Malta Forum for Internal Auditors

Practical Approach to the Implementation of Risk Assessment Process

29th July 2011 – 1400hrs - 1715hrs

Agenda

Introduction to the topic (methodology, reporting and plan preparation)	2.00 – 2.45
Airing of concerns/difficulties of implementation	2.45 – 3.15
Group discussions**	3.15 – 3.45
Coffee Break	3.45 – 4.00
Group presentations	4.00 – 4.40
Concluding comments	4.40 – 5.00

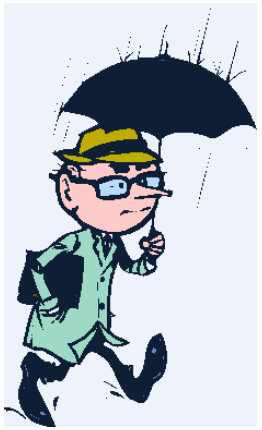
What is risk?

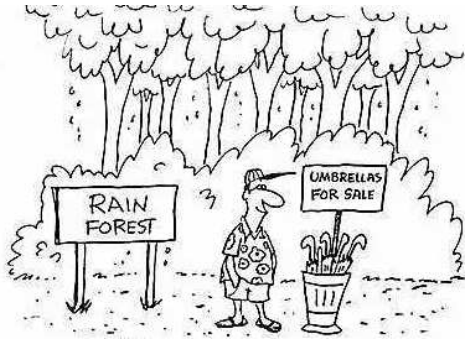
‘A probability or threat of a damage, injury, liability, loss, or other negative occurrence that is caused by external or internal vulnerabilities, and that may be neutralized through pre-emptive action’

‘The effect of uncertainty on objectives whether +ve or –ve’

Thinking of risk?

RISK





Analysing the risk profile

Risk Maturity	Key Characteristics	Internal Audit Approach
Naive	No formal approach	Promote risk management and rely on IA risk assessment
Aware	Scattered Silo based approach	Promote enterprise-wide approach to risk management and rely on IA risk assessment
Defined	Strategies & policies in place. Risk appetite defined.	Facilitate / liaise with risk management and use management assessment of risk where appropriate
Managed	Enterprise-wise approach to risk management developed and communicated	Audit risk management processes and use management assessment of risk when appropriate
Enabled	Risk management & internal control fully embedded in operations	Audit risk management processes & use management assessment of risks

Perception of risk has evolved

From back room ...	… to Board room
Low/operational level – risk management is a function of the internal auditors	The Board's overall responsibility (with Council / Board oversight)
Risk as a negative factor to be avoided	Risk as an opportunity factor to be controlled/insured
Risk managed in organisational silos	Risk managed in an integrated enterprise-wide fashion
Responsibility for risk management is delegated to lower levels	Risk management responsibility accepted by senior and line management
Unstructured and divergent risk management functions	Risk management is built into all corporate management systems

Defining Enterprise Risk Management

- A structured, consistent and continuous process across the whole organisation for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives
- The board has overall responsibility for ERM, in practice delegated to the management team. There may be a separate function that co-ordinates and manages these activities

…

The Board therefore needs to gain assurance that risk management processes are effective and that risks are managed

Various ERM frameworks

COSO’s ERM – Integrated framework

AS/NZ 4360/2004

British Standard 31100

ISO 31000

King Report on Corp Governance (I and II)

Components of a framework for managing risks

- Understand the organisation and its context
- Establish a risk management policy
- Assign responsibilities – risk owners
- Integration into organisational processes
- Assign resources
- Establish communication and reporting mechanisms
- Implement, monitor and review (KRIs)

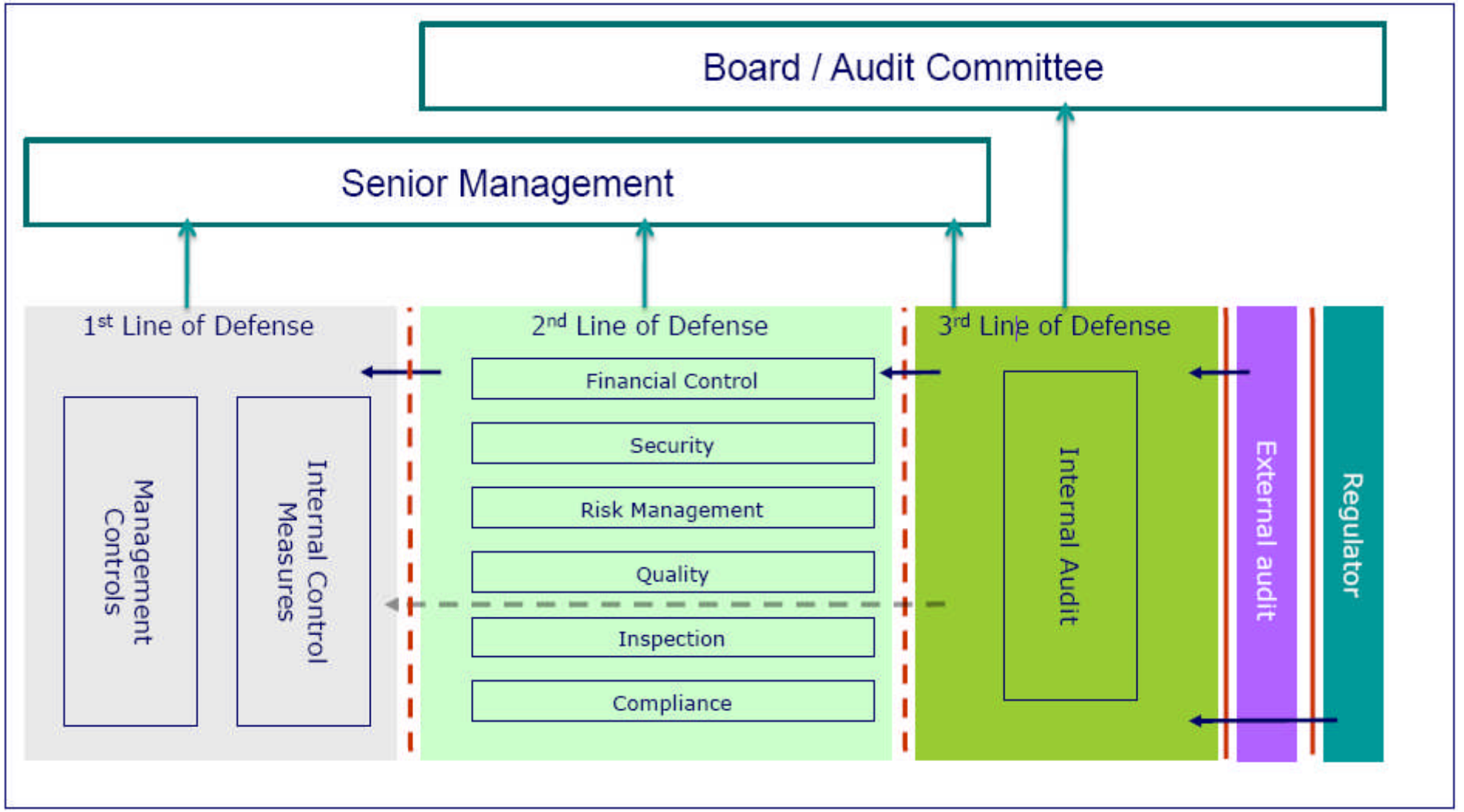
International standard ISO/31000 Risk management – Principles and guidelines

