

# Security & Compliance Challenges

Automate ISMS, BCM and ICS  
with RSA/Archer

Use Case: Business Resiliency

# About the Speaker.

- Thorsten Scheibel
- AMBCI
- DZ BANK AG
- Business Continuity & Crisis Manager
- 6 years GRC Experience



# About the Speaker.

- Lars Rudolff
- Management Consultant
- TÜV Rheinland i-sec GmbH
- Information Security/  
Risk Management
- Many Customer Projects  
with RSA Archer



# Agenda.

## Presentation DZ BANK/TÜV Rheinland

Initial Situation

Project Procedure

ICS Implementation

BCM Implementation

ISMS Implementation

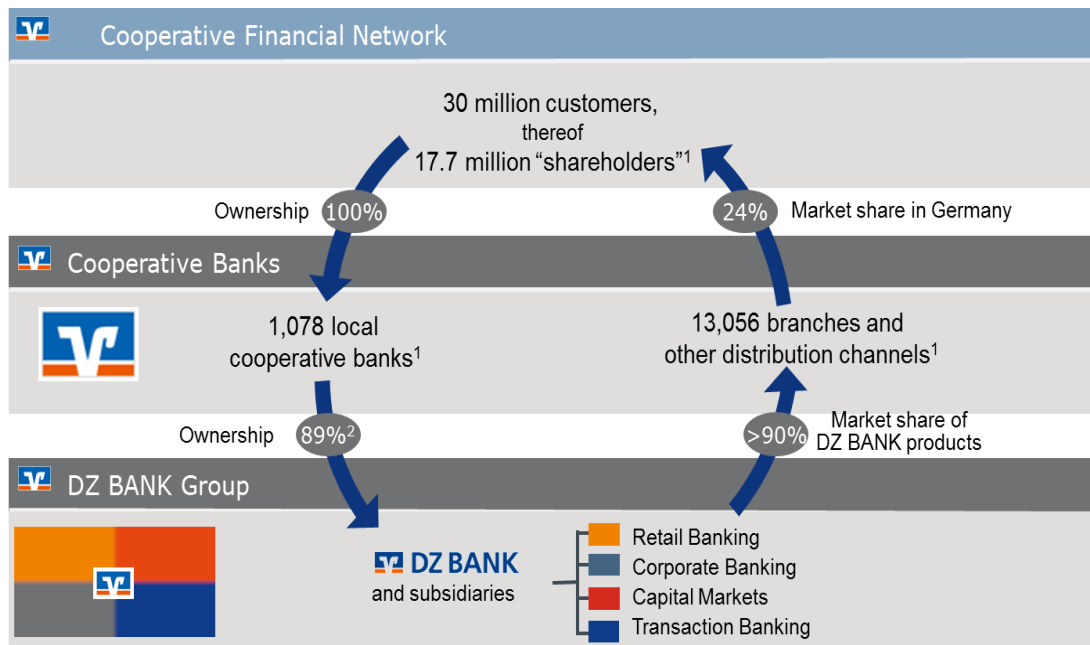
Outlook



- BANK
- ISO 22301 certified
- 4.000 Employees
- 3 years an RSA Archer customer

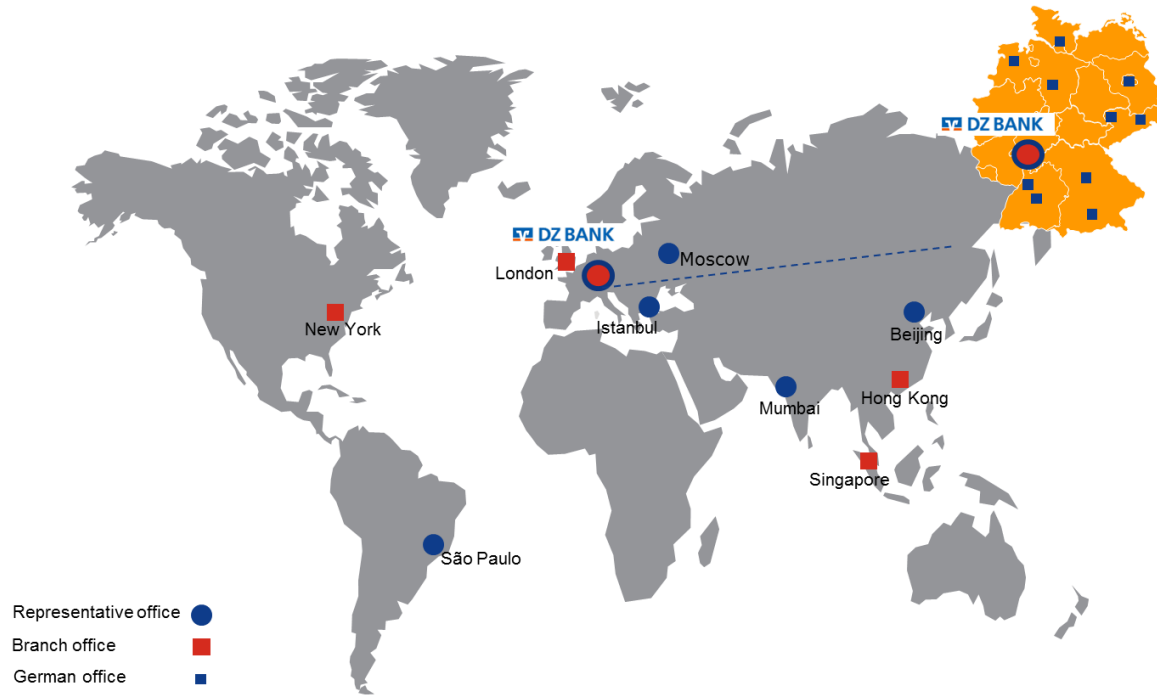
# Cooperative Financial Network.

Interaction  
within  
Germany



<sup>1</sup> 31.12.2013 according to the National Association of German Cooperative Banks, BVR; <sup>2</sup> Including indirect and direct participations

# DZ BANK's worldwide presence.



# TÜV Rheinland.

Your partner for Cyber SecurITy.

