reported intentionally;<br>Mismarking of position intentionally. |
| | | Theft and Fraud | Fraud/Credit fraud, theft/extortion/embezzlement/robbery,<br>Misappropriation of assets, malicious destruction of assets, forgery, smuggling, account impersonation, |

| | | | |
|---|---|---|---|
| | | | tax non-compliance intentional; bribes/kickbacks, insider trading (not on company's account) |
| External fraud | Losses due to an intentional fraud, misappropriation, violation of law or company rules by an external party | Theft and Fraud | Theft/robbery<br>Forgery |
| | | Systems Security | Hacking damage<br>Theft of information with financial loss |
| Employment Practices and Workplace Safety | Losses due to activity inconsistent with employment, health and physical safety of employees, claims, or from discrimination events. | Employee relations | Compensation, benefit, termination issues<br>Organized labour activity |
| | | Safe environment | General liabilities (slip and fall etc.)<br>Employee health and safety rules events |
| | | Diversity and discrimination | Losses or issues arising out of diversity and discrimination |
| Clients, Products, and Business Practices | | Suitability, disclosure and fiduciary | Fiduciary breaches/guideline violations<br>Suitability/disclosure issues (KYC etc.)<br>Breach of privacy<br>Aggressive sales<br>Account churning<br>Misuse of confidential information<br>Lender liability |
| | | Improper Business and market practices | Antitrust<br>Improper trade / market practices<br>Market manipulation<br>Insider trading on firm's account |

| | | | |
|---|---|---|---|
| | | | Unlicensed activity<br>Money laundering |
| | | Product Flaws | Product defects (unauthorised etc.)<br>Model errors |
| | | Selection, Sponsorship, and Exposure | Failure to investigate client as per guidelines<br>Exceeding client exposure limits |
| | | Advisory activities | Disputes over performance of advisory activities |
| Damage to physical assets | Losses from physical assets damage either intentional or from natural disaster | Disasters and other events | Natural disaster losses, human losses from external events like terrorism |
| Business Disruption and System Failures | Losses arising from disruption of business or system failures | Systems | Hardware, software, telecommunications, utility disruptions/outage |
| Execution, Delivery and Process Management | Losses from failed transactions processing or process management | Transaction capture, execution, and maintenance | Miscommunication, Data entry, maintenance or loading error,<br>Missed deadline/ responsibility<br>Model/ system mis-operation<br>Accounting error<br>Delivery failure<br>Collateral management failure<br>Reference data maintenance,<br>Other task mis-performance |
| | | Monitoring and reporting | Failed mandatory reporting obligation<br>Inaccurate external report (loss incurred) |
| | | Customer intake and documentation | Client permissions/disclaimers missing; Legal documents missing/incomplete |
| | | Customer/client account management | Unapproved access given to accounts<br>Incorrect client records leading to loss<br>Negligent loss or damage of client assets |
| | | Trade counterparties | Non-client counterparty mis-performance / disputes |

| | | | |
|---|---|---|---|
| | | | |
| | | Vendors and suppliers | Outsourcing,<br>Vendor disputes |

The process for identification and reporting of operational losses are recommended to be laid down in an internal process note approved by the competent authorities in the organisation, or the ORMC itself.

## 12.1 Identification

The organisation may identify an operational loss event by any or more of the following triggers:

- 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

As and when an event that falls under the above scenarios occurs, the following steps are recommended:

## 12.2 Quantification

The quantification of the event is to be done next;

It may have a direct financial loss impact (like excess payment to external party, or compensation to customers etc.) or not having an immediate direct financial impact (like a few instances of KYC due diligence failures, or a process failures not leading to compensation to customers etc.)

From a reporting perspective, it is necessary to enumerate all Operational risk events, since these are the failures in which the organisation needs to take some remedial action.

Only in those cases where direct financial loss is involved, an operational loss is booked.

While RBI, following the direction of Basel II norms, has detailed instructions applicable to banks on the handling of loss data and its impact on capital computation, other industries do not have such guidelines currently.

It is advisable to have an Operational Loss GL in the organisation where all financial loss instances can be booked. In case, a different GL has already taken in the loss by routine course of business, or inadvertently due to the loss not having been discovered earlier, it is advisable to book a credit in the original GL and the debit in the Operational Loss GL.

For example, an excess full and final settlement payment to an exiting employee, would have been booked under Salaries by normal course. But once the error is discovered, it is advisable to book it in a separate Operational Loss GL and credit the Salaries GL so that the financial reporting is appropriate. Further in a lending institution, if a loan is closed erroneously, the entire principal and other heads' outstanding is a real financial loss to the organisation; these need to be booked in the operational loss GL and the respective other GLs be credited with the amounts.

Some organisations book Fraud Losses in the Operational Loss GL (since fraud losses are also part of operational losses as per categorisation elaborated above), but some organisations maintain a separate GL for Fraud losses, so as to enable efficient reconciliation with other reporting requirements like Fraud reports to regulators and to track action taken against them.

In instances where a recovery of the loss is expected, the management is expected to track the event till its logical end by recovering whatever is possible thereby reducing the net operational loss.

## 12.3 Reporting

A report to the ORMC (and to the Board / Board Committee as may be necessary by regulation or by company policy) is recommended to include the following:

| *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* |
|---|---|---|---|---|---|---|---|
| | | | | | | | |

## 12.4 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.

The most important corrective activity after an event is to review the scenario for further happening of such risks. If that is possible then, the organisation may even set aside a financial provision for the same for estimated future events.

# 13. 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. It is now available almost instantaneously, creating possibilities for near real-time analysis.

