How to Set Up Integrated Security Governance Processes

Thorsten Scheibel
DZ BANK

Lars Rudolff
Secaron AG

Session ID: GRC-208

Session Classification: Intermediate

RSACONFERENCE EUROPE 2012

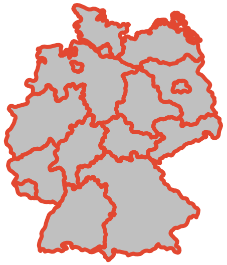
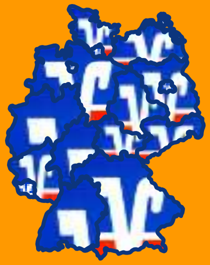
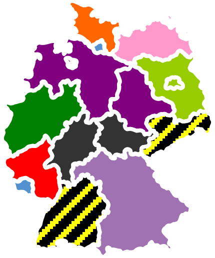
Agenda (Thorsten Scheibel)

- Introduction DZ BANK
- Integrated Security Governance Processes:
  Why do we need them?
- Corporate Security:
  What are the tasks and responsibilities?

Agenda (Lars Rudolff)

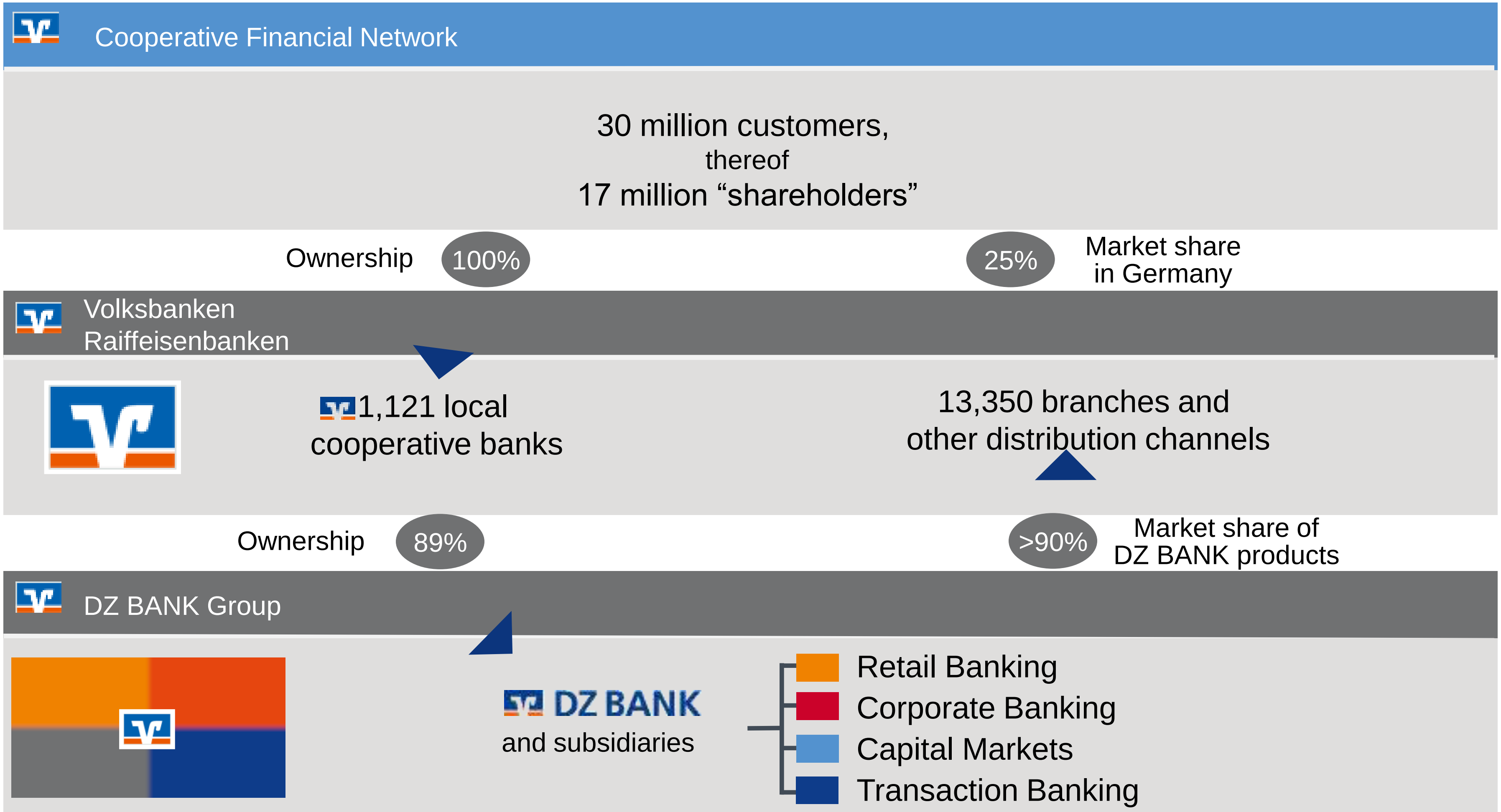
- Integration:
  How does it work?
- Success Factors:
  What needs to be considered?
- Summary:
  What did we learn from our project?
- Apply:
  What can you do after returing to your office?

The Three Pillars of the German Banking Sector

Regional focus			
Domestic market share*	<< 10% (each)	25%	38%
Banking sector	Private banking sector	Cooperative banking sector two central institutions: **DZ BANK Group** and WGZ BANK Group, 1,121 local coop. banks	Public banking sector 7 Landesbank groups (incl. DekaBank) 427 savings banks

* Market share according to deposits of private households end of 2011

German Cooperative Financial Network



Cooperative Financial Network

30 million customers,
thereof
17 million “shareholders”