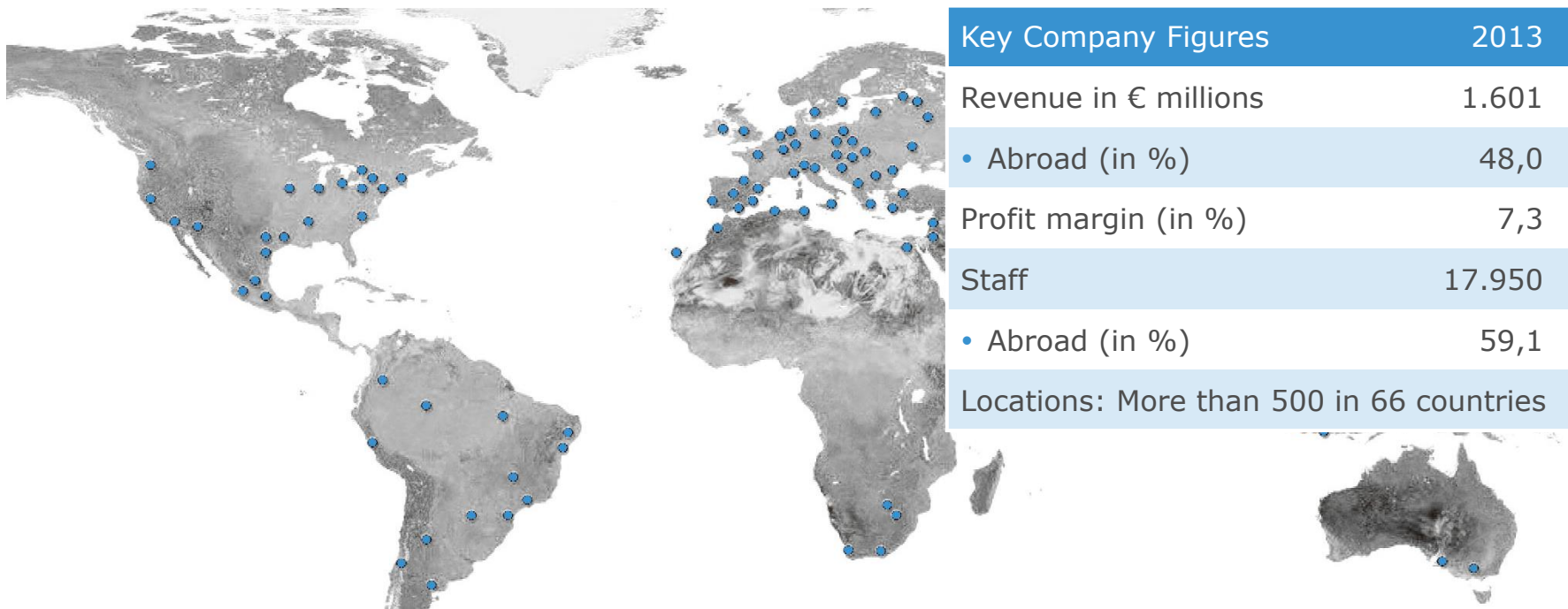


EMC<sup>2</sup>

RSA



# Present on all continents.



## Key Company Figures 2013

Revenue in € millions 1.601

• Abroad (in %) 48,0

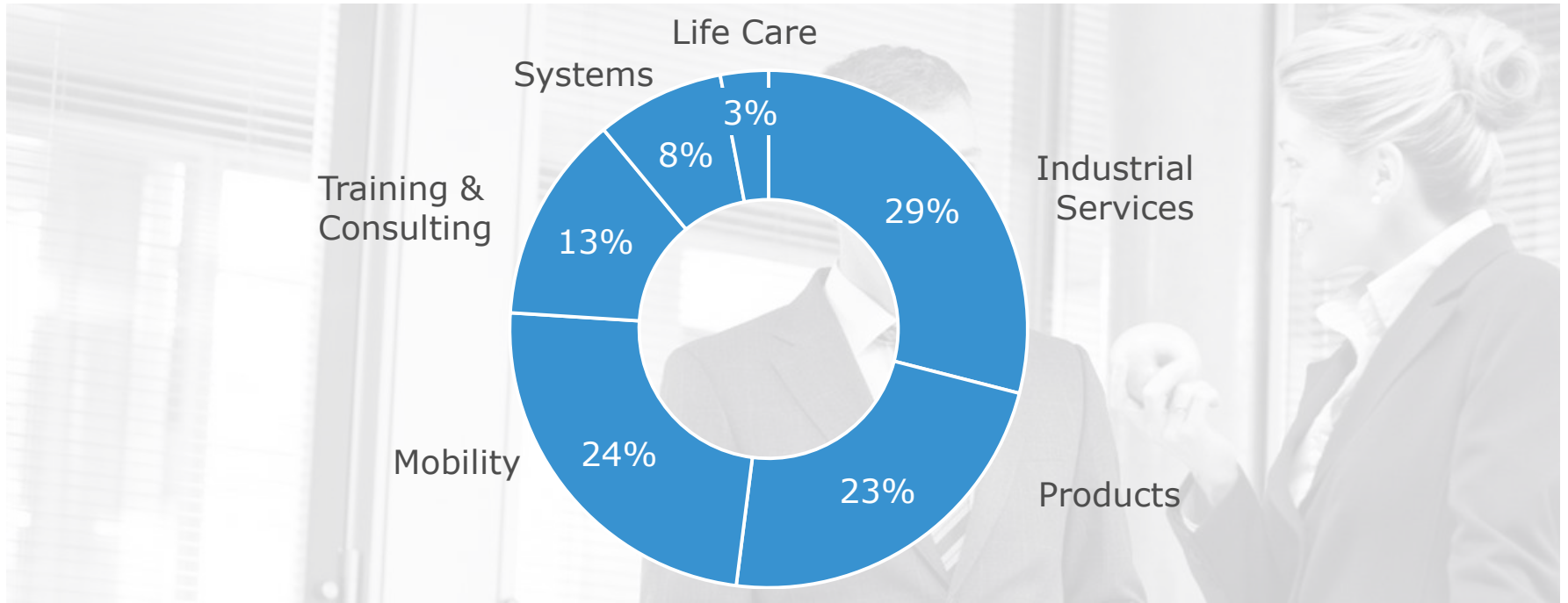
Profit margin (in %) 7,3

Staff 17.950

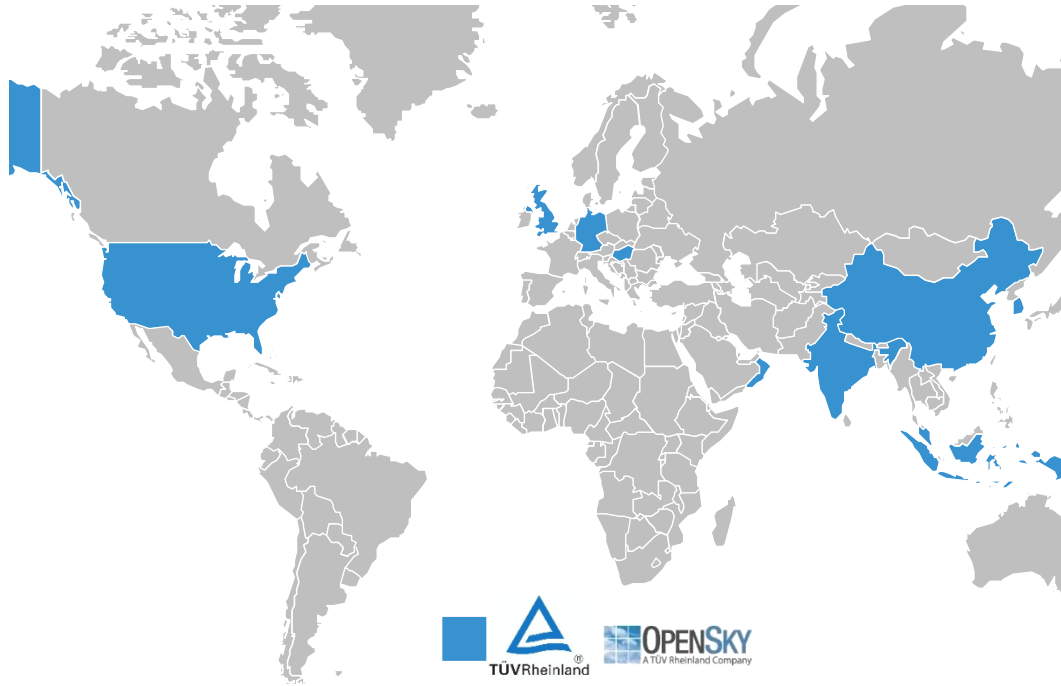
• Abroad (in %) 59,1

Locations: More than 500 in 66 countries

# Revenue share by business segment.



# World of ICT Services.



Revenue 2014: approx. 155 Mio. €

## ICT & Consulting Service Portfolio

- Cyber Security
- IT Infrastructure Services
- Management Consulting
- Business Engineering Services
- R&D Management
- Telco Service Solutions

