ENTERPRISE RISK MANAGEMENT (ERM)

The Conceptual Framework

ENTERPRISE RISK MANAGEMENT (ERM)

ERM Definition
The Conceptual Frameworks: CAS and COSO
Risk Categories
Implementing ERM
Why ERM?
ERM Maturity Model
Key Factors for ERM Success

ERM Definition

ERM Definition

ERM is the discipline by which an organization in any industry

- assesses;
- controls;
- exploits;
- finances; and
- monitors

risks from all sources for the purpose of increasing the organization short- and long-term value to its stakeholders.

(Casualty Actuarial Society, Overview of Risk Management P. 10)

ERM Definition

ERM is a process, affected by an entity's board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity goals."

(COSO, ERM-Integrated Framework, P. 8)

The Conceptual Frameworks for ERM

Conceptual Frameworks

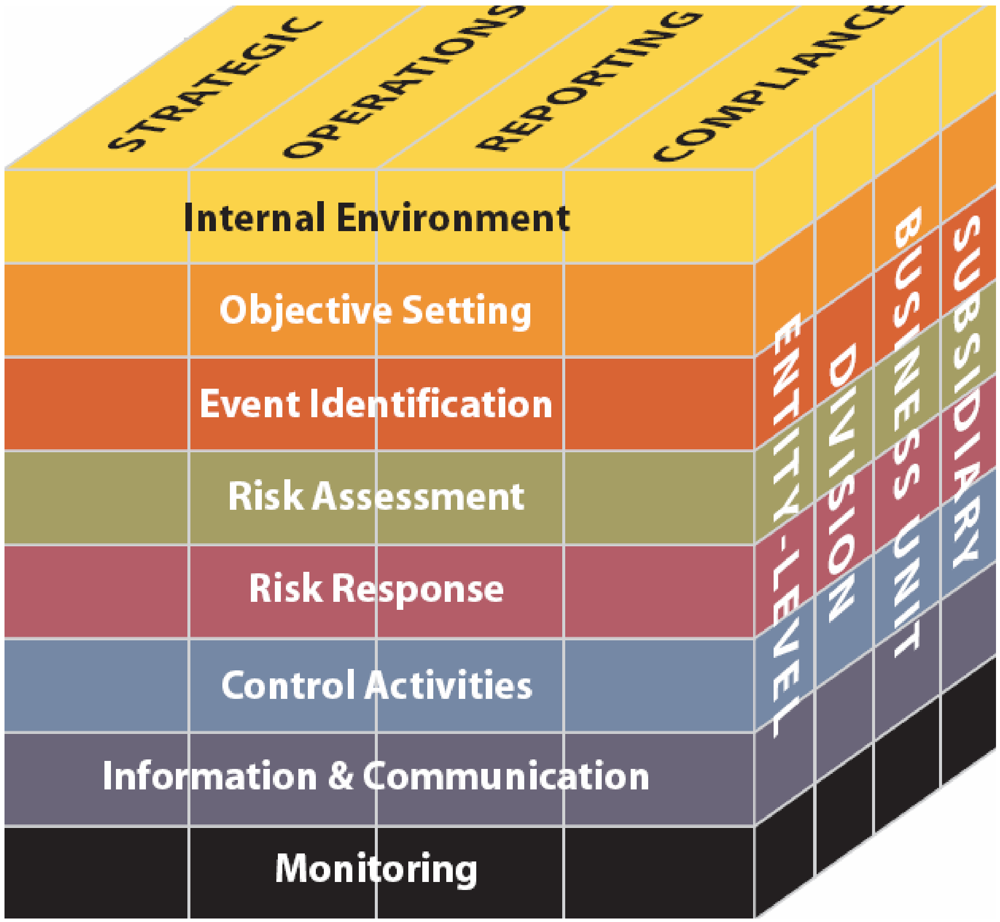
- Casualty Actuarial Society (CAS) Framework
- Committee of Sponsoring Organizations of the Treadway Commission (COSO) Framework

CAS Framework

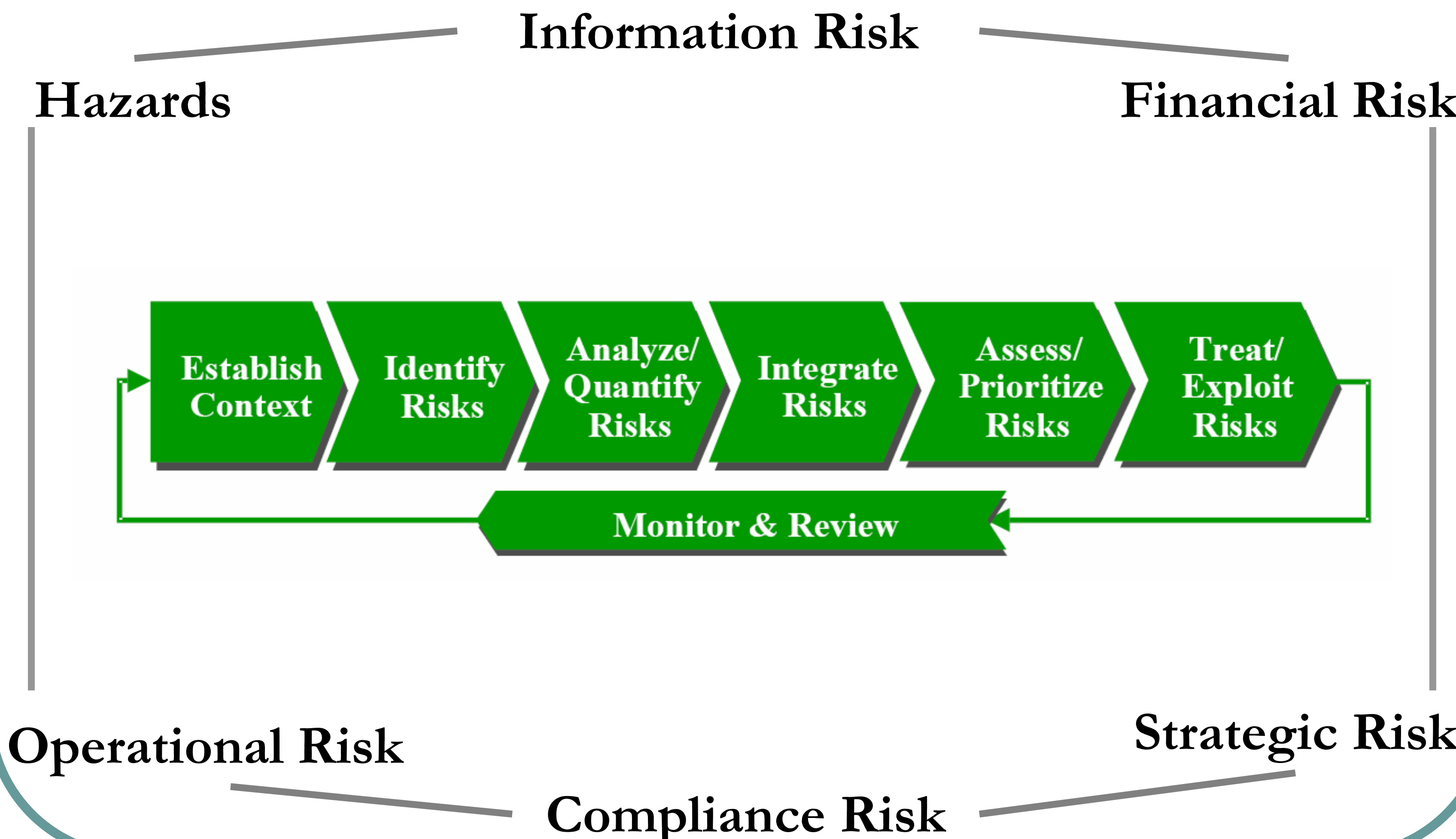
Hazards — Financial Risk

Operational Risk — Strategic Risk

COSO Framework



Merging CAS and COSO Models



Risk Categories

Hazards

- Fire
- Tornadoes
- Storms
- Hurricanes
- Earthquakes
- Terrorism
- Injuries to Employees and Third Parties

Financial Risk

- Adverse movement in exchange rates
- Adverse movement in interest rates
- Adverse movement in price and costs
- Credit Risk
- Liquidity Risk
- Bankruptcy Risk

Operational Risk

- Employee fraud
- Labor relations
- Production breakdowns
- Supply chain problems
- Problems in distribution
- Product quality issues
- Physical safety and security

