Compliance/ Performance Audit
Detailed Planning
Session-03

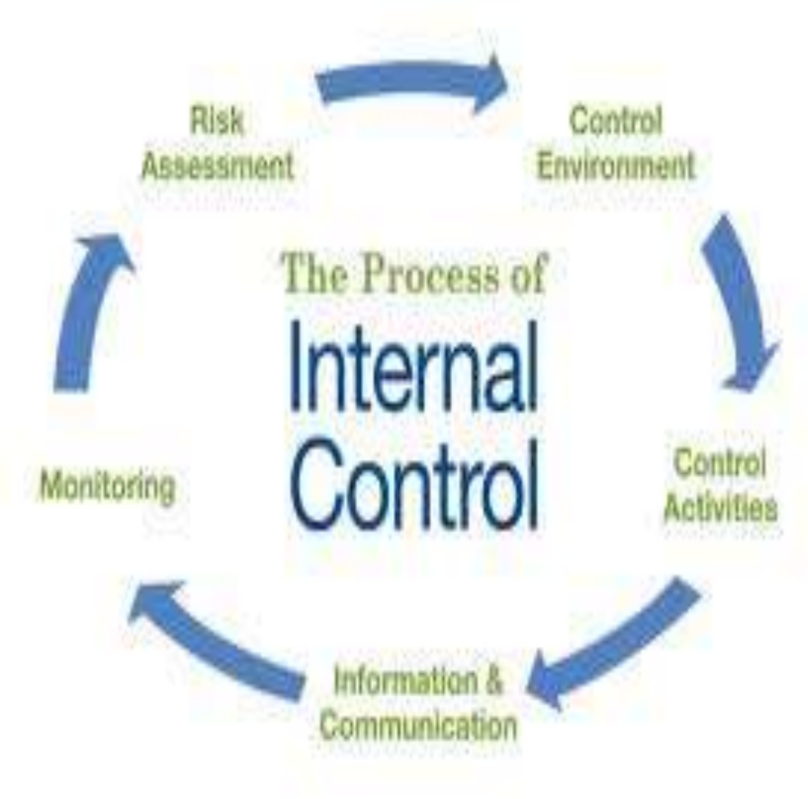
November - - 2018

Compliance/Performance Audit-Detailed Planning

- Understand the Controls
- Review the objectives, how the management measures them
- Identify the risks/ review risk registers
- Discuss the risk appetite/ boundaries set by the management
- Review the risk mitigation strategy

Internal Controls

- Internal Control is a process, effected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.



Source: Internal Control- integrated Framework, March 2013

Internal Controls

- As per the definition certain fundamental concepts are reflected:
  - Geared to the achievement of objectives in one or more categories- operations, reporting, and compliance
  - A process consisting of ongoing tasks and activities- a means to an end, not an end in itself

- The auditor needs to analyze whether the internal control systems providing reasonable assurance that:-
  - The business is planned and conducted in an orderly and prudent manner
  - Transactions and commitments entered into have proper authority
  - Management is able to safeguard the assets and control the liabilities of the business

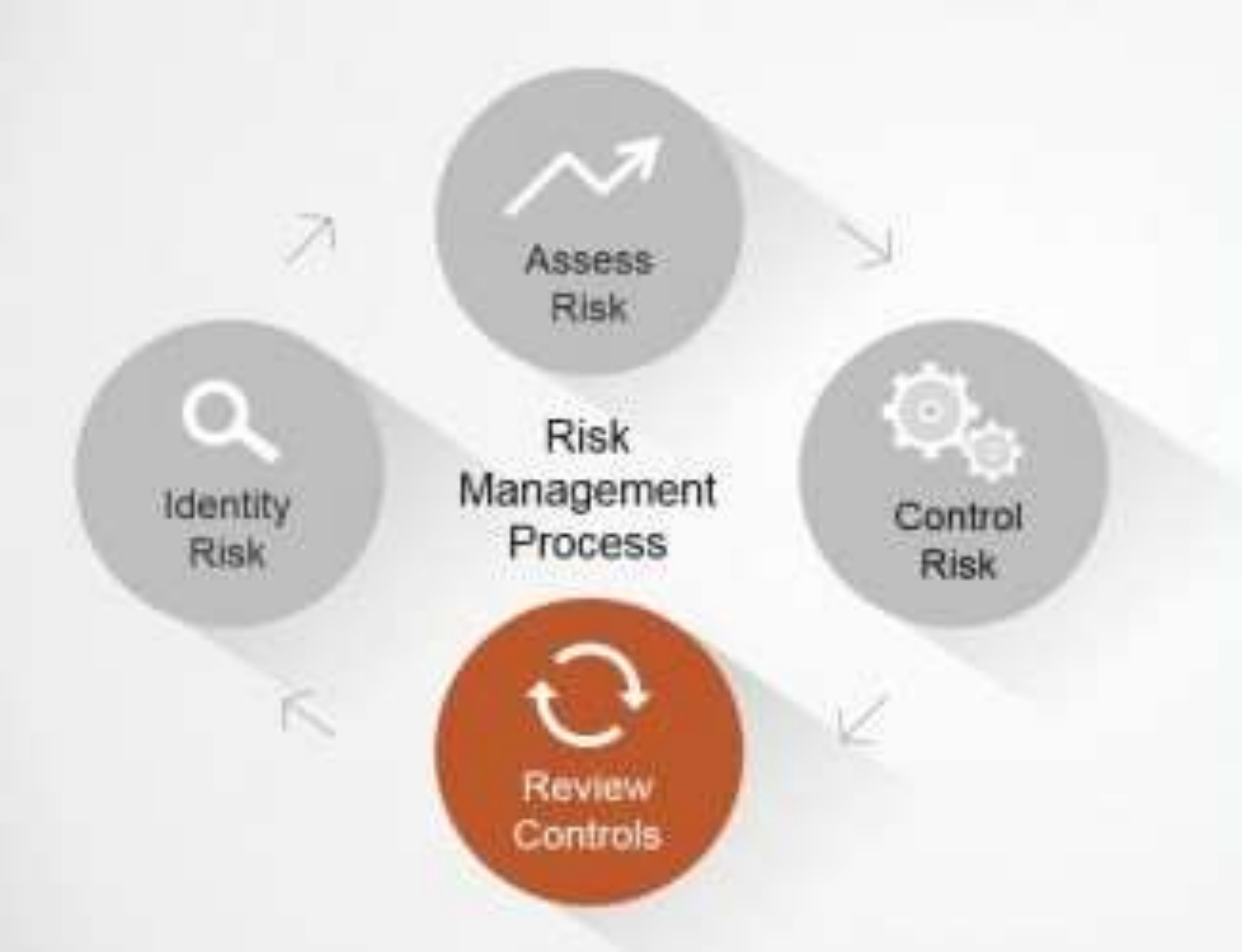
- There are measures to minimize the risk of loss from irregularities, fraud and error and to identify and rectify them when they occur
- The accounting and other records provide complete, accurate and timely information
- The risks are monitored and controlled on a regular and timely basis

