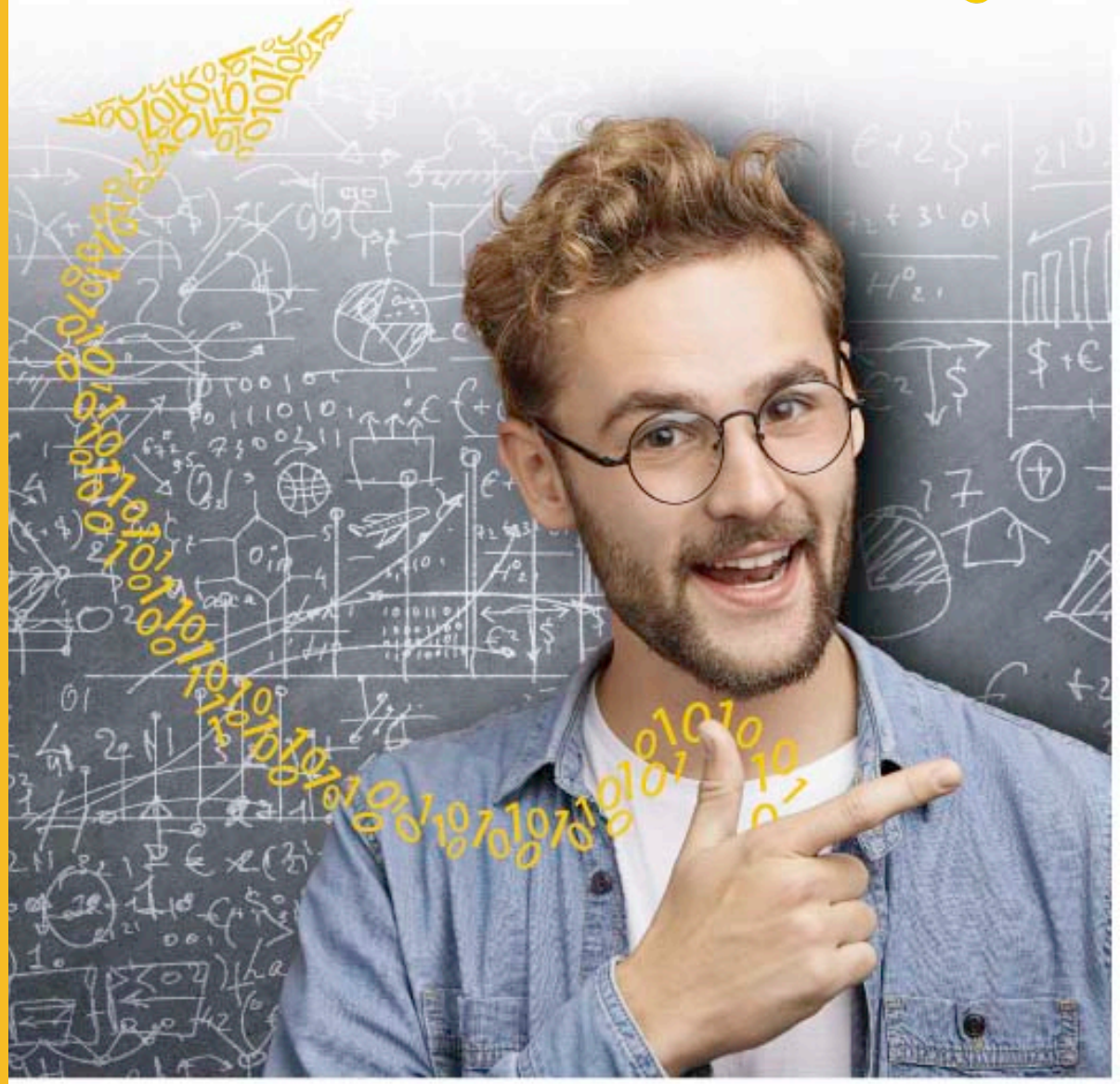
IT Risk, Continuity and Crisis Management



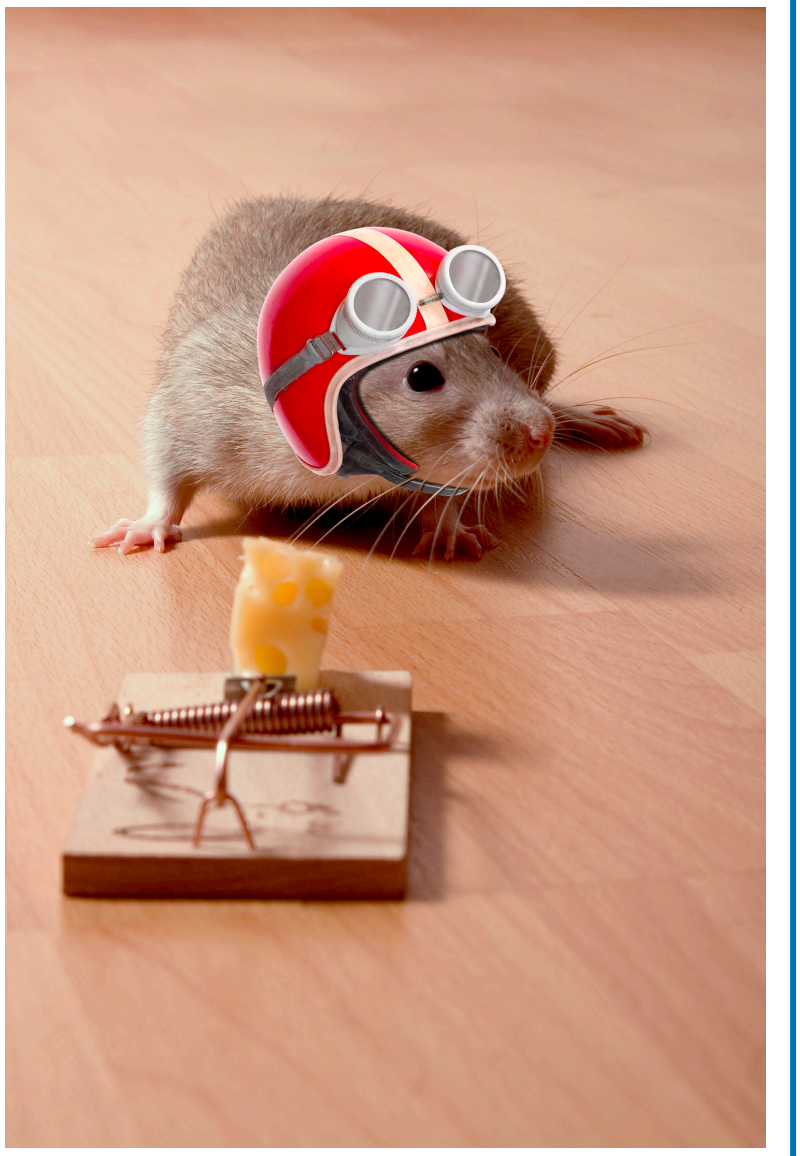
November 1, 2020

Lionel Pilorget

Agenda

- IT Risk Management
- Business Continuity Management (BCM)
- IT Service Continuity Management (ITSCM)
- IT Crisis Management

What is a Risk?



Stay motivated!

Take risks…

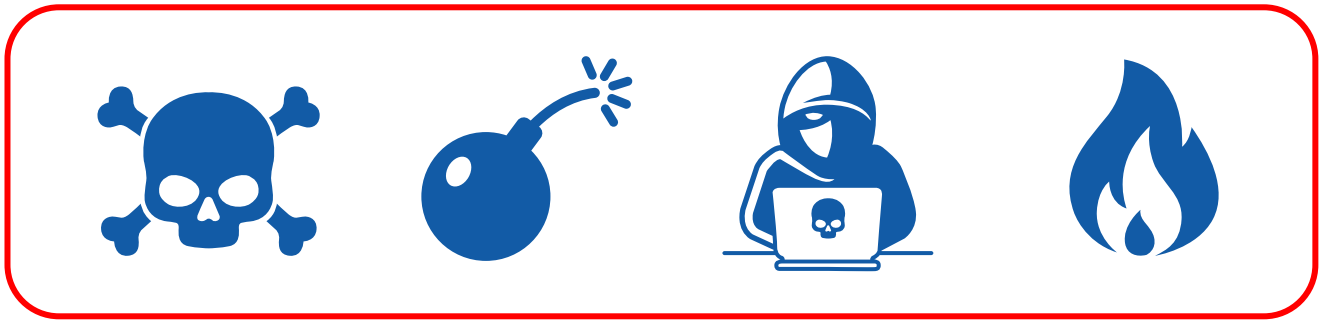
Definition of a risk

A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action

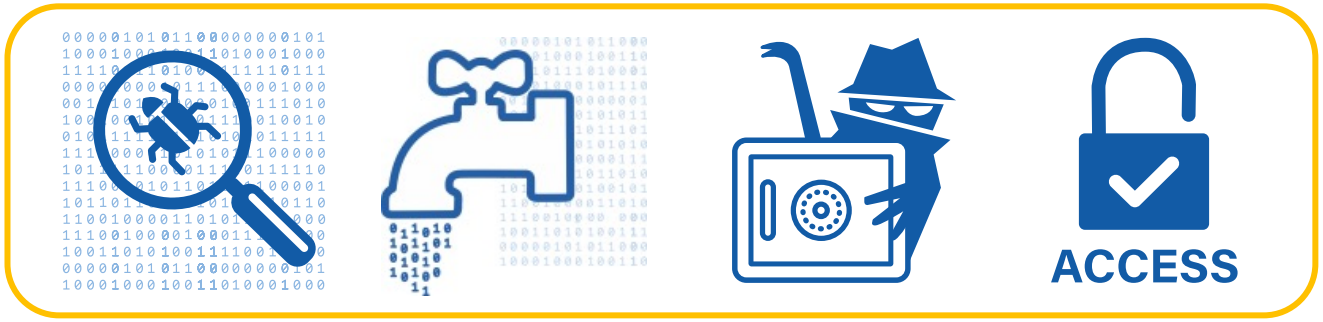
Source: http://www.businessdictionary.com/definition/risk.html

