Dr. Christoph Wall
electronic Administration and Services

Freie Universität Berlin

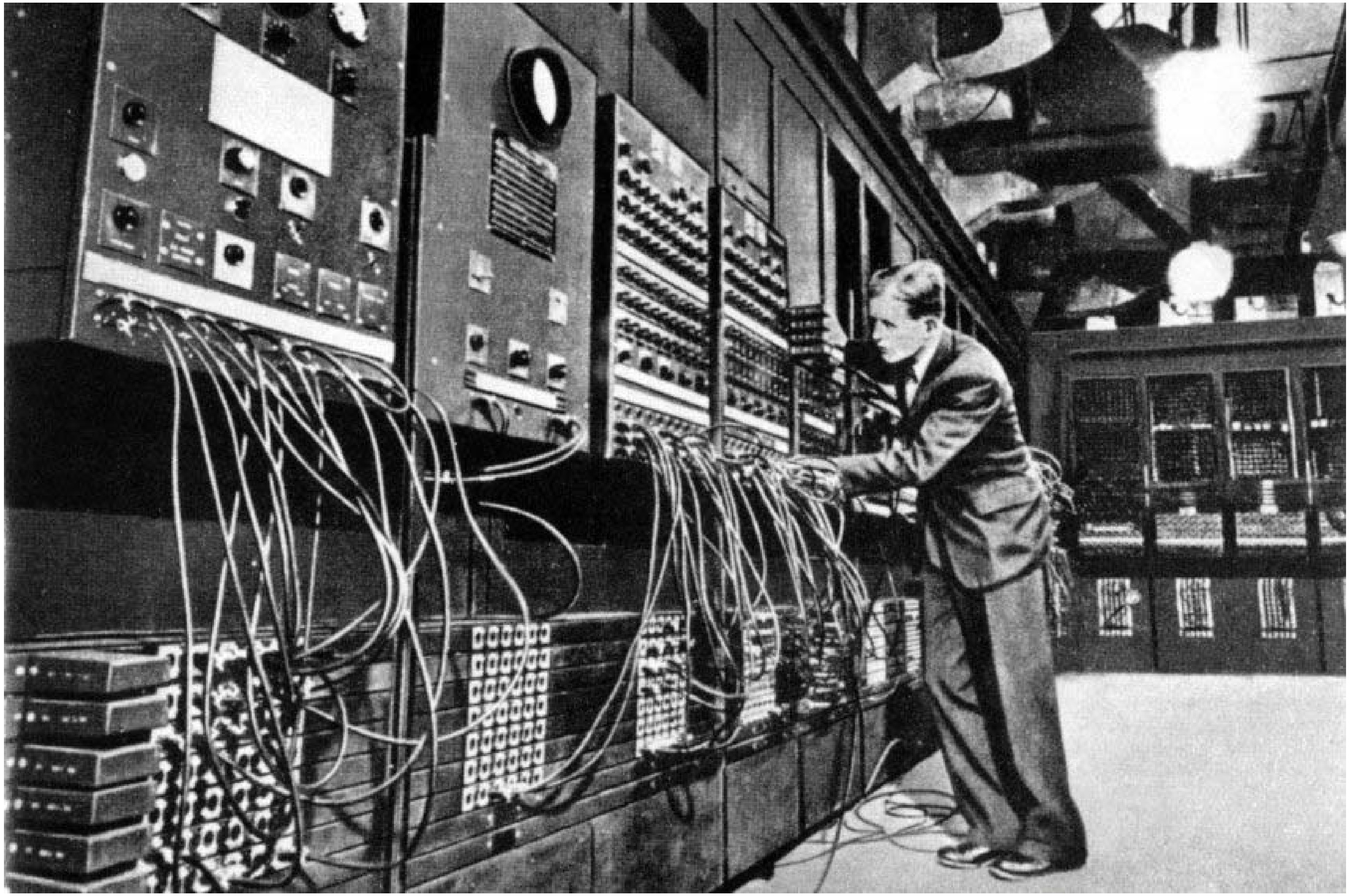
IT-Security

Governance and Technology

HERUG, 23.04.2013

Freie Universität Berlin

After computers got started …



… and went beyond their predicted numbers …

'I think there is a world market for about five computers'

Remark attributed to Thomas J. Watson (Chairman of the Board of IBM), 1943

… to connect people around the globe …

… I had a dream.

Can you picture what will be
So limitless and free

Jim Morrison

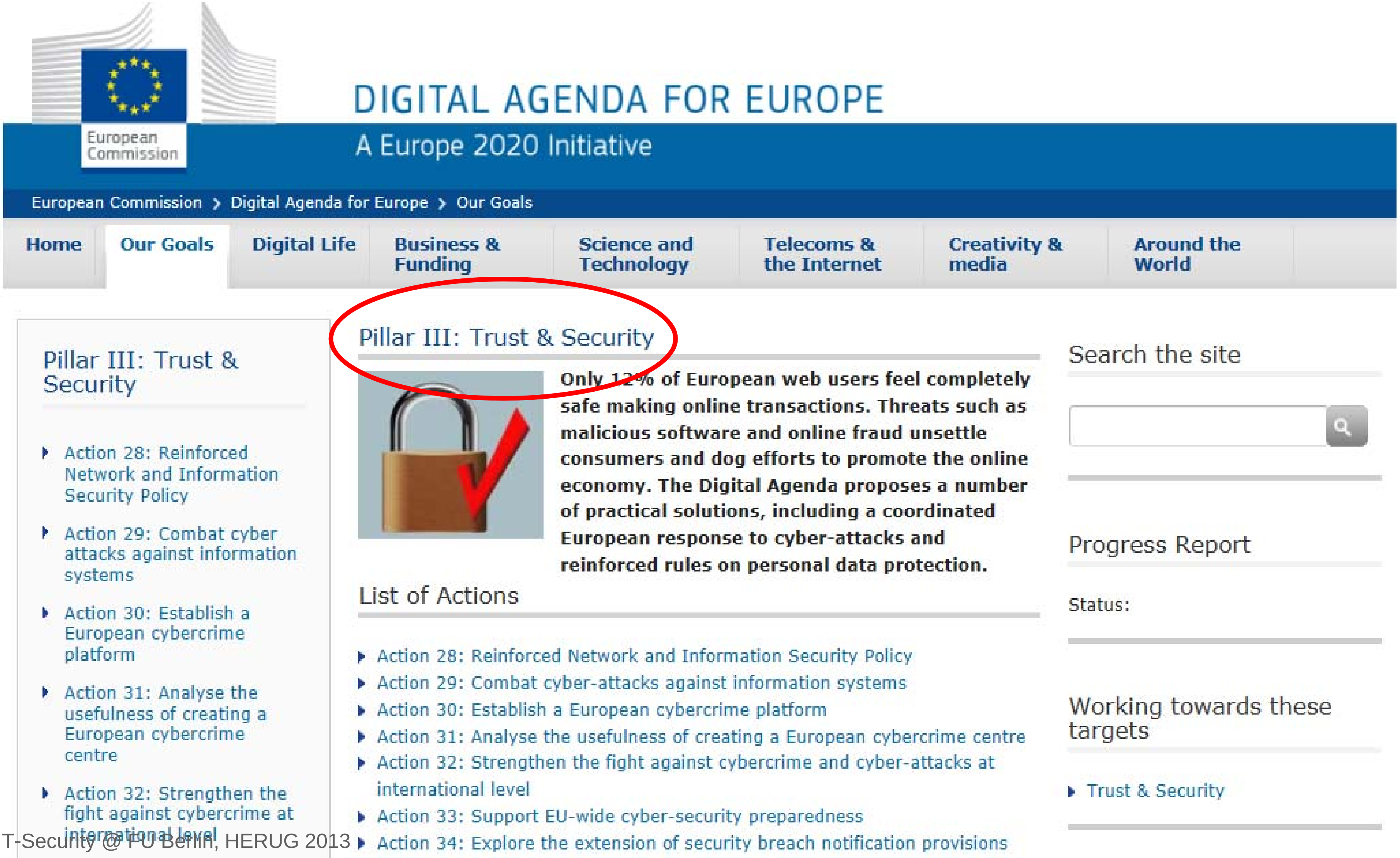
© Alessandro Bee (Italy)

But then I woke up …

© Bence Máté (Hungary)

… to find myself faced with the need for:

Europe needs it



DIGITAL AGENDA FOR EUROPE

A Europe 2020 Initiative

European Commission > Digital Agenda for Europe > Our Goals

Pillar III: Trust & Security

- Action 28: Reinforced Network and Information Security Policy
- Action 29: Combat cyber attacks against information systems
- Action 30: Establish a European cybercrime platform
- Action 31: Analyse the usefulness of creating a European cybercrime centre
- Action 32: Strengthen the fight against cybercrime at international level

Pillar III: Trust & Security

Only 12% of European web users feel completely safe making online transactions. Threats such as malicious software and online fraud unsettle consumers and dog efforts to promote the online economy. The Digital Agenda proposes a number of practical solutions, including a coordinated European response to cyber-attacks and reinforced rules on personal data protection.

List of Actions

- Action 28: Reinforced Network and Information Security Policy
- Action 29: Combat cyber-attacks against information systems
- Action 30: Establish a European cybercrime platform
- Action 31: Analyse the usefulness of creating a European cybercrime centre
- Action 32: Strengthen the fight against cybercrime and cyber-attacks at international level
- Action 33: Support EU-wide cyber-security preparedness
- Action 34: Explore the extension of security breach notification provisions

