IT Risk Management

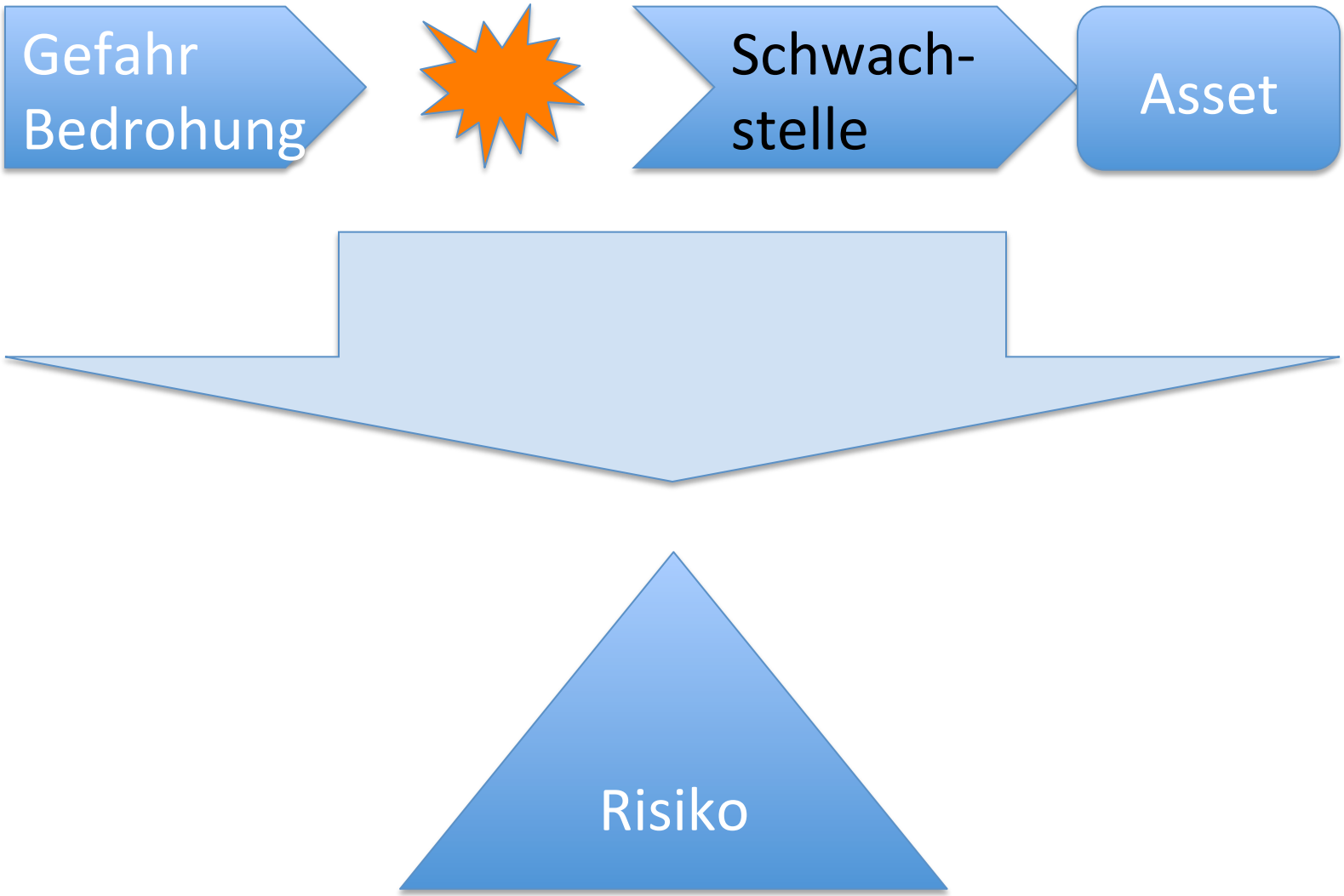
Digicomp Hacking Day, 11.06.2014

Umberto Annino

- Wer spricht?
  Umberto Annino
  Wirtschaftsinformatiker, Information Security

- Was ist ein Risiko?
  → Sicherheit ist das Komplementärereignis zum Risiko
  → Risiko ist Schaden mit Potenzial

Risiko



Realitätsabgleich

Compliance?

Risk Management?

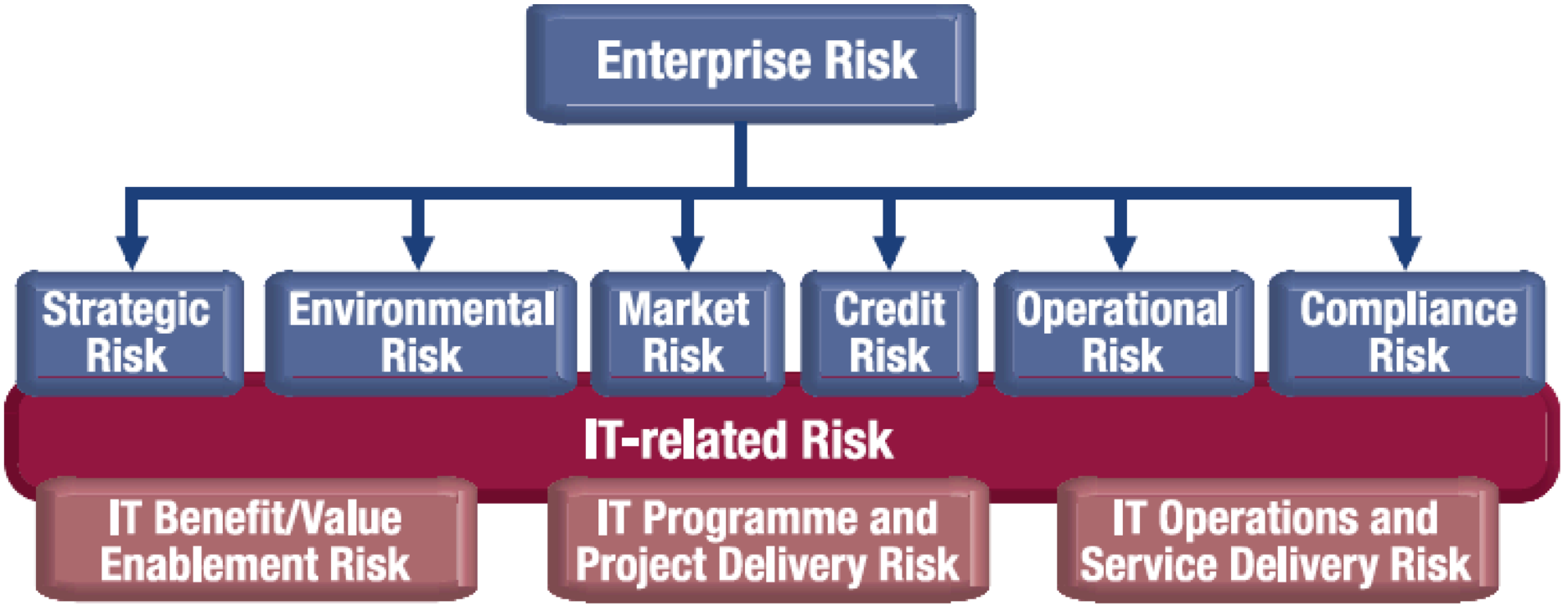
Operational Risk, Business Continuity?

IT, Information Security – Cyber Security?

Red Team, Threat Modeling, APT and openSSL? Big Data???

