

Swiss Re



Einsatz zSecure Suite bei Swiss Re

Table of contents

- Swiss Re Überblick
- IT Umfeld
- zSecure Business Case / technische Umsetzung
- Einsatz Command Verifier
- Compliance Reporting mit zSecure
- Einsatz zSecure Alert
- Ausblick

Swiss Re Ueberblick

Swiss Re at a glance



- Swiss Re is a **leading and highly diversified global reinsurer**, founded in Zurich (Switzerland) in 1863



- **149 years of experience** in providing wholesale re/insurance and risk management solutions.

- **We deliver both traditional and innovative offerings** in Property & Casualty and Life & Health that meet our clients' needs.

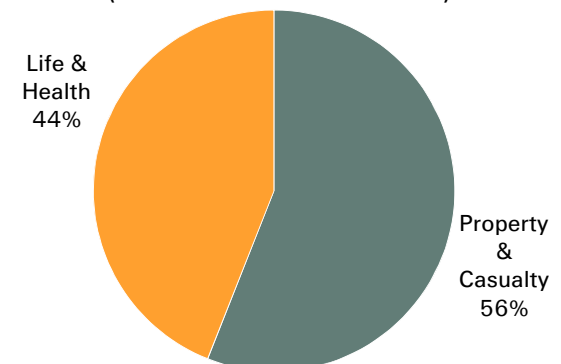
- **A pioneer in insurance-based capital market solutions**, we combine financial strength and unparalleled expertise for the benefit of our clients.







- **Our financial strength** is currently rated:
 Standard & Poor's: AA-/stable; Moody's A1/positive; A.M. Best: A+/stable

Key statistics in USD bn	FY 2010	FY 2011
Premiums earned:	19.7	21.3
Net income:	0.9	2.6
Shareholders' equity:	25.3	29.6
Return on equity:	3.6%	9.6%
Return on investments:	3.5%	5.1%
P&C combined ratio:	93.9%	101.6%
L&H benefit ratio:	88.7%	87.9%

Revenues by business
 (Total 2011: USD 21.3bn)



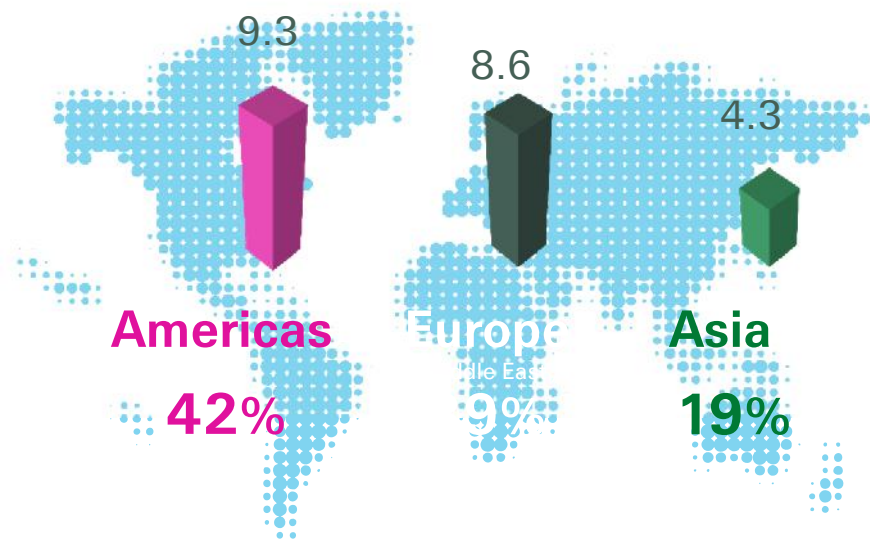
We enable risk-taking that is essential to enterprise and progress

Examples		
We identify and evaluate risks	Climate change identified as emerging risk almost 20 years ago	
We select and take risks	Insurance of most industrial risks	
We transfer and trade risks	Securitisation of earthquake and hurricane risks	
We educate and consult on risks	Over 50 risk-related publications during the last 12 months	

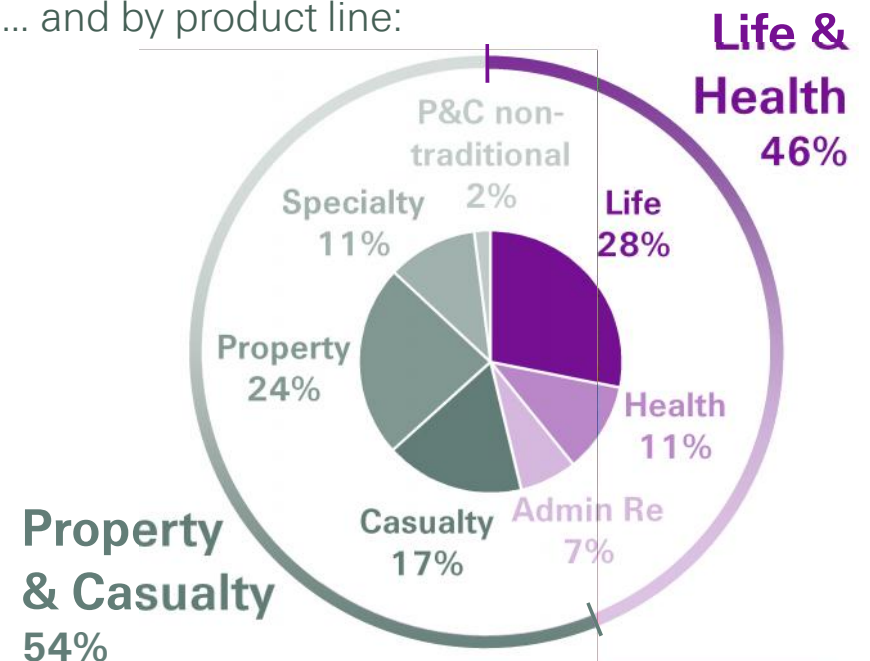
Swiss Re is broadly diversified by geography and product line