Strategic Risk

- Fluctuations in demand
- Competitors entry / rivalry
- Increase in intensity of competition
- Technological advances
- Social changes having an adverse impact on the business
- Economic cycles
- Adverse legislation

Information Risk

- Incorrect information leading to incorrect decision making
- Unavailability of required information
- Unauthorized access to confidential information by competitors
- Malicious attacks
- Cyber Crime
- Loss of Claims / lawsuits by the parties whom confidential information is disclosed

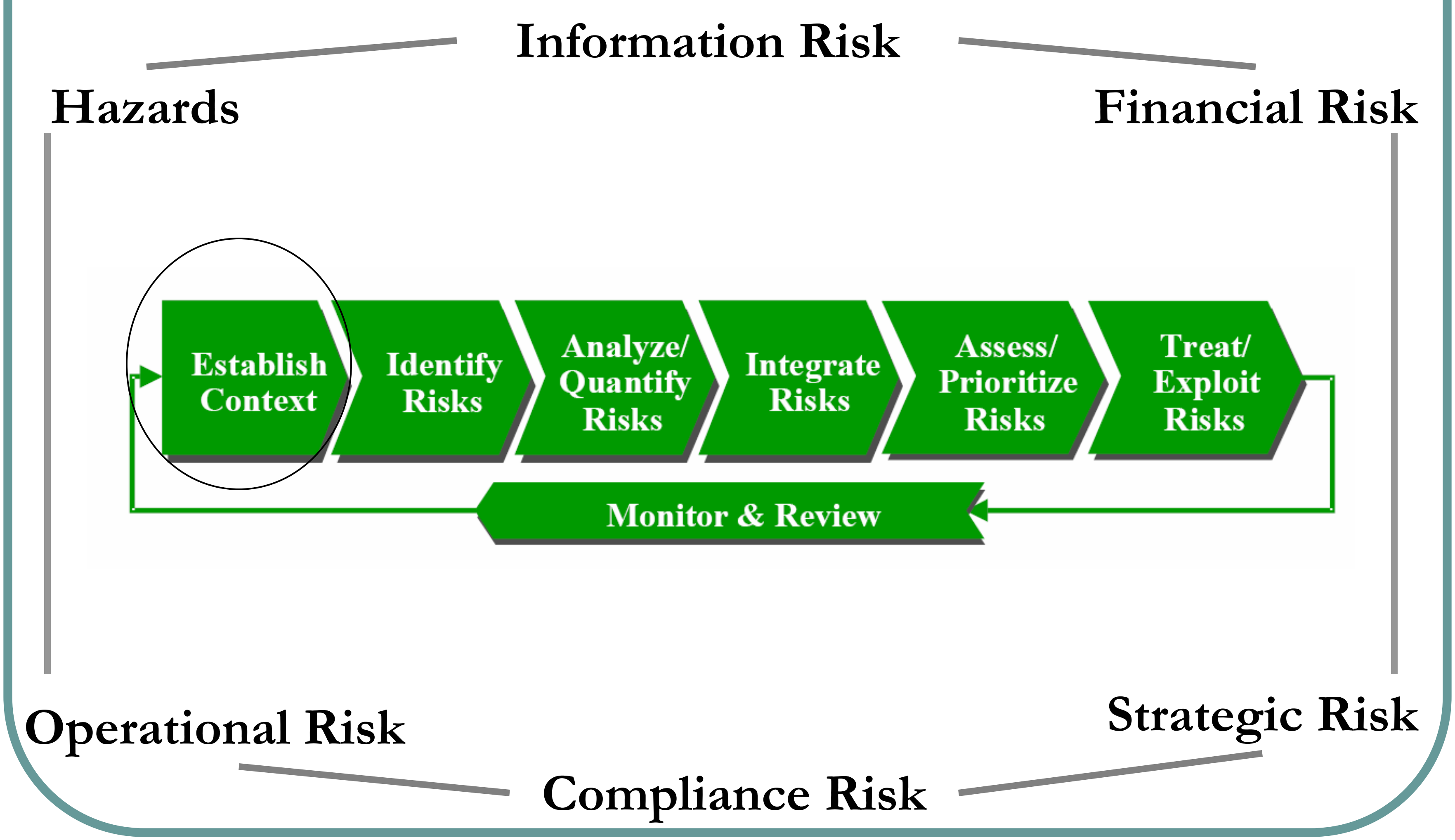
Compliance Risk

- Penalties and fines
- Reputation losses
- Claims by third parties
- Lawsuits
- Lack of understanding the law
- Inability to comply with a law or standard
- Losing patents / legal rights

Implementing ERM

Step 1: Establish Context

The Conceptual Framework



Establish Context

- Define the relationship of organization with its external and internal environment
- Perform SWOT Analysis
- Identify stakeholders
- Understand organization’s objectives and strategies
- Identify Key Performance Indicators (KPIs)
- Identify relevant key risk categories
- Identify existing risk management practices
- Determine the **“Risk Appetite”** of management

SWOT Analysis

	Positive Risk	**Negative Risk**
Internal	Strengths	Weaknesses
External	Opportunities	Threats

SWOT Analysis – An example

Positive risk	**Strengths** • Our tradespeople are exceptionally skilled • We have excellent relationships with our existing customers • Our work is considered high quality and our service reliable.	**Weaknesses** • Our tools of trade are second hand and may be unreliable • Ageing workforce • Limited familiarity with new technology.	Negative risk
	Opportunities • The only other plumber in town wants to retire • A new industry development is currently tendering to outsource trade services.	**Threats** • Somebody from out of town might buy retiring plumber's business • Another business may start up in town • Difficulties in recruiting new staff due to skill shortages • Loss of an existing employee leaving the business unable to cope with workload.	

Stakeholders Analysis

- Shareholders
- Potential Investors
- Management
- Employees
- Creditors / Bankers
- Government
- General Public

