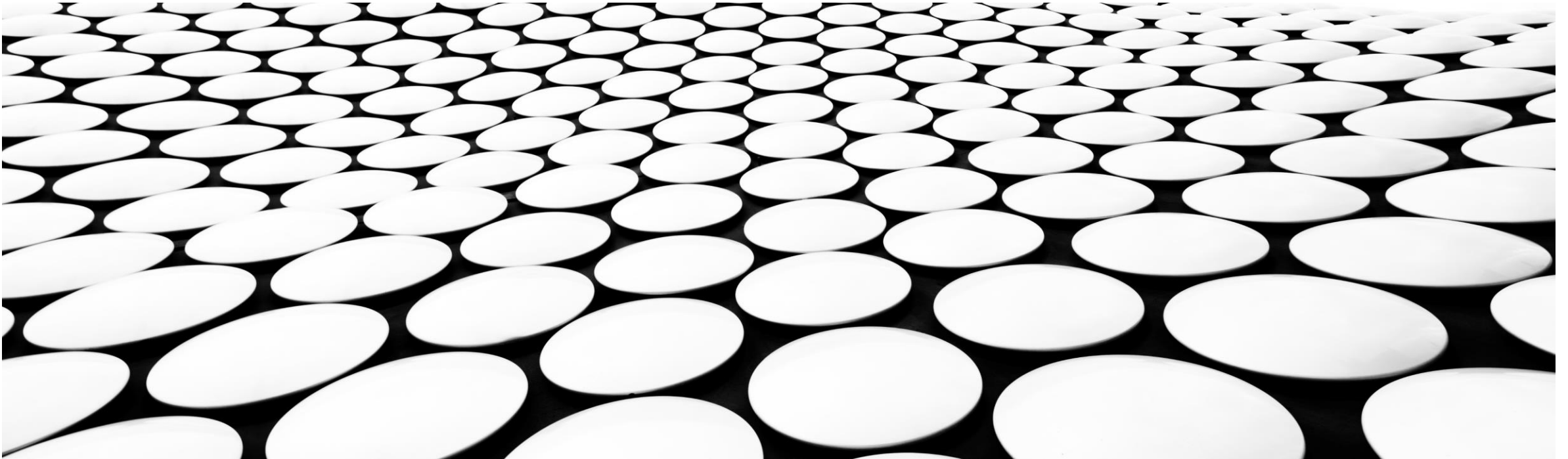

FINANCE FOR NON-FINANCE – MODULE VII

ENTERPRISE RISK MANAGEMENT – THE CONCEPT

B D CHATTERJEE FCA, ACMA, ACS, DIP IFR (ACCA) – UNITED KINGDOM



Types of Risk

<i>Strategic</i>	Political risk, talent and succession planning risk, and risk from dependencies on other organizations.
<i>Financial</i>	Risk of audit findings and other things that would undermine reporting integrity.
<i>Compliance</i>	Fraud risk and non-compliance with fair employment practices.
<i>Operational</i>	Risk that Programs fail to meet their objectives, natural disasters, and lack of technology availability.
<i>Reputational</i>	Risk related to reputation of the organization.

ENTERPRISE RISK MANAGEMENT – AN OVERVIEW

ERM is a process-based approach where the various components interact as part of an on-going, iterative process. COSO represents these relationships in a three-dimensional cube as shown below:



ENTERPRISE RISK MANAGEMENT – A FRAMEWORK



CONTROL ENVIRONMENT

It creates a set of standards, processes, and structures that provide the basis for carrying out internal control.

The Control Environment should ensure controls are in place, covering areas such as:

- Clear lines of responsibility and authority
- Procurement policy
- Three-way match in vendor payments
- Code of Ethics
- Whistle-blower policies
- Hiring practices
- Training programs

CONTROL ENVIRONMENT



Monitored through

Process Narratives
Organizational charts
Flowcharts
Questionnaires
Memorandums
Checklists