Internal audit – A provider of assurance on risk

- The profession of internal audit is fundamentally concerned with evaluating an organisation's management of risk
- The key to an organisation's success is to manage risk effectively
- The role of the internal auditor is to provide **assurance** to management that all **key** risks are being effectively covered
- An internal auditor's knowledge or the management of risk enables them to act as consultants and catalyst for change

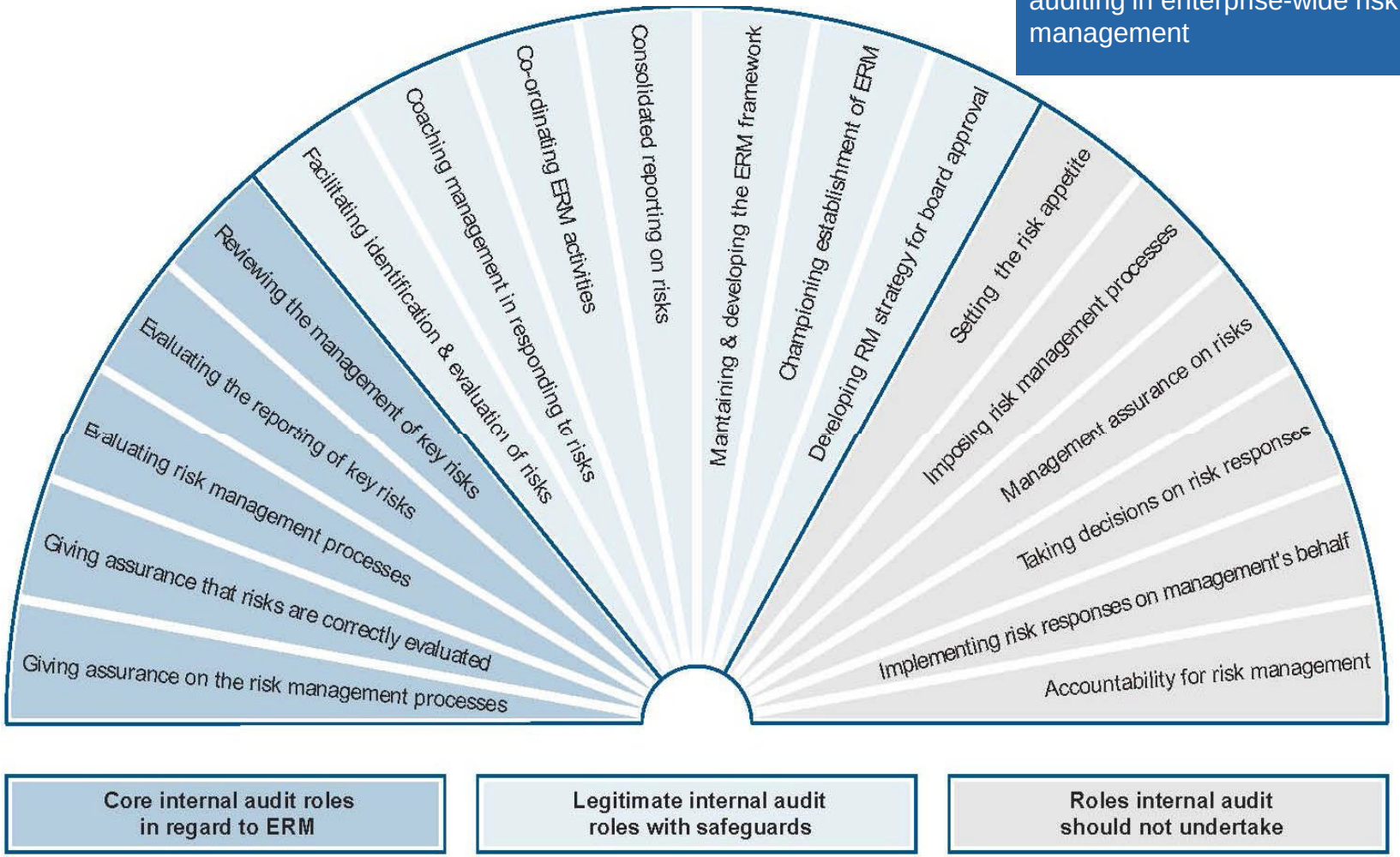
When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks – IIA Standard 2120.C3