Review the objectives

- Every organization sets for itself certain goals to achieve the overall. The auditor reviews these objectives to ascertain the performance of the entity
- The review of management objectives gives an insight into the overall working of the organization, how progressive it is,
  - Have the organization developed the Key Performance Indicators, Key Control Indicators, Key Risk Indicators

Contd..

- The management objectives help define the audit objectives broadly define the extent of audit examination and the approach to be adopted by the auditors.


Assess Risk
Control Risk
Review Controls
Identity Risk
Risk Management Process

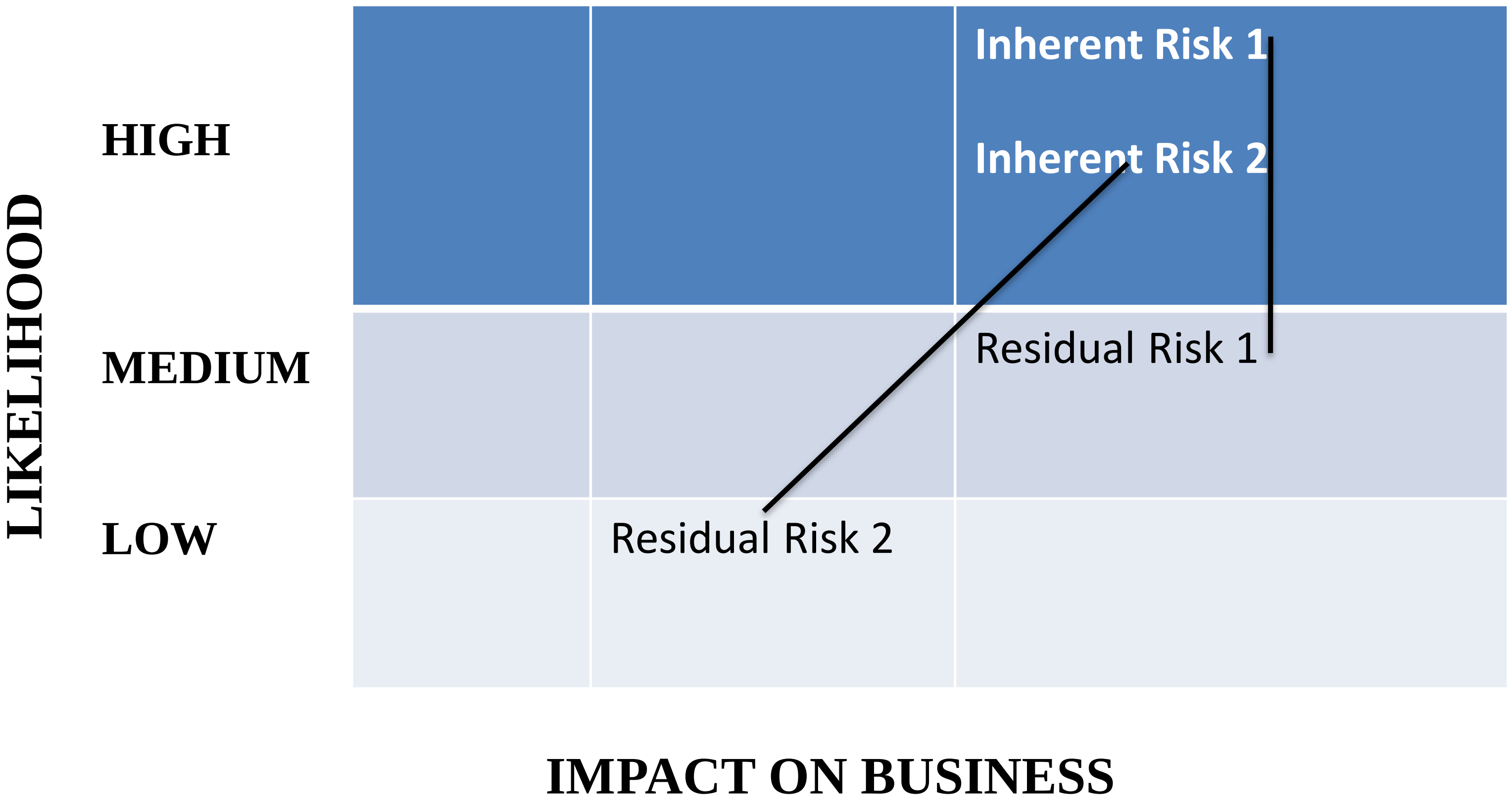
Risk Assessment

- Risk assessment is the identification and analysis of relevant risks to the achievement of objectives.
- Management needs to identify these risks in order to know the areas in which the internal control structure needs to be particularly strong.
- Conversely, risk assessment may indicate areas where risks are low, and therefore where the entity does not need to design elaborate internal control structures

Risk Assessment

- Proper risk assessment assists public sector entities in making informed decisions about the level of risk they are prepared to take and implementing the necessary controls in pursuit of the entities' objectives.
- Inherent risk is the pure risk, the risk before the controls or mitigation.
- The bigger the difference between the inherent & residual scores the more important the control (or mitigation procedure)