## IT Training

- Professional Training Solutions



# Agenda.

Presentation DZ BANK/TÜV Rheinland

Initial Situation

Project Procedure

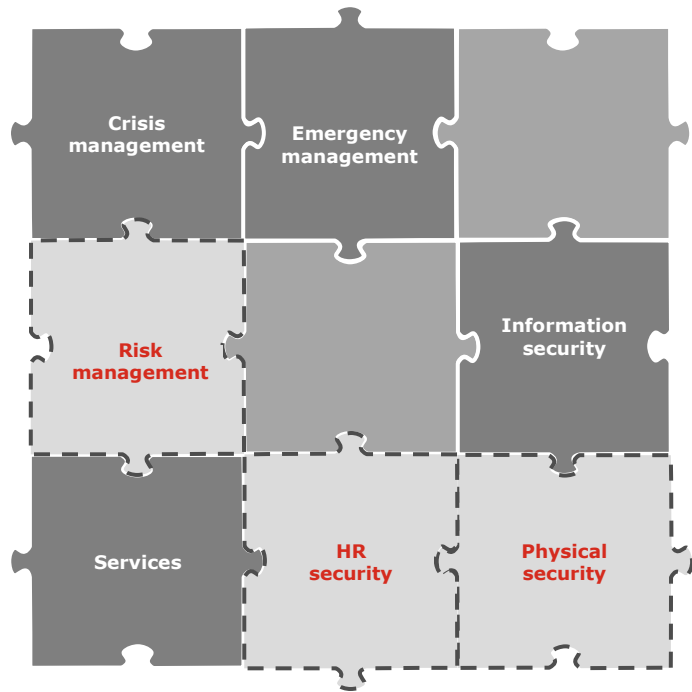
ICS Implementation

BCM Implementation

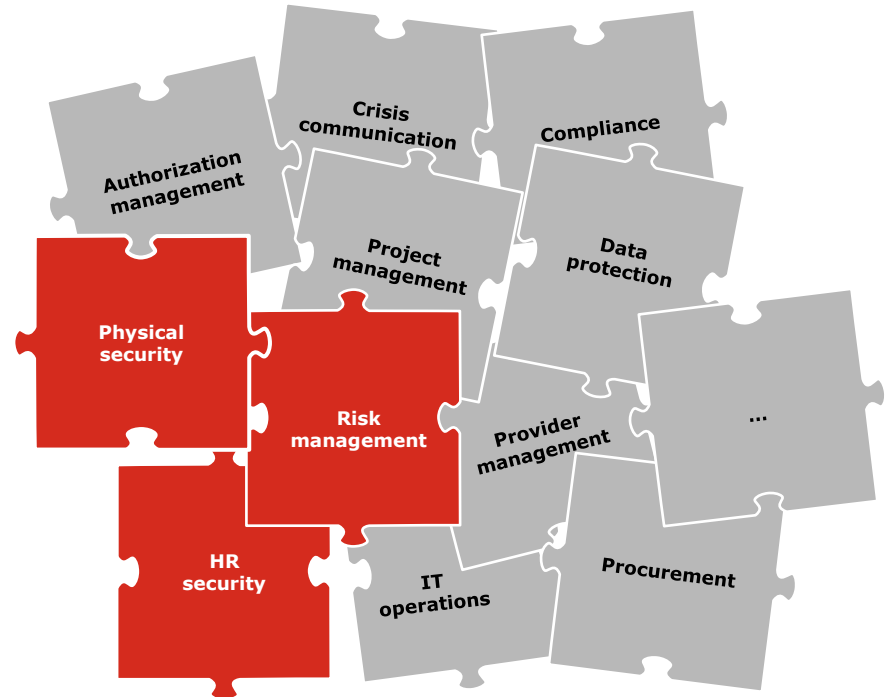
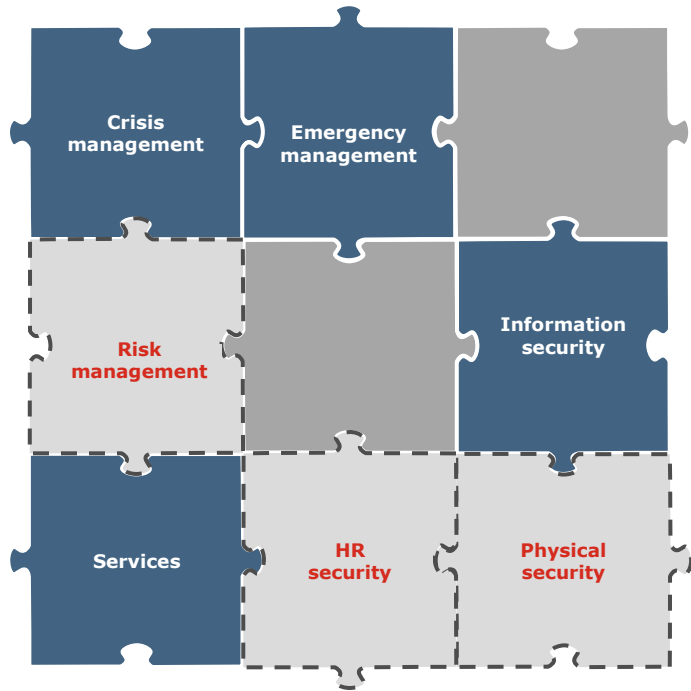
ISMS Implementation

Outlook

# Organizational Structure. Pre-existing Structure.



# Organizational Structure. Pre-existing Structure.



# Subjects. Application Areas.

## Corporate security

- BCM
- ISMS
- Physical security
- HR security
- Authorization management
- Security situation

## IT

- IT risk management
- IT compliance management
- ICS

# Challenges. Things Shared.



- Different subject areas
- Different project procedures

but ...

- Shared data
- Shared platform



# Agenda.

Presentation DZ BANK/TÜV Rheinland

Initial Situation

Project Procedure

ICS Implementation

BCM Implementation

ISMS Implementation

Outlook

# Standard. Project Procedure (1/3).

1

## Conception

- One-day training of main contact at client
- Workshops to coordinate functional requirements for “translation” into technical functions
- Creation of a prototype in RSA Archer
- Approval/partial approval by client

2

## Implementation

- Implementation in RSA Archer
- Testing by TÜV Rheinland
- Creation of documentation
- If necessary: Creation of interface documentation

# Standard. Project Procedure (2/3).

3

## Testing

- Installation in integration environment
- Testing by client on basis of coordinated test cases
- Adjustment based on feedback and updating of documentation

4

## Pilot

- Testing by selected client employees (later users of solution)
- Adjustment based on feedback and updating of documentation

# Standard. Project Procedure (3/3).

5

## Approval

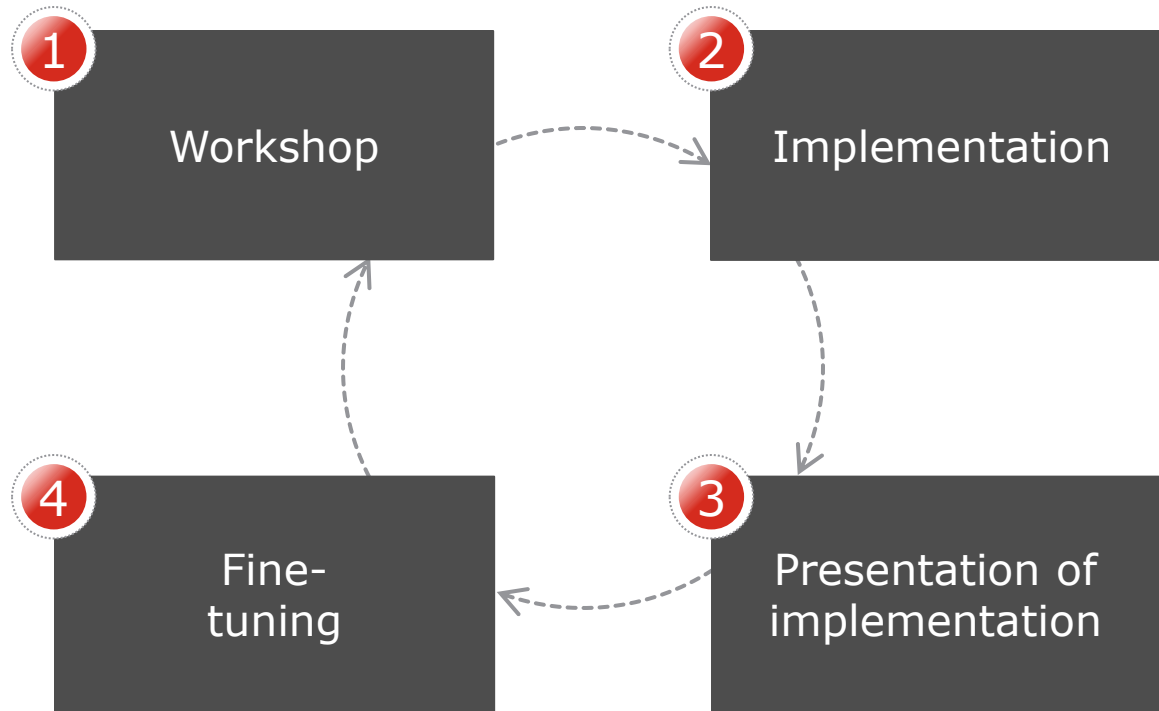
- Approval of documentation by client
- Approval of system by client