Ownership 100%

25% Market share in Germany

Volksbanken Raiffeisenbanken

1,121 local cooperative banks

13,350 branches and other distribution channels

Ownership 89%

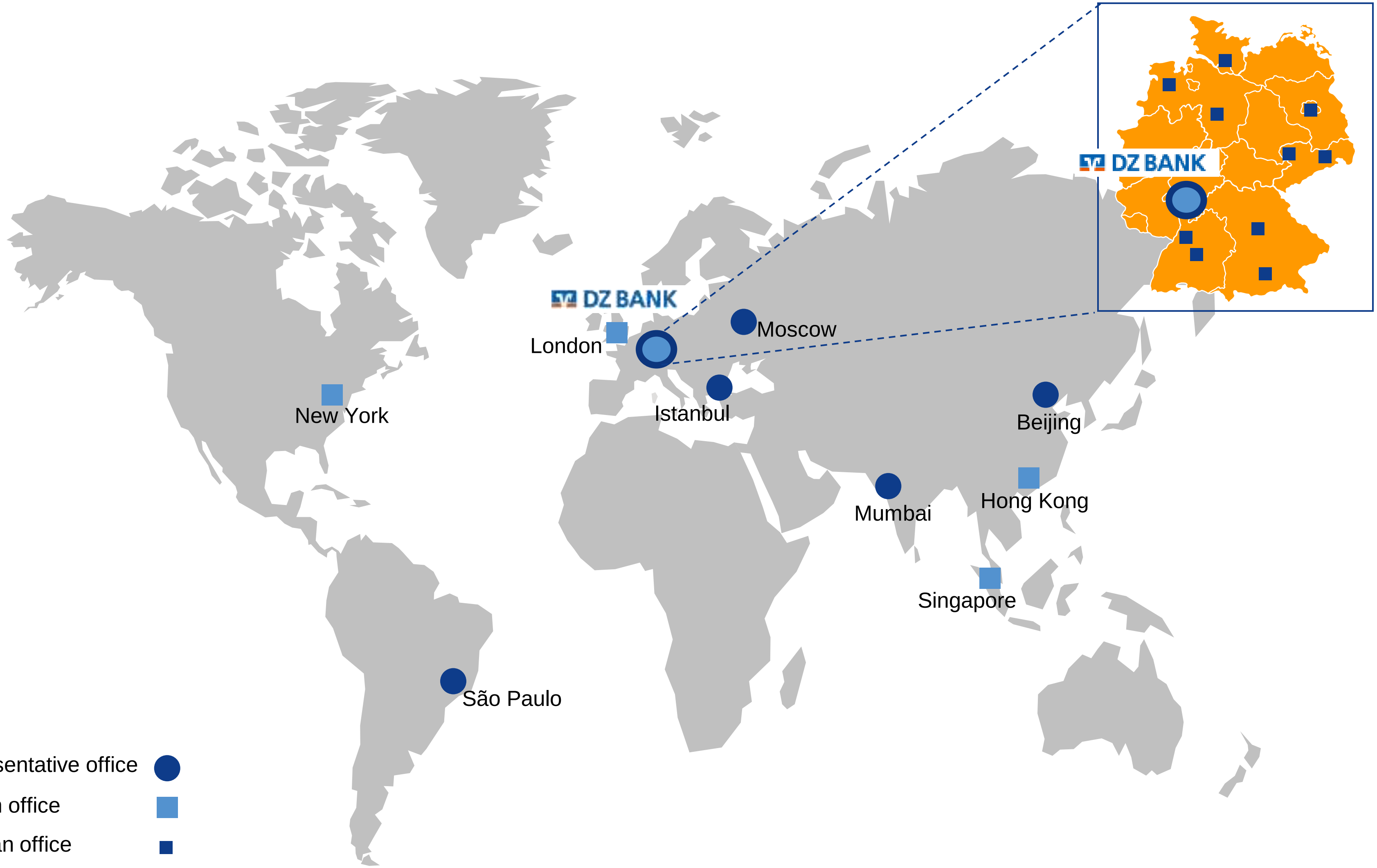
>90% Market share of DZ BANK products

DZ BANK Group

DZ BANK and subsidiaries

- 🟧 Retail Banking
- 🟥 Corporate Banking
- 🟦 Capital Markets
- 🟦 Transaction Banking

DZ BANK's Worldwide Presence - to Support Our Clients'Needs



Representative office ●

Branch office ■

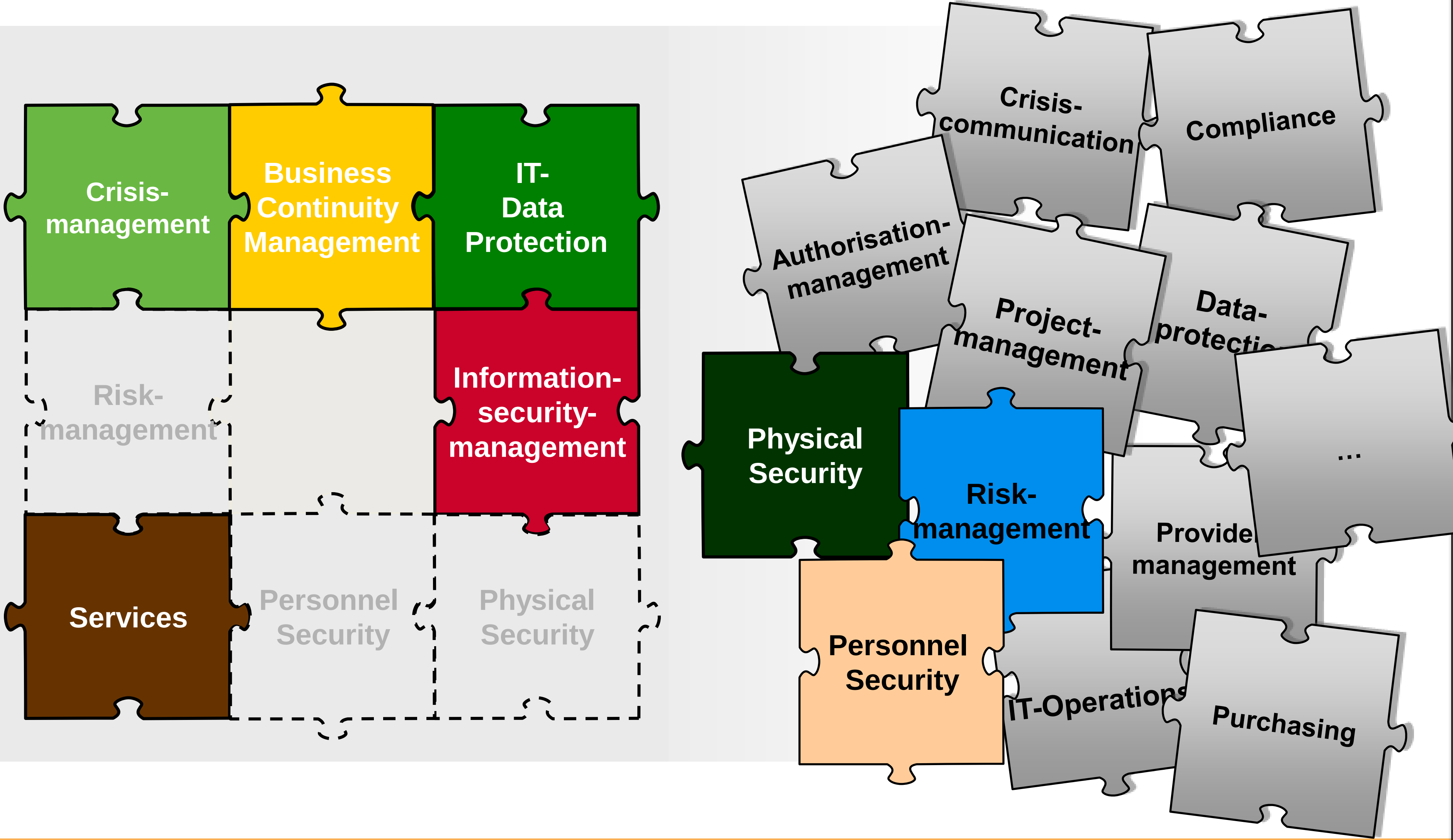
German office ▪

Integrated Security Governance Processes: Why do we need them?