Requirements of all stakeholder groups with respect to risk management

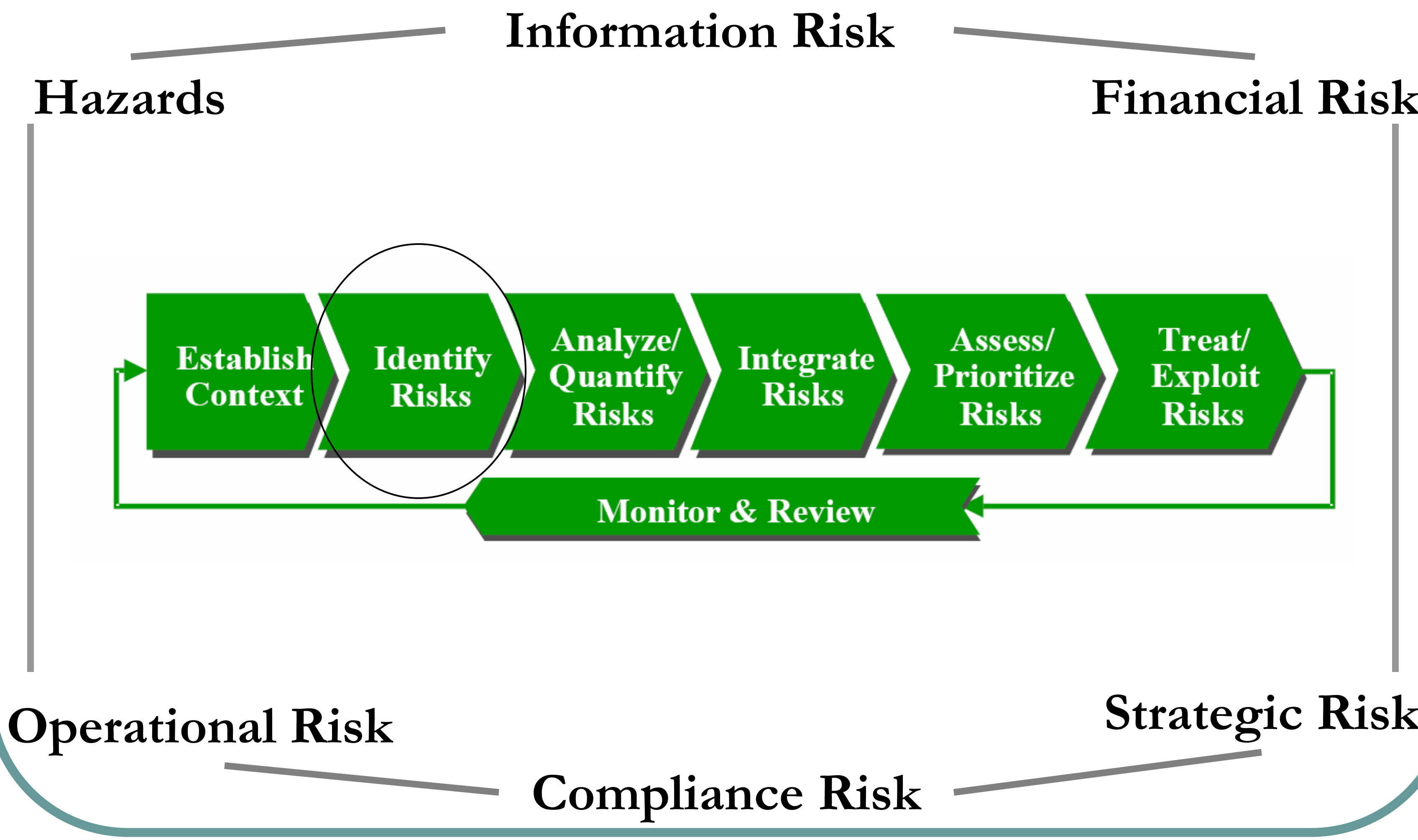
Key Performance Indicators

- Return on Capital Employed
- Net Profit of each division
- Customer Satisfaction Index
- % of Sales Returns
- Current Ratio
- Financial and Operating Leverage
- HR Training Hours

Implementing ERM

Step 2: Identify Risk

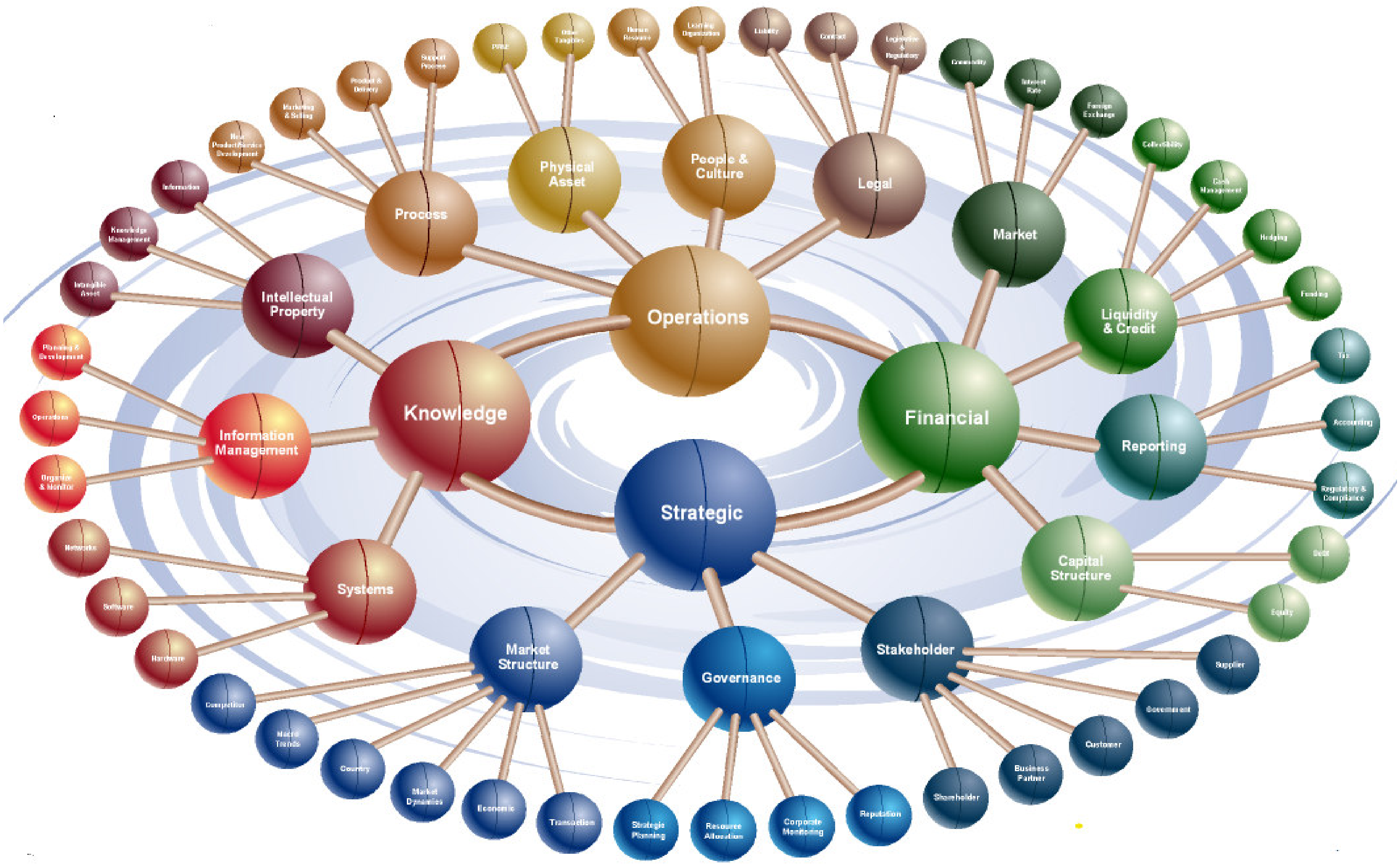
The Conceptual Framework



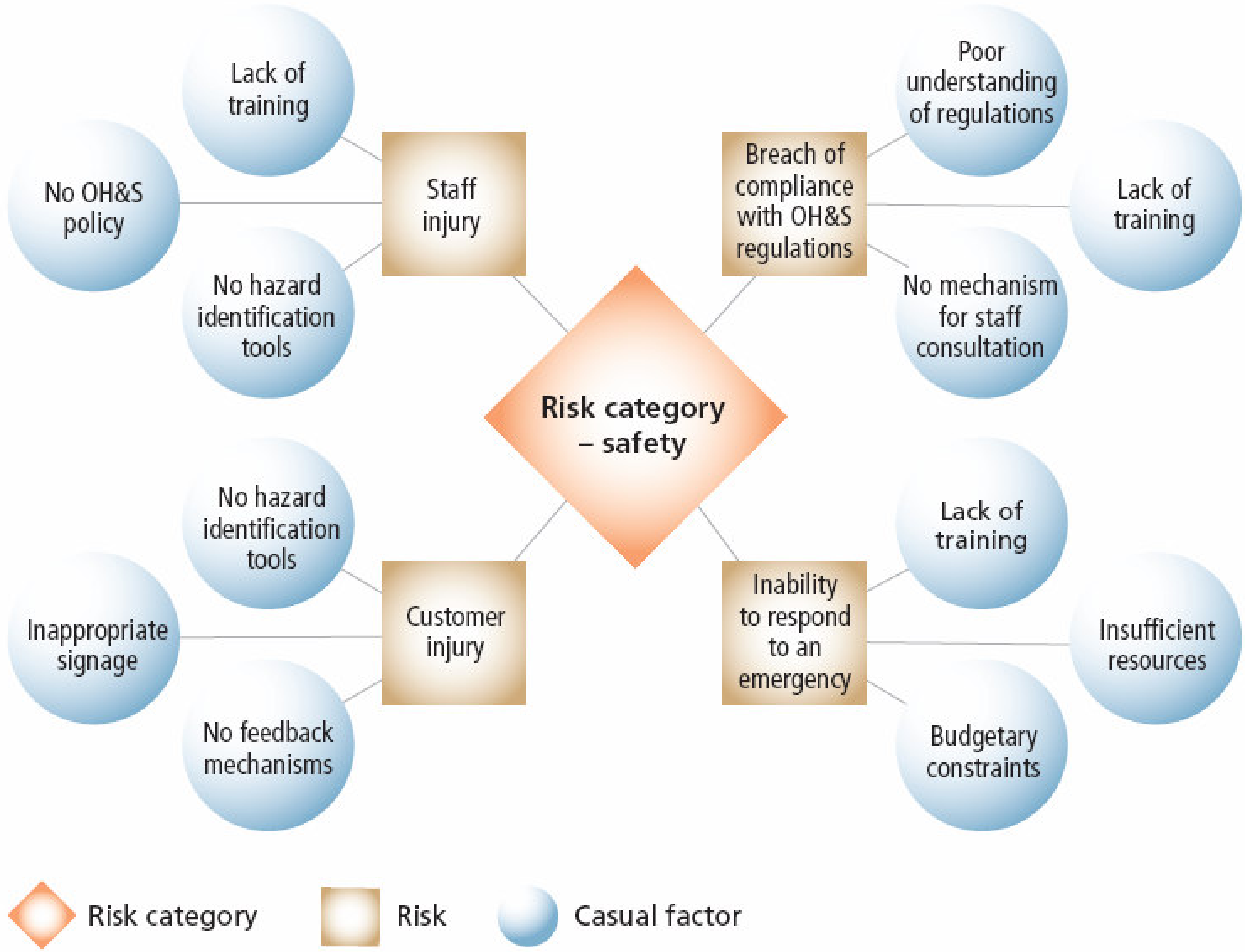
How to identify risks?