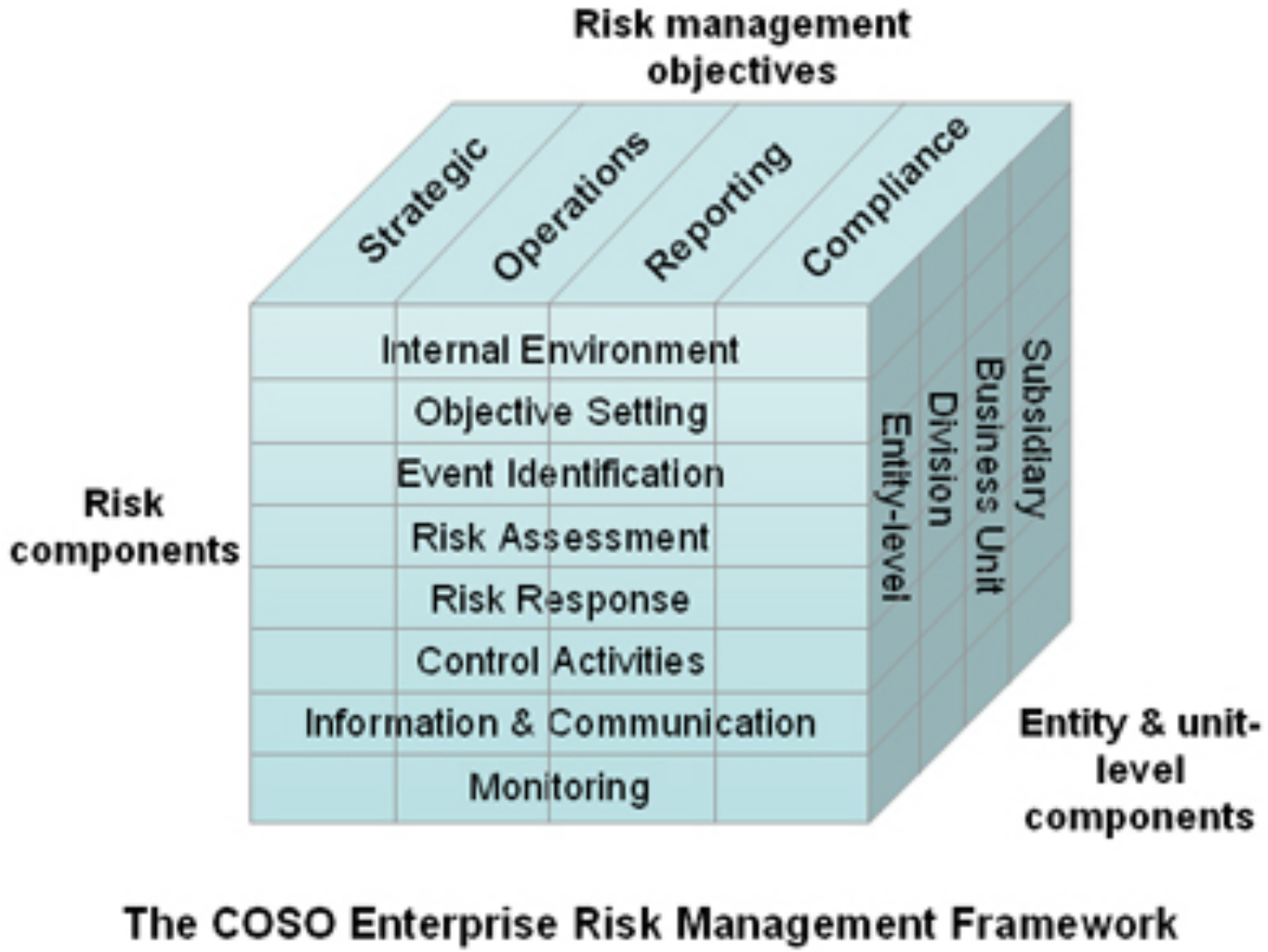
Security ™ vs. Compliance ™

IT Risiko in der Risiko-Hierarchie



COSO

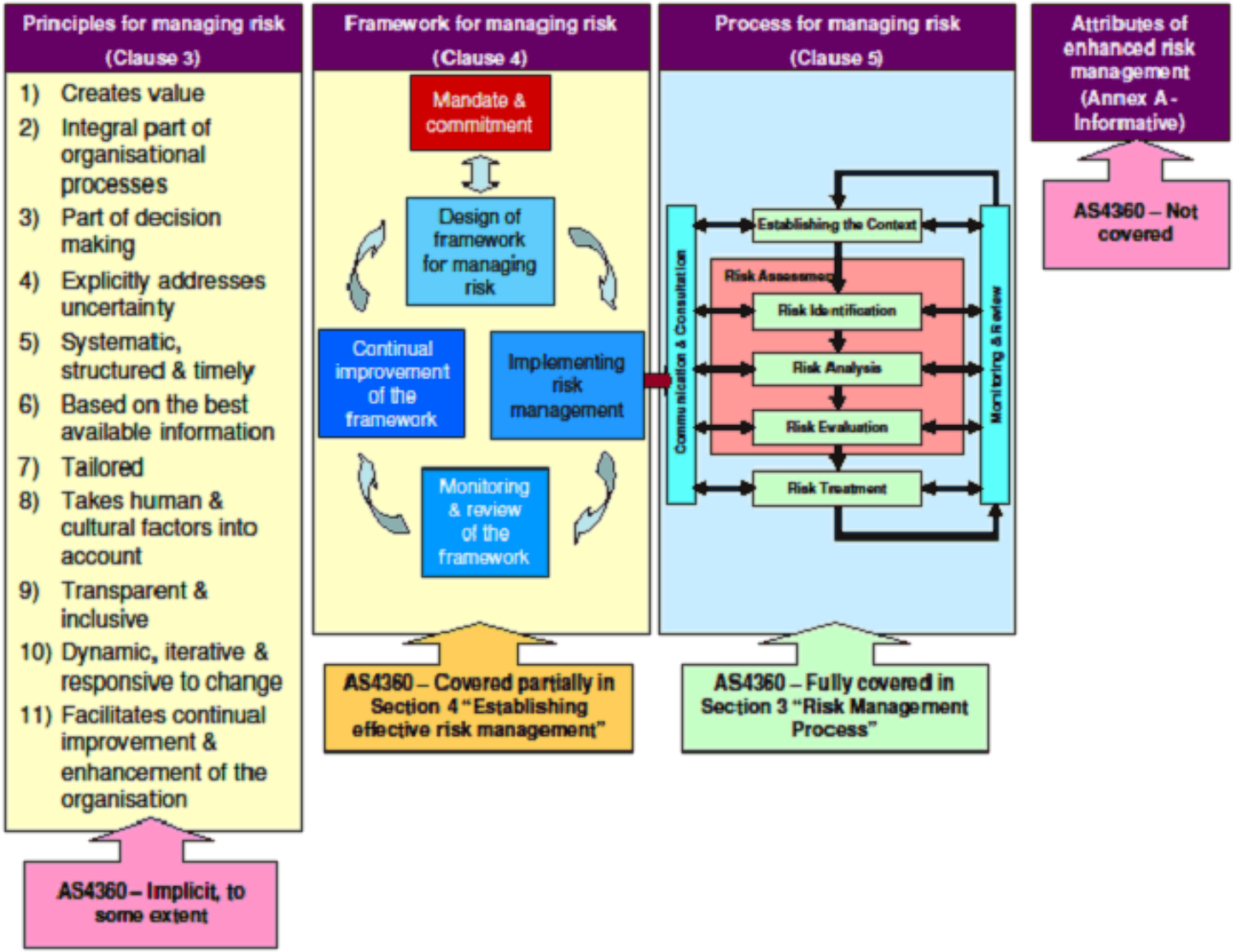
Enterprise Risk Management Framework



The COSO Enterprise Risk Management Framework

ISO 31000 Risk Mgmt (2009)

Guidelines and Principles and Framework



ISO 31000 Framework

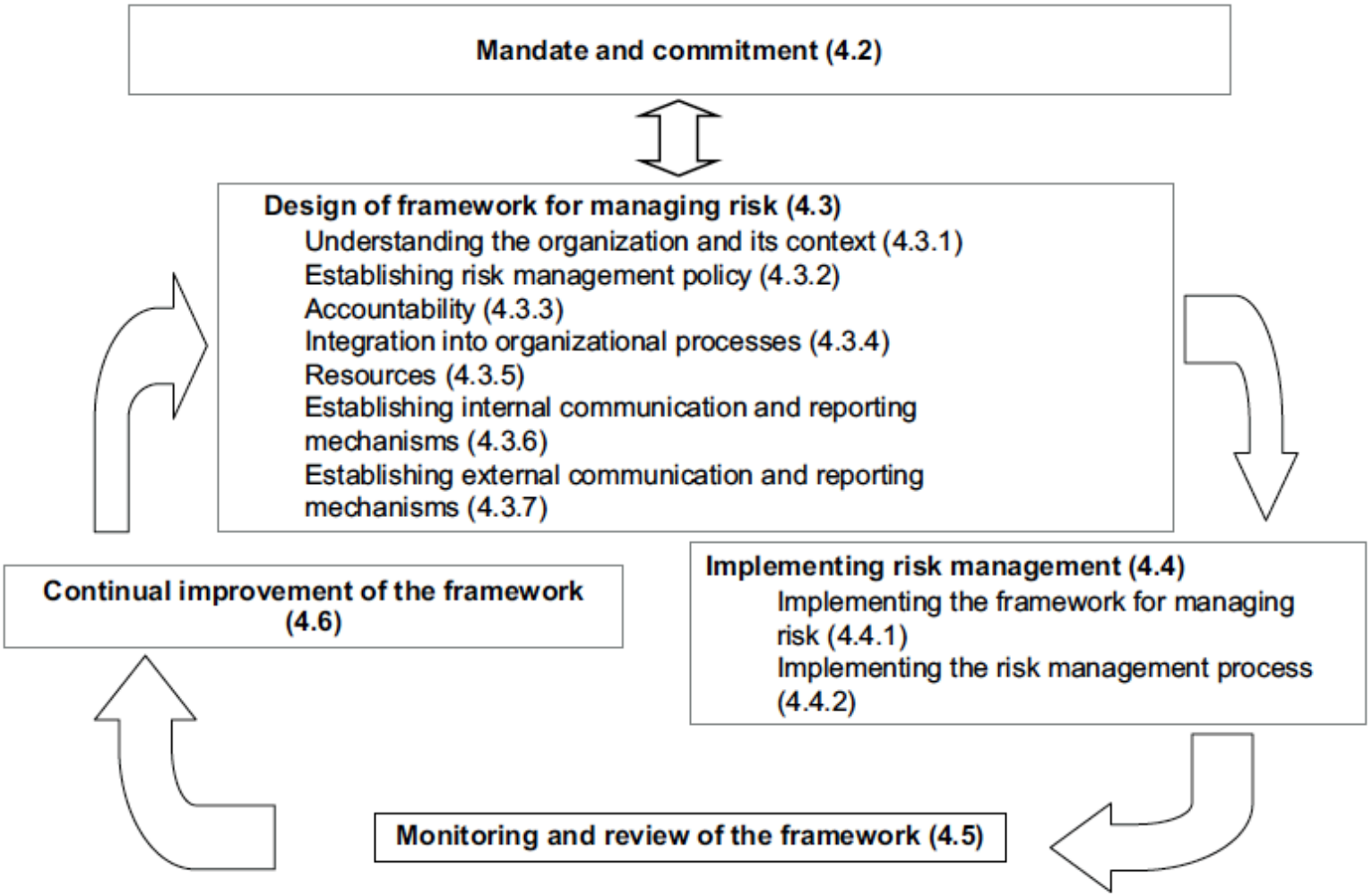


Figure 2 — Relationship between the components of the framework for managing risk