Risk Assessment



LIKELIHOOD

HIGH

MEDIUM

LOW

Inherent Risk 1

Inherent Risk 2

Residual Risk 1

Residual Risk 2

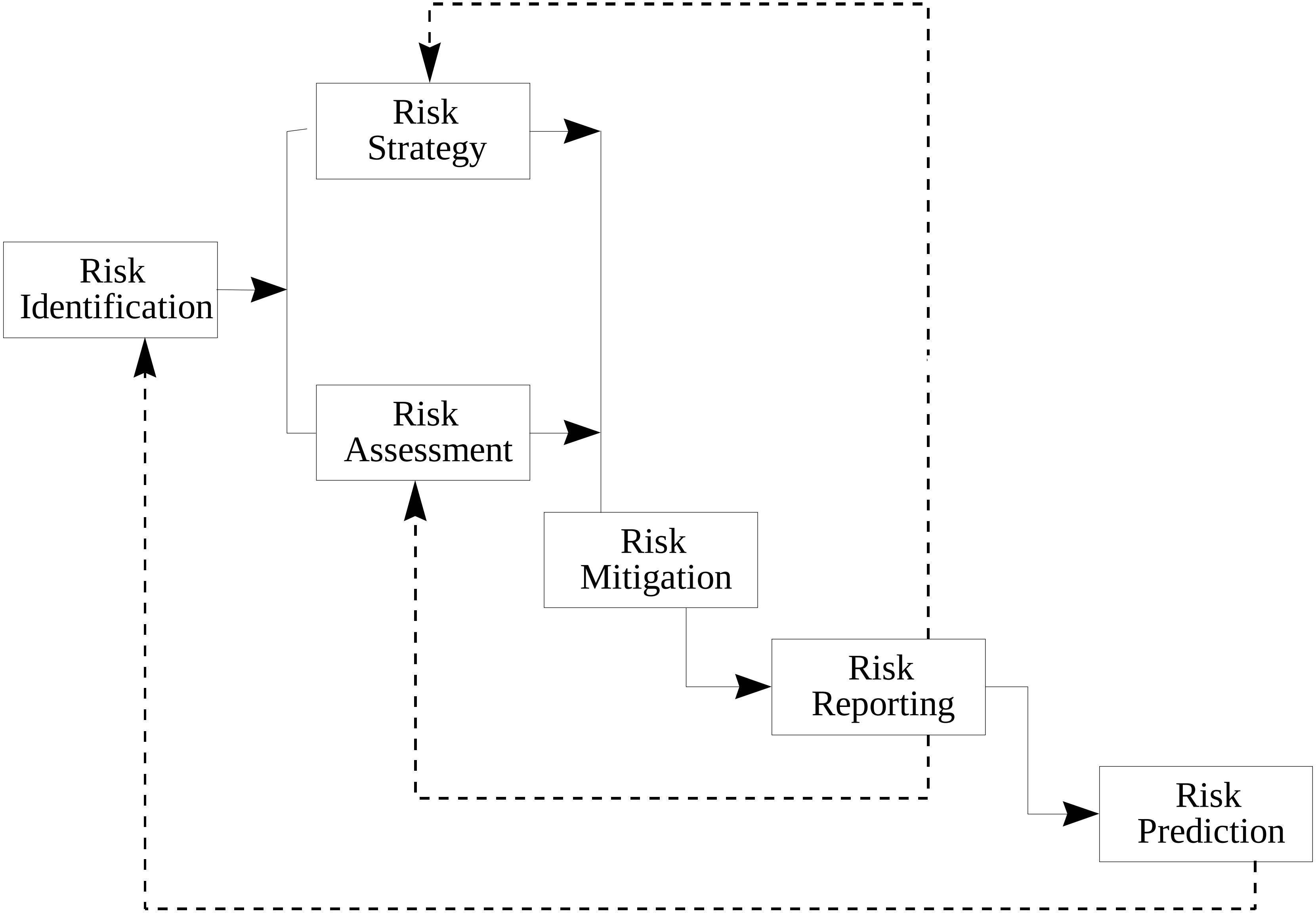
IMPACT ON BUSINESS

RISK RANKING: Probability Impact Matrix

PROBABILITY

	HIGH	MODERATE	LOW
HIGH	9	7	5
MODERATE	8	6	4
LOW	3	2	1

IMPACT



RISK ANALYSIS ACTIVITY MODEL

Risk Registers

- The risk register starts with a risk management plan.
- The risk register or risk log becomes essential as it records identified risks, their severity, and the actions steps to be taken. It can be a simple document, spreadsheet, or a database system, but the most effective format is a table.
- A table presents a great deal of information in just a few pages.
- Managers should view the risk register as a management tool through a review and updating process that identifies, assesses, and manages risks down to acceptable levels.

Risk Registers

- The register provides a framework in which problems that threaten the delivery of the anticipated benefits are captured.
- Actions are then taken to reduce the probability and the potential impact of specific risks.

Risk register

Audit assignment identified	Observed risks Strategy Governance Financial etc..	Existing operational &/or financial controls	Controls effectiveness Strong Moderate Weak	Probability & Occurrence High Moderate Low	Impact High Moderate Low

Risk Register

		RISK ANALYSIS					
TYPE OF RISK		*Likelihood it will occur*			*Probability of Adverse Impact*		
		High	Medium	Low	High	Medium	Low
Strategic Risks	*Examples*						
Political	Negative media coverage						
	Public Support						
Cultural	Inability to adapt to change						
	Leadership to achieve objectives						
External	Environment-related event						
	Economic/social changes						

Operational Risks

		Likelihood it will occur			***Probability of impact***		
Liability	Actions fail to consider the law	H	M	L	H	M	L
Process	Inefficient processes						
	Insufficient capacity						
	Process takes too long						
Integrity	Fraud, illegal acts						
	Loss of reputation						
Human Resources	Loss of corporate memory						
	Resources not matched to workload						
Info. Processing	Lack of timely, reliable information						
	Lack of modern technology						
Financial	Third party identification costs						
	Court settlements, awards						

Project Risks ***Likelihood*** ***Probability***

Technical	Requirements change	H	M	L	H	M	L
	Requirements are difficult to meet						