- Perform brainstorming sessions
- Perform risk surveys
- Conduct risk workshops
- Review and discuss internal audit reports
- Review and discuss reports of other assurance groups e.g. health & safety, quality assurance, security management etc.

Developing the Risk Universe



Developing the Risk Universe



Developing the Risk Register

	Risk dimension: security	Risk dimension: financial	Risk dimension: legal/compliance
Serial no.	1	2	3
Risk description	Cybercrime, including virus damage, identity theft, spyware, general fraud	Costs associated with online transactions outweigh benefits associated with initiative	Breach of regulations within e-business legislation
Impact			
Consequence			
Likelihood			
Level of risk			
Risk priority			
Treatment options			

Implementing ERM

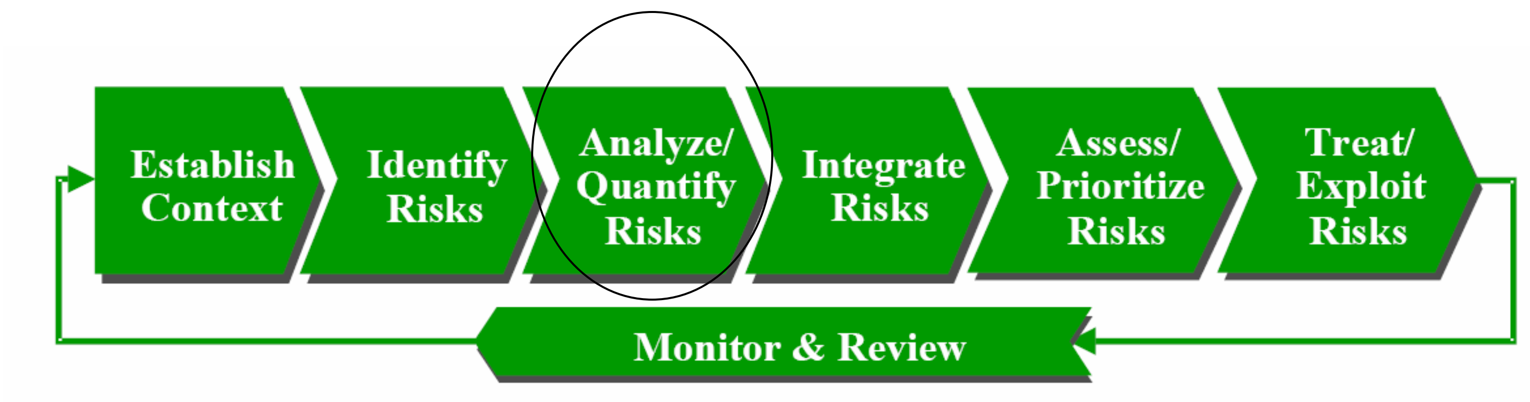
Step 3: Analyze / Quantify Risks

The Conceptual Framework

Information Risk

Hazards

Financial Risk



Operational Risk

Strategic Risk

Compliance Risk

Risk Measurement

Overall Risk = Likelihood x Magnitude

		Magnitude	
		High	Low
Likelihood	High	Extreme	Moderate
	Low	High	Low

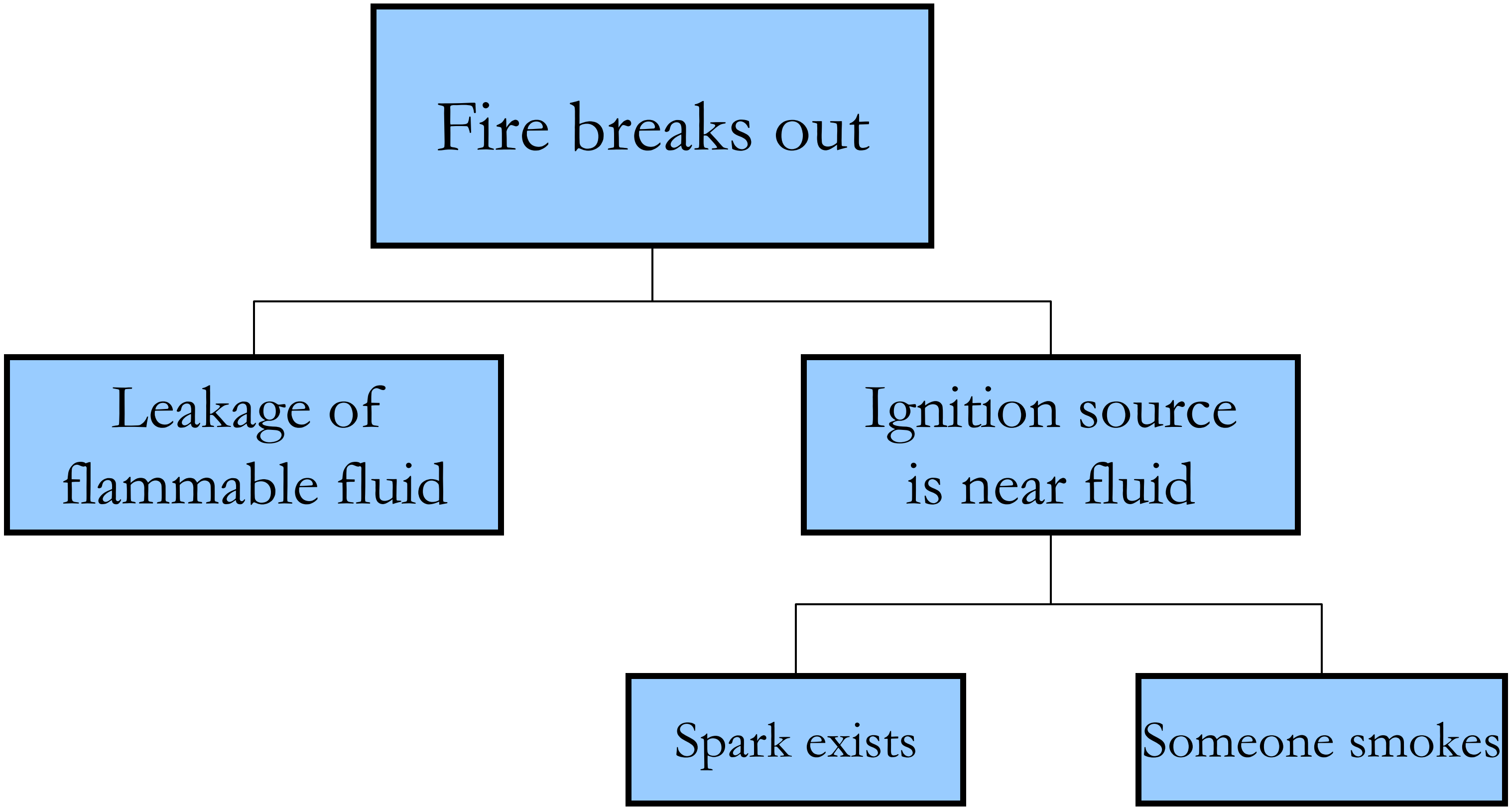
Risk Analysis Tools

- Qualitative Risk Analysis
- Fault Tree Analysis
- Probability Distribution (for Likelihood)
- Maximum Loss Estimation (for Magnitude)
- Risk and Control Matrix