ISO 31000

Processes

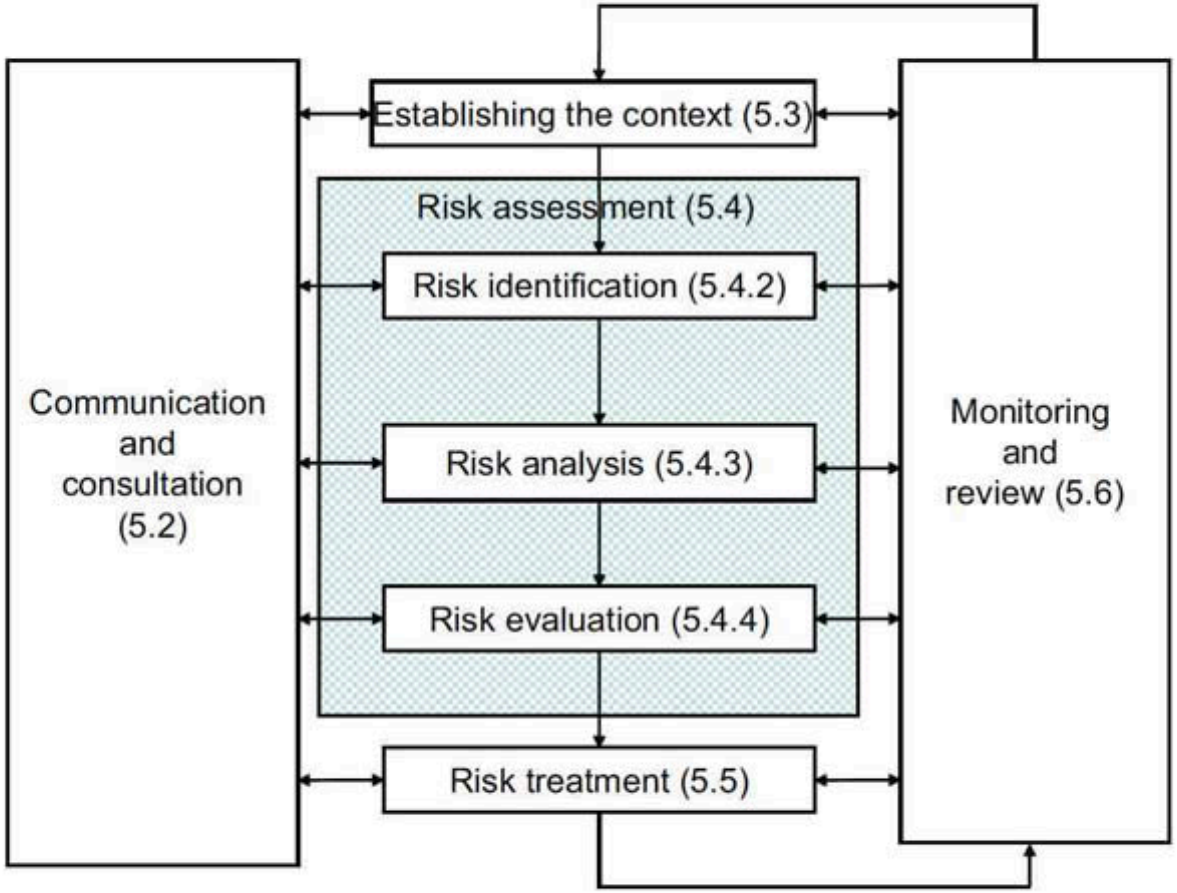


Figure 3 — Risk management process

ISO 31000 - Processes

→ Mandate and commitment

Design of framework for managing risk	Understanding of the organisation and its context
	Establishing risk management policy
	Accountability
	Integration into organisational processes
	Resources
	Establishing internal communication and reporting mechanisms
	Establishing external communication and reporting mechanisms
Implementing risk management	Implementing the framework for managing risk
	Implementing the risk management process
	Monitoring and review of the framework
	Continual improvement of the framework

ISO 31000 - Processes

Risk Management Process

- Communication and consultation
- Establishing the external context
- Establishing the internal context
- Establishing the context of the risk management process
- Defining risk criteria
- Risk assessment
  - Risk identification
  - Risk analysis
  - Risk evaluation
  - Risk treatment
- Monitoring and review
- Recording the risk management process

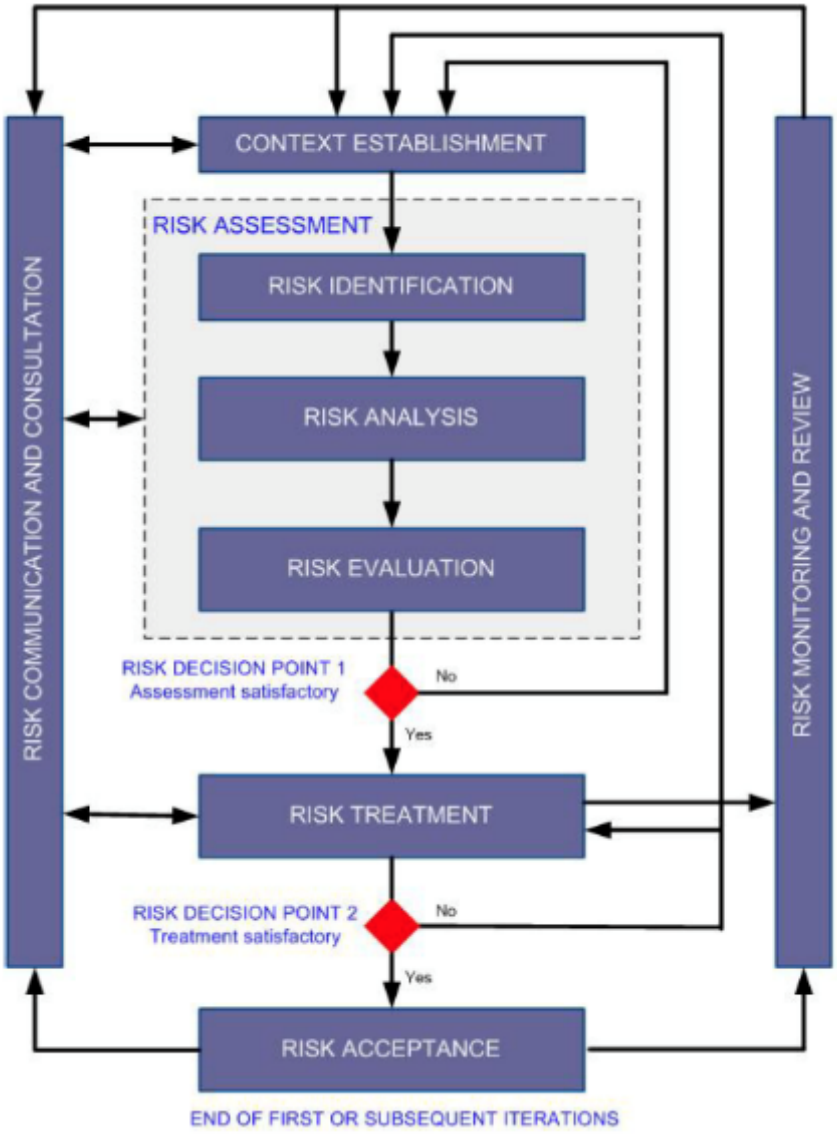
ISO 31000

Attributes of enhanced risk management

- Key outcomes
  - The organisation has a current, correct and comprehensive understanding of its risks
  - The organisation‘s risks are within its risk criteria
- Attributes
  - Continual improvement
  - Full accountability for risks
  - Application of risk management in all decision making
  - Continual communications
  - Full integration in the organisation‘s governance structure

ISO 27005

Information Security Risk Management



ISO 27005
Context Establishment

Basic Criteria	Risk management approach
	Risk evaluation criteria
	Impact criteria
	Risk acceptance criteria

