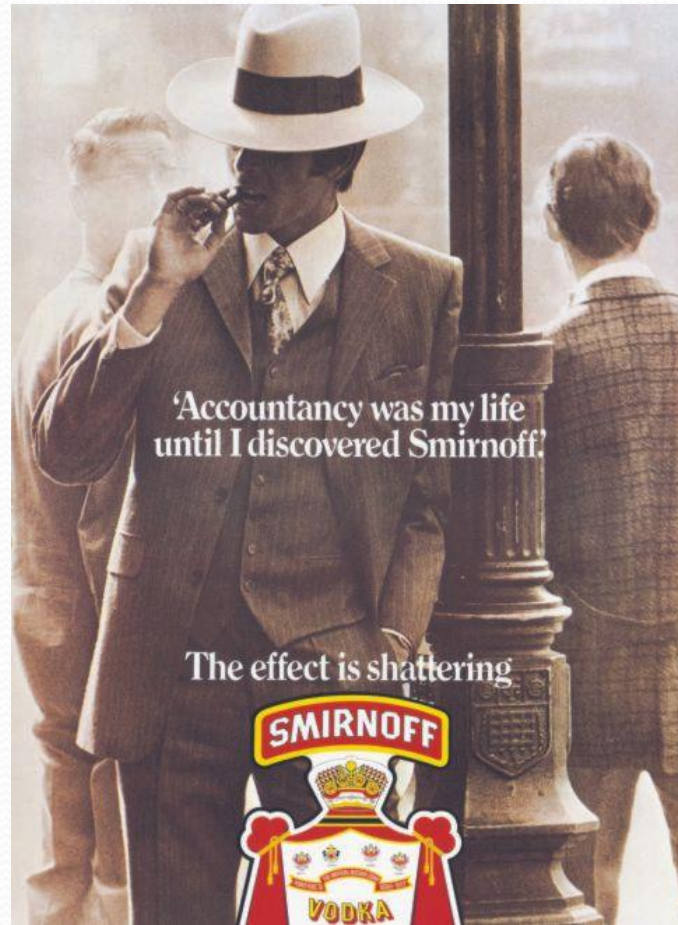


Effective Management of IT-related Business Risk

Urs Fischer, CPA, CRISC, CISA, CIA
Fischer IT GRC Consulting & Training



Urs Fischer



Agenda

- Risk and Risk Management
- Risk Function Perspective
- Risk Management Perspective
- Risk Scenarios
- Trends
- Summary and Wrap-Up – Questions & Answers

Would you do this with your children?



Agenda

- **Risk and Risk Management**
- Risk Function Perspective
- Risk Management Perspective
- Risk Scenarios
- Trends
- Summary and Wrap-Up – Questions & Answers

The COBIT 5 Family

COBIT® 5

COBIT 5 Enabler Guides

COBIT® 5:
Enabling Processes

COBIT® 5:
Enabling Information

*Other Enabler
Guides*

COBIT 5 Professional Guides

COBIT® 5 Implementation

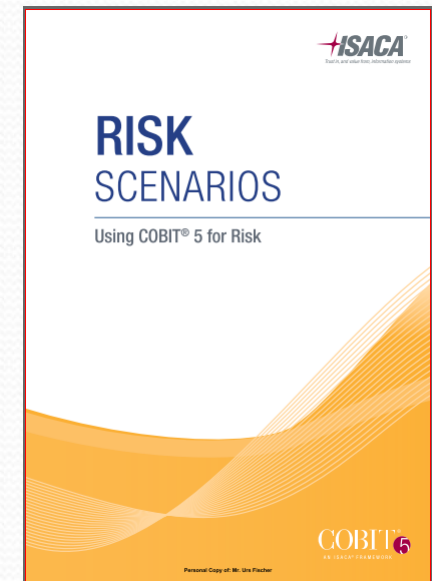
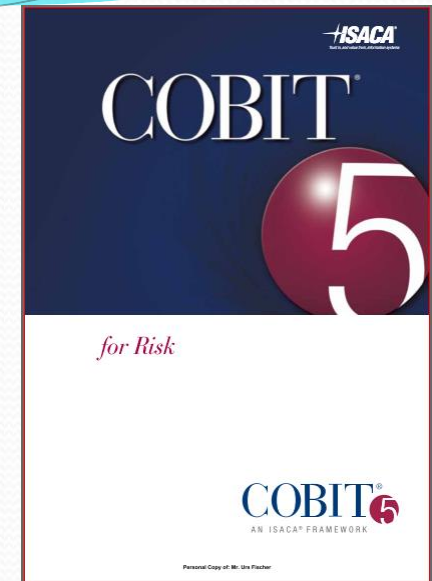
COBIT® 5
for Information
Security

COBIT® 5
for Assurance

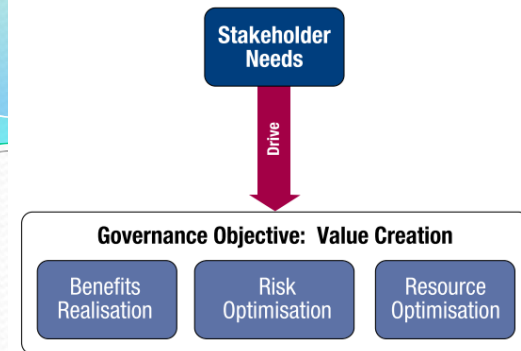
COBIT® 5
for Risk

*Other Professional
Guides*

COBIT 5 Online Collaborative Environment



Drivers for Risk Management



- Improve business outcomes, decision making and overall strategy by providing:
 - Stakeholders with substantiated and consistent opinions on the current state of risk throughout the enterprise
 - Guidance on how to manage the risk to levels within the risk appetite of the enterprise
 - Guidance on how to set up the appropriate risk culture for the enterprise
 - Wherever possible, quantitative risk assessments that enable stakeholders to consider the cost of mitigation and the required resources against the loss exposure

Effective Risk Management

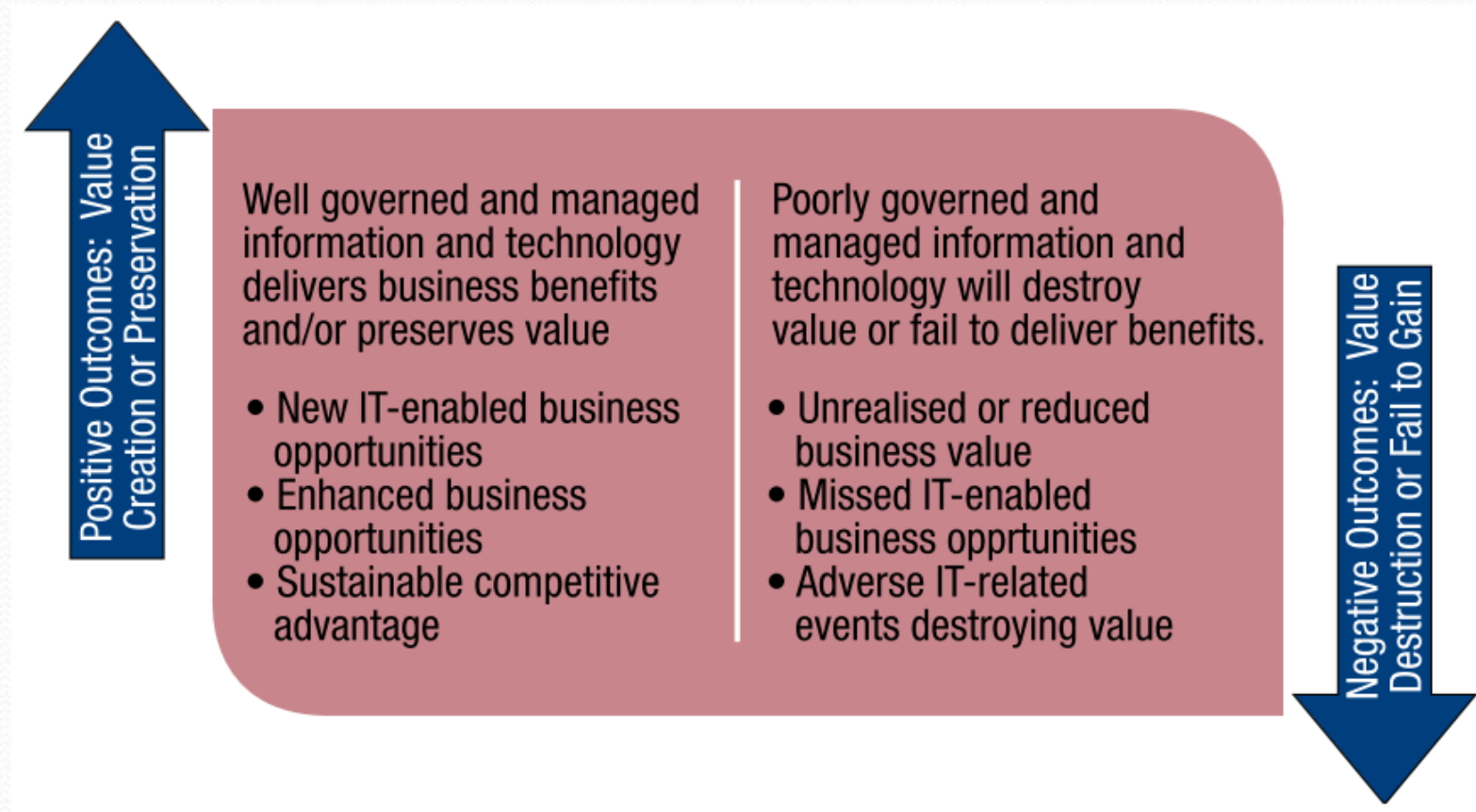
- Maintain focus on the business mission, goals and objectives
- Integrate IT risk management into enterprise risk management (ERM)
- Balance the costs and benefits of managing risk
- Promote fair and open communication
- Establish tone at the top, and assign personal accountability
- Promote continuous improvement as part of daily activities