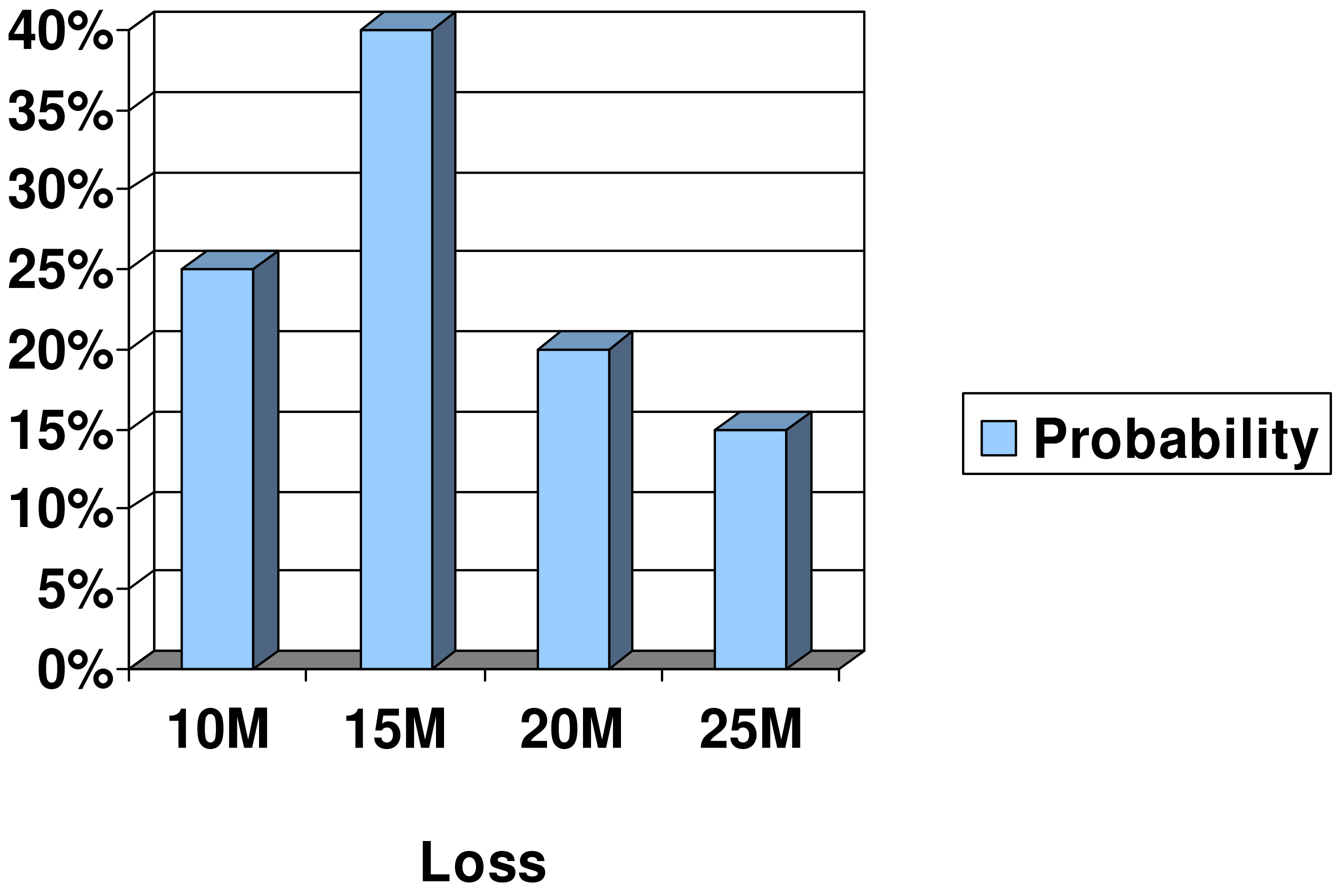
Qualitative Risk Analysis

	LEGEND	Extreme	High	Medium	Low					
	Consequence					Likelihood				
						Almost certain	Likely	Possible	Unlikely	Rare
	Commercial	Finance	Security	Safety	Legal and regulatory compliance	Almost certain to occur at some time.	Known to have been present or occurred/ likely to occur.	Not likely to occur in normal situations.	Unlikely to occur.	Has not occurred in the past and requires unusual circumstances to occur.
Significant	Significant loss of market share resulting in 10–30% loss of current clients and no increase in new clients over a three-month period.	Loss > 30% of total income or budget.	Fraud resulting in financial loss. Staff threat resulting in serious injury requiring hospitalisation. Significant reputation damage.	Death or multiple injuries requiring hospitalisation.	Investigation by authority and significant penalty awarded. Very serious litigation, including class actions. Closure of business.	Extreme	Extreme	Extreme	High	High
Major	Major loss of market share resulting in <10% loss of current clients. No new clients for 1–3 months.	Loss of 20–30% of total income or budget.	Fraud resulting in financial loss. Staff threat resulting in serious injury requiring hospitalisation. Some reputation damage.	Major injury requiring hospitalisation.	Major breach with potential major penalty and/or investigation and prosecution by authority. Major litigation. Future of the business threatened.	Extreme	Extreme	High	High	Medium
Moderate	Loss of market share. Current clients are retained but no new clients for 1–3 months.	Loss of 10–20% of total income or budget.	Staff threat resulting in some injury but no hospitalisation required. Minor reputation damage.	Minor injury – first aid required.	Serious breach with investigation by or report to authority. Moderate penalty possible.	High	High	Medium	Medium	Low
Minor	Minor loss of market share. Current clients are retained but new clients have visibly decreased (50% of normal uptake).	Loss < 10% of income or total budget.	Staff threatened, but no injury. No reputation damage.	No injury.	Low-level legal issue. Penalty or prosecution unlikely.	High	Medium	Medium	Low	Low

Fault Tree Analysis



Probability Distribution



Maximum Loss Estimation

Risk	Maximum Possible Impact	Estimated Loss in $ million
Earthquake	Entire factory will be destroyed	45,000
Sensitive information hacked	Lawsuits, advantage gained by competitors	15,300
Terrorist attack	Some facilities will be damaged	5,000
Competitor launched new product	Market share will be lost by 30%	3,000

Risk & Control Matrix

Example "What Can Go Wrong" Questions	Accounts payable subledger is reconciled to the general ledger.	Accounts payable subledger/aging is reviewed.	Accrual for goods received not invoiced is reviewed.	Advanced bookings are reviewed and approved by executive management.	Classification of PP&E versus expense is reviewed and approved by appropriate personnel.	Costs by department/division/etc. are compared to budget.	Debit memos are matched with vendor's credit memos.	Debit memos require approval.	Exceptions to 3-way match (purchase order, receiving report and invoice) are investigated daily.	Inventory count crews are supervised.	Movement of inventories during physical counts is controlled.	Out-of-balance reports are reviewed.	Overrides of validation edits are reported, reviewed and authoriz	Significant debit balances in individual vendor account investigated.
What ensures that coding of purchases is correct?					IT	IT							IT	
What ensures that payables for drop-shipped goods are recorded in a timely manner?														
What ensures that proper cut-off information is generated and used for purchases?				IT					IT	P	P			