Risk = Threat x Vulnerability

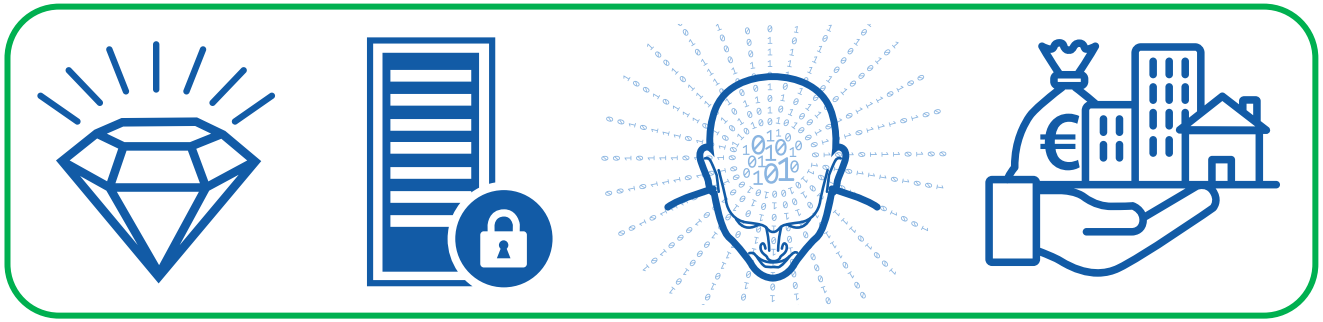
Threat:
Any possible danger



Vulnerability:
Any weakness in a system or organization



Asset:
Anything that has value to the organization



Threat - Vulnerability - Risk

Threat description	Vulnerability	What is the risk?
Terminated employee		Fraud and embezzlement
	Vendor has identified security flaws and patches have not been applied	
	Unauthorized access to data room	
Laptop lost or stolen		
Distributed Denial-of-Service (DDOS) attack		
	Air-conditioning system for data center is 10 years old	
Power outage		

Possible risks

Possible Threats

Disgruntled employee
Dishonest employee
Power outage
Criminal
Terrorist
Hacker
Press
Government
Nature

Possible Vulnerabilities

SW bugs
Human failure
Inefficient controls
HW flaws
Unsecured data
Inadequate BCM
Broken processes
Physical access
No HW inventory

Possible Risk

Financial loss
Damage of reputation
Fraud and embezzlement
Loss of confidence
Loss of life
Environmental pollution
Low SW quality
Low SW acceptance
Inefficient process
Dependency on supplier

Major business risks

- **Strategic Risk**: risks associated with significant investments for which there is high uncertainty about success and profitability

  These risks arise from:
  - Business Environment: Buyers and sellers interacting to buy and sell goods and services, changes in supply and demand, competitive structures and introduction of new technologies
  - Transaction: Assets relocation of mergers and acquisitions, spin-offs, alliances and joint ventures
  - Investor Relations: Strategy for communicating with individuals who have invested in the business
- **Financial Risk**: risks associated with the financial structure and transactions of the particular industry
- **Operational Risk**: risks associated with the operational and administrative procedures of the particular industry, especially potential losses resulting from inadequate system, management failure, faulty controls, fraud, and human error
- **Compliance Risk** (Legal Risk): risks associated with the need to comply with the rules and regulations of the government, closely related to reputation risks
- **Other risks**: risks like natural disaster (floods) and others depend upon the nature and scale of the industry

See also: Allianz Risk Barometer | AGCS

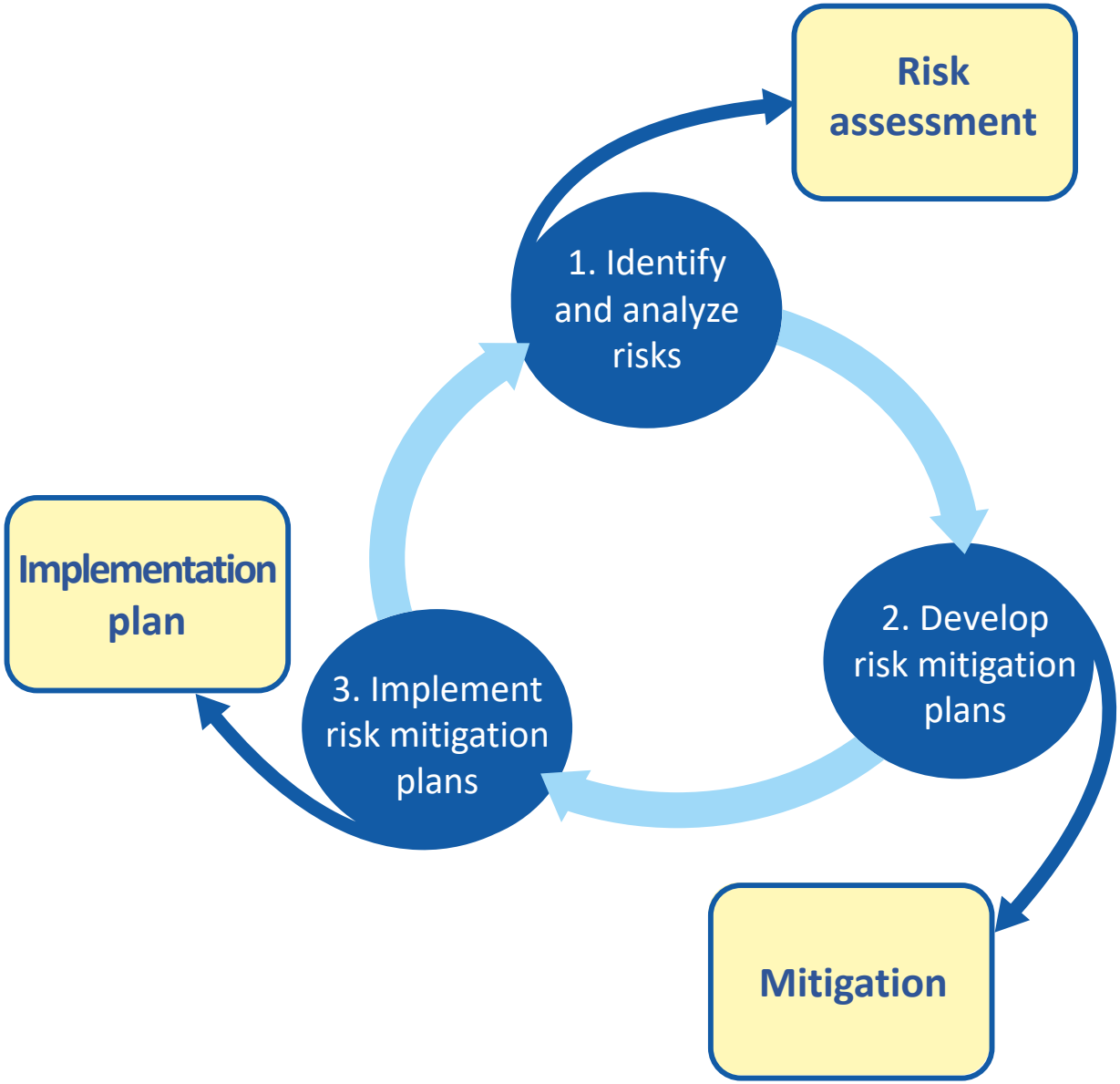
Source: Jolly, Adam (2003). Managing Business Risk: A Practical Guide to Protecting Your Business

Elementary Threats in IT

T 0.1 Fire
T 0.2 Unfavorable Climatic Conditions
T 0.3 Water
T 0.4 Pollution, Dust, Corrosion
T 0.5 Natural Disasters
T 0.6 Environmental Disasters
T 0.7 Major Events in the Environment
T 0.8 Failure or Disruption of the Power Supply
T 0.9 Failure or Disruption of Communication Networks
T 0.10 Failure or Disruption of Mains Supply
T 0.11 Failure or Disruption of Service Providers
T 0.12 Interfering Radiation
T 0.13 Intercepting Compromising Emissions
T 0.14 Interception of Information / Espionage
T 0.15 Eavesdropping
T 0.16 Theft of Devices, Storage Media and Documents
T 0.17 Loss of Devices, Storage Media and Documents
T 0.18 Bad Planning or Lack of Adaption
T 0.19 Disclosure of Sensitive Information
T 0.20 Information or Products from Unreliable Source
T 0.21 Manipulation of Hardware or Software
T 0.22 Manipulation of Information
T 0.23 Unauthorized Access to IT Systems
T 0.24 Destruction of Devices or Storage Media
T 0.25 Failure of Devices or Systems
T 0.26 Malfunction of Devices or Systems
T 0.27 Lack of Resources
T 0.28 Software Vulnerabilities or Errors
T 0.29 Violation of Laws or Regulations
T 0.30 Unauthorized Use or Administration of Devices or Systems
T 0.31 Incorrect Use or Administration of Devices or Systems
T 0.32 Abuse of Authorizations
T 0.33 Absence of Personnel
T 0.34 Attack
T 0.35 Coercion, Extortion or Corruption
T 0.36 Identity Theft
T 0.37 Reputation of Actions
T 0.38 Abuse of Personal Data
T 0.39 Malicious Software
T 0.40 Denial of Service
T 0.41 Sabotage
T 0.42 Social Engineering
T 0.43 Replaying Messages
T 0.44 Unauthorized Entry to Promises
T 0.45 Data Loss
T 0.46 Loss of Integrity of Sensitive Information