Premiums earned¹ 2011 (USD 22.2 billion)

by region (in USD bn)













... and by product line:



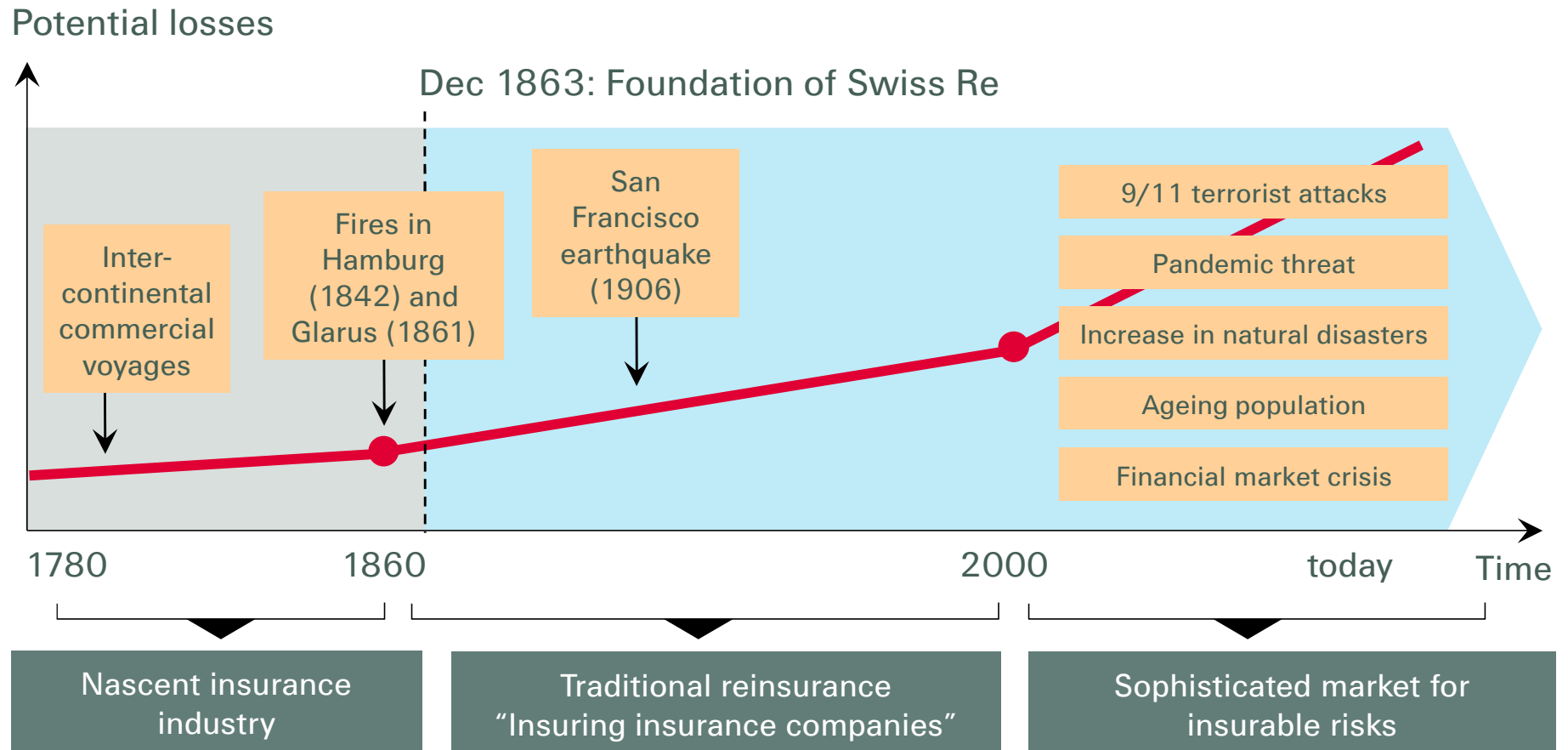
- Swiss Re benefits from geographic and business mix diversification and has the ability to reallocate capital to achieve profitable growth
- Combines accumulated expertise of over 149 years and continuing research with a widely recognised strong track record of innovation

¹ Includes fee income from policyholders

Important risks characterise our business

Examples		
Natural catastrophes	Earthquakes, Floods, Hurricanes, Tornadoes, ...	 
Fire, terrorism	Arson, Terror attack, ...	 
Pandemics	SARS, H5N1, H1N1, ...	 
Obesity	Health, Mortality, Liability, ...	 
Financial market risks	Credit, Equity, ...	 