Implementing ERM

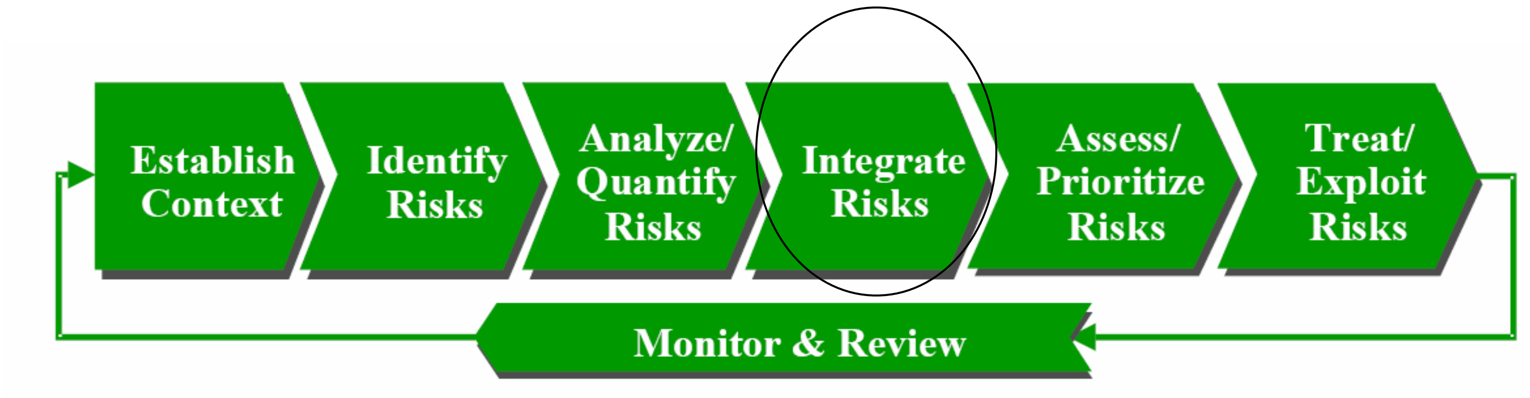
Step 4: Integrate Risks

The Conceptual Framework

Information Risk

Hazards

Financial Risk



Operational Risk

Strategic Risk

Compliance Risk

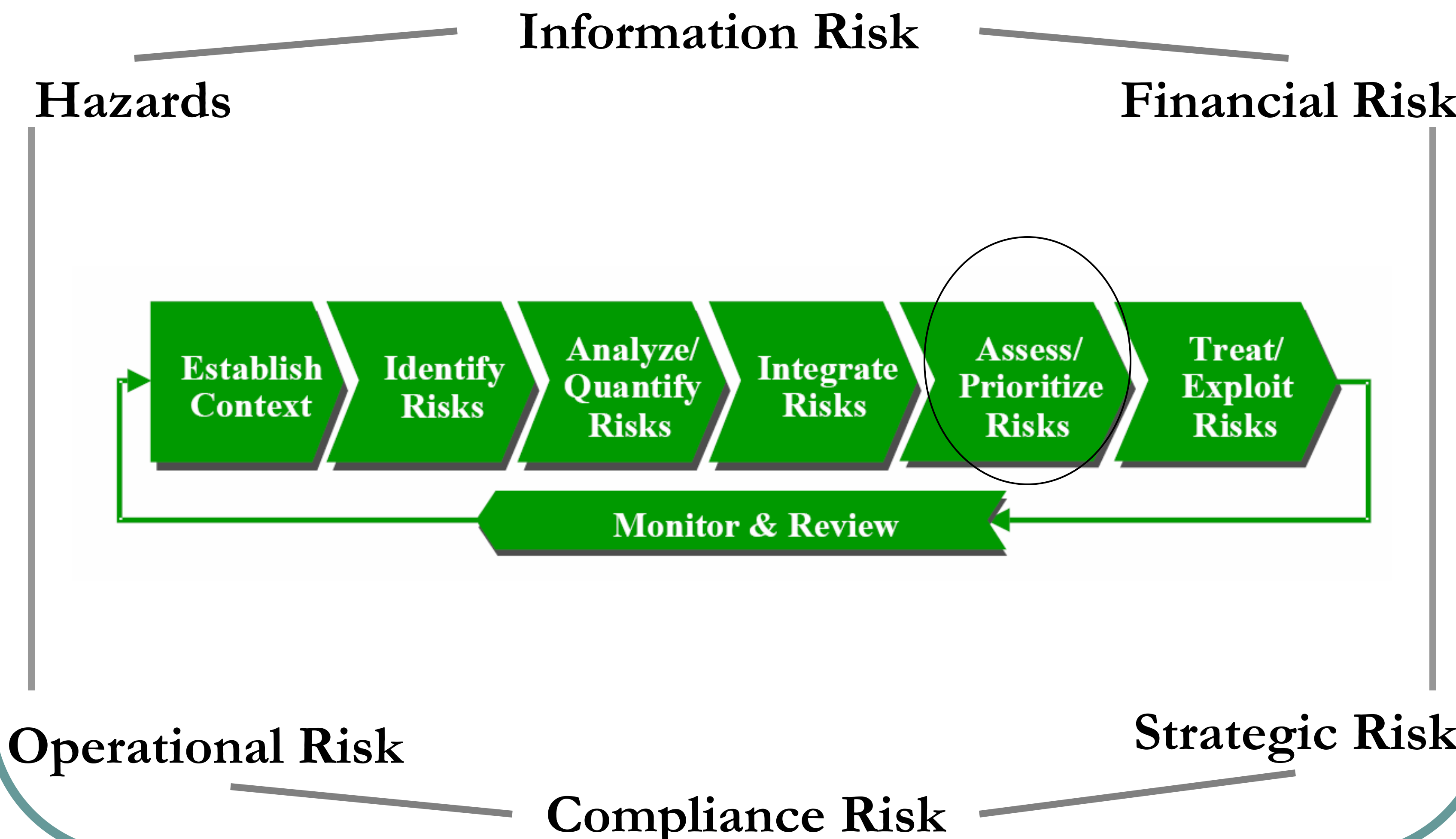
Integrate Risks

- Consolidate all identified risks
- Consolidate the likelihood and overall impact of each risk on Key Performance Indicators (KPIs)
- Align risks with business objectives

