

# Surviving and Thriving In Uncertainty: Creating the Risk Intelligent Enterprise

Angela Bryant

Leader, Enterprise Risk Management Centre  
of Excellence, Deloitte & Touche (M.E.)



# Agenda

The Risk Intelligence Imperative

Fundamentals of ERM

Our Risk Intelligence Point of View

Getting Started: A “How to” Guide

Overview of Leading Practices

Final Thoughts



# The Risk Intelligence Imperative

*“Life short, art long, opportunity  
fleeting, experience misleading,  
judgment difficult”*

Hippocrates, 400 B.C.

# The Risk Intelligence Imperative

...However, the *drivers* of risk are changing

- Profile of risks affecting organizations today is different than risks impacting organizations a decade ago
- Nature of business transactions (e.g. derivatives, hedging, etc.)
- Changes in technology
- Globalization
- Internal and external events
- High impact and low likelihood events affecting organizations in significant ways overnight



# The Risk Intelligence Imperative

... And the Board's interest in ERM is *evolving*

- Public accountability
- Regulatory pressures
- Stakeholder demands
- Cost of capital
- The Internet and social media



# The Risk Intelligence Imperative

## ERM is on the agenda for many reasons:

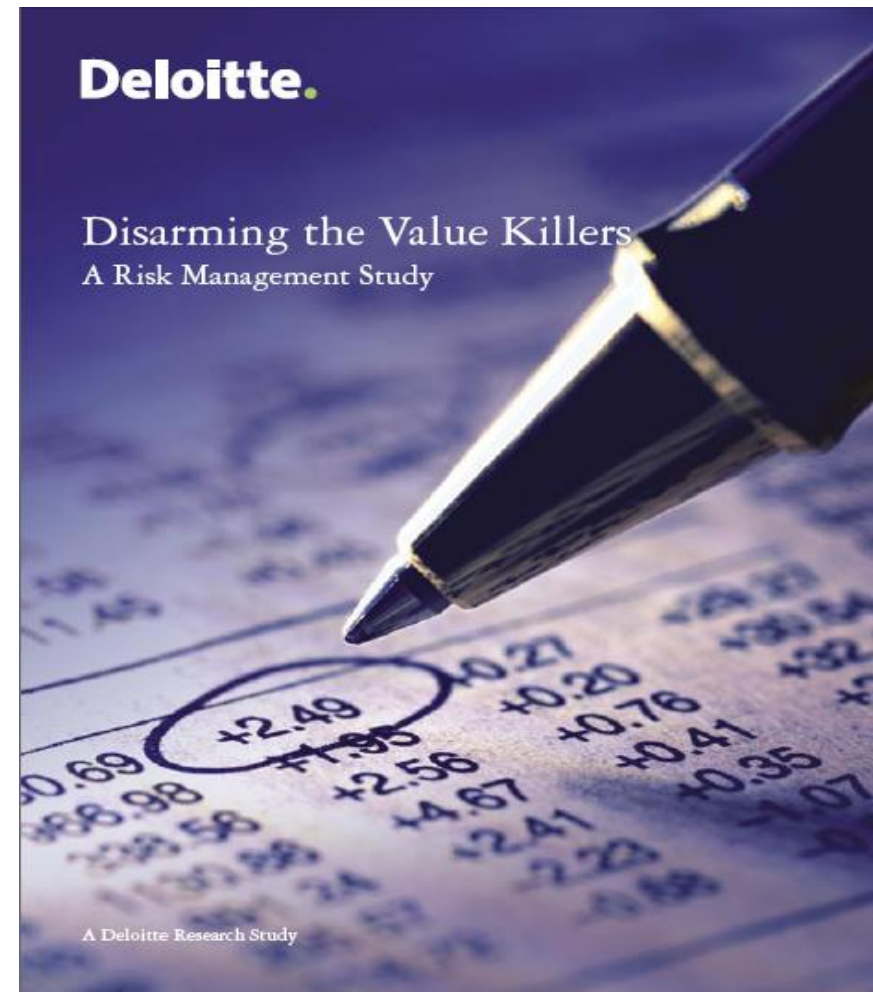
- Risk has never been a hotter topic with boards and senior executives
- No one is immune
- We have seen extraordinary periods of uncertainty and turbulence
- Speed of onset is much, much faster
- Many continue to struggle with “what went wrong?” and want answers
- High profile scandals / disasters are daily front page news, encouraging regulators to enforce risk management activities
- Financial analysts and rating agencies are increasingly interested in a company’s ERM capability; Moody’s and S&P have ERM listed as one of their evaluation criteria
- Enhanced disclosure requirements and increase in transparency are imminent
- In the GCC region, corporate governance is becoming mandatory for financial institutions and listed companies; risk management will follow
- Risk is personal

# The Risk Intelligence Imperative

## The Value Killers

- Almost 50% of global 1000 companies lost 20% or more in share price in less than a month during the past 10 years—some never recovered.
- Almost all organizations have risk management located in specialist silos.
- 80% of losses were due to interaction of multiple risks.
- Most major losses were the result of a series of high impact but low likelihood events.

**Source: Disarming the Value Killers:  
A Risk Management Study, Deloitte Research.**



# The Risk Intelligence Imperative

## Key questions to ask along the risk intelligence path:

- How prepared is our institution for the risks and opportunities that inevitably lie ahead?
- How can we find the unexpected before it finds us?
- How can we continue to grow our brand, improve our revenue, operating margins, and asset productivity despite uncertainty and turbulence?
- How do we effectively link strategy and risk management?
- How should we define our risk appetite and risk tolerances?



# The Risk Intelligence Imperative

## Continued:

- What are the best ways for boards to oversee that enterprise value and risk are appropriately managed?
- What is the most appropriate balance of roles and responsibilities between the board and executive (risk oversight versus risk management)?
- How can the board get reassurance that executive's reports about known and emerging risk exposures are reliable?
- How do we build consideration of risk into the way we make decisions?
- What further, if anything, should the board and executive practically do to improve our chances of survival and success?



# The Fundamentals of ERM

# What is Risk?

The correct definition of risk accommodates both the **protection of existing assets** and **the enhancement of future growth opportunities**:

*The potential for loss—or diminished opportunity for gain—caused by events that can adversely affect the achievement of a company's objectives.*

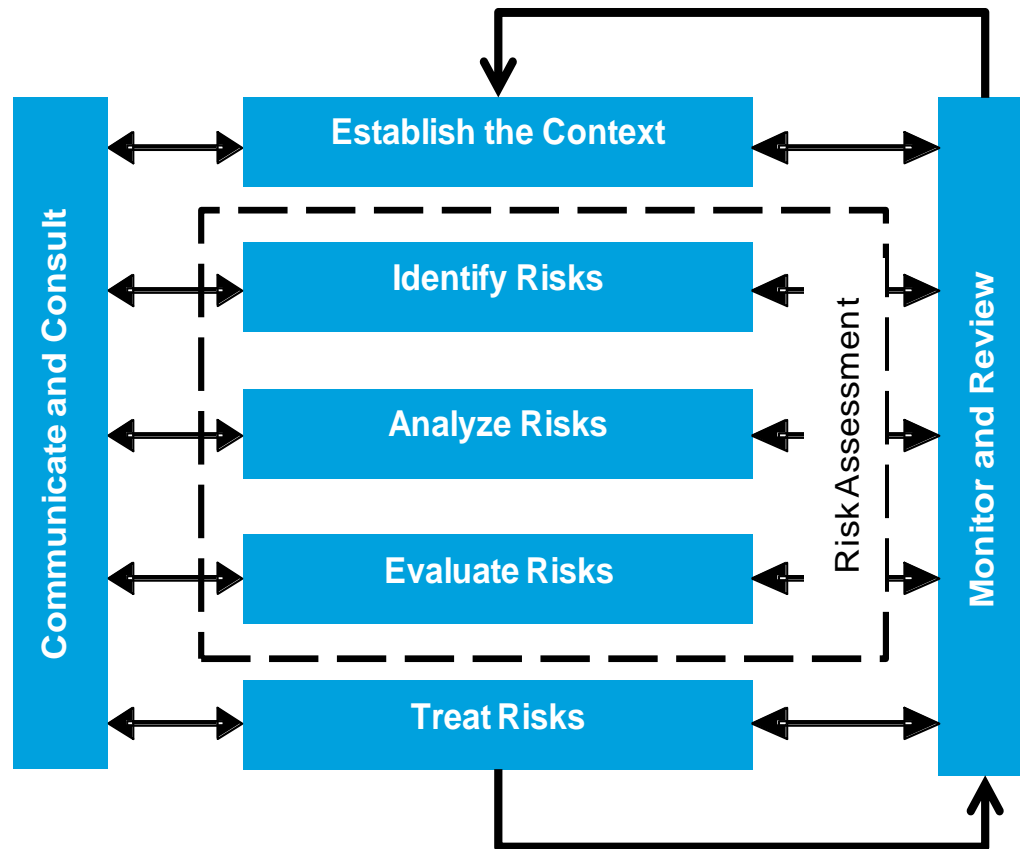
Risk Intelligent Enterprises consider the ability to anticipate and react to market opportunities to be as important as readiness for a potentially devastating business disruption.

Risk Intelligence is:

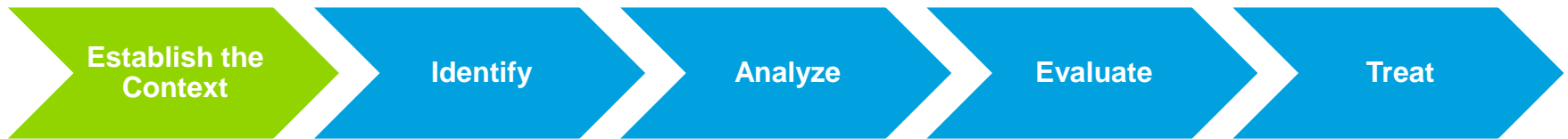
- A systematic capability to identify, measure, and respond to risks across an organization
- Understanding and managing the full spectrum of risks
- Understanding the interaction of different risks
- Establishing a clear linkage to shareholder value
- Having risk management embedded as a day-to-day activity
- Identifying the linkage between silos, and leveraging the expertise within them

# Selecting an ERM Framework

A common, leading practice framework used today is ISO 31000:2009, although others like COSO and CAS are also implemented. Below are the key components of ISO 31000 as an example.



# Establish the Context



Establishing the Context defines the parameters within which risks must be managed and the scope for the rest of the framework. This focuses ERM efforts on your environment, and defines the categories, criteria, and processes necessary to manage risks as a portfolio.

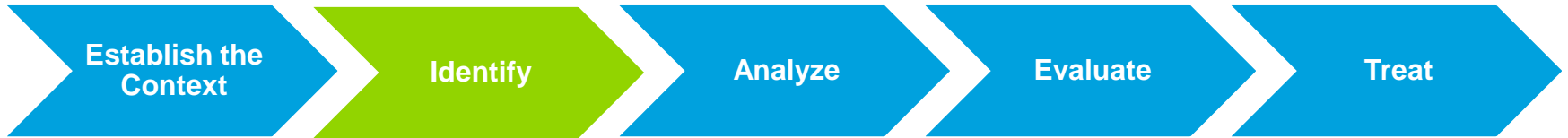
<p><b>Internal context - defines the organization</b></p>	<ul style="list-style-type: none"> <li>• Culture</li> <li>• Objectives</li> <li>• Structure</li> </ul>	<ul style="list-style-type: none"> <li>• People</li> <li>• Processes</li> <li>• Technology</li> </ul>
<p><b>External context - defines the relationship between the business and its environment</b></p>	<ul style="list-style-type: none"> <li>• Regulatory</li> <li>• Social</li> </ul>	<ul style="list-style-type: none"> <li>• Financial</li> <li>• Political</li> </ul>
<p><b>Risk management context - defines the goals of each activity, considering its costs and benefits</b></p>	<ul style="list-style-type: none"> <li>• Project objectives</li> <li>• Tasks / activities</li> <li>• Timelines</li> </ul>	<ul style="list-style-type: none"> <li>• Decisions required</li> <li>• Feasibility studies required</li> </ul>

# Establish the Context: Risk Appetite

As part of Establish the Context, the Risk Appetite is defined. It is the responsibility of the CEO and the Board to establish the Risk Appetite. The Risk Appetite Matrix is a commonly used tool to help guide you as you define your risk appetite.