Search the site

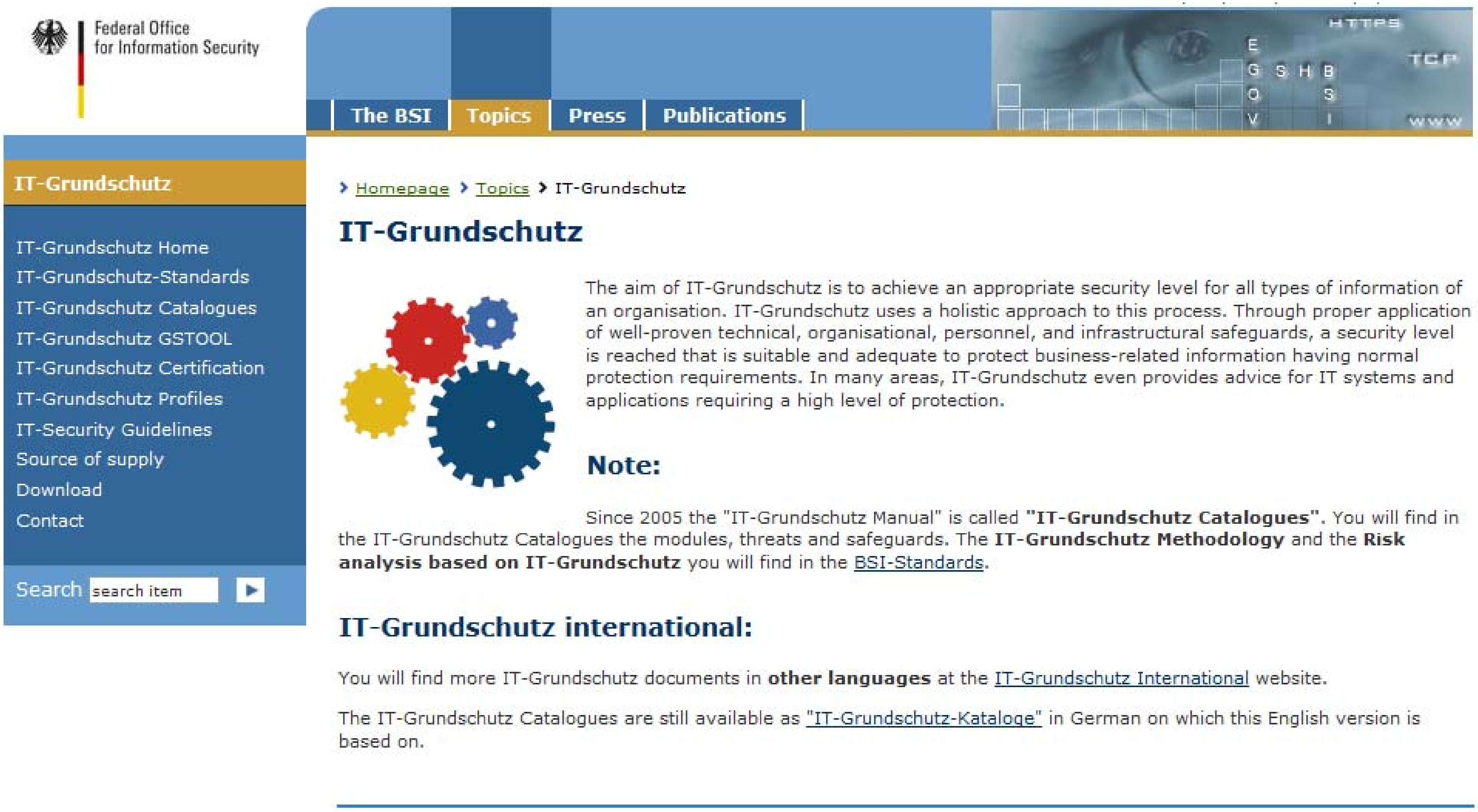
Progress Report

Status:

Working towards these targets

- Trust & Security

Germany needs it



IT-Grundschutz

The aim of IT-Grundschutz is to achieve an appropriate security level for all types of information of an organisation. IT-Grundschutz uses a holistic approach to this process. Through proper application of well-proven technical, organisational, personnel, and infrastructural safeguards, a security level is reached that is suitable and adequate to protect business-related information having normal protection requirements. In many areas, IT-Grundschutz even provides advice for IT systems and applications requiring a high level of protection.

Note:

Since 2005 the "IT-Grundschutz Manual" is called **"IT-Grundschutz Catalogues"**. You will find in the IT-Grundschutz Catalogues the modules, threats and safeguards. The **IT-Grundschutz Methodology** and the **Risk analysis based on IT-Grundschutz** you will find in the BSI-Standards.

IT-Grundschutz international:

You will find more IT-Grundschutz documents in **other languages** at the IT-Grundschutz International website.

The IT-Grundschutz Catalogues are still available as "IT-Grundschutz-Kataloge" in German on which this English version is based on.

The Freie Universität Berlin needs it

(IT Strategy)

Quality and Flexibility for Information and Processes

Comprehensive Offer of Information

Mobile Information

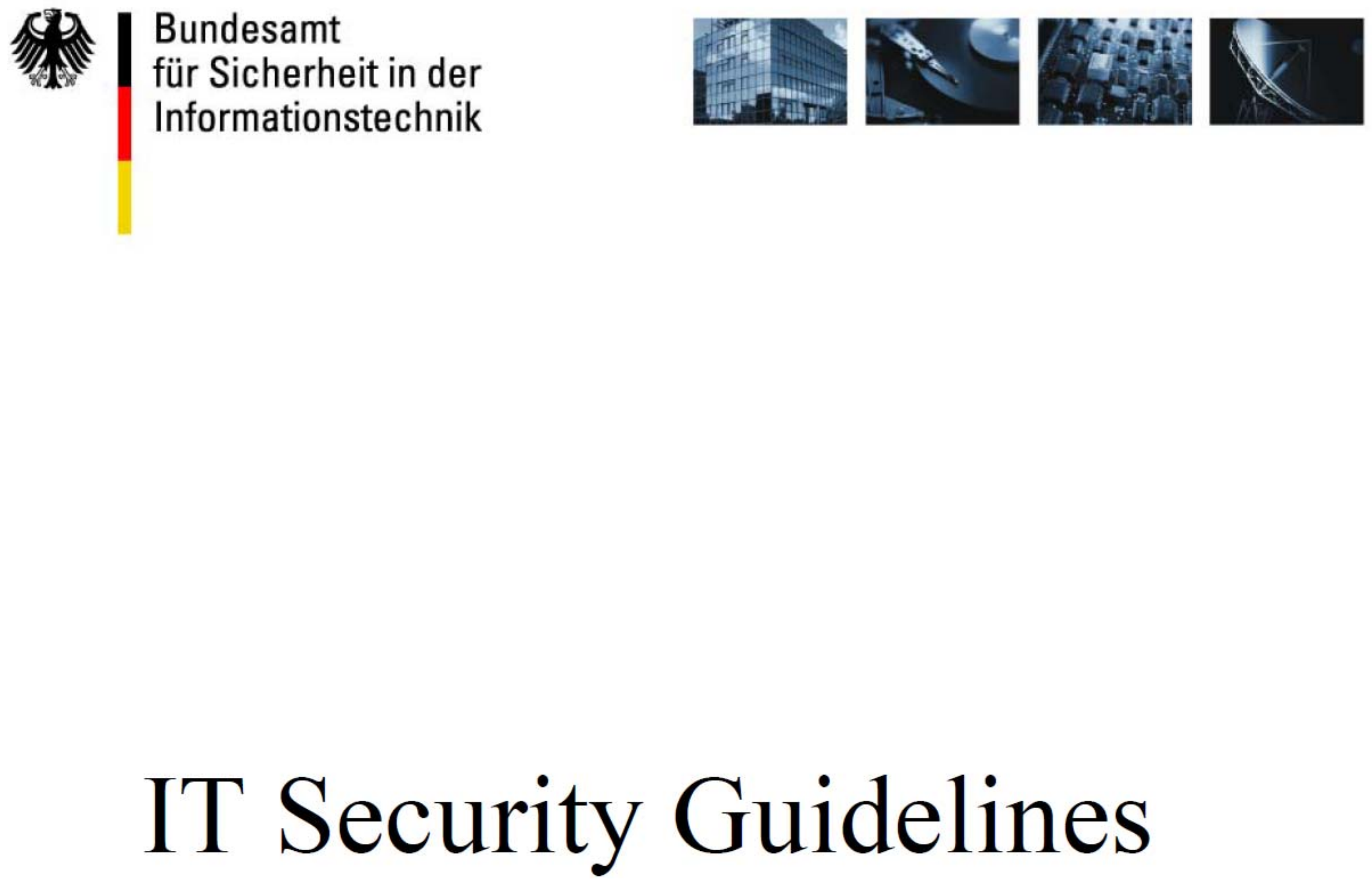
Smart Processes

Secure Data

Sustainable Use of Resources

Content Users

What is IT-Security?



Bundesamt
für Sicherheit in der
Informationstechnik

IT Security Guidelines

Fundamental Values of IT-Security

Confidentiality:

information that is confidential must be protected against unauthorized disclosure

Availability:

services, IT system functions, data and information must be available to users as required

Integrity:

data must be complete and unaltered

Elements of an IT-Security-Management-System

Governance

Risk assessment or analysis: A risk analysis provides information on the probability of the occurrence of a damaging event and what negative consequences the damage would have.

Security policy: In a security policy the security objectives and general security safeguards are formulated in the sense of the *official regulations of a company* or a public authority. Detailed security safeguards are contained in a more comprehensive security concept.

Technical

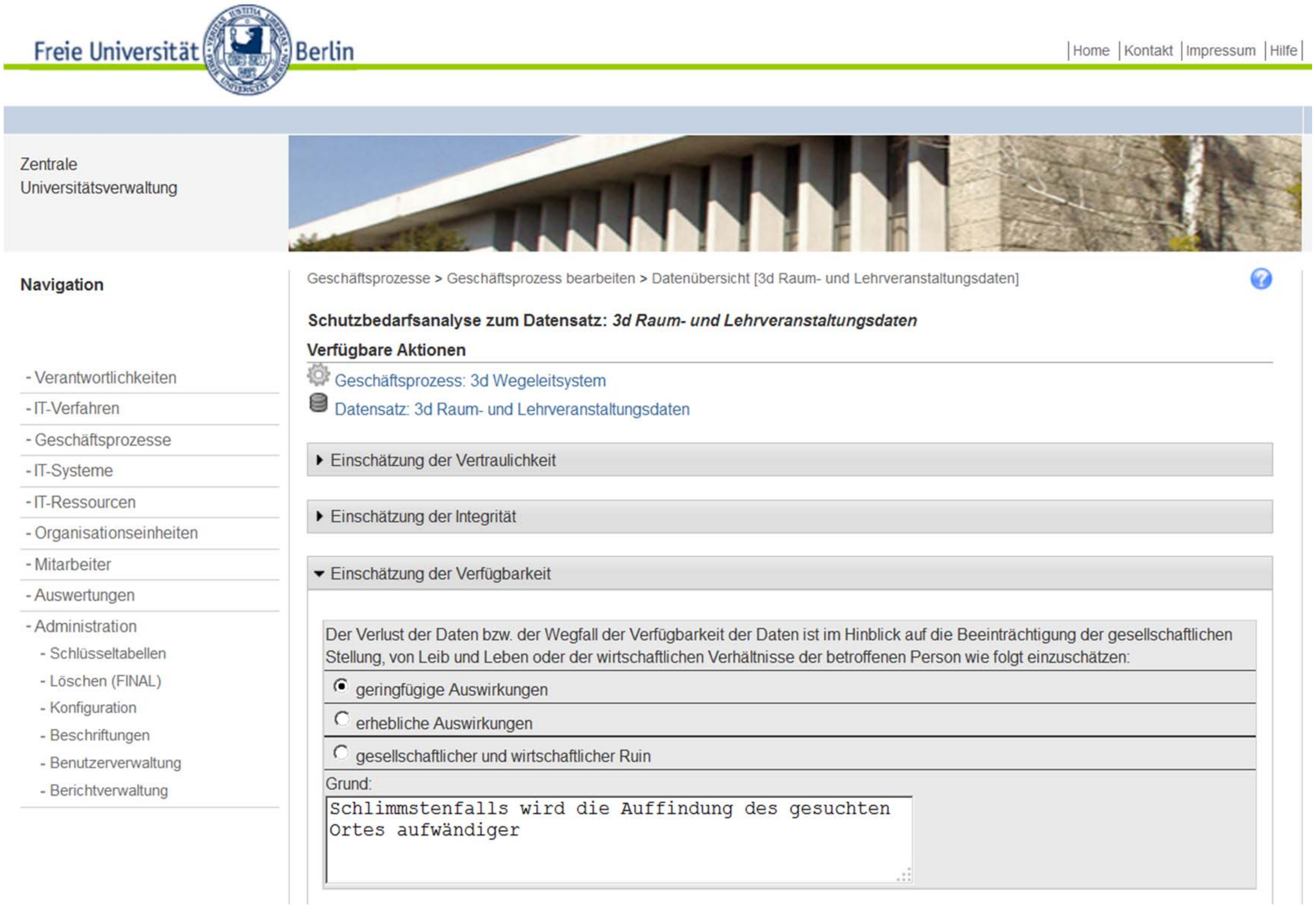
Authentication: When a person logs in on a system, the system runs a check in an authentication process to verify the identity of the person. The term is also used when the identity of IT components or applications is tested.

