How to Set Up Integrated Security Governance Processes

Thorsten Scheibel
DZ BANK

Lars Rudolff
Secaron AG
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 returning to your office?
The Three Pillars of the German Banking Sector

### Regional focus
- **Domestic market share***: << 10% (each)
- **Banking sector**: Private banking sector

### Public banking sector
- **25%**
- 7 Landesbank groups (incl. DekaBank)
- 427 savings banks

### Cooperative banking sector
- **25%**
- Two central institutions: DZ BANK Group and WGZ BANK Group, 1,121 local coop. banks

### Private banking sector
- **38%**

*Market share according to deposits of private households end of 2011*
German Cooperative Financial Network

Ownership: 100%

Volksbanken Raiffeisenbanken
- 1,121 local cooperative banks

Market share of DZ BANK products: >90%

DZ BANK Group
- Retail Banking
- Corporate Banking
- Capital Markets
- Transaction Banking
DZ BANK’s Worldwide Presence - to Support Our Clients’ Needs
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

- Crisis-management
- Business Continuity Management
- IT-Data Protection
- Information-security-management
- Physical Security
- Personnel Security
- Physical Security
- Risk-management
- Authorisation-management
- Project-management
- Data-protection
- Provide management
- IT-Operations
- Purchasing
- Compliance
- Crisis-communication

DZ BANK
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**
  - Interfaces
  - Role definition

- **Processes**
  - Role definition
  - Processes

- **Measures**
  - Categorization and prioritization of objectives for each action

**Roadmap**

- **Categorization and prioritization of objectives for each action**
Corporate Security: What are the tasks and responsibilities?
Corporate Security Topics

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

Roles in the business divisions
- IS Coordinator
- BC Coordinator
- ...

Experts
- ORx
- PSx
- KMx
- RVx
- ITx
- OSx
- ...

Corporate Security Department

Bank

CSRO
CSO
CSM
Manager

DZ BANK
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

Competence fields
- Hazard Assessment
- IT Data Protection

Bank

Experts
- ORx
- PSx
- KMx
- RVx
- ITx
- OSx

IS Coordinator
BC Coordinator

Core topics and interdisciplinary topics
Personnel Security
Physical Security
Information Security
Business Continuity Management
Crisis Management
Security Risk Management
Security Incident handling
Authorisation Management

IT Data Protection
Hazard Assessment

Bank Corporate Security Department

CSRO
CSO
CSM
Manager
Chief

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

Corporate Security Manager (CSM)
Responsible for:
- Head of corporate security department
- Reporting to CSO
## Corporate Security Organisation

<table>
<thead>
<tr>
<th>Bank</th>
<th>Corporate Security Department</th>
<th>Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experts</td>
<td>Core topics and interdisciplinary topics</td>
<td>Roles in the business divisions</td>
</tr>
<tr>
<td>ORx</td>
<td>PSx</td>
<td></td>
</tr>
<tr>
<td>KMx</td>
<td>ITx</td>
<td></td>
</tr>
<tr>
<td>…</td>
<td>…</td>
<td>…</td>
</tr>
</tbody>
</table>

### 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

Competence fields:
- Hazard Assessment
- IT Data Protection

Manager

**Corporate Security Department**

**IS Coordinator**
**BC Coordinator**

**Bank Corporate Security Department**

**CSRO**
**CSO**
**CSM**

Manager

**Core topics and interdisciplinary topics**

- Personnel Security
- Physical Security
- Information Security
- Business Continuity
- …

**ITx**
**OSx**
# Tasks and Responsibilities

<table>
<thead>
<tr>
<th>Physical &amp; Personnel Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Identifying and analysing vulnerabilities</td>
</tr>
<tr>
<td>- Developing safeguard strategies</td>
</tr>
<tr>
<td>- Physical security (measures e.g. for access control, video documentation)</td>
</tr>
<tr>
<td>- HR security (measures e.g. for recruitment, business travel)</td>
</tr>
<tr>
<td>- Monitoring, maintaining and checking the security level</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Preparing policy standards and guidelines for handling information and processing information in IT systems</td>
</tr>
<tr>
<td>- Monitoring guideline compliance</td>
</tr>
<tr>
<td>- Reporting to CSO on the current status for guideline compliance</td>
</tr>
<tr>
<td>- Supporting projects in regard to information security management requirements</td>
</tr>
</tbody>
</table>
## 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?

- Identify
- Estimate
- Evaluate
- Treat

Risks
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

- Assets
- Risk Management
- Measure Tracking
- Assessments
- Topic Specific Data

- Reporting
- Process Management
- Interfaces
Example: BC-Cockpit
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