Develop/ Implement	Process lacks structure, formality						
Management	Inadequate business case						
	Project decision not based on risk						

Risk appetite and tolerance

- Risk appetite can be defined as ‘the amount and type of risk that an organization is willing to take in order to meet their strategic objectives.
  - Organizations will have different risk appetites depending on their sector, culture and objectives.
- Risk appetite and tolerance need to be high on an entity management's agenda and is a core consideration of an enterprise risk management approach

Risk appetite and tolerance

- Risk appetite is a broad based description of the desired level of risk that an entity will take in pursuit of its mission
- Risk tolerance reflects the acceptable variation in outcomes relate to specific performance measures linked to objectives the entity seeks to achieve.
- The auditor while planning an audit must have an understanding of the risk appetite /tolerance of the entity

Maturity Rating

INTIAL:

- There is no or minimal awareness of the importance of risk management and there are no processes in place across the entity.
- Risk management is usually left to the individual and performed on an adhoc basis. Risk management is more reactive than proactive.

INCONSISTENT:

- There is organizational awareness of the importance of risk management.
- There are some formal processes in place for a few risks.
- There is limited standardization of risk management processes and risk management is conducted inconsistently across each risk and across each business unit.

Maturity Rating

CONSISTENT-DESIGNED:

- An enterprise risk management framework exists covering all major risks.
- Standardized risk management principles are defined and documented, basic training conducted. Consistent risk management processes with communication and accountability exist throughout the business but not all processes have been fully implemented.

Maturity Rating

CONSISTENT- IMPLEMENTED:

- Enterprise risk management is fully implemented across the business, consistently applied and used in decision making and day to day management. Risk management processes are measured, evaluated and fed back into continuous improvement.
- Principles and policies are implemented and aggregated reports are prepared and reported to those charged with governance. Risk management is proactive. Key Risk indicators are collected and monitored consistently.