Authorisation: Authorisation is the process of checking whether a person, an IT component or an application is authorised to perform a specific action.

Data protection: Data protection refers to the protection of personal data against misuse by third parties.

Data backup: Data backup involves making copies of existing data to prevent its loss.

Governance:
Risk assessment for FU IT-Systems



Schutzbedarfsanalyse zum Datensatz: ***3d Raum- und Lehrveranstaltungsdaten***

Verfügbare Aktionen

Geschäftsprozess: 3d Wegeleitsystem

Datensatz: 3d Raum- und Lehrveranstaltungsdaten

▸ Einschätzung der Vertraulichkeit

▸ Einschätzung der Integrität

▾ Einschätzung der Verfügbarkeit

Der Verlust der Daten bzw. der Wegfall der Verfügbarkeit der Daten ist im Hinblick auf die Beeinträchtigung der gesellschaftlichen Stellung, von Leib und Leben oder der wirtschaftlichen Verhältnisse der betroffenen Person wie folgt einzuschätzen:

● geringfügige Auswirkungen

○ erhebliche Auswirkungen

○ gesellschaftlicher und wirtschaftlicher Ruin

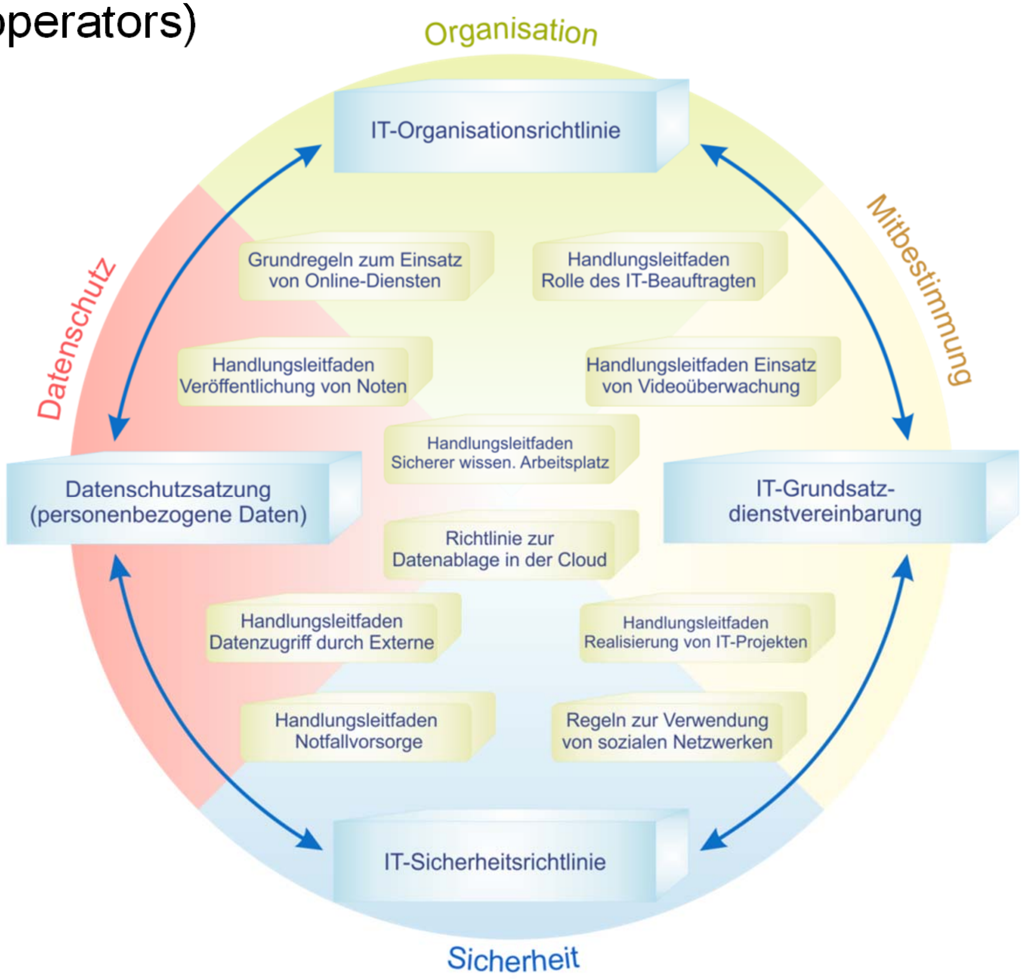
Grund:

```
Schlimmstenfalls wird die Auffindung des gesuchten
Ortes aufwändiger
```

Governance: Guidelines and Directives

"Essentially, procedures or policies are implemented to tell people (administrators, users and operators) how to use products to ensure information security within the organization."

Wikipedia


Organisation
IT-Organisationsrichtlinie
Mitbestimmung
Datenschutz
Grundregeln zum Einsatz von Online-Diensten
Handlungsleitfaden Rolle des IT-Beauftragten
Handlungsleitfaden Veröffentlichung von Noten
Handlungsleitfaden Einsatz von Videoüberwachung
Handlungsleitfaden Sicherer wissen. Arbeitsplatz
Datenschutzsatzung (personenbezogene Daten)
IT-Grundsatz-dienstvereinbarung
Richtlinie zur Datenablage in der Cloud
Handlungsleitfaden Datenzugriff durch Externe
Handlungsleitfaden Realisierung von IT-Projekten
Handlungsleitfaden Notfallvorsorge
Regeln zur Verwendung von sozialen Netzwerken
IT-Sicherheitsrichtlinie
Sicherheit

Freie Universität Berlin

„ Guideline for the IT-Organization at Freie Universität Berlin“

IT-Organisationsrichtlinie
für die
Freie Universität Berlin

Version 2.4.1

Juni 2009

Stakeholders of the IT-Organization

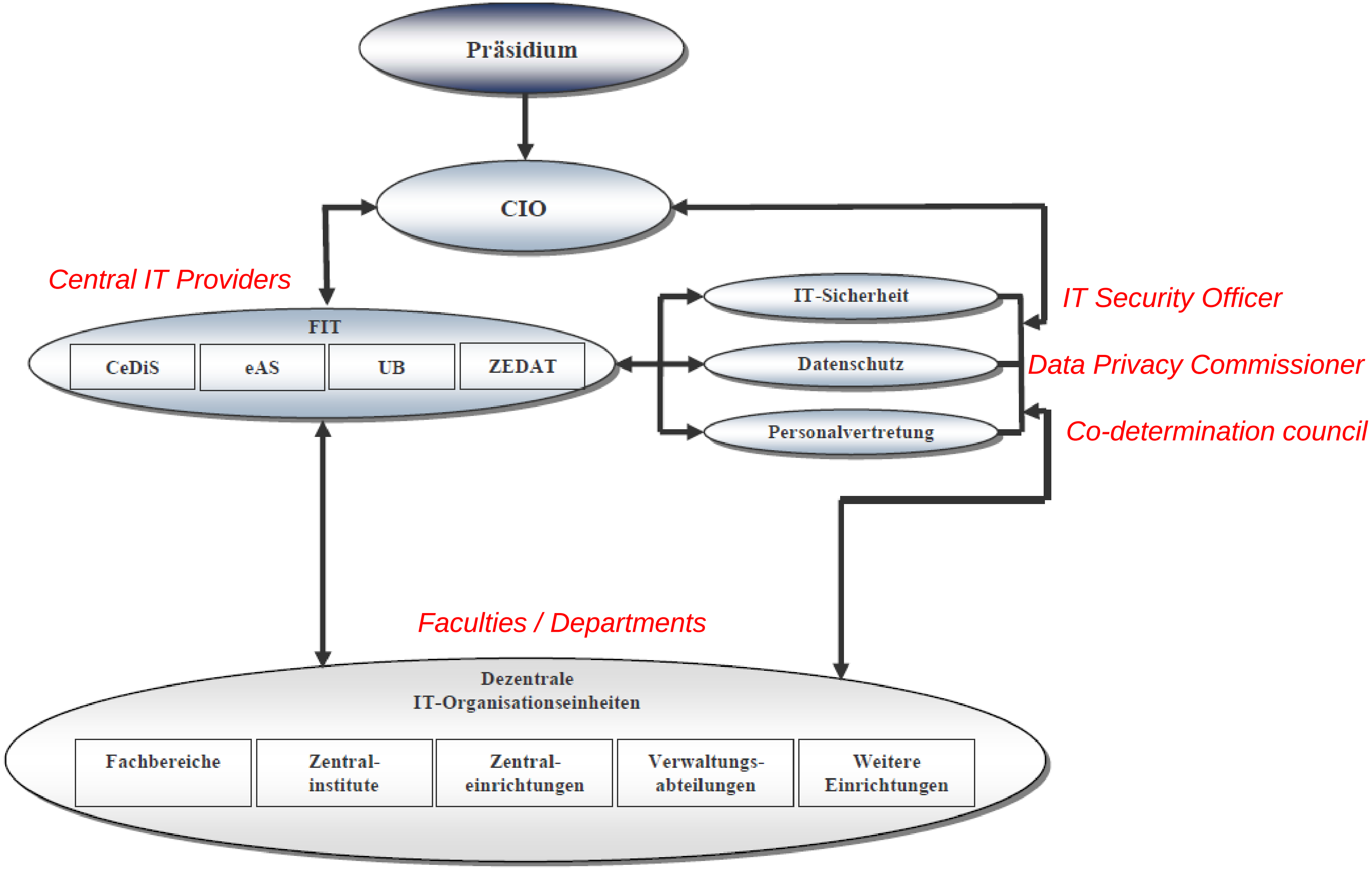
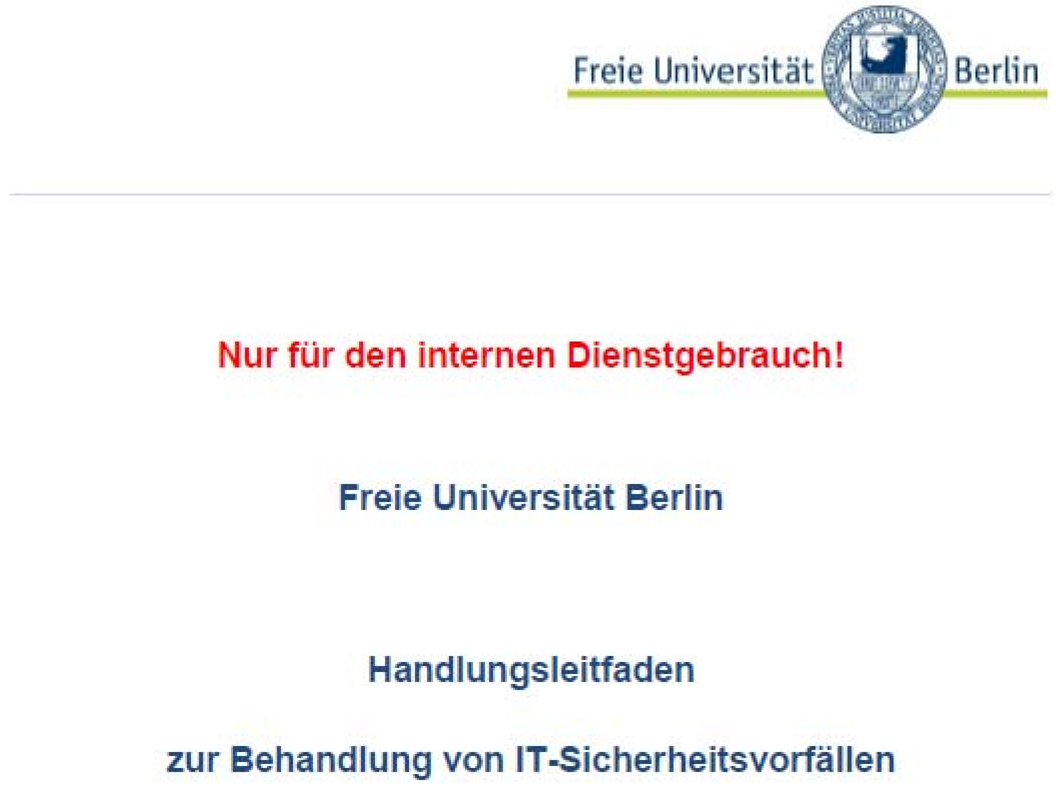