The Three Lines of Defense Model



Can do/can't do

IIA Position Paper – The role of internal auditing in enterprise-wide risk management



A consulting role with safeguards

- Management remains responsible for risk management
- IA responsibilities with regards to risk should be documented in the charter
- IA should not manage risks
- IA should provide advice, challenge and support to risk decision processes but cannot take decisions
- IA cannot give assurance for any part of the framework it is responsible for

The concept of ‘Combined Assurance’

Today

- No single view of assurance across organisation
- Differing perspectives on risk (audit vs business, inherent vs residual, BU vs Group)
- Potential for duplication and gaps in assurance
- Little Board/AC level visibility of the linkage between sources of assurance

Tomorrow

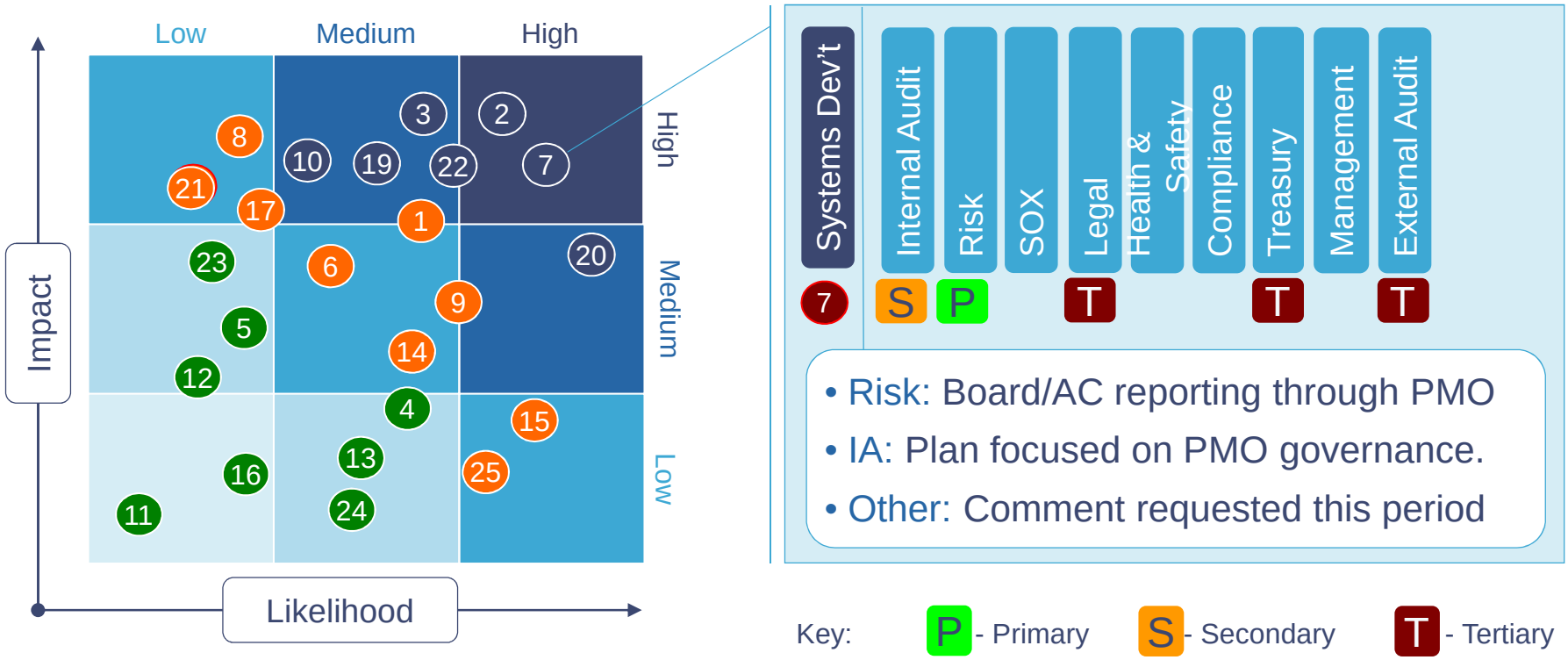
Assurance Need

Internal Audit	Health & Safety
Risk	Compliance
SOX	Treasury
Legal	External Audit

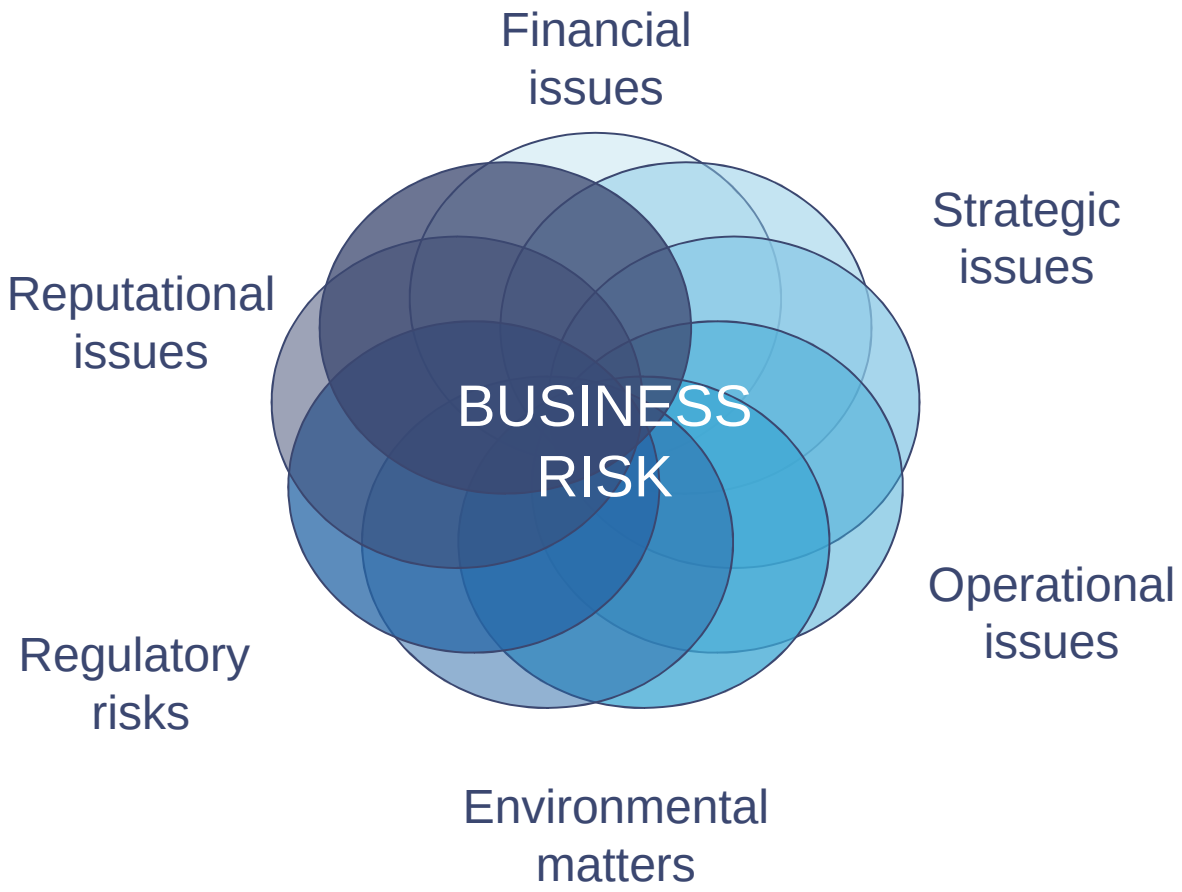
- Collaboration between assurance providers
- Develop common view of risk to organisation
- Presents to Board how key risks are being covered by assurance providers
- This Is More Than developing improvements in risk-based internal auditing

Combined assurance map – one view of the truth

- Promotes the definition of the assurance need by risk owners (expectation)
- Clarification by assurance providers on the actual assurance provided



Risk evolution



Risk assessment defined

The process for **identifying** and **evaluating events** that could **influence** the **achievement** of an organisation's **key business objectives**.

- Forms the foundation for an effective enterprise risk management program
- Empowers management to focus its attention on the most significant risks and make more informed decisions
- Yields forward-looking insight, not only allowing organisations to avoid risks, but providing a more meaningful clarity around the risks they face

Risk assessment defined (Cont)

A Risk assessment is NOT:

- A detailed review of a specific business process
- A conclusion on the business process and controls
- The performance of detailed testing of transactions related to the process
- A validation of statements made during the management and staff interview process
- The end step of process and control analysis
- An audit

Internal audit's role in Risk assessment

Every organisation approaches risk assessments differently. The objective of the annual risk assessment for IA purposes is to enable focus on areas of perceived risk

- Internal audit role may vary depending on whether management has already performed a risk assessment:
  - **YES**, then IA must review risk assessment to ensure risk analysis is appropriate sufficiently recent, right people involved in its creation/update, and scope sufficient to address main risks of the organisation
  - **NO**, then IA should create one for purposes of creating the audit plan
- Use industry and functional specialists to better understand risks and to identify the appropriate reviews to add to the audit plan

Essential steps in performing a Risk assessment

Final deliverable

Summary of Risk profile

Key Function	Risk Classification	Risk No.	Detailed Risk	Likelihood	Risk Impact	Controls
A. Finance Section *Objective: Direct, control and administer the financial activities of the organisation and provide the Chief Executive and the Board with financial assessments and information to assist them in decision-taking.*						
Billing & Debt Collection	Financial / Operational	1	Incorrect invoice details leading to inaccurate charging or charging the wrong customer.	M	M	Medium
	Financial	2	Services rendered are not billed.	M	H	Medium
	Financial	3	Sales invoices do not represent actual services rendered within the proper period.	L	L	Medium
	Financial / Operational - Fraud	4	Waiving or reducing amount due either through credit notes or manual adjustments.	M	H	Medium
	Regulatory	5	Charges billed and/or VAT thereon are not in compliance with laws and regulations.	L	H	Medium
	Financial / Operational	6	Payments received not properly recorded and cheques received may inadvertently not be deposited in the bank.	L	H	Strong
	Financial	7	Bad debts arising from irrecoverable amounts charged.	M	H	Strong

Sources of information

- Obtain understanding of the business by reviewing:
  - Vision and mission statements
  - Organisational chart
  - Policies & procedures
  - Financial statements
- Laws and regulations (both local and foreign)
- Previous internal audit engagement reports
- Conduct meetings with management

Identify relevant business objectives

Key Function	Risk Classification	Risk No.	Detailed Risk	Likelihood	Risk Impact	Controls
A. Finance Section *Objective: Direct, control and administer the financial activities of the organisation and provide the Chief Executive and the Board with financial assessments and information to assist them in decision-taking.*						
Billing & Debt Collection	Financial / Operational	1	Incorrect invoice details leading to inaccurate charging or charging the wrong customer.	M	M	Medium
	Financial	2	Services rendered are not billed.	M	H	Medium
	Financial	3	Sales invoices do not represent actual services rendered within the proper period.	L	L	Medium