Swiss Re has over 149 years of expertise in managing risk and capital



Swiss Re's history

1863	Founding of the company
1906	San Francisco Earthquake, Swiss Re establishes its reputation
1910	First branch office in New York
1950-1956	Opening of offices in South Africa, Canada, Australia, Hong Kong
1968-1976	Creation of several advisory and service companies in Asia and South America
1994	Refocus on core business - selling majority shares in several insurance companies
from 1995	Development of financial services offerings
1996-2001	Strengthening of life and health business through several acquisitions
2003-2004	Strengthening market position in Asia
2006	Successful acquisition and integration of GE Insurance Solutions
2008	Successful acquisition of Barclays Life Discontinued all financial market activities that are not insurance related
2009-2010	Fully restored capital strength, sharpened focus on core business

IT Umfeld historisch / heute

■ 1996 – 2006

Akquisitionen -> Integration diverser Rechenzentren

ungebremstes Wachstum -> organisatorische Veränderungen, Globalisierung der IT, viele Plattformen, Standorte, Projekte, Wildwuchs

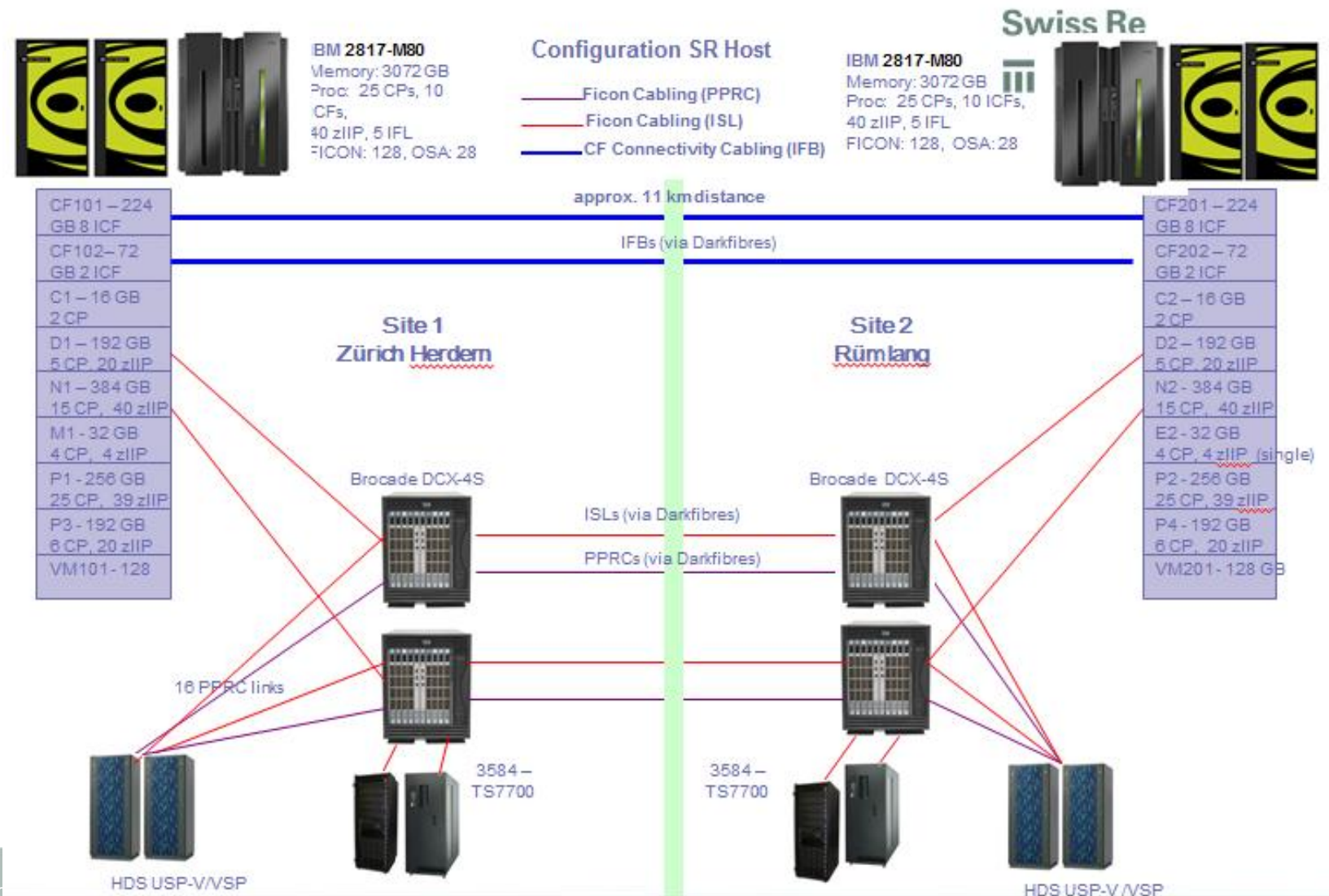
■ 2007 – heute

Finanzmarktkrise -> Kostendruck, Server-Konsolidierung, Reduktion der Komplexität, Abbau von (IT-)Standorten, teilweise Auslagerung von IT-Services (Bratislava, Bangalore). Operations komplett an IBM Polen ausgelagert sowie selektives Outsourcing von Engineering Aufgaben an IBM.