Abbildung 1: Darstellung der IT-Organisationsstruktur an der Freien Universität Berlin. Die Pfeile weisen auf operative Beziehungen hin.

Directive for handling security incidents



Freie Universität Berlin

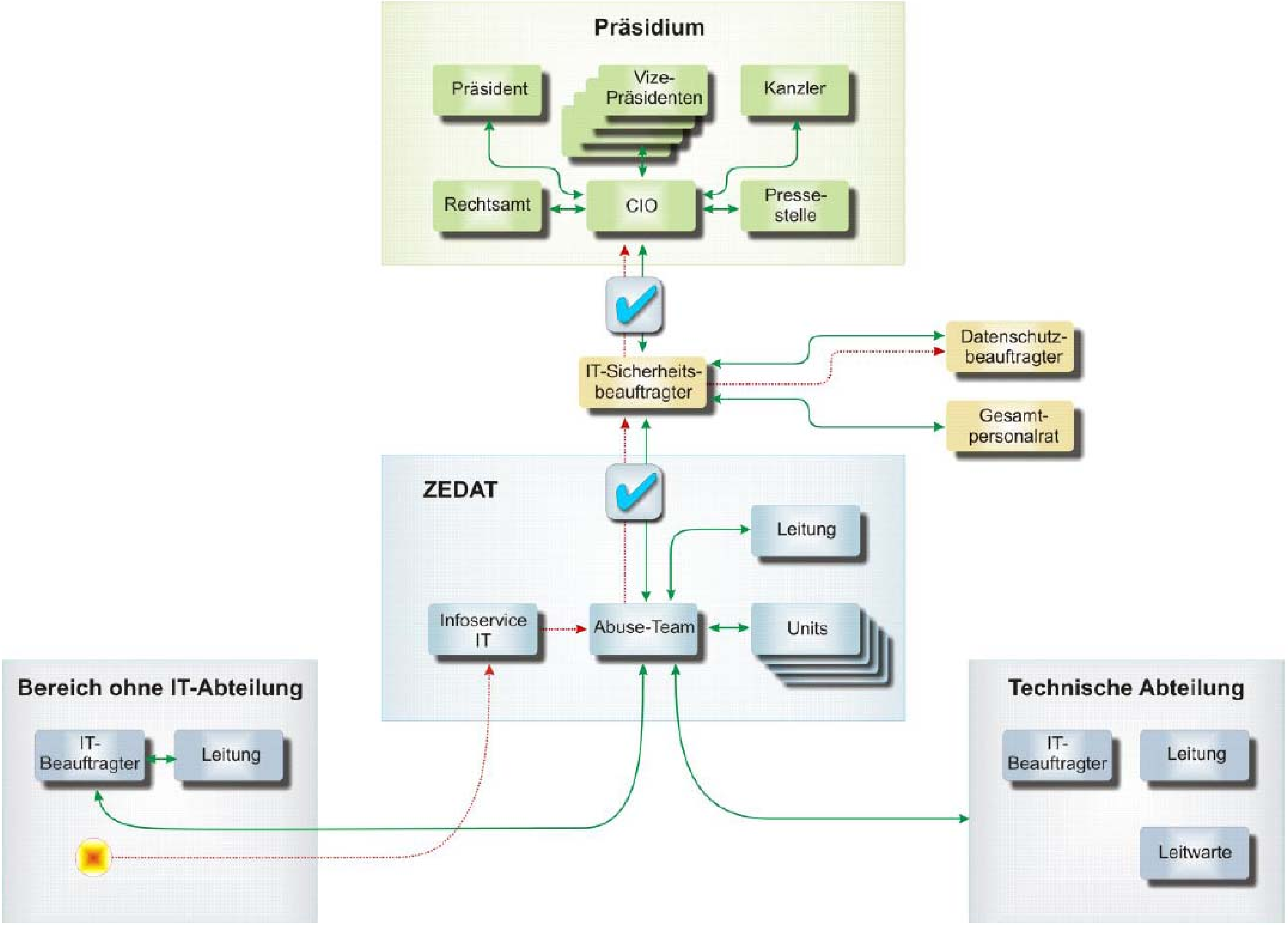
Nur für den internen Dienstgebrauch!

Freie Universität Berlin

Handlungsleitfaden

zur Behandlung von IT-Sicherheitsvorfällen

Alarm chain

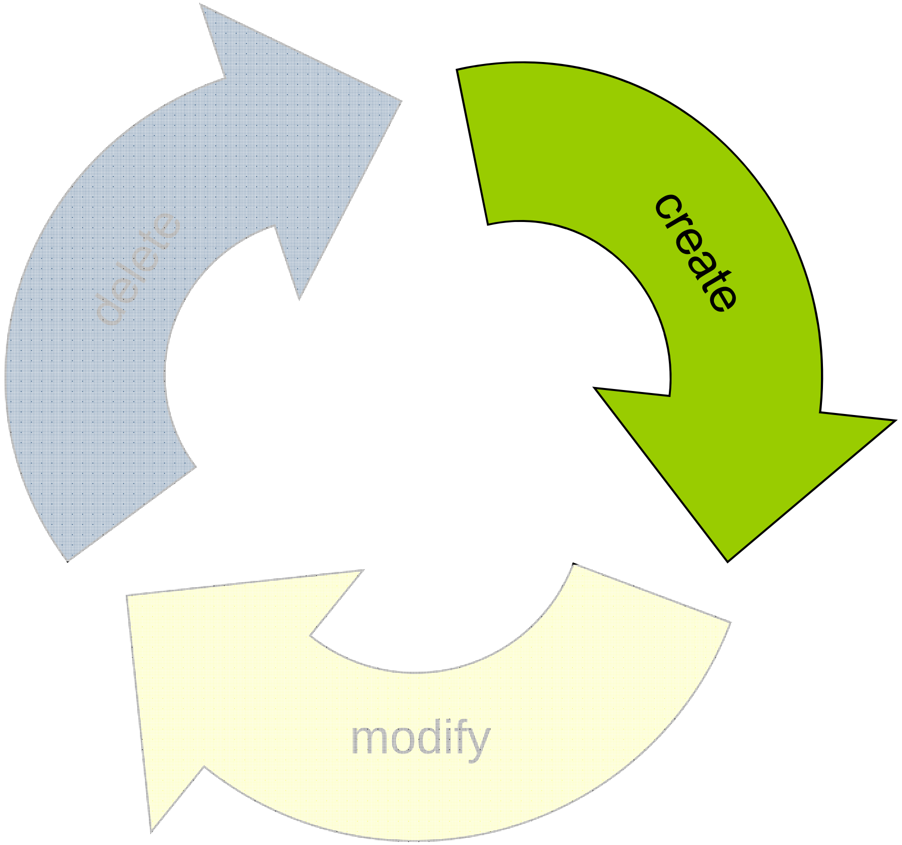

Präsidium
Präsident
Vize-Präsidenten
Kanzler
Rechtsamt
CIO
Presse-stelle
Datenschutz-beauftragter
IT-Sicherheits-beauftragter
Gesamt-personalrat
ZEDAT
Leitung
Infoservice IT
Abuse-Team
Units
Bereich ohne IT-Abteilung
IT-Beauftragter
Leitung
Technische Abteilung
IT-Beauftragter
Leitung
Leitwarte