→Scope and Boundaries
→Organisation for information security risk management

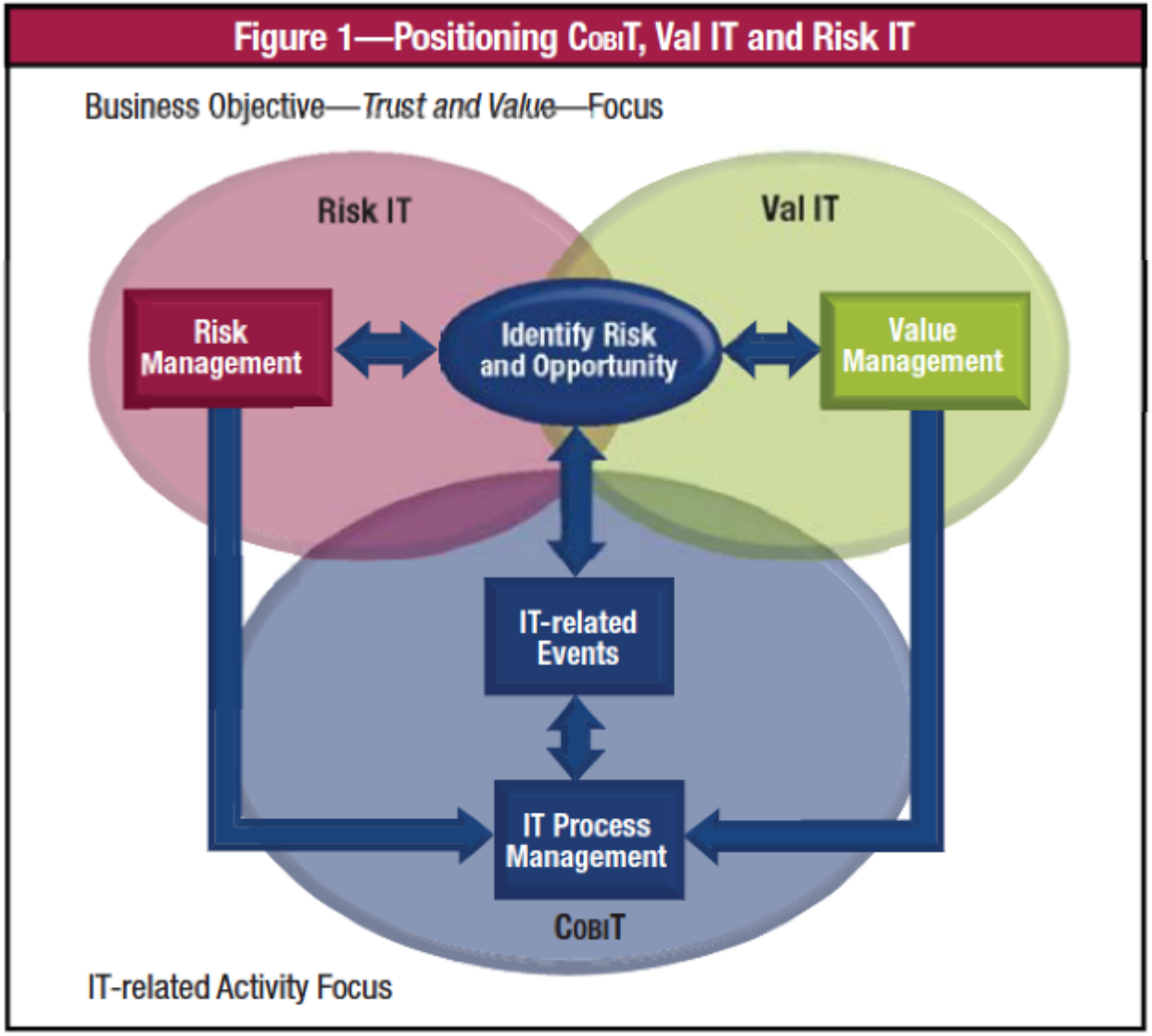
ISO 27005

Information security risk assessment

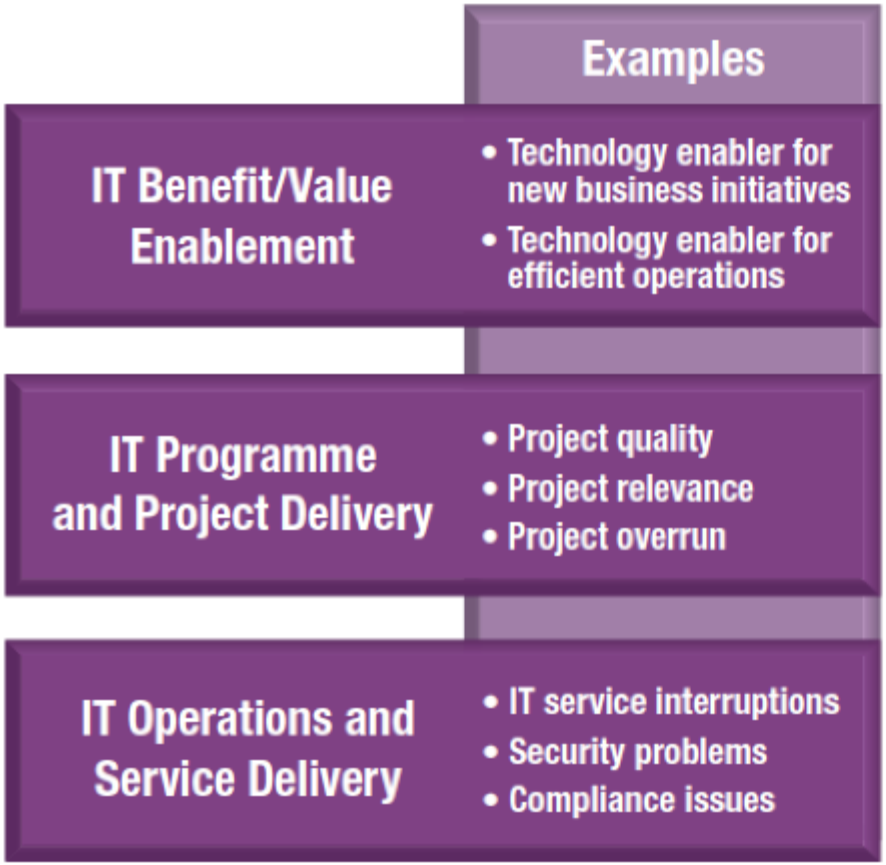
Risk identification	Identification of assets
	Identification of threats
	Identification of existing controls
	Identification of vulnerabilities
	Identification of consequences
Risk analysis	Risk analysis methodologies
	Assessment of consequences
	Assessment of incident likelihood
	Level of risk determination