IT Risk Categories

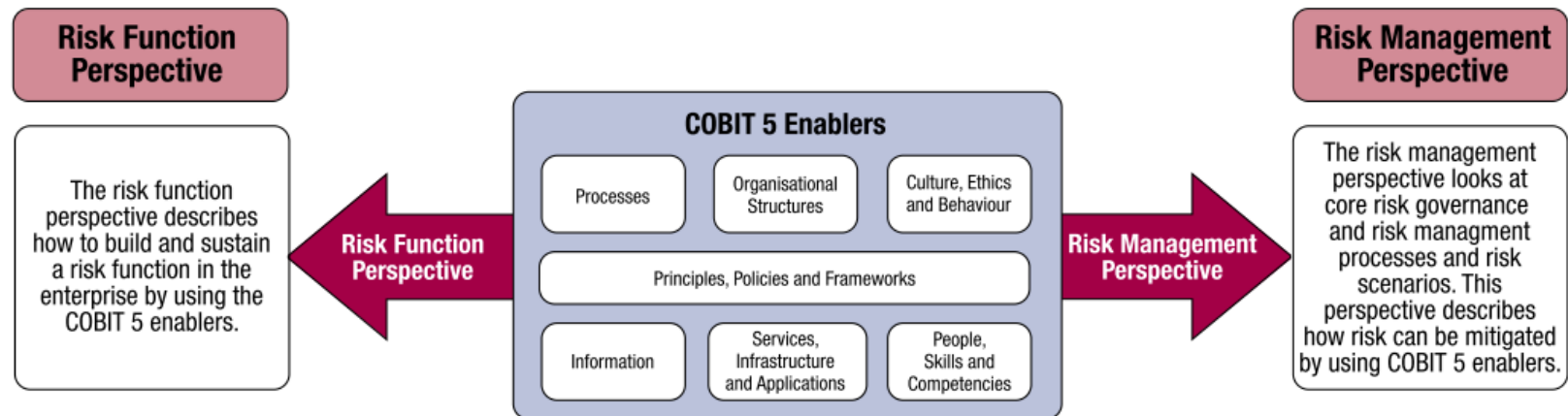
	Examples
IT Benefit/Value Enablement	<ul style="list-style-type: none">• Technology enabler for new business initiatives• Technology enabler for efficient operations
IT Programme and Project Delivery	<ul style="list-style-type: none">• Project quality• Project relevance• Project overrun
IT Operations and Service Delivery	<ul style="list-style-type: none">• IT service interruptions• Security problems• Compliance issues



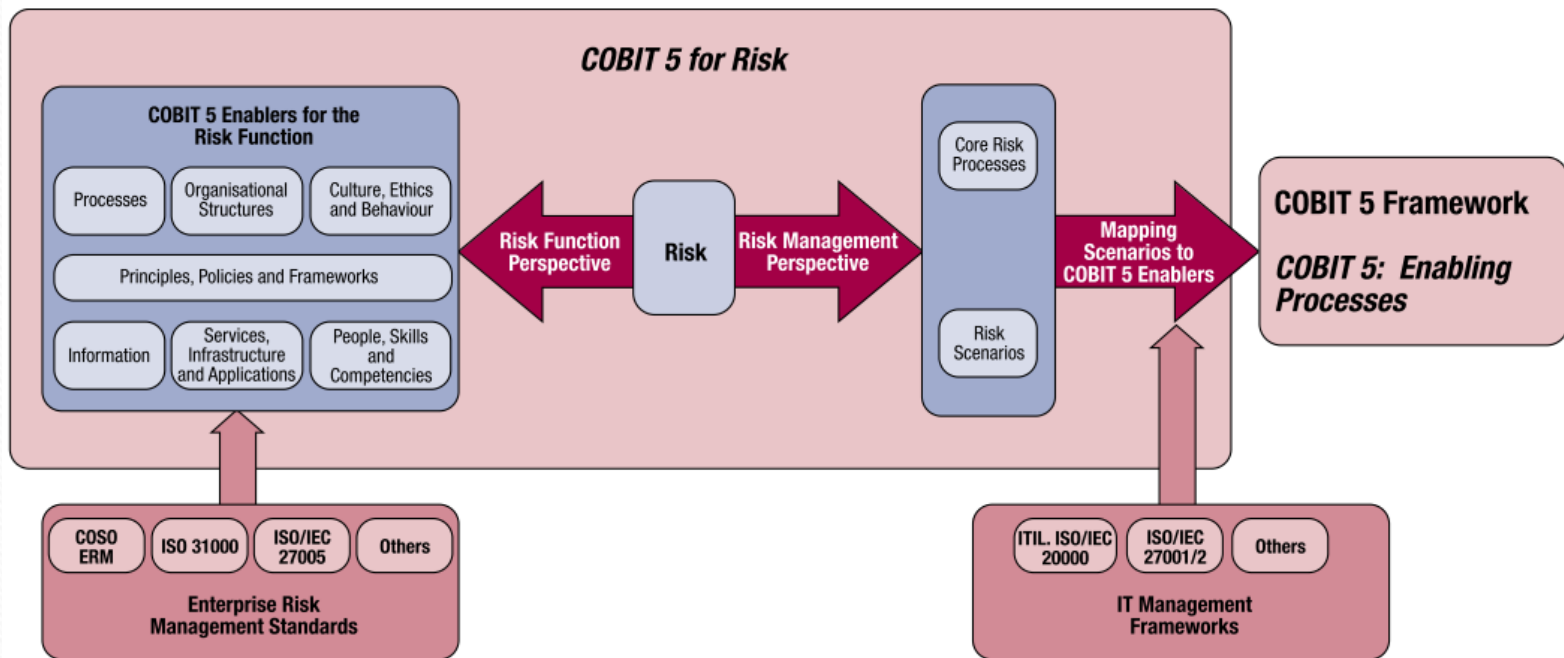
Duality of Risk



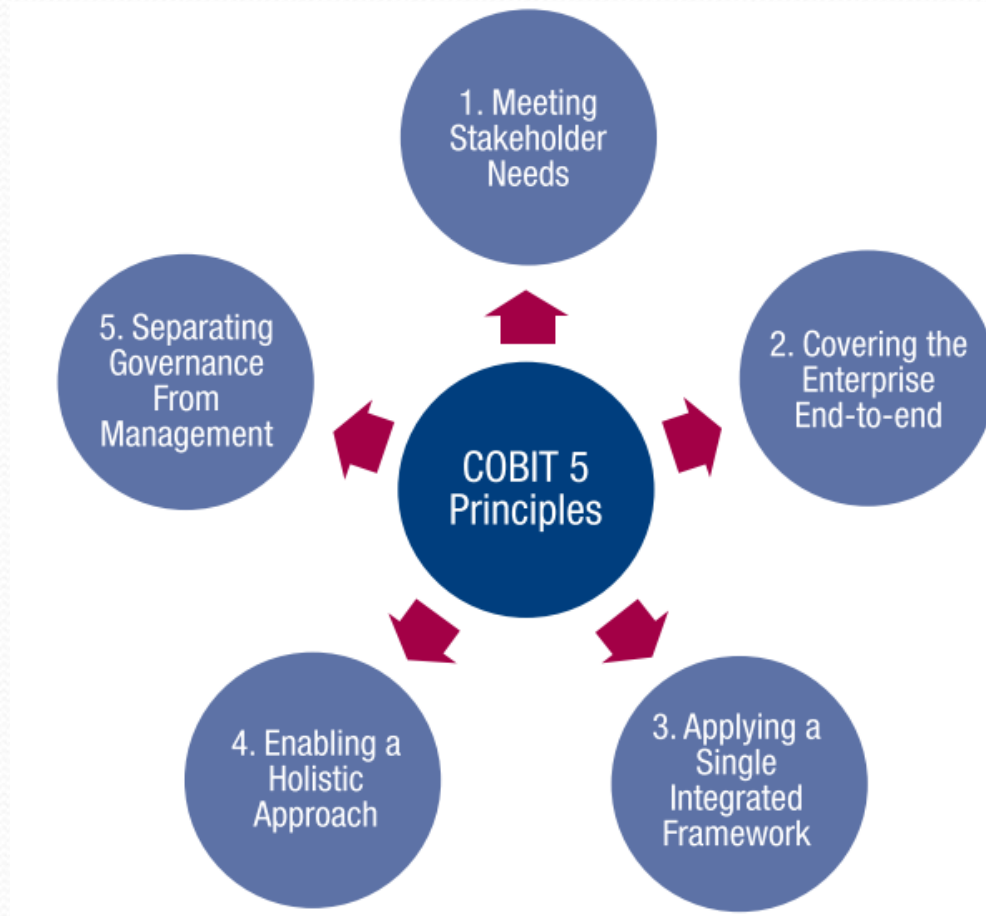
Terminology



Scope of COBIT 5 for Risk



Applying COBIT 5 Principles to Managing Risk



Risk Governance

- Sets the direction and strategy of the risk assessment efforts
- Defines risk culture and acceptable levels of risk
- Makes risk-aware business decisions
- Ensures that the risk management function is operating effectively to identify, manage, monitor and report on current and potential risks facing the enterprise

Risk Management

- Responsible for implementing IT risk operational activities while following policies set by those responsible for risk governance
- The means by which the governance body achieves IT risk objectives

Agenda

- Risk and Risk Management
- **Risk Function Perspective**
- Risk Management Perspective
- Risk Scenarios
- Trends
- Summary and Wrap-Up – Questions & Answers

Risk Function Perspective

Each enabler contributes, e.g.

- Processes (EDM01, APO01, etc.)
- Information flows (risk universe, risk profile, etc.)
- Organisational structures (ERM Committee, risk function, etc.)