Technology:
SAP Functionality to support IT-Security

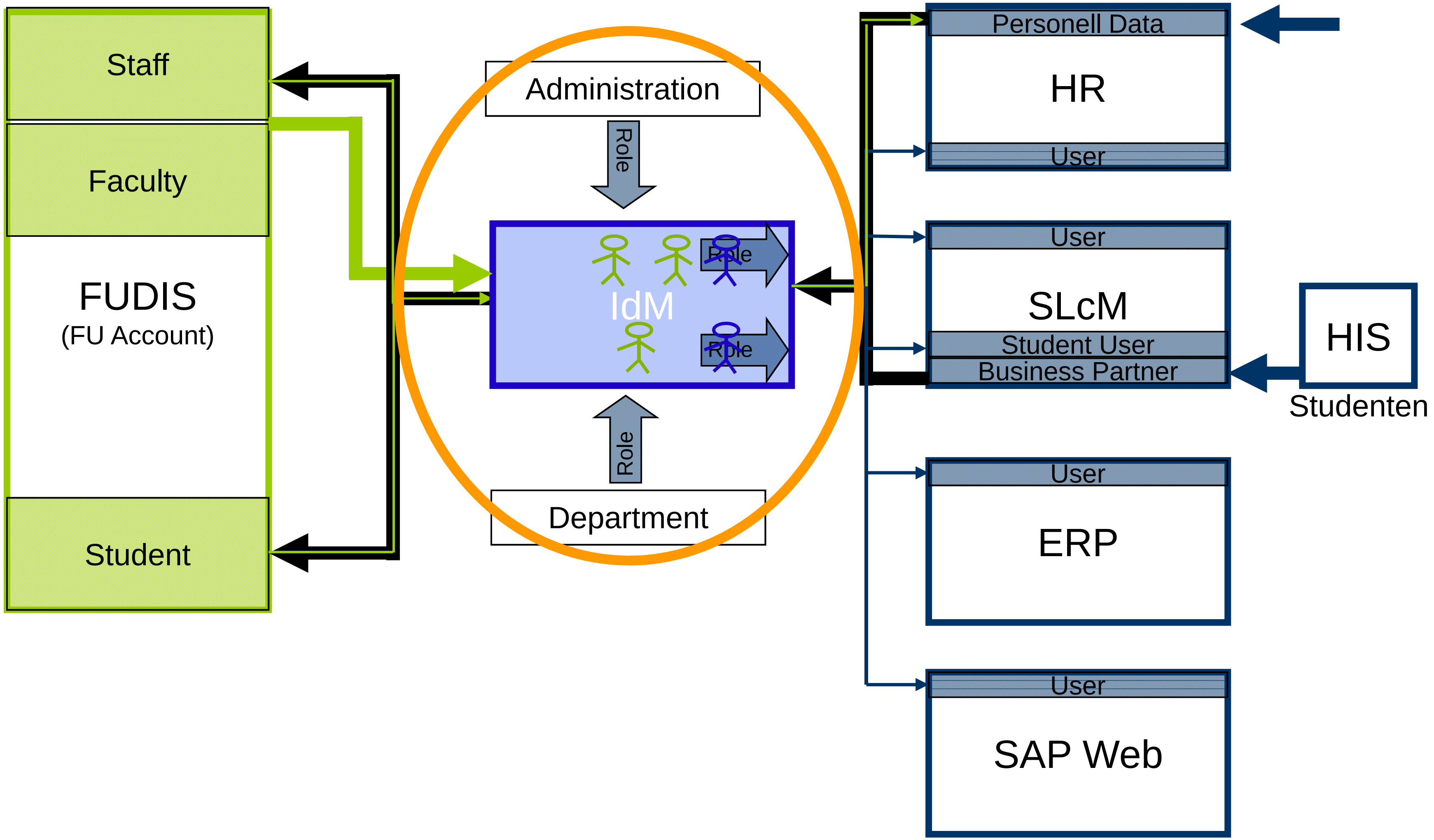
- Identity Management
  - Event-based onboarding
- Authentification
  - SSO with User Name/Password
- Role based Authorization
  - Design of User-Roles
  - Workflow for role allocation
- Layers of security for Web-Portal-Access to SAP backend
- Security Optimazation Self-Service (SOS Report)
  - e.g. Segregation of duties
- Action log for intrusion detection
- Identity Management
  - Automatic user deactivation
- Backup and Restore Support

Identity Management

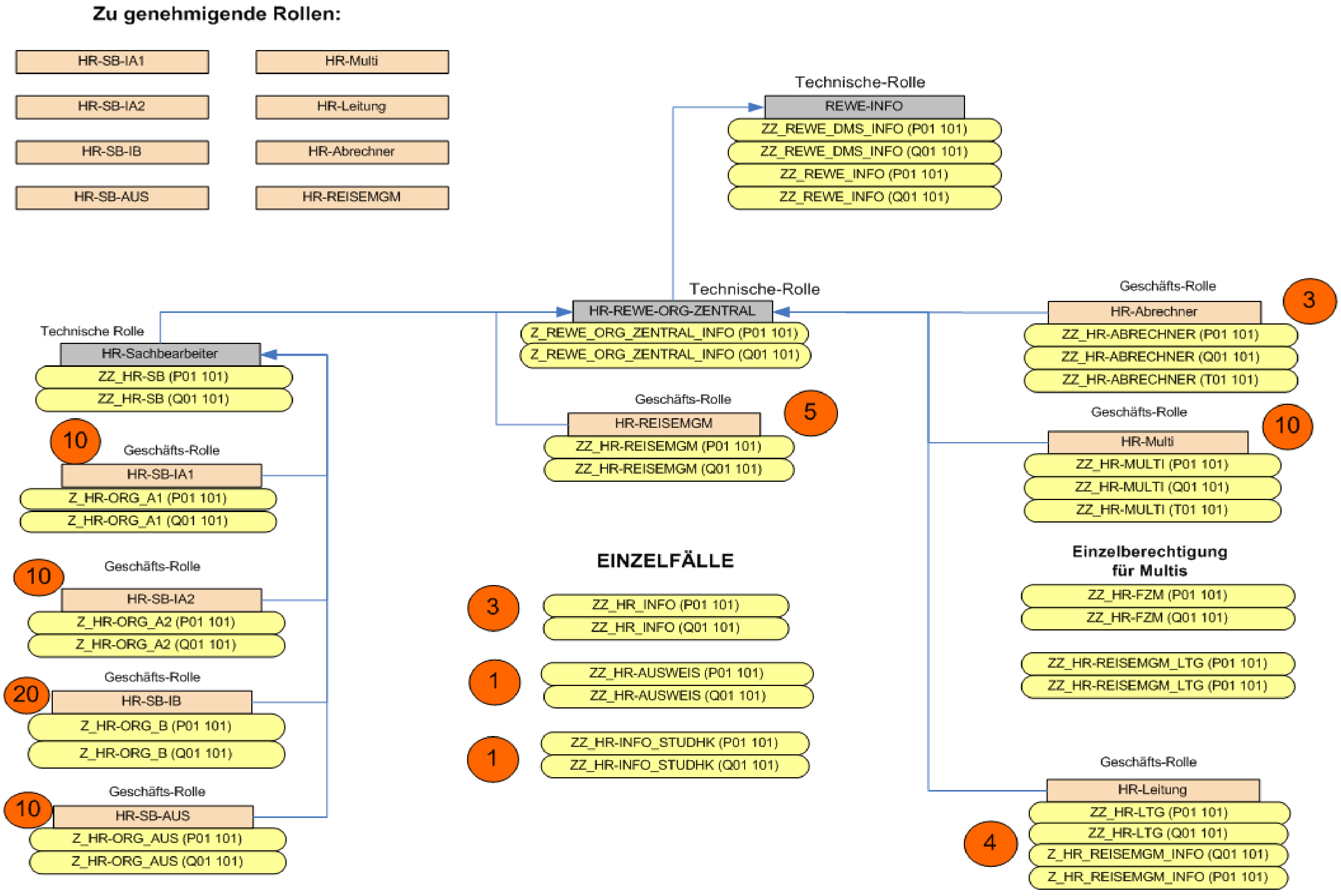
User Lifecycle Management Stage 1



Create/modify (Onboarding & Berechtigung)



Cascading role design



Zu genehmigende Rollen:

HR-SB-IA1	HR-Multi
HR-SB-IA2	HR-Leitung
HR-SB-IB	HR-Abrechner
HR-SB-AUS	HR-REISEMGM

Technische-Rolle
REWE-INFO
ZZ_REWE_DMS_INFO (P01 101)
ZZ_REWE_DMS_INFO (Q01 101)
ZZ_REWE_INFO (P01 101)
ZZ_REWE_INFO (Q01 101)

Technische-Rolle
HR-REWE-ORG-ZENTRAL
Z_REWE_ORG_ZENTRAL_INFO (P01 101)
Z_REWE_ORG_ZENTRAL_INFO (Q01 101)

Technische Rolle
HR-Sachbearbeiter
ZZ_HR-SB (P01 101)
ZZ_HR-SB (Q01 101)

10 Geschäfts-Rolle
HR-SB-IA1
Z_HR-ORG_A1 (P01 101)
Z_HR-ORG_A1 (Q01 101)

10 Geschäfts-Rolle
HR-SB-IA2
Z_HR-ORG_A2 (P01 101)
Z_HR-ORG_A2 (Q01 101)

20 Geschäfts-Rolle
HR-SB-IB
Z_HR-ORG_B (P01 101)
Z_HR-ORG_B (Q01 101)

10 Geschäfts-Rolle
HR-SB-AUS
Z_HR-ORG_AUS (P01 101)
Z_HR-ORG_AUS (Q01 101)

5 Geschäfts-Rolle
HR-REISEMGM
ZZ_HR-REISEMGM (P01 101)
ZZ_HR-REISEMGM (Q01 101)

EINZELFÄLLE

3
ZZ_HR_INFO (P01 101)
ZZ_HR_INFO (Q01 101)

1
ZZ_HR-AUSWEIS (P01 101)
ZZ_HR-AUSWEIS (Q01 101)

1
ZZ_HR-INFO_STUDHK (P01 101)
ZZ_HR-INFO_STUDHK (Q01 101)

3 Geschäfts-Rolle
HR-Abrechner
ZZ_HR-ABRECHNER (P01 101)
ZZ_HR-ABRECHNER (Q01 101)
ZZ_HR-ABRECHNER (T01 101)

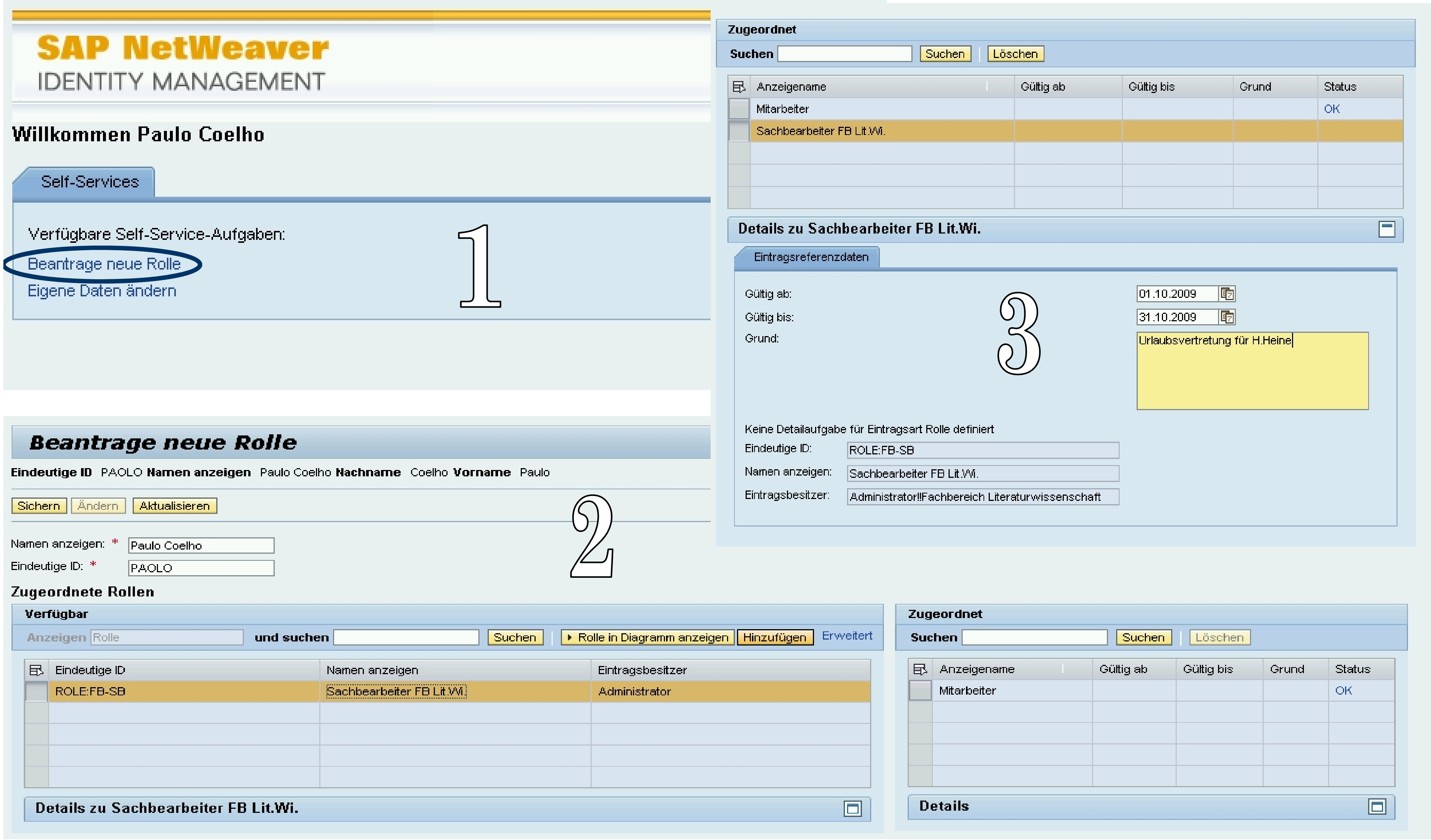
10 Geschäfts-Rolle
HR-Multi
ZZ_HR-MULTI (P01 101)
ZZ_HR-MULTI (Q01 101)
ZZ_HR-MULTI (T01 101)