Problems/Issues

- Many decentralized responsibilities
- Various security aspects clearly associated with an organizational unit
- Inconsistent use of terminology, definitions and documentation
- No main point of contact
- Different security aspects managed in different organizational units
- Redundancies or adjustment problems in terms of responsibilities and measures
- Overview of all security related issues not available

Overview of the Current Organization



DZ BANK

RSA CONFERENCE EUROPE 2012

Objectives

- Creating an appropriate corporate security department
- Alignment to business processes of DZ BANK
- Compliance with, for example, statutory or regulatory requirements
- Centralized controlling using Key Performance Indicators (KPIs)
- Developing an overall corporate security strategy
- Involvement of stakeholders

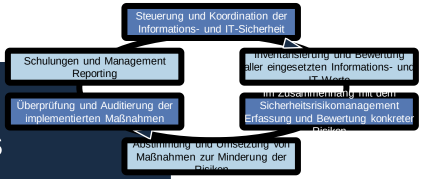
Step-by-Step Procedure

1. Inventory of processes, roles, responsibilities, documentation, plans and templates
2. Gap analysis
3. „Blueprint“
4. Identification and implementation of „quick wins“
5. Project roadmap
6. Definition of phases for implementation

General Conditions for Each Topic of Corporate Security

Policies and documentation

Processes



Steuerung und Koordination der Informations- und IT-Sicherheit

Inventarisierung und Bewertung aller eingesetzten Informations- und IT-Werte

im Zusammenhang mit dem Sicherheitsrisikomanagement Erfassung und Bewertung konkreter Risiken

Abstimmung und Umsetzung von Maßnahmen zur Minderung der Risiken

Überprüfung und Auditierung der implementierten Maßnahmen

Schulungen und Management Reporting

Interfaces

Role definition

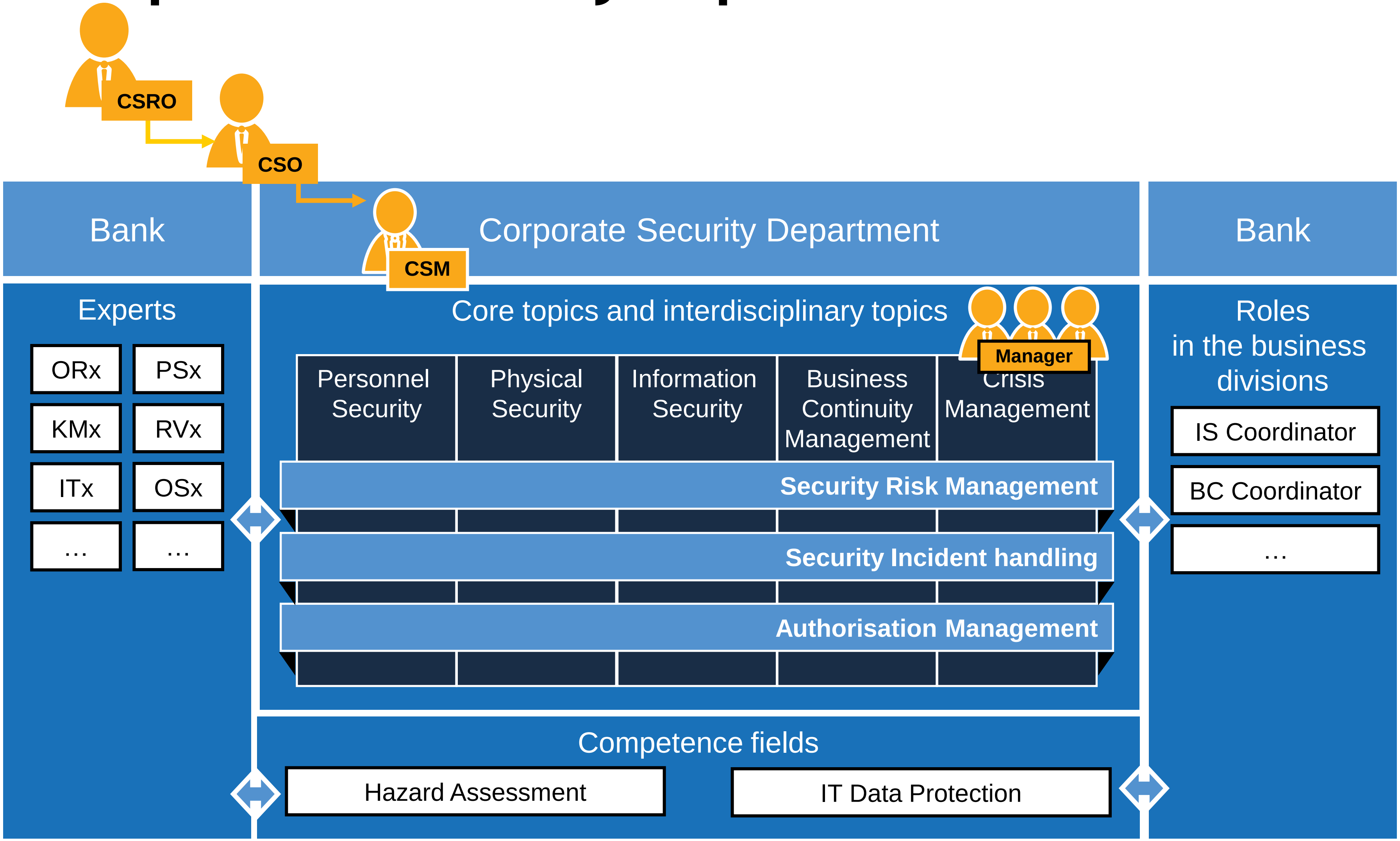
Measures

Roadmap

Categorization and prioritization of objectives for each action

Corporate Security: What are the tasks and responsibilities?