Maturity Rating

OPTIMIZED:

- Risk management is fully addressed and embedded into day to day management.
- Sophisticated and advanced risk management processes are used for all major risk types.
- Risk management is used as a key value driver supporting decision making and pursuit of opportunities.
- Risks, including emerging risks are proactively identified and monitored through key risk indicators and predictive risk analytics

Organizational culture

- **Risk Averse**
  - Management tends to stick with what they know
  - The organization is very reactive
  - Inward looking
  - Strategies do not change very often
  - Mistakes are personalized

- **Risk Embracing**
  - It has a ‘Can do’ culture
  - Strategies and policies change regularly to reflect changing circumstances
  - Exploit opportunities & empowers people
  - Making a mistake is acceptable
  - Outward looking

Risk Culture

- Risk culture consists of the norms and traditions of behavior of individuals and of groups within an organization that determine the way in which they identify, understand and confront the risk faced by the organization .
- The organizational culture provides an insight into the overall profile of the organization and its level of preparedness

Risk Response

- Risk response is the process of developing strategic options, and determining actions, to enhance opportunities and reduce threats to the project's objectives.
- The relevant person in-charge is assigned to take responsibility for each risk response. This process ensures that each risk requiring a response has an owner monitoring the responses.
- The auditor need to examine whether responses to all identified risks have been developed/ operational

RISK
MITIGATION

Risk Exposures

Risk Exposures	
Tolerate	Accept the risk
Transfer	Let someone else manage the risk on your behalf
Terminate	Eliminate the risk
Treat	Take cost- effective in-house actions to reduce the risks

Audit Scope

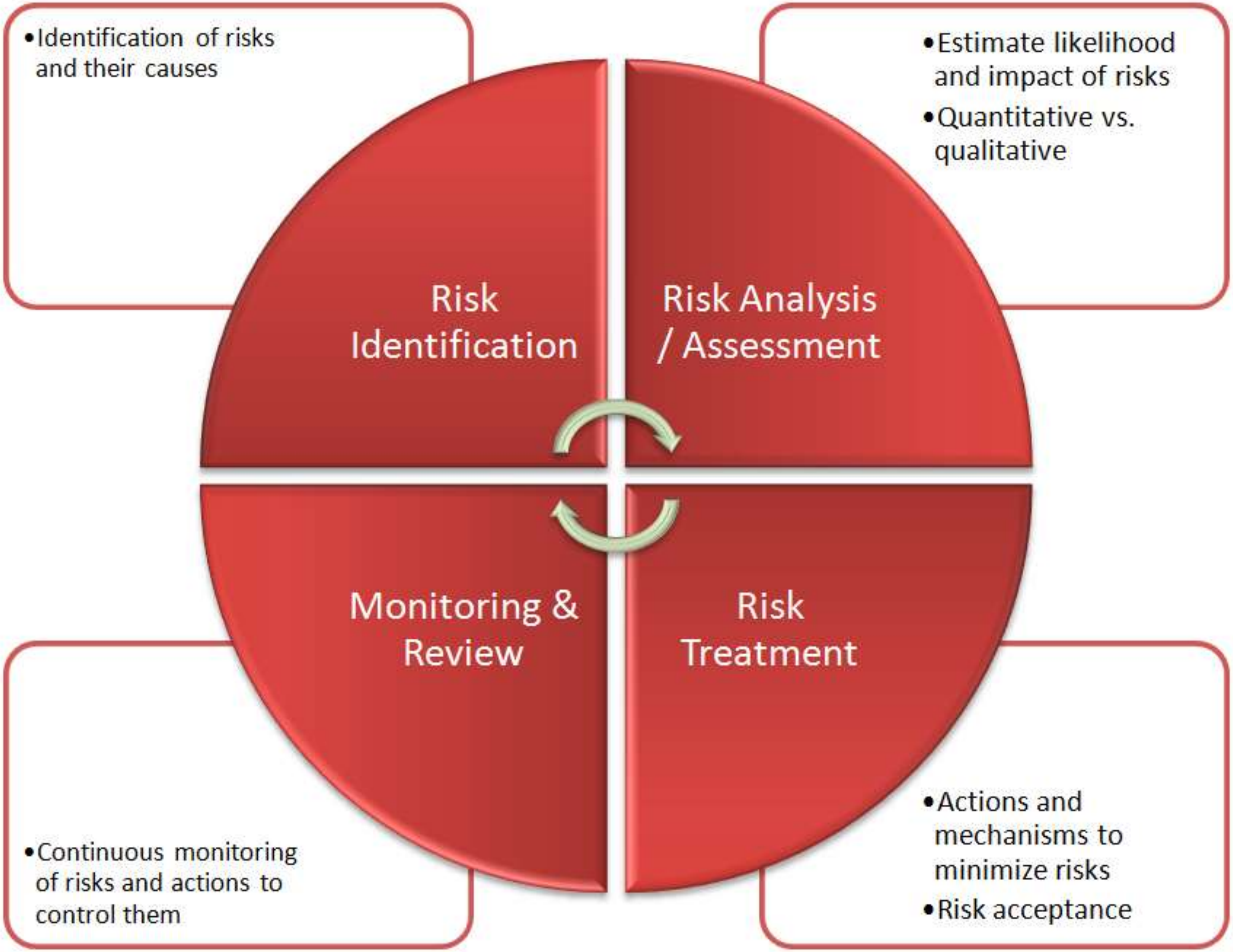
- Extent of audit coverage in terms of time period, nature of the organization or any aspect which results in a meaningful audit activity
- Audit scope largely depend on audit objectives, state of record- keeping, data management of audited body
- Audit scope is determined in the light of risk assessment, control evaluation, entity profile, past audit findings

Contd..

