Network Security

Information Security Governance

Prof. Dr. Henning Trsek, Institute Industrial IT

Motivation -

An initial real world case study

Agenda of todays lecture

- **Information Security Management System**
- **Plan - Information Security Risk Management**
- **Compliance and Data Protection (DSGVO)**
- **Direct - Information Security Policies and Controls**
- **Monitor and Evaluate - Information Security Measurement: Security Intelligence KPIs**

Definition Information Security

Information security

Ensures that the security objectives **Confidentiality, Integrity** and **Availability** of all information assets of an organization are always met.

Information assets are

Information and information processing systems, which have a certain **value** for the organization

Also business processes are concerned, as long as they depend on the previous systems and information.

Information in **all possible types and formats** are concerned: printed, spoken, audio, video, IT-Systems

Security objectives

- **Confidentiality**
  - Information assets are only available and disclosed to authorized persons and systems
- **Integrity**
  - Information assets are always complete and correct
- **Availability**
  - Information assets can be used whenever needed
- **Other objectives can be defined, if needed (e.g. non repudiation, authenticity, data protection, etc.)**

Agenda of todays lecture

- **Information Security Management System (ISO 27001, BSI 100-1)**
- **Plan - Information Security Risk Management**
- **Compliance and Data Protection (GDPR)**
- **Direct - Information Security Policies and Controls**
- **Monitor and Evaluate - Information Security Measurement: Security Intelligence KPIs**

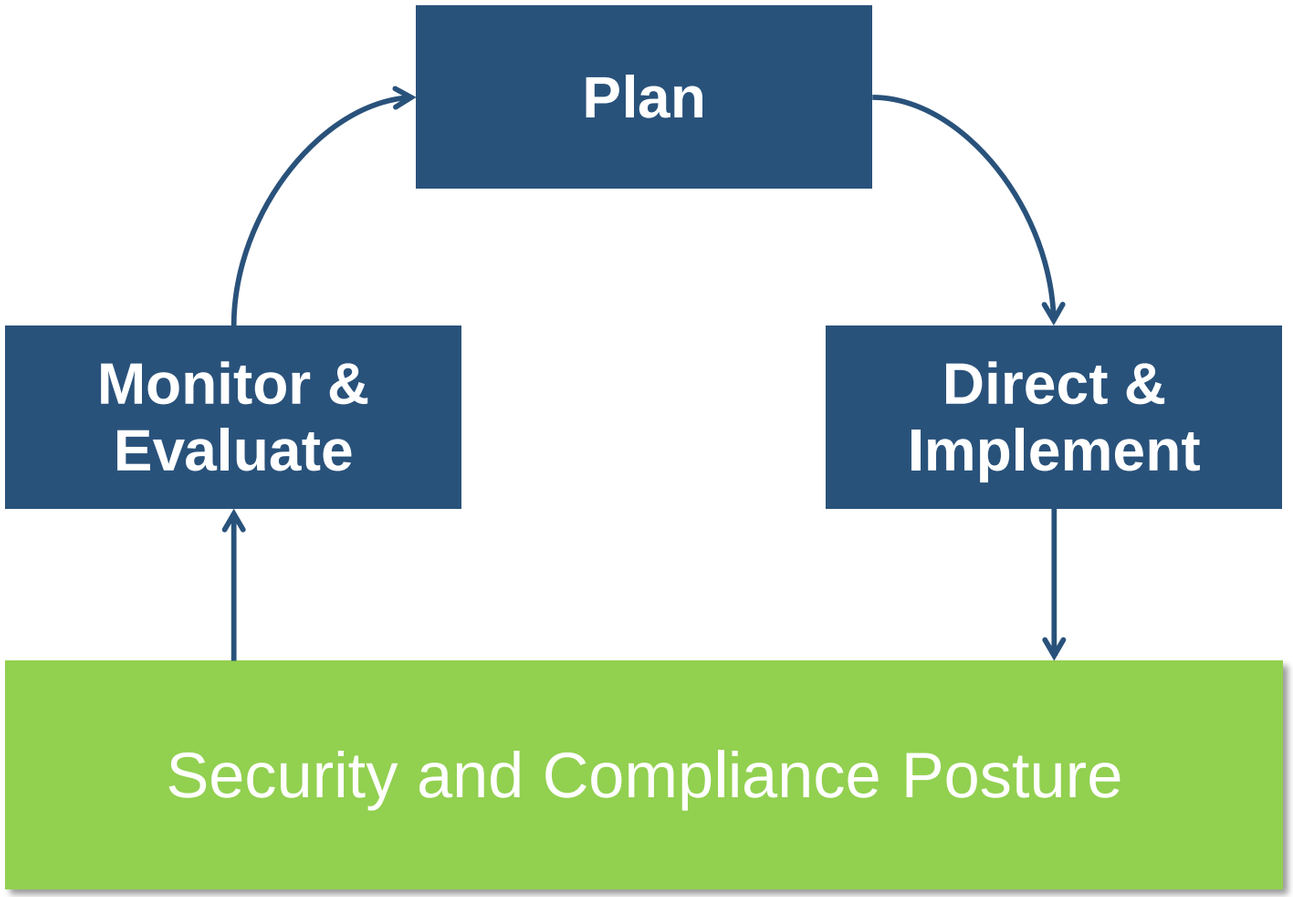
Security as process

- **Security is not a state or something alike, it is a process, i.e., it is exposed to continuous dynamics**
  - Freqently changing threat landscape
  - Changes in regulations
  - Technological progress
  - Hacker also progress …
  - Threats for companies are growing faster (Internet) as Security architectures, technologies and processes
- **Security must be actively managed, maintained and improved:**
  - Analysis of existing IT systems, and systems to be implemented
  - Identification of assets
  - Define objectives and controls
  - Measure and monitor them regularly
  - Find Vulnerabilities and Improvements
  - Plan and implement them
  - Consider IT-Security aspects during disposal
  - Security as part of the development process

Security as a Process – ISO 27001

Setup the Information Security Management process according to an established standard (ISO 27001)

ISO 27001 - A Control System



Typical Motivation

Risk Management

- Corporate risk management (e.g. KontraG) requires reporting information security risks
- *Use a systematic, standard-based method that*
- *Allows selection and prioritization of security controls and*
- *Is integrated with the existing frameworks.*

Compliance and External Audits

- Organization is subject to legal requirements (e.g. data protection and privacy) and external audits (e.g. SAS 70)
- *Are controls in line with auditing standards (e.g. COBIT)?*
- *Is compliance ensured?*
- *Is operating effectiveness attestable?*

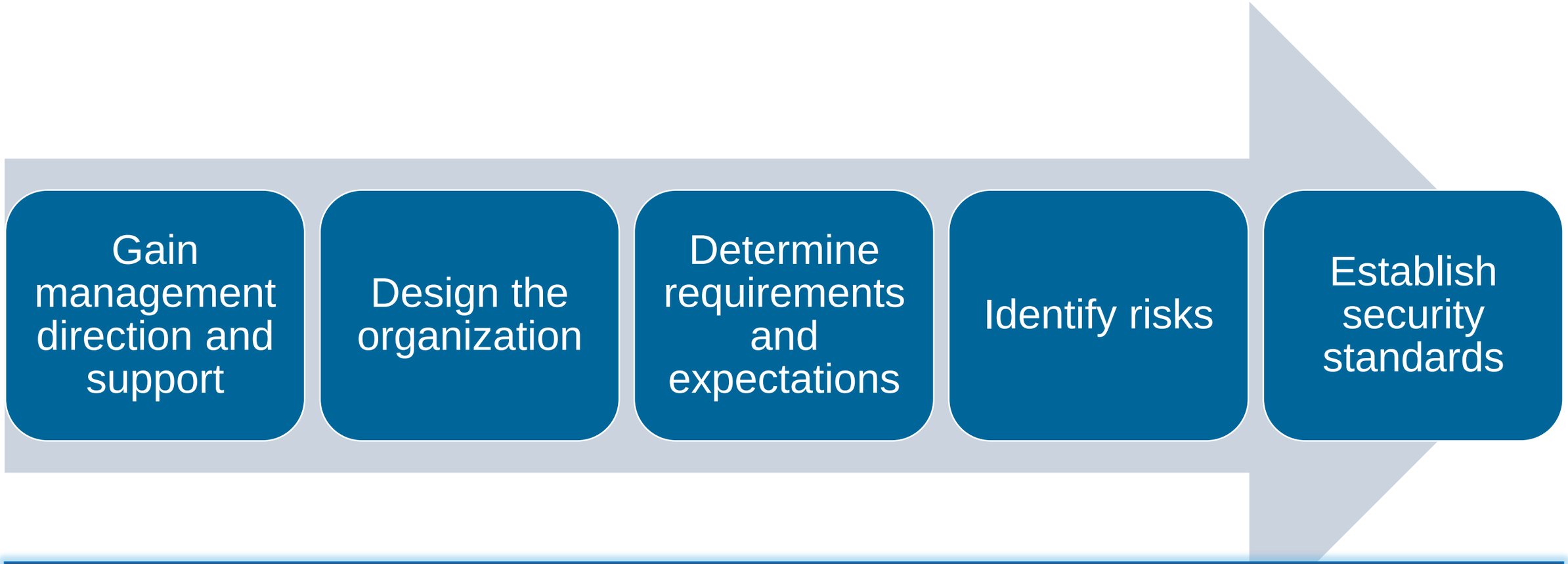
Security Policies and Guidelines

- Policies and technical safeguards evolved over the past years
- *Are controls appropriate, consistent, and & up-to-date?*
- *Are controls in line with best practices?*
- *Are controls usable for audits?*
- *Establish a controlled safeguard selection process*