Source: BSI, Threats Catalogue

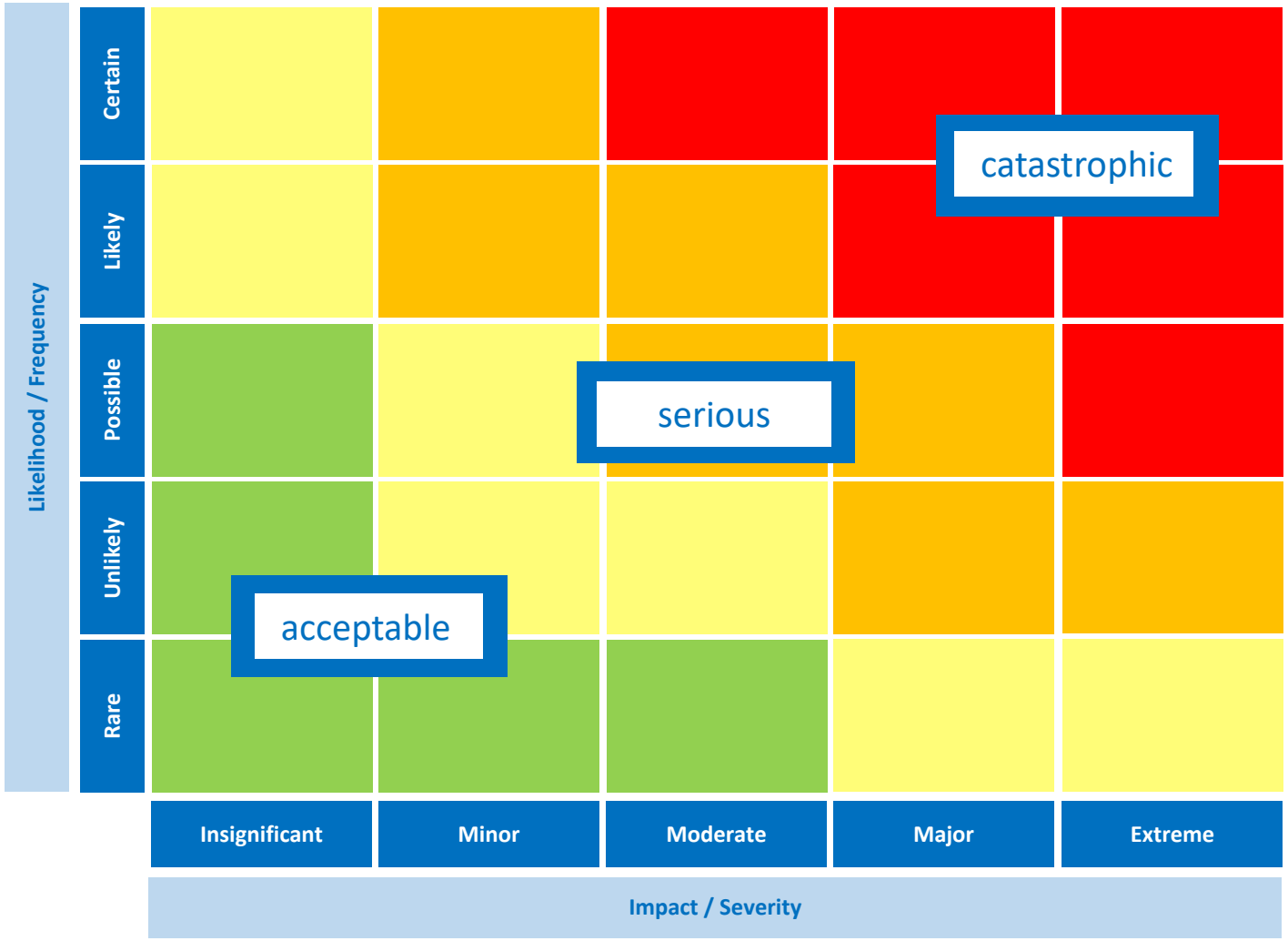
Risks need to be managed



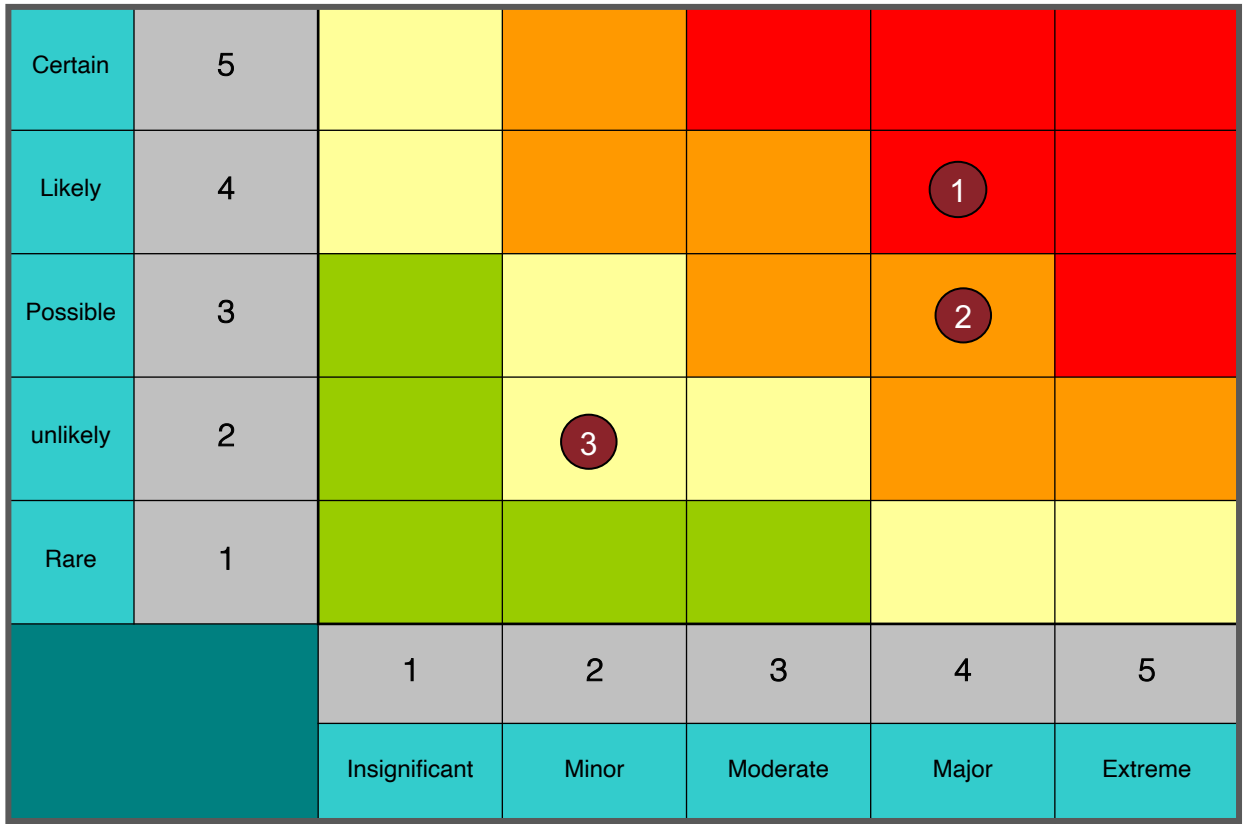
Risk Assessment based on Impact and Likelihood

- **Likelihood**: between certain (P ~ 1) and unlikely (P ~ 0)
- **Impact**: between low and catastrophic

Visualize Risks on the Risk Matrix



Example: Risks by Implementing an Online Solution



Risks

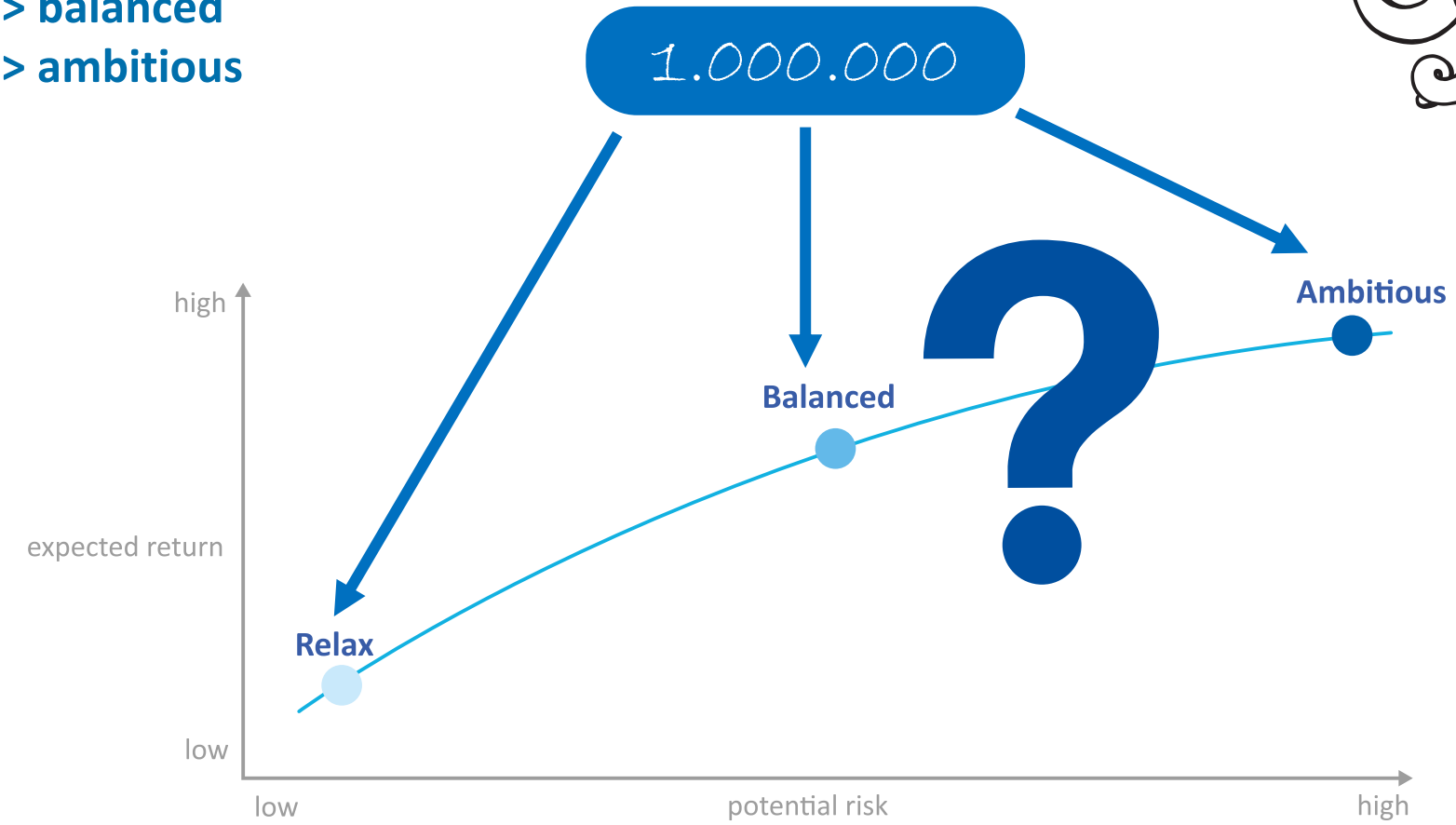
1. Stability of the new online solution
2. Customer support for onboarding
3. Data protection conformity (inactive user & notification on private email)

Legend

- Worst
- Stable
- Better
- New
- Closed
- On hold

Is your appetite for risk high?