Corporate Security Topics



CSRO

CSO

CSM

Manager

Bank

Experts

ORx

PSx

KMx

RVx

ITx

OSx

…

…

Corporate Security Department

Core topics and interdisciplinary topics

Personnel Security

Physical Security

Information Security

Business Continuity Management

Crisis Management

Security Risk Management

Security Incident handling

Authorisation Management

Competence fields

Hazard Assessment

IT Data Protection

Bank

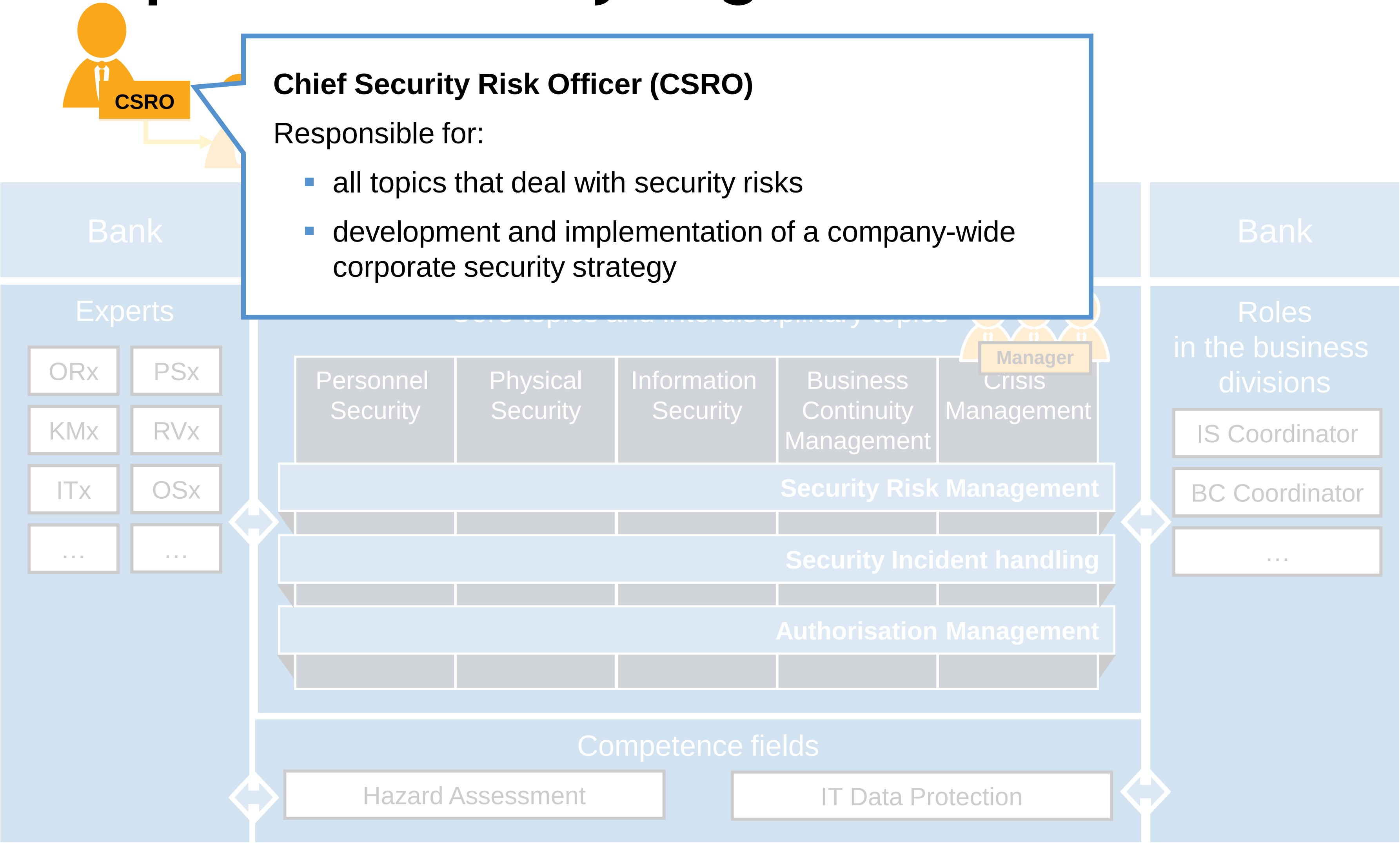
Roles in the business divisions

IS Coordinator

BC Coordinator

…

Corporate Security Organisation

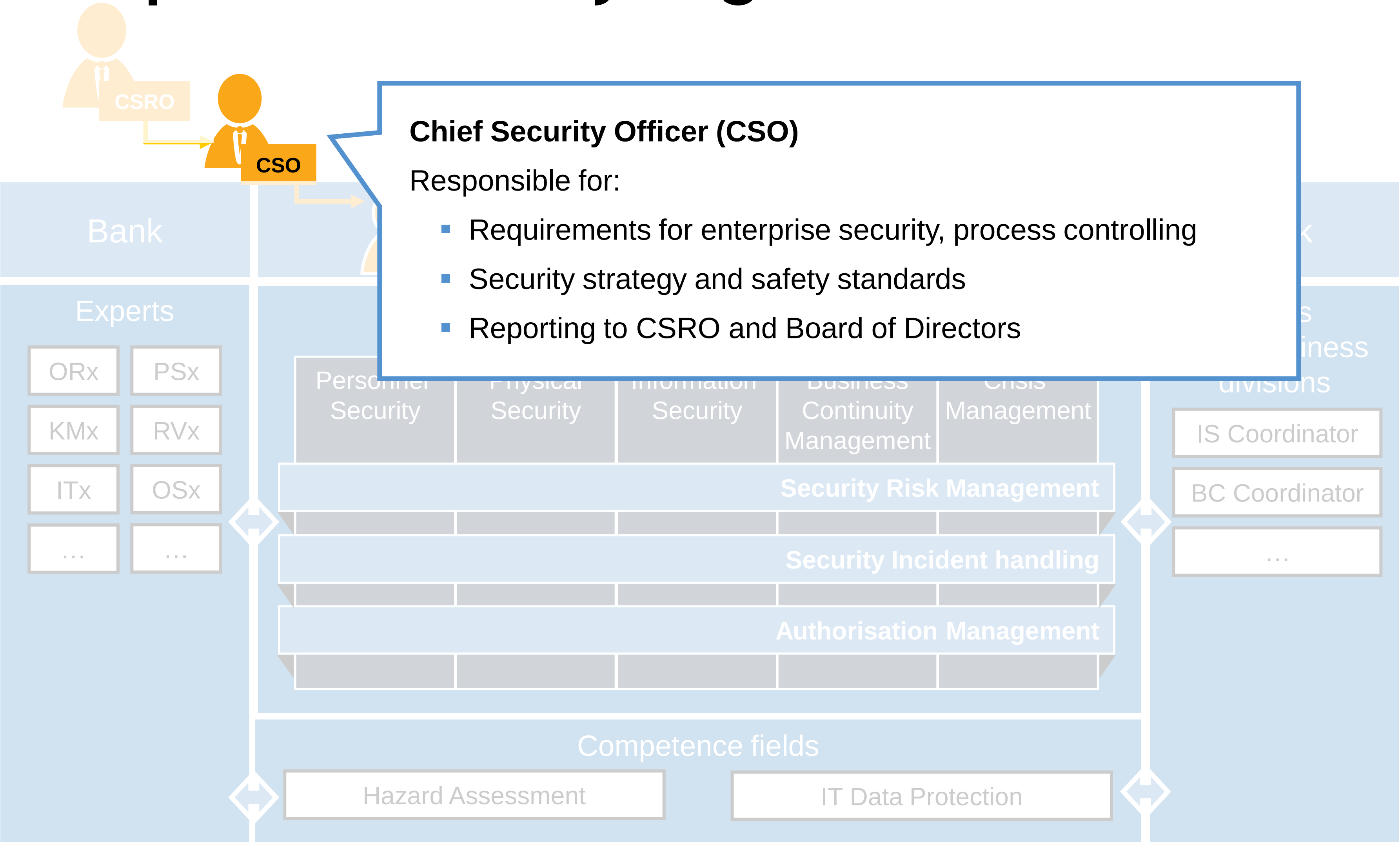


Chief Security Risk Officer (CSRO)