Measuring Security

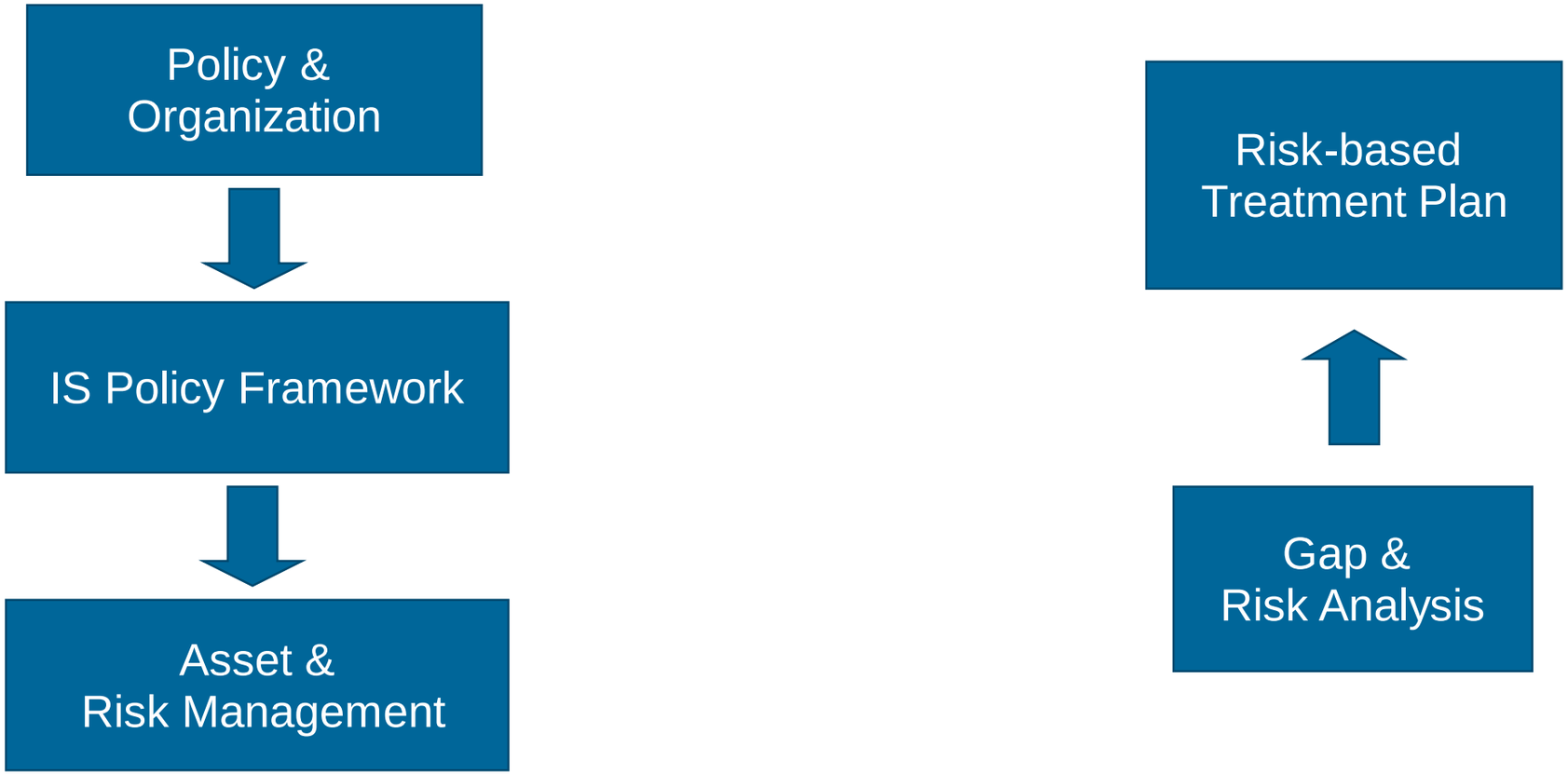
- Controls are in place and running
- *Monitoring and reporting status, performance and development*
- *Detecting and assessing weaknesses*
- *Attesting operating effectiveness*

Key Steps to Setup the Process



In practice, it is not as straight-forward as an arrow!

… you will have to work top-down and bottom-up



Challenges & Experiences

Common Basis

Interfaces and Integration

Organization

Challenges & Experiences

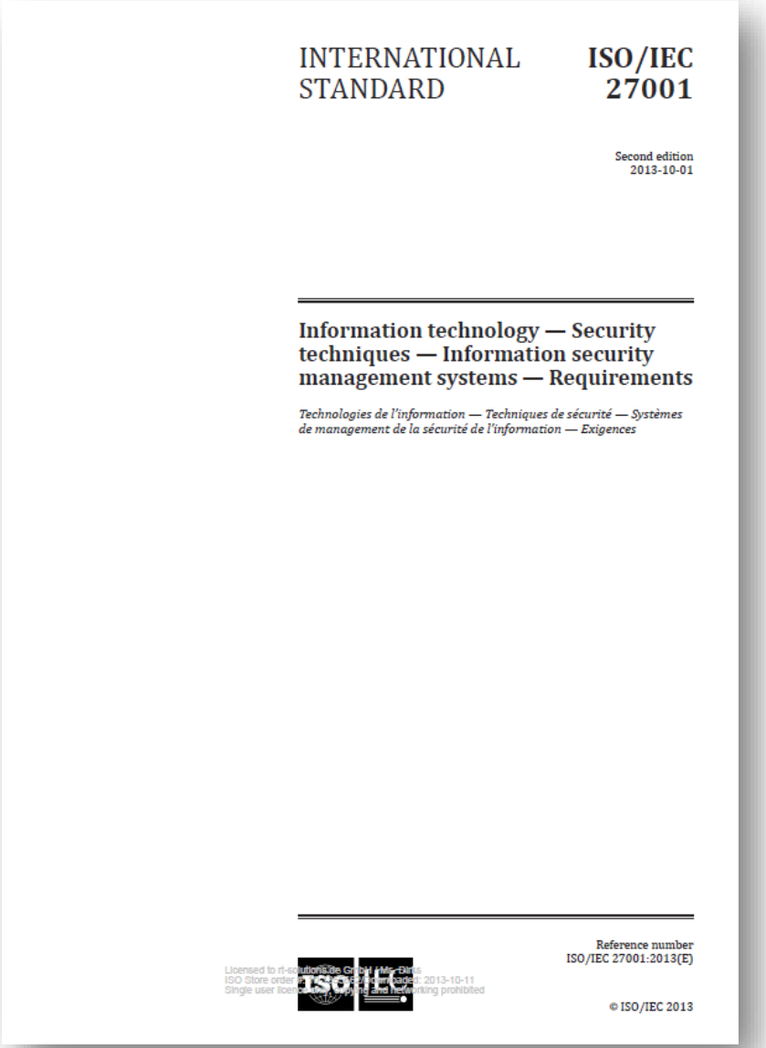
Best Practices & Priorities

Manageable Core Processes

Monitoring & Audit

ISO 27001 -

Lets take a brief look into the standard?



INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Agenda of todays lecture

- Information Security Management System
- **Plan - Information Security Risk Management (ISO 27005)**
- Compliance and Data Protection (GDPR)
- Direct - Information Security Policies and Controls
- Monitor and Evaluate - Information Security Measurement: Security Intelligence KPIs

Risk Management is not just a legal requirement

To setup a comprehensive, doable and effective IT/IS Risk Management framework in line with ERM requirements and good practice

(Or to improve the existing framework in that direction)

- Enterprise Risk Management is a legal and good governance requirement and IT risks have to be integrated
  Auditors have it in scope as a consequence

- Growing recognition of the dependency on information and IT and the reality of threats
  IT risks are still not recognized as material business risk and have no top-level visibility though

- Risk Management is the core of IS and key to IT Management
  It enables risk-based selection, prioritization, business alignment, resource allocation of security controls and reaction to findings, vulnerabilities, innovations,…

For key areas have to be addressed

Policy

Organization

Tools

Processes

The RM policy sets scope, directions and cornerstones

Policy contains

- **Scope in terms of organizational units and type of risks**
- **Objectives of the risk management**
- **Criteria to evaluate risks and decide about their priority, reporting and acceptability (in line with ERM scales)**
- **Risk management approach**
- **Accountabilities and reporting lines**
- **Key Controls for the RM processes to achieve comparable assurance**

Organization combines accountability with communication, resources and authority

Accountability & Responsibility

- Ownership of the policy
- Ownership of the process
- **Management of the process**
- **Ownership of risks (service providers and business)**

Reporting

- Defined reporting lines (depending on level of risk)
- To key stakeholders in IT and the business
- **Including effectiveness of controls and the framework**

Risk aware culture!

Skills & Resources

- Responsibilities communicated, understood and accepted
- **Persons in charge have required skills, resources and authority**
- Risk-aware culture established

Integration

- Into ERM
- Into IT planning and decision processes
- **Into business alignment**
- Into service change and operations processes

Process includes comprehensive risk assessment, response, control activities

Risk Identification

- Systematic approach
- Comprehensive regarding threats, processes & assets affected, and business impact
- Consideration of interdependencies leading to cumulative, cross-divisional risks

Risk Evaluation

- In financial, reputational and compliance terms
- Of both the inherent and the residual risk
- Aligned with the scales of the ERM

Risk Treatment

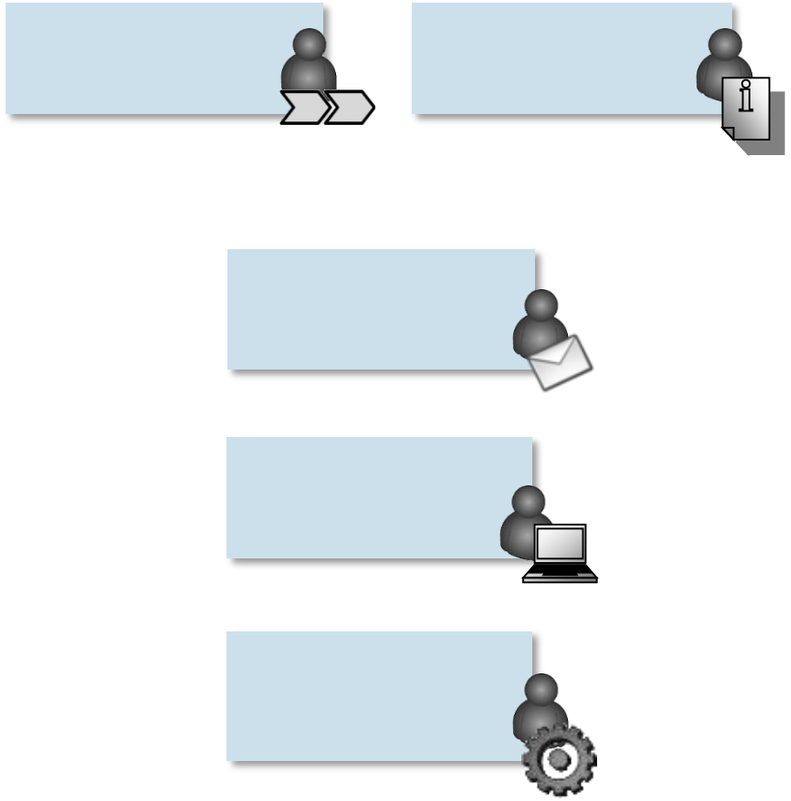
- Selection and implementation of treatment options
- Risks are communicated to relevant stakeholders
- Decision about risk treatment plans and acceptance of residual risks