Implementing ERM

Step 5: Assess / Prioritize Risks

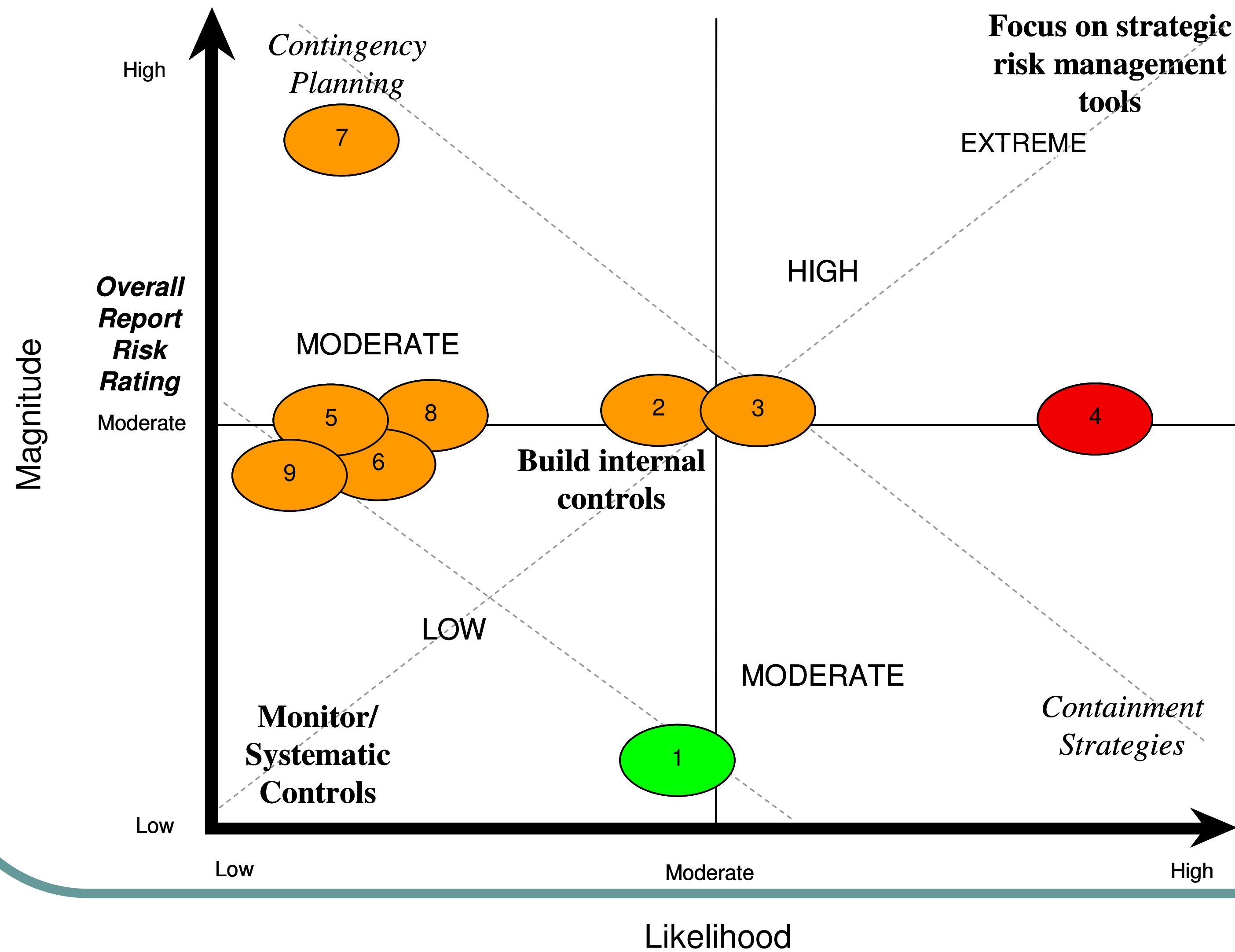
The Conceptual Framework



Risk Prioritization

	LEGEND	Extreme	High	Medium	Low					
	Consequence					**Likelihood**				
						Almost certain	**Likely**	**Possible**	**Unlikely**	**Rare**
	Commercial	**Finance**	**Security**	**Safety**	**Legal and regulatory compliance**	Almost certain to occur at some time.	Known to have been present or occurred/ likely to occur.	Not likely to occur in normal situations.	Unlikely to occur.	Has not occurred in the past and requires unusual circumstances to occur.
Significant	Significant loss of market share resulting in 10–30% loss of current clients and no increase in new clients over a three-month period.	Loss > 30% of total income or budget.	Fraud resulting in financial loss. Staff threat resulting in serious injury requiring hospitalisation. Significant reputation damage.	Death or multiple injuries requiring hospitalisation.	Investigation by authority and significant penalty awarded. Very serious litigation, including class actions. Closure of business.	Extreme	Extreme	Extreme	High	High
Major	Major loss of market share resulting in <10% loss of current clients. No new clients for 1–3 months.	Loss of 20–30% of total income or budget.	Fraud resulting in financial loss. Staff threat resulting in serious injury requiring hospitalisation. Some reputation damage.	Major injury requiring hospitalisation.	Major breach with potential major penalty and/or investigation and prosecution by authority. Major litigation. Future of the business threatened.	Extreme	Extreme	High	High	Medium
Moderate	Loss of market share. Current clients are retained but no new clients for 1–3 months.	Loss of 10–20% of total income or budget.	Staff threat resulting in some injury but no hospitalisation required. Minor reputation damage.	Minor injury – first aid required.	Serious breach with investigation by or report to authority. Moderate penalty possible.	High	High	Medium	Medium	Low
Minor	Minor loss of market share. Current clients are retained but new clients have visibly decreased (50% of normal uptake).	Loss < 10% of income or total budget.	Staff threatened, but no injury. No reputation damage.	No injury.	Low-level legal issue. Penalty or prosecution unlikely.	High	Medium	Medium	Low	Low

Risk Prioritization



Implementing ERM

Step 6: Treat / Exploit Risks

The Conceptual Framework

Information Risk

Hazards

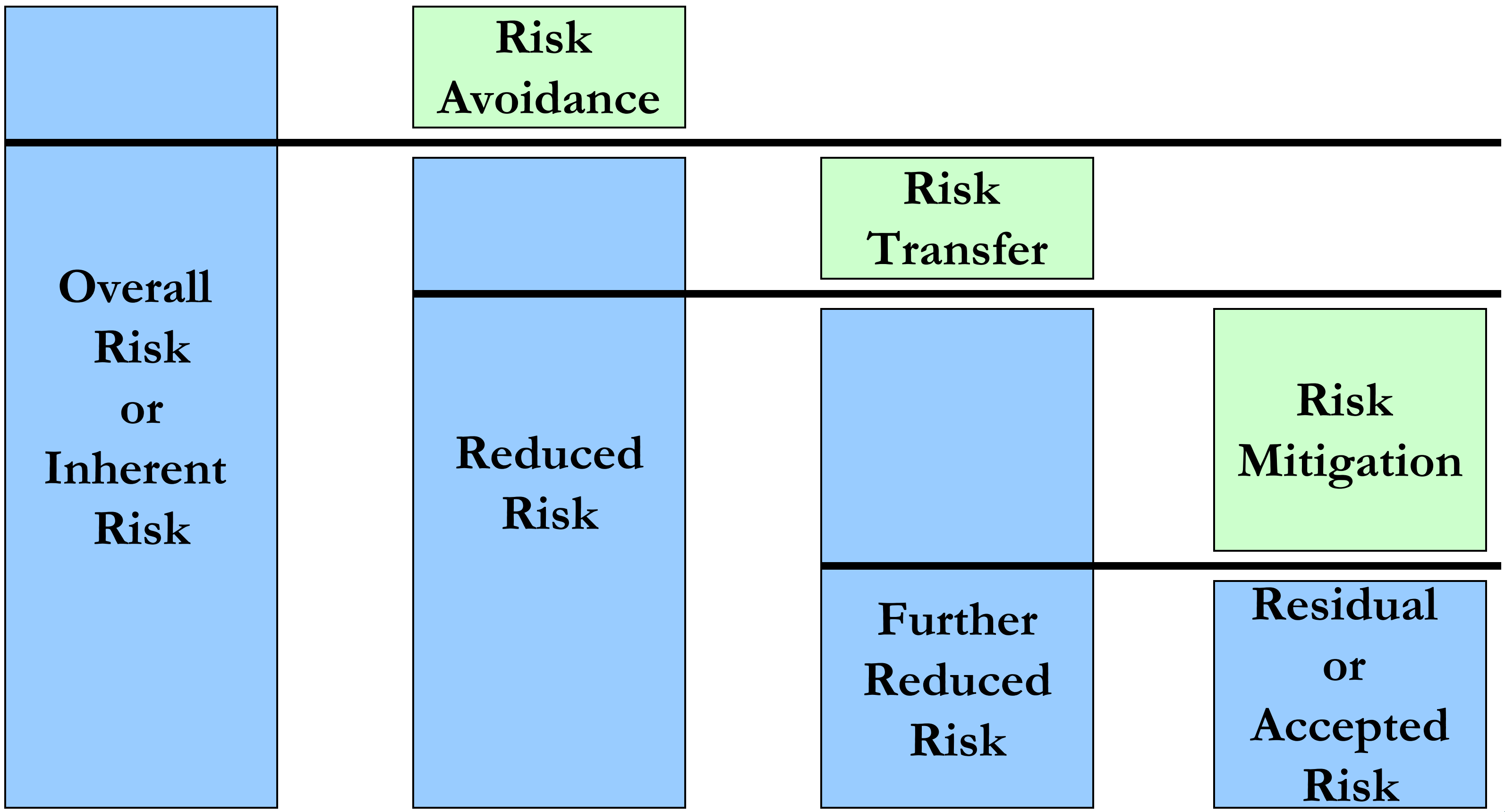
Financial Risk

Operational Risk

Strategic Risk

Compliance Risk

Risk Treatment Strategies



Risk Treatment Tools

- **Risk Avoidance:** Quit the activity which results in exposure to risks e.g. avoid dealing in cash or foreign currency
- **Risk Transfer:** Insurance, Factoring
- **Risk Mitigation:** Internal control, Hedging, Credit Management, Business Continuity Planning etc.
- **Risk Acceptance:** Exploit the risk to get benefit