Responsible for:

- all topics that deal with security risks
- development and implementation of a company-wide corporate security strategy

Corporate Security Organisation



Chief Security Officer (CSO)

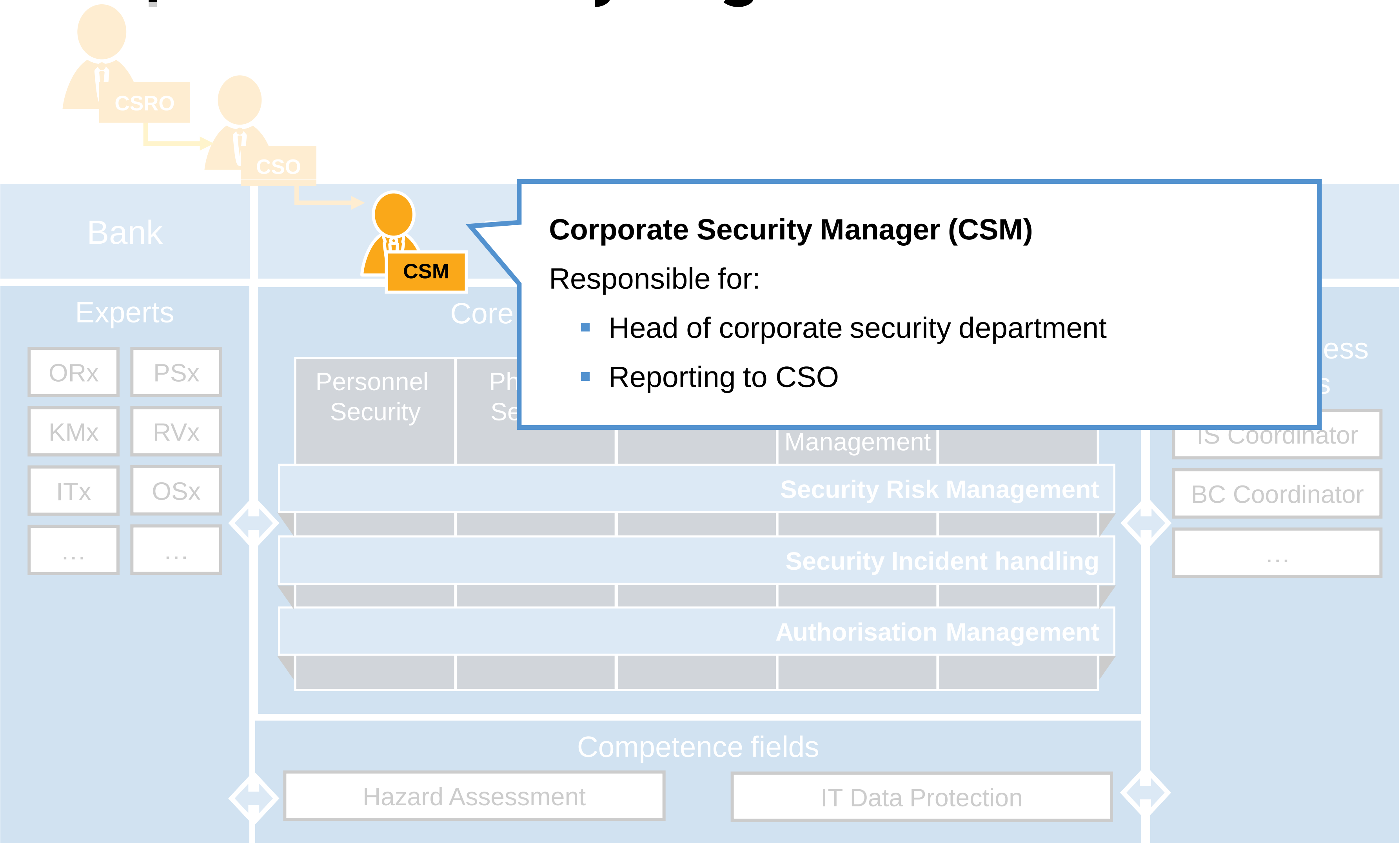
Responsible for:

- Requirements for enterprise security, process controlling
- Security strategy and safety standards
- Reporting to CSRO and Board of Directors