	Risk Seeking	Risk Tolerant	Risk Neutral	Moderately Risk Averse	Risk Averse
<b>Philosophy towards risk taking</b>	Taking risk is considered part of company's strategy	Company takes an aggressive approach towards taking risk	Company takes a balanced approach to risk taking	Company takes a cautious approach towards taking risk	Company accepts as little risk as possible
<b>Risk return relationship</b>	Risk exposure is sacrificed in exchange for higher returns	Return objectives are given a higher priority over risk exposure	Risks and return objectives are given equal considerations	Risk management objectives are given a higher priority over returns	Higher returns are sacrificed in exchange for greater protection
<b>Preferred risk treatment approach</b>	Risk is accepted as much as regulations permit	Preference to accept or reduce risk through internal measures	No preference towards risk treatment approaches	Preference to avoid risk or transfer it to an outside party or use secondary mechanism	Those risks that can not be effectively treated or transferred are avoided
<b>Risk treatment decision criteria</b>	Minimum if any risk treatment actions are taken	Risk treatment actions are taken when a strong cost effectiveness case can be made	Risk treatment actions are made based on cost effectiveness & management priorities	Occurrence costs are given a relatively higher priority when risk treatment actions are considered	Risk treatment actions are made even though prevention cost can be greater than occurrence costs

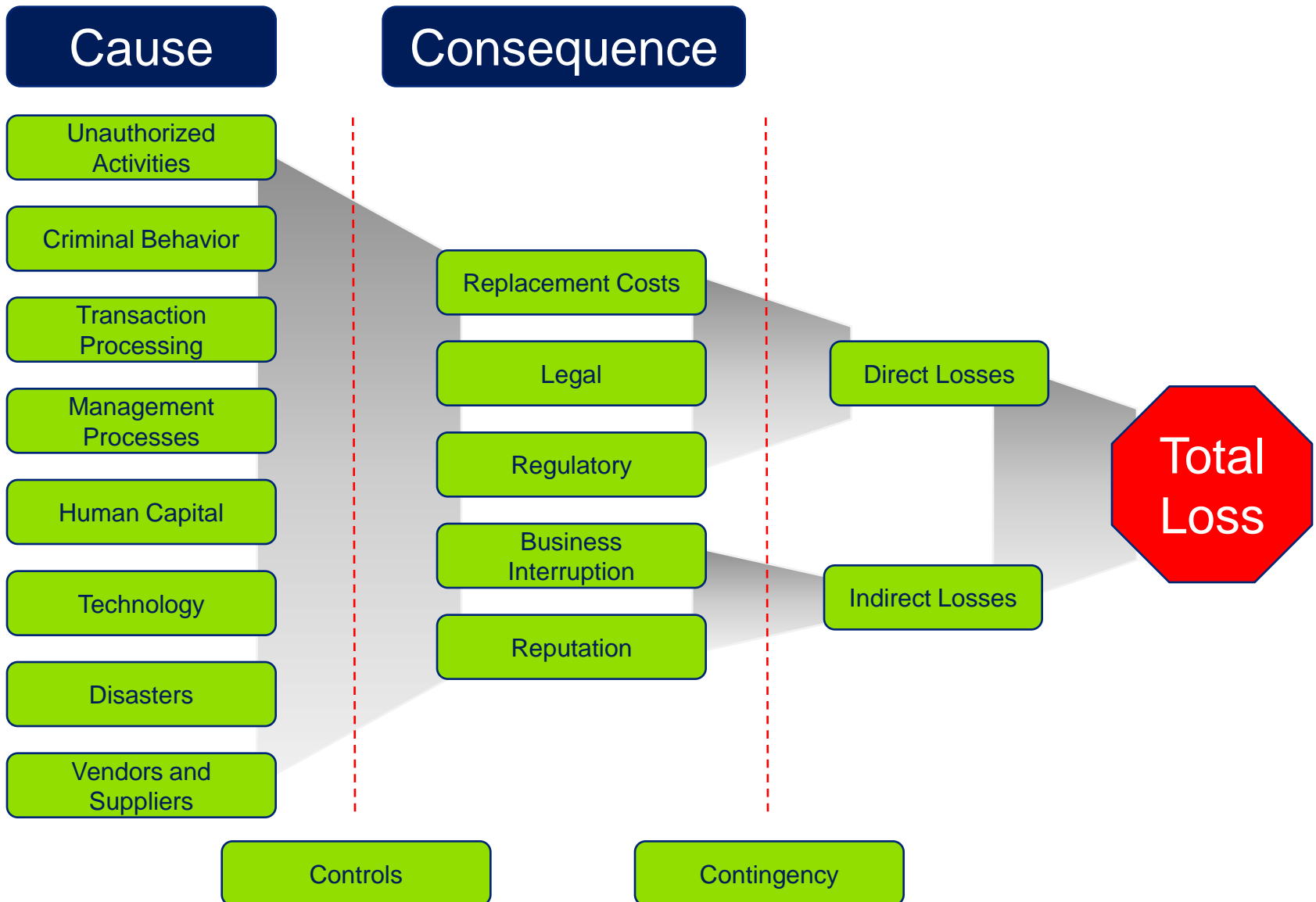
# Identify Risks



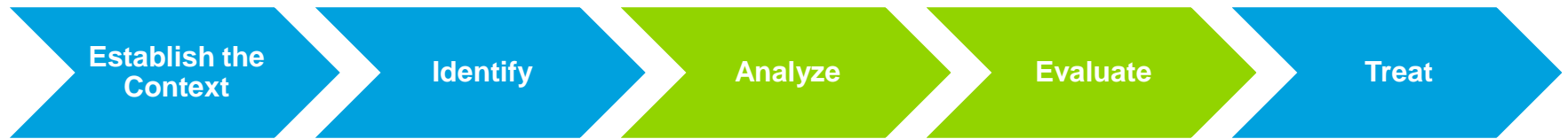
Identifying Risks and their triggers and consequences is a first step in understanding the risks that may prevent your company from achieving its objectives, its overall risk exposure, and how risks should be managed.

- ❑ Using a robust process is critical, because a risk not identified at this stage may be excluded in the Analyze phase. The following should be considered:
  - **What can happen, where and when?** Generate a list of sources of risks and events.
  - **Why and how it can happen?** Consider possible root causes and scenarios.
  - **How bad can it get?** Identify possible consequences.
- ❑ All risks should be identified, regardless of whether they are under the organization's control.

# Identify Risks: Causes and Consequences



# Analyze and Evaluate Risks



Analyzing Risks helps us understand the magnitude of both the positive and the negative consequences of a risk event, as well as the likelihood of those consequences occurring. This will enable you to prioritize risks, and therefore initiate risk treatments effectively.

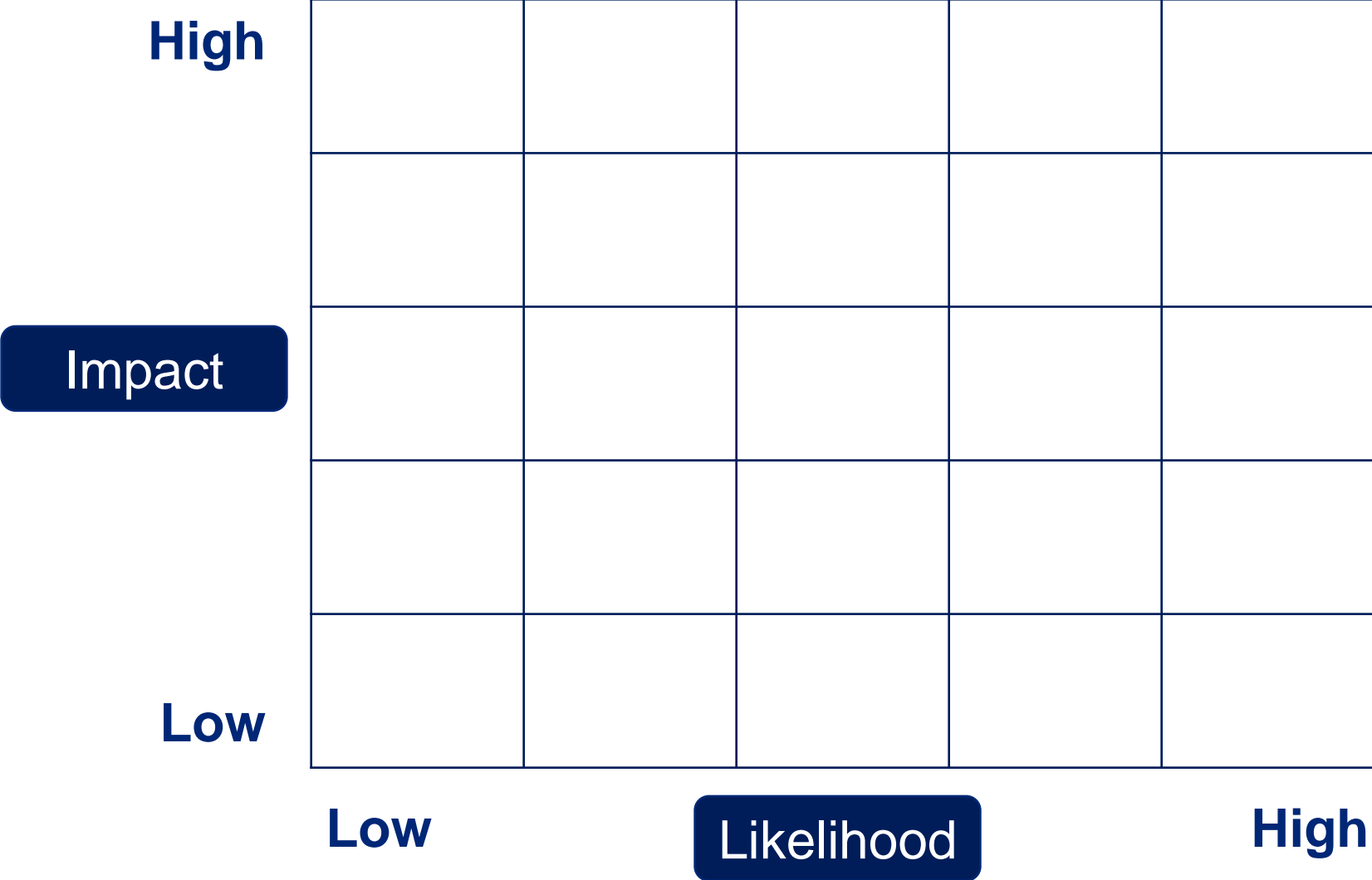
- ❑ The likelihood of an event occurring is a function of the number of ways it can occur.
  - How many times an event has happened in the past?
  - Have conditions changed in a way that could increase the likelihood of a risk occurring?
- ❑ Once likelihood is estimated, the impacts of risk are assessed using impact scales.
  - What is the cumulative impact of the risk? For example, what is the total financial impact, how much service downtime occurred, were there legal or regulatory fines?

# Analyze and Evaluate Risks: Impact & Likelihood

Risks can be assessed and measured using semi-quantitative impact and likelihood ratings. The results from a semi-quantitative risk assessment can be risk rated using a simple device commonly called a heat map. Heat maps are useful for prioritizing and selecting risks for further quantitative analysis.