Supporting Process for the Risk Function

Processes for Governance of Enterprise IT

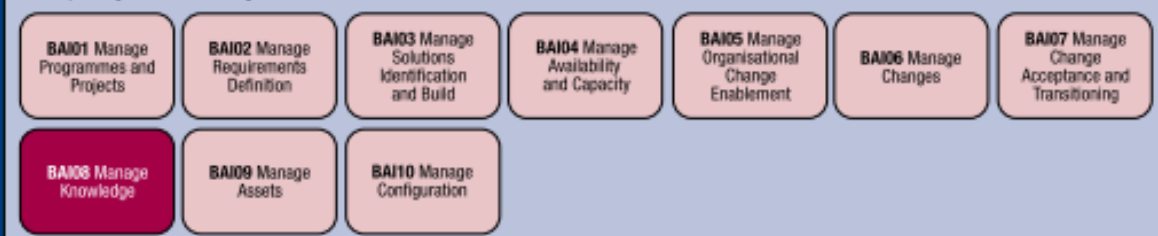
Evaluate, Direct and Monitor



Align, Plan and Organise



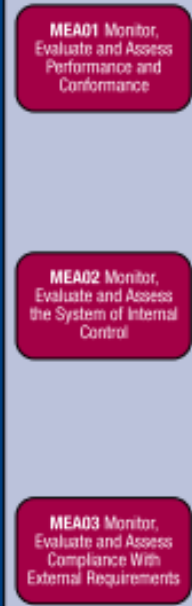
Build, Acquire and Implement



Deliver, Service and Support



Monitor, Evaluate and Assess

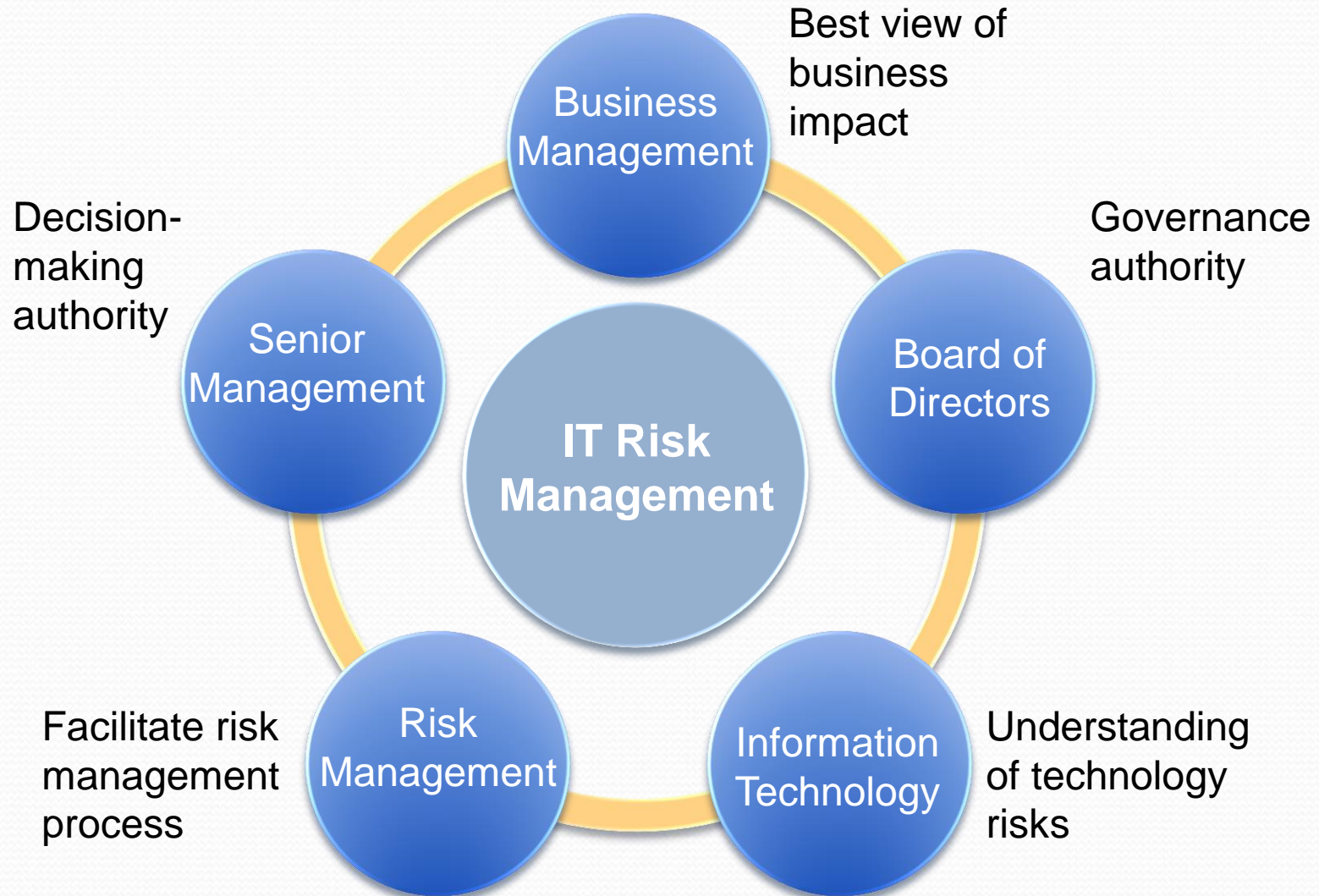


Processes for Management of Enterprise IT

Establish responsibility for:

- The risk **framework** in totality
- Risk **policy** setting and the project team's willingness to take risk
- Various elements of the risk **process**, such as identifying threats, through to producing risk response and reporting
- Implementation of the actual **measures** taken in response to the risks
- **Interdependent** risks that cross organizational boundaries, whether they be related to business processes, IT systems or other projects
- The risk **log**

Stakeholders in Risk Management



Lines of Defence Against Risk

Board/Enterprise Risk Committee

Operations

1st Line of Defence

Operations

**Enterprise Risk
Group**

2nd Line of Defence

Risk Function

Compliance

3rd Line of Defence

Audit Department

RACI Chart Demonstrates

- **Responsible (R)**—Those who must ensure that the activities are completed successfully
- **Accountable (A)**—Those who own the required resources and have the authority to approve the execution and/or accept the outcome of an activity
- **Consulted (C)**—Those whose opinions are sought on an activity (two-way communication)
- **Informed (I)**—Those who are kept up to date on the progress of an activity (one-way communication)

Elements of Risk Culture




Benefits of open communication of risk:

Management will understand the actual IT risk exposures, enabling informed risk decisions

Raise awareness within the enterprise, and encourage the integration of risk mindfulness into their daily duties

External stakeholders will be able to see that good risk management practices are in use

Consequences of poor communication of risk:




False sense of confidence about the levels of risk



Lack of direction or strategic risk planning



Poor communication of risk levels to clients, investors or regulators



Perception that the enterprise is trying to cover up known risk from stakeholders

Agenda

- Risk and Risk Management
- Risk Function Perspective
- **Risk Management Perspective**
- Risk Scenarios
- Trends
- Summary and Wrap-Up – Questions & Answers

Risk Management Perspective

Governance and management (e.g. how to identify, analyse and respond to risk)

- EDM03
Ensure risk optimisation
- APO12
Manage risk
- Risk scenarios

COBIT 5 Process Identification	Reasoning
EDM03 Ensure Risk Optimisation	<p>This process covers the understanding, articulation and communication of the enterprise risk appetite and tolerance and ensures identification and management of risk to the enterprise value that is related to IT use and its impact. The goals of this process are to:</p> <ul style="list-style-type: none">• Define and communicate risk thresholds and make sure that key IT-related risk is known.• Effectively and efficiently manage critical IT-related enterprise risk.• Ensure IT-related enterprise risk does not exceed risk appetite.
AP012 Manage Risk	<p>This process covers the continuous identification, assessment and reduction of IT-related risk within levels of tolerance set by enterprise executive management. Management of IT-related enterprise risk should be integrated with overall ERM. The costs and benefits of managing IT-related enterprise risk should be balanced by:</p> <ul style="list-style-type: none">• Collecting appropriate data and analysing risk• Maintaining the risk profile of the enterprise and articulating risk• Defining the risk management action portfolio and responding to risk

Risk Assessment

A top-level IT risk assessment is used to scope and prioritize further risk management action:

- Identifies high risk areas
- Provides an overview of major risk factors
- Will identify the major risk scenarios
- Should be repeated regularly

Risk Evaluation

Identified risks must be evaluated to determine their significance

- Compare estimated risk against given risk
- Output is a prioritized list of risks presented in business terms

Risk Analysis

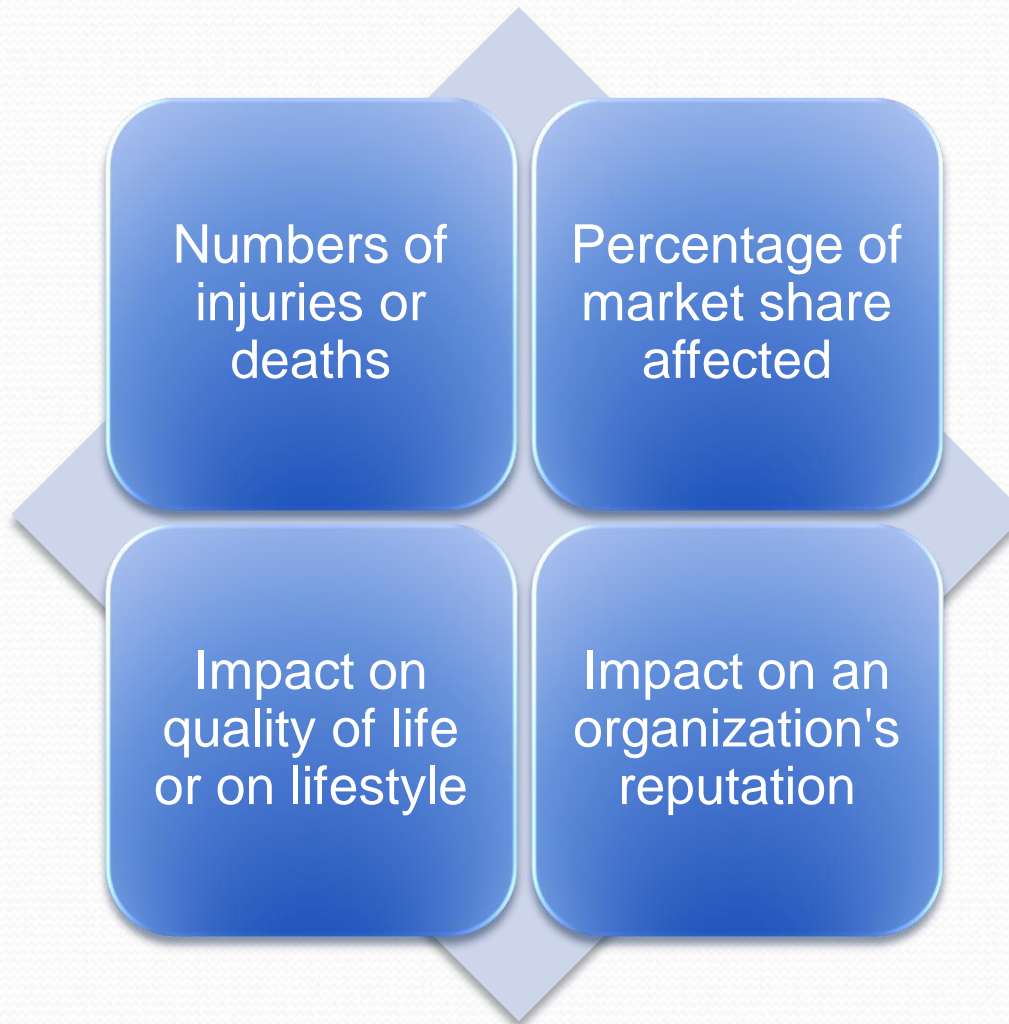
Analyze the scenarios to determine the probabilities of occurrence

- Validate data for accuracy and completeness first
- Data can be used to select risk response options
- Format the output for reporting purposes

Measuring consequences in financial terms:

- Provides a common metric for comparing dissimilar conditions
- Provides a compelling motivation for action

Can measure consequences in terms of:



Expressing Consequences

COBIT Information Criteria

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

Expressing Consequences

Balanced Scorecard (BSC)

- Financial
- Customer
- Internal
- Growth

Expressing Consequences

Extended BSC

- Financial
 - Share value
 - Profit
 - Revenue
 - Cost of capital
- Customer
 - Market share
 - Customer satisfaction
 - Customer service
- Internal
 - Regulatory compliance
- Growth
 - Competitive advantage
 - Reputation

Expressing Consequences

- Agility
- Accuracy
- Access
- Availability

Westerman

Expressing Consequences

- Strategic
- Operations
- Reporting
- Compliance

COSO ERM

Expressing Consequences

- Productivity
- Response
- Replacement
- Competitive advantage
- Legal
- Reputation

FAIR

Agenda

- Risk and Risk Management
- Risk Function Perspective
- Risk Management Perspective
- **Risk Scenarios**
- Trends
- Summary and Wrap-Up – Questions & Answers

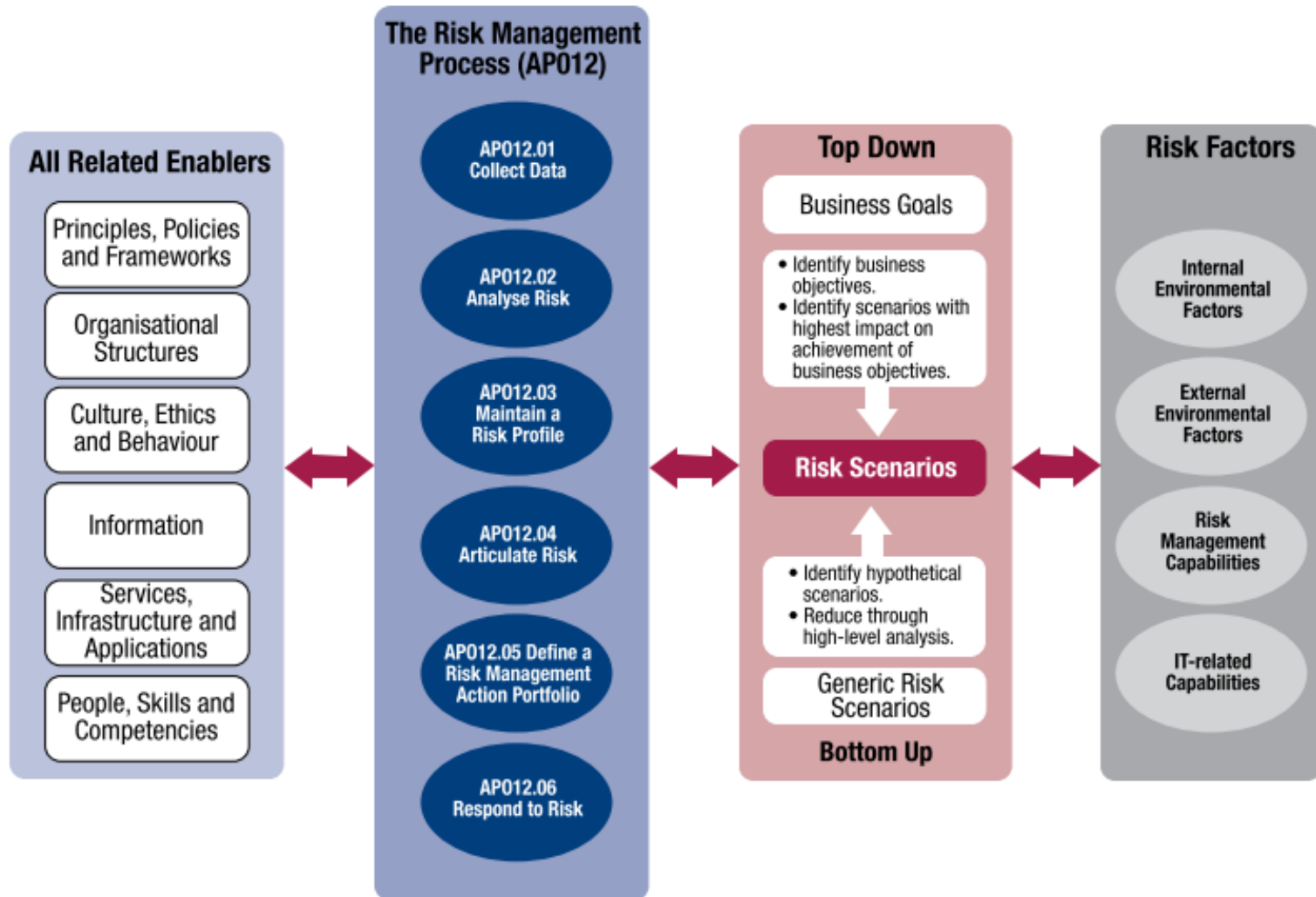
Risk Scenario

- A description of an event that, when and if it should occur, can lead to a business impact
- A technique used to make risk more concrete and tangible and enable effective risk assessment and analysis
- Used during risk analysis where the frequency and impact of risk are estimated and recorded

Risk scenario development is the core approach to:

- Bring practicality
- Provide insight
- Encourage organizational engagement
- Provide improved analysis and structure to the complex nature of enterprise risk

Risk Scenarios



Top-down Scenario Identification

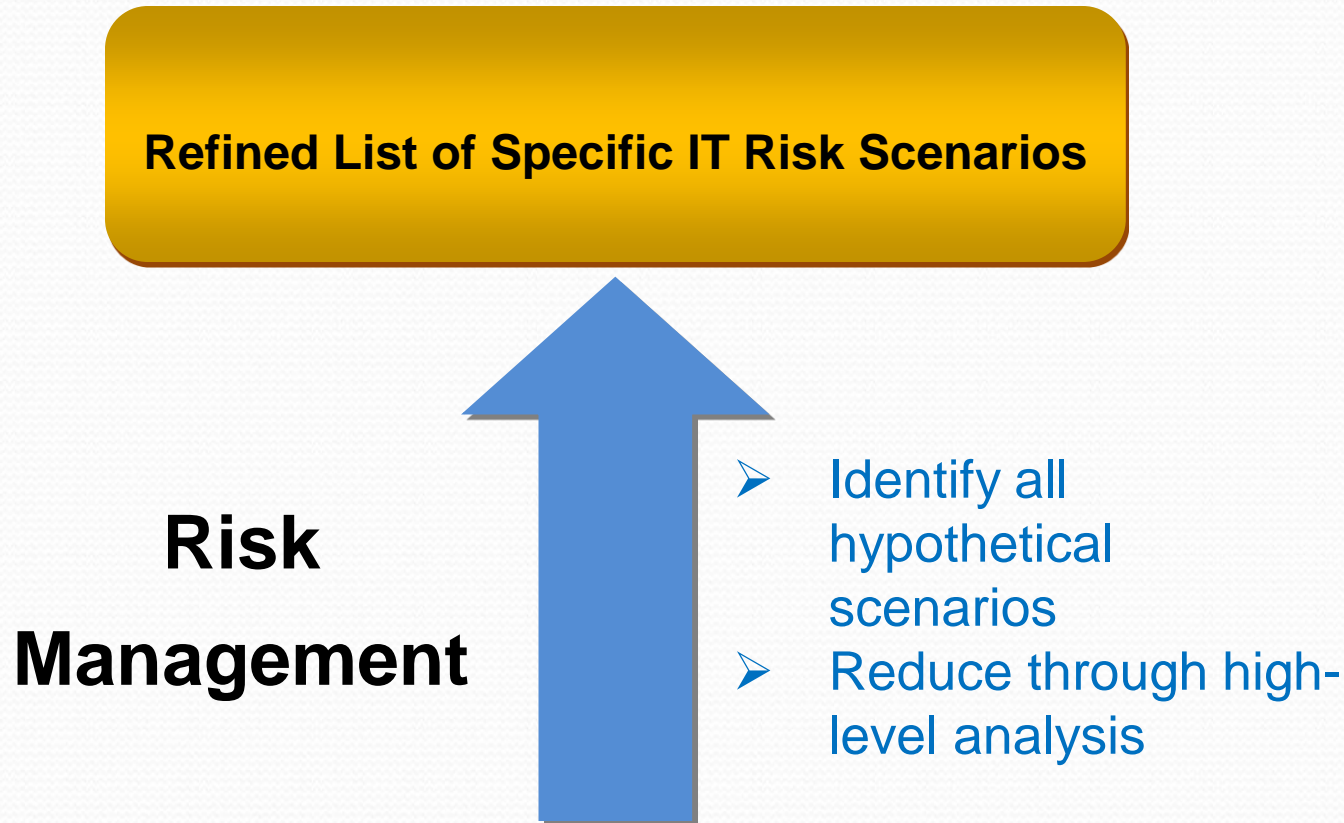
**Risk
Governance**



- Identify business objectives
- Identify scenarios with most impact on achievement of objectives

Refined List of Specific IT Risk Scenarios

Bottom-up Scenario Identification



Risk Scenario Workflow

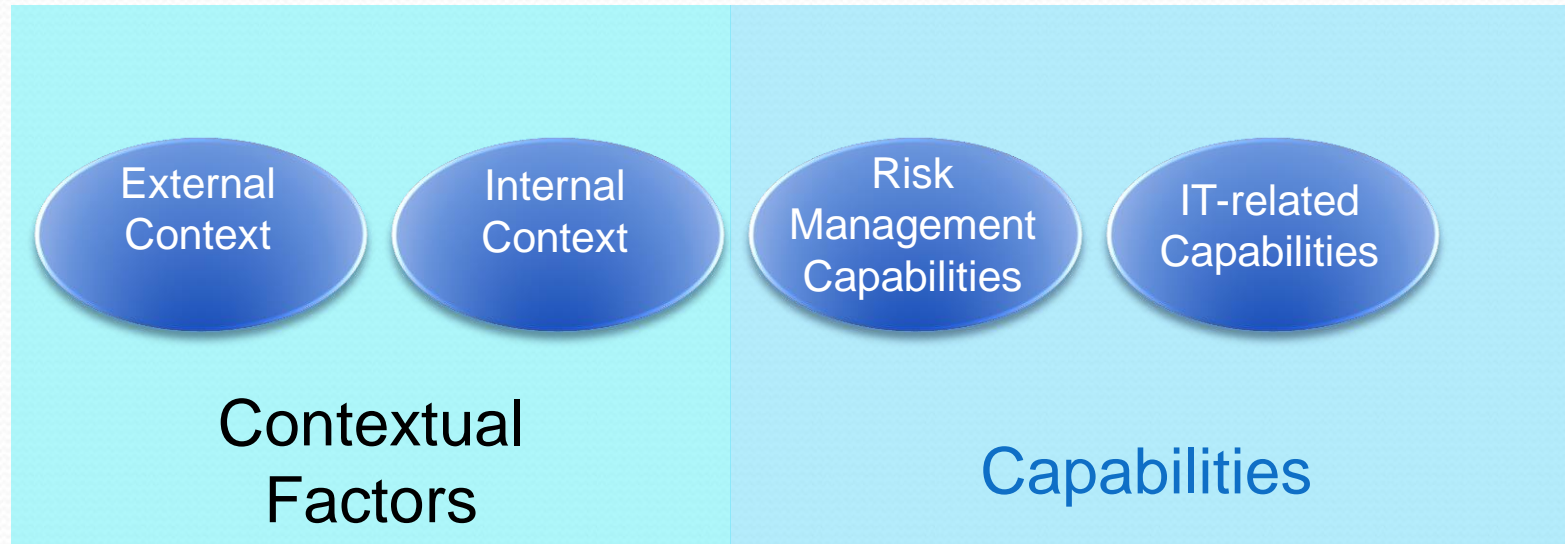
Use generic scenarios to define a set for your enterprise; include some less common situations.