DZ BANK

RSA CONFERENCE EUROPE 2012

Corporate Security Organisation



CSRO

CSO

CSM

Bank

Experts

ORx PSx

KMx RVx

ITx OSx

… …

Core

Personnel Security

Ph Se

Management

Security Risk Management

Security Incident handling

Authorisation Management

ess s

IS Coordinator

BC Coordinator

…

Competence fields

Hazard Assessment

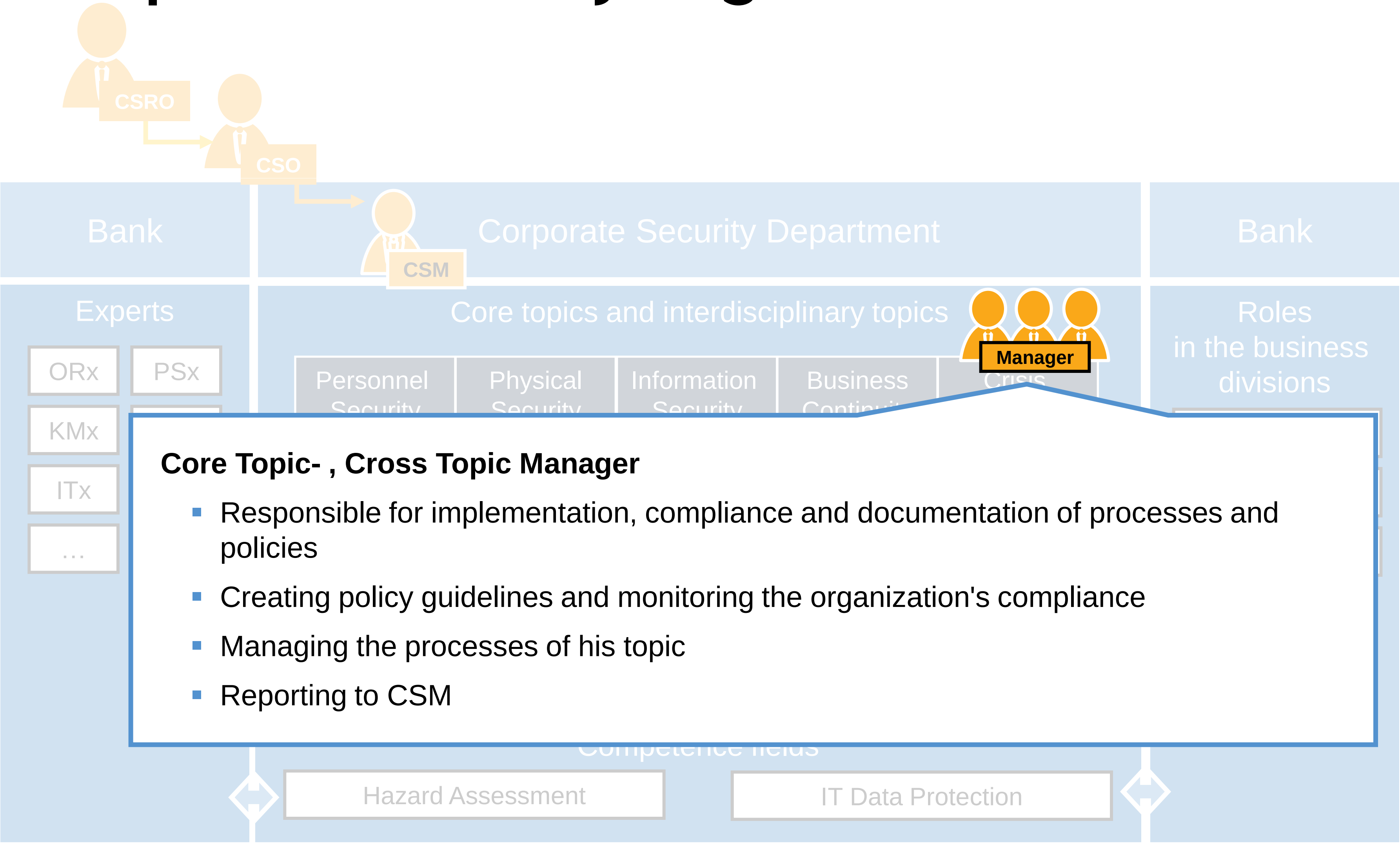
IT Data Protection

Corporate Security Manager (CSM)

Responsible for:

- Head of corporate security department
- Reporting to CSO

Corporate Security Organisation



CSRO

CSO

CSM

Bank

Corporate Security Department

Bank

Experts

ORx

PSx

KMx

ITx

…

Core topics and interdisciplinary topics

Manager

Personnel Security

Physical Security

Information Security

Business Continui

Crisis

Roles in the business divisions

Competence fields

Hazard Assessment

IT Data Protection

Core Topic- , Cross Topic Manager

- Responsible for implementation, compliance and documentation of processes and policies
- Creating policy guidelines and monitoring the organization's compliance
- Managing the processes of his topic
- Reporting to CSM

Tasks and Responsibilities

Physical & Personnel Security

- Identifying and analysing vulnerabilities
- Developing safeguard strategies
  - Physical security (measures e.g. for access control, video documentation)
  - HR security (measures e.g. for recruitment, business travel)
- Monitoring, maintaining and checking the security level

Information Security

- Preparing policy standards and guidelines for handling information and processing information in IT systems
  - Monitoring guideline compliance
  - Reporting to CSO on the current status for guideline compliance
  - Supporting projects in regard to information security management requirements

Tasks and Responsibilities

Business Continuity & Crisis Management

- Developing and improving suitable methods
- Advising and supporting the BC/crisis organisation
- Advising projects on BC-Management needs and requirements
- Requesting and checking the emergency plans within the financial conglomerate of the DZ BANK Group
- Participating / initiation of cross-divisional drills and tests, analysing and evaluating the results
- Reporting

Tasks and Responsibilities

Security Risk Management

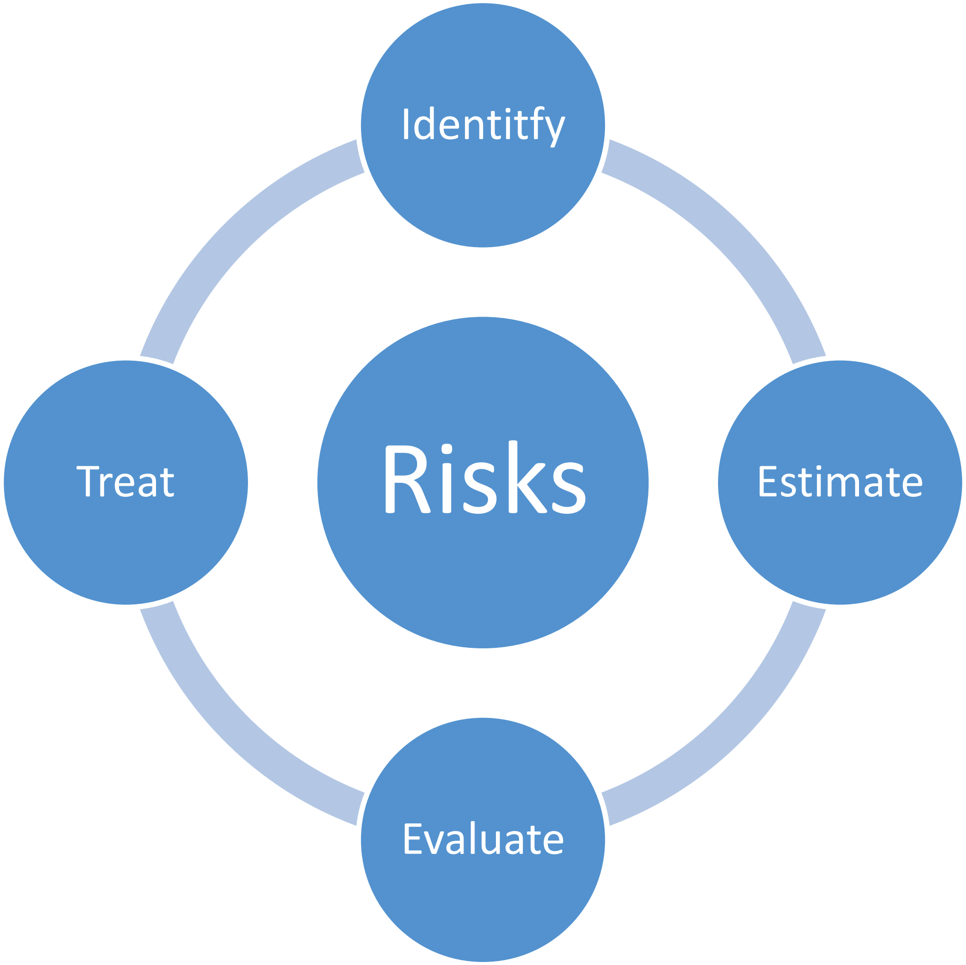
- Conducting security risk analyses
- Evaluating the security risk
- Recognising and evaluating cross-topical risk interdependencies
- Tracking of measures

Security Incident Handling

- Centralized, coordinated handling of security incidents
- Coordinating and checking measures for handling security incidents

Integration:
How does it work?