- The scope of an audit is determined by answering the following questions:
  - *What? What specific questions or hypotheses are to be examined?*
  - What kind of study seems to be appropriate?
  - *Who? Who are the key players involved and the auditee(s)?*
  - *Where? Are there limitations in the number of locations to be* covered?
  - *When? Are there limitations on the time frame to be covered?*

THANK YOU

Risk Identification & Mitigation



- Identification of risks and their causes

Risk Identification

Risk Analysis / Assessment

- Estimate likelihood and impact of risks
- Quantitative vs. qualitative

Risk Treatment

- Actions and mechanisms to minimize risks
- Risk acceptance

Monitoring & Review

- Continuous monitoring of risks and actions to control them

Risk identification

- Risk identification determines which risk might affect the project and documents their characteristics
- Risk identification is an iterative process because new risks may become known as the entity/ project progresses

Risk identification

- Risk identification activity must include project manager, risk management team (if assigned), subject matter experts from outside the project team, customers, end users, stakeholders and risk management experts

- Determining what risks or hazards exist or are anticipated, their characteristics, remoteness in time, duration, period, and possible outcomes

Risk identification

- The risk identification process usually leads to the Qualitative Risk Analysis process. Alternatively, it can lead directly to the Quantitative Risk Analysis process when conducted by an expert risk manager

Risk identification: Tools& Techniques, and outputs

INPUTS

- Enterprise environmental factors
- Organizational process assets
- Project scope statement
- Risk management plan
- Project management plan

Tools & Techniques

- Documentation reviews
- Information gathering techniques
- Checklist analysis
- Assumptions analysis
- Diagramming techniques

OUTPUTS

- Risk register

Risk identification: Inputs

- Enterprise environmental factors
  - Published information including commercial data bases, academic studies, benchmarking, or other industry studies, may also be useful in identifying risks

Risk identification: Inputs

- Organizational process assets
  - Information on prior activity/projects may be available from previous activity/ project files, including actual data and lessons learned

Risk identification: Tools & Techniques

- Scope statement
  - Activity assumptions are found in the scope statement. Uncertainty in activity assumptions should be evaluated as potential causes of risk

Risk identification: Tools & Techniques

- Risk management plan
  - Key inputs from the risk management plan to the risk identification process are the assignments of roles and responsibilities, provision for risk management activities in the budget and schedule, and categories of risk which are sometimes expressed in an RBS

Risk identification: Outputs

- Organizational management plan
  - The risk identification process also requires an understanding of the schedule, cost and quality management plans found in the organizational management plan. Output of other knowledge area processes should be reviewed to identify possible risks across the entire project

Risk identification: Tools & techniques

- Documentation reviews
  - A structured review may be performed of project documentation, including plans, assumptions, prior project files, and other information. The quality of the plans, as well as consistency between those plans and with the project requirements and assumptions, can be indicators of risk in the project

Risk identification: Tools & techniques

- Information gathering techniques

  The following information gathering techniques can be used in identifying risk

  - Brainstorming
    - The goal of brain storming is to obtain a comprehensive list of project risks. The project team usually performs brainstorming, often with a multidisciplinary set of experts not on the team.

Risk identification: Tools & techniques

- Ideas about risk are generated under the leadership of a facilitator.
- Categories of risk, such as risk breakdown structure, can be used as framework.
- Risks are then identified and categorized by type

Contd..

- Delphi technique
  - The Delphi technique is a way to reach a consensus of experts. The risk managers participate in this technique anonymously.
  - A facilitator uses a questionnaire to solicit ideas about the important risks.
  - The responses are summarized and then re-circulated to the experts for further comment.
  - Delphi technique helps reduce the bias in the data and keeps any one person from having undue influence on the outcome

Contd..

- Interviewing
  - Interviewing experienced project participation stakeholders, and subject matter experts can identify risks. Interviews are a major source of risk identification data gathering

Contd..

- Root cause identification
  - This is an inquiry in to the essential causes of entity’s risks. It sharpens the definition of risk and allows grouping risks by causes. Effective risk responses can be developed if the root cause of the risk is addressed

Contd..

- SWOT analysis
  - This technique ensures examination of the project from each of the SWOT perspectives, to increase the breadth of considered risks.

Risk identification: Tools & techniques

- Checklist analysis
  - Risk identification checklist can be developed based on historical information and knowledge that has been accumulated from previous similar projects and from other sources of information.