Impact Severity	Financial Impact (US\$)	Employees	Health, Safety, and Natural Environment	Community and Reputation	Legal																																								
1 - Incidental	Less than 5,000,000	Negligible or isolated staff dissatisfaction	No medical treatment required; quickly and easily reversible effects on biological or physical environment	Slight, medium-term social impacts on local population; mostly repairable damage to items of cultural significance; minor, adverse local public and media attention	Isolated, quickly remedied noncompliance with regulations or contracts																																								
2 - Minor	5,000,000 or less than 20,000,000	General staff morale and attitude problems; increase in staff turnover	Objective but reversible disability requiring hospitalization for people; minor, short-term effects on environment but not affecting ecosystem functions	Ongoing social issues; small, yet repairable damage to items of cultural significance; attention from media; heightened concern by local community	Repeated, slowly remedied contractual or regulatory noncompliance; minor fines imposed																																								
3 - Moderate	20,000,000 or less than 50,000,000	Poor reputation as an employer; widespread staff attitude problems; high staff turnover	Moderate, irreversible disability or impairment to one or more persons; serious environmental effects where recovery takes between 1-5 years	Ongoing serious social issues; significant damage to structures or items of cultural significance; criticism by national government	Widespread, prolonged contractual or regulatory																																								
4 - Major	50,000,000 or less than 200,000,000	Some senior managers leave; high turnover of experienced staff; company not perceived as employer of choice; some shortfalls in nationalization targets	Single fatality or significant, irreversible disability to one or more persons; serious impairment of ecosystem functions where recovery takes between 5-20 years	<table border="1"> <thead> <tr> <th colspan="5">Impact</th> </tr> <tr> <th>1 - Incidental</th> <th>2 - Minor</th> <th>3 - Moderate</th> <th>4 - Major</th> <th>5 - Severe</th> </tr> </thead> <tbody> <tr> <td>Medium</td> <td>High</td> <td>High</td> <td>Very High</td> <td>Very High</td> </tr> <tr> <td>Medium</td> <td>High</td> <td>High</td> <td>Very High</td> <td>Very High</td> </tr> <tr> <td>Medium</td> <td>Medium</td> <td>High</td> <td>High</td> <td>Very High</td> </tr> <tr> <td>Low</td> <td>Medium</td> <td>High</td> <td>High</td> <td>Very High</td> </tr> <tr> <td>Low</td> <td>Low</td> <td>Medium</td> <td>Medium</td> <td>High</td> </tr> <tr> <td>Low</td> <td>Low</td> <td>Medium</td> <td>Medium</td> <td>High</td> </tr> </tbody> </table>		Impact					1 - Incidental	2 - Minor	3 - Moderate	4 - Major	5 - Severe	Medium	High	High	Very High	Very High	Medium	High	High	Very High	Very High	Medium	Medium	High	High	Very High	Low	Medium	High	High	Very High	Low	Low	Medium	Medium	High	Low	Low	Medium	Medium	High
Impact																																													
1 - Incidental	2 - Minor	3 - Moderate	4 - Major	5 - Severe																																									
Medium	High	High	Very High	Very High																																									
Medium	High	High	Very High	Very High																																									
Medium	Medium	High	High	Very High																																									
Low	Medium	High	High	Very High																																									
Low	Low	Medium	Medium	High																																									
Low	Low	Medium	Medium	High																																									
5 - Severe	200,000,000 or more	A large number of senior managers or experienced staff leave; significant shortfalls in nationalization targets	Multiple fatalities or significant, irreversible effects to >50 persons; very serious, widespread impairment of ecosystem functions where recovery takes more than 20 years																																										

# How are Risks Plotted?



# How are Impact and Likelihood Measured?

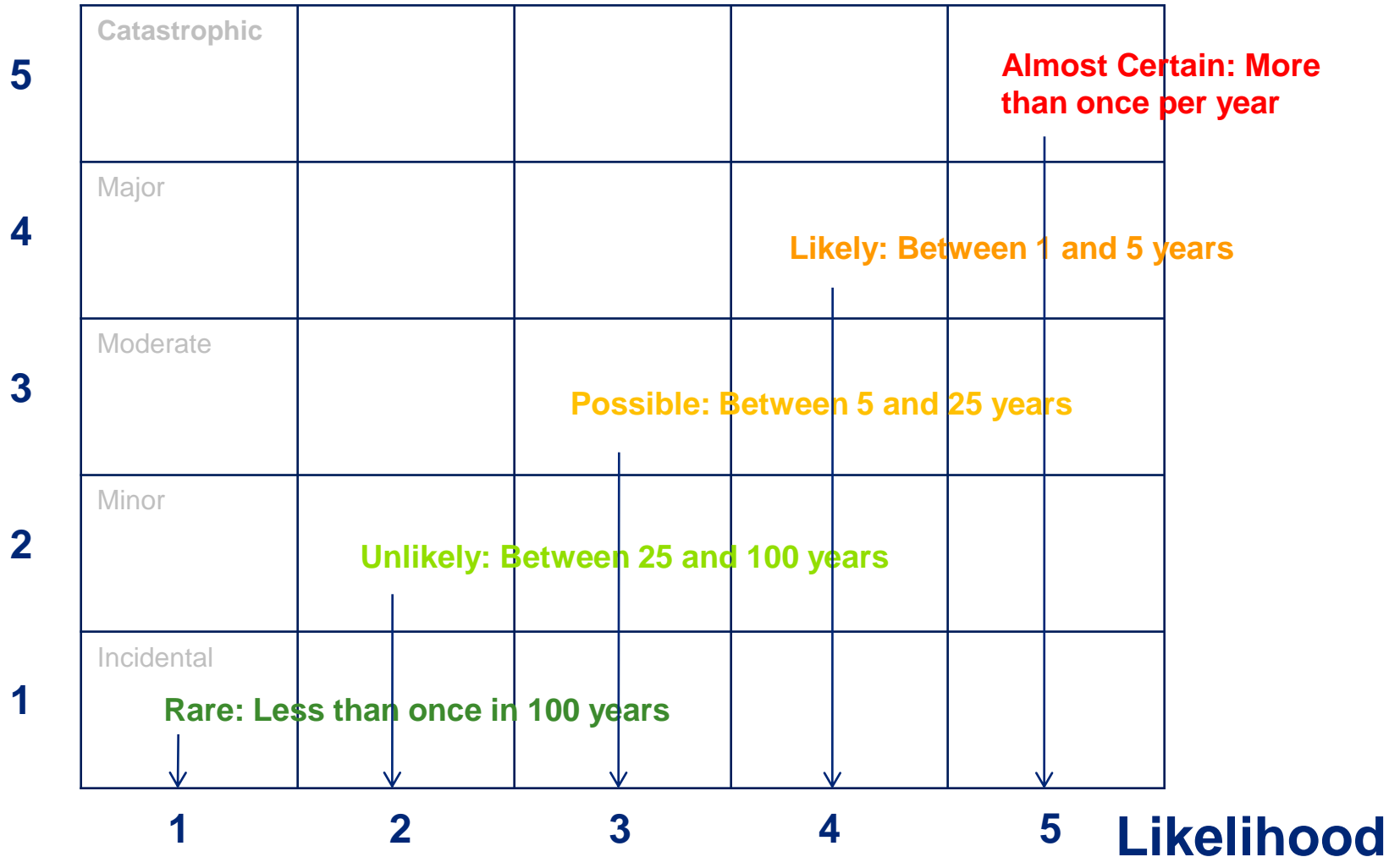
## Impact

5	<b>Catastrophic: Threat of total loss</b>			
4	<b>Major: Extreme financial loss, senior management turnover, extensive injuries or death, operational failures, long term reputational damage, serious breach of regulation</b>			
3	<b>Moderate: High financial loss, high management turnover, extensive injuries, operational downtime, mid-term reputational damage, non-compliance.</b>			
2	<b>Minor: Medium financial loss, staff morale issues, minor injuries, some attention from local media, fines and penalties.</b>			
1	<b>Incidental: Some financial loss, isolated staff dissatisfaction, quickly remedied compliance breaches.</b>			