Risk Monitoring and review

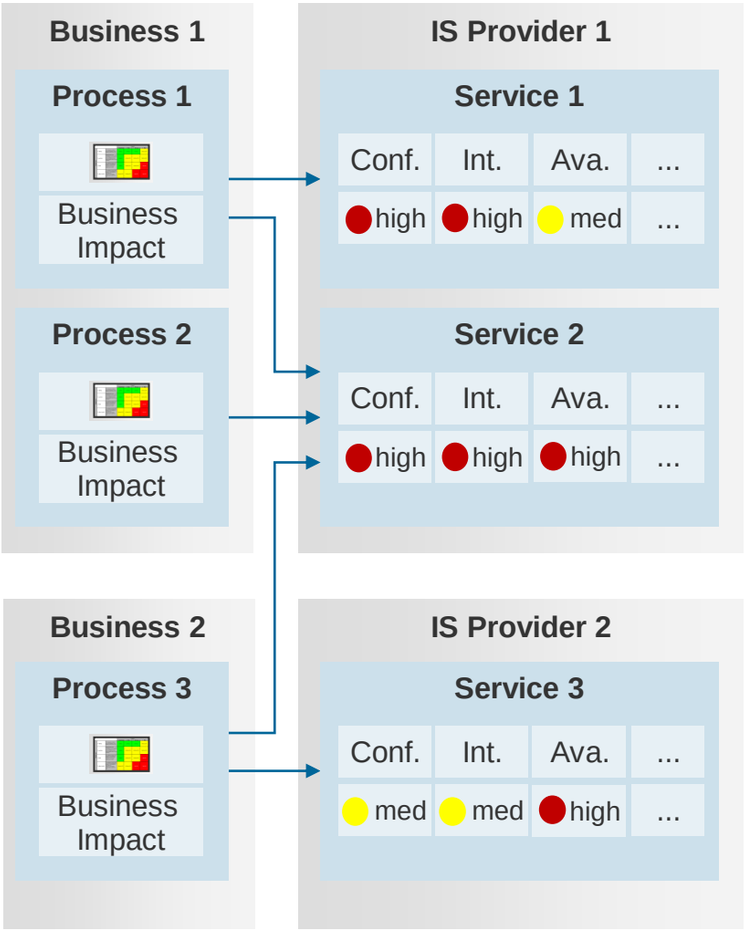
- Observation of risks using early indicators (KRI)
- Monitoring the effectiveness of key controls
- Monitoring the effectiveness of the process and the completeness and quality of results
- Tuning the process, resources and capacities

Identification of business critical assets is the starting point of RM

- Includes identification, valuation and ownership of assets
- Should use business impact criteria and what-if scenarios
- Enable/requires business involvement
- Is the root of risk ownership
- Must have the right level of aggregation
- Should leverage existing processes, units and tools (e.g. architecture)



An inventory of high business impact services is setup and maintained



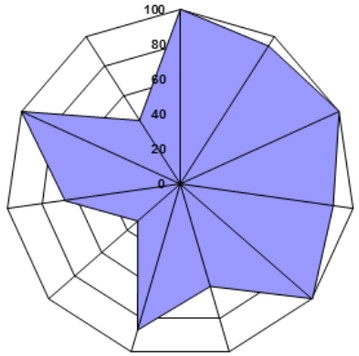
- All services are classified for all objectives based on business impact
- Setup close cooperation with internal customers on
  - Business impacts and
  - Risk tolerance
- Should leverage IT architecture, customer relations, BPM
- Results documented in the architecture model

Methods and tools support risk assessment

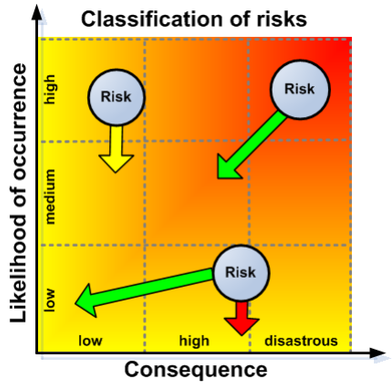
- **To support the identification of risks**
  Agreed and easy to understand threat catalogues and asset catalogues
- **To support evaluation of risks**
  Scales for measuring the impact, likelihood and risk matrix that fit to the accuracy of estimation, easy-to-use, in line with ERM
- **To support the monitoring and reporting of risk**
  All risks are maintained in a risk register and risk reporting is possible for different kinds of views
- **To support risk treatment**
  Tracking of control effectiveness and control activities
- **To support the overall risk management**
  Implementing work flows, tracking of activities, differentiated reporting

Risk Management Approaches for Controls Selection

- **Baseline approach**
  - Conform to an accepted reference standard as well as compliance requirements
  - E.g. ISO 27002, IT Baseline Protection Catalogues, BDSG



- **Risk management approach**
  - Identify significant risks
  - Evaluate risks based on simple, discrete scales: impact and likelihood



- **Recommended: Hybrid approach**
  - Define and implement minimal control catalog for baseline protection
  - Select further controls based on risk reduction

BSI Publications

BSI-Standards for Information Security

BSI-Standard 200-1
Management systems for information security (ISMS)

BSI-Standard 200-2
IT baseline protection methodology

BSI-Standard 200-3
Risk analysis based on IT baseline protection

BSI-Standard 100-4
Business continuity management

IT-Baseline Protection Compendium

Chapter 1 Introduction
Chapter 2 Layered architecture and Modelling

Elementary threats

Layers
Process modules:
- ISMS (security management)
- ORP (organisation and personnel)
- CON (concepts and procedures)
- OPS (operations)
- DER (detection and response)

System modules:
- IND (Industrial IT)
- APP (applications)
- SYS (IT systems)
- NET (networks and communication)
- INF (infrastructure)

Idea and objective of the IT baseline protection (BSI Grundschutz)

Idea

- Organisation deploys typical components (e.g. Server, Clients, common Operating Systems)
- No comprehensive risk analysis, instead based on common threats and their likelihood
- Recommendation of a set of suitable of Security controls
- Implementation guidance for controls

Objective

- Establish an extensible standard Security level
- Achieve an optimal effectiveness by implementing tested and validated controls

BSI baseline protection - Structure of the compendium

- **Module oriented**
  - Selection based on the components of the IT
- **Structured in several layers**

Process modules

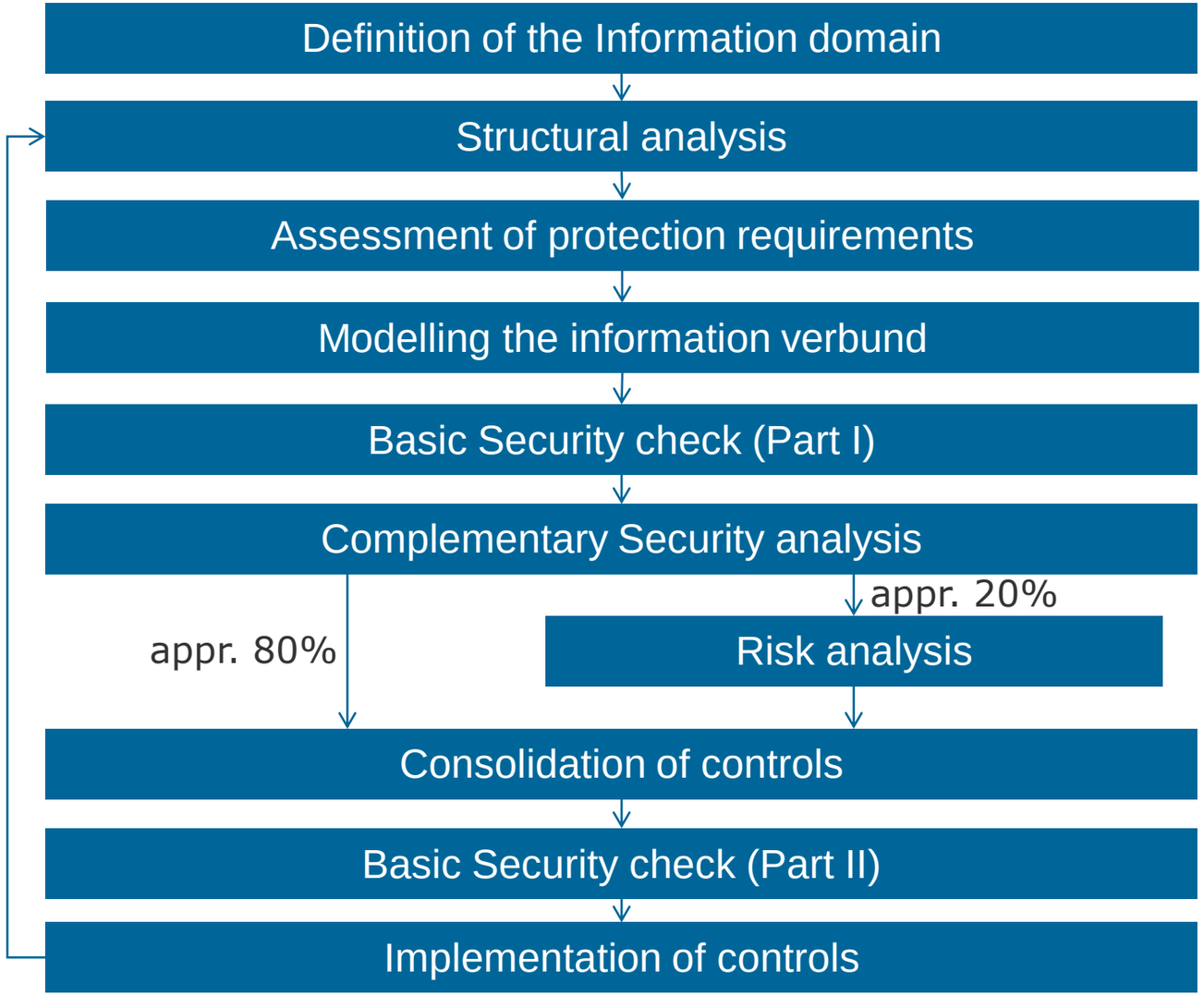
- ISMS (implemented requirements)
- ORP (Organisation and personnel)
- CON (concepts and procedures)
- OPS (operations)
- DER (detect & response)