Risk identification: Tools & techniques

- The lowest level of the RBS can be used as a risk checklist.
- While a checklist can be quick and simple, it is impossible to build an exhaustive one. The checklist should be reviewed periodically for future use.

Contd..

- Assumptions analysis
  - Every activity is conceived and developed based on a set of hypotheses, scenarios, or assumptions.
  - Assumptions analysis is a tool that explores the validity of assumptions as they apply to the project.
  - It identifies risks to the project from inaccuracy, inconsistency, or incompleteness of assumptions

Contd..

- System or process flow chart
  - These show how various elements of a system interrelate, and the mechanism of causation
- Influence diagrams
  - These are graphical representation of situations showing causal influences, time ordering of events, and other relationships among variables and outcomes

Risk identification: Outputs

- Risk register
  - The primary outputs from risk identification are the initial entries into the risk register, which becomes a component of the organizational management plan.
  - The risk register ultimately contains the outcomes of the other risk management processes as they are conducted.

Contd..

- The preparation of the risk register begins in the risk identification process with the following information, and then becomes available to other activities and processes.
  - List of identified risk
    - The identified risks including their root causes and uncertain assumptions, are described. Risks can cover nearly any topics

Contd..

Examples:

There could be a risk that industrial relations disputes at the ports will delay and subsequently, delay completion of the construction phase.

Contd..

- List of potential responses
  - Potential responses to a risk may be identified during the risk identification process. These responses, if identified may be useful as inputs to the risk response planning process

- Root cause of risk
  - These are the fundamental conditions or events that may give rise to the identified risk

Contd..

- Updated risk categories
  - The process of identifying risks can lead to new risk categories being added to the list of risk categories. The RBS developed in the Risk Management Planning process may have to be enhanced or amended, based on the outcomes of the risk identification process

Risk assessment

- Risk assessment is the identification and analysis of relevant risks to the achievement of objectives.
- Management needs to identify these risks in order to know the areas in which the internal control structure needs to be particularly strong. Conversely, risk assessment may indicate areas where risks are low, and therefore where the entity does not need to design elaborate internal control structures

Effective ways to assess risk

- Analyzing risks in third party operations
  - In analyzing its payroll and benefits cycle, a company identifies risks related to the completeness and accuracy of employee data maintained by its third-party payroll service provider.

Effective ways to assess risk

- These risks include the risk of incomplete or inaccurate processing of data by the payroll administrator due to ineffective review and authorization controls, which could lead to errors in the financial reporting of compensation and benefits expenses

Effective ways to assess risk

- – Additionally, the company identifies risks related to improper review controls, which could result in the set up of fictitious employees, leading to further risks of fraudulent financial reporting

Contd..

- Analyzing risk across functions
  - A $ 20 M retailer with 75 employees and 10 retail stores convenes the department heads representing finance, HR, merchandizing, operations and administration (management), and performs a risk analysis by functional department.
  - The risks are rated from 1 to 5 (1 being the least risky and 5 the most risky) and are based on both significance of the business and likelihood of occurrence.

Contd..

- The analysis is performed by discussion in a working session format, and the results are documented in a table that outlines the specific risk together with the rating and the factors that contribute to the rating. Risk identified related to revenue recognition is documented as follows:
    - Revenue may not be recognized in accordance with GAAP
    - Risk rating=5

Contd..

- Factors contributing to risk rating
  - Complexity of rules for revenue recognition
  - Knowledge level of people responsible for recording sales transactions

Contd..

- Complexity of promotion and discount transactions
- Aggressive sales targets
- Incentives and bonus structure
- Supporting systems limitations

Contd..

- Analyzing risk for information technology
  - In a $ 20 M retailer with three information technology support personnel, application and general computer controls are driven by the critical application identified that support the financial reporting process.
  - This approach helps the company establish which information systems management will rely on.

Contd..

- IT management meets with the business process owners to review the results of the business process risk assessment.
- IT works to gain an understanding of how application data is utilized in the financial reporting process and determines whether there are other user controls (manual controls) in place that would mitigate the need for application and general computer controls

Contd…

- IT management creates a revised listing of critical applications that need to be addressed when designing application and general computer controls
- IT management maps the critical applications to the operating systems, databases and IT processes that support those applications.
  - Packaged software and third party web application typically reduce the number of IT processes applicable to those applications

Qualitative risk analysis

- Qualitative risk analysis includes methods for prioritizing the identified risks for further action
- Qualitative risk analysis assesses the priority of identified risks using their probability of occurring, the factors such as the time frame and risk tolerance of the project constraints of cost, schedule, scope and quality.

Contd..

- Definitions of the levels of probability and impact, and expert interviewing , can help to correct biases that are often present in the data used in this process
- The time criticality of risk- related actions may magnify the importance of a risk.
- An evaluation of the quality of the available information on project risks also helps understand the assessment of the risks’ importance to the project

Contd..