Identify relevant business objectives

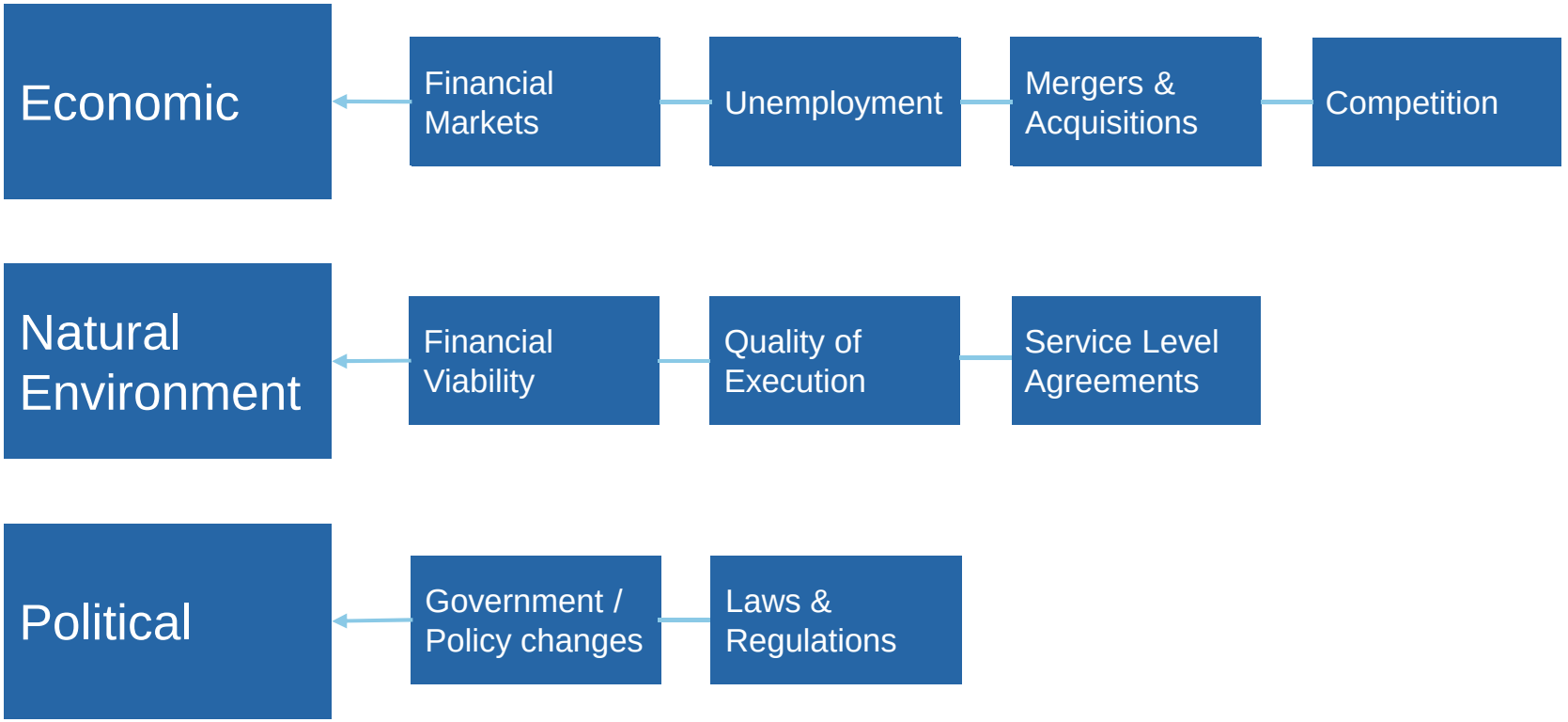
- Provides a basis for subsequently identifying potential risks that could affect the achievement of objectives, and ensure the resulting risk assessment and management plan is relevant to the critical objectives of the organization

- It is important to understand how these fit in with the strategy and how much risk the organization is willing to assume in pursuit of these objectives