You can invest 1 Million…
What is your investment strategy?
-> relax
-> balanced
-> ambitious

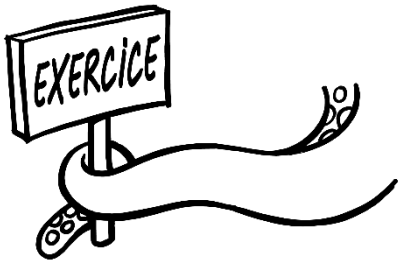


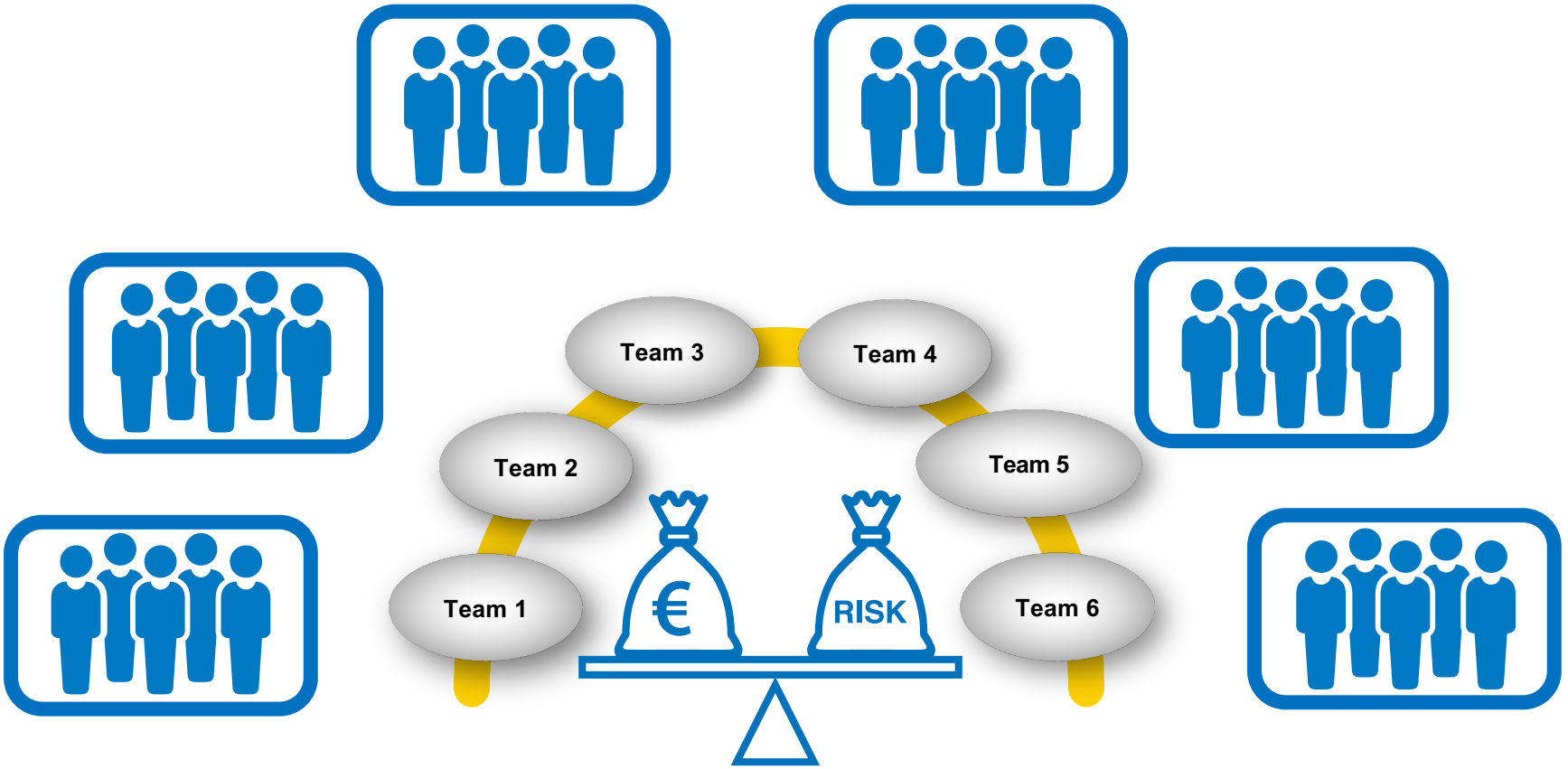
<--- risk capacity versus risk tolerance --->

How big is the risk appetite for IT risks?

Risks concerning:

- **IT Projects**
- **IT Services**





Fill in the table for IT projects

Risk Criticality Score*	Time	Cost	Scope	Quality
4 - Unacceptable				
3 - Critical				
2 - Moderate				
1 - Low				

** can be defined as an absolute value or as a percentage of a quantity to be specified*

Fill in the table for IT services

Risk Criticality Score*	Number of customers impacted	Compliance violations	Financial losses
4 - Unacceptable			
3 - Critical			
2 - Moderate			
1 - Low			

** can be defined as an absolute value or as a percentage of a quantity to be specified*

Example of Risk Rating for Projects

Definition	Category	Parameter	Value
Very High	Time	Timelines are impacted by 3 months+	5
	Cost	Project budget exceeds by >15%	
	Scope	Final solution is non-effective	
	Quality	Final solution is non-effective	
High	Time	Timelines are impacted by 2-3 months	4
	Cost	Project budget exceeds by 10-15 %	
	Scope	Scope impact is unacceptable to Project Sponsor	
	Quality	Reduction in quality is unacceptable to Project Sponsor	
Medium	Time	Timelines are impacted by 1-2 months	3
	Cost	Project budget exceeds by 5-10 %	
	Scope	Major areas of scope affected with impact to end users	
	Quality	Quality reduction requires sponsor acknowledgement and approval	
Low	Time	Timelines are impacted by <1 months	2
	Cost	Project budget exceeds by <5%	
	Scope	Minor areas of scope affected and a small impact to users	
	Quality	Minor areas affected by quality issues with small impact to users	
Very Low	Time	Insignificant time increase	1
	Cost	Insignificant cost increase	
	Scope	Scope change is barely noticeable to user	
	Quality	Quality degradation is barely noticeable to user	

Example of Risk Tolerance

Impact Score (T = Time, B = Budget, S = Scope, Q = Quality)						
	20	20	40	60	80	100
	19	19	38	57	76	95
	18	18	36	54	72	90
	17	17	34	51	68	85
	16	16	32	48	64	80
	15	15	30	45	60	75
	14	14	28	42	56	70
	13	13	26	39	52	65
	12	12	24	36	48	60
	11	11	22	33	44	55
	10	10	20	30	40	50
	9	9	18	27	36	45
	8	8	16	24	32	40
	7	7	14	21	28	35
	6	6	12	18	24	30
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Likelihood of Occurence				

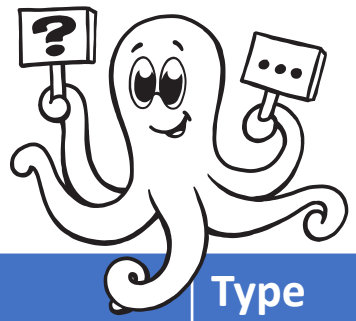
IMPACT	ACTION	REPORTING
EXTREME	• Urgent and active management required • Risk treatment plan MUST be implemented IMMEDIATELY to reduce the risk exposure to an acceptable level • Regular Reporting Required	• Immediate notification to sponsor • Included in Status Reporting • Special briefing to Steering Committee • Weekly updates
HIGH	• Management attention required • Risk treatment plan required • Regular Reporting Required	• Notification to sponsor • Included in Status Reporting • Steering Committee Informed • Biweekly updates
MODERATE	• Management responsible to monitor • Focus on ensuring internal controls are effective and monitoring the ongoing risk	• Maybe Included in Status Reporting • May inform Steering Committee • Monthly updates
LOW	• Monitor using routine practices • Focus on ensuring internal controls are effective	• Communication within project team periodically • No Status Reporting

Risk Mitigation

Risk avoidance:
eliminating any exposure to risk that poses a potential threat

Risk limitation:
reducing the likelihood and severity of a possible loss

Which Mitigation?

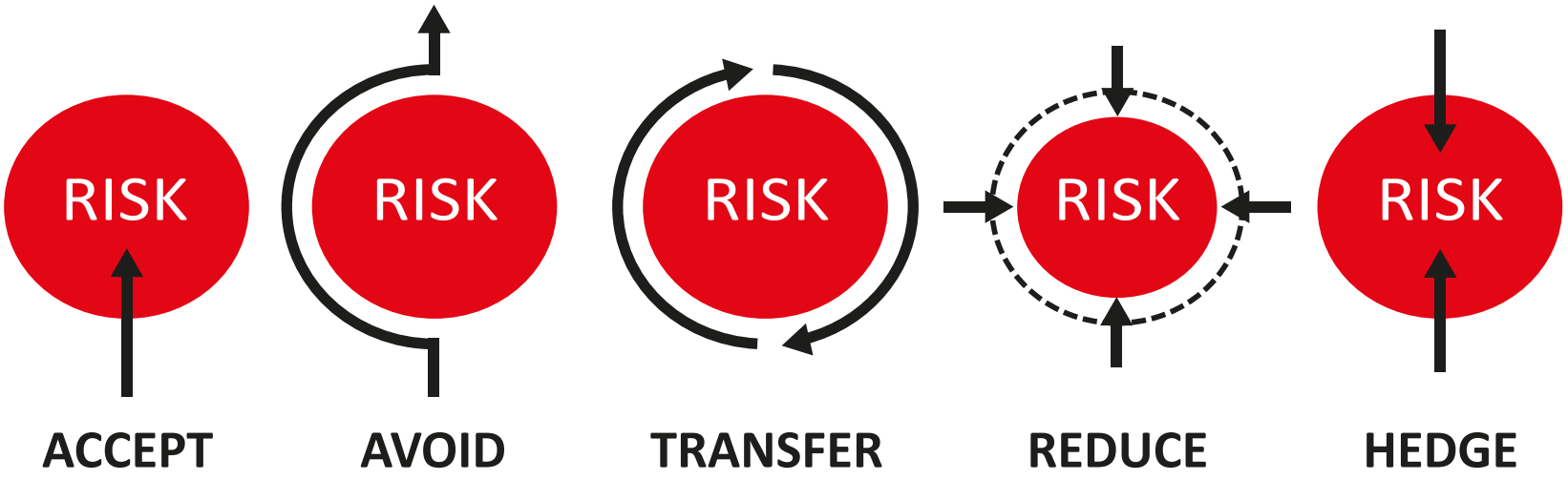


Risk	Mitigation Measures	Type A: avoidance L: limitation
Low acceptance of the new solution	- Xxx - Xxx - Xxx	A L ...
Budget overrun	- Xxx - xxx	
Low data protection	- Xxx - Xxx	
No resource available	- Xxx - Xxx - Xxx	

Budget and report mitigation measures

- Implement controls to manage mitigation measures (responsible, deadline, status)
- Measure the results of the mitigation measures (effects, dates) and adjust them

Risk Mitigation Strategies



Business Continuity Management (BCM)