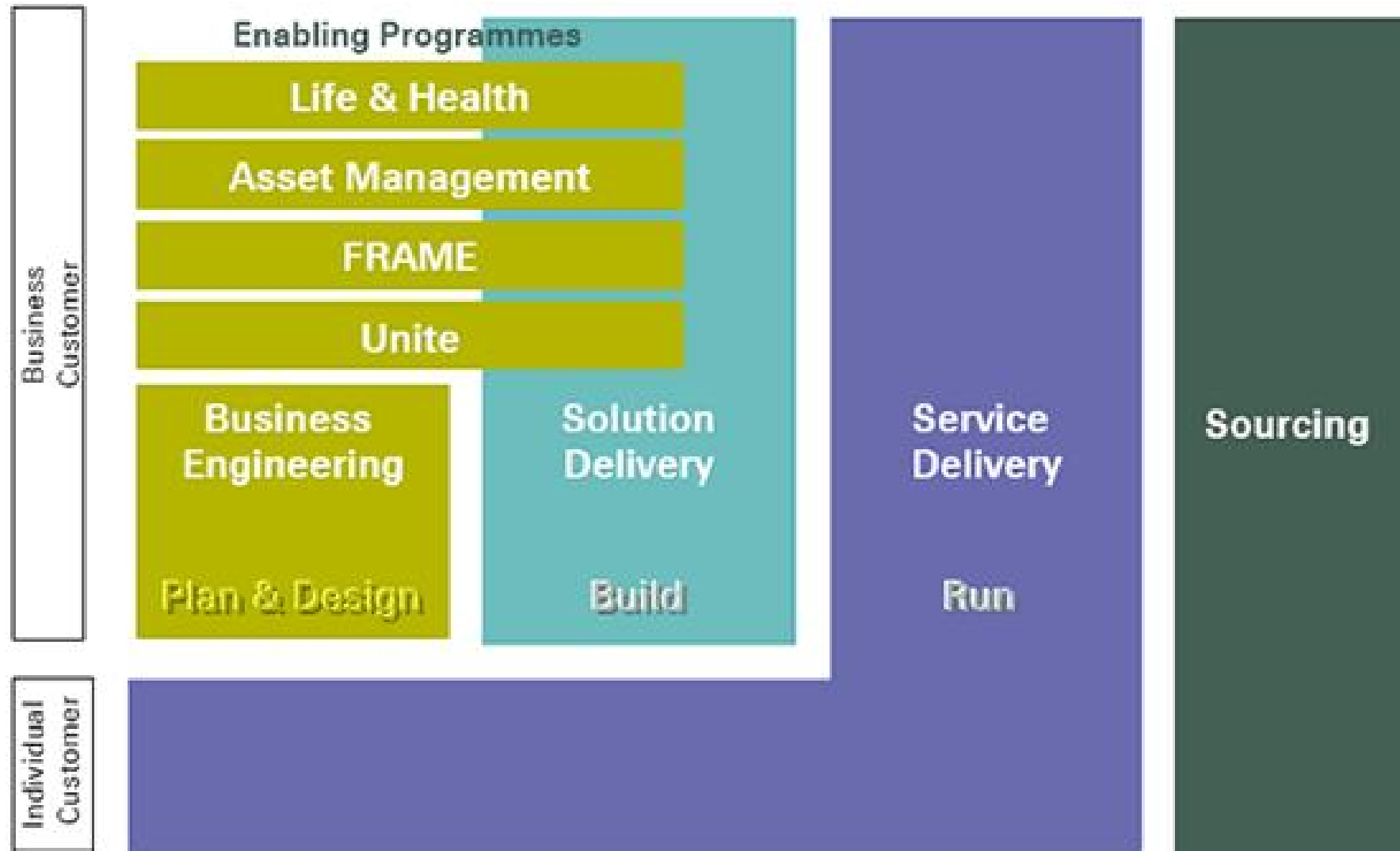
zEnterprise – einige Zahlen...

- 2 Sites (Site1, CPUA, Herdern and Site2, CPUB, Rümlang)
- 2 full-fledged IBM2817-M80 (a.k.a z196)
- 80 Processors (27 CPs, 10 ICFs, 5 IFLs, 25 zIIPs, 13 unused) each
- 3 Terrabytes memory each
- 2627 traditional MSUs, 2469 new workload MSUs each
- 6 OSA Gbe Adapter for z/OS each
- 4 10 Gbe Adapters for NETEZZAs each
- 7 LPARs each

zEnterprise Server - layout



IT Operating model and organisation



Risiken aus meiner Sicht

- Diebstahl vertraulicher Kundeninformationen, zum Beispiel Details bezüglich Lebensversicherungsverträgen
- Verkauf von Kundendaten, Vertragsdetails an Konkurrenz -> Wirtschaftsspionage
- Ausfall von IT-Infrastruktur -> Finanztransaktionen können nicht durchgeführt werden, Zinsverlust, empfindliche Strafen
Publikation von Quartals- oder Jahresergebnissen erfolgt nicht rechtzeitig -> Reputationsverlust
- Manipulation von Geschäftsbericht-relevanten Daten
- teilweise Ueberautorisierung von Administratoren führt zu Umgehung von definierten Prozessen
- dezentralisierte Security-Administration führt teilweise zu intransparenten oder fehlerhaften Definitionen



zSecure Business Case / technische Umsetzung

Business Case (wichtigste Punkte)

- Hauptfokus auf Integration in bestehendes Security-Umfeld, und operationelle Risiken, teilweise auf Reputationsrisiken hingewiesen
- granulare Vergabe und Real-Time Monitoring bei Verwendung von Administrationsrechten
- Kosten- und Komplexitätsreduktion der Security-Administration
- Aufräumen der RACF Datenbank ohne Produktionsausfälle
- Hohe Integration ins z/OS Umfeld – Nutzung des bestehenden Maintenance-Konzepts, Unterstützung oder mindestens tolerieren neuer RACF Funktionen bei GA
- verbesserte Qualität der Definitionen in der RACF Datenbank
- Return on Investment (ROI) konnte nur schwer ermittelt werden