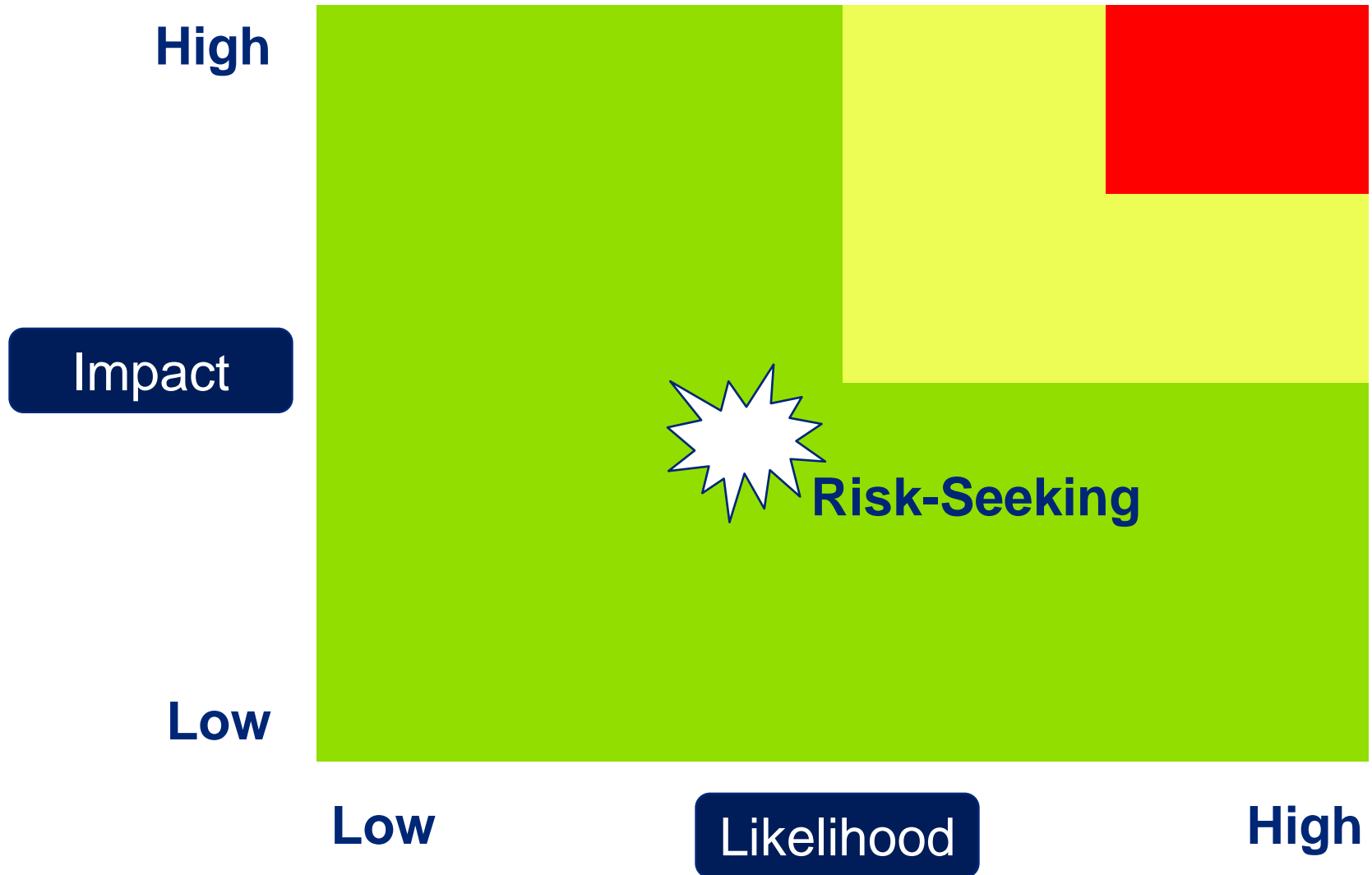
## Likelihood

# How are Impact and Likelihood Measured?

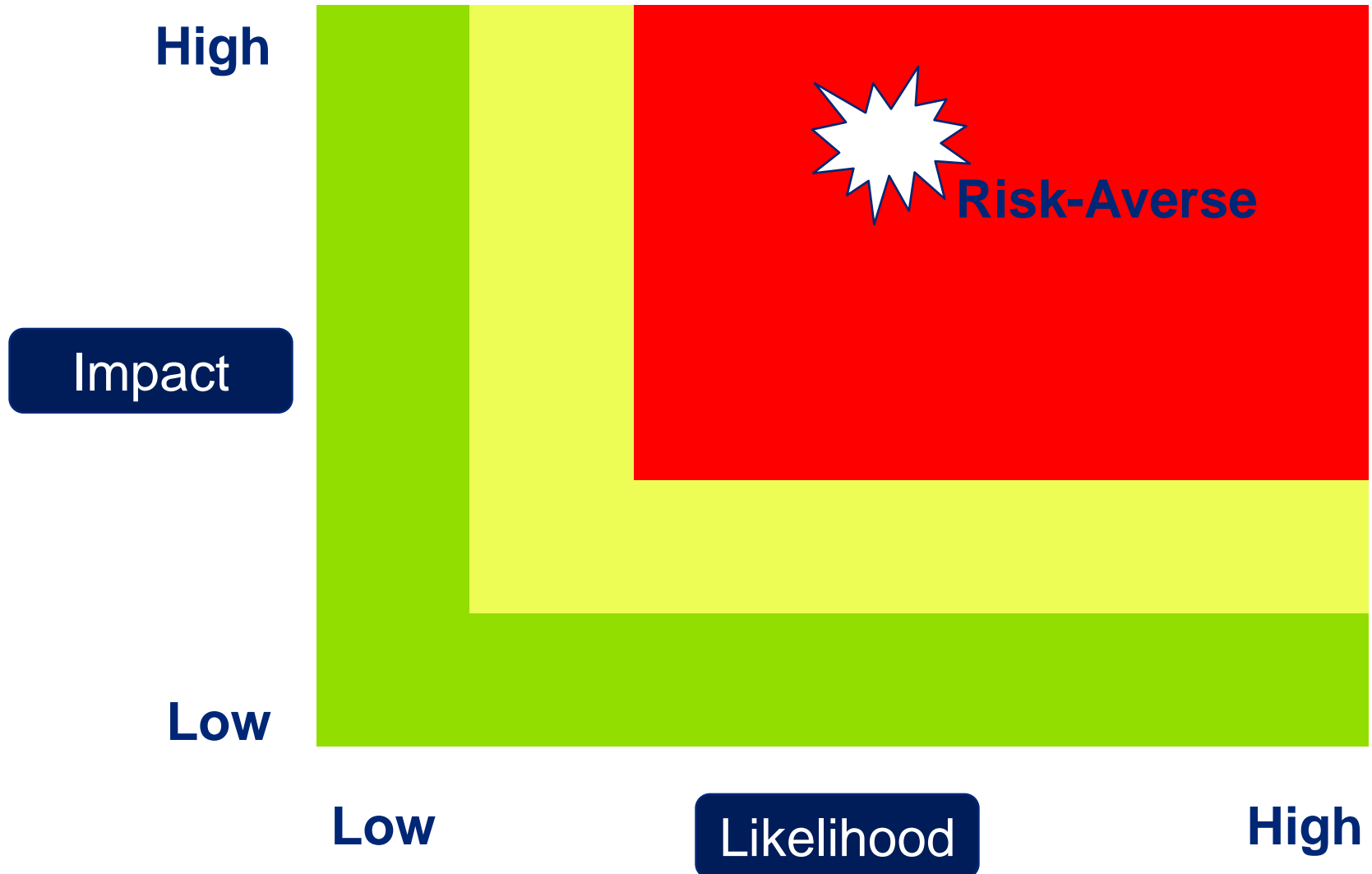
## Impact



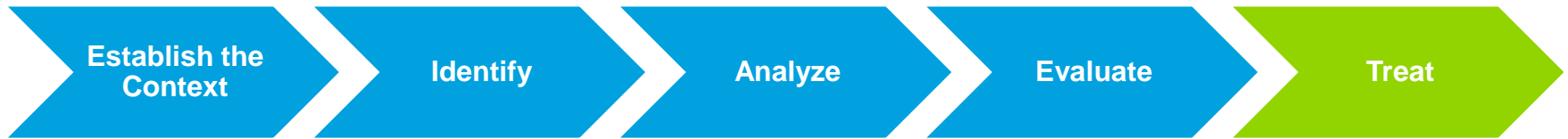
# Defining Risk Appetite Based on Impact & Likelihood



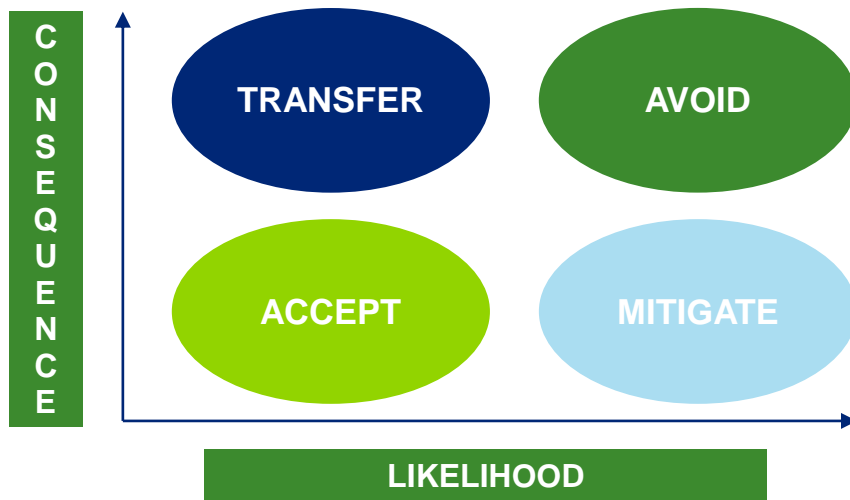
# Defining Risk Appetite Based on Impact & Likelihood



# Treat Risks



Treating Risks involves identifying risk options, assessing them, and implementing treatment plans. A combination of response strategies are used to reduce the residual risk below a defined risk tolerance threshold. Once a risk treatment is implemented, the actual residual risk is measured and compared to the expected residual risk to determine if further action is required.



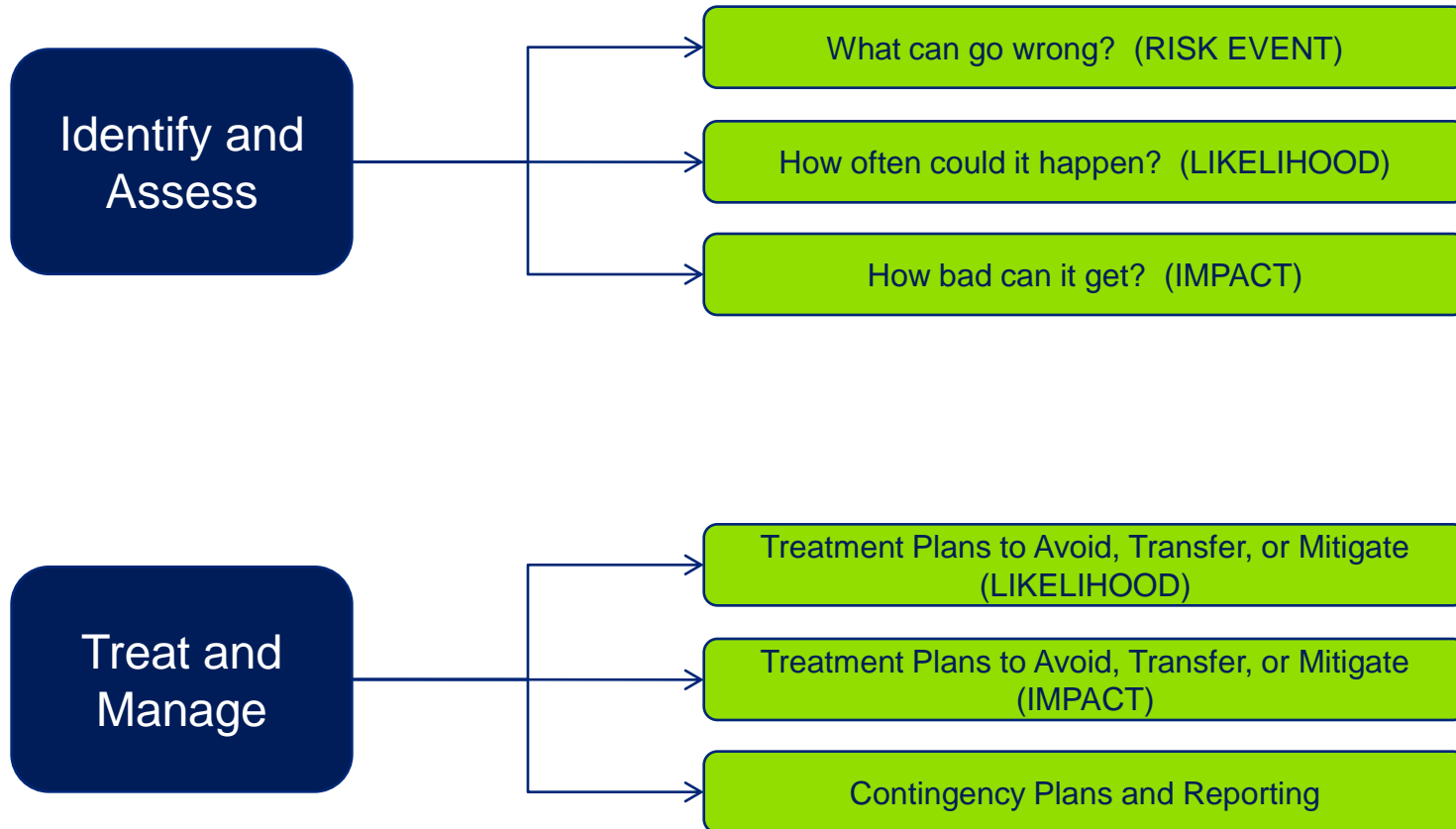
**Avoid:** the risk cannot be mitigated and must be eliminated.

**Transfer or share:** another party bears or shares part of the risk. NOTE: This does not mean the risk is no longer present or not the responsibility of the organization.

**Mitigate or control:** the risk must be beared and its threat can not be avoided or transferred. Risks are reduced until residual risk falls below the risk tolerance threshold.