Clear lines of responsibility and authority

Procurement policy

Three way match in vendor payments

Code of Ethics

Whistleblower policies

Hiring practices

Training programs

Global Chart of Accounts

RISK ASSESSMENT

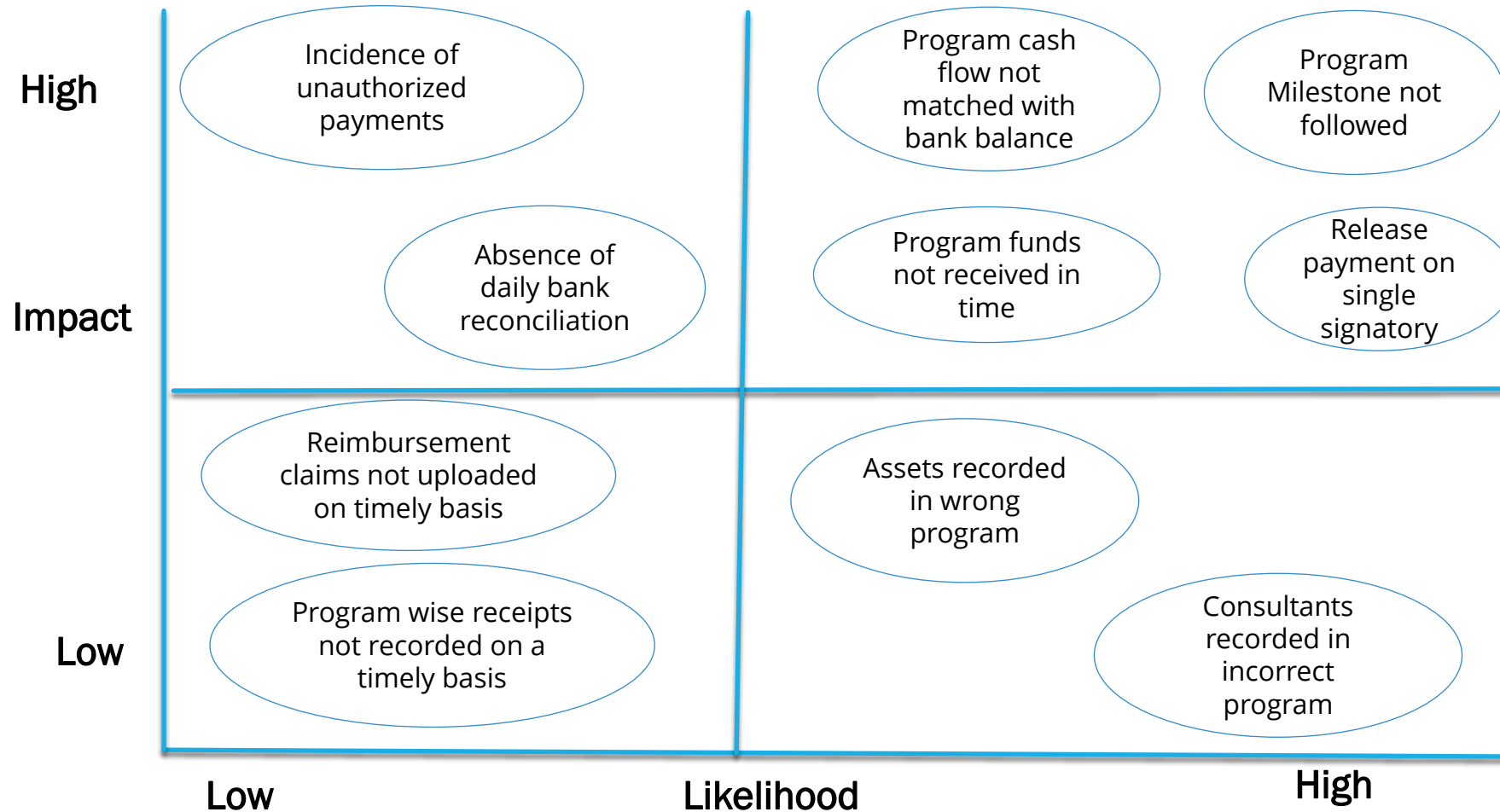
Risk Assessment factors	Risks
1. Materiality of the amounts	<ul style="list-style-type: none">● Large value/transaction● High volume of transactions● Significant impact on key ratios or disclosures
2. Complexity of the process	<ul style="list-style-type: none">● Limited internal skills● Multiple data handoffs● Highly technical in nature
3. History of accounting adjustments	<ul style="list-style-type: none">● Accounting errors● Valuation adjustments, etc.
4. Propensity for change in	<ul style="list-style-type: none">● Business processes or controls● Related accounting