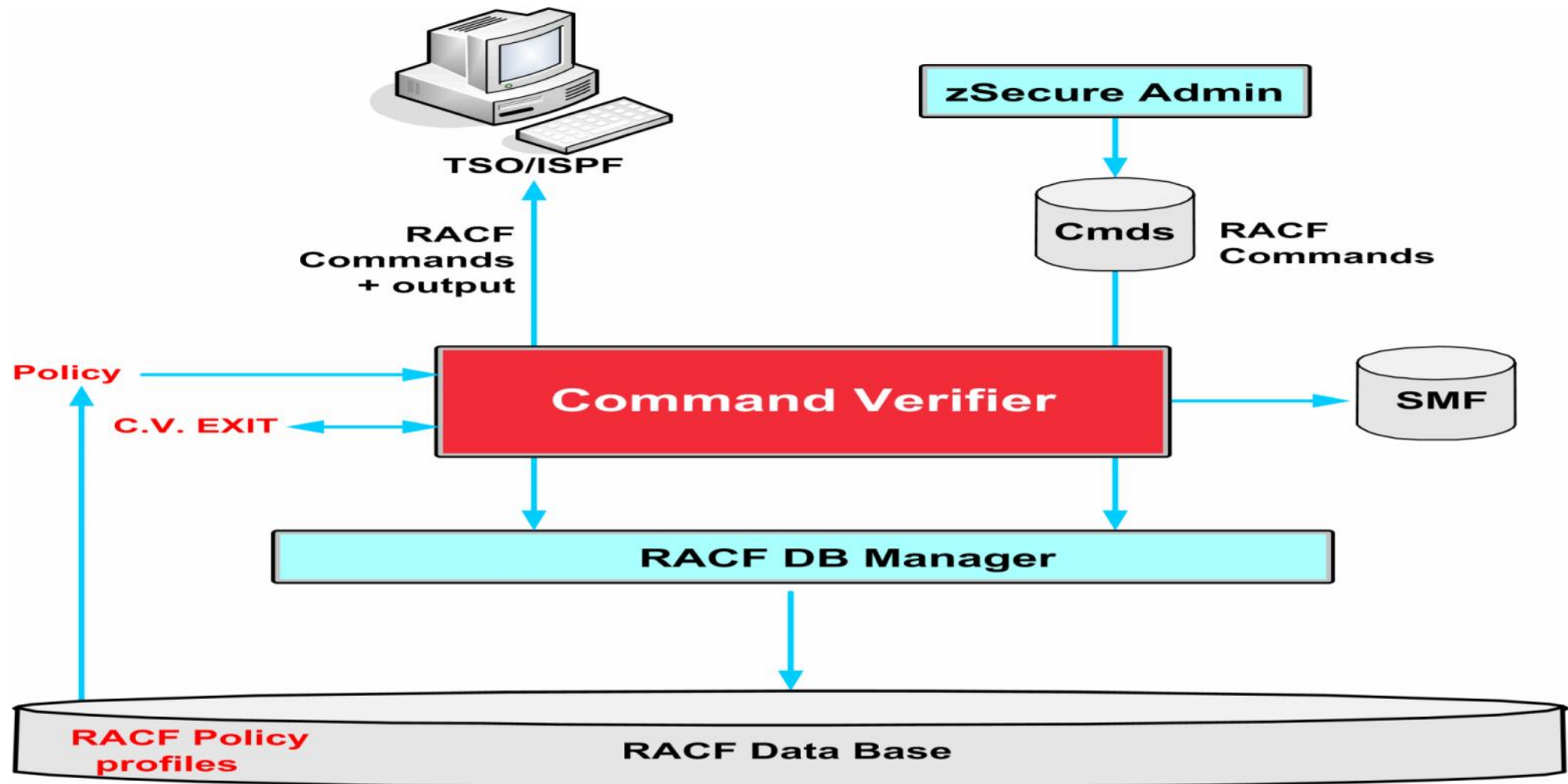
Welche Erfolge haben wir mit zSecure erzielt (1)

- Externer Auditor (IBM) ist in der Lage sich mittels zSecure Audit einen raschen Überblick über die Risiken im z/OS Umfeld zu verschaffen. Erstellung von Standard Audit-Reports anstelle Verwendung einer Vielzahl von selbstgestrickten Tools.
- zSecure Access Monitor wurde auf sämtlichen LPAR's implementiert und sammelt Daten für sämtliche erfolgten RACF Zugriffsprüfungen.
- Umstellung aller alten ITRM Reports auf zSecure abgeschlossen. Monatliches Reporting mit ~60 Detailreports.
- zSecure Alert für Realtime-Monitoring implementiert.

Welche Erfolge haben wir mit zSecure erzielt (2)

- Implementation von zSecure Command Verifier auf sämtlichen LPAR's erlaubt uns eine granulare Zuteilung von Administrationsrechten. Gewisse SETROPTS Optionen, welche in unserer Umgebung keinen Sinn machen oder sogar gefährlich sind wurden komplett unterbunden.
Qualität der RACF Definitionen wurde verbessert indem nun in systemnahen Klassen (FACILITY, OPERCMDS, ...) automatisch ein OWNER zugewiesen wird.
Die Verwendung von WARNING mode oder DATASET Profilen mit UACC>READ wurde unterbunden.
Aktivierung des "Command Audit Trail" erlaubt uns auf einfache Weise herauszufinden welche Änderungen an einem Account oder RACF Profile gemacht wurden.