System modules

- APP (applications)
- SYS (IT systems)
- IND (Industrial IT)
- NET (networks and communication)
- INF (infrastructure)

Information domain

- Higher aspects
- Infrastructure
- IT systems
- Applications
- Employees



Complementary Security Analysis and Risk Analysis following BSI 200-3

- **Risk analysis required for objects/groups with …**
  - … high or very high protection requirements
  - … no available module in the IT baseline protection
  - … a very specific application scenario being not yet considered

- **Four phases:**
  - Overview of threats
  - Risk assessment
  - Treatment of risks
  - Consolidation of the concept

Risk analysis following BSI 200-3 (Example)

Baustein Nr.	Titel	Objekt
INF.7	Office room	Room 101
INF.2	Server room	Room 203
INF.5	Room for technical Infrastructure	Room 205
SYS.1.1	Common Server	SRV01
SYS.1.1	Common Server	SRV02
SYS.1.3	Server under Unix	SRV03

Risk analysis following BSI 200-3 (Example)

Baustein Nr.	Titel	Objekt
INF.7	Office room	~~Room 101~~
INF.2	Server room	~~Room 203~~
INF.5	Room for technical Infrastructure	Room 205
SYS.1.1	Common Server	~~SRV01~~
SYS.1.1	Common Server	SRV02
SYS.1.3	Server under Unix	SRV03

1. Remove all objects, which do not require a risk analysis

Risk analysis following BSI 200-3 (Example)

Baustein Nr.	Titel	Objekt
~~INF.7~~	~~Office room~~	~~Room 101~~
~~INF.2~~	~~Server room~~	~~Room 203~~
INF.5	Room for technical Infrastructure	Room 205
~~SYS.1.1~~	~~Common Server~~	~~SRV01~~
SYS.1.1	Common Server	SRV02
SYS.1.3	Server under Unix	SRV03

1. Remove all objects, which do not require a risk analysis
2. Remove all modules without an object

Risk analysis following BSI 200-3 (Example)

- **Objekt: SRV02**

Gefährdungen

Maßnahmen

	G1	G2	G3	G4		

Risk analysis following BSI 200-3 (Example)

- **Objekt: SRV02**

Gefährdungen

Maßnahmen	G1	G2	G3	G4	G5	G6

3. Analyse additional threats

Risk analysis following BSI 200-3 (Example)

- **Objekt: SRV02**

Gefährdungen

Maßnahmen

	G1	G2	G3	G4	G5	G6
M1	✓					
M2	✓	✓				(✓)
M3				✓		
M4			✓	✓	✓	

3. Analyse additional threats
4. Check whether all existing threats are sufficiently addressed by controls

Risk analysis following BSI 200-3 (Example)

- **Objekt: SRV02**

Gefährdungen

Maßnahmen	G1	G2	G3	G4	G5	G6
M1	✓					
M2	✓	✓				(✓)
M3				✓		
M4			✓	✓	✓	
M5		✓				✓
M6						✓
M7				✓		✓

3. Analyse additional threats
4. Check whether all existing threats are sufficiently addressed by controls
5. If threats are not yet covered: risk reduction

Agenda of todays lecture

- Information Security Management System
- Plan - Information Security Risk Management
- **Compliance and Data Protection (GDPR)**
- Direct - Information Security Policies and Controls
- Monitor and Evaluate - Information Security Measurement: Security Intelligence KPIs

Compliance - Motivation

- **Compliance**
  - Adherence to external legal, regulatory, audit or contractual requirements
  - A key driver for information security
- **Actually, it tends to become the sole focus**
- **That‘s why some consider it a threat to security**
- **External requirements are changing and applicability to your business may change**

You need a **process to preserve compliance** and you need awareness that **compliance does not imply security**

A few examples

- KonTraG
- Financial reporting (SOX, EuroSOX, BilMoG)
- Intellectual property rights
- Data Protection and Privacy
- Export Restrictions
- TKG, TMG

Data protection

- Organisation
- Register of processing operations
- Organisational and technical controls
- Contractual data processing
- Third countries

Compliance Approach

Identify applicable laws

Derive security requirements for information assets

Integrate in the risk management process

- Identify and evaluate risks
- Define and implement security controls

Assess and improve compliance

- Controls effectiveness
- Applicability of laws

Data protection – intro

- **Objective: Protection of personal data**
  - Customer data, employee data, supplier data, private email and phone usage, …
- **Motivation**
  - Regulatory obligation
  - Protection of the image
- **Examples of data protection violations -> Data theft**
  - Carelessness
    - Customer data on a CD
      (tax fraud)
  - Deliberately
    - Forbidden employee monitoring

General data protection regulation (GDPR) - Objectives

- Protection of basic rights and the fundamental freedom of natural persons, especially their right of the protection of personal identifiable data

- Uniform and equal high level of data protection within the EU

- Avoidance of competitive advantages of specific companies and strengthening of civil rights as well as the EU domestic market

GDPR in a nutshell

- “Marktort” principle
- New definitions of specific data (genetic, profiling, etc.)
- Privacy by design, privacy by default, right of deletion
- Data protection cause estimation
- Obligation to report incidents (within 72h)
- Extended documentation responsibilities (DPMS)
- Extended penalties (4% of the world wide turnover / 20 Mio. EUR)

Agenda of todays lecture

- Information Security Management System
- Plan - Information Security Risk Management
- Compliance and Data Protection (DSGVO)
- **Direct - Information Security Policies and Controls (ISO 27002)**
- Monitor and Evaluate - Information Security Measurement: Security Intelligence KPIs

Direct – IS Policies and Controls

- Setup a baseline standard
- Based on an accepted best practice (ISO 27002)
- Be determined to comply with it
- Use a layered structure with
  - Defined responsibilities and
  - Verifiable controls

Direct – IS Policies and Controls
Policy

Inhalt

Direct – IS Policies and Controls Standards

Control Areas to be Considered

Follow ISO‘s structure…

- **Organization of Information Security**
- **Human Resources Security**
- **Asset Management**
- **Access Control**
- **Cryptography**
- **Physical and Environmental Security**
- **Operations Security**
- **Communications Security**
- **System Acquisition, Development and Maintenance**
- **Supplier Relationships**
- **Information Security Incident Management**
- **Information Security Aspects of Business Continuity Management**

Consider no. of documents, ownership, readership,…

Structure of Standards & Procedures

- **Purpose**
- **Scope**
- **Responsibility**
- **Main part:**
  - Controls, Concepts, Procedures
- **Document approval**
- **Revision history**
- **Document owner**
- **References**
- **Terms & definitions**

Controls Structure

- **What?**
  - Precise but not too detailed
  - General in scope but auditable
- **For which assets?**
  - Based on classification and type
- **Who?**
  - Explicit responsibilities, stating roles
- **How?**
  - Set out key requirements and recommendations for control implementation

Not: What might have been done? What might be said about the topic?...

Control Example

- **Concise and verifiable controls with defined responsibilities**

4.1 Dokumentation der Betriebsverfahren

Schutzziele: Vertraulichkeit, Verfügbarkeit, Integrität

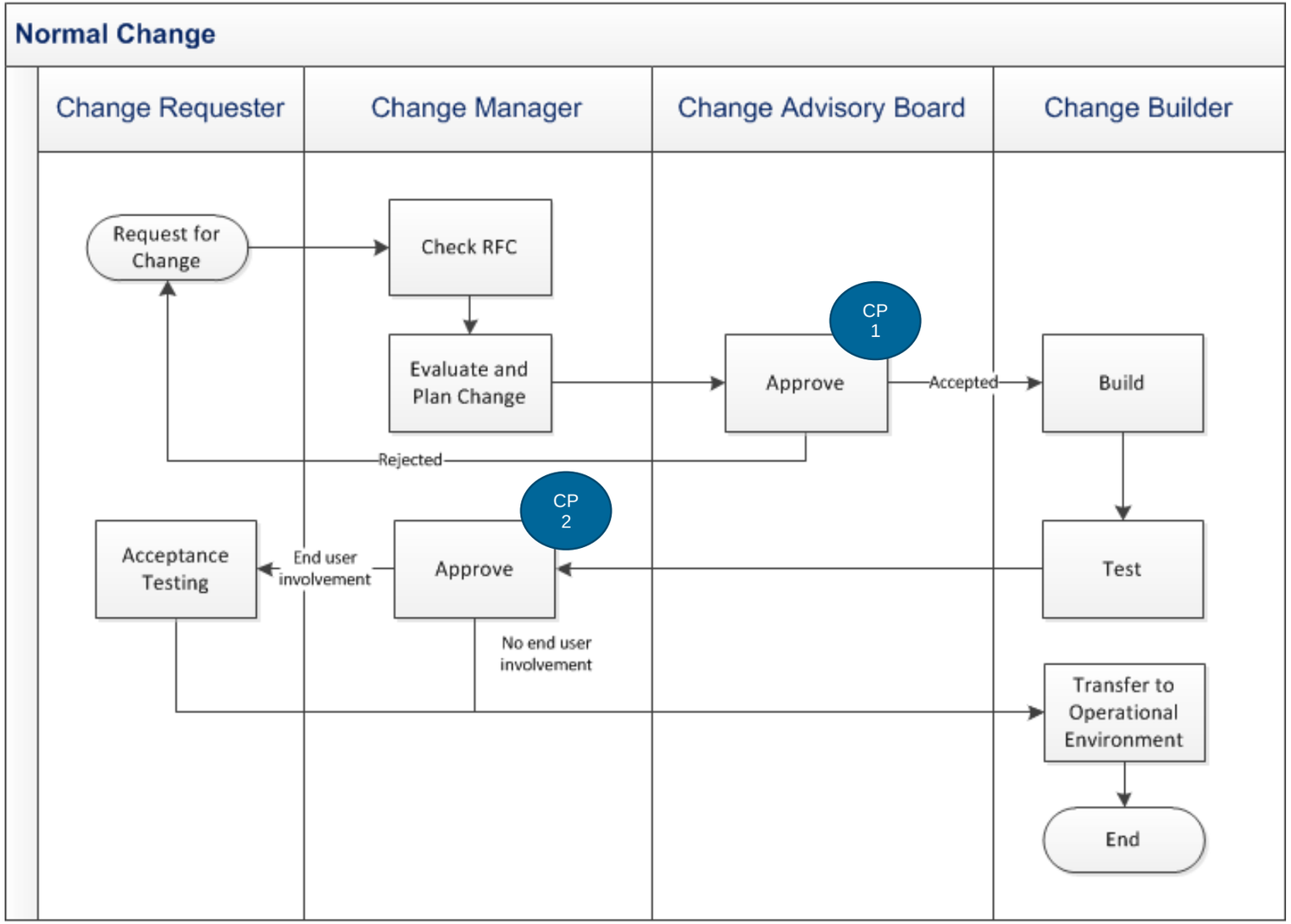
Maßnahmenbeschreibung	**Schutz-bedarfsklasse** [ab]	**Verantwortlicher**
Vor der Produktionseinführung eines neuen informationsverarbeitenden Systems[1] wird ein Betriebshandbuch erstellt, das die Betriebsverfahren, Verantwortlichen und Zugriffsregelungen festlegt. Das Betriebshandbuch ist dem *Informationssicherheitsbeauftragten* auf Anfrage zur Einsicht vorzulegen und muss allen darin festgelegten Verantwortlichen verfügbar sein.	Niedrig	System owner
Prüfung der Maßnahme: Für jedes informationsverarbeitende System liegt ein Betriebshandbuch vor.		