**Accept:** the cost of implementing mitigation strategies outweighs the benefits.

# Summary of ERM Framework Components



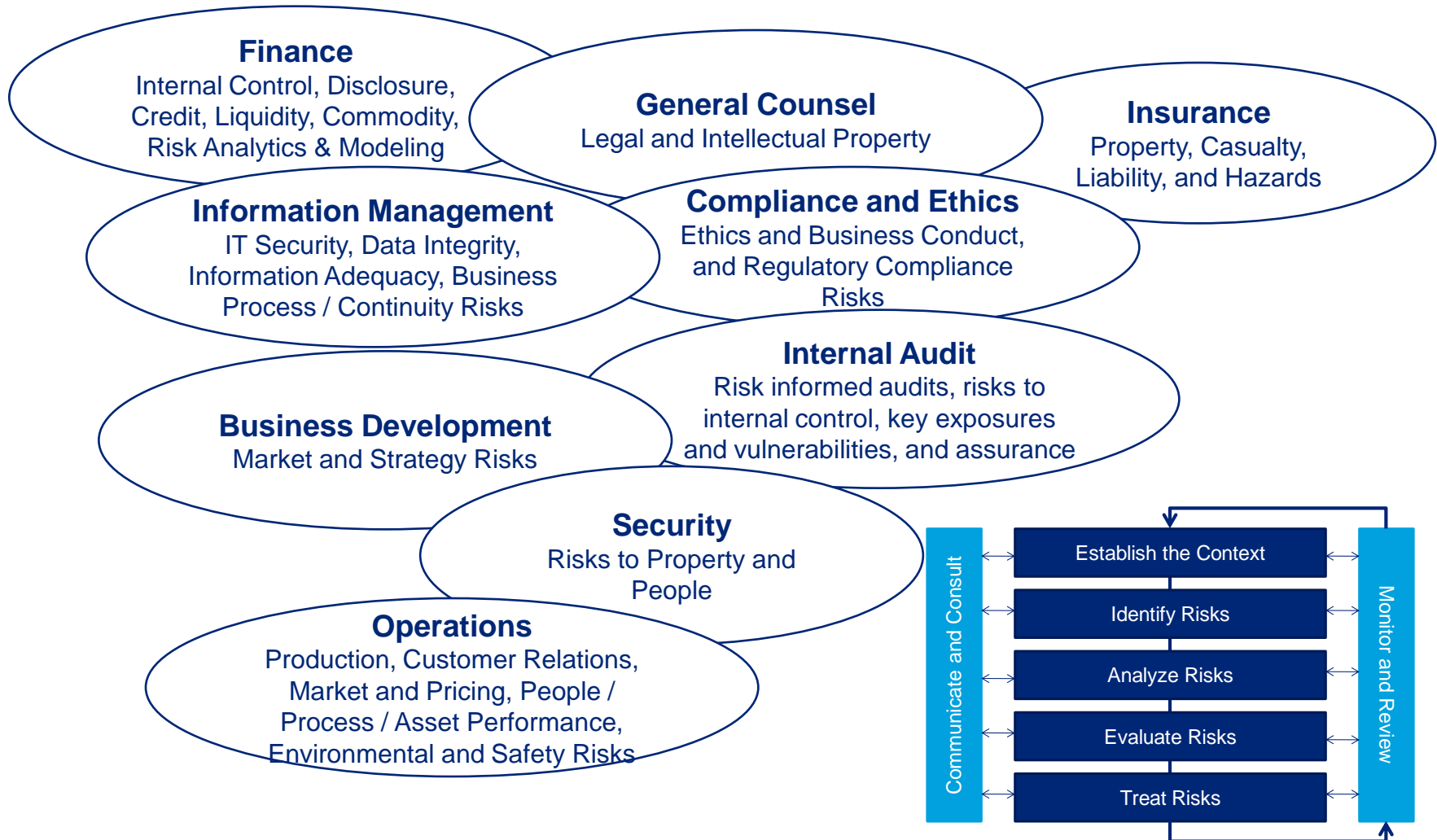
# Our Risk Intelligence Point of View

# Why ERM Should Be Adopted

- It is a proactive, consistent, and process driven management tool to better identify, understand, and respond to a broad range of strategic, operational, compliance, and financial risks.
- It addresses the following issues and opportunities:
  - Confirm major risks, exposures and opportunities
  - Increase Board and stakeholder confidence
  - Manage expected risk exposure to within acceptable limits (risk appetite)
  - Ensure appropriate risk taking authority
  - Reduce the potential for unanticipated financial impacts
  - Make better risk-reward decisions by quantifying impact on value
  - Assure that capital is being allocated based on risk and opportunity
  - Reduce the cost of risk management
  - Reduce management's time to respond to risk inquiries
  - Create a more risk aware culture
  - Improve long term competitive position and responsiveness
  - Prepare for rating agency's increased focus on risk management capability

# The Importance of Risk Integration

Most organizations rely on multiple sources for answers. However, risk oversight and an integrated approach is usually lacking.



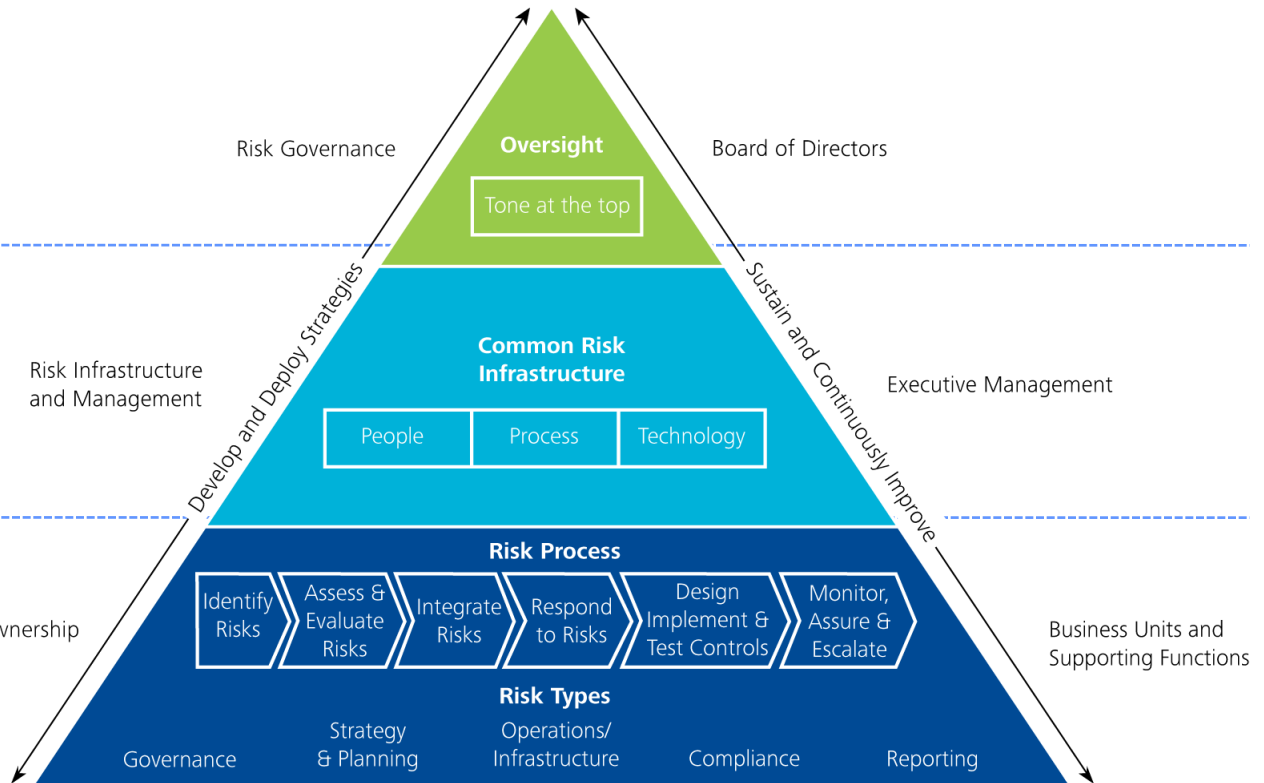
# Our ERM Point of View

## The 9 principles for building a Risk Intelligent Enterprise™

### Nine principles for building a risk intelligent enterprise

- Common definition of risk
  - Common risk framework
  - Roles and responsibilities
  - Transparency for governing bodies
- 
- Common risk infrastructure
  - Executive management responsibility
  - Objective assurance and monitoring
- 
- Business unit responsibility
  - Support of pervasive functions

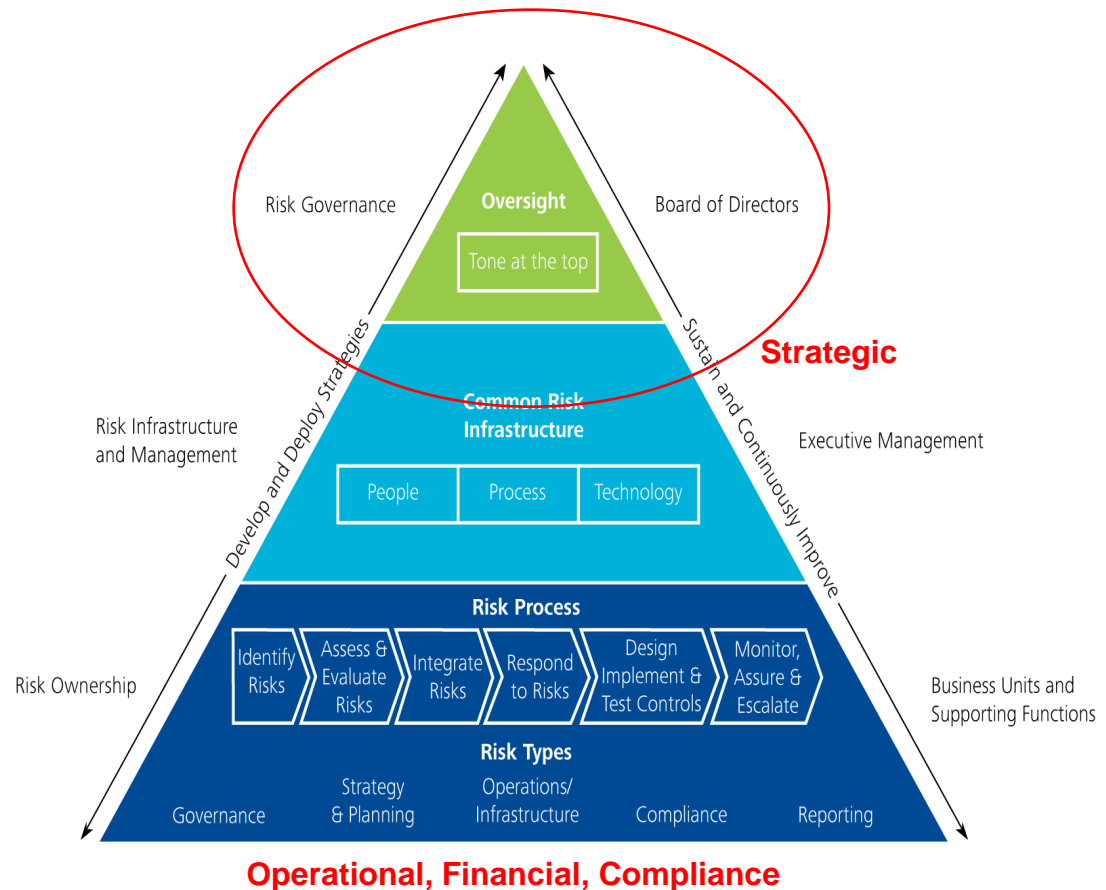
### The risk intelligent enterprise



# The Risk Intelligence Transformation

Four major risk categories from a senior stakeholder's perspective are:

- **Strategic Risks** –risks both to the strategic objectives and of the strategic objectives. The C-suite identifies the top risks thru the planning process and obtain concurrence from the Board
- **Operational Risks** –major risks that impact the organization's ability to achieve the strategic plan
- **Financial Risks** –include financial reporting, valuation, hedging, market and liquidity risks and credit risks in financial institutions
- **Compliance Risks** –unrewarded risks, typically the primary focus for enterprise risk management activities