Command Verifier Funktion



SETROPTS

Problem: gewisse SETROPTS Einstellungen sind sehr gefährlich,
werden nur einmal gesetzt oder machen überhaupt keinen Sinn

Lösung: Gewisse Optionen komplett unterbinden

- C4R.RACF.MLS.*
CONTROL SETROPTS MLS SETTINGS
- C4R.RACF.OPTION.ADDCREATOR
CONTROL SETROPTS (NO)ADDCREATOR OPTION
- C4R.RACF.OPTION.ADSP
CONTROL SETROPTS (NO)ADSP OPTION
- C4R.RACF.OPTION.EGN
CONTROL SETROPTS (NO)EGN OPTION
- C4R.RACF.OPTION.GRPLIST
CONTROL SETROPTS (NO)GRPLIST OPTION

CONTROLLED SPECIAL

- Problem: Storage Managers benötigen system wide SPECIAL

- Lösung:

C4R.PERMIT.=CTLSPEC	Cont. SPECIAL on PERMIT command
C4R.RDEFINE.=CTLSPEC	Cont. SPECIAL on RDEFINE command
C4R.\$BETA.ACL.*.**	
C4R.DASDVOL.ACL.*.**	
C4R.FACILITY.ACL.BETA.**	
C4R.FACILITY.ACL.FDRPAS.**	
C4R.FACILITY.ACL.STGADMIN.**	
C4R.MGMTCLAS.ACL.*.**	
C4R.STORCLAS.ACL.*.**	
C4R.DATASET.ACL.*.*.*.**	changes to any dataset profile

System SPECIAL kann dem Storage Management entzogen werden !

Schutz von speziellen Dataset profiles

- Problem: Modifikationen an DATASET profiles, welche APF autorisierte Datasets schützen, dürfen nur von einem eingeschränkten Personenkreis vorgenommen werden

- Lösung:

```
C4R.DATASET.=NOCHANGE.*.** APPLDATA(LEVEL=99)
```

```
ALTDSD 'TCPIP.SEZALOAD' LEVEL(99)
```

```
permit 'TCPIP.SEZALOAD' generic id(MVUSER) access(READ)
```

führt nun zu ➔

C4R646E Management of locked profiles not allowed, command terminated

Erlaube nur Gruppen in der Access Liste von Dataset Profiles

- Problem: Vergabe von Rechten auf Userid-Ebene ist unschön.
Rechte sollten nur an Gruppen vergeben werden.
- Lösung:
C4R.DATASET.ACL./GROUP.**

permit 'TCPIP.**' generic id(MVUSER) access(READ)

führt zu ➔

C4R602E ACL entry MVUSER is not a group, command terminated

Self-PERMIT auf Dataset Profiles durch Administratoren

- Problem: Administratoren können ihren eigenen Account in die Access-Liste von Dataset-Profiles eintragen
- Lösung:
`C4R.DATASET.ACL.=RACUID.**`

`permit 'TCPIP.**' generic id(own-user) access(READ)`

führt zu ➔

C4R607E ACL setting for self to READ not allowed, command terminated

Verhindern von UACC ALTER/UPDATE/CONTROL auf Dataset Profiles

- Problem: Mindestens UACC(ALTER/UPDATE/CONTROL) sind bei uns nicht mehr erwünscht. Auch UACC(READ) ist verpönt.
- Lösung:
`C4R.DATASET.UACC.ALTER.**`

`altdsd 'tcpip.**' uacc(alter)`

führt zu ➔

`C4R600E UACC ALTER setting not allowed, command terminated`

Automatisches hinzufügen von Schlüsselwörtern zu Commands

- Problem: Ausführen des LISTDSD commands ohne Schlüsselwort GENERIC macht normalerweise keinen Sinn
- Lösung:
C4R.LISTDSD.TYPE.AUTO.*.**

LISTDSD dataset(TCPIP.SEZALOAD)

führt zu ➔

C4R913I LISTDSD DATASET('TCPIP.SEZALOAD') GEN
INFORMATION FOR DATASET TCPIP.SEZALOAD (G)

...

Setzen von Passwörtern verhindern

- Problem: Bei bestimmten technischen Accounts darf auf keinen Fall das Passwort neu gesetzt werden
- Lösung:
C4R.USER.PASSWORD.*.\$SSLUSER

alu \$ssluser password(abcd123)

führt zu ➔

C4R496E Password management not allowed, command terminated

WARNING mode verhindern

- Problem: setzen von WARNING mode auf Profiles führt zu Security-Löchern
- Lösung:
C4R.*.ATTR.WARNING.**

altdsd 'tcpip.**' warning

führt zu ➔

C4R611E Warning mode not allowed, command terminated

Command Verifier – Audit Trail

C4R736I Command Audit Trail for USER SRZXXX

C4R739I Connect:	BDGTPUS Added on 10.117/12:05 by BLRXXX
C4R739I	CIC1WP3 Removed on 10.123/09:50 by SRZXXX
C4R739I	CIC1WP4 Removed on 10.123/09:50 by SRZXXX
C4R739I	CIC1PP3 Removed on 10.123/09:50 by SRZXXX
C4R739I	CIC1PP4 Removed on 10.123/09:50 by SRZXXX
C4R739I	CICAP1 Removed on 10.123/09:50 by SRZXXX
C4R739I	CIC10 Removed on 10.123/09:50 by SRZXXX
C4R739I	CIC11 Removed on 10.123/09:50 by SRZXXX
C4R739I	CIC13 Removed on 10.123/09:50 by SRZXXX
C4R739I	CIC14 Removed on 10.123/09:50 by SRZXXX
C4R739I	CIC14A Removed on 10.123/09:50 by SRZXXX
C4R739I	CIC14B Removed on 10.123/09:50 by SRZXXX
C4R739I	CIC14C Removed on 10.123/09:50 by SRZXXX