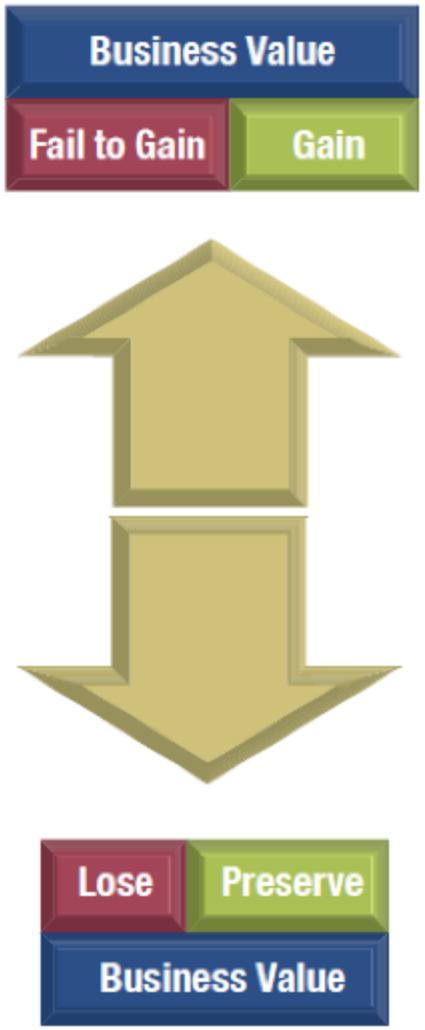
ITGI RiskIT Framework

Positionierung



IT Risk (high level) categories

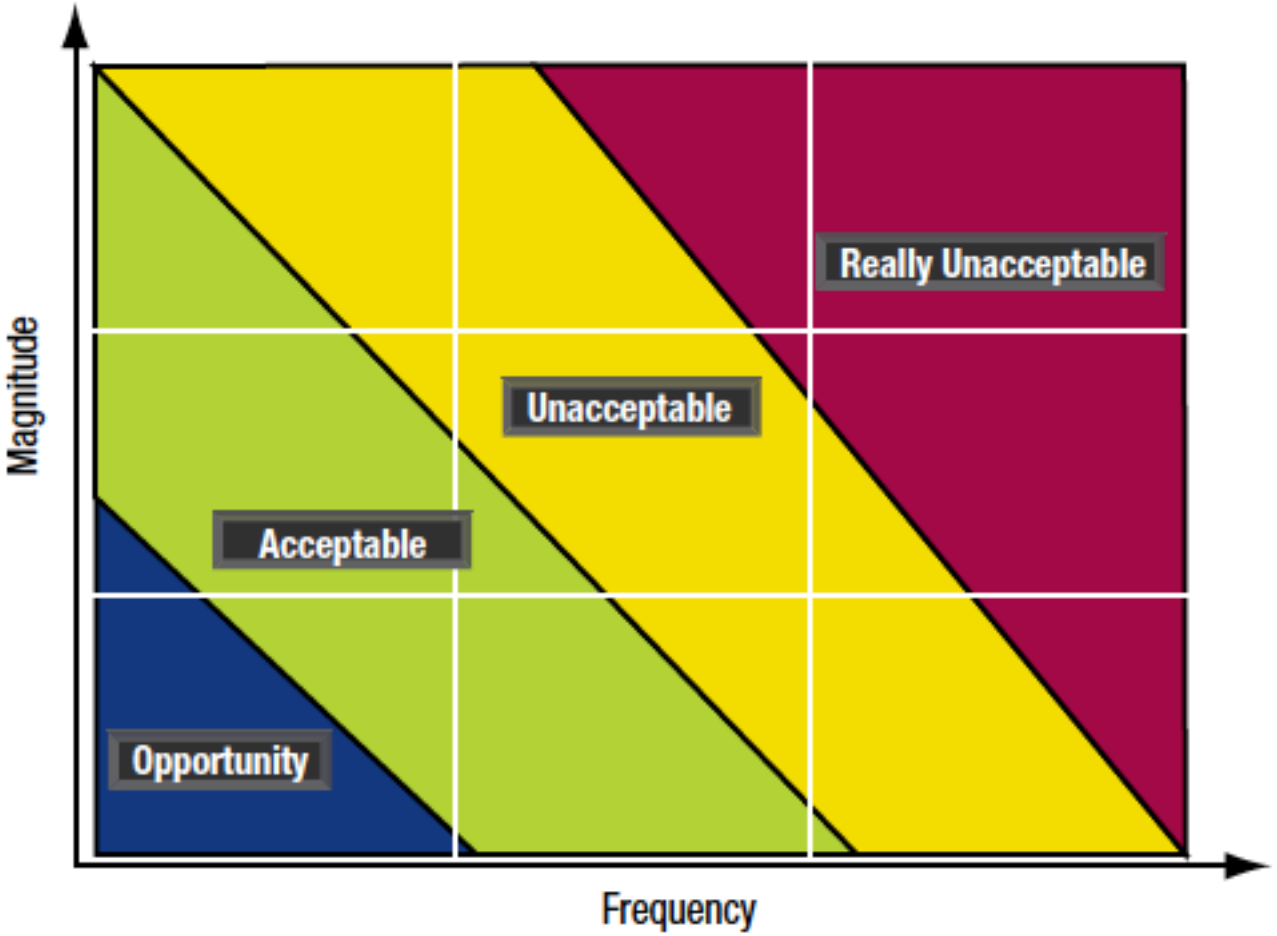




RiskIT Framework

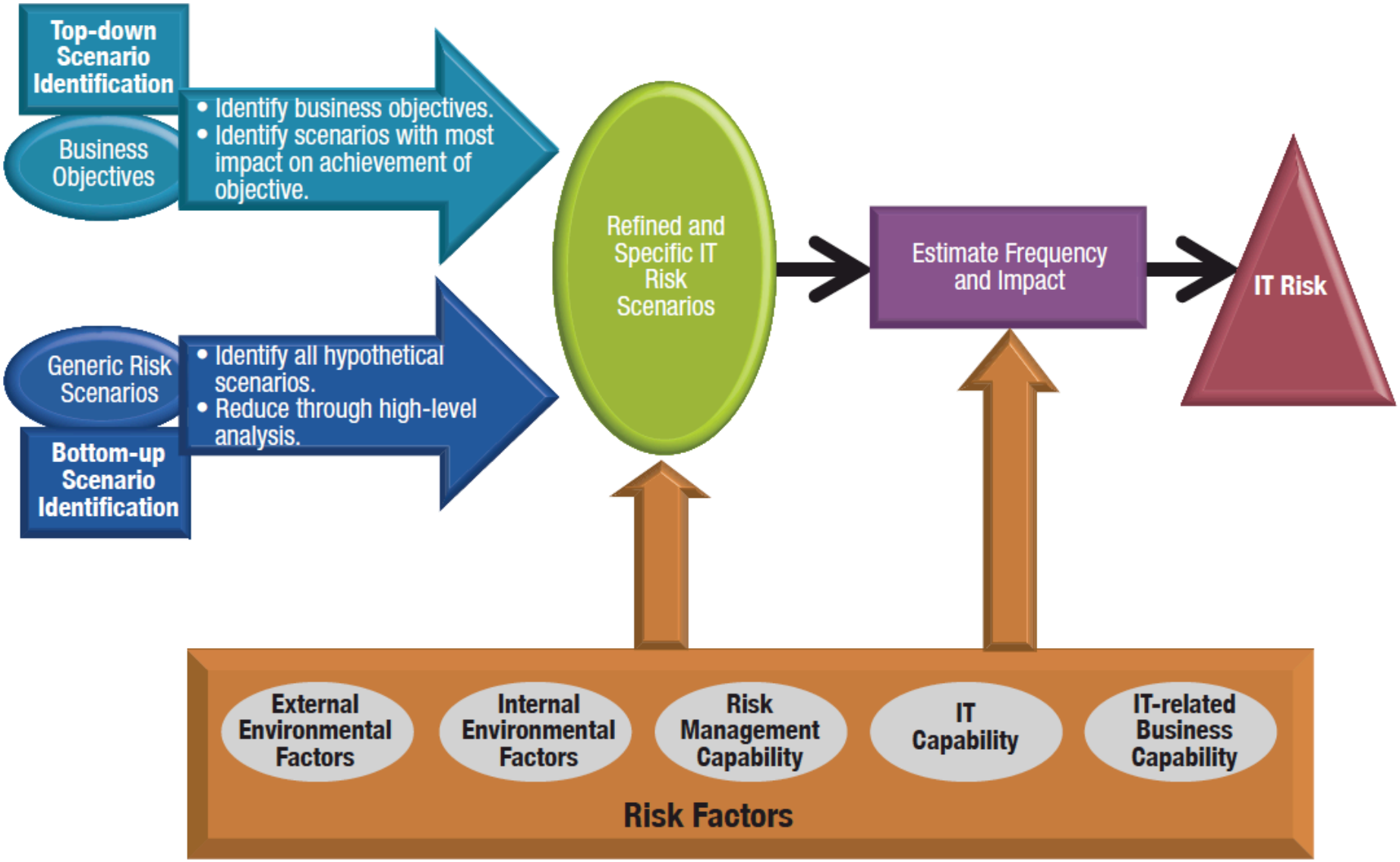
Risk maps...