6

## Go Live

- Transfer of functions and data to be migrated into live system

# Project Procedure. Alternative.



# Agenda.

Presentation DZ BANK/TÜV Rheinland

Initial Situation

Project Procedure

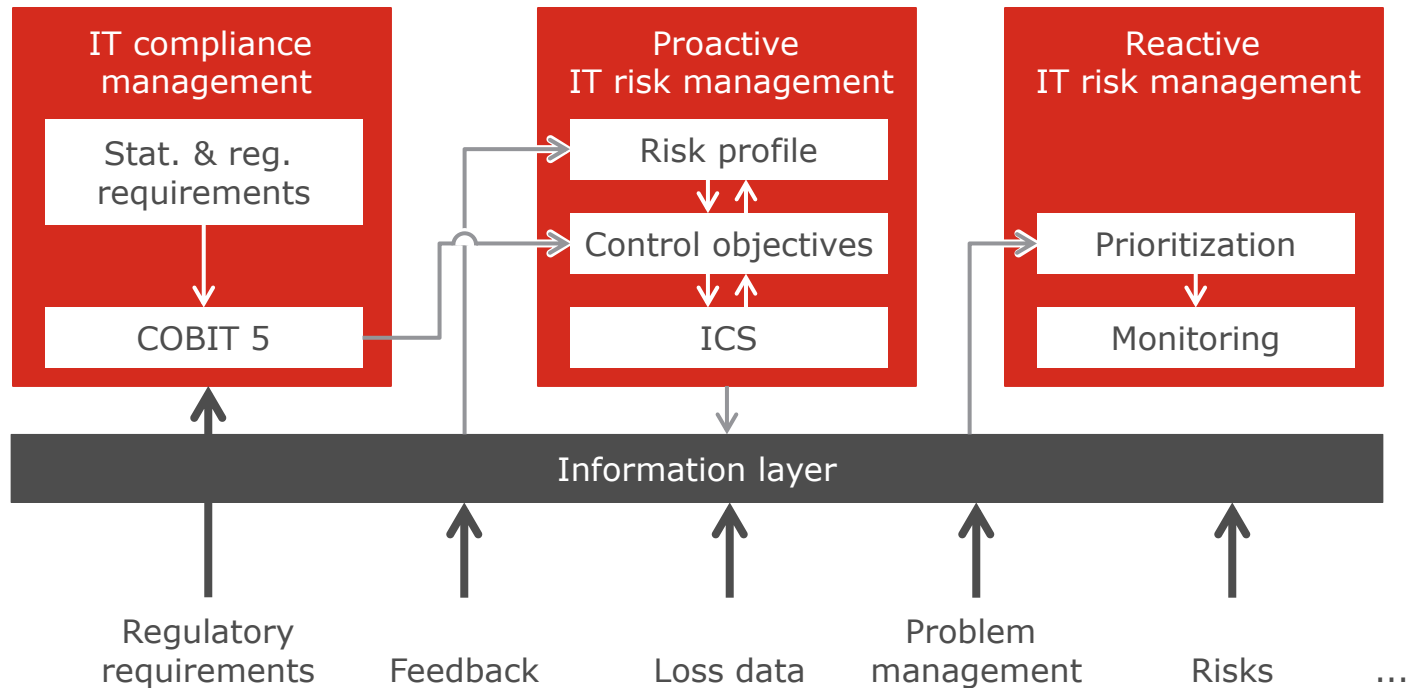
**ICS Implementation**

BCM Implementation

ISMS Implementation

Outlook

# IT Risk. Compliance Management.



# IT Compliance Management.

## Variants.

**DZ BANK**  
Zusammen geht mehr.

Preferences Reports Help Logout Search: IT-Risk und Compliance

Willkommen Notfallmanagement BC-Cockpit Krisenmanagement **IT-Compliance** Proaktives IT-Risikomanagement Reaktives IT-Risikomanagement ITRC Administration IT-Datenschutz IT-Notfallmanagement Sicherheitsvorfall Glossar Administration

Dashboard: Gesetze - Kontrollziele Welcome, Lars Rudloff Options

Liste relevanter Gesetze und Standards

**MaRisk**

Die Mindestanforderungen an das Risikomanagement (BA), abgekürzt MaRisk (BA), sind Verwaltungsanweisungen, die mit einem Rundschreiben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) für die Ausgestaltung des Risikomanagements in deutschen Kreditinstituten veröffentlicht wurden. Sie wurden von der BaFin erstmals mit Rundschreiben 18/2005 vom 20. Dezember 2005 veröffentlicht und zuletzt am 14. Dezember 2012 durch das Rundschreiben 10/2012 (BA) geändert.

**COBIT 5.0**

COBIT 5 stellt ein umfassendes Rahmenwerk bereit, das Unternehmen dabei unterstützt, ihre Ziele im Rahmen der Governance und des Managements der Unternehmens-IT zu erreichen. Kurzum: COBIT 5 hilft Unternehmen, einen optimalen IT-Wert zu generieren, indem sie für ein ausgeglichenes Verhältnis zwischen der Nutzenrealisierung, der Optimierung von Risiko (auf verschiedenen Ebenen) und der Nutzung von Ressourcen sorgen. COBIT 5 ermöglicht eine ganzheitliche Governance und ein ganzheitliches Management der IT für das gesamte Unternehmen. Dabei werden alle funktionalen Zuständigkeitsbereiche von Unternehmen und IT lückenlos integriert und die IT-bezogenen Interessen interner und externer Anspruchsgruppen berücksichtigt. COBIT 5 ist ein generischer Ansatz und damit für Unternehmen aller Größen geeignet, egal ob es sich um Wirtschaftsunternehmen, gemeinnützige Organisationen oder Einrichtungen des öffentlichen Sektors handelt.

Berichte

**Bericht Umsetzung der MaRisk-Vorgaben (MaRisk - Kontrollziele)**

Mit diesem Bericht kann die Erfüllung der MaRisk-Vorgaben durch die Kontrollziele nachgewiesen werden.

**Bericht Nicht umgesetzte MaRisk-Vorgaben**

Dieser Bericht zeigt den Handlungsbedarf hinsichtlich der Anforderungen aus der MaRisk. Alle an die IT gestellten Vorgaben aus der MaRisk sind umzusetzen d. h. mit Kontrollziele und weiter mit Kontrollpunkten zu belegen.

**Bericht Umsetzungsstatus der COBIT-Vorgaben**

Dieser Bericht enthält die Übersicht aller COBIT-Vorgaben, die durch definierte Kontrollziele umgesetzt wurden.

**Bericht Nicht umgesetzte COBIT-Vorgaben**

Hier werden alle COBIT-Vorgaben aufgelistet, die noch nicht mit Kontrollzielen hinterlegt wurden.



# Proactive. IT Risk Management ICS.

**DZ BANK**  
Zusammen geht mehr.

Preferences Reports Help Logout Search: IT-Risk und Compliance

Willkommen Notfallmanagement BC-Cockpit Krisenmanagement IT-Compliance **Proaktives IT-Risikomanagement** Reaktives IT-Risikomanagement ITRC Administration More

KS Self Assessment

Dashboard: Proaktives IT-Risikomanagement Welcome, Lars Rudolf Options

**Risiken Heatmaps**  
Heatmap IT-Betriebsrisiken

Auswirkungen	(No Selection)	(1) gering	(2) mittel	(3) hoch	(4) sehr hoch
(4) sehr hoch					
(3) hoch		2			
(2) mittel		1	4	2	
(1) gering		2	3	1	
(No Selection)					

Eintrittshäufigkeit

**Proaktives IT-Risikomanagement (SK)**

- [Bericht: IT-Risikoprofil - Risikoneigung](#)  
Die Darstellung zeigt die aktuelle Risikoneigung des IT-Managements je Risikogruppe gemäß Strategie.
- [Bericht: IT-Risikoprofil - Risikoneigung \(graphisch\)](#)
- [Bericht: IT-Risikoprofil - Risikokatalog](#)
- [Bericht: IT-Risikoprofil - Risikoereignisse inkl. Bewertung und Kontrollziele](#)  
Dieser Bericht zeigt alle Risikoereignisse inkl. der aktuellen Bewertung der Eintrittswahrscheinlichkeit und der Auswirkungen sowie die dazugehörigen Kontrollziele
- [Bericht: Kontrollziele mit Treibern und Risikoereignisse](#)
- [Bericht: IKS von den Risikoereignissen bis zu den Kontrollpunkten](#)  
Der Bericht zeigt das IKS von den Risikoereignissen bis zum Kontrollpunkt.

**Prozesse - Kontrollpunkte** **Proaktives IT-Risikomanagement (PV)**

# Reactive. IT Risk Management.

**DZ BANK**  
Zusammen geht mehr.

Preferences Reports Help Logout Search: IT-Risk und Compliance

Willkommen Notfallmanagement BC-Cockpit Krisenmanagement IT-Compliance Proaktives IT-Risikomanagement **Reaktives IT-Risikomanagement** ITRC Administration IT-Datenschutz IT-Notfallmanagement Sicherheitsvorfall Glossar Administration

Dashboard: Reaktives IT-Risikomanagement Welcome, Lars Rudloff Options

**Aktivitäten**

Name ▲	Aktivität Owner	Beschreibung	Status	Kontrollpunkte	Kontrollziele	Risikoereignisse
Maßnahme 12	Rudolff, Lars		In Bearbeitung			
Maßnahme 13	Rudolff, Lars		In Bearbeitung			

Page 1 of 1 (2 records)

**Reaktives IT-Risikomanagement Reports**

- [Zeit alle Moniten an](#)
- [Zeit alle Problems an](#)
- [Zeit alle Verluste an](#)
- [Zeit alle IT-Sec-Restrisiken an](#)

**Moniten**

- [Moniten](#)
- [Moniten ohne Aktivitäten](#)
- [Moniten ohne Proaktives IT-Risikomanagement](#)

**Problems**

- [Problems](#)
- [Problems ohne Aktivitäten](#)
- [Problems ohne Proaktives IT-Risikomanagement](#)

# Agenda.

Presentation DZ BANK/TÜV Rheinland

Initial Situation

Project Procedure

ICS Implementation

BCM Implementation

ISMS Implementation

Outlook

# BCM Implementation



- Performance of business impact analysis
- Preparation of BIA report
- Preparation of business continuation plans
- Exercises and tests
- Administration of emergency workplaces