Aufbau IT Regulations Monitoring (alt)

- angesichts fehlender Vorgaben gemäss “best practice”
- mehrheitlich selbstgestrickte Lösung in Form von REXX, Assembler, DFSORT Routinen. Monatliche Reports mit hohem Detaillierungsgrad aber ungenügender Gesamtübersicht. Vorhande Risiken schlecht ersichtlich **und nicht** quantifizierbar
- verschiedenste Datenquellen für Reporting: SMF Sätze, RACF Database Offload, RACF Live Datenbank, ICHDSM, z/OS Kontrollblöcke, HFS Unload, zSecure Freeze Datasets
- 60 Reports in verschiedenen Kategorien (Basis Betriebssystem-Security, Qualitätsreporting, SMF-Auditing, PARMLIB-Änderungen, Zugriff auf kritische Betriebssystem-Services und Ressourcen (Commands, Tools, RACF-Datenbank, APF-Datasets)
- hohe Komplexität, fehleranfällig, hoher Aufwand für Anpassungen an verändertes Umfeld, neue Betriebssystemversionen, etc.

IT Regulations Monitoring - Reports

- Verify APF datasets
- Verify Setropts
- Inactive Accounts
- Accounts with residual data
- Highly privileged accounts (SPECIAL, OPERATIONS, AUDITOR)
- Accounts with weak passwords
- Profiles in warning mode
- Program Properties Table (PPT)
- RACF Exits
- Command security (OPERCMDS)
- USW.

Monatlicher HTML-Report für ITRM

E:\compliance-report-oct2012.html

<DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">

z/OS Compliance reporting summary for October 2012

System	Collection date and time
D1	30Oct2012 10:38
D2	30Oct2012 10:38
N1	30Oct2012 10:38
N2	30Oct2012 10:38
P1	30Oct2012 10:38
P2	30Oct2012 10:38
P3	30Oct2012 10:38
P4	30Oct2012 10:38
CHHCD001	9Nov2012 15:21

Report	Importance	Entries	Incorrect	Exception	Non-compliant	Description
1001	high	424	0	0	0	APF data sets: CHHCD001
1002	high	376	0	0	0	RACF SETROPTS settings: CHHCD001
1003	low	9335	8012	12	8000	Inactive users: CHHCD001
1004	low					No residual ids found
1005a	high	13	0	0	0	Privileged users: CHHCD001
1005b	high	65	0	0	0	Restricted administrators: CHHCD001
1006	medium	2	2	0	2	Weak passwords: CHHCD001
1008	medium	2625	1378	1378	0	Started task users: CHHCD001
1009	medium	11534	1197	2	1195	Elevated UACC value: CHHCD001
1010	high					No profiles in WARNING mode
1011	low	23738	22	0	22	Profiles with missing documentation: CHHCD001
1012	medium	48	0	0	0	LINKLST and LPALST data sets: CHHCD001
1013	medium					All systems have compliant attributes for IBM directories
1014	medium	124	0	0	0	Program properties: D1
1014	medium	124	0	0	0	Program properties: D2
1014	medium	124	0	0	0	Program properties: N1
1014	medium	124	0	0	0	Program properties: N2
1014	medium	124	0	0	0	Program properties: P1
1014	medium	124	0	0	0	Program properties: P2
1014	medium	124	0	0	0	Program properties: P3
1014	medium	124	0	0	0	Program properties: P4
1015	high	1147	0	0	0	System exits: CHHCD001

zSecure Alert

- Produkt wurde installiert und Customized. Es wurden auch Custom Alerts erstellt. Erstaunlich einfach zu installieren/verwenden.
- Alerts werden momentan noch per Email versendet.

Alert: Change to command verifier policy C4R.DEBUG
 Profile added/changed in class XFACILIT

Alert id	4300
Date and time	08Oct2010 13:49:25.71
Profile	C4R.DEBUG
User	SLCSP1 SCHMIDT MARCEL
Job name	SLCSP1
System ID	M1
Command	PERMIT C4R.DEBUG ACCESS(READ) CLASS(XFACILIT)
Command	ID(FCTS0099)

Alert policy

Id	Category	#alerts	#selected
1	User alerts	20	14
7	Group alerts	2	2
2	Data set alerts	12	11
3	General resource alerts	7	6
4	UNIX alerts	9	4
5	RACF control alerts	5	3
6	System alerts	17	6
0	Other alerts	3	2

Alert policy – User alerts (1)

Alert	Id	Sel
Logon by unknown user	1101	No
Logon with emergency userid	1102	No
Logon of a userid with UID(0) (Unix superuser)	1103	Yes
Highly authorized user revoked for pwd violatio	1104	Yes
System authority granted	1105	Yes
System authority removed	1106	Yes
Group authority granted	1107	Yes
Group authority removed	1108	No
SPECIAL authority used by non-SPECIAL user	1109	Yes
non-OPERATIONS user accessed data set with OPER	1110	Yes
Invalid password attempts exceed limit	1111	No

Alert policy – User alerts (2)

Password history flushed	1112	Yes
Suspect password changes	1113	No
Connect authority>=CREATE set	1114	No
Too many violations	1115	Yes
UID(0) assigned	4100	Yes
Superuser assigned	4101	Yes
Password of highly authorized user reset	4104	Yes
Invalid password attempts exceed limit	4111	Yes
Connect authority>=CREATE set	4114	Yes

Alert policy – Group alerts

Group alerts

Select the alert you want to work with.