Perform validation against business objectives.

Reduce the number of scenarios to a manageable set; keep a list for future review.

Add one unspecified scenario for response to unforeseen events.

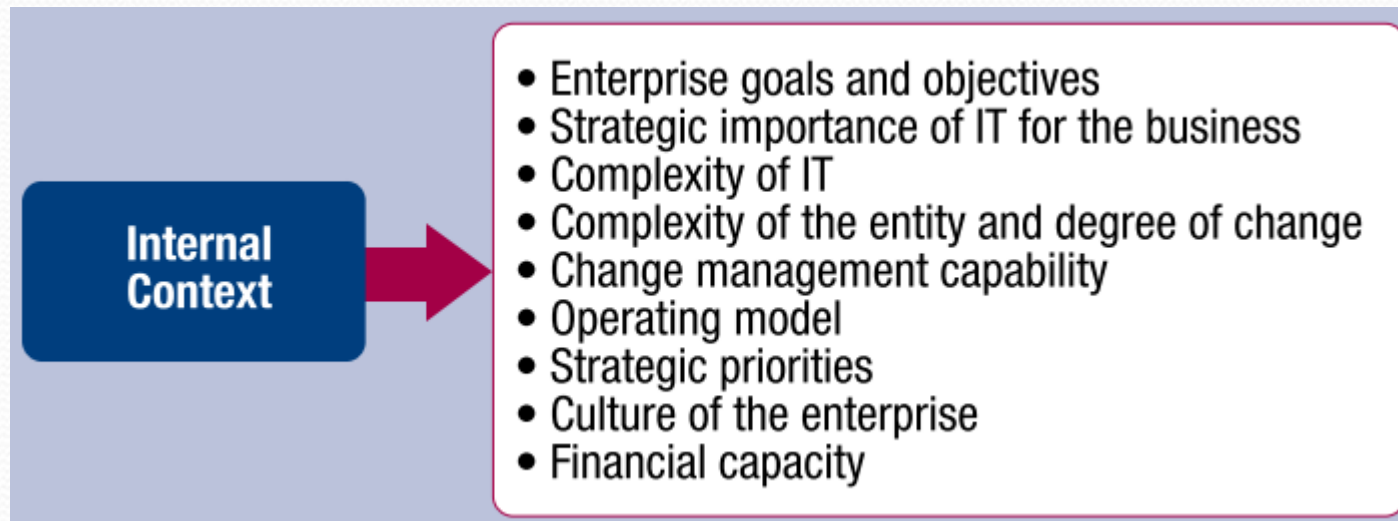
Risk Factor Categories



External Context



Internal Context



Risk Management Capabilities

**Risk
Management
Capabilities**



- Risk governance
- Risk management

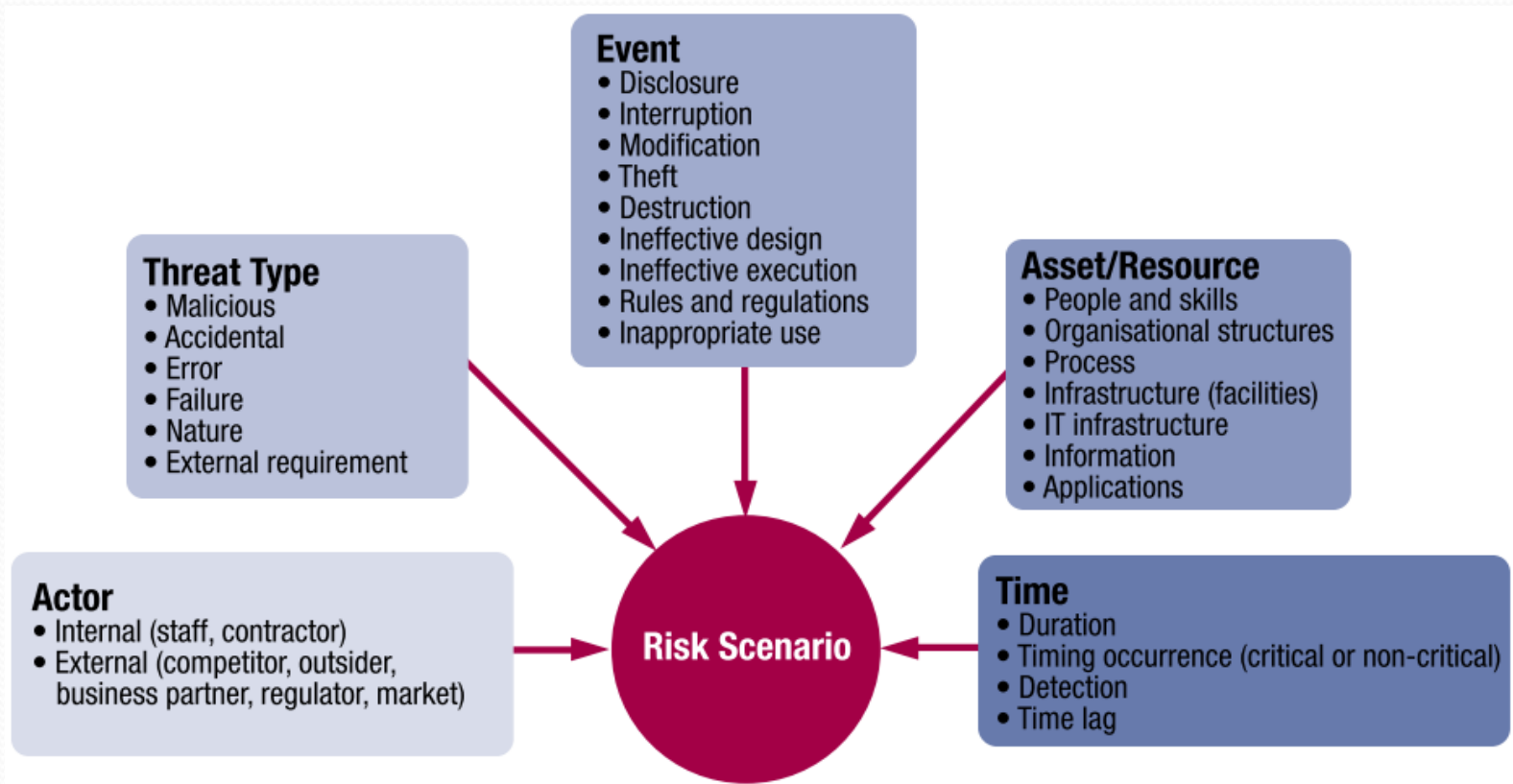
IT-related Capabilities

**IT-related
Capabilities**



- Evaluate, direct and monitor (EDM)
- Align, plan and organise (APO)
- Build, acquire and implement (BAI)
- Deliver, service and support (DSS)
- Monitor, evaluate and assess (MEA)