BCM Definition

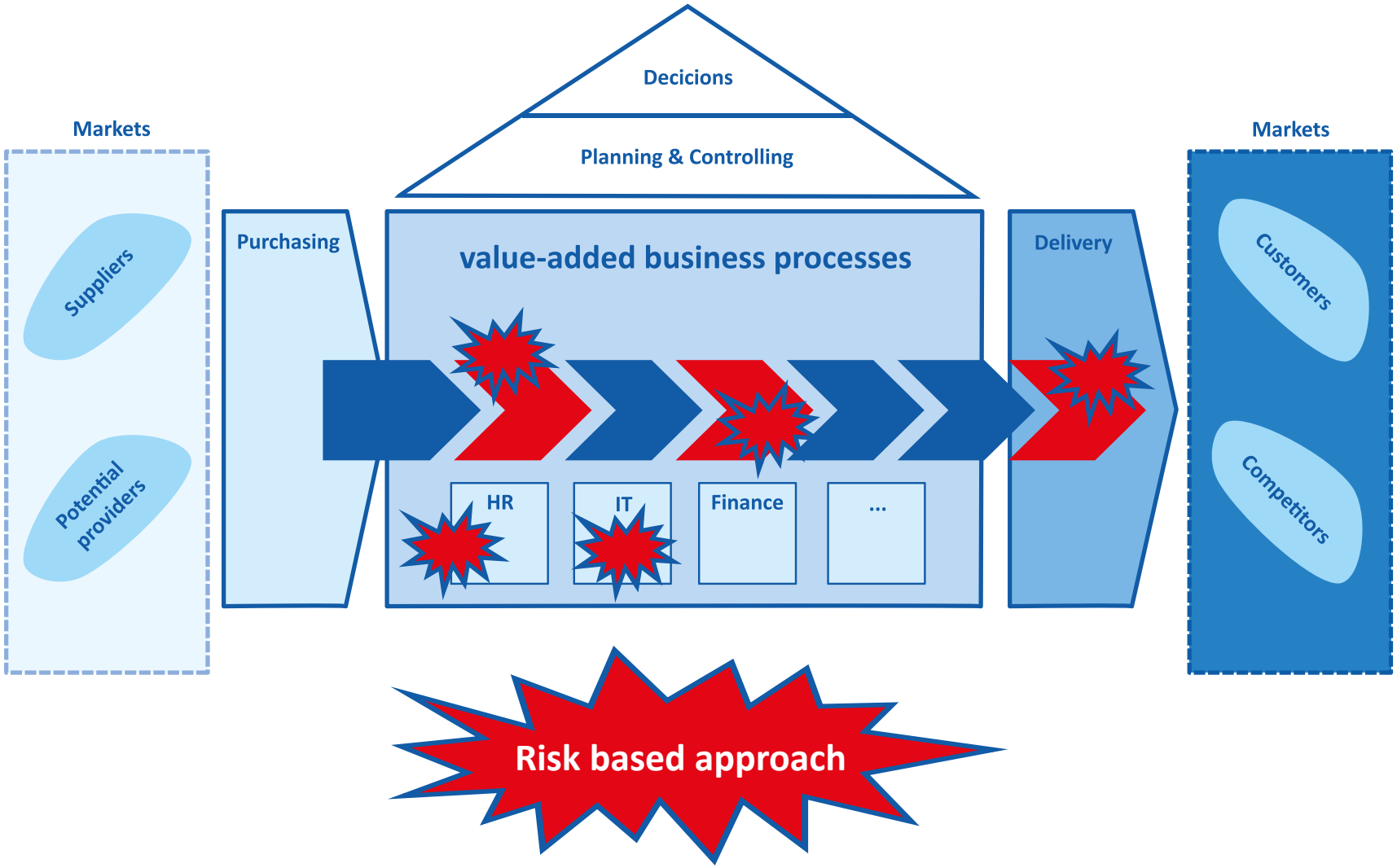
BCM is an enterprise-wide approach designed to ensure that critical business functions can be maintained or restored in time in the event of internal or external events.

BCM aims at minimizing the financial, legal and reputational impact of such events.

Examples of potential critical situations:

- "Accidental" events, such as fire or explosion
- Terror attacks, sabotage
- Natural catastrophes such as floods or earthquakes
- Loss of personnel, e.g. due to a pandemic
- Failure of building service engineering and/or energy supply (e.g. electricity)
- Failure of IT systems or infrastructures (hardware or software failure)
- Failure of communication systems or telecom providers
- Failure of external suppliers (e.g. outsourcing) such as information providers

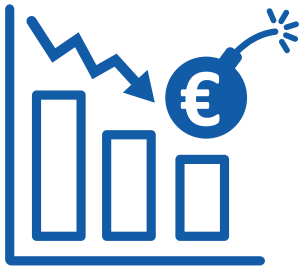
BCM aims at maintaining critical functions



Examples of Crisis Scenarios

Unavailability of facilities

Unavailability of IT Systems



Cash crisis

Unavailability of employees

Threat analysis

selected scenarios with critical impact

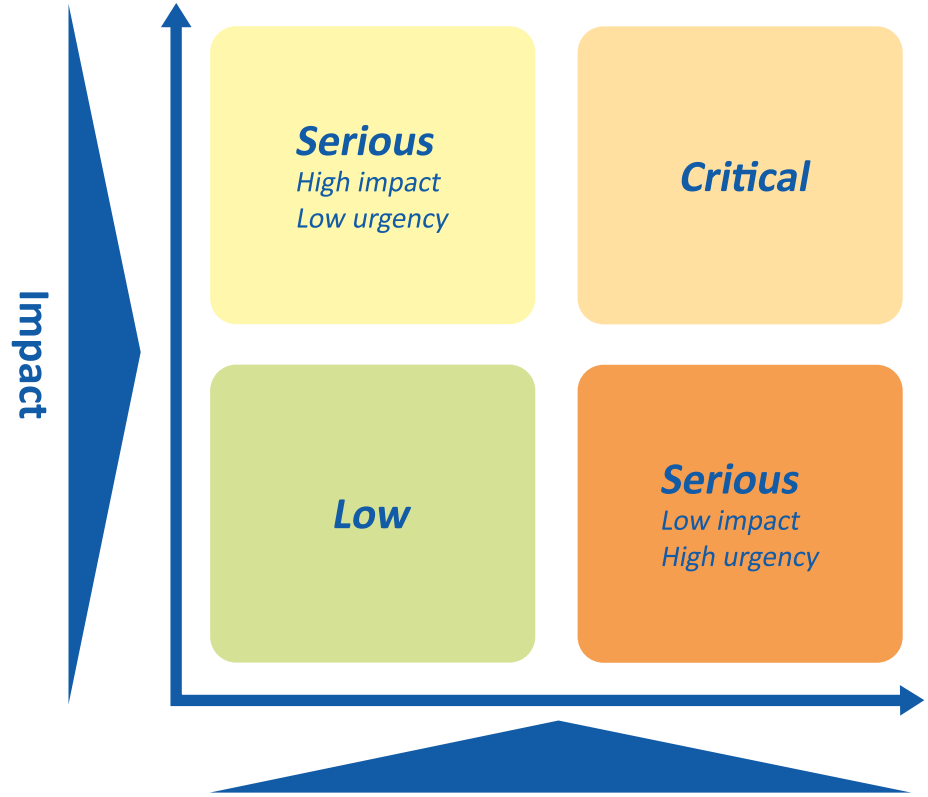
Personal injury : Danger to the health of employees, customers, local residents

Financial losses : Missed revenues, personnel costs,..

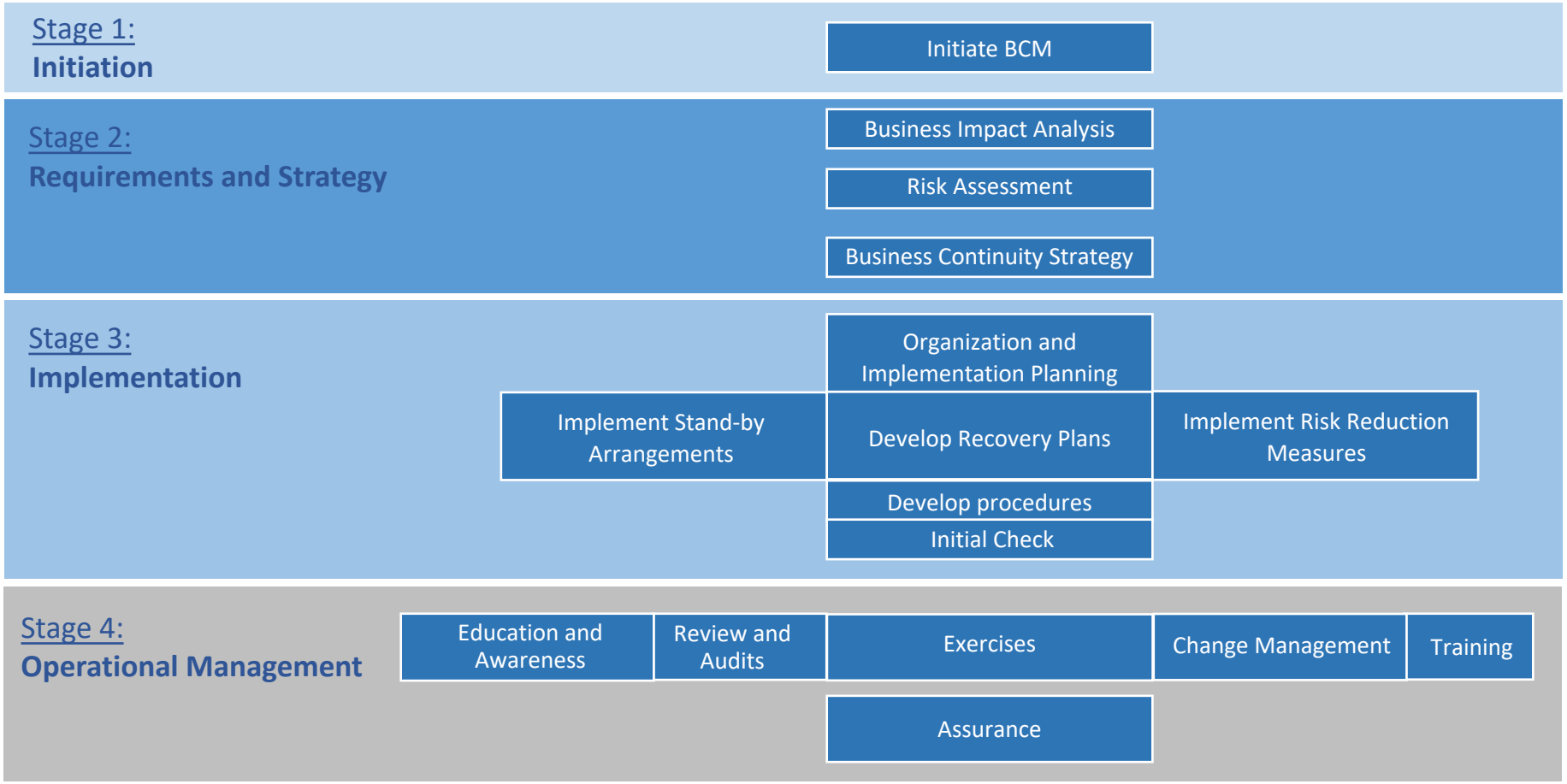
Image and reputation damage

Business impediments : Important data and information not available (calculation data, risk management, cash and liquidity balance,data)