- Risk appetite
- Risk tolerance
- Risk culture

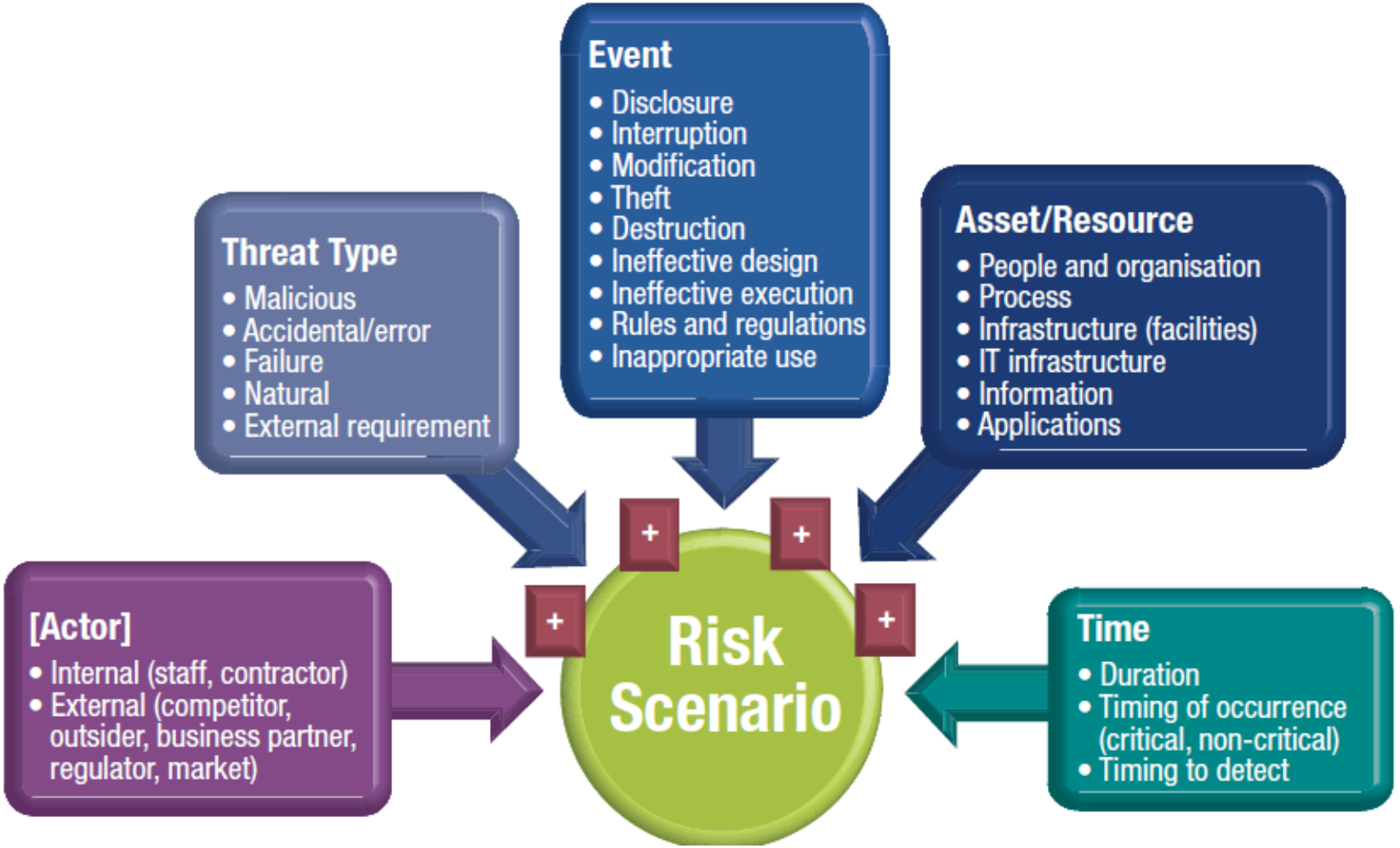


Risk culture

IT risk scenario development

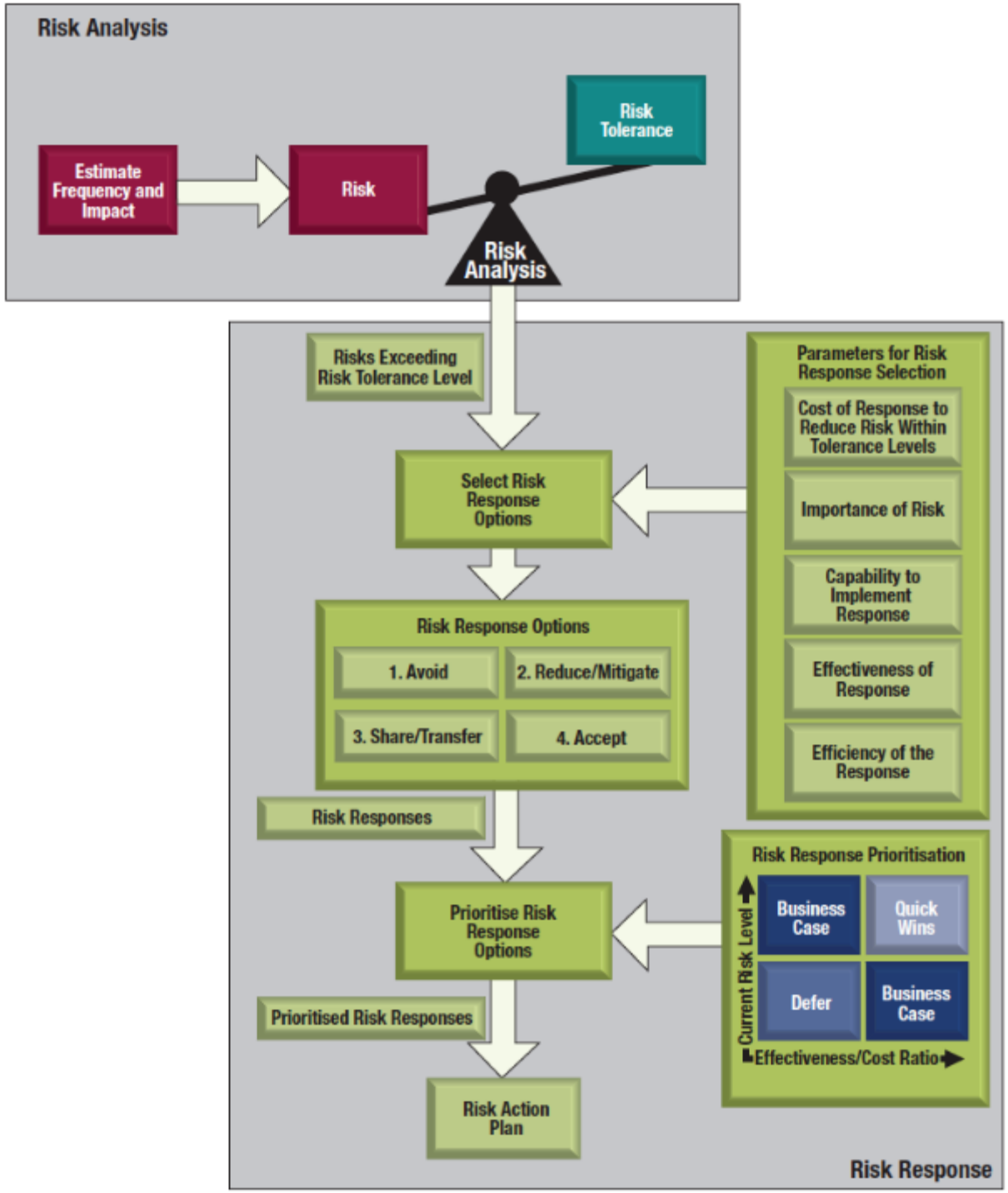


Risk scenario components

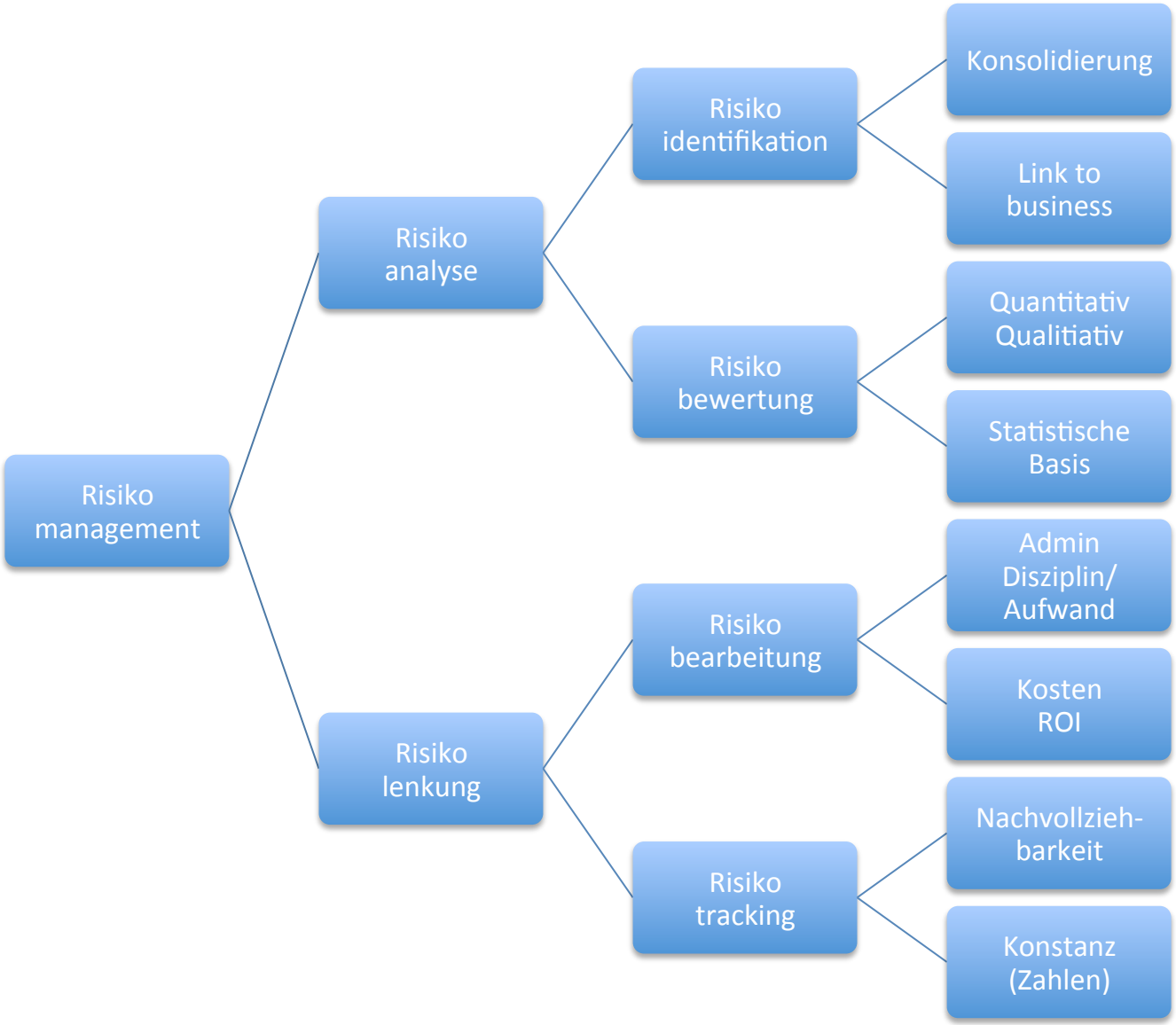


Aber: scenario based...
→ keeping it real!

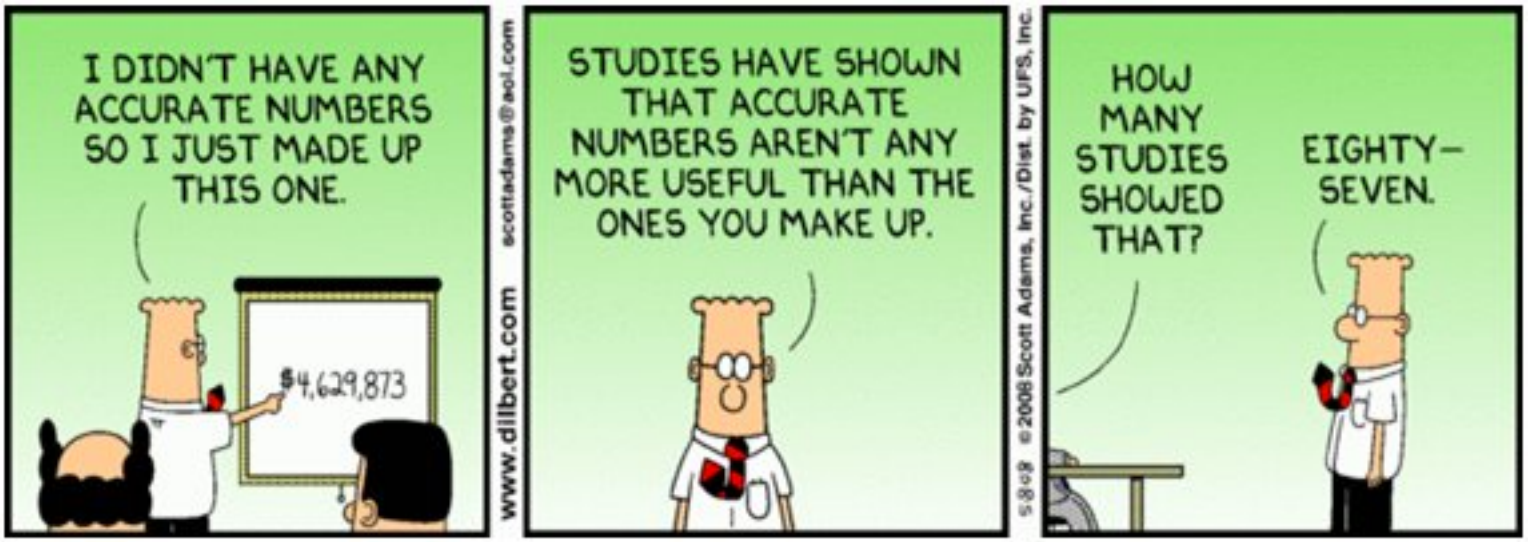
IT Risk Response options and prioritisation