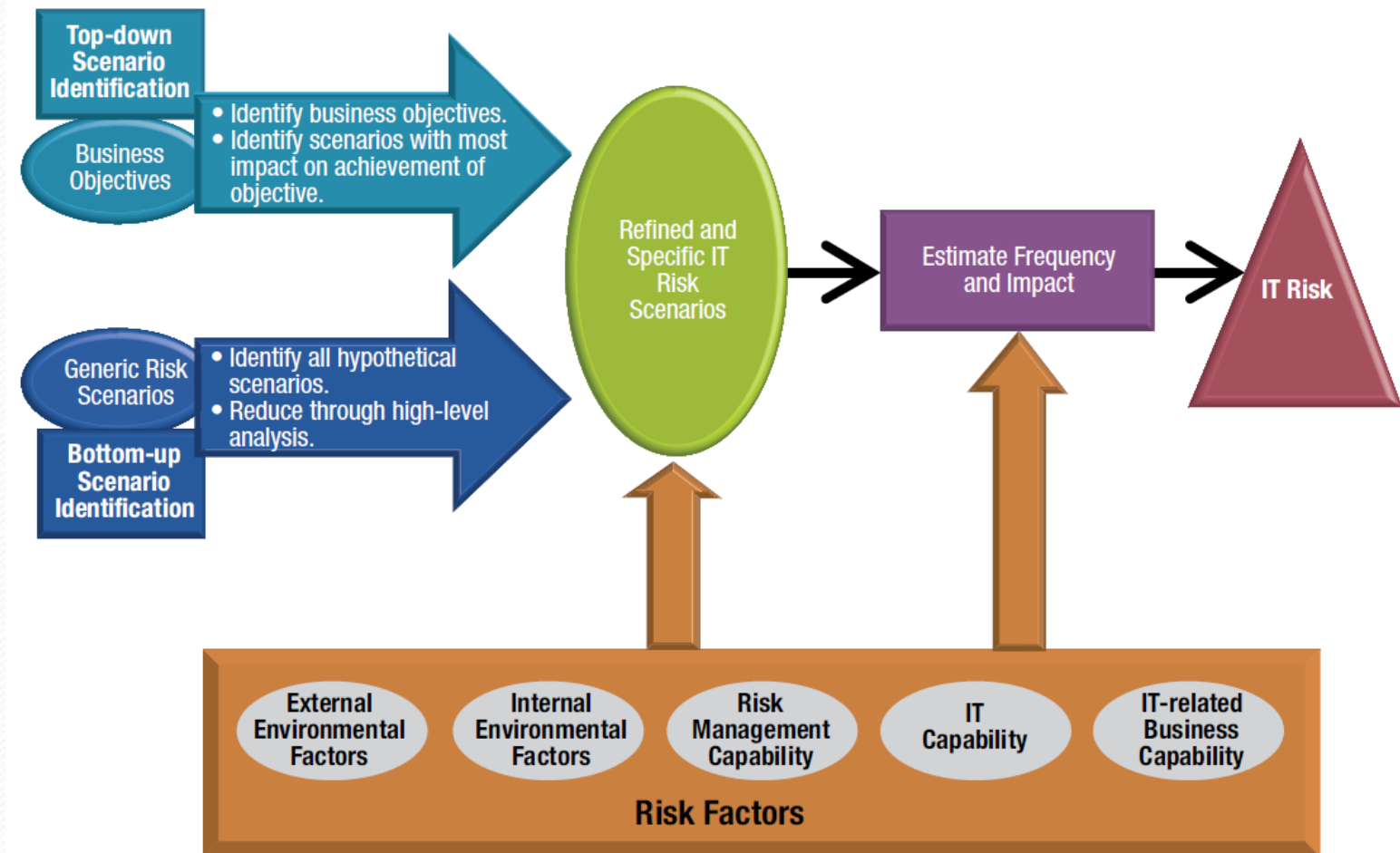
IT Risk Scenario Structure



Generic risk example build with this structure

Ref.	Risk Scenario Category	Risk Type			Example Scenarios	
		IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Negative Example Scenarios	Positive Example Scenarios
0408	IT expertise and skills <i>(cont.)</i>	S	P	P	There is an overreliance on key IT staff.	Job rotation ensures that nobody alone possesses the entire knowledge of the execution of a certain activity.
0409		S	P	P	There is an inability to update the IT skills to the proper level through training.	Training, attending seminars and reading thought leadership ensures that IT staff is up to date with the latest developments in its area of speciality.
0501	Staff operations (human error and malicious intent)	S	S	P	Access rights from prior roles are abused.	HR and IT administration co-ordinate on a frequent basis to ensure timely removal of access rights, avoiding the possibility of abuse.
0502		S		P	IT equipment is accidentally damaged by staff.	
0503		S		P	There are errors by IT staff (during backup, during upgrades of systems, during	The 4-eye principle is applied, decreasing the possibility of errors before moving to

IT Risk Scenario Development Summary



When developing a set of scenarios,
consider:

Expertise and experience

Thorough understanding of the environment

Input from all parties involved

Brainstorming approach

Gain buy-in from affected parties

When developing a set of scenarios, consider (continued):

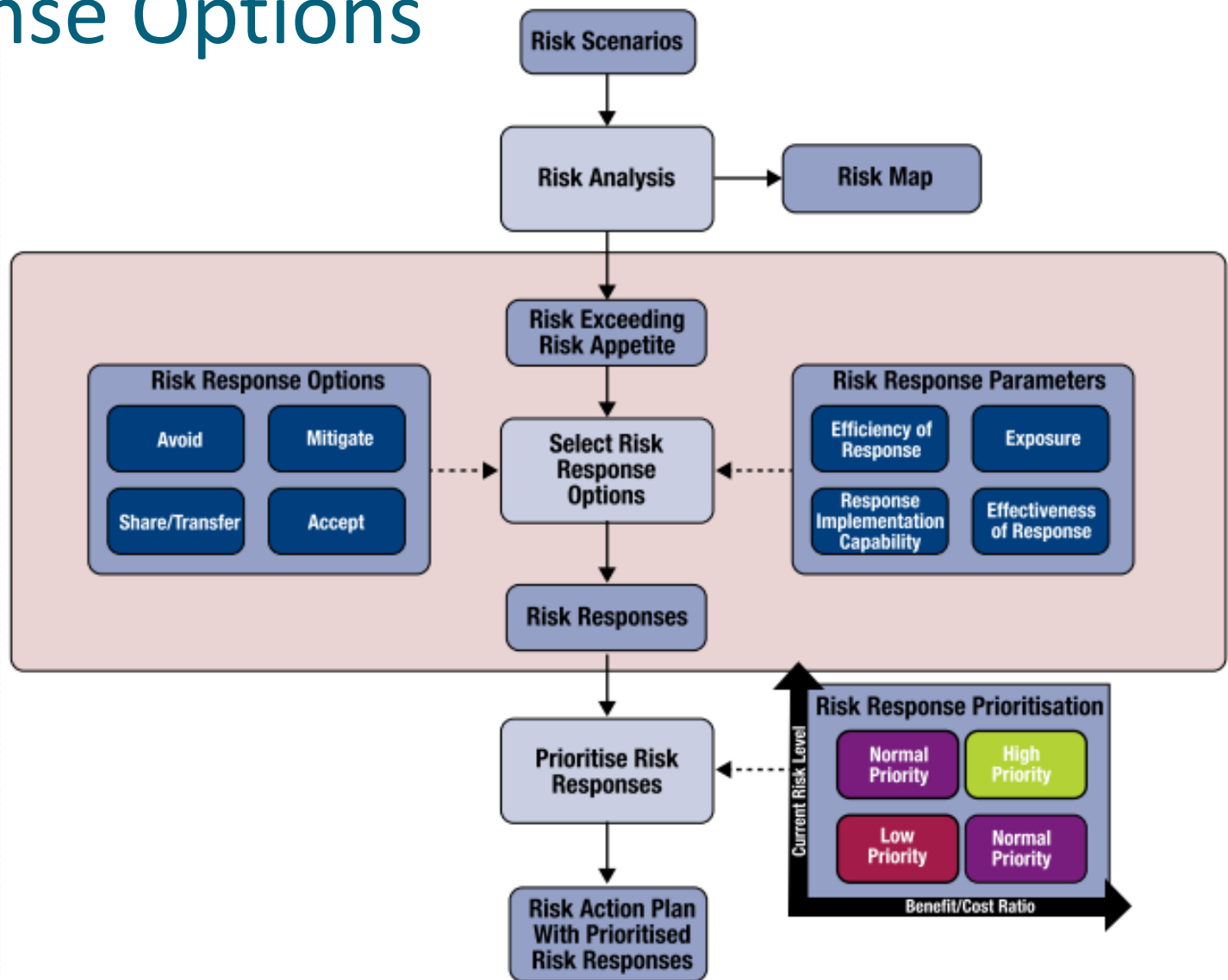
Include staff familiar with vulnerabilities.

Include external third-party vendors, law enforcement and others.

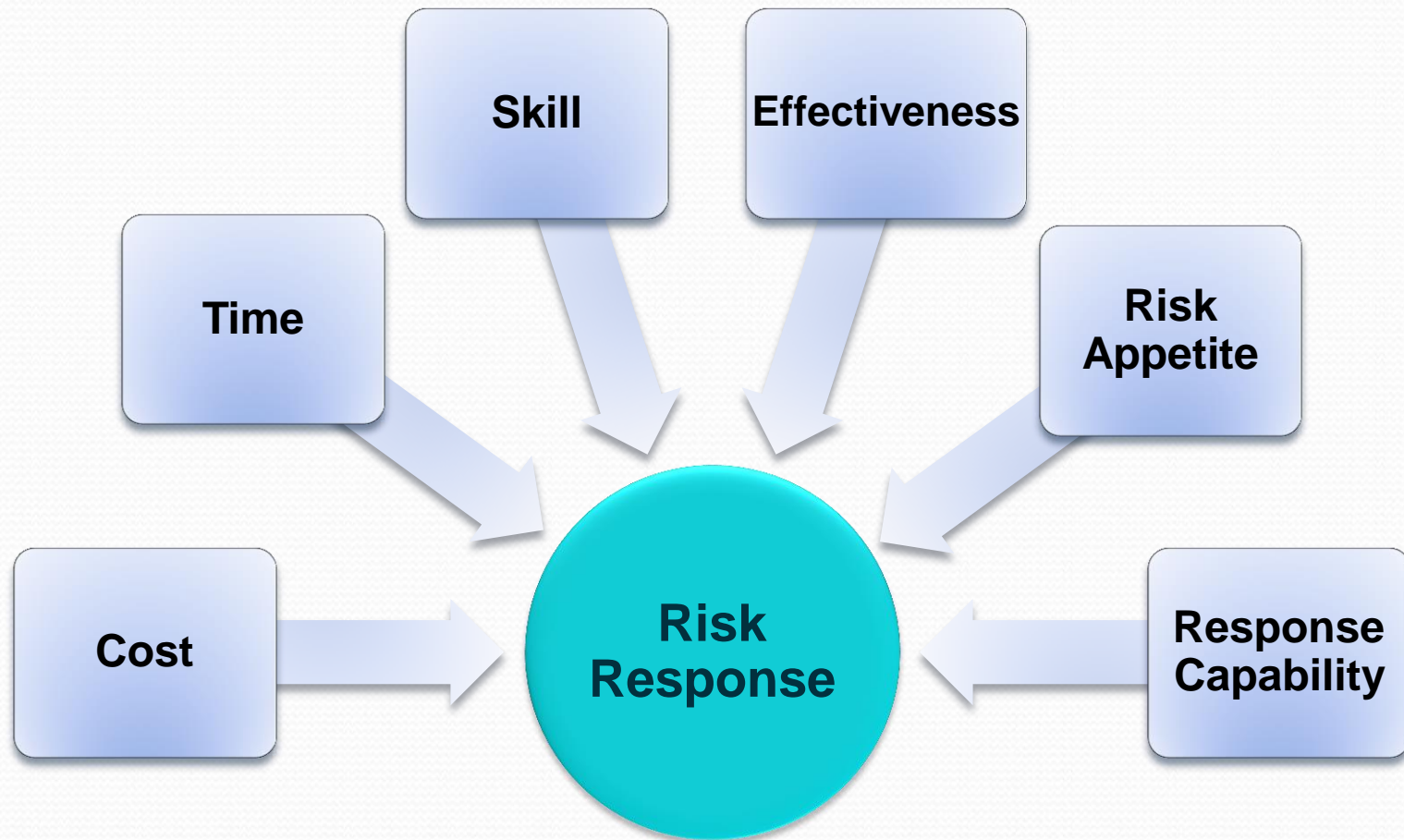
Do not include worst-case events; they rarely materialize.

Remember to include the upside of risk.