# Interfaces. Connection.



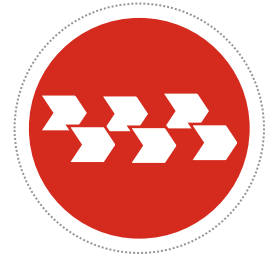
Personnel



IT applications



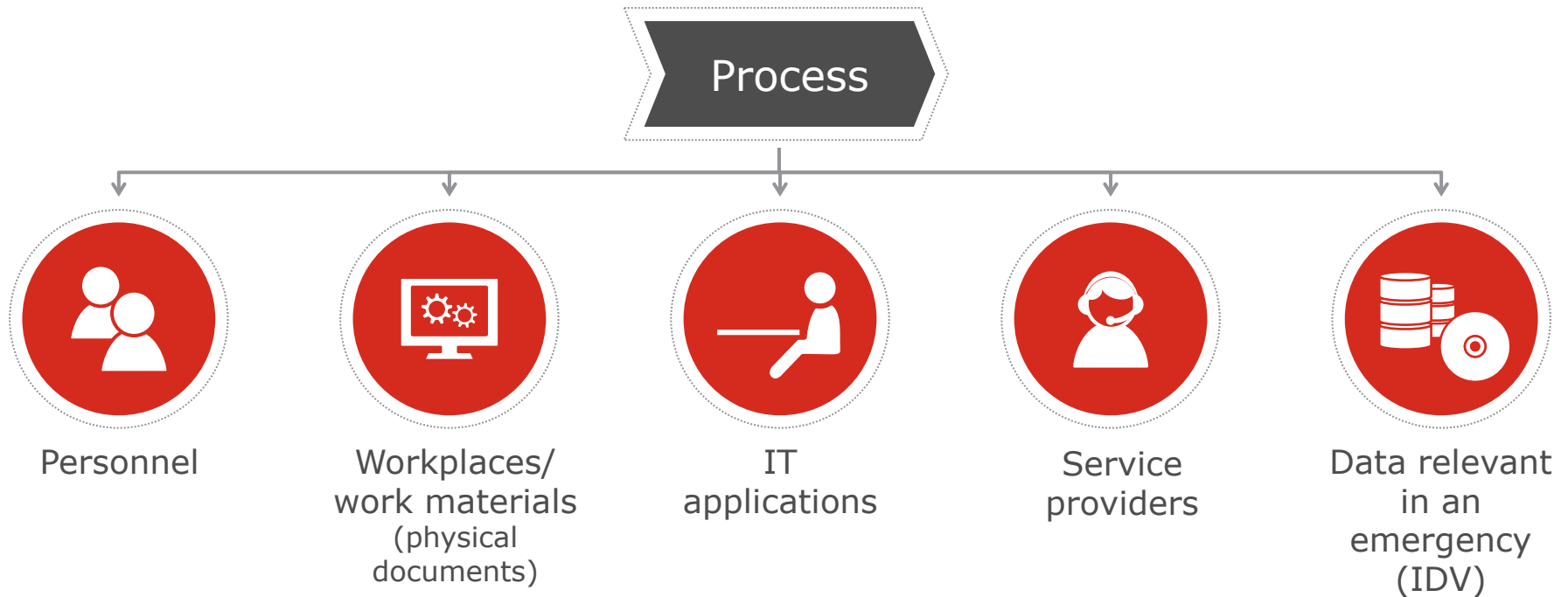
Service providers



Processes

**RSA**® Archer® GRC

# Link. Resources.



# MTD Evaluation.

General Information		Business Impact Analysis														
Status of the Business Impact Analysis		Evaluate Business Processes	Contingency Staff	Resources	Deadline of Event											
<b>▼ Rating</b>																
<b>Rating:</b>	<b>Krisenmanagement durchführen</b>	< 4h	< 1d	< 2d	< 5d	< 10d < 30d										
	Economic damage	(3)	(3)	(3)	(3)	(3)										
	Violations of laws and guidelines, contractual infringements	(1)	(1)	(1)	(1)	(1)										
	Impact on reputation	(2)	(3)	(3)	(3)	(3)										
	<b>Legend</b>	(1) = No or negligible consequences (2) = Tolerable		(3) = Considerable (4) = Serious												
<b>MTD:</b>	< 4h					<b>Evaluation Comment:</b>										
<b>Impact:</b>																
<b>Single-Point-Of-Failures:</b>																
<b>▼ Economic damage</b>																
Select impact classes																
<b>economic loss (&lt; 4h):</b>	<input type="radio"/> (1) <input type="radio"/> (2) <input checked="" type="radio"/> (3) <input type="radio"/> (4)															
<b>economic loss (&lt; 1d):</b>	<input type="radio"/> (1) <input type="radio"/> (2) <input checked="" type="radio"/> (3) <input type="radio"/> (4)															
<b>economic loss (&lt; 2d):</b>	<input type="radio"/> (1) <input type="radio"/> (2) <input checked="" type="radio"/> (3) <input type="radio"/> (4)															
<b>economic loss (&lt; 5d):</b>	<input type="radio"/> (1) <input type="radio"/> (2) <input checked="" type="radio"/> (3) <input type="radio"/> (4)															
<b>economic loss (&lt; 10d):</b>	<input type="radio"/> (1) <input type="radio"/> (2) <input checked="" type="radio"/> (3) <input type="radio"/> (4)															
<b>economic loss (&lt; 30d):</b>	<input type="radio"/> (1) <input type="radio"/> (2) <input checked="" type="radio"/> (3) <input type="radio"/> (4)															
		<table border="1"> <thead> <tr> <th>Impact class</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>(1) No or negligible consequences</td> <td> <ul style="list-style-type: none"> <li>No noteworthy consequences (e.g. loss less than €10,000)</li> <li>Hardly any noteworthy impact of the company's business workflows perceptible</li> </ul> </td> </tr> <tr> <td>(2) Tolerable</td> <td> <ul style="list-style-type: none"> <li>The financial damage remains at a tolerable level for DZ BANK AG (e.g. loss less than €100,000)</li> <li>The impact on other business divisions, customers or contractual partners is negligible</li> </ul> </td> </tr> <tr> <td>(3) Considerable</td> <td> <ul style="list-style-type: none"> <li>The damage causes considerable financial losses (e.g. loss between €100,000 and €1,000,000)</li> <li>The damage has significant consequences for the company's business workflow</li> <li>Other business divisions, customers or contractual partners are noticeably impacted</li> </ul> </td> </tr> <tr> <td>(4) Serious</td> <td> <ul style="list-style-type: none"> <li>The financial damage is serious for DZ BANK AG (e.g. if the loss exceeds €1,000,000)</li> <li>The interruptions to the company's business workflows are no longer consist of minor inconveniences</li> <li>Other business divisions, customers or contractual partners are seriously impacted</li> </ul> </td> </tr> </tbody> </table>					Impact class	Description	(1) No or negligible consequences	<ul style="list-style-type: none"> <li>No noteworthy consequences (e.g. loss less than €10,000)</li> <li>Hardly any noteworthy impact of the company's business workflows perceptible</li> </ul>	(2) Tolerable	<ul style="list-style-type: none"> <li>The financial damage remains at a tolerable level for DZ BANK AG (e.g. loss less than €100,000)</li> <li>The impact on other business divisions, customers or contractual partners is negligible</li> </ul>	(3) Considerable	<ul style="list-style-type: none"> <li>The damage causes considerable financial losses (e.g. loss between €100,000 and €1,000,000)</li> <li>The damage has significant consequences for the company's business workflow</li> <li>Other business divisions, customers or contractual partners are noticeably impacted</li> </ul>	(4) Serious	<ul style="list-style-type: none"> <li>The financial damage is serious for DZ BANK AG (e.g. if the loss exceeds €1,000,000)</li> <li>The interruptions to the company's business workflows are no longer consist of minor inconveniences</li> <li>Other business divisions, customers or contractual partners are seriously impacted</li> </ul>
Impact class	Description															
(1) No or negligible consequences	<ul style="list-style-type: none"> <li>No noteworthy consequences (e.g. loss less than €10,000)</li> <li>Hardly any noteworthy impact of the company's business workflows perceptible</li> </ul>															
(2) Tolerable	<ul style="list-style-type: none"> <li>The financial damage remains at a tolerable level for DZ BANK AG (e.g. loss less than €100,000)</li> <li>The impact on other business divisions, customers or contractual partners is negligible</li> </ul>															
(3) Considerable	<ul style="list-style-type: none"> <li>The damage causes considerable financial losses (e.g. loss between €100,000 and €1,000,000)</li> <li>The damage has significant consequences for the company's business workflow</li> <li>Other business divisions, customers or contractual partners are noticeably impacted</li> </ul>															
(4) Serious	<ul style="list-style-type: none"> <li>The financial damage is serious for DZ BANK AG (e.g. if the loss exceeds €1,000,000)</li> <li>The interruptions to the company's business workflows are no longer consist of minor inconveniences</li> <li>Other business divisions, customers or contractual partners are seriously impacted</li> </ul>															

# Contingency staff.

General Information | Business Impact Analysis

Status of the Business Impact Analysis | Evaluate Business Processes | Contingency Staff | Resources | Deadline or Event