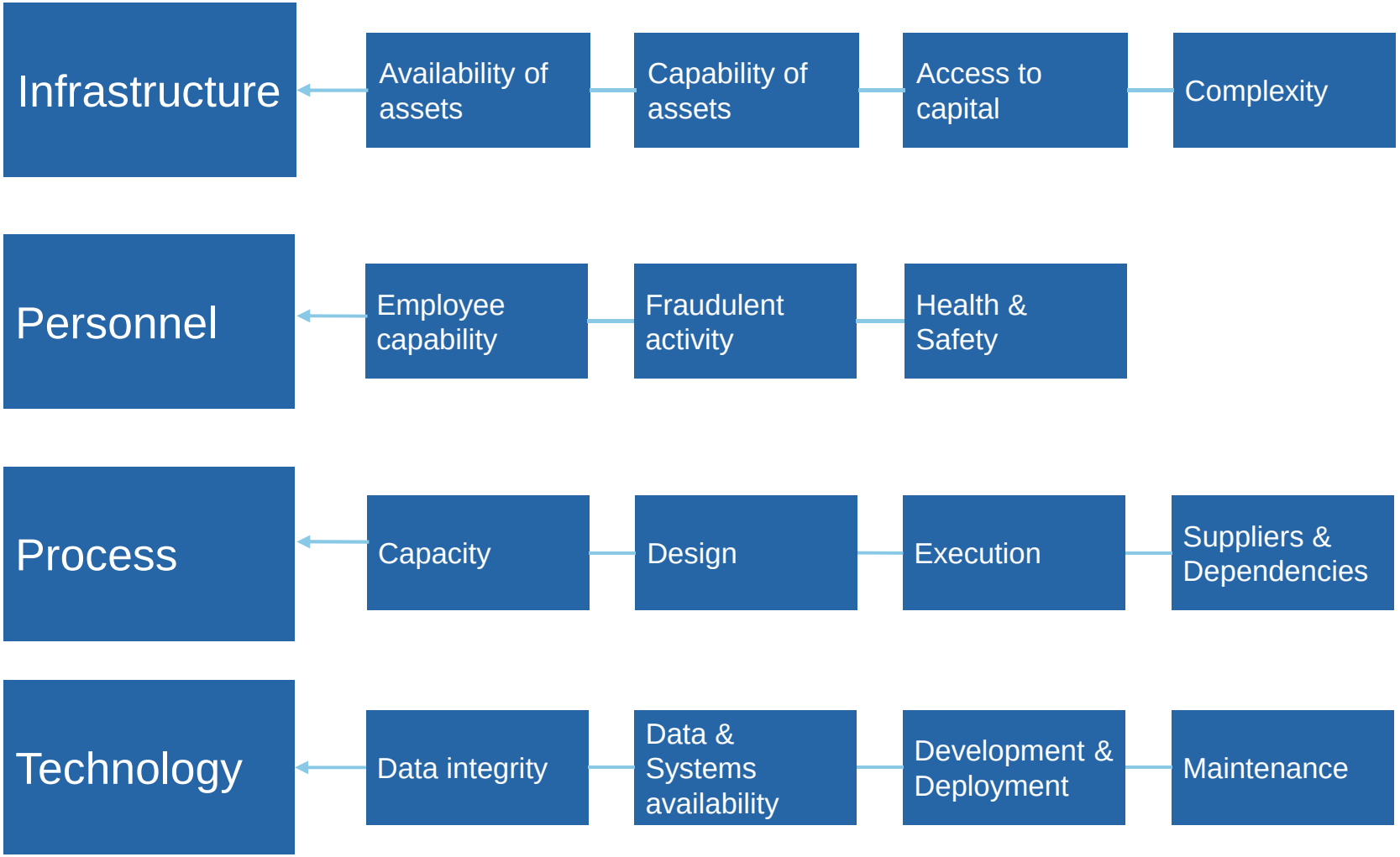
Identify events that could affect the achievement of objectives

- “Events” refers to prior and potential incidents occurring within or outside the organization that can have an effect, either positive or negative, upon the achievement of the organization’s stated objectives or the implementation of its strategy and objectives

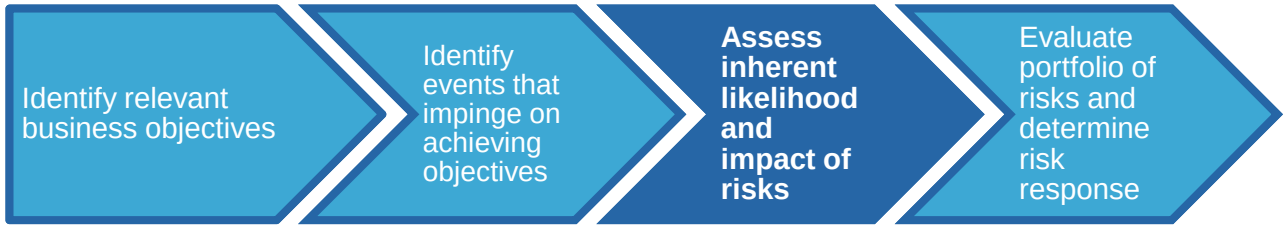
Identify events that could affect the achievement of objectives – External Factors



Identify events that could affect the achievement of objectives – Internal Factors

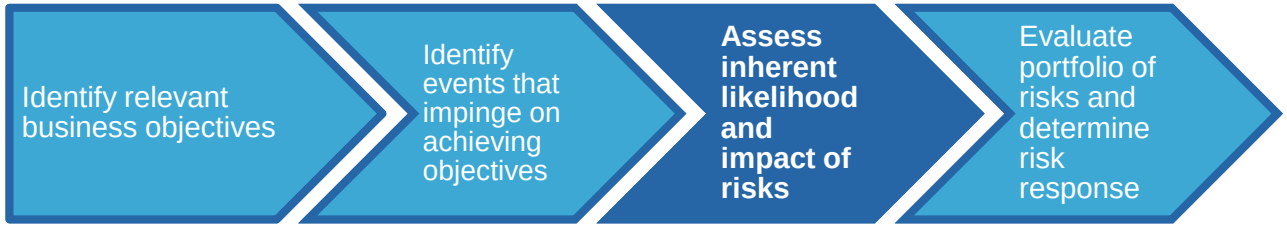


Assess likelihood and impact of risks



Key Function	Risk Classification	Risk No.	Detailed Risk	Likelihood	Risk Impact	Controls
A. Finance Section *Objective: Direct, control and administer the financial activities of the organisation and provide the Chief Executive and the Board with financial assessments and information to assist them in decision-taking.*						
Billing & Debt Collection	Financial / Operational	1	Incorrect invoice details leading to inaccurate charging or charging the wrong customer.	M	M	Medium
	Financial	2	Services rendered are not billed.	M	H	Medium
	Financial	3	Sales invoices do not represent actual services rendered within the proper period.	L	L	Medium
	Financial / Operational - Fraud	4	Waiving or reducing amount due either through credit notes or manual adjustments.	M	H	Medium
	Regulatory	5	Charges billed and/or VAT thereon are not in compliance with laws and regulations.	L	H	Medium
	Financial / Operational	6	Payments received not properly recorded and cheques received may inadvertently not be deposited in the bank.	L	H	Strong
	Financial	7	Bad debts arising from irrecoverable amounts charged.	M	H	Strong

Assess likelihood and impact of risks (Cont)