Verwalten von IT Risiken



Quantifizieren von IT Risiken

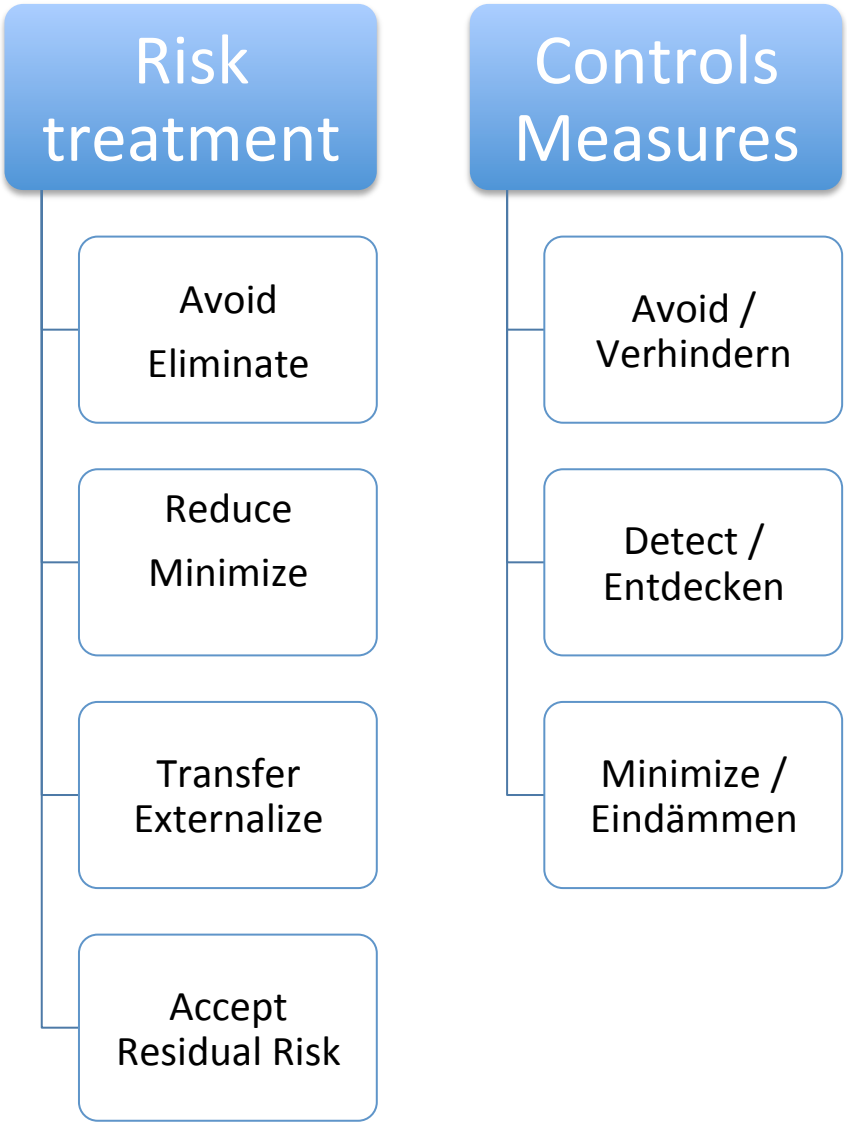


Big Data? Loss DB?
Komplexität von Informationssystemen (und Software)?

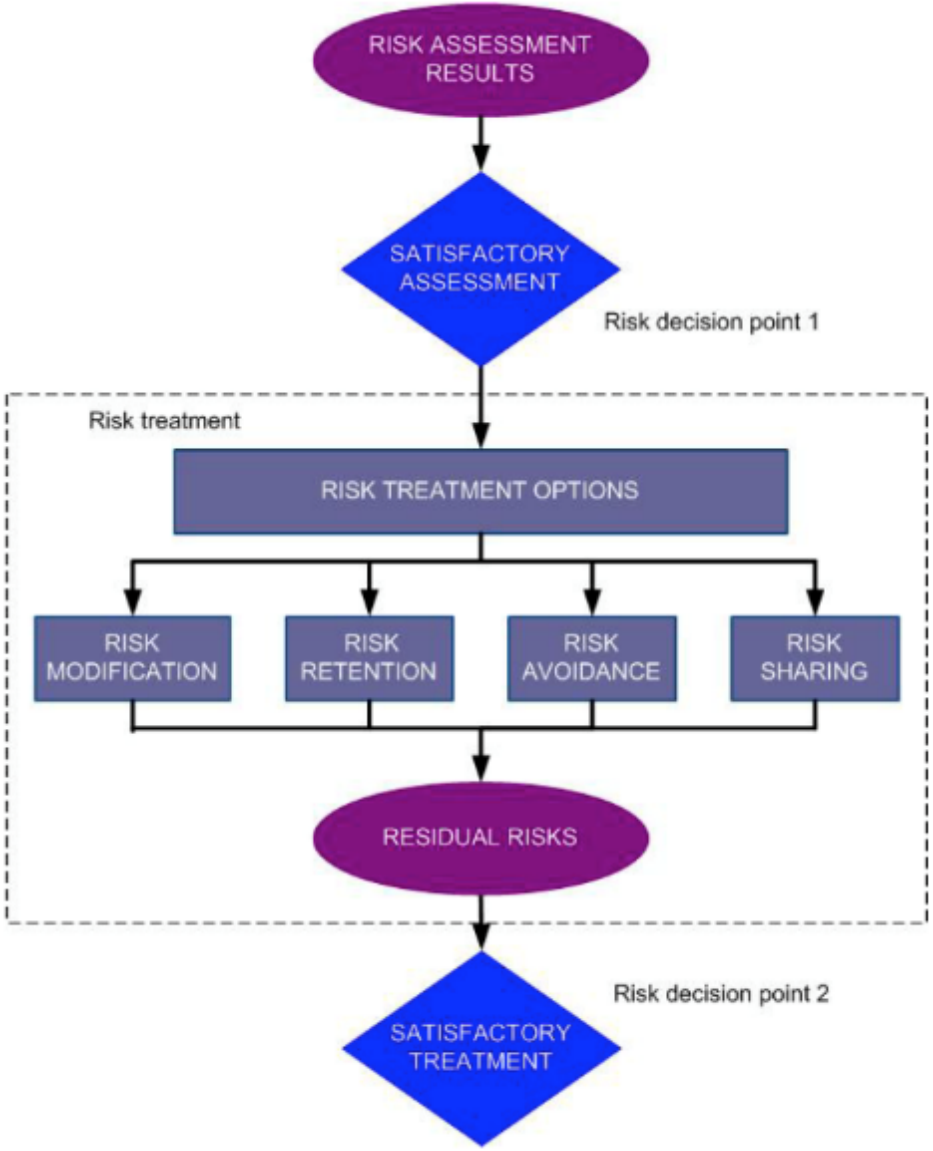
Quantifizieren von IT Risiken

- In der Praxis eher qualitativ statt quantitativ
  - Fehlende statistische Basis
  - Prinzipiell komplexe Systeme
  - Wenig akuter Bedarf zur Quantifizierung → über Verknüpfung mit Business Process
- Konsolidierung der Werte für Management Reporting als Grundlage für Quantifikation
- In der Praxis eher „erste Schritte“ statt best practise
- ISO 27005, ITGI RiskIT Framework und Practictioner Guide bieten brauchbare Grundlagen (Framework)