Einzelberechtigung für Multis
ZZ_HR-FZM (P01 101)
ZZ_HR-FZM (Q01 101)

ZZ_HR-REISEMGM_LTG (P01 101)
ZZ_HR-REISEMGM_LTG (P01 101)

4 Geschäfts-Rolle
HR-Leitung
ZZ_HR-LTG (P01 101)
ZZ_HR-LTG (Q01 101)
Z_HR_REISEMGM_INFO (Q01 101)
Z_HR_REISEMGM_INFO (P01 101)

IdM role provisioning workflow



SAP NetWeaver
IDENTITY MANAGEMENT

Willkommen Paulo Coelho

Self-Services

Verfügbare Self-Service-Aufgaben:

Beantrage neue Rolle

Eigene Daten ändern

Beantrage neue Rolle

Eindeutige ID PAOLO **Namen anzeigen** Paulo Coelho **Nachname** Coelho **Vorname** Paulo

Sichern | Ändern | Aktualisieren

Namen anzeigen: * Paulo Coelho

Eindeutige ID: * PAOLO

Zugeordnete Rollen

Verfügbar

Anzeigen Rolle **und suchen** Suchen | Rolle in Diagramm anzeigen | Hinzufügen | Erweitert

Eindeutige ID	Namen anzeigen	Eintragsbesitzer
ROLE:FB-SB	Sachbearbeiter FB Lit.Wi.	Administrator

Details zu Sachbearbeiter FB Lit.Wi.

Zugeordnet

Suchen Suchen | Löschen

Anzeigename	Gültig ab	Gültig bis	Grund	Status
Mitarbeiter				OK

Details

Zugeordnet

Suchen Suchen | Löschen

Anzeigename	Gültig ab	Gültig bis	Grund	Status
Mitarbeiter				OK
Sachbearbeiter FB Lit.Wi.				

Details zu Sachbearbeiter FB Lit.Wi.

Eintragsreferenzdaten

Gültig ab: 01.10.2009

Gültig bis: 31.10.2009

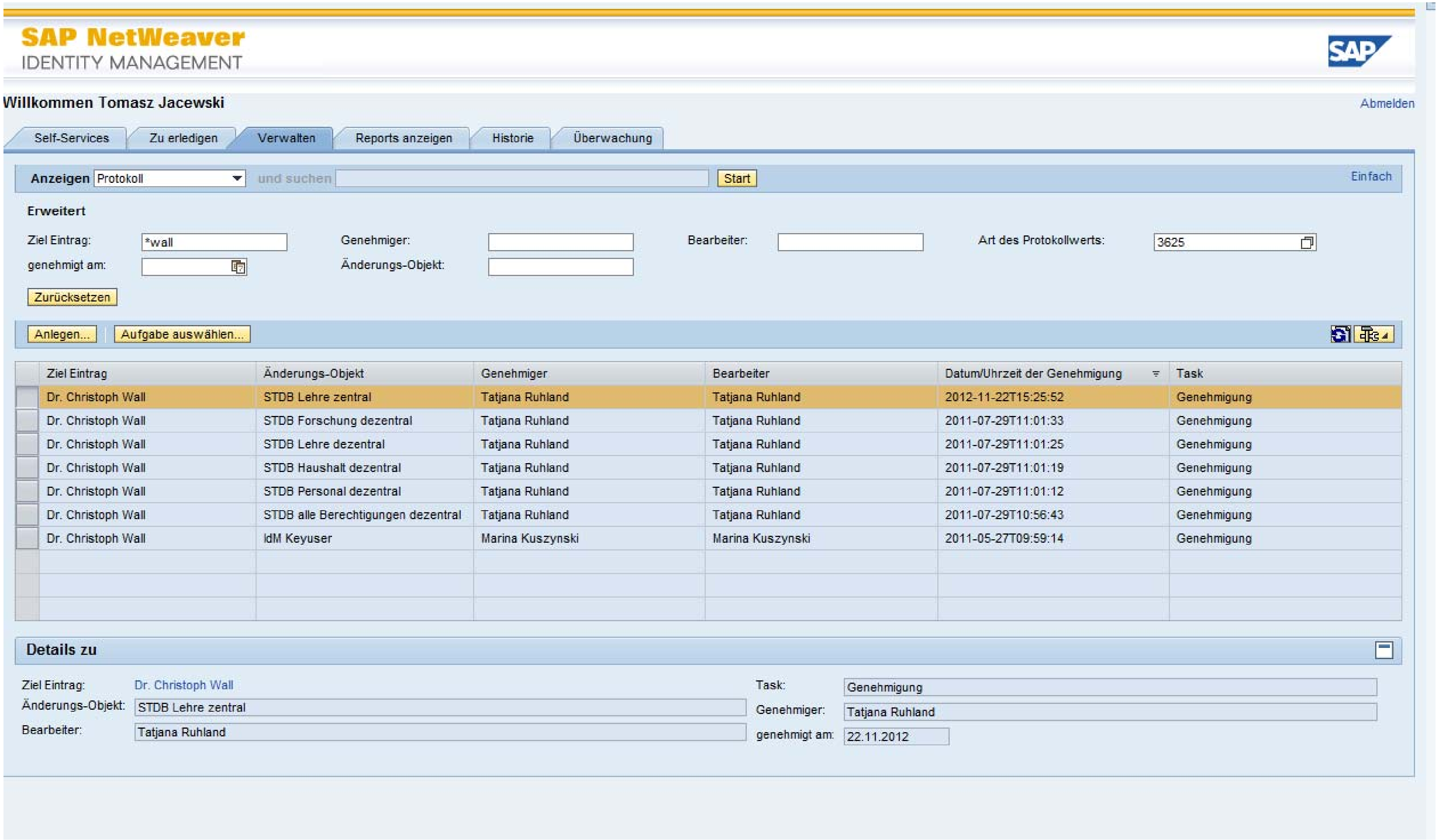
Grund: Urlaubsvertretung für H.Heine

Keine Detailaufgabe für Eintragsart Rolle definiert

Eindeutige ID: ROLE:FB-SB

Namen anzeigen: Sachbearbeiter FB Lit.Wi.

Eintragsbesitzer: Administrator!!Fachbereich Literaturwissenschaft



Willkommen Tomasz Jacewski

Anzeigen: Protokoll und suchen Start

Erweitert

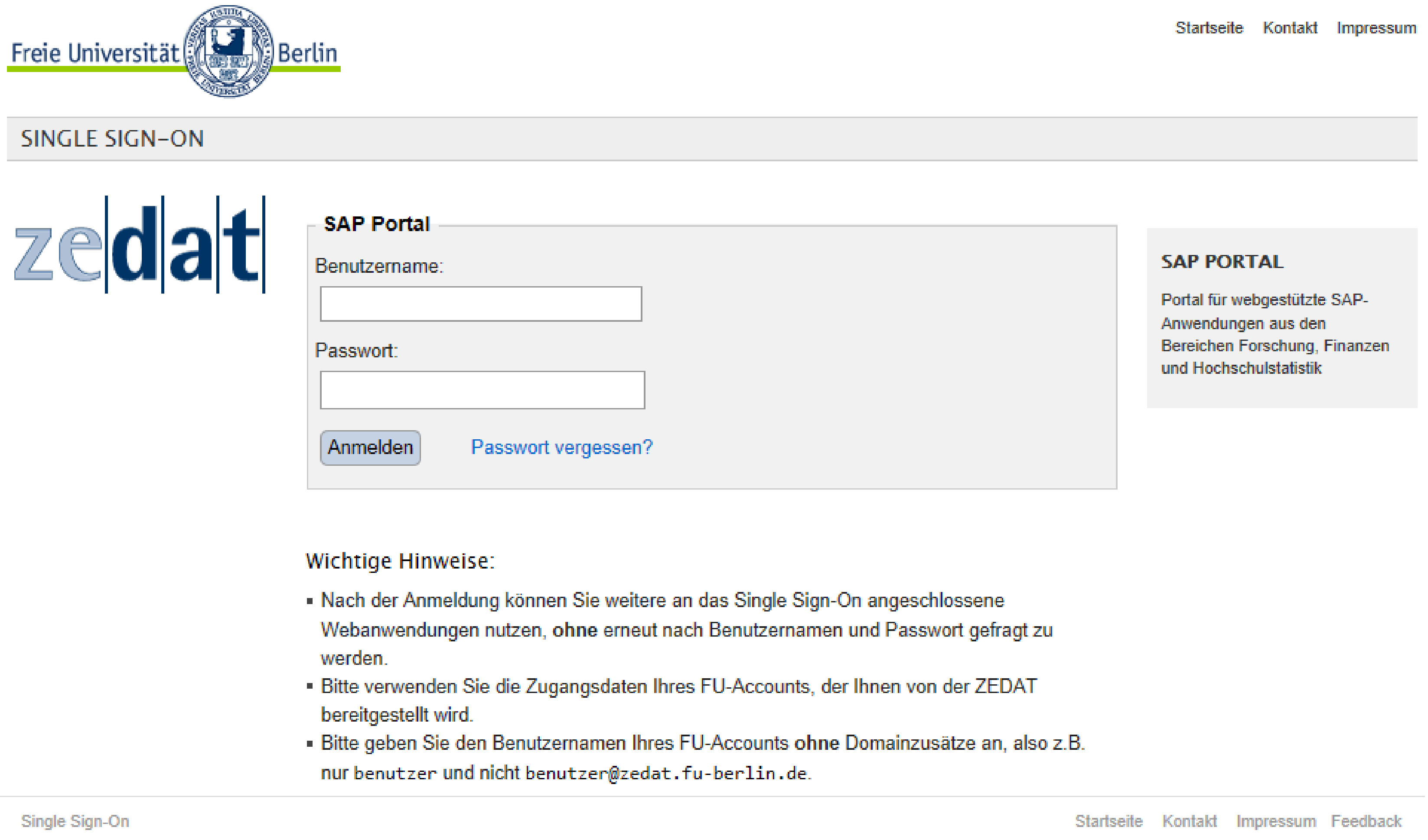
Ziel Eintrag:	*wall	Genehmiger:		Bearbeiter:		Art des Protokollwerts:	3625
genehmigt am:		Änderungs-Objekt:					