Security Risk Management - Central Management of the Integrated Processes



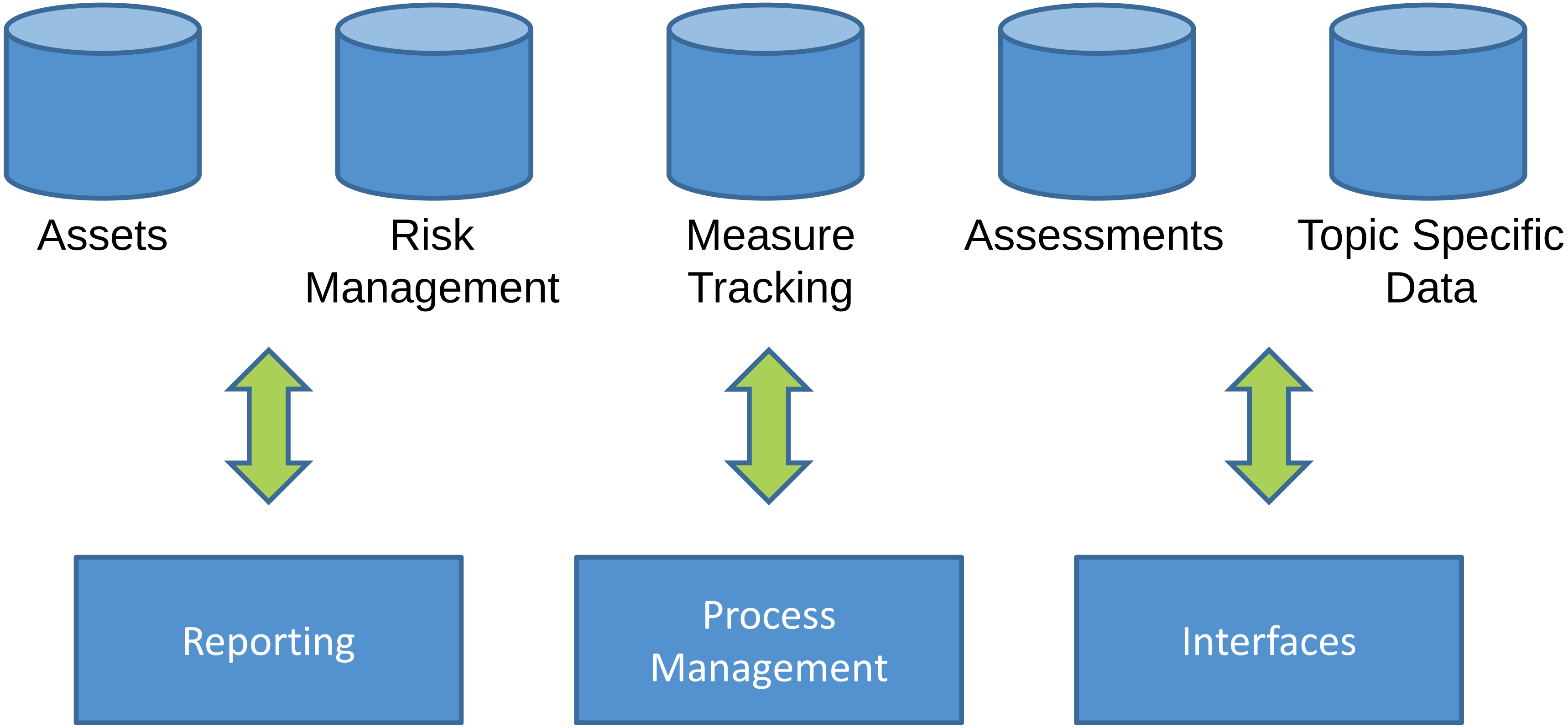
Centralized Services

- Definitions and infrastructure
  - Definition of consistent evaluation schemes and KPIs
  - Central asset repository for all core topics
- Management and reporting
  - Process management
  - Prioritization (risks and measures)
  - KPI
  - Management reports

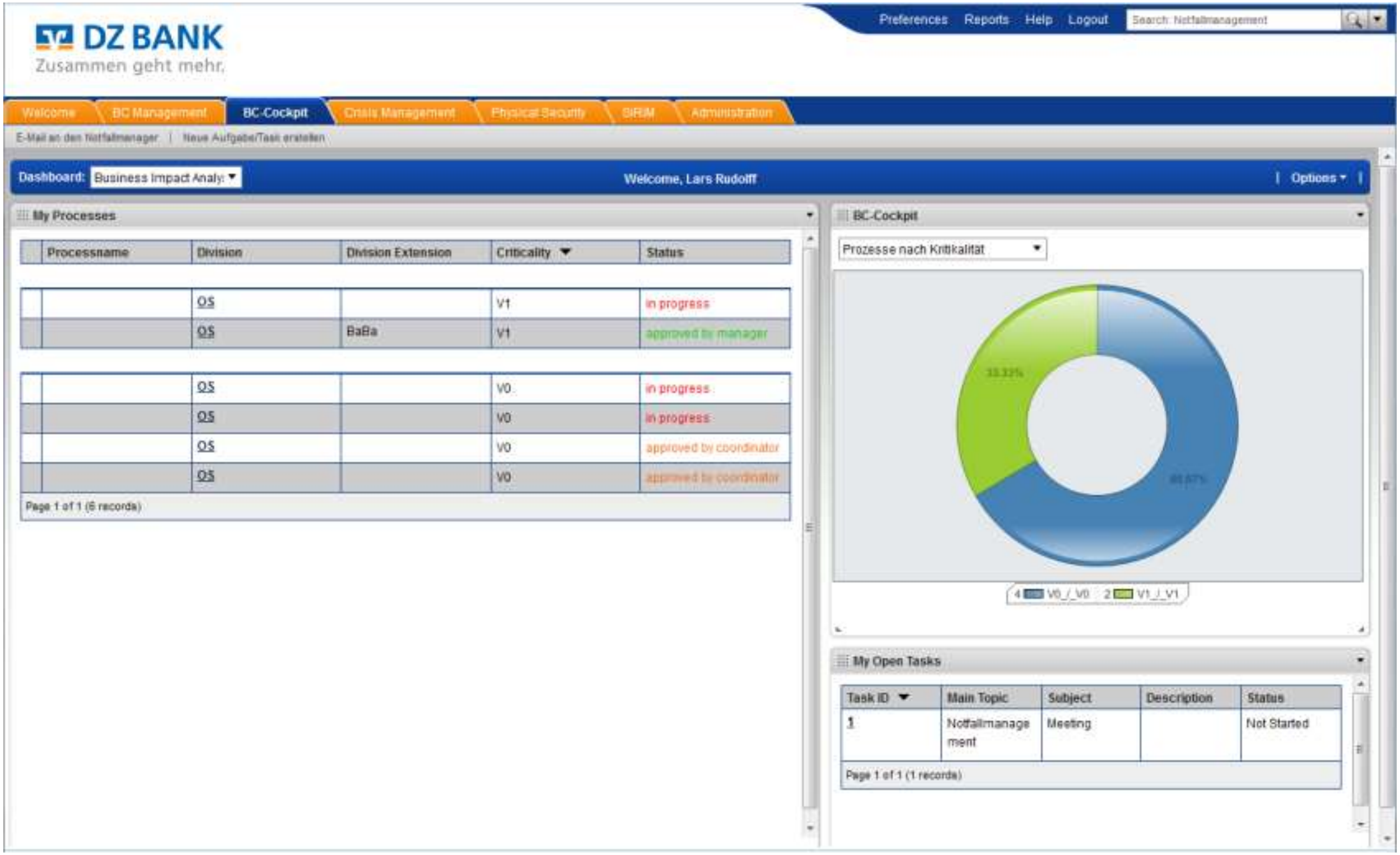
Shared Processes (Excerpt)