RISK ASSESSMENT

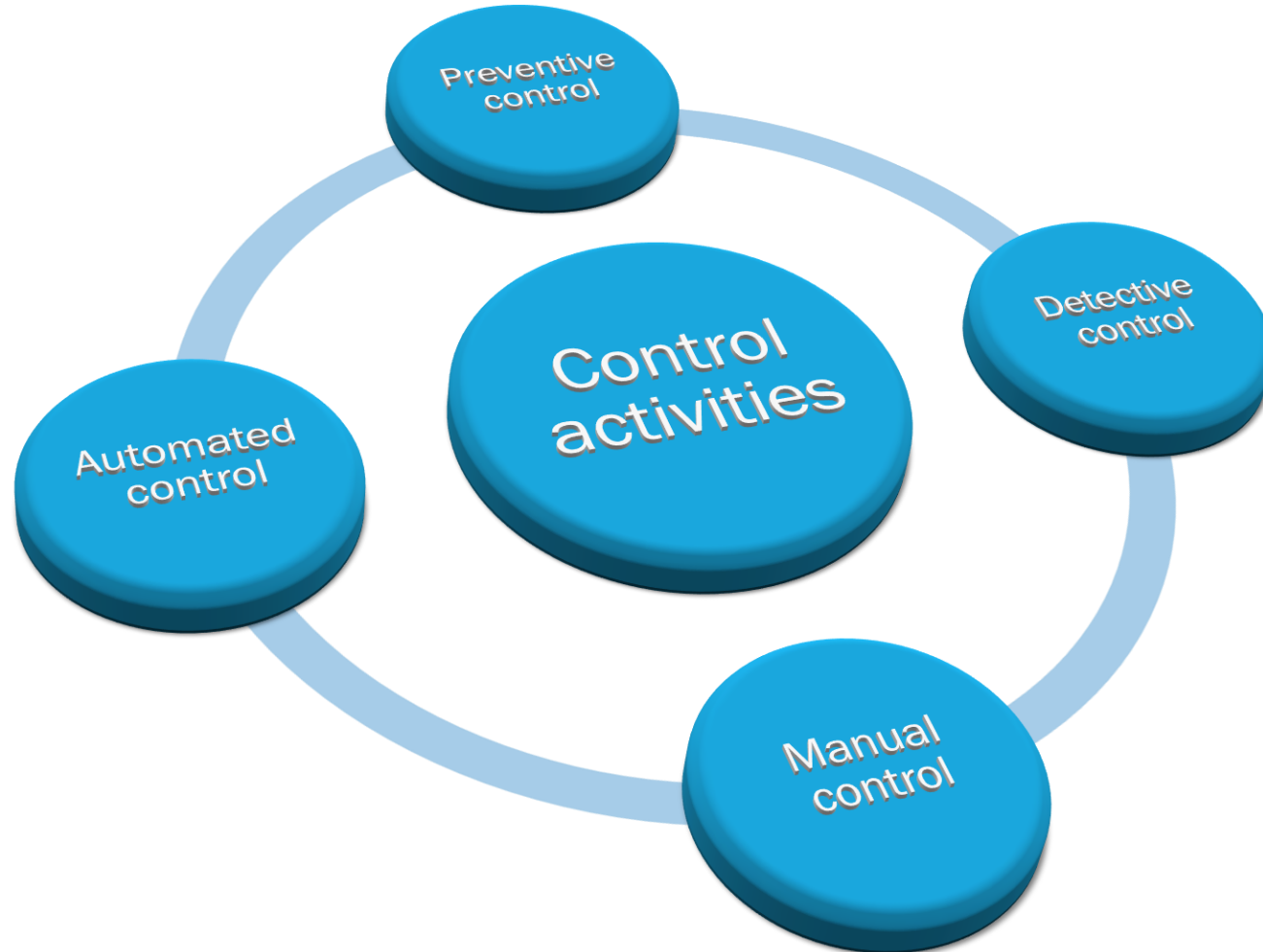
Considerations to assess risk

<i>Internal considerations</i>	<i>External considerations</i>
<ol style="list-style-type: none">1. Use of qualitative/quantitative methods2. Change in management responsibilities3. Weak or unresponsive tone at the top4. Human capital – quality of personnel hired/retained5. Employee sabotage6. System security weaknesses7. Rapid growth8. Changes in processes or access to assets	<ol style="list-style-type: none">1. Technological advancements (more tools available, as well as existing tools we are using are outdated)2. Changing/evolving client/constituent needs or expectations3. Changing legislative requirements and new laws/regulations4. Decentralized organization operations5. Natural disasters6. Impact of program, political, and economic changes

RISK ASSESSMENT – ENTERPRISE RISK MAP



CONTROL ACTIVITIES



CONTROL ACTIVITIES

Preventive controls	<p><i>Prevent</i> the occurrence of a negative event in a proactive manner.</p> <p>Examples</p> <ul style="list-style-type: none">Bank transfers with two signaturesSegregation of dutiesSecurity and surveillance systems in high-risk areas, andPre-numbered invoices and cheques
Detective controls	<p><i>Detect</i> the occurrence of a negative event <i>after</i> the fact in a reactive manner.</p> <p>Examples</p> <ul style="list-style-type: none">Supervisor review & approvalAudit trail for each transactionReports that are run showing user activityReconciliation of accounts payable

CONTROL ACTIVITIES

Manual controls	Require action to be taken by employees. Examples include Obtaining a supervisor's approval for overtime Reconciling bank accounts, and Matching receiving to Purchase Orders