# Assessing the Maturity of ERM Capabilities

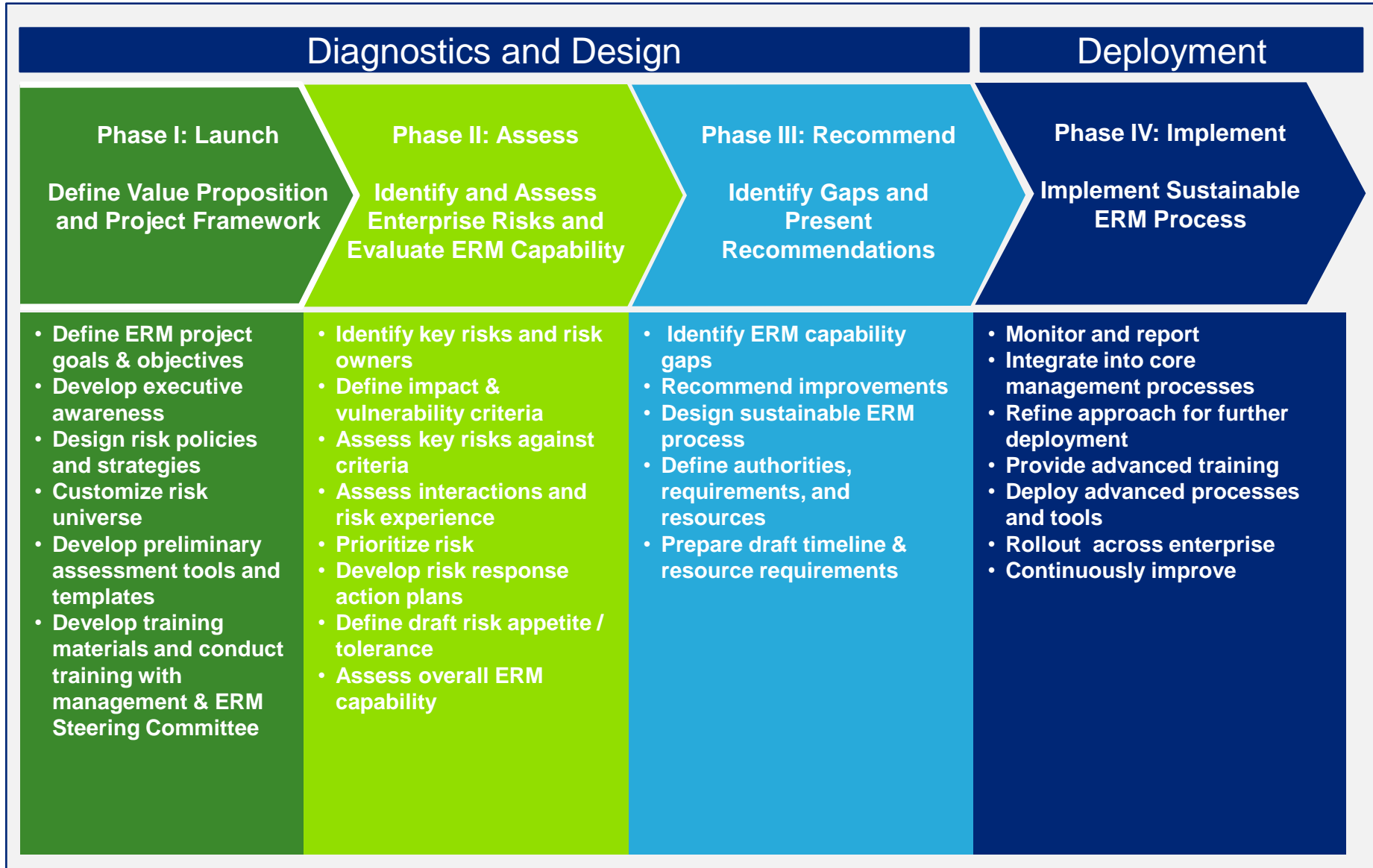
As a first step, current ERM capabilities can be evaluated and a roadmap for desired, future maturity developed.



Representative Attributes				
<ul style="list-style-type: none"> <li>• Ad hoc/chaotic</li> <li>• Depends primarily on individual heroics, capabilities, and verbal wisdom</li> </ul>	<ul style="list-style-type: none"> <li>• Risk is defined differently at different levels and in different parts of the organization</li> <li>• Risk is managed in silos</li> <li>• Limited focus on the linkage between risks</li> <li>• Limited alignment of risk to strategies</li> <li>• Disparate monitoring &amp; reporting functions</li> </ul>	<ul style="list-style-type: none"> <li>• Identify risk universe</li> <li>• Common risk assessment/response approach developed and adopted</li> <li>• Organization-wide risk assessment performed, action plans implemented in response to high priority risks</li> <li>• Communication of top strategic risks to the Senior Management Team</li> </ul>	<ul style="list-style-type: none"> <li>• Risk management activities coordinated across business areas</li> <li>• Risk analysis tools developed and communicated</li> <li>• Enterprise risk monitoring, measuring, and reporting</li> <li>• Scenario planning</li> <li>• Opportunity risks identified and exploited</li> <li>• On-going risk assessment processes</li> </ul>	<ul style="list-style-type: none"> <li>• Risk discussion is embedded in strategic planning, capital allocation, product development, etc.</li> <li>• Early warning system to notify the risks above established thresholds to Board and management</li> <li>• Linkage to performance measures and incentives</li> <li>• Risk modeling</li> </ul>

# Getting Started: A “How To” Guide

# Typical Approach for Launching an ERM Program



# Risk Identification Workshops

Risk identification workshops can kick start the ERM initiative, which is a key input to...

- Early engagement of executive team
- Top down identification of key risks of and to strategic objectives
- Dialogue to challenge business assumptions and discuss risk intelligent alternatives

	Step 1: Review Objectives and Strategies	Step 2: Conduct Executive Interviews	Step 3: Conduct Executive Workshop
Activities	<p>Gain an understanding of your overall strategies and objectives, including:</p> <ul style="list-style-type: none"> <li>• Key business assumptions</li> <li>• KPIs</li> <li>• Identification of risk stakeholders</li> <li>• Identify the risks of the strategy and objectives</li> </ul>	<p>Prepare for and conduct focused interviews to identify:</p> <ul style="list-style-type: none"> <li>• Key Risks</li> <li>• Key Opportunities</li> <li>• Perspectives of Total Cost of Risk (TCOR)</li> <li>• Risk Appetite (boundaries)</li> </ul>	<p>Prepare and conduct executive workshop</p> <ul style="list-style-type: none"> <li>• Educate participants</li> <li>• Review assumptions framework</li> <li>• Use aspects of Root-Cause Analysis and similar tools to determine key risks and opportunities</li> <li>• Refine and ratify risk appetite</li> <li>• Estimate of Total Cost of Risk</li> <li>• Agree on Vital Few Key Risks and Opportunities</li> </ul>
Outcomes	<ul style="list-style-type: none"> <li>• Summary of organization strategies, assumptions, and objectives</li> </ul>	<ul style="list-style-type: none"> <li>• Preliminary list of Key Risks and Opportunities</li> <li>• Initial Risk Appetite Model</li> </ul>	<ul style="list-style-type: none"> <li>• Revised assumptions</li> <li>• TCOR estimates</li> <li>• Updated list of Key Risks and Opportunities</li> </ul>

# Risk Identification Processes

Risk identification workshops can kick start the ERM initiative, which is a key input to... a **customized** risk framework that allows further identification of relevant risks for assessment...

Risk Category	Specific Risk Areas	Example Risks	
Regulatory and Compliance	Fraud, kickbacks, and abuse	-Fraudulent Financial Reporting -Misstatements from misappropriation of assets	-Bribery -Violation of laws and regulations -Unauthorized expenditures
	Sarbanes Oxley	-Financial disclosure -Financial restatement	-Non-compliance -Implementation requirements
	External Audit	-Accurate/ timely reporting -Full disclosure	-Financial system impact -Qualified opinion
Strategic and Environmental	Organization and Governance	-Adequate succession planning -Leadership effectiveness -Decision making practices	-Accountability -Misalignment of goals and objectives
	Market Demand	-Market penetration / critical mass -Shifting service needs	-Emerging opportunities -New markets -Customer choice / loyalty
	Community and Public Relations	- Media relations	- Support/ loyalty / trust

# Risk Assessment Processes

Risk identification workshops can kick start the ERM initiative, which is a key input to... a customized risk framework that allows further identification of relevant risks for assessment... using a consistent enterprise-wide process...

A web-based survey can be used to capture management's perspective regarding risk impact, vulnerability and speed of onset.

## Risk: Organizational change

**Definition:** Inability of the organization to effectively adopt change resulting in the inability to achieve objectives

**Risk causes/conditions:** 1. Continuous change in the organization. 2. Poorly executed change management process. 3. Ineffective communication. 4. Resistance to changes due to successful past performance

**IMPACT-(Click for rating criteria definitions)**The potential for negative consequences of this risk event, without regard to anything that may be in place to deal with this event. Impact can be expressed in both financial and non-financial areas such as reputation, legal/regulatory, customer, employees, or operations. How severe would the impact of this risk event be?

**VULNERABILITY -(Click for rating criteria definitions)**The remaining impact of the risk (residual) which takes into account any controls/ strategies / mitigation factors. Considering your assessment of Impact as well as your knowledge of the effectiveness of controls/ strategies/ mitigation factors that are in place to deal with this risk, what is our vulnerability to this risk?

Low			Medium				High		
1	2	3	4	5	6	7	8	9	10

NA  1  2  3  4  5  6  7  8  9  10

Low			Medium				High		
1	2	3	4	5	6	7	8	9	10

NA  1  2  3  4  5  6  7  8  9  10

Previous Page

Next Page

# Risk Prioritization Processes

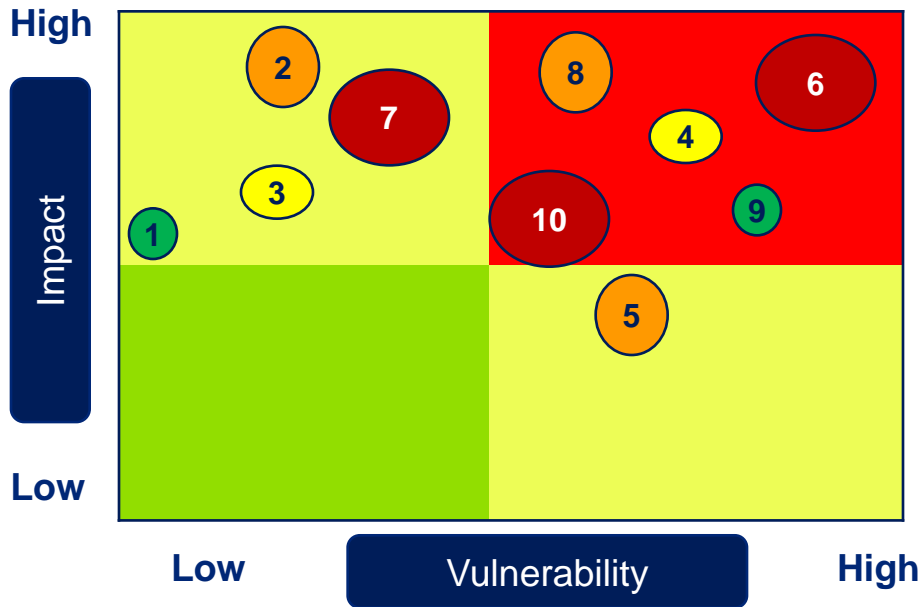
Risk identification workshops can kick start the ERM initiative, which is a key input to... a customized risk framework that allows further identification of relevant risks for assessment... using a consistent enterprise-wide process... that is based on consistent prioritization criteria...

Risk thresholds will be consistently used to prioritize risks across the organization.