Violation of legal or regulatory requirements : Legal or regulatory requirements cannot be met



BCM needs to be implemented step-by-step

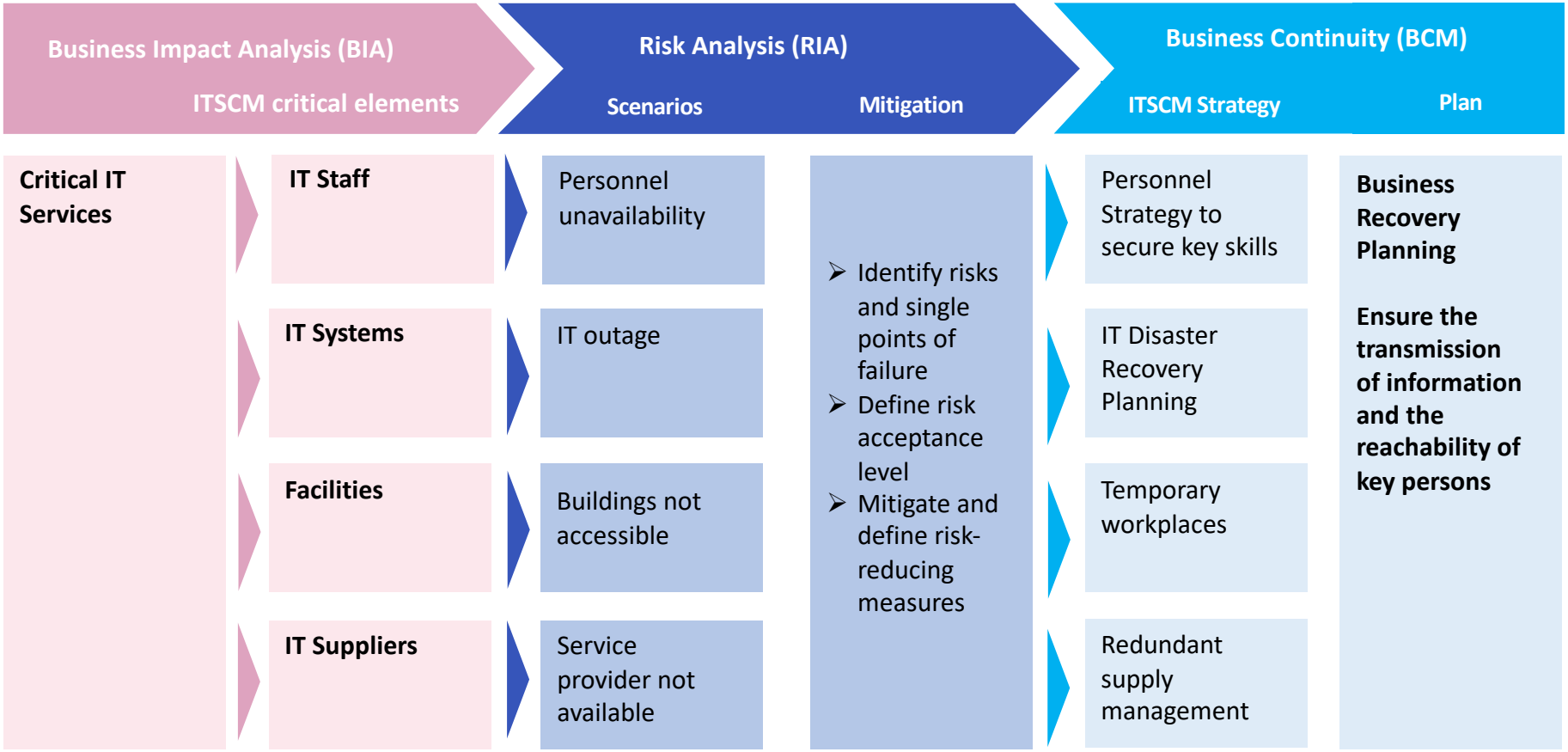


BCM needs to be planned

Project Phases	Q 1.1	Q 1.2	Q 1.3	Q 1.4	Q 2.1	Q2.2	Q 2.3	Q 2.4
Phase 1: Project setup Concept and policy development								
Phase 2: Business Impact Analysis Definition of ambition level, identification of business-critical processes and underlying critical resources, sign-off								
Phase 3: Business Continuity Strategy Definition of the basic procedure in case of failure of critical resources, basic decisions on the provision of replacement resources, sign-off								
Phase 4: Business Continuity Plans Detailed planning, procedures and responsibilities in case of failure of critical resources								
Phase 5: Business Continuity Testing and Training Review of BC plans for timeliness, implementation and effectiveness, professional training of employees with BCM tasks								

IT Service Continuity Management (ITSCM)

ITSCM is part of the BCM



ITSCM is part of the IT Service Catalogue

Following recovery objectives must be defined in case of a service outage:

- **Recovery Point Objective** (RPO) defines the maximum acceptable data loss in the event of a crisis
- **Recovery Time Objective** (RTO) defines the time period within which a service or a system must be recovered

Recovery Time Objective (Systems)	☐ **Highly available** RTO < 4 h	System recovery is critical The system must be continuously maintained during the main operating time • Automatic failover / hot stand-by • Dual site
	☐ **Highly reliable** RTO < 8 h	System recovery is essential The system may be minimally interrupted during the main operating time • Manual failover / cold stand-by • Dual site
	☐ **Conventional** RTO < 36 h	System is not essential The system can be interrupted • Rebuild overail system • Contingency system in second site available
	☐ **Basic** RTO < 4 weeks	System is not essential The system can be interrupted • Rebuild overail system • No contingency system available
Recovery Point Objective (Data)	☐ **Fault tolerant** (uninterrupted)	Data timeliness and/or data integrity are business critical and must be maintained under all circumstances • Duplexing • Hot Backup
	☐ **Standard** (RPO previous day)	Data timeliness and/or data integrity are essential. In case of a data loss the data status at the end of the previous day will be restored. • Data backup onvernight
	☐ **Uncritical** (RPO previous week)	Data timeliness and/or data integrity are not essential. In case of a data loss the data status at the end of the previous week will be restored • Data backup over weekend

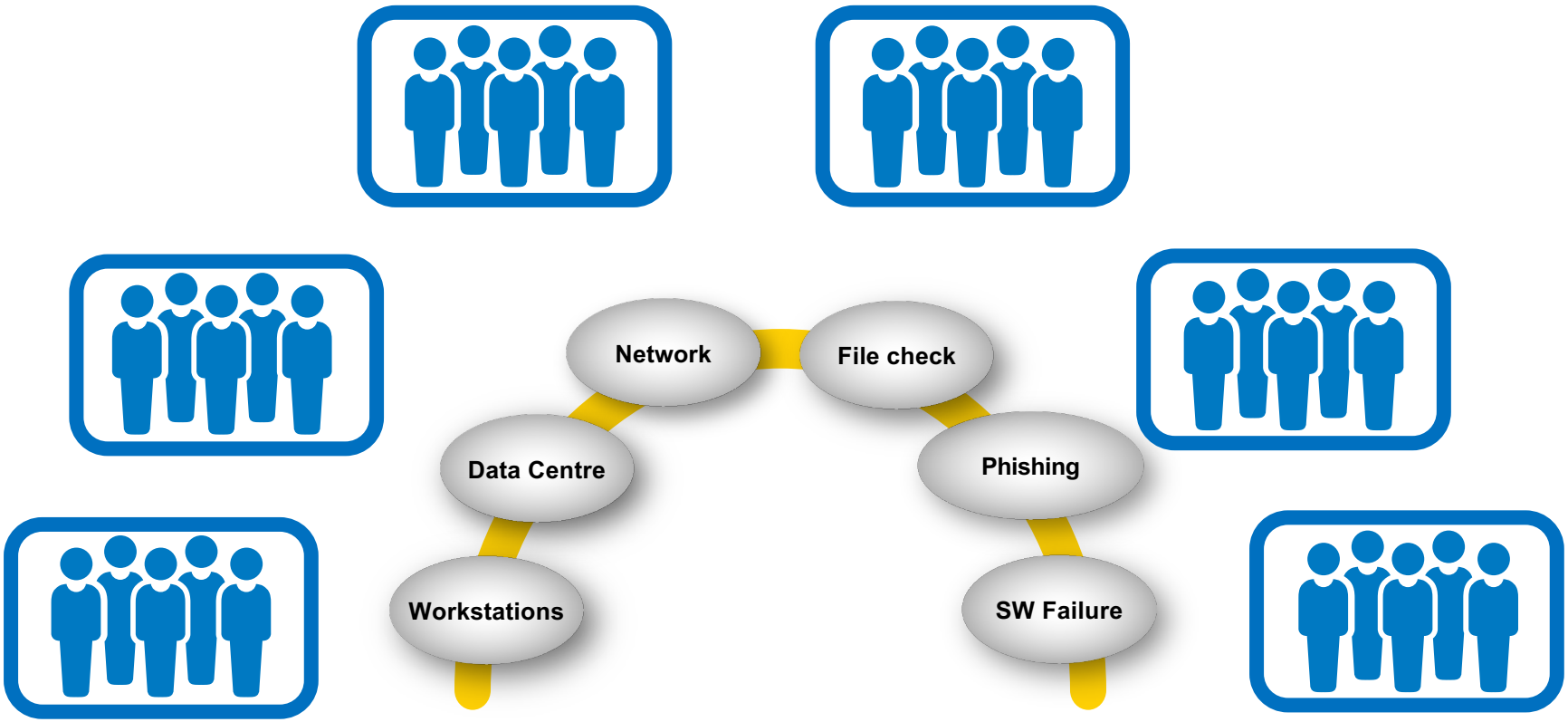
Disturbances need to be classified

Definition of impact	Measurement Criteria: Reponse time		Locations affected		Users affected	Category
Total loss of service and subsequently loss of a core component	More than 30 seconds	AND	All	OR	More than 20 %	**SEVERITY A** Service down
An important function of an IT service is not available	More than 30 seconds	AND	At least one	OR	More than 20 %	**SEVERITY B** Major Impact
Individual, less important functions of an IT service are not available	More than 30 seconds	-		AND	Less than 20 %	**SEVERITY C** Minor Impact
Disruptions which have no (or only minimal) impact on the use of an IT service thanks to system design (e.g. redundancy)	More than 30 seconds	-		AND	Less than 5 %	**SEVERITY D** Minimal Impact