▼ Contingency Staff Summary

Necessary Human-Resources:	Roles	Quantity for regular operations	Quantity for emergency operations					
			< 4h	< 1d	< 2d	< 5d	< 10d	< 30d
	Krisenmanager	1	1	1	1	1	1	1
	Total Staff	1	1	1	1	1	1	1

Workarounds: Vertretung innerhalb von DSOU geregelt

▼ Contingency Staff Row 1

Personnel / role	Krisenmanager
Quantity for regular operations	1
< 4h	1
< 1d	1
< 2d	1
< 5d	1
< 10d	1
< 30d	1



# Resources.

General Information | Business Impact Analysis

Status of the Business Impact Analysis | Evaluate Business Processes | Contingency Staff | Resources | Deadline or Event

▼ Facilities Recovery Procedures | Add New |

Name ▲	MTD	Description	Workarounds	Return To Normal Operations
Frankfurt_Westend_1_Krisenmanagement_durchfuehren			Weitere Krisenstabsräume bei der Union Investment und R+V Versicherung	

▼ IT-Applications Recovery Procedures | Add New |

Name ▲	MTD	Description	Workarounds	Return To Normal Operations
RSA_Archer_Krisenmanagement_durchfuehren	< 1d		Ausgedruckte Version der Dokumente in den Krisenstabsräumen und auf den USB-Sticks der Krisenstabsmitglieder.	Pflege von aktuellen Informationen in RSA/Archer

▼ Work Equipment, IDV and Web Application Recovery Procedures | Add New |

Name ▲	MTD	Description	Workarounds	Return To Normal Operations
Fact24-Krisenmanagement_durchfuehren			Manuelle Alarmierung der Krisenstabsteilnehmer per Telefon	

▼ External Service Providers Recovery Procedures | Add New |

Name ▲	MTD	Description	Workarounds	Return To Normal Operations
No Records Found				

▼ Inter-divisional Interfaces for other Divisions (Recovery Procedures) | Add New |

Name ▲	MTD	Description	Workarounds	Return To Normal Operations
No Records Found				

▼ Additional Information

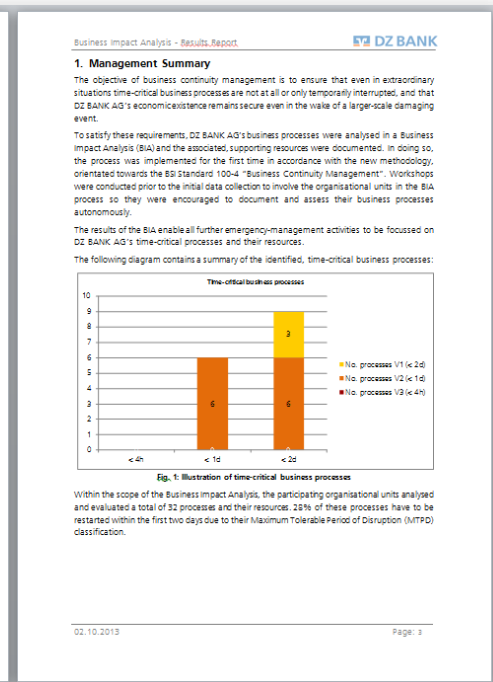
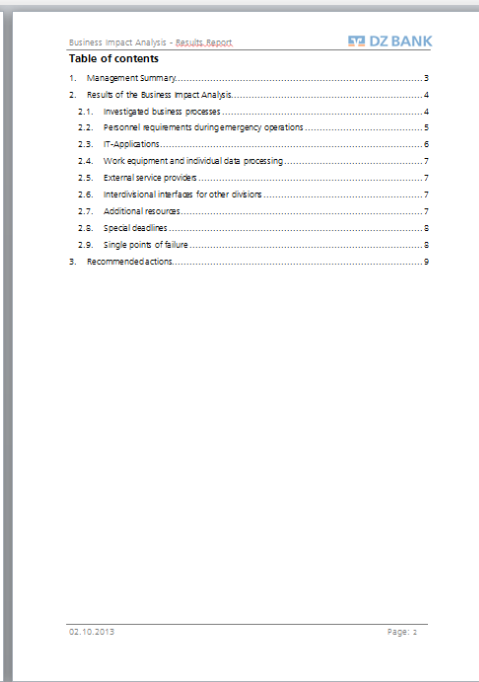
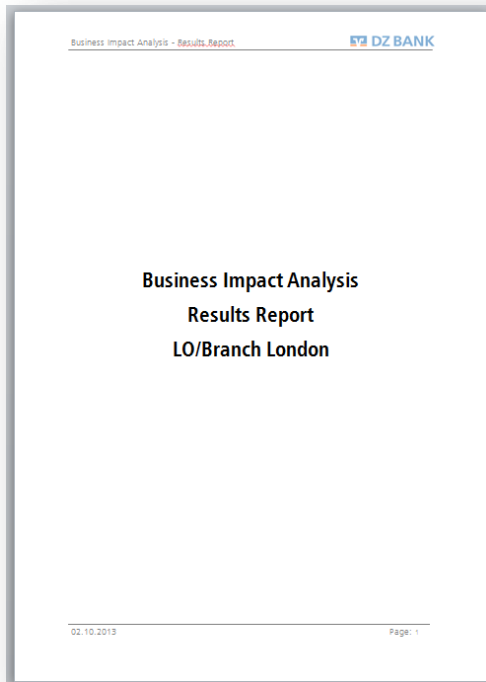
Workplace Equipment:  Fax  Handelsrechner  Spezialdrucker

Additional Resources:

Additional Attachments | Add New |

Name	Size	Type	Upload Date
No Records Found			

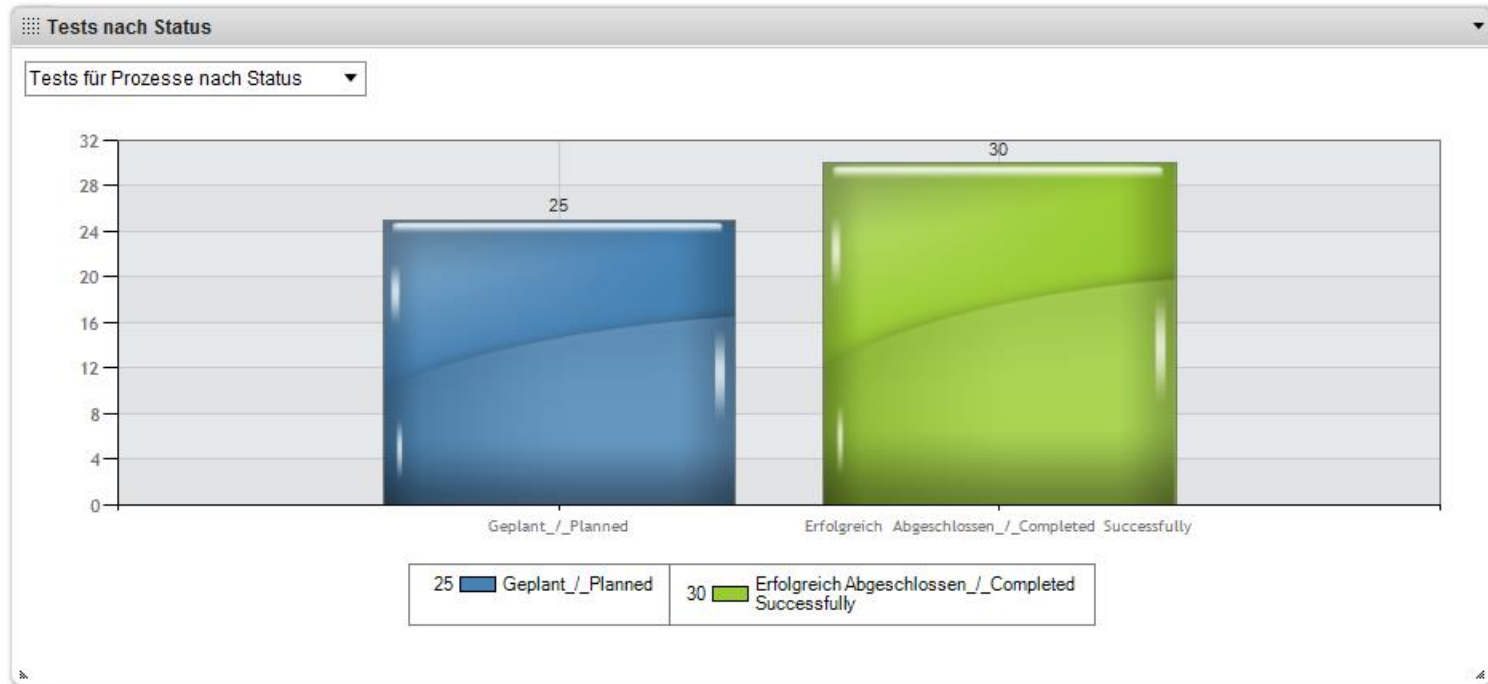
# BIA report.