Likelihood of occurrence – the possibility that a given risk will occur

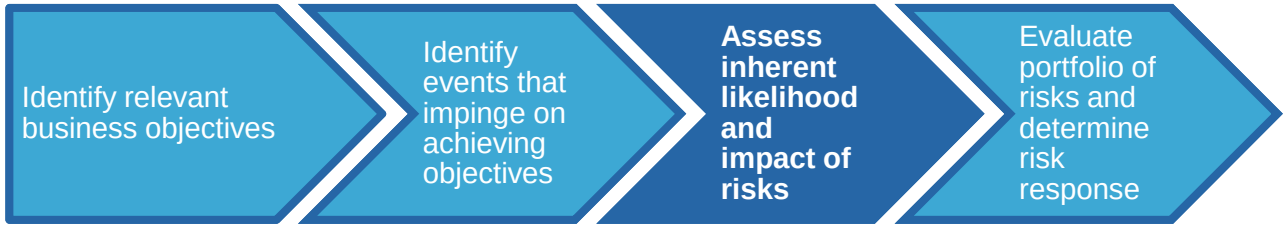
Assessment	Indicators	
Likely	Likely to occur in a one year time period	> 90% chance
Possible	Likely to occur in a 5 year time period.	> 50% chance
Remote	Not likely to occur in a 10 year time period.	> 10% chance

Assess likelihood and impact of risks (Cont)

Business impact – the effect that a occurring risk will have on the business operations, reputation, earnings, or shareholder value

Assessment	Mission/objectives	Financial	Reputation
High	■ High impact on achievement of mission/objectives	€xx - €xx costs/revenue	■ substantial, long term ■ widespread publicity
Medium	■ Medium impact on achievement of mission/objectives	€xx - €xx costs/revenue	■ short term to medium term ■ some publicity
Low	■ Low impact on achievement of mission/objectives	€xx - €xx costs/revenue	■ minor short term ■ limited or no publicity

Assess likelihood and impact of risks (Cont) – Inherent and Residual Risk



Inherent (or gross) risk assessment: This is performed to assess risks that are direct results of both external and internal factors BEFORE any controls or responses are applied.

INTERNAL AUDIT FOCUS

Residual risk assessment: This is performed to assess the remains of the inherent risk assessment AFTER the effect of any applied controls or responses.

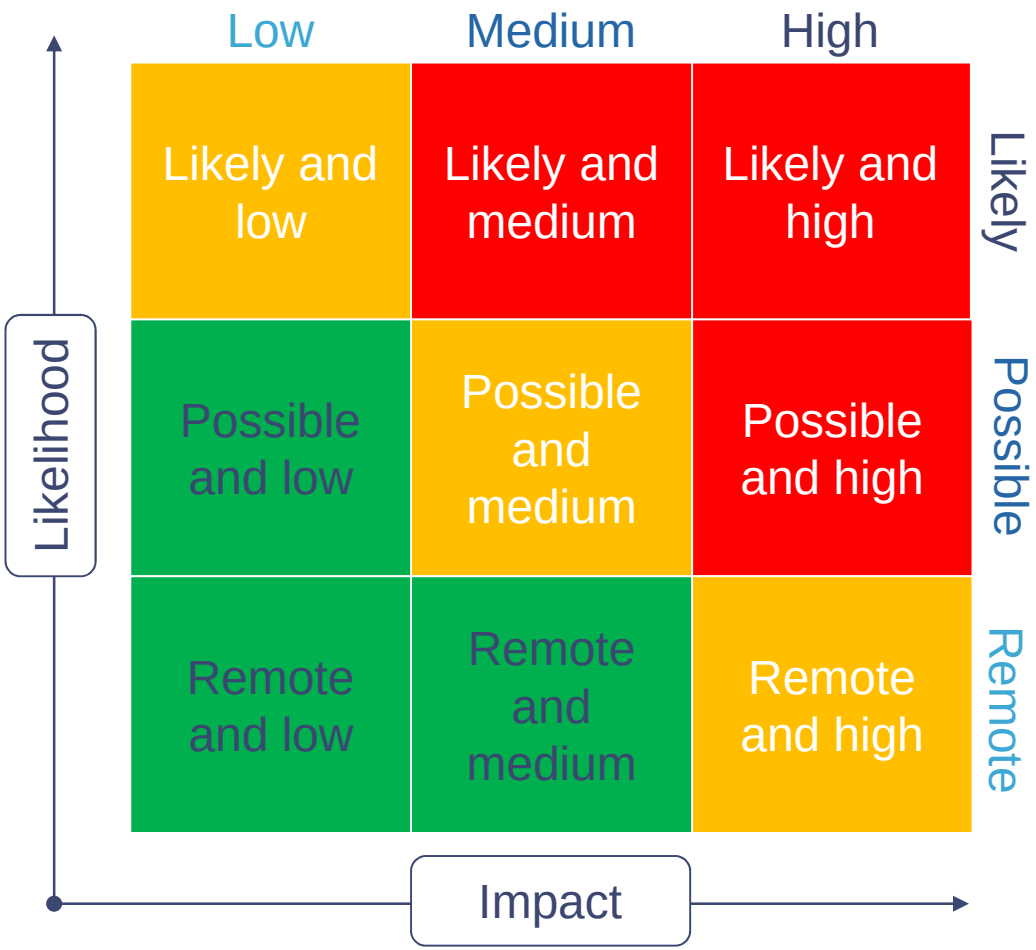
Emerging risk: Emerging risks are large-impact, hard to predict and rare events beyond the realm of normal expectations.