- Qualitative risk analysis is usually a rapid and cost-effective means of establishing priorities for risk response planning and lays the foundation for quantitative risk analysis, if this is required

Qualitative risk analysis: Tools & techniques

- Risk probability and impact assessment
  - Risk probability and impact assessment investigates the likelihood that each specific risk will occur.
  - Risk impact assessment investigates the potential effect on an organization/project objectives such as time, cost, scope or quality including both negative effects for threats and positive effects for opportunities

Contd..

- – Probability and impact are assessed for each identified risk. Risks can be assessed in interviews or meetings with participants selected for their familiarity with the risk categories on the agenda
- – The level of probability for each risk and its impact on each objective is evaluated during the interview or meeting explanatory detail, including assumptions justifying the levels assigned is also recorded

Contd..

- Risk probabilities and impacts are rated according to the definitions given in the risk management plan
- Risks with low rating of probability and impact will not be rated, but will be included on a watch list for future monitoring

Contd..

- Probability and impact matrix
  - Risks can be prioritized for further quantitative analysis and response, based on their risk rating.
  - Evaluation of each risk’s importance is typically conducted using a look- up table or a probability and impact matrix

Contd..

- The matrix specifies combinations of probability and impact that lead to rating the risks as low, moderate, or high priority. Descriptive terms or numeric values can be used, depending on organizational preferences.

Risk response

- Risk response is the process of developing strategic options, and determining actions, to enhance opportunities and reduce threats to the project’s objectives.
- A team member is assigned to take responsibility for each risk response.
- This process ensures that each risk requiring a response has an owner monitoring the responses, although the owner may delegate implementation of a response to someone else

Strategies for negative risks

- Three strategies typically deal with threats that may have negative impacts on organizational objectives
- Avoid
  - Risk avoidance involves changing the management plan to eliminate the threats posed by an adverse risk, to isolate the organization’s objectives from the risk’s impact, or to relax the objectives that is in jeopardy, such as extending the project schedule or reducing scope

Contd…

- Transfer
  - Risk transfer requires shifting the negative impact of a threat, along with ownership of the response, to a third party.
  - Transferring the risk simply gives another party responsibility for its management and does not eliminate it.
    - Contracts may be used to transfer liability for specified risks to another party

Contd..

- Mitigate
  - Risk mitigation implies a reduction in the probability of an adverse risk event to an acceptable threshold.
    - Adopting less complex processes, conducting more tests or choosing a stable supplier are examples of mitigation actions

Strategies for positive risks

- Exploit
  - This strategy may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized.
  - Directly exploiting responses include assigning more talented resources to the project to reduce the time to completion, or to provide better quality than originally planned

Strategies for positive risks

- Share
  - Sharing a positive response involves allocating ownership to a third party who is best able to capture the opportunity for the benefit of the organization
- Enhance
  - This strategy modifies the size of an opportunity by increasing probability and positive impact, and by identifying and maximizing key drivers of these positive-impact risks.

Risk Monitoring & Control

- Risk monitoring and control is the process of identifying, analyzing and planning for newly arising risks, keeping track of the identified risks and those on the watch list, reanalyzing existing risks, monitoring trigger conditions for contingency plans, monitoring residual risks, and reviewing the execution of risk response while evaluating their effectiveness.
  - The risk monitoring and control process applies techniques, such as variance and trend analysis, which require the use of performance data generated during work execution

Contd...

- Risk monitoring and control as well as other risk management processes, is an ongoing process for a certain activity. Other purposes of risk monitoring and control are to determine if:
  - Activity assumptions are still valid

Contd..

- – Risk, as assessed, has changed from its prior stat, with analysis of trends
- – Proper risk management policies and procedures are being followed
- – Contingency reserves of cost or schedule should be modified in line with the risks of the project

Contd..

- Risk monitoring and control can involve choosing alternative strategies, executing a contingency or fallback plan, taking corrective action, and modifying the project management plan. Risk monitoring and control tools and techniques include;
  - Risk reassessment
    - Risk monitoring and control often requires identification of new risks and reassessment of risks, using the requisite processes. It should be an agenda item at team status meetings.

Contd..

- Risk audits
  - Risk audits examine and document the effectiveness of risk responses in dealing with identified risks and their root causes, as well as the effectiveness of the risk management process.

Contd..

- Variance and trend analysis
  - Trends in project execution should be reviewed using performance data, EV analysis and other methods of project variance and trend analysis for monitoring overall performance. Outcomes from these analyses may forecast potential deviation of the project at completion from cost and schedule targets. Deviations from the baseline plan may indicate the potential impact of threats and opportunities

Contd..

- Technical performance measurement
  - Technical performance measurement compares technical accomplishments during project execution to the project management plan's schedule of technical achievements. Deviations, such as demonstrating more or less functionality than planned at a milestone, can help to forecast the degree of success in achieving the project's scope

Contd..

- Reserve analysis
  - Throughout execution of project, some risks may occur, with positive or negative impacts on budget or schedule contingency reserves. Reserve analysis compares the amount of contingency reserves remaining to the amount of risk remaining at any time in the project in order to determine if the remaining reserve is adequate

Contd..

- Status meetings
  - Organizational risk management can be an agenda item at periodic status meetings. Risk management becomes easier the more often it is practiced