# BCP.

<p>BCP-Plan - London Branch</p> <p style="text-align: right;">DZ BANK</p> <h2 style="text-align: center;">Business Continuity Plan LO – London Branch</h2> <p style="text-align: right;">11/10/2013 Page 1</p>	<p>BCP-Plan - London Branch</p> <p style="text-align: right;">DZ BANK</p> <p><b>Change History</b></p> <table border="1"> <thead> <tr> <th>Date</th> <th>Version</th> <th>Author / Review</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td>11/10/2013</td> <td>1.0</td> <td>Schickel, Thorsten</td> <td>Docu-Revision: 000401 BNA48</td> </tr> </tbody> </table> <p style="text-align: right;">11/10/2013 Page 2</p>	Date	Version	Author / Review	Comment	11/10/2013	1.0	Schickel, Thorsten	Docu-Revision: 000401 BNA48	<p>BCP-Plan - London Branch</p> <p style="text-align: right;">DZ BANK</p> <p><b>Table of Contents</b></p> <table border="0"> <tr><td>1 Purpose and objectives of the business continuity plan.....</td><td>4</td></tr> <tr><td>2 Processes of the branch.....</td><td>6</td></tr> <tr><td>3 Special dates.....</td><td>6</td></tr> <tr><td>4 Alerting procedure, escalation and communication.....</td><td>7</td></tr> <tr><td>4.1 Communication within DZ BANK.....</td><td>7</td></tr> <tr><td>4.1.1 Emergency team.....</td><td>8</td></tr> <tr><td>4.1.2 Additional internal contacts.....</td><td>8</td></tr> <tr><td>4.2 External communication.....</td><td>9</td></tr> <tr><td>4.2.1 External contacts of the division.....</td><td>9</td></tr> <tr><td>5 General instructions.....</td><td>10</td></tr> <tr><td>6 Site failure scenario.....</td><td>13</td></tr> <tr><td>6.1 General.....</td><td>13</td></tr> <tr><td>6.2 Buildings and assembly points.....</td><td>13</td></tr> <tr><td>6.3 Emergency team room.....</td><td>13</td></tr> <tr><td>6.4 Alternative site and emergency workspaces.....</td><td>13</td></tr> <tr><td>6.5 Further required resources.....</td><td>14</td></tr> <tr><td>6.6 Measures for the preparation of emergency operation.....</td><td>14</td></tr> <tr><td>6.7 Emergency operation with site failure.....</td><td>15</td></tr> <tr><td>6.8 Return to normal operation.....</td><td>17</td></tr> <tr><td>7 Scenario of IT application failure.....</td><td>20</td></tr> <tr><td>7.1 IT applications.....</td><td>20</td></tr> <tr><td>7.2 Measures for the preparation of emergency operation.....</td><td>21</td></tr> <tr><td>7.3 Emergency operation in the event of application failure.....</td><td>21</td></tr> <tr><td>7.4 Return to normal operation.....</td><td>23</td></tr> <tr><td>8 Scenario of staff shortage.....</td><td>23</td></tr> <tr><td>8.1 General.....</td><td>23</td></tr> <tr><td>8.2 Measures for the preparation of emergency operation.....</td><td>25</td></tr> <tr><td>8.3 Emergency operation in the event of staff absence.....</td><td>25</td></tr> <tr><td>8.4 Return to normal operation.....</td><td>27</td></tr> <tr><td>9 Scenario of service provider failure.....</td><td>32</td></tr> <tr><td>9.1 Required service providers.....</td><td>32</td></tr> <tr><td>9.2 Measures for the preparation of emergency operation.....</td><td>32</td></tr> <tr><td>9.3 Emergency operation in the event of a service provider failure.....</td><td>32</td></tr> <tr><td>9.4 Return to normal operation.....</td><td>33</td></tr> <tr><td>10 Cross-divisional interfaces for other divisions.....</td><td>35</td></tr> <tr><td>11 Cross-divisional interfaces from other divisions.....</td><td>36</td></tr> <tr><td>12 Appendix.....</td><td>37</td></tr> </table> <p style="text-align: right;">11/10/2013 Page 3</p>	1 Purpose and objectives of the business continuity plan.....	4	2 Processes of the branch.....	6	3 Special dates.....	6	4 Alerting procedure, escalation and communication.....	7	4.1 Communication within DZ BANK.....	7	4.1.1 Emergency team.....	8	4.1.2 Additional internal contacts.....	8	4.2 External communication.....	9	4.2.1 External contacts of the division.....	9	5 General instructions.....	10	6 Site failure scenario.....	13	6.1 General.....	13	6.2 Buildings and assembly points.....	13	6.3 Emergency team room.....	13	6.4 Alternative site and emergency workspaces.....	13	6.5 Further required resources.....	14	6.6 Measures for the preparation of emergency operation.....	14	6.7 Emergency operation with site failure.....	15	6.8 Return to normal operation.....	17	7 Scenario of IT application failure.....	20	7.1 IT applications.....	20	7.2 Measures for the preparation of emergency operation.....	21	7.3 Emergency operation in the event of application failure.....	21	7.4 Return to normal operation.....	23	8 Scenario of staff shortage.....	23	8.1 General.....	23	8.2 Measures for the preparation of emergency operation.....	25	8.3 Emergency operation in the event of staff absence.....	25	8.4 Return to normal operation.....	27	9 Scenario of service provider failure.....	32	9.1 Required service providers.....	32	9.2 Measures for the preparation of emergency operation.....	32	9.3 Emergency operation in the event of a service provider failure.....	32	9.4 Return to normal operation.....	33	10 Cross-divisional interfaces for other divisions.....	35	11 Cross-divisional interfaces from other divisions.....	36	12 Appendix.....	37
Date	Version	Author / Review	Comment																																																																																	
11/10/2013	1.0	Schickel, Thorsten	Docu-Revision: 000401 BNA48																																																																																	
1 Purpose and objectives of the business continuity plan.....	4																																																																																			
2 Processes of the branch.....	6																																																																																			
3 Special dates.....	6																																																																																			
4 Alerting procedure, escalation and communication.....	7																																																																																			
4.1 Communication within DZ BANK.....	7																																																																																			
4.1.1 Emergency team.....	8																																																																																			
4.1.2 Additional internal contacts.....	8																																																																																			
4.2 External communication.....	9																																																																																			
4.2.1 External contacts of the division.....	9																																																																																			
5 General instructions.....	10																																																																																			
6 Site failure scenario.....	13																																																																																			
6.1 General.....	13																																																																																			
6.2 Buildings and assembly points.....	13																																																																																			
6.3 Emergency team room.....	13																																																																																			
6.4 Alternative site and emergency workspaces.....	13																																																																																			
6.5 Further required resources.....	14																																																																																			
6.6 Measures for the preparation of emergency operation.....	14																																																																																			
6.7 Emergency operation with site failure.....	15																																																																																			
6.8 Return to normal operation.....	17																																																																																			
7 Scenario of IT application failure.....	20																																																																																			
7.1 IT applications.....	20																																																																																			
7.2 Measures for the preparation of emergency operation.....	21																																																																																			
7.3 Emergency operation in the event of application failure.....	21																																																																																			
7.4 Return to normal operation.....	23																																																																																			
8 Scenario of staff shortage.....	23																																																																																			
8.1 General.....	23																																																																																			
8.2 Measures for the preparation of emergency operation.....	25																																																																																			
8.3 Emergency operation in the event of staff absence.....	25																																																																																			
8.4 Return to normal operation.....	27																																																																																			
9 Scenario of service provider failure.....	32																																																																																			
9.1 Required service providers.....	32																																																																																			
9.2 Measures for the preparation of emergency operation.....	32																																																																																			
9.3 Emergency operation in the event of a service provider failure.....	32																																																																																			
9.4 Return to normal operation.....	33																																																																																			
10 Cross-divisional interfaces for other divisions.....	35																																																																																			
11 Cross-divisional interfaces from other divisions.....	36																																																																																			
12 Appendix.....	37																																																																																			
<p>BCP-Plan - London Branch</p> <p style="text-align: right;">DZ BANK</p> <p><b>1 Purpose and objectives of the business continuity plan</b></p> <p>The business continuity plan (BCP) is intended to ensure that within a short space of time emergency operation can be restored and the essential processes can be completely or partly re-started.</p> <p>At the same time the general protection goals <b>maintained</b> throughout the Bank apply to the branch:</p> <ul style="list-style-type: none"> <li>Protection of life and limbs of the staff, external employees and guests always take precedence</li> </ul>	<p>BCP-Plan - London Branch</p> <p style="text-align: right;">DZ BANK</p> <p><b>2 Processes of the branch</b></p> <p>The processes assessed in this section are the result of the Business Impact Analysis (BIA) and are therefore subject to regular updating.</p> <table border="1"> <thead> <tr> <th>Business process</th> <th>Division</th> <th>MTBD</th> </tr> </thead> <tbody> <tr> <td>Deal Management LO</td> <td>LO-DF</td> <td>V2 (e 16)</td> </tr> <tr> <td>Control Accounts LO</td> <td>LO-OSL</td> <td>V2 (e 16)</td> </tr> <tr> <td>Asset Reconciliation LO</td> <td>LO-OSL</td> <td>V2 (e 16)</td> </tr> <tr> <td>Settlement LO</td> <td>LO-OSL</td> <td>V2 (e 16)</td> </tr> <tr> <td>Executive Liaison LO</td> <td>LO-DF</td> <td>V2 (e 16)</td> </tr> </tbody> </table>	Business process	Division	MTBD	Deal Management LO	LO-DF	V2 (e 16)	Control Accounts LO	LO-OSL	V2 (e 16)	Asset Reconciliation LO	LO-OSL	V2 (e 16)	Settlement LO	LO-OSL	V2 (e 16)	Executive Liaison LO	LO-DF	V2 (e 16)	<p>BCP-Plan - London Branch</p> <p style="text-align: right;">DZ BANK</p> <p><b>3 Special dates</b></p> <p>The critical dates and events per process listed in this section are similarly the result of the BIA, where the month-end dates always relate to the period from the 25th calendar day of a month to the 31st calendar day of the subsequent month.</p> <table border="1"> <thead> <tr> <th>Process</th> <th>Month-end</th> <th>End of quarter</th> <th>Year-end</th> </tr> </thead> <tbody> <tr> <td>CCO/AVL - Company CDO/AVL forms LO</td> <td>no</td> <td>no</td> <td>no</td> </tr> <tr> <td>Compliance Monitoring LO</td> <td>no</td> <td>no</td> <td>no</td> </tr> <tr> <td>Control Process LO</td> <td>yes</td> <td>no</td> <td>no</td> </tr> </tbody> </table>	Process	Month-end	End of quarter	Year-end	CCO/AVL - Company CDO/AVL forms LO	no	no	no	Compliance Monitoring LO	no	no	no	Control Process LO	yes	no	no																																																
Business process	Division	MTBD																																																																																		
Deal Management LO	LO-DF	V2 (e 16)																																																																																		
Control Accounts LO	LO-OSL	V2 (e 16)																																																																																		
Asset Reconciliation LO	LO-OSL	V2 (e 16)																																																																																		
Settlement LO	LO-OSL	V2 (e 16)																																																																																		
Executive Liaison LO	LO-DF	V2 (e 16)																																																																																		
Process	Month-end	End of quarter	Year-end																																																																																	
CCO/AVL - Company CDO/AVL forms LO	no	no	no																																																																																	
Compliance Monitoring LO	no	no	no																																																																																	
Control Process LO	yes	no	no																																																																																	