Assess likelihood and impact of risks (Cont) -

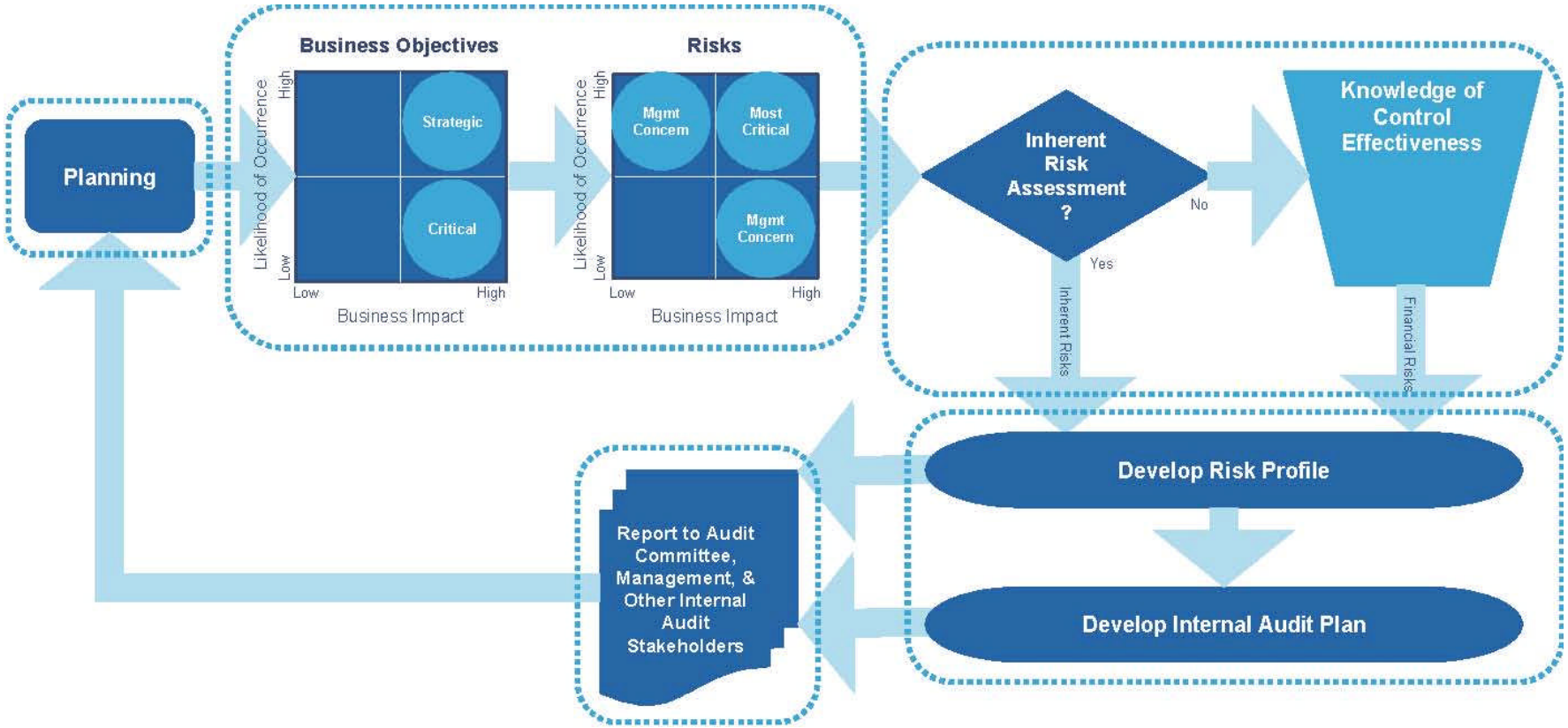
Summary of Risk Profile

Key Function	Risk Classification	Risk No.	Detailed Risk	Likelihood	Risk Impact	Controls
A. Finance Section *Objective: Direct, control and administer the financial activities of the organisation and provide the Chief Executive and the Board with financial assessments and information to assist them in decision-taking.*						
Billing & Debt Collection	Financial / Operational	1	Incorrect invoice details leading to inaccurate charging or charging the wrong customer.	M	M	Medium
	Financial	2	Services rendered are not billed.	M	H	Medium
	Financial	3	Sales invoices do not represent actual services rendered within the proper period.	L	L	Medium
	Financial / Operational - Fraud	4	Waiving or reducing amount due either through credit notes or manual adjustments.	M	H	Medium
	Regulatory	5	Charges billed and/or VAT thereon are not in compliance with laws and regulations.	L	H	Medium
	Financial / Operational	6	Payments received not properly recorded and cheques received may inadvertently not be deposited in the bank.	L	H	Strong
	Financial	7	Bad debts arising from irrecoverable amounts charged.	M	H	Strong

Likelihood and impact heatmap



Overview of whole process



Airing of concerns/difficulties of implementation

Group discussions

Group discussion A

Getting management ‘buy in’ in the risk assessment process

- Relevance of a Risk Management framework
- Risk Management responsibilities at Board, management and individual employee levels
- Value added to the organization
- Outputs from a risk management process
- Measuring and monitoring - Risk performance indicators

Group discussion B

Deriving the audit plan using the risk assessment work:

- Business objectives - (what can be done if these are not readily defined)
- Review of the organisation's risk assessment
- Level of risk awareness in the organization
- Likelihood and impact – difficulty/ease of measurement
- Setting the risk appetite
- Knowledge/assessment of control effectiveness
- Use of industry specialists

Group discussion C

Liaising with other professionals in the organisation who may be involved in risk assessment

- Identifying the people in your organisation that perform risk-related tasks
- Use of work and findings of other assurance providers
- Making sure that all aspects of risk are covered for IA purposes
- Keeping updated with work and findings of assurance providers, being internal or external to your organisation

Group discussion D

Interviewing and other problems encountered in the risk assessment process

- Interviewing – formal or an informal approach?
- Communication of risk assessment objectives
- Agreement on risk classification
- Making sure all risks are covered
- Aligning risks to business objectives

…others

Coffee Break

Group presentations

Concluding comments and questions