Risk Response Workflow and Risk Response Options



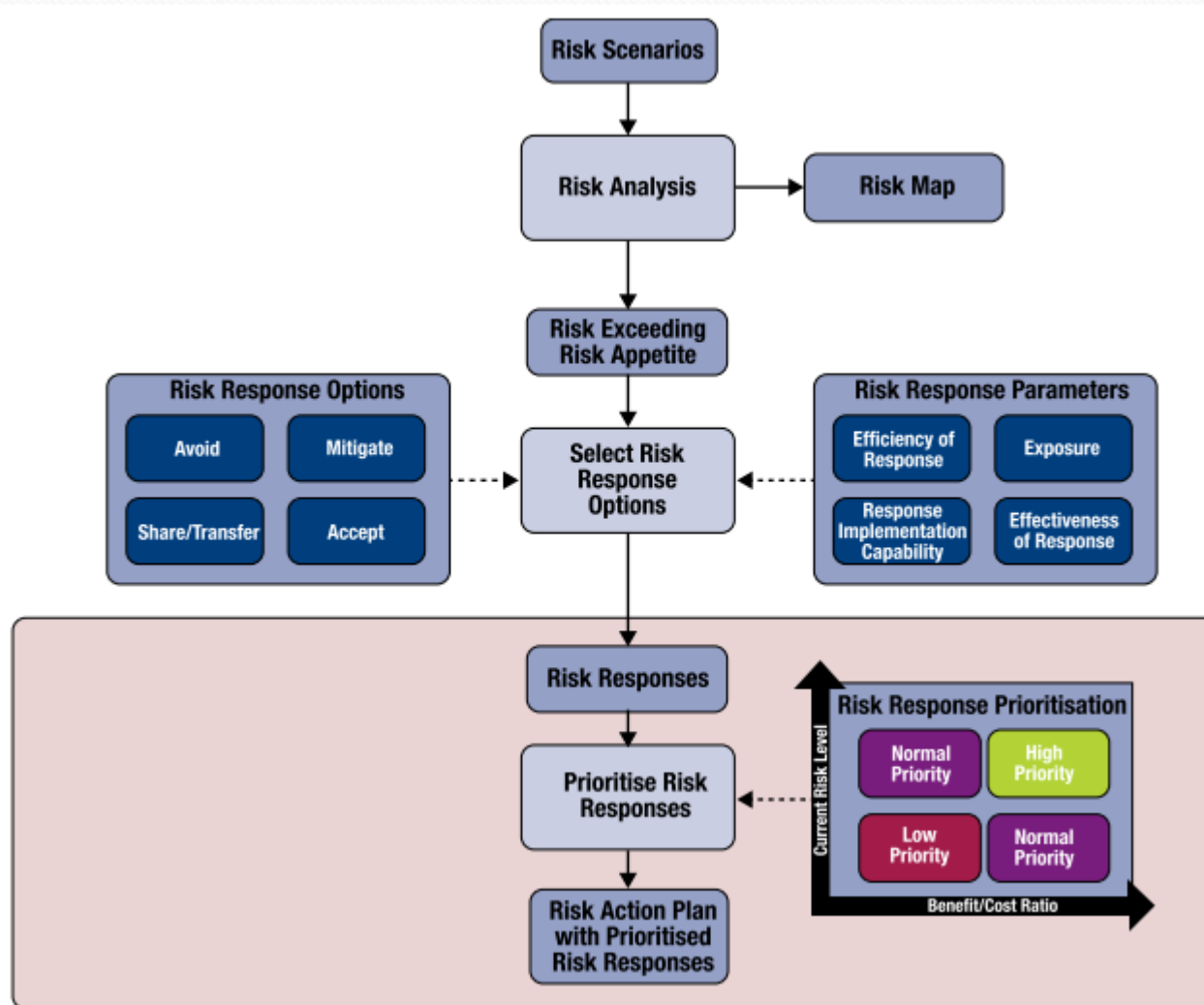
Factors when selecting risk response:



What Risk Response?



Risk Response Selection and Prioritisation



Agenda

- Risk and Risk Management
- Risk Function Perspective
- Risk Management Perspective
- Risk Scenarios
- **Trends**
- Summary and Wrap-Up – Questions & Answers

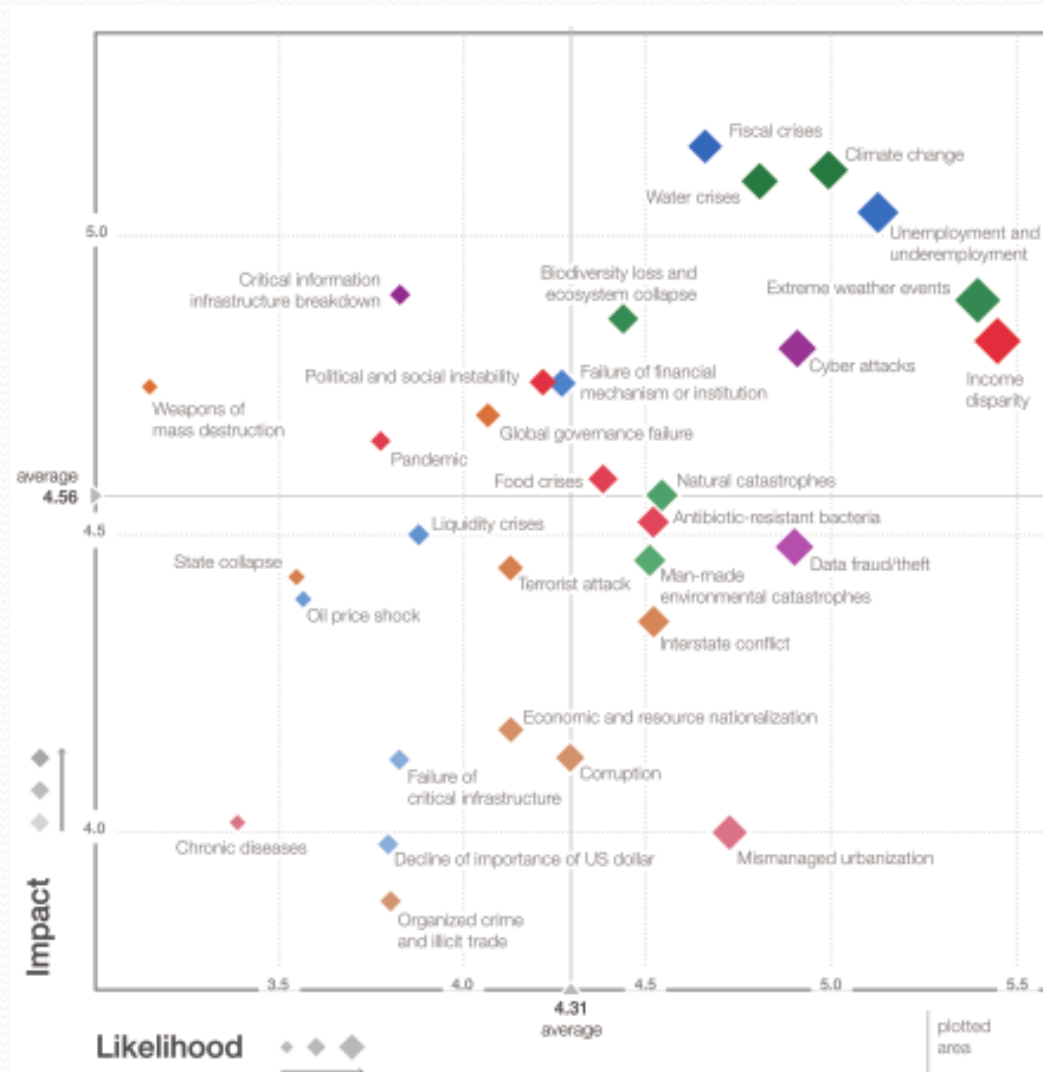
Global Risks 2014 WEF (31 Risks)

- Technology Risk
 - Breakdown of critical information infrastructure and networks
 - Escalation in large-scale cyber attacks
 - Massive incident of data fraud/theft
- Economic Risk
 - Failure/shortfall of critical infrastructure
- Environmental Risk
 - Greater incidence of extreme weather events (e.g. flood, storms, fires)
 - Greater influence of natural catastrophes (e.g. earthquakes, tsunamis, volcanic eruptions, geomagnetic storms)

Global Risks 2014 WEF (31 Risks) cont.

- Geopolitical
 - Global governance failure
 - Major escalation in organized crime and illicit trade
 - Large-scale terrorist attacks
- Societal
 - Pandemic outbreak
 - Mismanaged urbanization (e.g. planning failures, inadequate infrastructure and supply chains)
- Environmental Risk
 - Greater incidence of extreme weather events (e.g. flood, storms, fires)
 - Greater influence of natural catastrophes (e.g. earthquakes, tsunamis, volcanic eruptions, geomagnetic storms)