Impact Criteria	Financial	Reputation	Legal/Regulatory	Customers	Employees	Operations					
<b>HIGH</b>	Impact that may reduce earnings before taxes more than \$XX or negatively impact cash flow by more than \$XX	Potential for sustained negative national media attention. Significant loss of reputation.	Major federal or state scrutiny. Investigations subject to substantial fines and penalties	Wide-spread impact on customer satisfaction. Serious threat to future growth.	Significant loss of staff, critical widespread impact on morale, or severe injury to employees	Significant loss of operations and distribution capacity (e.g. no access to distribution center). Wide-spread service					
							<b>Vulnerability Criteria</b>	<b>CONTROL EFFECTIVENESS &amp; EFFICIENCY</b>		<b>CAPABILITY</b>	<b>PREVIOUS RISK EXPERIENCE</b>
							<b>Description</b>	<b>Controls / Mitigation</b>	<b>Monitoring/ Testing / Reporting</b>	<b>People/ Skills/ Knowledge</b>	<b>Costs, Audit, Regulatory</b>
							<b>RATING</b>				
<b>MEDIUM - HIGH</b>	Having read the rating criteria for medium and high, please select this option if the vulnerability rating falls in between the range of medium and high	<b>HIGH</b>	No controls / mitigation plans exist; Controls / Mitigation plans exist but are not consistently applied; Controls need to be tested	Ad hoc and informal risk analysis; Risk sources and emerging indicators have not been identified; No formal reporting schedule	Limited level of internal staff capable of managing risk potential; Limited access to external resources	Major recent adverse experience resulting in cumulative costs/fines of greater than XX% of revenue					
<b>MEDIUM</b>	Impact that may reduce earnings before taxes by up to \$XX or negatively impact cash flow up to \$XX	Having read the rating criteria for medium and high, please select this option if the vulnerability rating falls in between the range of medium and high	<b>MEDIUM - HIGH</b>	Having read the rating criteria for medium and high, please select this option if the vulnerability rating falls in between the range of medium and high	Moderate level of internal staff with skill set for managing risk potential; Moderate access to	Moderate recent adverse experience resulting in cumulative costs/fines of XX-X% of revenue.					
<b>LOW - MEDIUM</b>	Having read the rating criteria for low and medium, please select this option if the vulnerability rating falls in between the range of low and medium		<b>MEDIUM</b>	Controls/ mitigation plans need to be updated and improved; Lack of routine controls testing	Risk sources have been identified and are periodically monitored; No formal reporting						
			<b>High</b>			Very rapid onset; little or no warning, instantaneous.					
<b>LOW</b>	Impact that may reduce earnings before taxes less than \$XX or negatively impact cash flow less than \$XX		Having read the rating criteria for low and medium, please select this option if the vulnerability rating falls in between the range of low and medium	<b>LOW - MEDIUM</b>	Having read the rating criteria for low and medium, please select this option if the vulnerability rating falls in between the range of low and medium			Several days or one month to occur.			
		<b>Medium-High</b>		Controls/ mitigation plans are in place, consistently applied and routinely tested; Controls/ Mitigation plans are an integral part of standard operations	For recent monitoring and reporting		Moderate onset; several weeks or months to occur.				
		<b>Low - Medium</b>				Several months to one year to occur.					
			<b>LOW</b>				Very slow onset; Several years to occur.				

# Risk Prioritization Processes

Risk identification workshops can kick start the ERM initiative, which is a key input to... a customized risk framework that allows further identification of relevant risks for assessment... using a consistent enterprise-wide process... that is based on consistent prioritization criteria... to produce a risk heat map and prioritized risk list...



ID	Risks
1	Risk Name
2	Risk Name
3	Risk Name
4	Risk Name
5	Risk Name
6	Risk Name
7	Risk Name
8	Risk Name
9	Risk Name
10	Risk Name

Dot size reflects speed of onset:



# Risk Ranking and Prioritization

Use survey results to develop an initial risk prioritization that will guide executive interviews.

Rank	By Impact		By Vulnerability		By Speed of Onset	
1	Customer retention	4.49	Revenue growth objectives	3.52	Succession Planning	4.13
2	High customer concentration	4.23	Significant customer concentration	3.42	BCM and contingency planning	3.52
3	Adverse regulatory changes	4.19	Succession planning	3.39	Significant customer concentration	3.29
4	Quality	4.03	Talent management	3.35	Quality	3.15
5	Revenue growth objectives	3.91	Adverse regulatory changes	3.19	IT dependence	3.03
6	Xxx	3.89	Xxx	3.18	Xxx	3.00

Risk	Ranking (by average vulnerability)			
	Overall	BOD	SVP	VP
Revenue Growth Objectives	1	1	1	1
High Customer Concentration	2	4	2	4
Adverse regulatory changes	3	2	7	3
Talent Management	4	3	5	2
Succession Planning	5	6	12	5
Xxx	6	8	6	6

- Revenue Growth Objectives is a top concern for all levels.
- Talent Management is a top 5 concern for SVPs and VPs, but not BODs.
- Succession Planning is a top 10 concern for VPs and BODs, but not SVPs.
- There is wide variation in rankings for XXXX and XXXX

# Prioritizing Risks and Taking Action

Prioritize recommended actions including the assignment of ownership and monitoring responsibilities, and conduct deep dive risk assessments as appropriate

## Recommended Ownership and Monitoring

- Risk 3
- Risk 4
- Risk 7
- Risk 8

### Establish Ownership and Monitoring

- Identify Executive Risk Owners and establish accountability.
- Monitor effectiveness of mitigation efforts and exposure to new events or trends.
- Implement a reporting method including escalation pathways.
- Integrate with key strategic decision making processes.
- Obtain independent assurance (e.g. internal audit).

## Recommended Deep Dive Risk Assessments

- Risk 1
- Risk 2
- Risk 5
- Risk 6

### Conduct Deep Dives

- Evaluate the risk exposure including quantification as necessary.
- Assess current risk capabilities against risk appetite.
- Identify gaps and areas for improvement.
- Identify recommended risk response strategies.

# In-Depth Risk Analysis

A tool for in-depth analysis of priority risks



<b>Risk Event and Description:</b>		<b>Team Chair:</b>	
------------------------------------	--	--------------------	--



<b>Impact Rating:</b>		<b>Vulnerability Rating:</b>		<b>Speed of Onset Rating:</b>	
-----------------------	--	------------------------------	--	-------------------------------	--



Contributing Risk Factors	How are these Risk Factors currently monitored?	Monitored by	What would warrant taking action?	What else can potentially be monitored?	Dashboard reporting?



Current Mitigation Activities:	Activities / Initiatives in Planning or Being Considered:



Plan / Key Assumptions	Potential Scenarios



<b>Overall Risk Response (Implement/improve mitigation, Accept as is, Monitor etc.):</b>	
--	--



Risk Response Action Items	Owner	Timing	Target Date	Resources Needed	Risk or Risk Factor Addressed	Status
						Green
						Red
						Yellow
						Green

# Detailed Risk Profiles

Used to capture risk response action plans, monitoring processes, key risk indicators...

## Definition of Human Capital Risks

Failure to manage the knowledge, skills, and experiences of employees, thereby enabling ZZZ Co. to execute our business model and achieve critical objectives

## Executive Risk Owner(s)

John Doe, Director of HR

## Risk Details

- **Attract and retain talent** - Inability to attract, select, hire, and retain talented personnel that achieve results while living the company's values.
- **HR policies and compliance** - Lack of internal HR and other company policies or lack of compliance against such policies.
- **Appropriate training** - Failure to provide employees with the opportunity to obtain skills needed to do their jobs through on-the-job training, classes, seminars, or conferences.
- **Culture** – Limited adoption/acceptance of the desired corporate traits.
- **Succession planning** – Failure to plan for executive and employee succession, as well as specific training and grooming, creates many single points of failure.
- **Pay and benefits** – Perception of moving towards norm/averages creates a culture of mediocrity, leading to mediocre results.

## Current Responses

Initiative to improve talent levels in key positions – recent key new hires

Top talent retention initiatives

Worldwide benefits policy effort - Initiative to review and update all Global HR policies and guidelines

Professional development and training

## Monitoring Processes

SVP Dashboard / Scorecard  
Annual Comp Committee review

Sarbanes Oxley: back office (HR)

Quarterly reporting of training stats

## Key Risk Indicators

Number of bad hires











Attrition rates  
Pay and rewards

Employee survey results






Number of courses provided  
Budget per employee

# Detailed Risk Profiles

... and as a dashboard for ongoing risk monitoring / status reporting

Risk Rank (A)	Risk Description	Residual Risk Score (B)	Residual Risk Direction (C)	Risk Response Status (D)	Exec Risk Owner	Status of Additional RM Activities Initiated
1	Pricing and Margin Management Initiative	4.45			Xxx	-All low margin contracts reviewed by task force -Profitability analysis pre-approval strengthened -Contract pricing /product change process improving
2	Mid-Market Growth Initiative	4.09			Xxx	-Contract sales compensation program being evaluated
3	Global Growth Initiative	3.87			Xxx	-Model being evaluated by management
4	Business Continuity Planning	3.72			Xxx	-A project has been initiated to develop appropriate BC plans for all major operations and facilities
5	IT Back-up and Disaster Recovery	3.69			Xxx	-Key steps completed to improve IT BU – consolidated data center, developed offsite facility -New steps being planned to improve recovery time

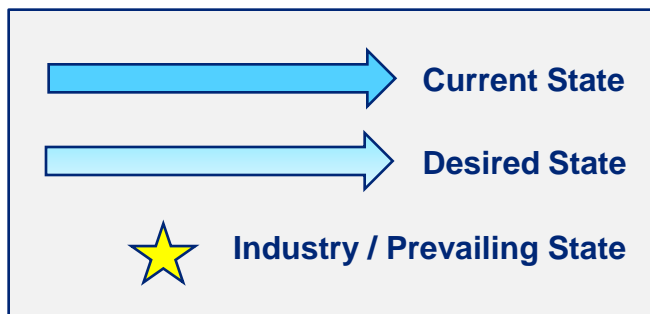
## (D) Risk Response Status

-  **Exceeds requirement:** The risk management processes have been over-engineered for the level of risk involved
-  **Meets requirement:** The risk management processes are appropriate for the level of risk identified
-  **Needs strengthening (minor):** Minor improvements in risk management processes are necessary to “meet requirements”
-  **Needs strengthening (major):** Major improvements in risk management processes are necessary to “meet requirements”
-  **Un-established:** Risk management processes not established yet.