Vorgaben zur Maßnahmenumsetzung

Das Betriebshandbuch muss mindestens die folgenden Bestandteile umfassen.

Direct – IS Policies and Controls Procedures

Example: Change Management Procedure



Lifecycle of Standards & Procedures

Implementation of Standards & Procedures

- **Obtain approval & budget**
- **Prepare additional materials**
  - Checklists, forms, training slides, working instructions
- **Communicate**
  - Raise awareness
  - Get support
  - Brief & instruct
  - Train
- **Implement processes & technical controls**
- **Collect “Master Data”**

Challenges & Experiences

- Scope
- Interfaces and Integration
- Organization
- Structure
- Best Practices & Priorities

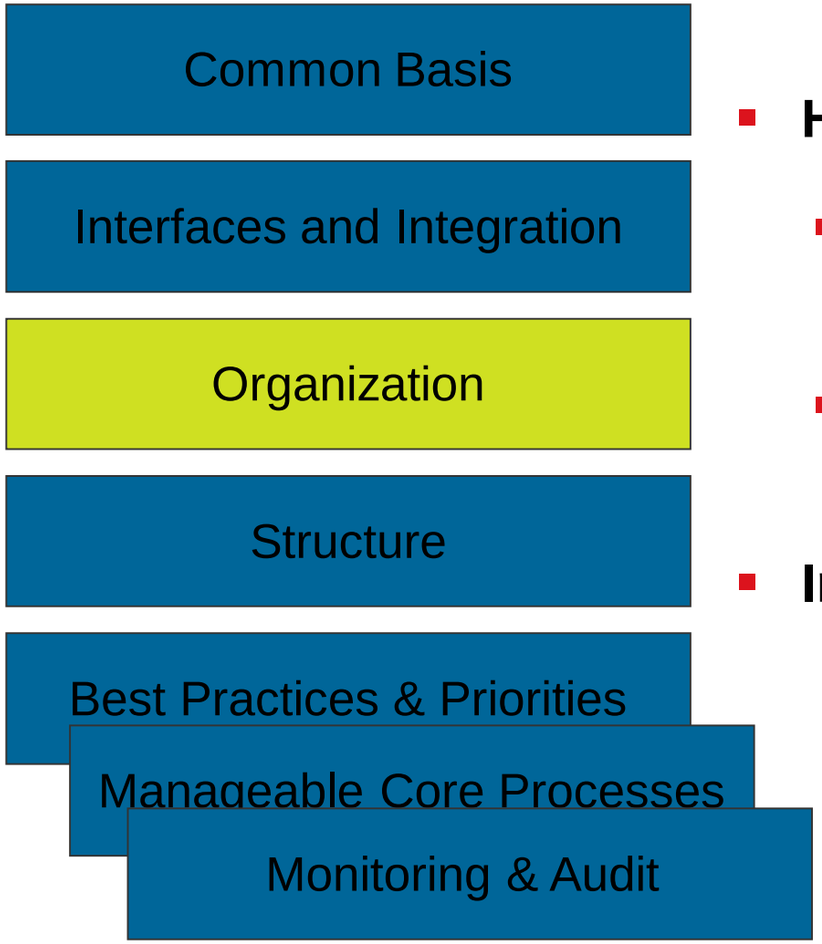
- **Common understanding of notions, goals and approach**
- **Scope (controllable and defendable, stakeholder expectations) and security domains**
- **Information or IT security?**
- **Have or implement a policy?**
- **Which standard?**
- **Bottom up or top down or both?**

Challenges & Experiences

- Common Basis
- Interfaces and Integration
- Organization
- Structure
- Best Practices & Priorities

- **Other management systems and processes**
  - Risk management
  - BCM
  - QM,…
- **Audit standards controls**
  - (Internal) audit, FARG, SAS 70, ….

Challenges & Experiences



- **How to**
  - Select, co-ordinate, and approve controls and
  - Plan, monitor, and audit their implementation
- **In a large-scale group of companies**

Common Basis

Interfaces and Integration

Organization

Structure

Best Practices & Priorities

- **Policy hierarchy**

Challenges & Experiences

- Common Basis
- Interfaces and Integration
- Organization
- Structure
- Best Practices & Priorities

- **Policy hierarchy**
- **Structure of the upper layers**
- **Concise and auditable formulation of controls**
- **With defined responsibilities and**
- **The right level of abstraction (lists of controls, task of the security group)**

Challenges & Experiences

Common

Interfaces and

Organiza

Structu

Best Practices

Inhaltsverzeichnis

Challenges & Experiences

Common

Interfaces and

Organiza

Structu

Best Practices

Common

Interfaces and

Organiza

Structu

Best Practices

4.1 Dokumentation der Betriebsverfahren

Schutzziele: Vertraulichkeit, Verfügbarkeit, Integrität

Maßnahmenbeschreibung	**Schutz-bedarfsklasse** [ab]	**Verantwortlicher**
Vor der Produktionseinführung eines neuen informationsverarbeitenden Systems[1] wird ein Betriebshandbuch erstellt, das die Betriebsverfahren, Verantwortlichen und Zugriffsregelungen festlegt. Das Betriebshandbuch ist dem *Informationssicherheitsbeauftragten* auf Anfrage zur Einsicht vorzulegen und muss allen darin festgelegten Verantwortlichen verfügbar sein.	Niedrig	Lt. AGSM
Prüfung der Maßnahme: Für jedes informationsverarbeitende System liegt ein Betriebshandbuch vor.		

Vorgaben zur Maßnahmenumsetzung

Das Betriebshandbuch muss mindestens die folgenden Bestandteile umfassen.

- Beschreibung des informationsverarbeitenden Systems
- Informationsverantwortlicher, Bereitsteller und Betreiber des informationsverarbeitenden Systems

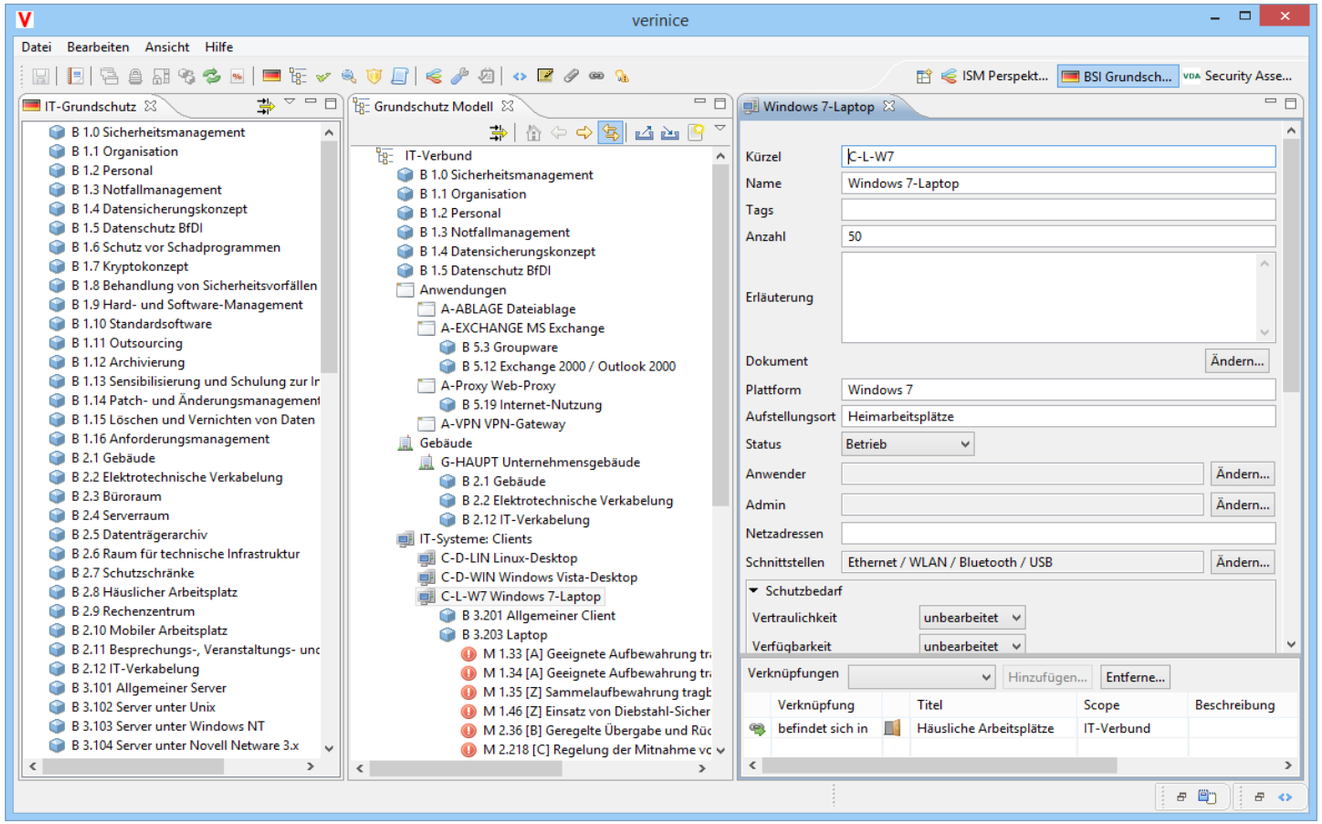
Challenges & Experiences

- Common Basis
- Interfaces and Integration
- Organization
- Structure
- Best Practices & Priorities