# Drills and Tests dashboard.



# Planning & documentation.

▼ General Information			
Name:	Business continuity test	Status:	Planned
Type:	(2) Process		
Start:	10/22/2014	Finished:	
Test Scenario:	Denial of access to the branch building		
Test Objectives:	Problem free operation at business continuity site within the MTPD		

▼ Affected Resources			
IT-Applications:		Processes:	<a href="#">Settlement LO</a>
Service Provider:		Facility:	<a href="#">London_Cheapside 150</a> <a href="#">London_DR-Location Phoenix House</a>
Participant:		Divisions:	<a href="#">LO</a>

▼ Script			
	Point in Time ▲	Duration	Event
No Records Found			

▼ Results			
Documentation:			
<b>Attachments</b>			
Name	Size	Type	Upload Date
No Records Found			

▼ Open Measures				<a href="#">Add New</a>
Measure ID ▲	Status	Due Date	Related To	
No Records Found				

► History Log

# Agenda.

Presentation DZ BANK/TÜV Rheinland

Initial Situation

Project Procedure

ICS Implementation

BCM Implementation

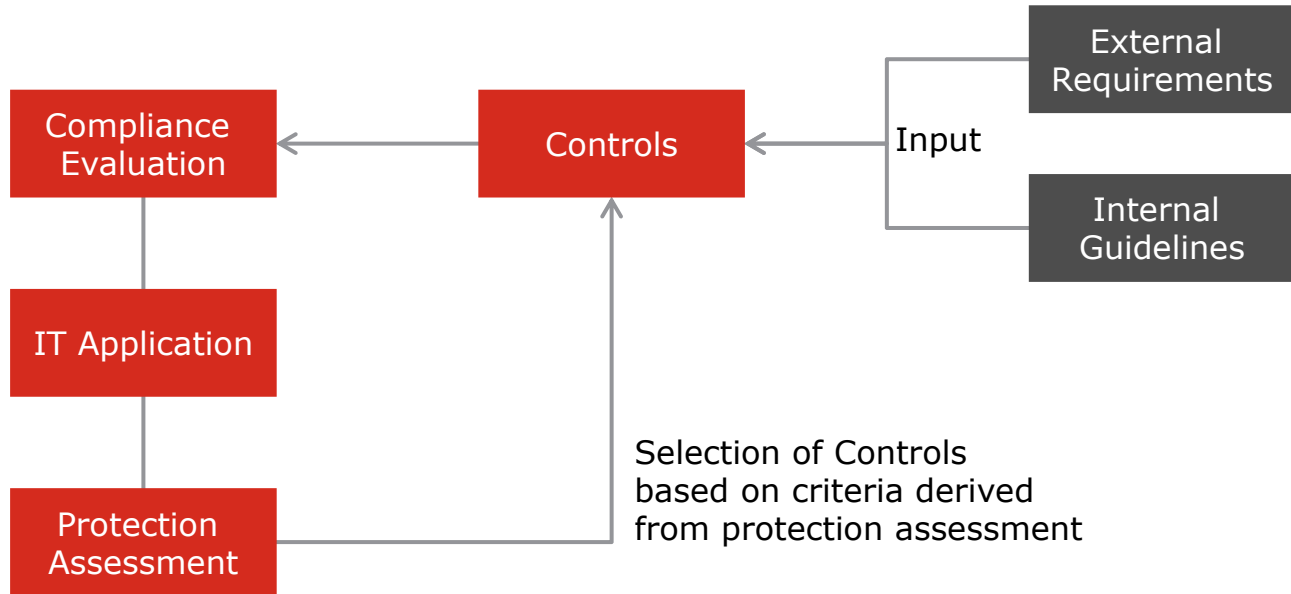
**ISMS Implementation**

Outlook



# Excerpt. Data Model.

## Security Concept.





# Protection Assessment.

The screenshot shows the DZ BANK ISCE (Information Security Cockpit) interface. The header includes the DZ BANK logo and the slogan "Zusammen geht mehr." The navigation bar contains various modules: Willkommen, ISCE, ISCE-Cockpit, Notfallmanagement, BC-Cockpit, Krisenmanagement, IT-Compliance, Proaktives IT-Risikomanagement, Reaktives IT-Risikomanagement, and More. The main content area is titled "Schutzbedarfsfeststellung: ADOBE ACROBAT READER - 202679" and shows "0 of 21 Completed". The interface is divided into several sections: Workflow, Technische Informationen, and Einstufung Schutzklasse. Under "Einstufung Schutzklasse", there are three sub-sections: Grunddaten der Anwendung, Geschäftsprozess-Unterstützung, and Schnittstellen. The "Grunddaten der Anwendung" section contains three questions:

- 1.1 Software-Typ (1):** Um welche Art der Software Bereitstellung handelt es sich?
  - (1) Standard-Software (externer Anbieter)
  - (2) Individual-Software (externer Anbieter)
  - (3) Individual-Software (Eigenentwicklung)[Edit](#)
- 1.2 Software-Typ (2):** Um welchen Typ des Anwendungsystems handelt es sich?
  - (1) Desktop-Anwendung
  - (2) Web-Applikation (Nutzung über Web-Browser)
  - (3) Server-Anwendung[Edit](#)
- 1.3 Betreiber:** Bitte wählen Sie aus, durch wen das Anwendungssystem betrieben wird. Bei der Auswahl ist insbesondere auf die Vertragsbeziehung zu externen Betreibern abzustellen.
  - (1) DZ-BANK - Bereich IT (eigene Infrastruktur)
  - (2) DZ-Bank - Bereich IT (fremde Infrastruktur)

At the bottom of the form, there are three buttons: "Save and Close", "Save and Continue", and "Cancel".

# Agenda.

Presentation DZ BANK/TÜV Rheinland

Initial Situation

Project Procedure

ICS Implementation

BCM Implementation

ISMS Implementation

Outlook

# Outlook Synergies.



- Standard process
- Roll-out across DZ BANK Group
- Evaluation of operator model

# Success Factors. Successful Implementation.



- Conception and harmonization of processes
- Conception and implementation of your requirements
- Integration into existing system landscape
- Application operation
- Comprehensive project experience

Thank you.