# Capability Maturity Assessment

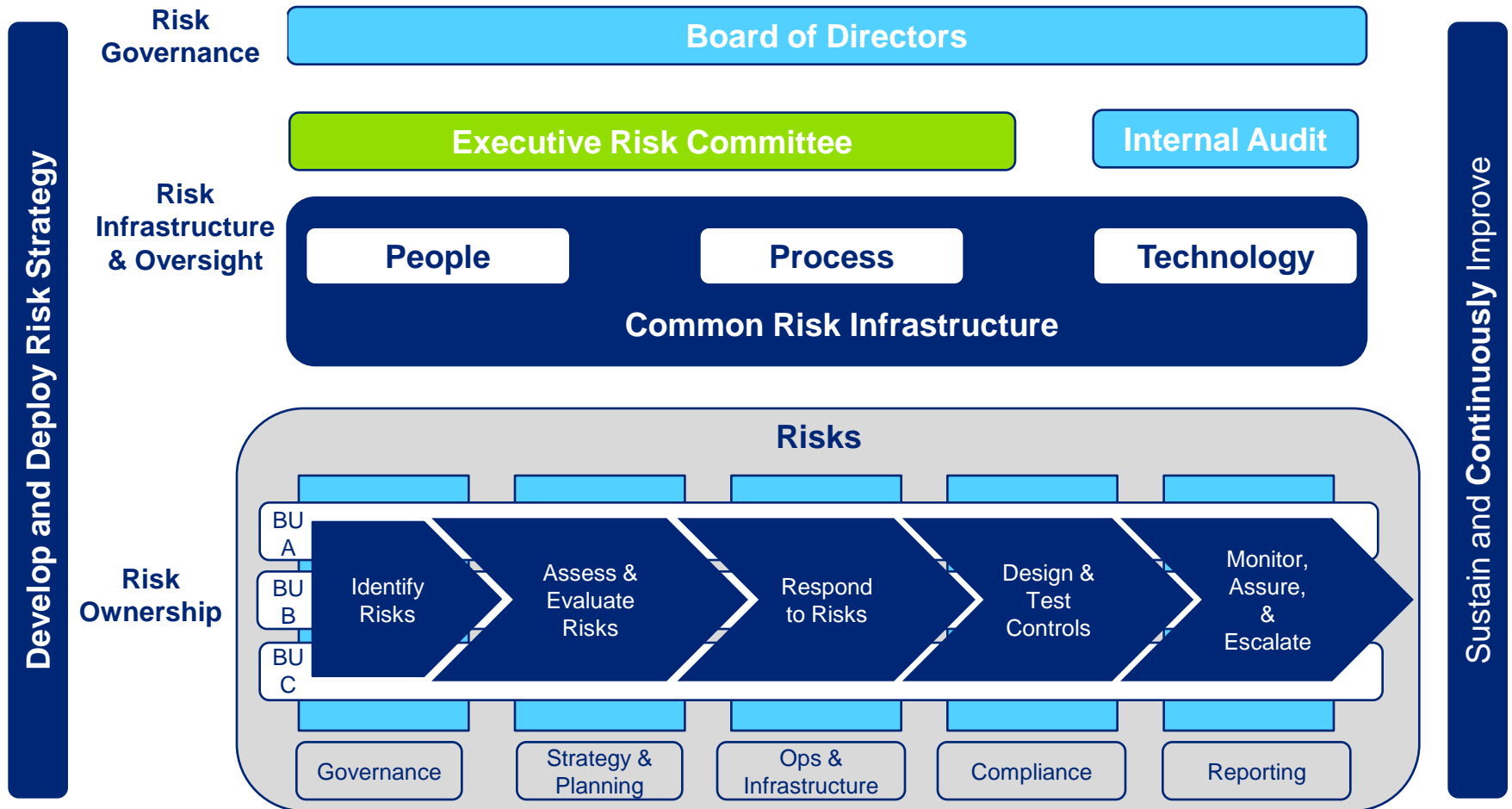
Conducting a capability maturity assessment and gap analysis...

	Weak	Adequate		Strong	Excellent
	Initial / Ad Hoc	Frag-mented	Compre-hensive	Integrated	Strategic
Strategy and Policy					
Appetite & Tolerance					
Governance Structure					
Risk Categories					
Qualitative Methods					
Quantitative Methods					
Reporting					
Emerging Risk Mgmt					
Risk Aggregation					
Change Management					
People Skills and Resources					
Validation and Assurance					



# ERM Framework

Conducting a capability maturity assessment and gap analysis... supports the development of a customized ERM Framework to improve risk management capabilities including...



# Risk Governance Structures

Conducting a capability maturity assessment and gap analysis... supports the development of a customized ERM Framework to improve risk management capabilities including...well defined risk governance roles and responsibilities.

## Board of Directors & CEO

The Board of Directors has ultimate accountability for all risk but can delegate responsibility to senior management

## CRO &/or Risk Committee

“ERM Oversight”

Clearinghouse for risks, policy, appetite setting, and governance

## Business Areas “Manage Risks”

- Risk identification
- Risk self-assessments
- Strategy and actions to address risk within policy
- Ensure compliance with ERM policies and procedures
- Provide assertions on risk exposure

## ERM Organization “Supports CRO, Risk Committee, SVPs, and the Board”

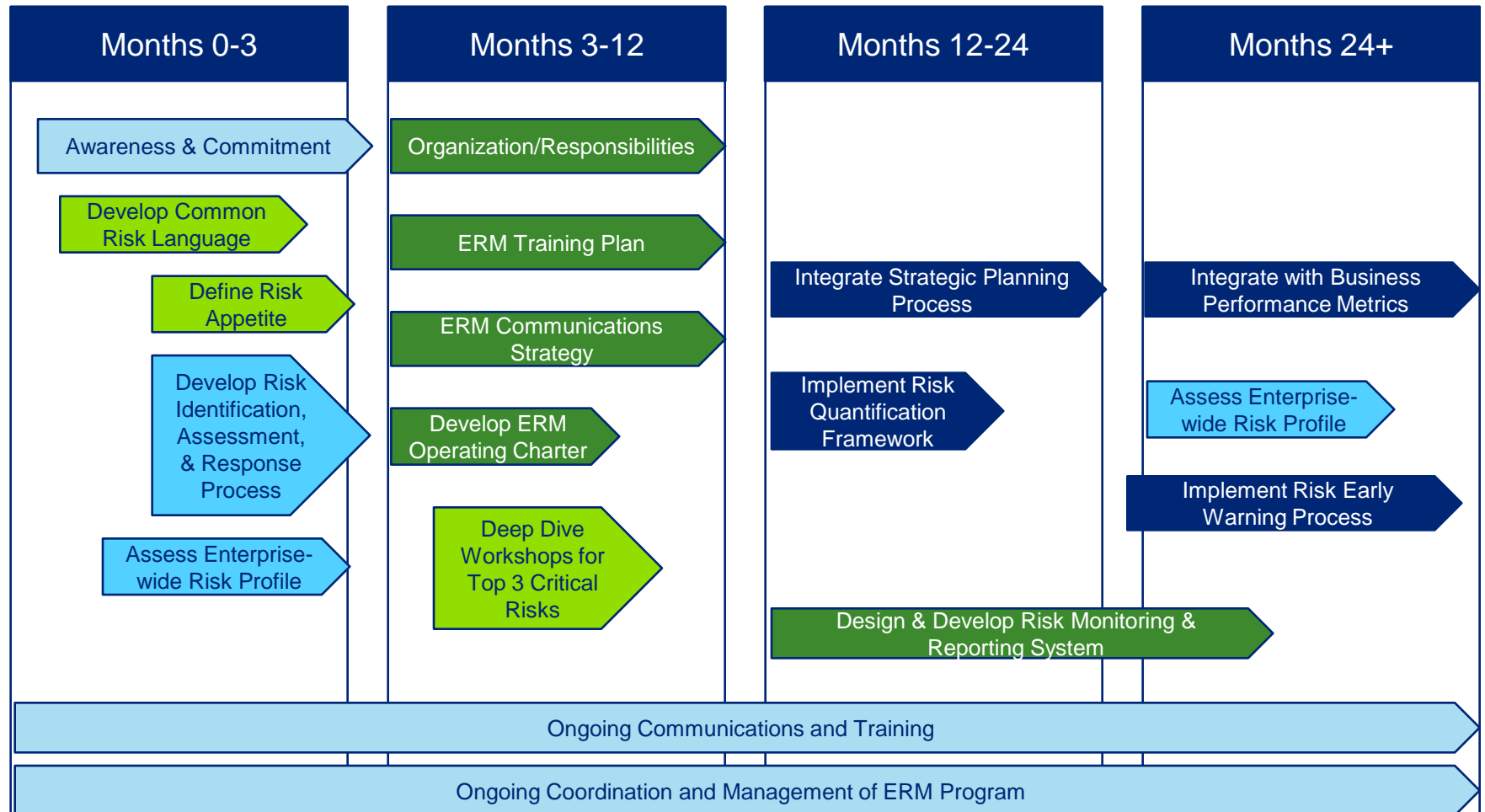
- Governance, policy, and appetite implementation and coordination
- Risk assessment methods
- Measurement, aggregation, reporting rules and tools
- Monitor risk exposure status and report to Board

## Audit “Provides Independent Assurance”

- Periodic validation of control and compliance
- Objective review of risk management process
- Independent assurance to management and Board on assertions of risk exposure

# Implementation Roadmap

Executing the ERM framework is supported by a well defined implementation roadmap and timeframe.



# Overview of Leading Practices

# Examples of Emerging Practices

- Holding monthly meetings of ERM Steering Committees and Councils
- Creating ERM policy statements to clarify expectations and accountabilities
- Assigning executive ownership of risk categories
- Creating the position of ERM Director, VP-Risk & Compliance, VP-Risk Management, etc.
- Conducting annual enterprise wide risk assessments
- Leveraging cross functional risk review/response teams
- Developing risk-based audit plans
- Using risk assessments to rationalize internal controls and compliance efforts
- Maintaining a Risk Book or Risk Dashboard for C-level executives
- Increasing focus on risk quantification
- Conducting in-depth analysis of financial risk – market, credit, liquidity
- Increasing focus on product/market, business continuity, and crisis management risk
- Considering internal and external risk factors in Strategic Planning and Budgeting processes
- Creating risk scenarios/alternative response strategies

# Lessons Learned

- Engage management early in the process (begin with a strategic risk dialogue)
- Identify key risks to enterprise value ...avoid trying to boil the ocean
- Apply a structured, field-proven approach for effective and efficient ERM program design and implementation
- Leverage a sound repository of tools and templates
- Leverage existing processes within the company; integrated, not bolted on
- Support the ERM process with subject matter experts for in-depth analysis and solutions
- Work with an experienced ERM advisor to accelerate buy-in and ensure knowledge transfer throughout the process

# Final Thoughts

# The Total Cost of Risk

**Cost of Risk Management:  
Prevention and Preparation**



**Small, but easy to see**

**Cost of Failure:  
Response and Recovery**

**Huge, but hard to see**

**Cost of Failure + Cost of Risk Management = Total Cost of Risk**

**Goal: Shrink the whole iceberg**

# Practical Solutions for Our Clients

- Improve preparedness for the risks and opportunities that inevitably lie ahead
- Find the unexpected before it finds you
- Continue to grow your brand, improve your revenue growth, operating margins and asset productivity despite uncertainty and turbulence
- Effectively link strategy and risk management
- Practically define your risk appetite and tolerances
- Determine the best ways for the board to oversee that enterprise value and risk are being appropriately managed
- Determine the most appropriate balance of roles and responsibilities between board and executive (risk oversight vs. risk management)
- Improve the board's ability to get reassurance that executive's reports about known and emerging enterprise risk exposures are reliable
- Identify opportunities for the board and executive to practically improve your chances of survival and success

# Thank You

## **Angela M. Bryant**

Deloitte

Leader, ERM Centre of Excellence

+971 (0) 4 369 8999 Work  
abryant@deloitte.com

Emaar Business Park, Building 1  
PO Box 282056  
Dubai, UAE

## **Rami Wadie**

Deloitte

Leader, Enterprise Risk Services, Kuwait

+965 22438060 x 108 Work  
rwadie@DELOITTE.COM

# Deloitte.

## About Deloitte:

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 140 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's approximately 169,000 professionals are committed to becoming the standard of excellence.

Deloitte's professionals are unified by a collaborative culture that fosters integrity, outstanding value to markets and clients, commitment to each other, and strength from cultural diversity. They enjoy an environment of continuous learning, challenging experiences, and enriching career opportunities. Deloitte's professionals are dedicated to strengthening corporate responsibility, building public trust, and making a positive impact in their communities.

## About Deloitte & Touche (M.E.):

Deloitte & Touche (M.E.) is a member firm of Deloitte Touche Tohmatsu Limited (DTTL) and is the first Arab professional services firm established in the Middle East region with uninterrupted presence for over 85 years. Deloitte & Touche (M.E.) is among the region's leading professional services firms, providing audit, tax, consulting, and financial advisory services through 26 offices in 15 countries with over 2,400 partners, directors and staff. Deloitte & Touche (M.E.) is a 2009 Hewitt Best Employer in the Middle East. Deloitte & Touche (M.E.) is a Tier 1 advisor in the GCC region (International Tax Review World Tax 2010 Rankings) and was recognized as the 2010 Best Consulting Firm of the Year in the First Complinet GCC Compliance Awards.