- **Determine gaps against the selected best practices**
- **Prioritize implementation of controls**
- **Check what is feasible**
- **Co-ordinate with stakeholders**

IS Policy based on „IT-Grundschutz“

- The policy creation process can *and should* be supported by suitable software, e.g. verinice



Scope

↓

Objects and Links

↓

Safeguards

↓

Supplementary Analysis

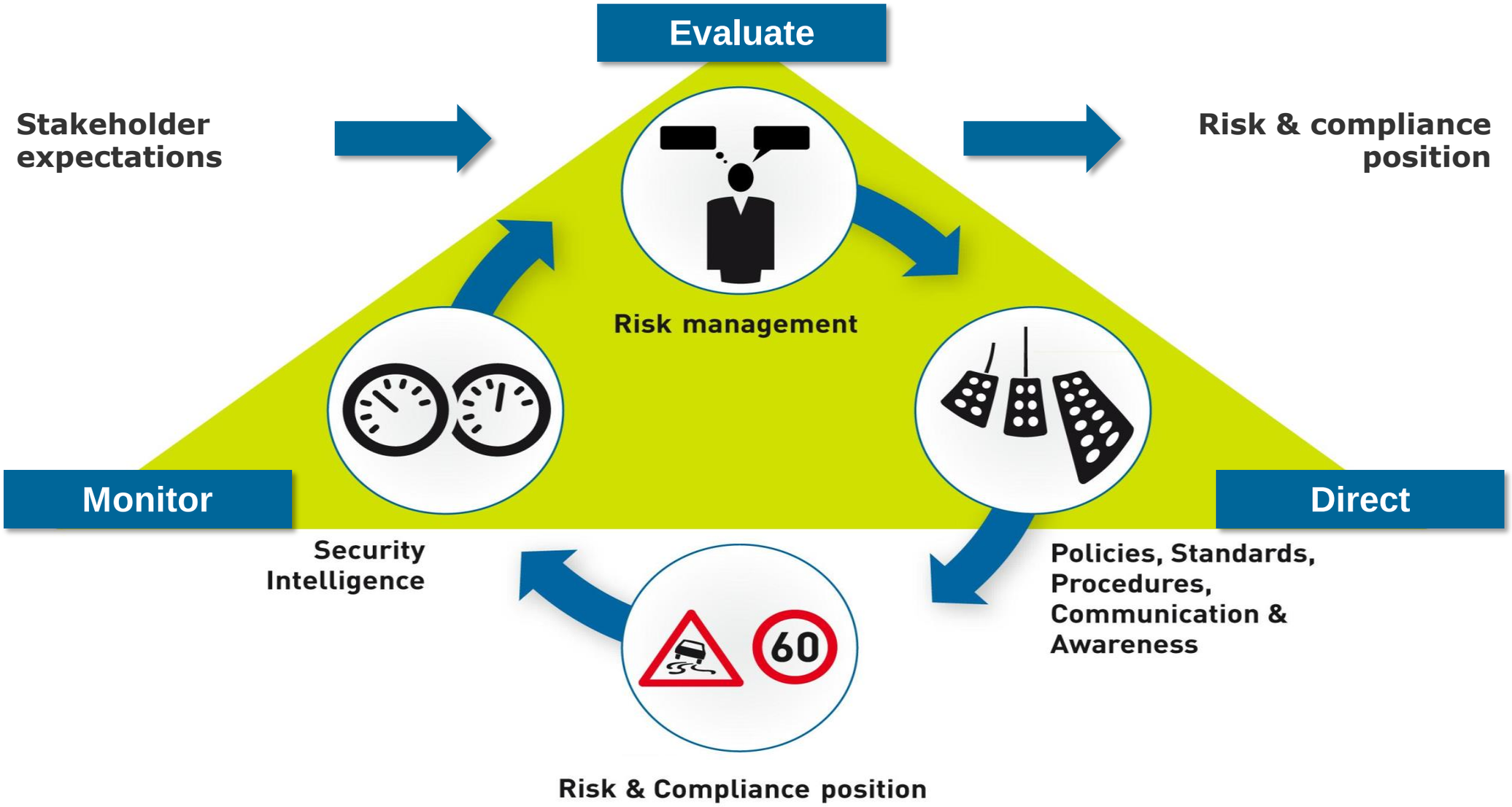
↓

Documentation, Reports

Agenda of todays lecture

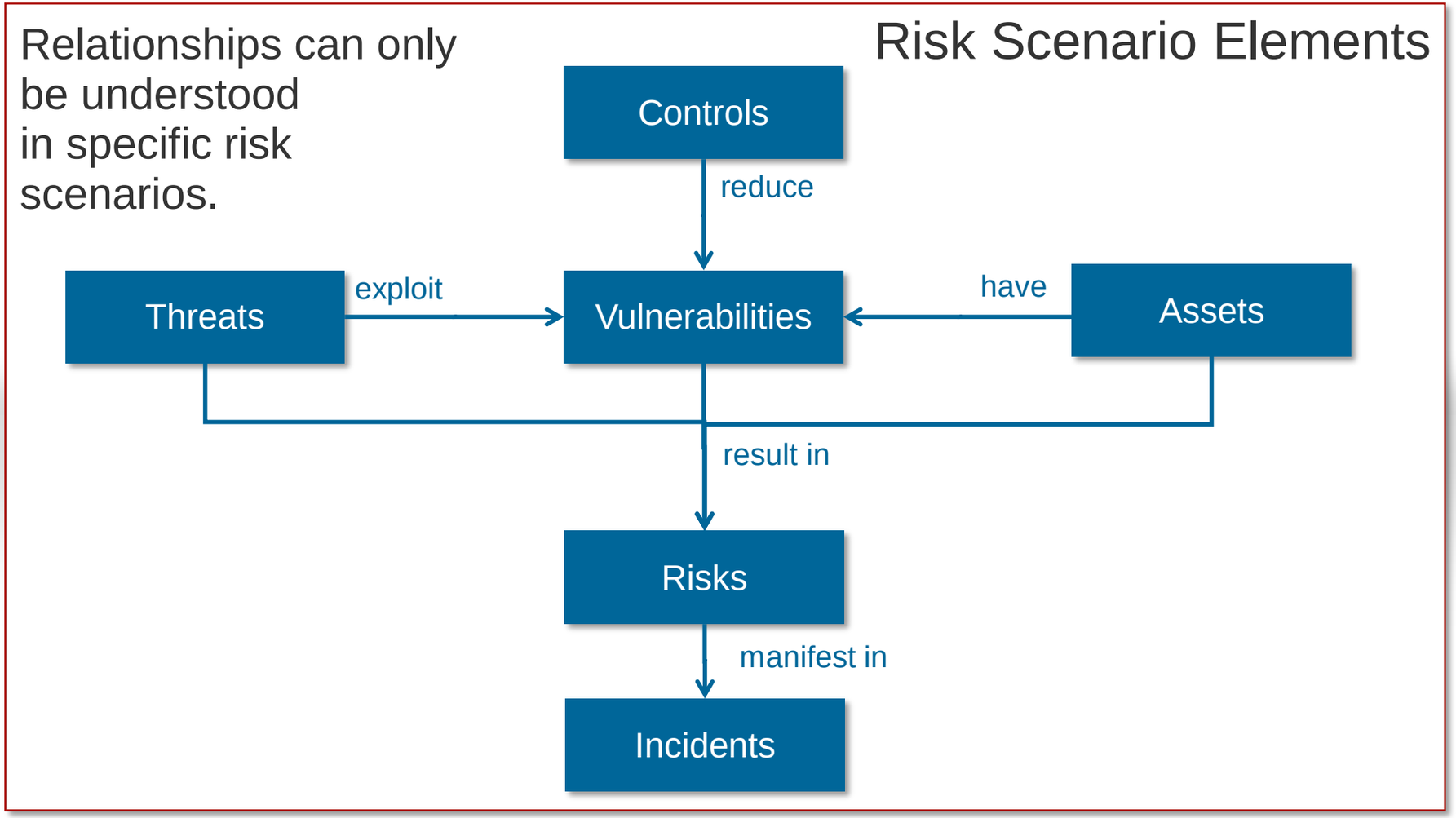
- Information Security Management System
- Plan - Information Security Risk Management
- Compliance and Data Protection (DSGVO)
- Direct - Information Security Policies and Controls
- **Monitor and Evaluate - Information Security Measurement: Security Intelligence KPIs (ISO 27004)**

No governance without KPIs
No KPIs without governance



KPIs must model the key causal relationships of the risk context

Relationships can only be understood in specific risk scenarios.