WEF: The Global Risk Landscape



WEF: Likelihood – Top 5

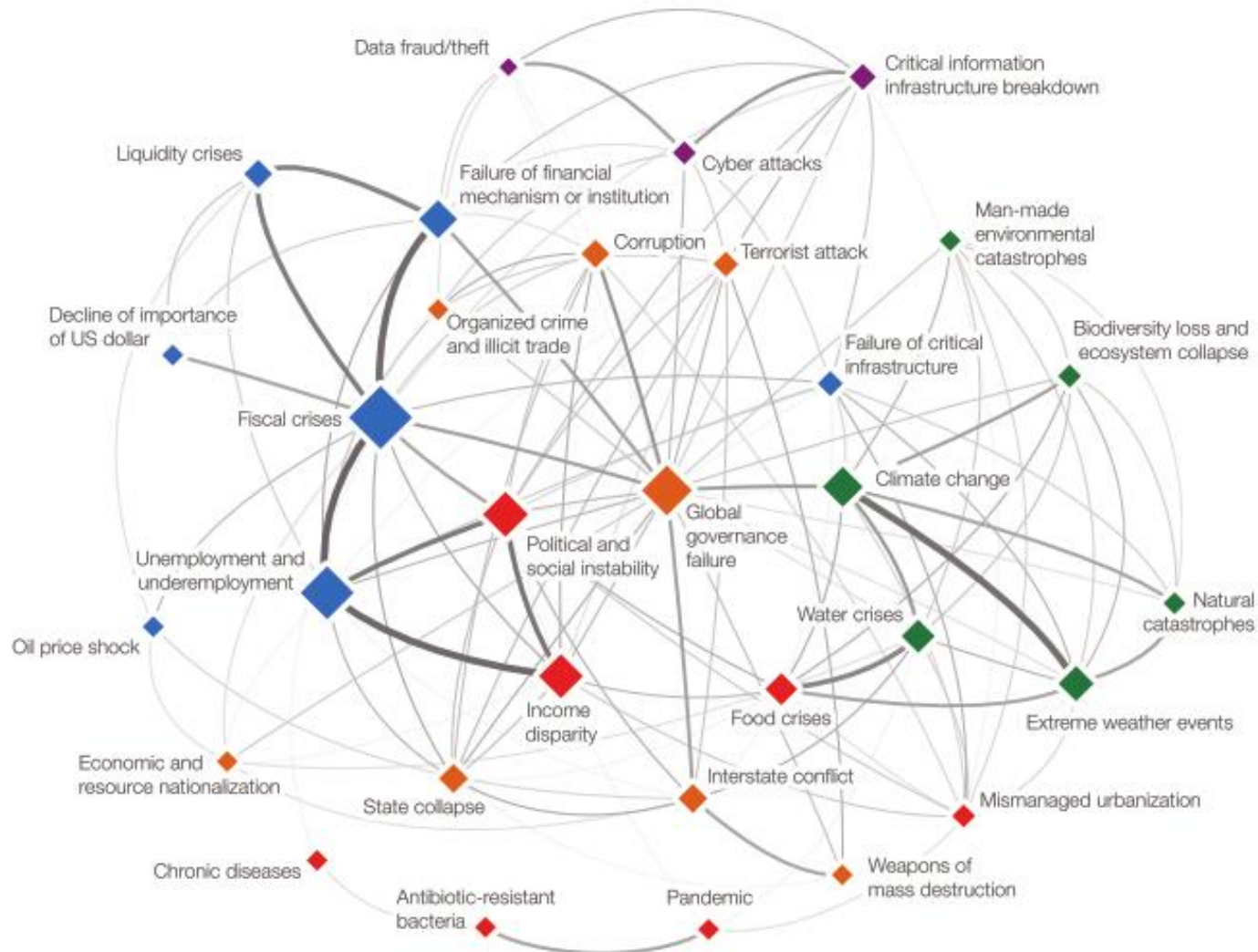
	2007	2008	2009	2010	2011	2012	2013	2014
1st	Breakdown of critical information infrastructure	Asset price collapse	Asset price collapse	Asset price collapse	Storms and cyclones	Severe income disparity	Severe income disparity	Income disparity
2nd	Chronic disease in developed countries	Middle East instability	Slowing Chinese economy (<6%)	Slowing Chinese economy (<6%)	Flooding	Chronic fiscal imbalances	Chronic fiscal imbalances	Extreme weather events
3rd	Oil price shock	Failed and failing states	Chronic disease	Chronic disease	Corruption	Rising greenhouse gas emissions	Rising greenhouse gas emissions	Unemployment and underemployment
4th	China economic hard landing	Oil and gas price spike	Global governance gaps	Fiscal crises	Biodiversity loss	Cyber attacks	Water supply crises	Climate change
5th	Asset price collapse	Chronic disease, developed world	Retrenchment from globalization (emerging)	Global governance gaps	Climate change	Water supply crises	Mismanagement of population ageing	Cyber attacks

WEF: Impact – Top 5

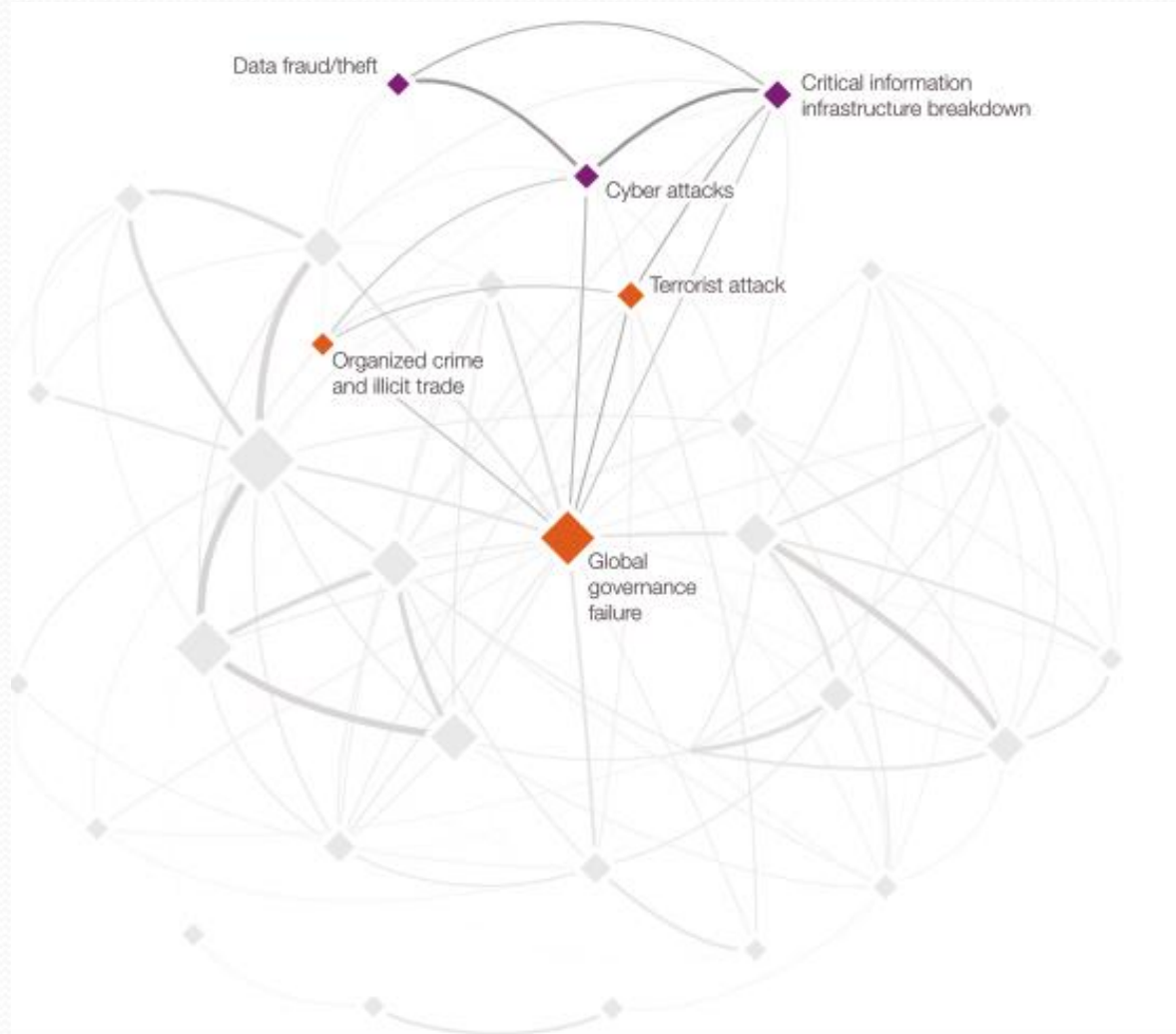
	2007	2008	2009	2010	2011	2012	2013	2014
1st	Asset price collapse	Asset price collapse	Asset price collapse	Asset price collapse	Fiscal crises	Major systemic financial failure	Major systemic financial failure	Fiscal crises
2nd	Retrenchment from globalization	Retrenchment from globalization (developed)	Retrenchment from globalization (developed)	Retrenchment from globalization (developed)	Climate change	Water supply crises	Water supply crises	Climate change
3rd	Interstate and civil wars	Slowing Chinese economy (<6%)	Oil and gas price spike	Oil price spikes	Geopolitical conflict	Food shortage crises	Chronic fiscal imbalances	Water crises
4th	Pandemics	Oil and gas price spike	Chronic disease	Chronic disease	Asset price collapse	Chronic fiscal imbalances	Diffusion of weapons of mass destruction	Unemployment and underemployment
5th	Oil price shock	Pandemics	Fiscal crises	Fiscal crises	Extreme energy price volatility	Extreme volatility in energy and agriculture prices	Failure of climate change adaptation	Critical information infrastructure breakdown

■ Economic
 ■ Environmental
 ■ Geopolitical
 ■ Societal
 ■ Technological

WEF: Interconnections Map 2014



The Worst-Case Scenario: “Cybergeddon”



Agenda

- Risk and Risk Management
- Risk Function Perspective
- Risk Management Perspective
- Risk Scenarios
- Trends
- **Summary and Wrap-Up – Questions & Answers**

Summary and Wrap-Up

Questions and answers



Thank you very much!

fischer

IT GRC

BERATUNG
SCHULUNG

Contact Details:

Urs Fischer CPA (Swiss), CRISC, CISA, CIA
Fischer IT GRC Consulting & Training

Xing: https://www.xing.com/profile/Urs_Fischer12

Linkedin: http://www.linkedin.com/profile?viewProfile=&key=43663087&trk=tab_pro

fischer
IT GRC BERATUNG
SCHULUNG

Urs Fischer
Geschäftsführer

Dorfstrasse 1A
CH-5430 Wettingen
T+F +41 56 430 29 29
M +41 79 457 79 89
www.fischer-it-grc.ch
urs@fischer-it-grc.ch

Urs Fischer

- CPA (Swiss) by origin, CRISC, CISA & CIA
- 5 year external auditor
- Switch to IT Audit – In IT Audit for 13 years incl. Head of IT Audit
- 2004-2010 Head IT Governance & Risk Management
- Since 2011 independent IT GRC Consultant and Trainer (different mandates with e.g. Swisscom, UBS, PostFinance, Medecins Sans Frontiers, Swiss Re, ISACA etc.)

- Co-Author of CobiT4 and participant of the development workshops for COBIT5
- Co-Developer of CobiT Control Practices
- Co-Developer of ISACA's "IT Control Objectives for Cloud Computing"
- **Chair of the Task Force that developed 'Risk IT' and 'Risk IT Practitioner's Guide'**
- **Expert reviewer of 'COBIT 5 for Risk'**
- **Lead-Developer of ISACA's "Risk Scenarios Using COBIT 5"**

- Board member of ISACA CH Chapter for about 8 years
- Member of the CobiT Steering Committee for 3 years
- Member and Chair of ISACA's EuroCACS Conference Programme Committee for 6 years
- 2008 – 2009 Chair of ITGI's 'Risk IT' Task Force
- 2009 – 2010 Chair of ISACA's CRISC Task Force
- 2006 – 2011 Member of ISACA Audit Committee (2008 – 2011 Chairman)
- 2010 – 2011 Member of ISACA's Guidance and Practice Committee
- 2009 – 2012 Member of ISACA's Credentialing Board
- 2010 – 2012 Chair of ISACA's CRISC Committee
- 2012 – Member of ISACA/ITGI's Nomination Committee

- 2010 Receiver of the 'John W. Lainhart IV – Common Body of Knowledge Award'