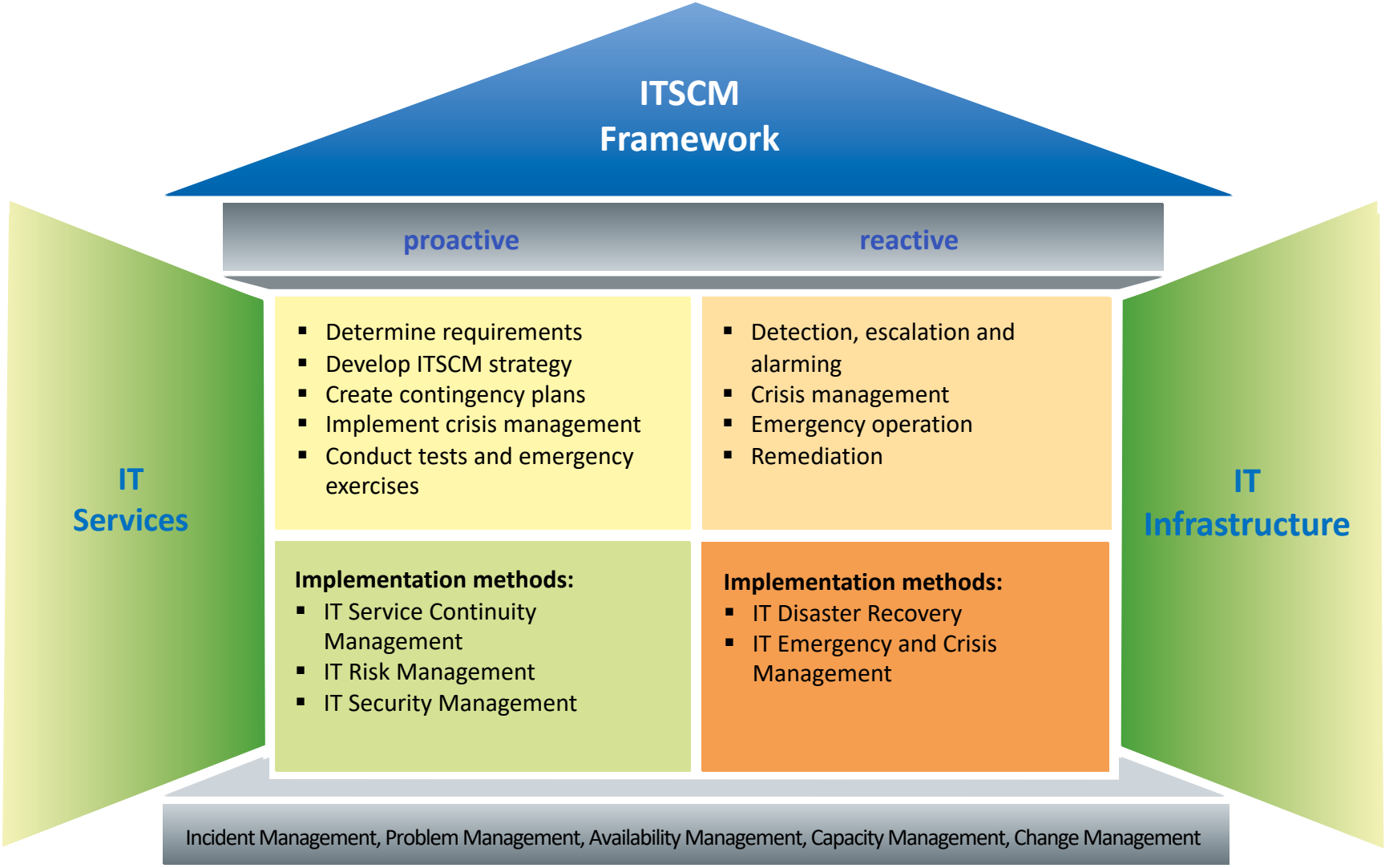
Define the ITSCM measures needed in case of…

Scenarios

- No workstation available at one location
- Power outage in a data center
- No network
- A file check for incoming files no more running
- Phishing email with users who clicked on a fake link
- Wrong programming (of instance wrong currency rates, 1 USD = 2 CHF)

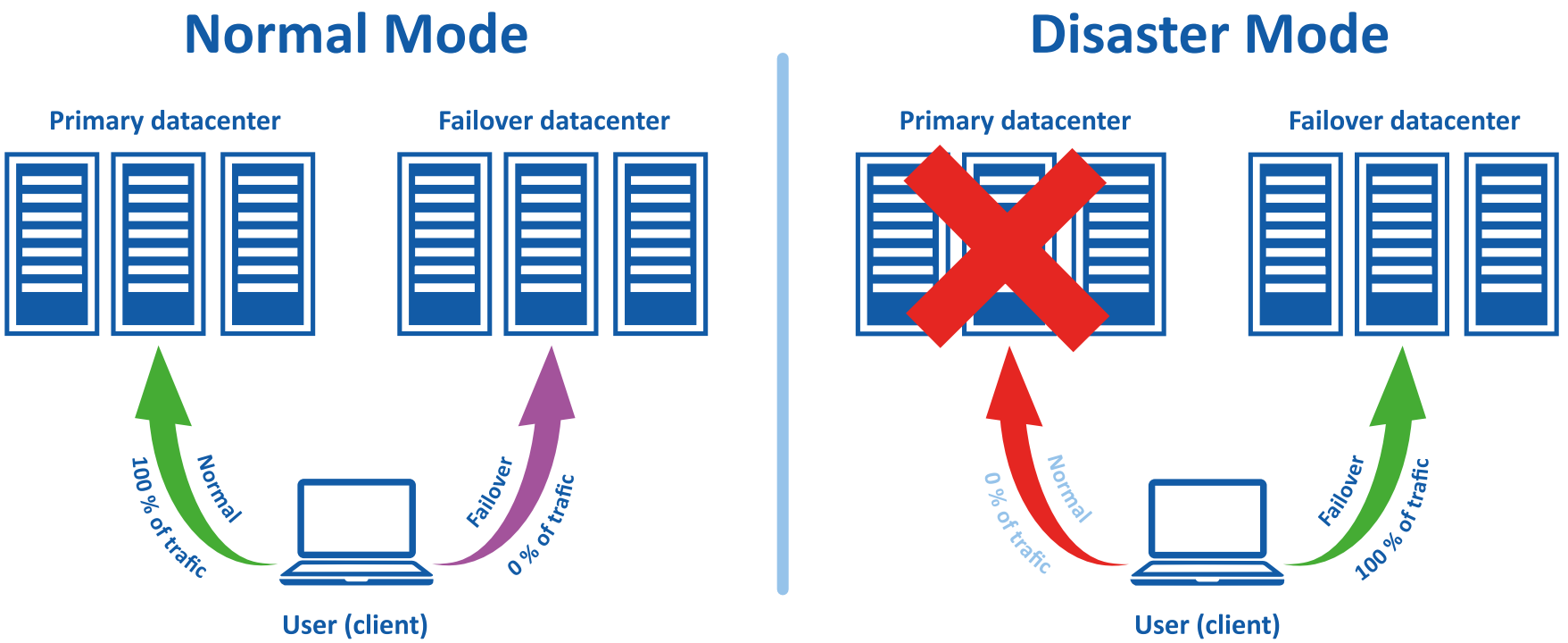


Proactive and reactive measures are needed



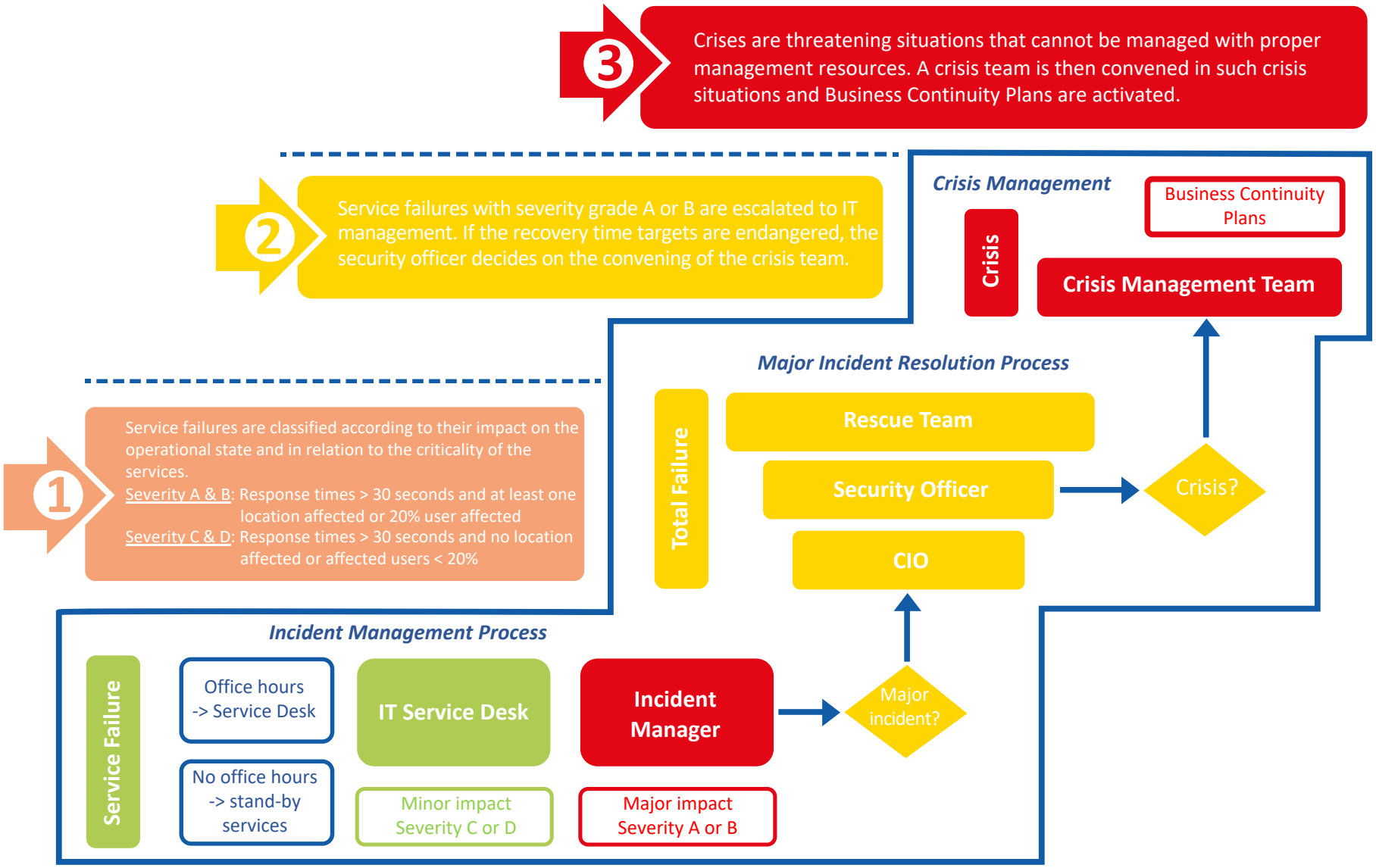
Failover as an example

Failover enables a switch to a redundant environment.
When a primary system component fails, the failover reduces or eliminates negative user impact.