Automated controls	These are Built into the network infrastructure and software applications. Examples include Passwords Data entry validation checks, and Batch controls

INFORMATION AND COMMUNICATION

- Accurate, timely information is necessary to properly carry out internal control responsibilities in support of the achievement of an organization's objectives.
- Communication is the continual, iterative process of providing, sharing, and obtaining that necessary information.

MONITORING ACTIVITIES

Monitoring activities are evaluations used to ascertain whether components of internal control are *present* and *functioning*. These evaluations can be split into two categories:

- **Ongoing** evaluations are built into business processes and provide timely information on the underlying controls.
- **Separate** evaluations are conducted periodically and vary in scope and frequency based on prior assessments of risk, the effectiveness of *ongoing* evaluations, and other management considerations such as resource prioritization. Separate evaluations include Internal Audit activities.

INFORMATION AND COMMUNICATION

The things to communicate	Initiatives Goals Changes Opportunities Feedback Questions Answers Policies Procedures Standards Expectations

MONITORING CONTROL

Monitoring activities are evaluations used to ascertain whether components of internal control are *present and functioning*

Ongoing evaluations are built into business processes and provide timely information on the underlying controls.

Separate evaluations are conducted periodically and vary in scope and frequency based on prior assessments of risk, the effectiveness of *ongoing* evaluations.

Examples:

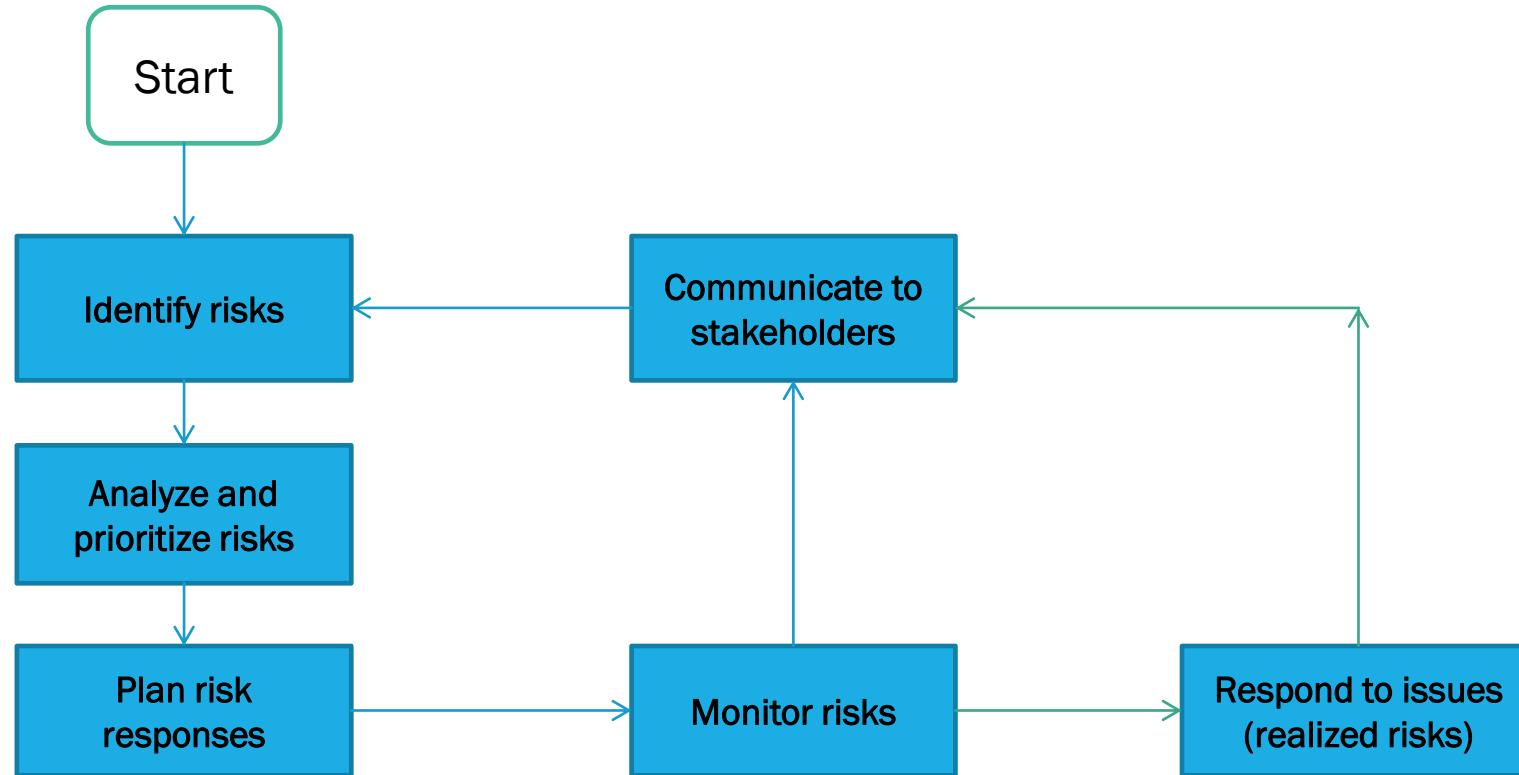
Internal Audit activities.

Forensic audit and investigation.

INTERNAL CONTROL PRINCIPLES

Internal control principles	Process Narrative
<i>(a) Establish Delegation of Authority</i>	Across organization hierarchy and value chain
<i>(b) Assign Accountability</i>	Assign each task to only one person and make him accountable
<i>(c) Segregate Duties</i>	Don't make one employee responsible for all parts of a process, preferably in the lines of segregation of custody, recording and approval functions
<i>(d) Restrict Access</i>	Don't provide access to systems, information, assets, etc. unless needed to complete assigned responsibilities; except for the power user/system administrator, no single user can have access to the entire system
<i>(e) Document Procedures and Transactions</i>	Prepare documents to show that activities have occurred; Develop audit trail of each activity
<i>(f) Independently verify</i>	Check others' work, introduce maker, checker and approver concept

RISK MANAGEMENT PROCESS



Successful risk management is a continuously iterative process

RISK MANAGEMENT PLAN

Understand the concept of risk in all our operations

Prioritize risks through Risk Maps in each country or legal entity

Implement Leadership certification of all compliance activities in each country or legal entity

Implement Global Chief Financial Officer certification process of all compliance activities for the group along with implementation of robust checks and controls.

Visit each country or legal entity to explain the concept of risk management and implement effective a certain GO LIVE date.

RISK MANAGEMENT QUESTIONNAIRE

Business Planning, Management and Control Environment

Budgeting and budgetary control

Revenue to Cash

Procurement to Payable

Attendance Records and Payroll

Record to report transaction

Information systems, Management and controls



THANK YOU!