Ziel Eintrag	Änderungs-Objekt	Genehmiger	Bearbeiter	Datum/Uhrzeit der Genehmigung	Task
Dr. Christoph Wall	STDB Lehre zentral	Tatjana Ruhland	Tatjana Ruhland	2012-11-22T15:25:52	Genehmigung
Dr. Christoph Wall	STDB Forschung dezentral	Tatjana Ruhland	Tatjana Ruhland	2011-07-29T11:01:33	Genehmigung
Dr. Christoph Wall	STDB Lehre dezentral	Tatjana Ruhland	Tatjana Ruhland	2011-07-29T11:01:25	Genehmigung
Dr. Christoph Wall	STDB Haushalt dezentral	Tatjana Ruhland	Tatjana Ruhland	2011-07-29T11:01:19	Genehmigung
Dr. Christoph Wall	STDB Personal dezentral	Tatjana Ruhland	Tatjana Ruhland	2011-07-29T11:01:12	Genehmigung
Dr. Christoph Wall	STDB alle Berechtigungen dezentral	Tatjana Ruhland	Tatjana Ruhland	2011-07-29T10:56:43	Genehmigung
Dr. Christoph Wall	IdM Keyuser	Marina Kuszynski	Marina Kuszynski	2011-05-27T09:59:14	Genehmigung

Details zu

Ziel Eintrag:	Dr. Christoph Wall	Task:	Genehmigung
Änderungs-Objekt:	STDB Lehre zentral	Genehmiger:	Tatjana Ruhland
Bearbeiter:	Tatjana Ruhland	genehmigt am:	22.11.2012

Single Sign On



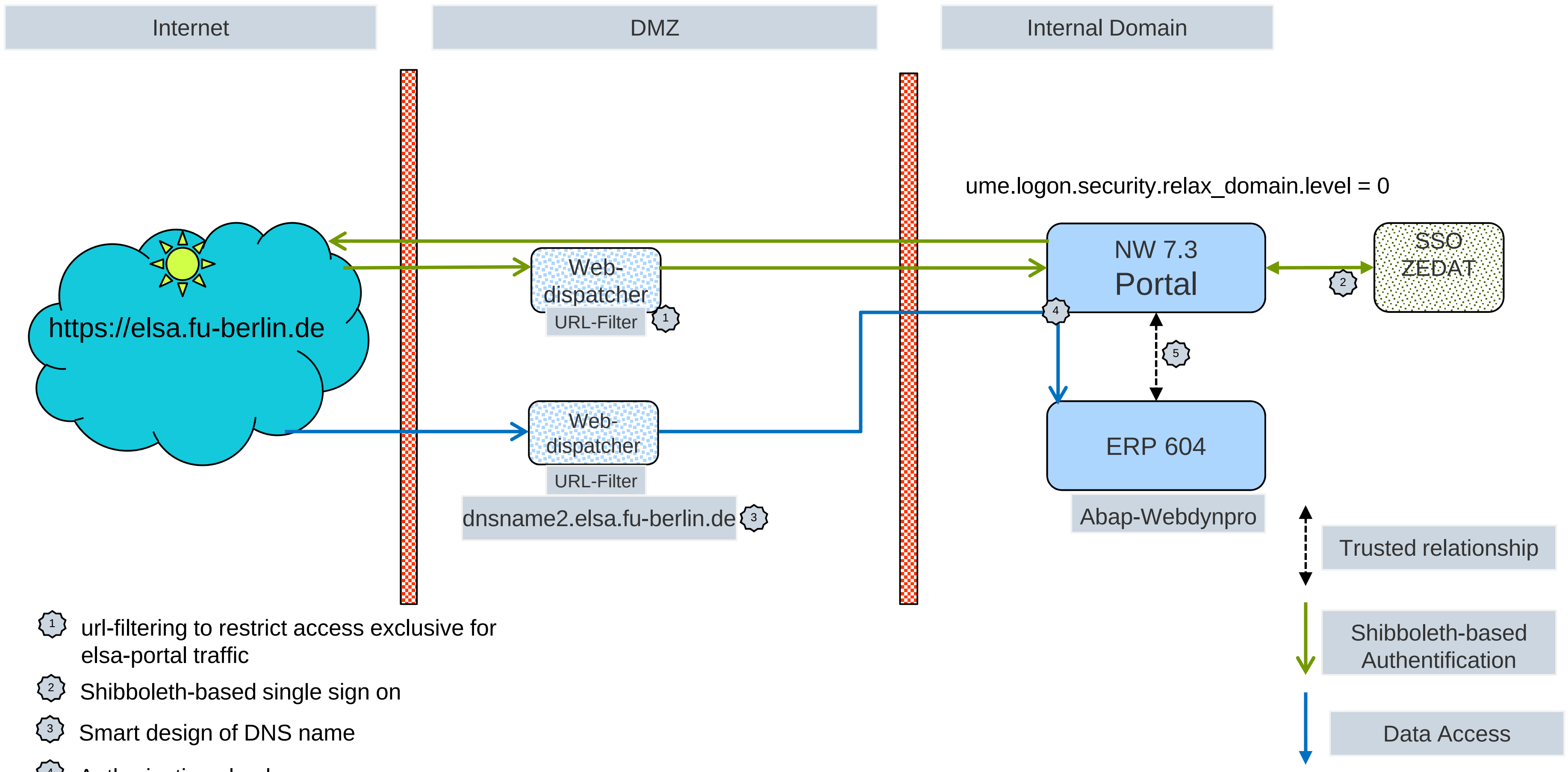
SAP PORTAL

Portal für webgestützte SAP-Anwendungen aus den Bereichen Forschung, Finanzen und Hochschulstatistik

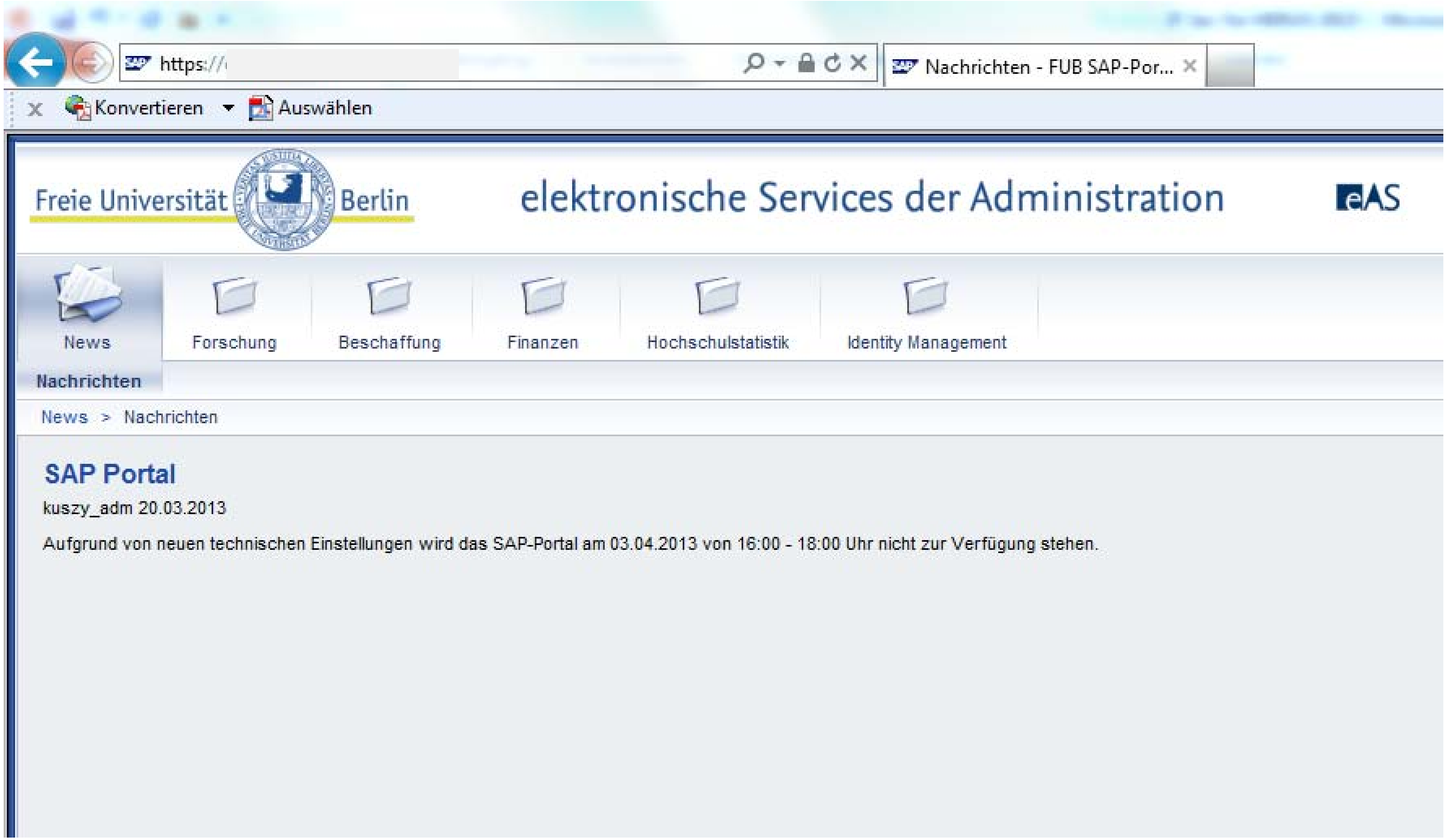
Wichtige Hinweise:

- Nach der Anmeldung können Sie weitere an das Single Sign-On angeschlossene Webanwendungen nutzen, **ohne** erneut nach Benutzernamen und Passwort gefragt zu werden.
- Bitte verwenden Sie die Zugangsdaten Ihres FU-Accounts, der Ihnen von der ZEDAT bereitgestellt wird.
- Bitte geben Sie den Benutzernamen Ihres FU-Accounts **ohne** Domainzusätze an, also z.B. nur `benutzer` und nicht `benutzer@zedat.fu-berlin.de`.