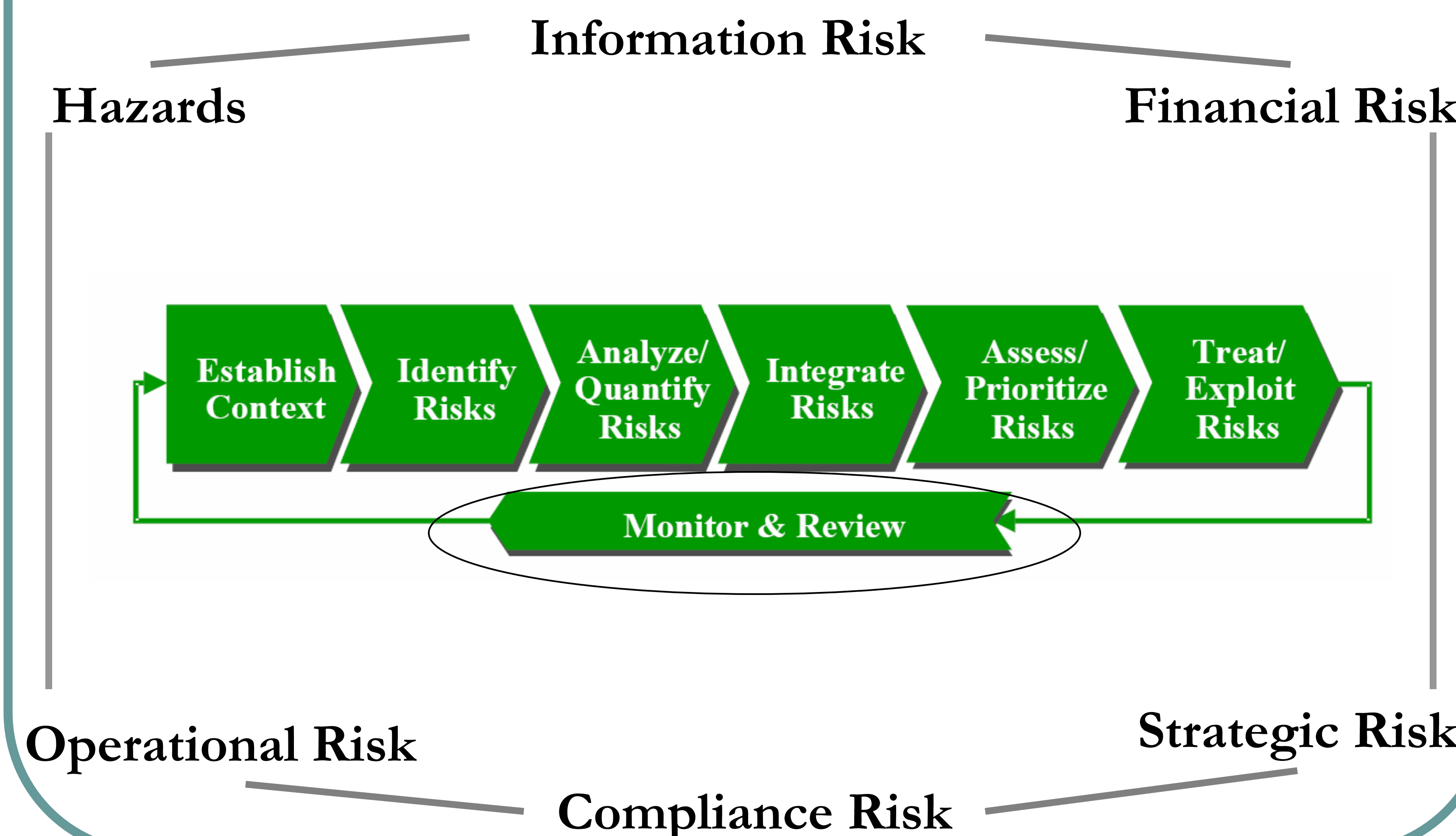
The Complete Risk Register

	Risk dimension: security	Risk dimension: financial	Risk dimension: legal/compliance
Serial no.	1	2	3
Risk description	Cybercrime, including virus damage, identity theft, spyware, general fraud	Costs associated with online transactions outweigh benefits associated with initiative	Breach of regulations within e-business legislation
Impact	Direct financial loss, reputation damage, equipment damage, system unavailability	Direct financial loss due to increased fees Customer loss due to increased costs	Possible fine and/or legal prosecution
Consequence	Significant	Moderate	Moderate
Likelihood	Likely	Likely	Possible
Level of risk	Extreme	High	Moderate
Risk priority	1	2	3
Treatment options	1. Update anti-virus software and check firewall viability 2. Review requirements to ensure secure online banking 3. Develop and test security policies 4. Develop disaster recovery plan	Develop business case to identify impact of increased fees	1. Review all legislation 2. Consult solicitor to seek advice 3. Develop and test compliance policies and procedures

Implementing ERM

Step 7: Monitor & Review Risks

The Conceptual Framework



Risk Monitoring Tools

- Key Risk Indicators (KRIs)
- Risk Governance, Policies & Procedures
- Establishing the Risk Management Department
- Risk Register
- Risk Reporting
- Internal Audit

Develop Key Risk Indicators (KRIs)

- Market share
- Number of direct competitors
- Loss caused by frauds during the period
- Total exposure to foreign exchange risk
- Number of significant internal control weaknesses reported
- % of price fluctuation
- Bad debts written off
- Avoidable losses during the period

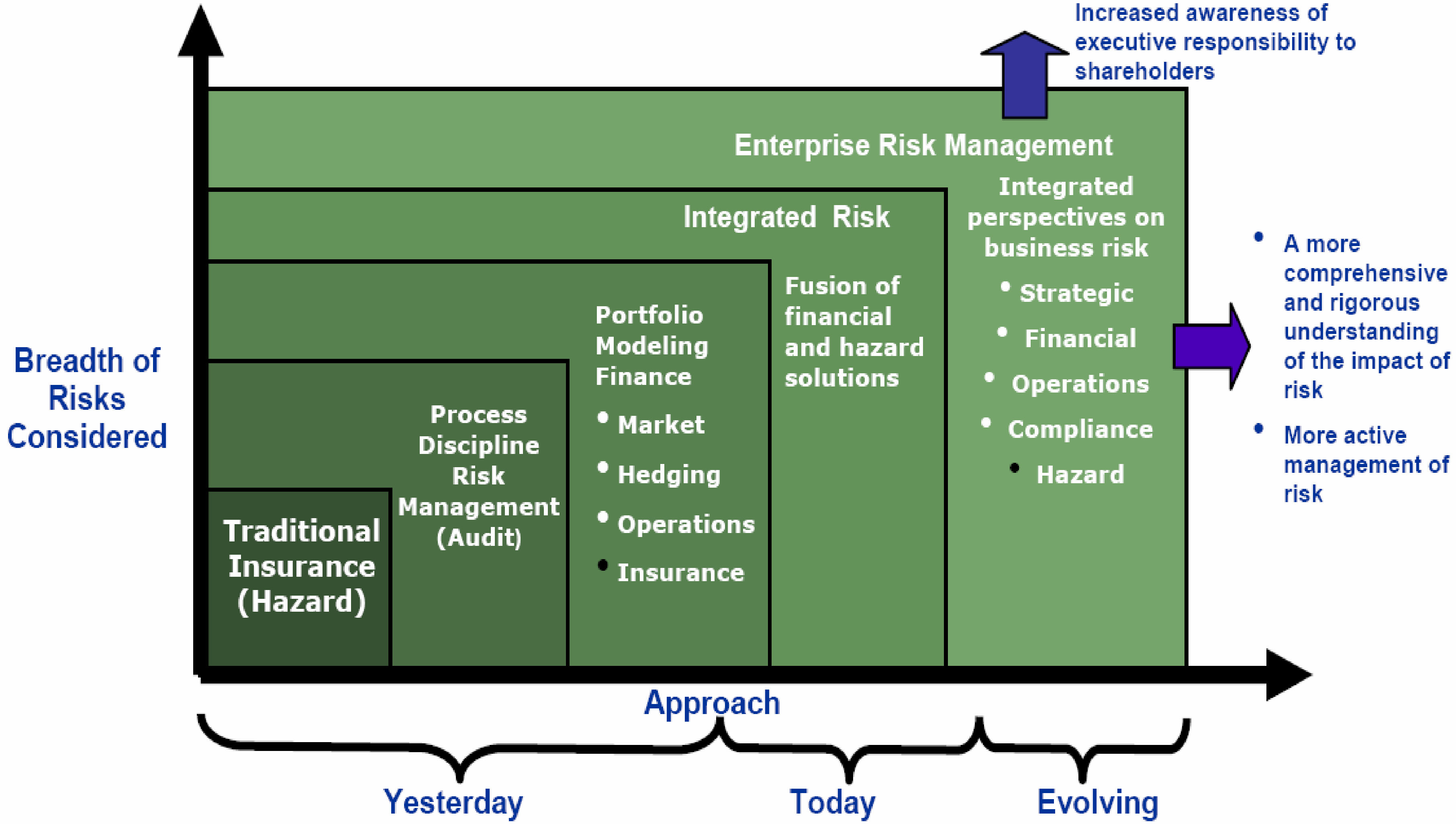
ERM: Other Issues

- **Why ERM?**
- **ERM Maturity Model**
- **Key Factors for Success of ERM**

Why ERM?????

- Reduced losses
- Enhanced business processes
- Improved reputation
- Enhanced control over the business
- Reduced penalties
- Secured information
- Effective use of technology
- Fewer surprises
- Effective decision making
- Improved corporate governance

ERM Maturity Model



ERM Maturity Model

The Risk Intelligent Enterprise Maturity Model

How capable is your company today? How capable does it need to be? Every industry, company and division is probably at a different stage of development. Where should they be and how do they get there?

Key Factors for ERM Success

- **Agreed risk strategy:** The audit committee and management must provide guidance on the appropriate strategy and approach to risk management aligned to the organisational structure.
- **Clear governance framework:** The audit committee will usually delegate day-to-day governance through an oversight structure that includes a Chief Risk Officer.
- **Efficient risk management processes:** The organisation needs firm procedures for assessing and continuously monitoring risks on an enterprise wide basis.
- **Appropriate technology:** Effective systems providing access to information about risk identification, assessment and solutions to support the risk management process.
- **Co-ordination of risk management functions:** Integrated risk functions embedded within the business to leverage expertise across the entire organisation.
- **The right culture and capability:** Everyone in organization must be attuned to the risk culture and performance measurements must be risk based.

Thank you