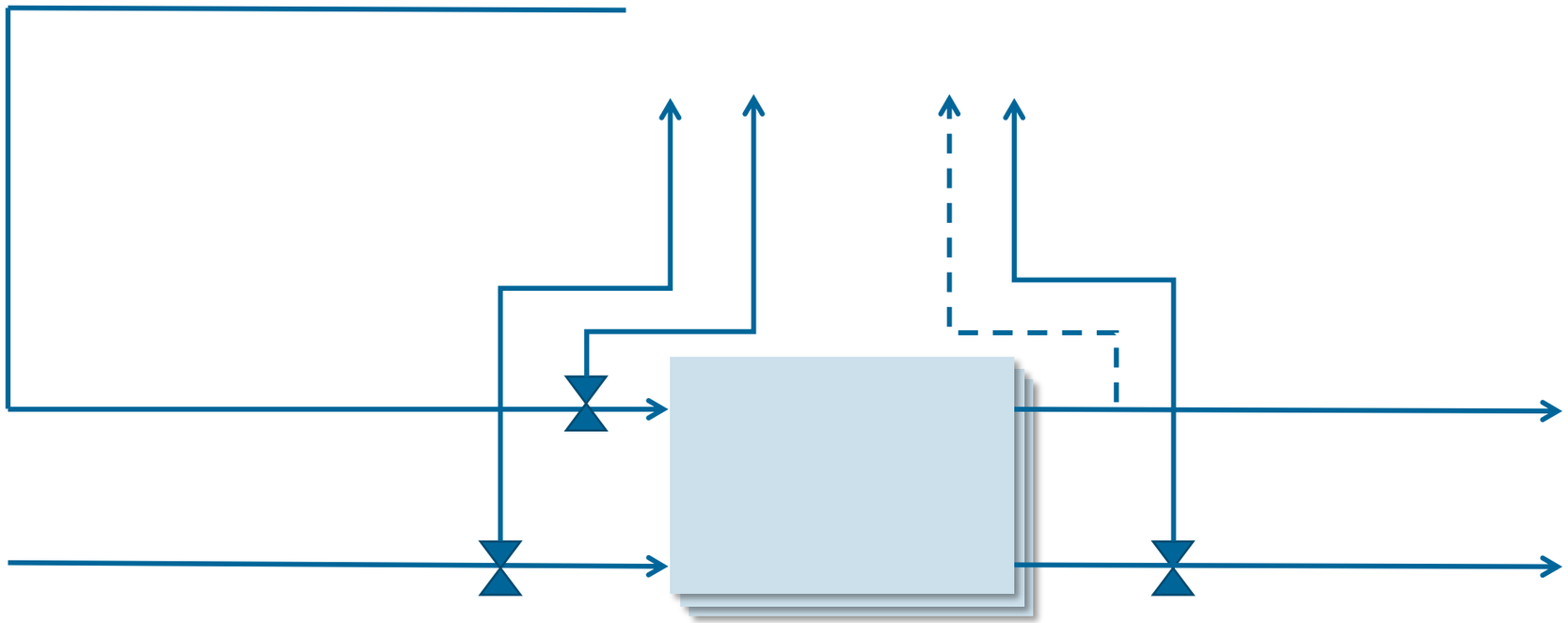


Example Risk Scenario

Risk scenario	Clients Malware Protection
Assets	▪ All client systems
Threats	▪ All types of malware (Virus, Spyware, etc.)
Potential impact	▪ Failure of client systems
Controls / Vulnerabilities	▪ People: Security awareness of employees ▪ Process: Patch management ▪ Technology: Endpoint protection software (Antivirus, HIPS)
Risks	▪ Insecure version of Internet Explorer rolled out can not be patched due to application dependency
Incidents	▪ Failure of a high number of clients due to virus infection

Controls-, threats-, risk-level and incidents should be on your scorecard

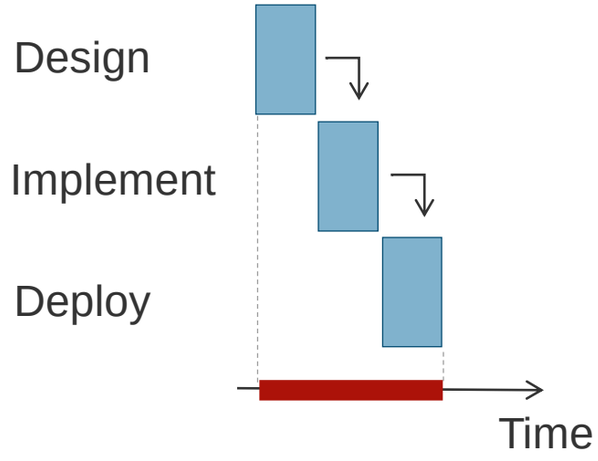
Measuring causes and effects enables you to understand, communicate and react to what is going on.



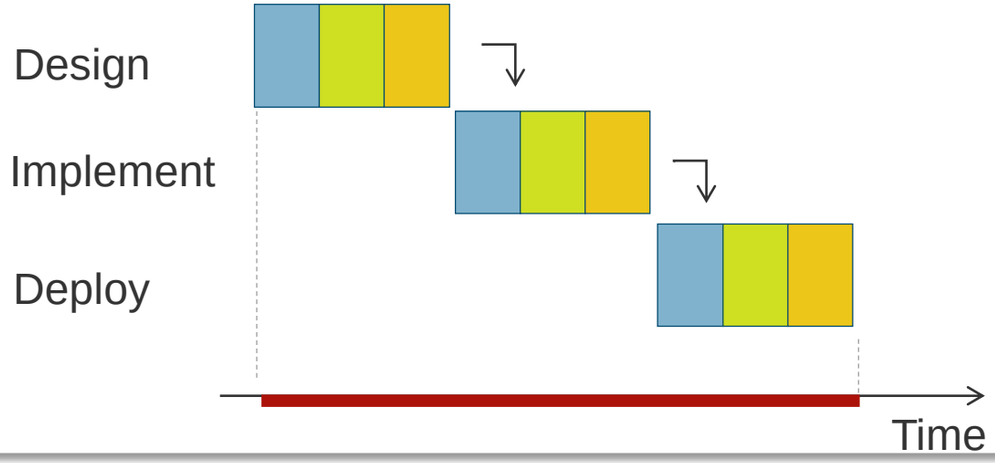
Example KPI

KPI	Amount of timely removed vulnerabilities	
Category	Coverage of the controls	
Control	Vulnerability Management Process	
Description	Ratio in percent of the amount of vulnerabilities, where the controls have been implemented successfully and the vuln. have been removed in time	
Berechnungs-schema	▪ X = A / B * 100 % ▪ A: Amount of Vuln. out of the set „B“, for which the desired controls are implemented ▪ B: Amount of Vuln. for which the given deadline for the control implementation is within the considered time frame	
Bewertungs-schema	Low Risk	KPI value = 100 % for Vulnerabilities of criticality High AND KPI value > 90 % for Vulnerabilities of criticality Medium
	Medium Risk	Prerequisites for low risk and high risk are not fulfilled
	High Risk	KPI value < 90 % for Vulnerabilities of criticality High OR KPI value < 75 % for Vulnerabilities of criticality Medium
Analysis dimensions	Time, Vulnerability criticality, Vulnerability responsibilities, Vulnerability controls	
Adressee	CISO	
Purpose	Ensure that vulnerabilities are removed in a given time	
Source systems	Vulnerability management databases	

Start with a focused scope capturing your key risk scenarios

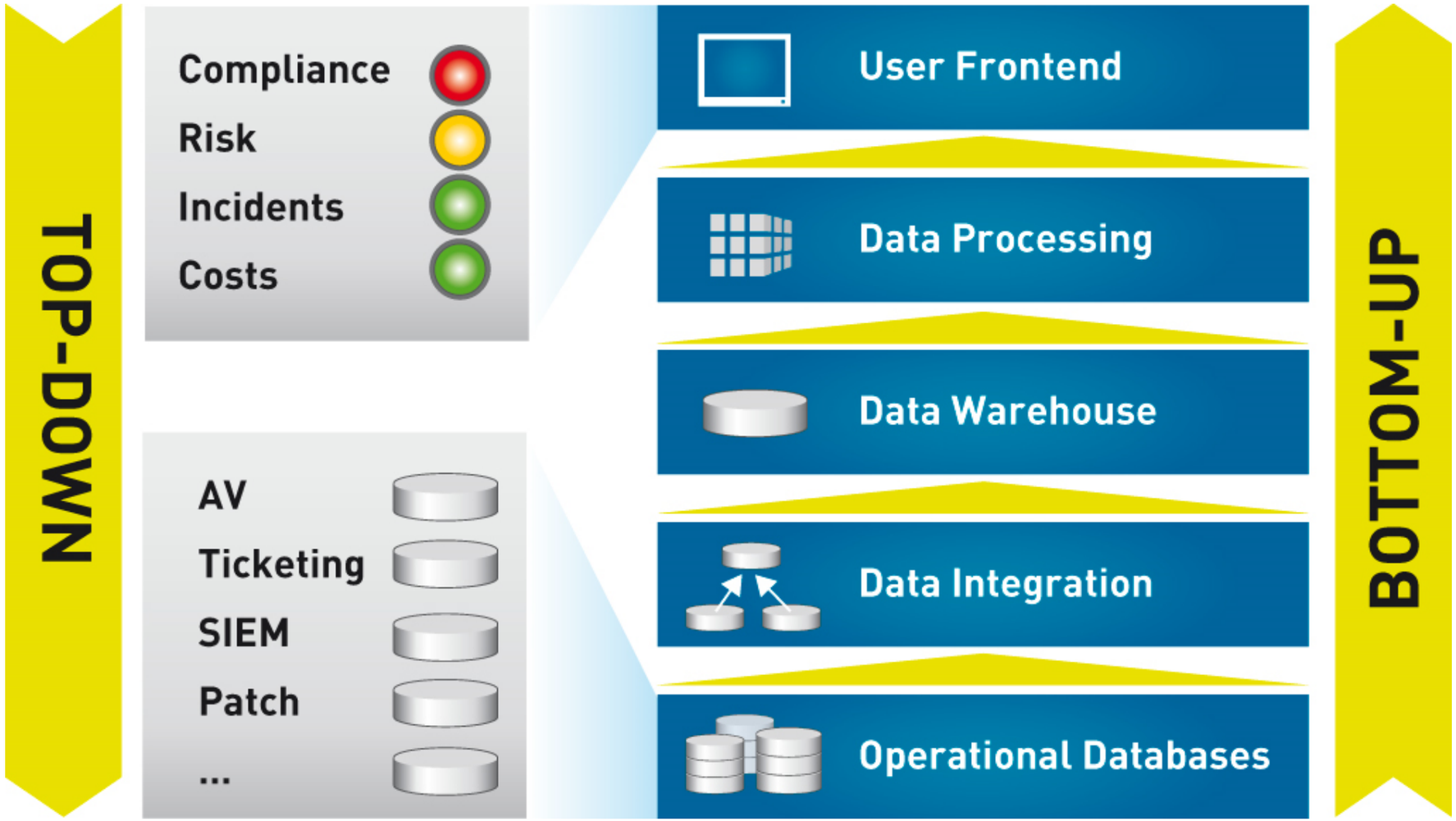


Smart approach
Early value delivery to stakeholders ensures support for future extensions in the smart approach