The following line commands are available: A(Preview), C(opy), D(elete), E(dit), I(nsert), W(Who/Where), S(elect), U(nselect), B(rowse)

Alert	Id	Sel	gECSWU	CA	EM
Connect to an important group	1701	Yes	gE WU	Y	N
Remove from an important group	4701	Yes	gE WU	Y	N

Alert policy – Remove from an important group

```
Description . . Remove from an important group
Member prefix    RAC
Alert id . . . . 4701  Severity . . . . I  (I, W, E or S)
Data source . . SMF
Parameters . . .
Panel name . . . C2PP3ZBD  (Panel for additional customization)
```

Specify SMF records to be collected for this alert

```
Type Sub    Type Sub    Type Sub    Type Sub    Type Sub
80
```

Specify WTO filters for this alert

```
Prefix    Prefix    Prefix    Prefix    Prefix
```

```
Allowable destination types  /  E-mail  /  Cellphone  /  SNMP  /  WTO
                             /  Unix Syslog          /  Action command
```

```
Specify action . . . . . N  (Y/N)
```

```
Extended Monitoring alert . . N  (Y/N)
```

```
View/edit the alert skeleton      ISPF Skeleton RACS4701
```

Alert policy – Dataset alerts

Alert	Id	Sel
WARNING mode access on data set	1201	Yes
Setting UACC>=UPDATE on a DATASET profile	1202	Yes
Setting UACC>NONE on a DATASET profile	1203	Yes
Update on APF dataset	1204	Yes
Data set added to APF list	1205	Yes
Data set removed from APF list	1206	Yes
Data set addition to APF list detected	1207	Yes
Data set removal from APF list detected	1208	No
Setting WARNING mode on data set profile	4200	Yes
Update on PARMLIB dataset	4201	Yes
Update on sensitive program library	4202	Yes
Update on APF dataset (with member and volume)	4204	Yes

Alert policy – General resource alerts

Alert	Id	Sel
Catchall profile used for STC	1301	No
Audited program has been executed	1302	Yes
WARNING mode access on general resource	1303	Yes
Changing command verifier policy profile (XFACI	4300	Yes
Changes to system profiles (e.g. OPERCMDS, STAR	4301	Yes
Assignment of TRUSTED or PRIVILEGED attributes	4302	Yes
ID(*) specified on the PERMIT command	4303	Yes

Alert policy – Unix alerts

Alert	Id	Sel
UNIX file access violation	1401	Yes
Global write specified when altering file mode	1402	Yes
Global read specified when altering file mode	1403	Yes
Extended attribute changed (RACF event based)	1404	No
Audited UNIX program has been executed	1405	No
Superuser privileged UNIX program executed	1406	No
Superuser privileged shell obtained by user	1407	No
Superuser privileges set on UNIX program	1408	No
Extended attribute changed (UNIX event based)	1409	Yes

Alert policy – System alerts (1)

Alert	Id	Sel
SMF data loss started	1601	Yes
SMF logging resumed after failure	1602	Yes
SVC definition changed	1603	Yes
IBM Health Checker found low severity problem	1604	No
IBM Health Checker found medium severity problem	1605	Yes
IBM Health Checker found high severity problem	1606	Yes
SMF record flood detected	1607	No
SMF record flood starts dropping records	1608	No
IP attacks blocked by filter no longer logged	1609	No
IP attacks blocked by default filter no longer	1610	No
IP SMF 119 subtype no longer written	1611	No
IP filtering and IPsec tunnel support deactivat	1612	No

Alert policy – System alerts (2)

IP ports below 1024 no longer reserved	1613	No
IP interface security class changed	1614	No
IP filter rules changed	1615	No
SETPROG EXIT command issued	4601	Yes
EXIT definition changed	4603	No

Ausblick

- Umstellung der Audit Reports auf ISO 27000 geplant.
- laufender RACF cleanup anhand zSecure Access Monitor Daten
- Weiterleitung der Real-Time Monitoring Events (zSecure Alert) auf die Omnibus Infrastruktur (automatisches erstellen von Incident Tickets) anstelle von Emails
- Einführung von zSecure Admin für Helpdesk und Access Management im Q1 2013 (Passwort Reset)

Swiss Re



Thank you

Basic Copyright Notice & Disclaimer for Swiss Re Presentations provided to External Parties

©2009 Swiss Re. All rights reserved. You are not permitted to create any modifications or derivatives of this presentation without the prior written permission of Swiss Re.

This presentation is for information purposes only and contains non-binding indications as well as personal judgment. It does not contain any recommendation, advice, solicitation, offer or commitment to effect any transaction or to conclude any legal act. Any opinions or views expressed are of the author and do not necessarily represent those of Swiss Re. Swiss Re makes no warranties or representations as to this presentation's accuracy, completeness, timeliness or suitability for a particular purpose. Anyone shall at its own risk interpret and employ this presentation without relying on it in isolation.

In no event will Swiss Re or one of its affiliates be liable for any loss or damages of any kind, including any direct, indirect or consequential damages, arising out of or in connection with the use of this presentation.