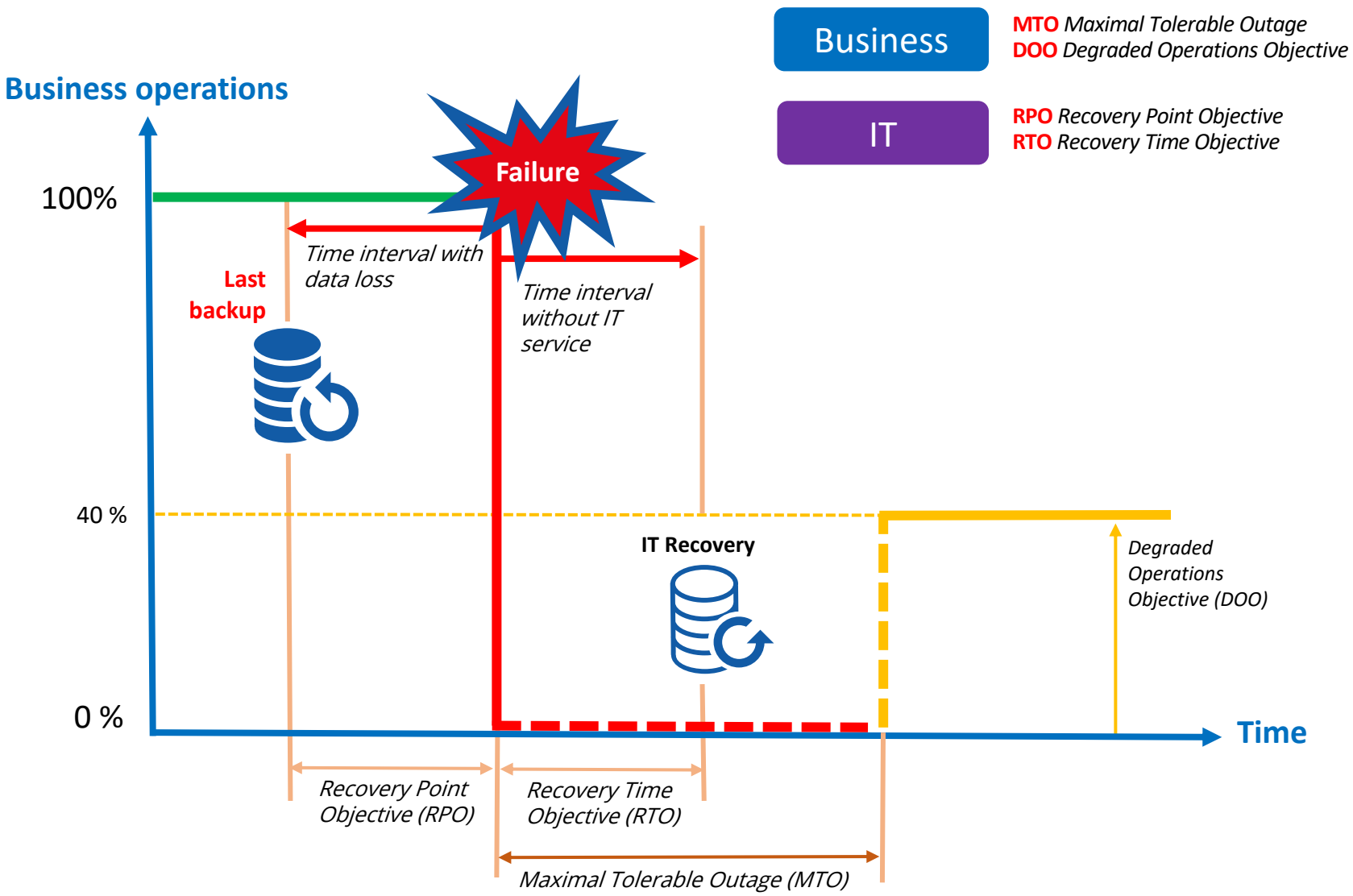
Crisis Management

Response to an Emergency



Levels of Escalation

Recovery Principle



The Disaster Recovery Plan

A disaster recovery plan helps to establish a written plan of action for what happens **when, not if,** disaster strikes. This is the most important part of your business continuity framework.

If you do not know what will happen if an application goes down or a company critical system decides to not work, you are off to a tough start.

Best Practices for IT Disaster Recovery

1 **Back up data regularly**
Monitor backup procedures and make sure that the stored data is useable

Operate 2 to 3 different data centres 2
Aim for Tier 4 certified redundant data centres

3 **Provide secure and redundant connectivity**
Have a dual provider strategy in place

Manage and update your IT assets 4
Keep updating your infrastructure and ensure system lifecycle

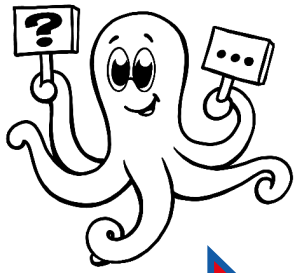
5 **Plan enough server capacity**
Monitor carefully your server capacity and anticipate performance issues

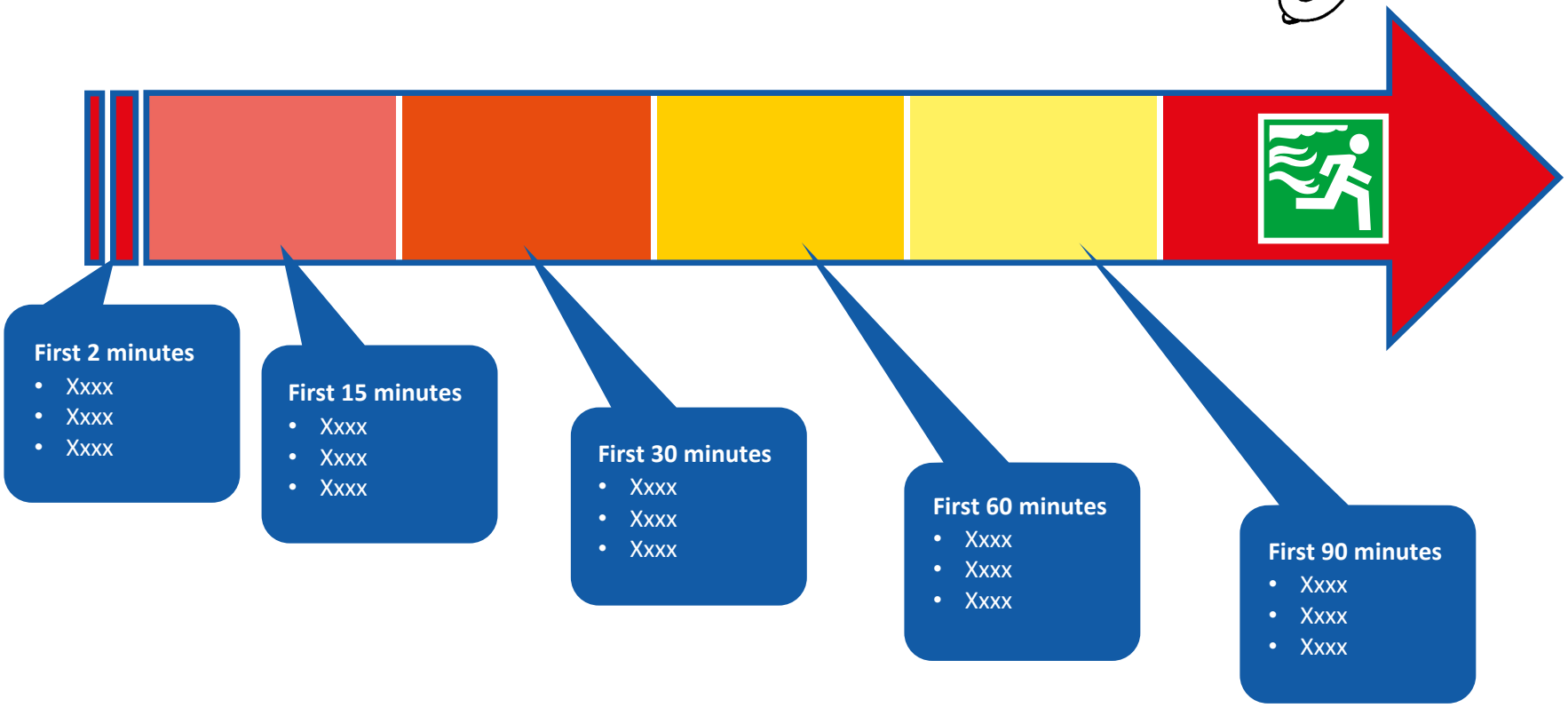
Train your staff 6
Train system owners and avoid a risk concentration on a few employees

7 **Conduct a failover test once a year**
Organise a switchover of systems over a few days

Test recovery plans, especially for new systems 8
Use the possibility of new productive infrastructures to check a recovery plan

Example: Emergency Evacuation

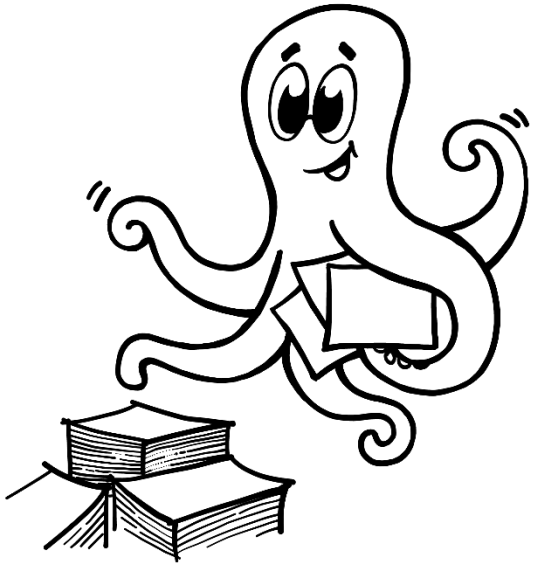




Stay safe and be prepared

Take away and must know!

- Definition of a risk
- Know the risk management process
- Draw a risk matrix
- Understand the BCM principles
- Know the meaning of RPO and RTO



Literature

- Jolly A (2003) Managing Business Risk: A Practical Guide to Protecting Your Business. Kogan Page, London and Sterling
- Pilorget L, Schell T (2018) IT Management. Springer, Wiesbaden

---

- Federal Office for Information Security

  https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.html

KNOWLEDGE

www.know-ledge.ch