The convergence of the secular trends of exponential growth in data volume, concomitant geometric increase in computational capacity and the resultant development of sophisticated algorithms is fuelling rapid technology advances and business disruptions. The field of risk management is not immune to these changes and we are witnessing significant changes in the discipline.

## 13.1 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. In contrast, a machine learning program dynamically responds to change in data / situation by changing the rules that govern the behaviour.

Machine learning, meanwhile, 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. In that sense, the algorithm "learns" from new data inputs and gets better over time.

Techniques such as regression, support vector machines, and k-means clustering have been in use for decades. Others, while developed previously, have become viable only now that vast quantities of data and unprecedented processing power are available. Deep Learning and Reinforcement learning are good example of newly developed machine learning techniques.

At the most basic level, machine learning techniques can be divided into two primary groups:

- Supervised Learning
- Unsupervised Learning

Supervised Learning refers to the statistical analysis that aims to map the behaviour of a certain variable on the basis of some other variables. The principal aim of these methods is to fit a model that relates the set of independent variables to the dependent variable. The model in turn is largely used for future prediction of better understanding of the relationship between the independent and dependent variables. Bulk of the machine learning methods such as linear regression, logistic regression, boosting, and support vector machines operate in the supervised learning domain.

Unsupervised Learning, as the name suggests, refers to statistical methods that aim to delve into the challenging realm of data that has no dependent or response variable i.e. there is no variable that supervises the behaviour of the algorithm. The primary aim of this kind of analysis is to understand the relationships between the variables or between the observations. One statistical learning tool that we may use in this setting is cluster analysis, or clustering.

Machine Learning methods can also be categorized on the basis of the nature of the variables handled. Regression methods primarily deal with variables that are quantitative in nature e.g. a person's age, height, or income, the value of a house, and the price of a stock. In contrast, Classification methods deal with qualitative variables i.e. variables that take on values in one of K

different classes, or categories. Examples of qualitative class variables include a person's gender (male or female), the brand of product purchased (brand A, B, or C), whether a person defaults on a debt (yes or no), or a cancer diagnosis (Acute Myelogenous Leukemia, Acute Lymphoblastic Leukemia, or No Leukemia).

## 13.2 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. Banks are expected to conduct regular and comprehensive bottom-up stress tests for a number of scenarios across all asset classes. Big Data technologies present fresh opportunities to address these challenges.

Vast, comprehensive and near real-time data has the potential to improve monitoring of risk, risk coverage, and the stability and predictive power of risk models. In a number of key domains – particularly operational and compliance risk – Big Data technologies will allow the development of models that will support every day.

Post-crisis, financial institutions are now expected to have thorough knowledge of their clients. Increasingly, forward-thinking banks harness Big Data to develop more robust predictive indicators in the credit risk domain. New data sources - including social media and marketing databases – are being used to gain greater visibility into customer behaviour. This information can augment traditional data sources including financial, socio-demographic, internal payments and externals loss data.

Together, the data sets can produce a highly robust, comprehensive risk indicator. Rather than waiting to review loan clients' financial reports to discover loan-servicing problems, firms can utilise Big Data technologies to detect early warning signals by observing clients' on-going behaviours, and act in time.

The high cost of money laundering cases has prompted banks to seek new ways to address the severe limitations in current anti-money laundering risk management. Traditional approaches to anti money laundering remain dependent on rule-based, descriptive analytics to process structured data. This system clearly has limitations - without automated algorithms, detecting information within the wealth of data requires laborious keyword searches and manual sifting through reports.

Big Data analytics can improve the existing processes in AML operations. Its approaches allow for the advanced statistical analysis of structured data, and advanced visualisation and statistical text mining of unstructured data. These approaches can provide a means to quickly draw out hidden links between transactions and accounts, and uncover suspicious transaction patterns. Advanced analytics can generate real-time actionable insights, stopping potential money laundering in its tracks, whilst still allowing fund transfers for crucial economic and human aid to troubled regions. Big data technologies can identify incidents, help draw a wider picture, and allow a bank to raise the alarm before it's too late.

Business Analytics is heavily used in Liquidity Forecasting, Asset Liability Management, Operational & Compliance Risk as well as in Credit Risk model.

## 13.3 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 works by studying how human brain thinks and how humans learn, decide and work while trying to solve a problem, and then the outcomes of this study is used in developing intelligent software and systems. It has been dominant in many fields such as:

Gaming – It plays a crucial role in strategic games such as chess, poker etc.

Natural Language Processing – It is possible to interact with the computer that understands natural language spoken by humans.

Expert Systems - There are some applications which integrate machine, software, and special information to impart reasoning and advising. They provide explanation and advice to the users.

Vision Systems - These systems understand, interpret, and comprehend visual input on the computer.

For example,

- Doctors use clinical expert system to diagnose the patient.
- Police use computer software that can recognize the face of criminal with the stored portrait made by forensic artist.

AI is also used in Speech Recognition, Handwriting Recognition, and Intelligent Robots etc.

Artificial Intelligence is dependent on large amounts of data. So proper big data architecture needs to be set up for AI that involves architecture like Hadoop clusters, Spark Clusters etc. So that the processing of the data is faster and smooth.

## 13.4 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.

This technology is perceived by many commentators to have significant potential to disrupt payment, clearing, settlement and related activities. DLT is expected to radically redefine the payment and settlement landscape and is expected to produce the following 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

## 14. 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, for instance. Depending on the cover available and opted for, other losses due to terrorist attacks, natural disasters etc. can also be covered. Cash transit insurance and fidelity insurance are off quoted examples.

These three examples are based on loss categories of Damage to Assets, External fraud and Internal fraud. 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.