- Process Assessment
  - Business Impact Analysis (BCM)
  - Resource identification for other core topics
- Application Assessment
  - Vulnerabilities and risks within information security
  - Input for data protection
- Guidelines for facilities
  - Measures for physical security
  - Preparation for crisis events (BCM)

Centralized Data Management



Example: BC-Cockpit



Dashboard: Business Impact Analy: ▾

Welcome, Lars Rudolff

My Processes

Processname	Division	Division Extension	Criticality ▼	Status
	OS		V1	in progress
	OS	BaBa	V1	approved by manager
	OS		V0	in progress
	OS		V0	in progress
	OS		V0	approved by coordinator
	OS		V0	approved by coordinator

Page 1 of 1 (6 records)

BC-Cockpit

Prozesse nach Kritikalität ▾

My Open Tasks

Task ID ▼	Main Topic	Subject	Description	Status
1	Notfallmanagement	Meeting		Not Started

Page 1 of 1 (1 records)

Interfaces

- Technical interfaces for
  - Applications
  - Service Providers
  - Processes
  - Contacts
  - ...
- Process interfaces to
  - Enterprise Risk Management
  - Operation Risk Management
  - IT Risk and Compliance Management
  - ...

Benefits

Reduce Costs

- Centralize asset and data management
- Avoid gathering information multiple times
- Define measures that cover multiple core topics

Improve Quality

- Improve comparability through consistent evaluation schemes

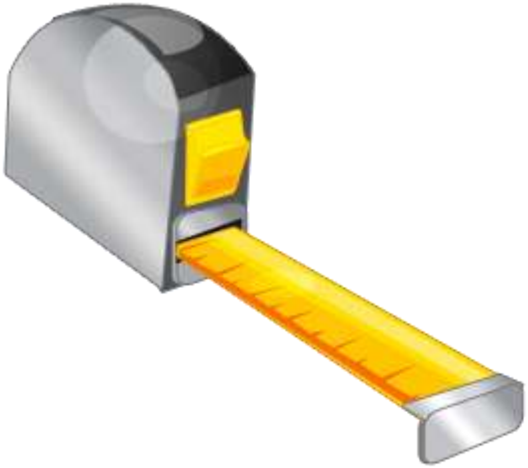
Strengthen Acceptance

- Link information to create a comprehensive picture
- Provide valuable data for various stakeholders with DZ BANK

Success Factors: What needs to be considered?

Evaluation and Reporting

- Define consistent evaluation schemes
- Select significant PKIs considering
    - Objectives
    - All core topics
    - Achievable thresholds
- Report what your management is interested in



Tool Support

- Select a tool that
  - supports your processes
  - automates as much as possible
  - contains an easy-to-use reporting engine
  - protects your critical data using a state-of-the-art authorization concept

Roll-Out

- Don‘t forget to...
  - ... ask your management for support
  - ... test everything before you roll it out
  - ... talk to all the stakeholders beforehand

Summary:
What did we learn from our project?

Summary

Approach

- One size fits all? - There is no „blueprint“ working in every company
- Don‘t reinvent the wheel! Reuse existing processes and procedures
- Avoid mistakes others already made! - Benefit from external experience

Challenges & Benefit

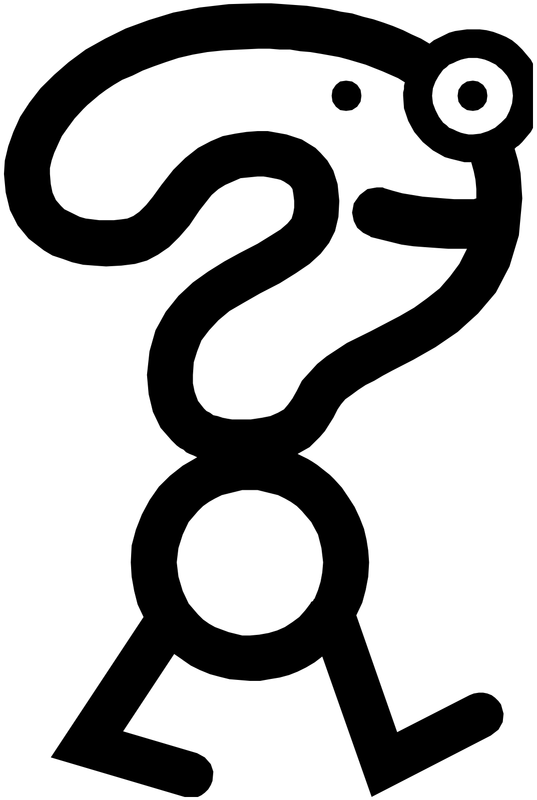
- Manage change
- Emphasize the benefit when talking to stakeholders
- It’s a hard way to go but it’s worth it!

Apply: What can you do after returning to your office?

3 Specific Actions

1. Identify governance processes in or around your area of responsibility
2. Think about whether...
   - ... similar information is gathered multiple times
   - ... the same contacts are interviewed multiple times
   - ... it would make sense to share information
   - ... some routine tasks can be automated
3. Talk to the other managers about integrating their and your governance processes

Any Questions or Comments Right Now?



Any Questions or Comments Later On?

- Please do not hesitate to contact us:
  - Thorsten.Scheibel@dzbank.de
  - Rudolff@secaron.de