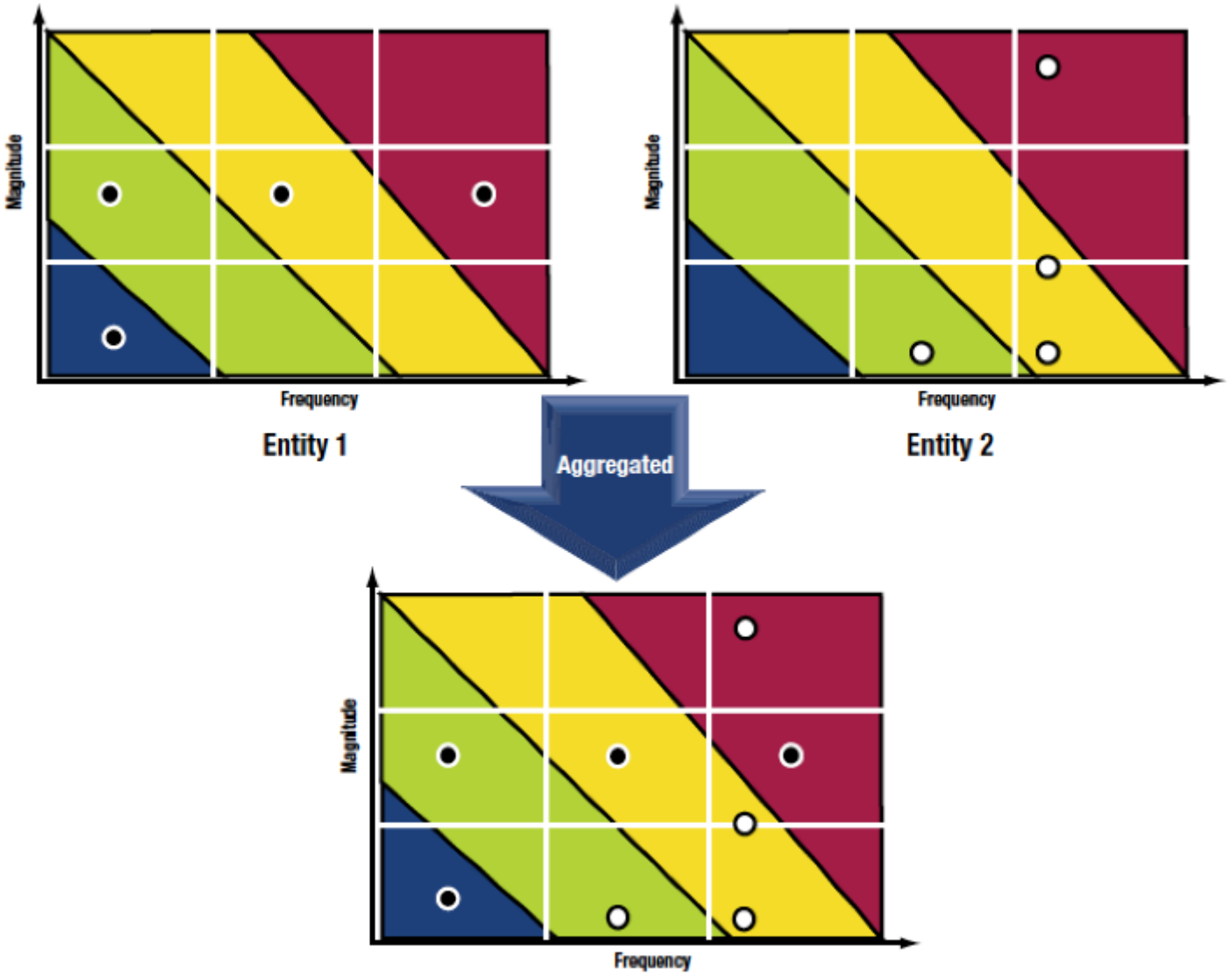
Risk Treatment



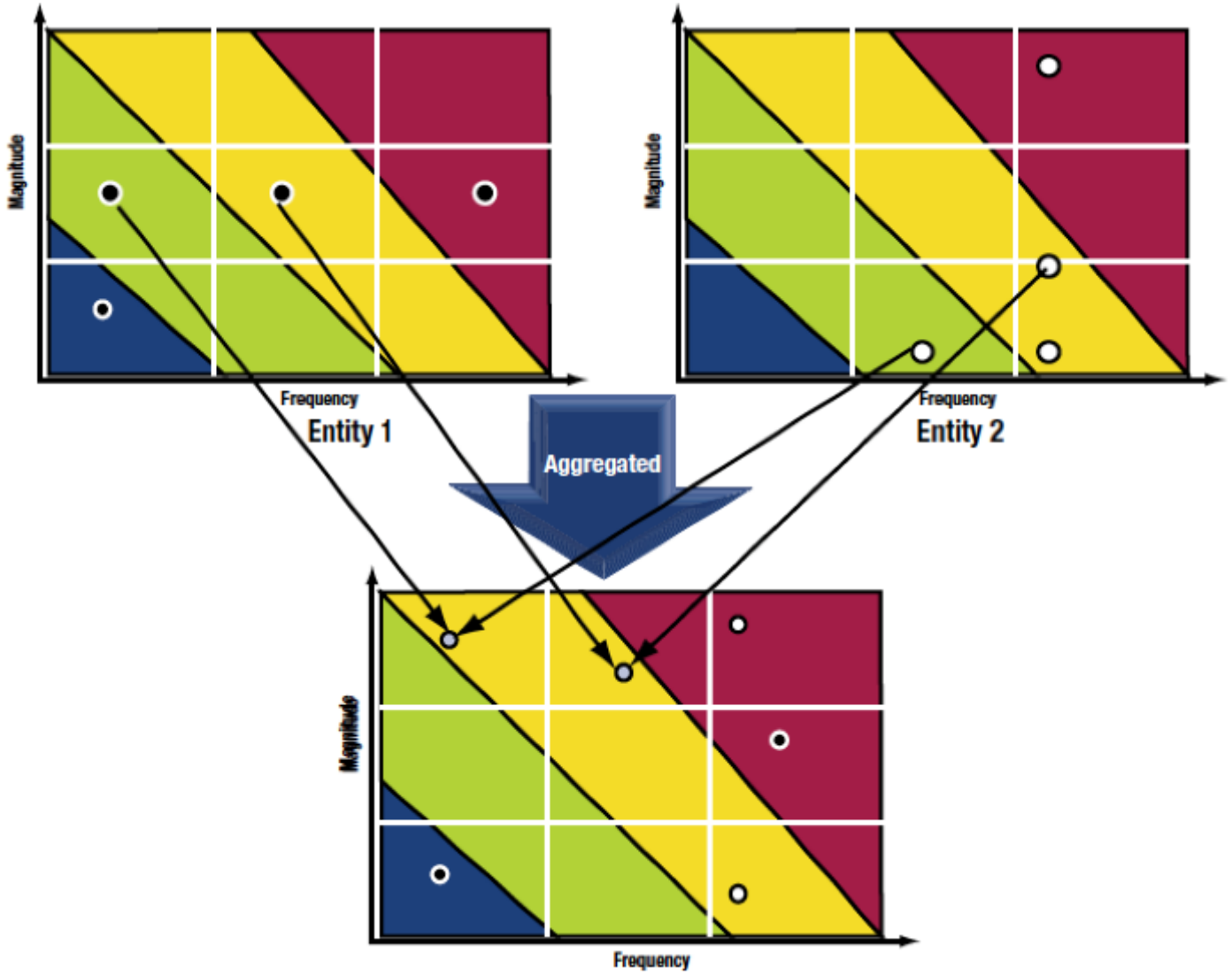
Risk Treatment – ISO 27005

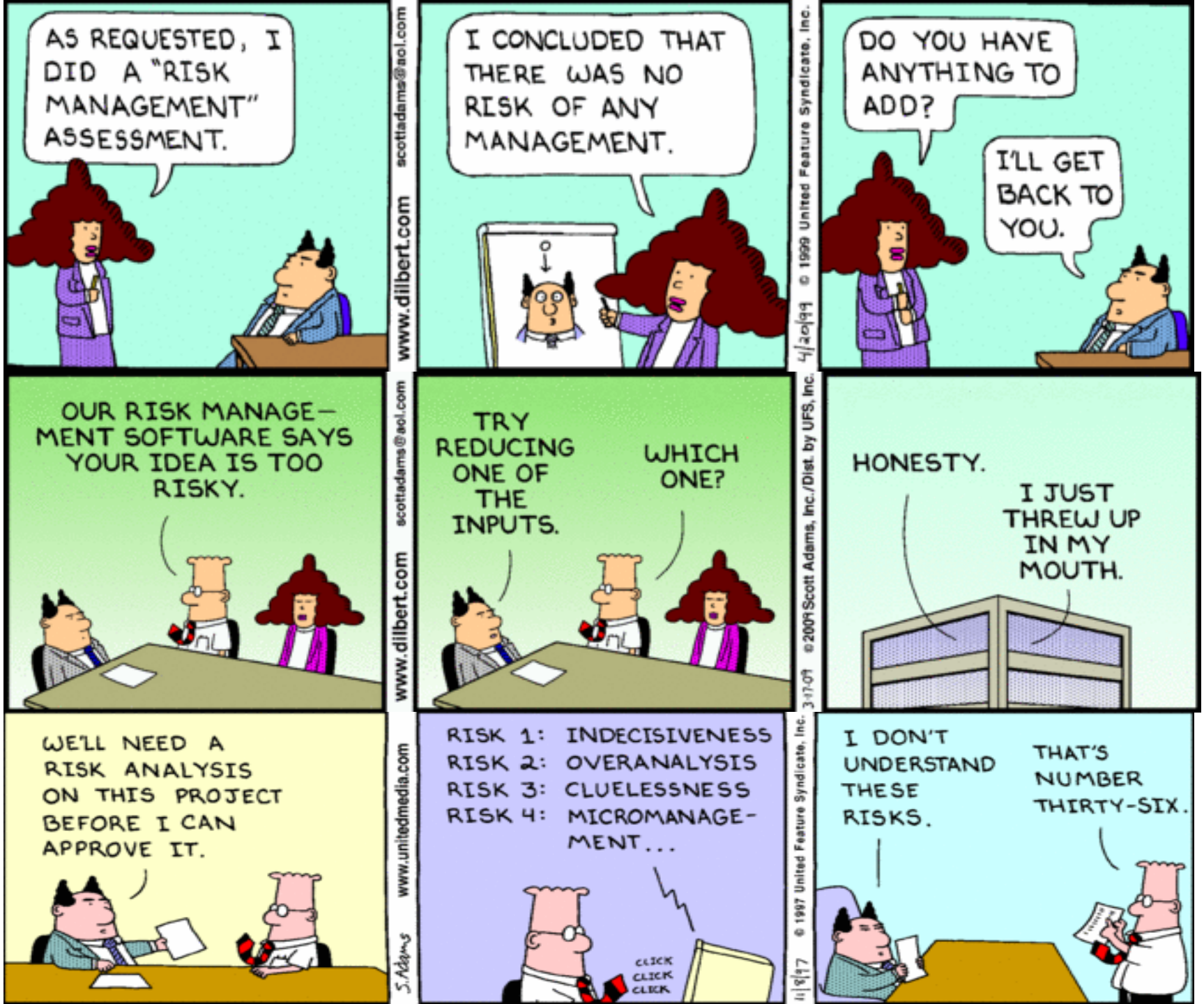


Konsolidieren von IT Risiken
Disjointed risks



Konsolidieren von IT Risiken shared risks




AS REQUESTED, I DID A "RISK MANAGEMENT" ASSESSMENT.
I CONCLUDED THAT THERE WAS NO RISK OF ANY MANAGEMENT.
DO YOU HAVE ANYTHING TO ADD?
I'LL GET BACK TO YOU.
www.dilbert.com scottadams@aol.com
© 1999 United Feature Syndicate, Inc.
4/20/99
OUR RISK MANAGE-MENT SOFTWARE SAYS YOUR IDEA IS TOO RISKY.
TRY REDUCING ONE OF THE INPUTS.
WHICH ONE?
HONESTY.
I JUST THREW UP IN MY MOUTH.
www.dilbert.com scottadams@aol.com
©2001 Scott Adams, Inc./Dist. by UFS, Inc.
3-17-01
WE'LL NEED A RISK ANALYSIS ON THIS PROJECT BEFORE I CAN APPROVE IT.
RISK 1: INDECISIVENESS
RISK 2: OVERANALYSIS
RISK 3: CLUELESSNESS
RISK 4: MICROMANAGE-MENT...
CLICK CLICK CLICK
I DON'T UNDERSTAND THESE RISKS.
THAT'S NUMBER THIRTY-SIX.
www.unitedmedia.com
S. Adams
© 1997 United Feature Syndicate, Inc.
1/8/97