All-in-one approach
Without visible results you might loose support during the early phases of the all-in-one approach

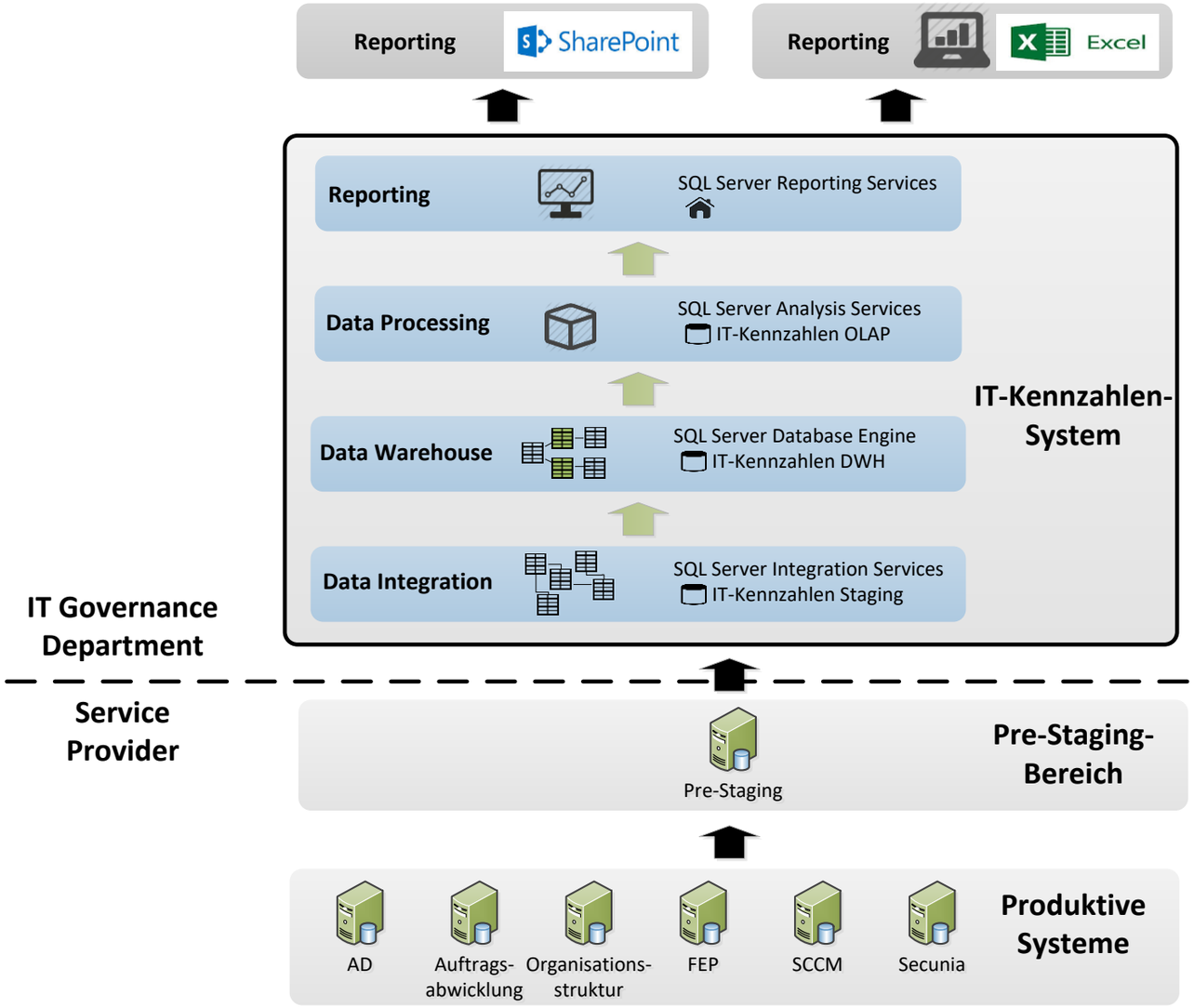
Combining top-down and bottom-up leads to meaningful and measurable KPIs



Case Study 1
Project Overview

- **Customer**
  - National Research Centre (Head of Information Security)
- **Goal: establish defined and well accepted KPIs for IT management**
  - Achieve common understanding between IT Governance, Service Provider and Customers
  - Take decisions based on facts
- **First realisation**
  - Risk scenario: malware protection
  - Project scope: definition of KPIs and implementation
  - Assets in scope for the implementation: clients
- **Extensions on other IT areas is planned (e.g. DMZ services, incident management)**

Case Study 1
System Architecture



Case Study 1
Management Cockpit

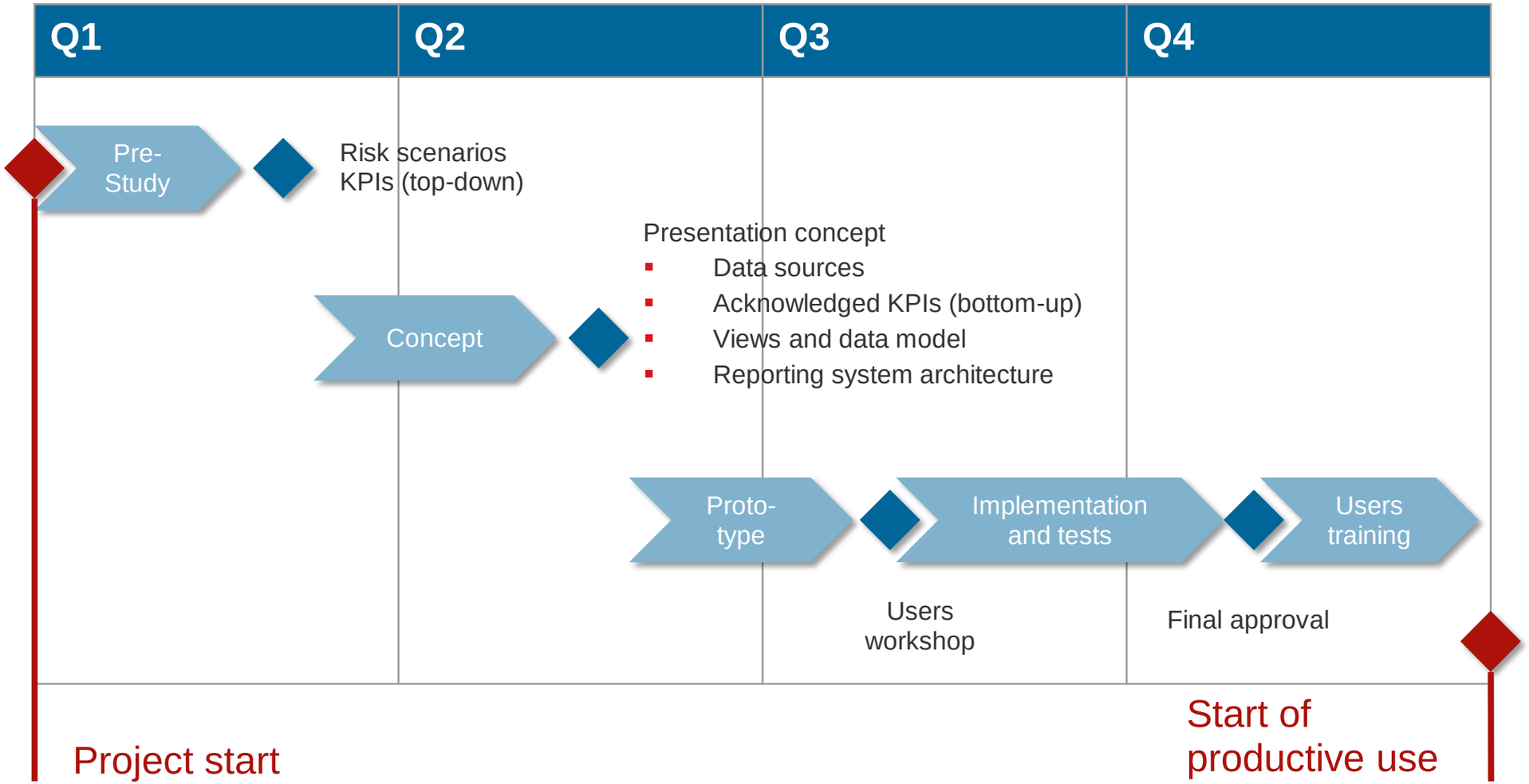
Windows 7 Sicherheit - Übersicht

	Wert	Status	Tendenz	Details
Umsetzungsgrad der Schutzmaßnahmen				
Anteil der Systeme mit konformer Antivirus-Software				Details
Anteil der Systeme mit aktuellem Patchstand				Details
IT-Sicherheitsvorfälle				
Anzahl der Schadcode-Vorfälle				Details
Abdeckungsgrad des Kennzahlensystems				
Anteil der betrachteten Systeme				

Detailed reports
- Per OU
- Per Software
- Per Client

Remark:
The KPI values are random

KPI Dashboard for selected scenarios is possible within an year



Information Security Governance - Summary

- **Information Security Management System is required**
  - Based on ISO 27001 / BSI
  - It is an IT-wide and company-wide activity
- **Recommended approach**
  - Combine top-down (risk management) and bottom-up (baseline and existing controls)
  - Clearly define responsibilities and verifications
  - Be committed to implement the controls
  - Management support is indispensable
  - Consider monitoring and evaluation from the beginning