Security layers for SAP access



1. url-filtering to restrict access exclusive for elsa-portal traffic
2. Shibboleth-based single sign on
3. Smart design of DNS name
4. Authorization check
5. Certificate-based trusted relationship between portal and backend

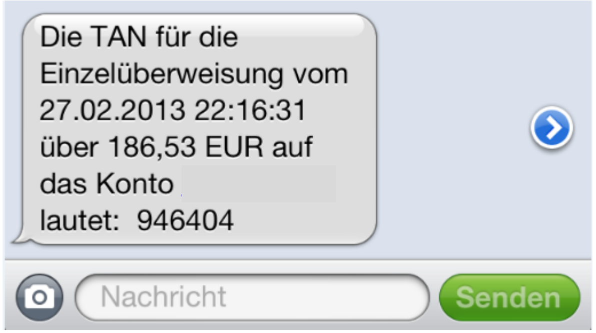


SAP Portal

kuszy_adm 20.03.2013

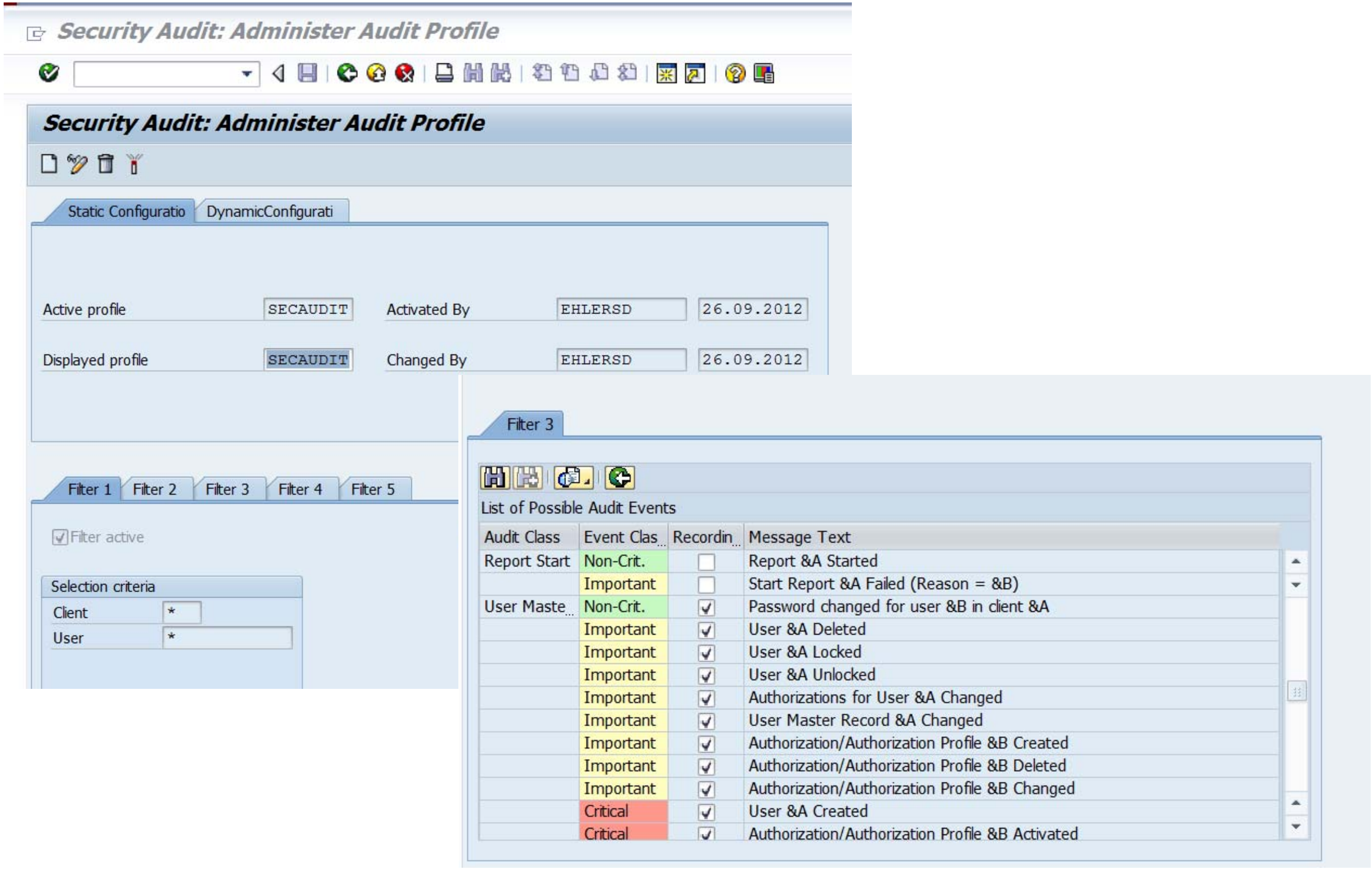
Aufgrund von neuen technischen Einstellungen wird das SAP-Portal am 03.04.2013 von 16:00 - 18:00 Uhr nicht zur Verfügung stehen.

Future Potential: Strong Authentification



Die TAN für die Einzelüberweisung vom 27.02.2013 22:16:31 über 186,53 EUR auf das Konto [redacted] lautet: 946404

Security Audit Log: Configuration (SM19)



Security Audit: Administer Audit Profile

Static Configuratio | DynamicConfigurati

Active profile	SECAUDIT	Activated By	EHLERSD	26.09.2012
Displayed profile	SECAUDIT	Changed By	EHLERSD	26.09.2012

Filter 1 | Filter 2 | Filter 3 | Filter 4 | Filter 5

☑ Filter active

Selection criteria

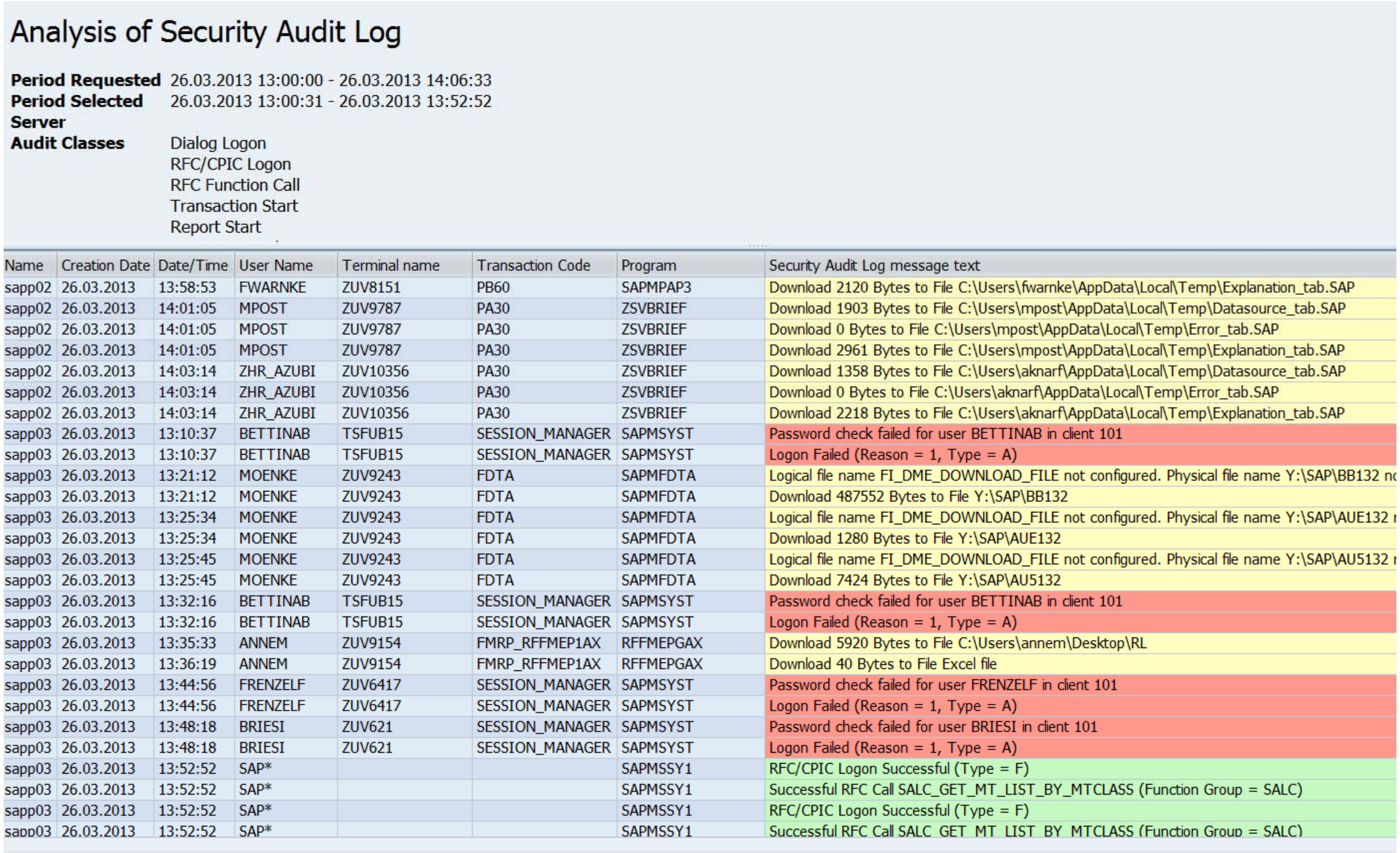
Client	*
User	*

Filter 3

List of Possible Audit Events

Audit Class	Event Clas...	Recordin...	Message Text
Report Start	Non-Crit.	☐	Report &A Started
	Important	☐	Start Report &A Failed (Reason = &B)
User Maste...	Non-Crit.	☑	Password changed for user &B in client &A
	Important	☑	User &A Deleted
	Important	☑	User &A Locked
	Important	☑	User &A Unlocked
	Important	☑	Authorizations for User &A Changed
	Important	☑	User Master Record &A Changed
	Important	☑	Authorization/Authorization Profile &B Created
	Important	☑	Authorization/Authorization Profile &B Deleted
	Important	☑	Authorization/Authorization Profile &B Changed
	Critical	☑	User &A Created
	Critical	☑	Authorization/Authorization Profile &B Activated

Security Audit Log: Analysis (SM20)



Analysis of Security Audit Log

Period Requested 26.03.2013 13:00:00 - 26.03.2013 14:06:33
Period Selected 26.03.2013 13:00:31 - 26.03.2013 13:52:52
Server
Audit Classes Dialog Logon
RFC/CPIC Logon
RFC Function Call
Transaction Start
Report Start

Name	Creation Date	Date/Time	User Name	Terminal name	Transaction Code	Program	Security Audit Log message text
sapp02	26.03.2013	13:58:53	FWARNKE	ZUV8151	PB60	SAPMPAP3	Download 2120 Bytes to File C:\Users\fwarnke\AppData\Local\Temp\Explanation_tab.SAP
sapp02	26.03.2013	14:01:05	MPOST	ZUV9787	PA30	ZSVBRIEF	Download 1903 Bytes to File C:\Users\mpost\AppData\Local\Temp\Datasource_tab.SAP
sapp02	26.03.2013	14:01:05	MPOST	ZUV9787	PA30	ZSVBRIEF	Download 0 Bytes to File C:\Users\mpost\AppData\Local\Temp\Error_tab.SAP
sapp02	26.03.2013	14:01:05	MPOST	ZUV9787	PA30	ZSVBRIEF	Download 2961 Bytes to File C:\Users\mpost\AppData\Local\Temp\Explanation_tab.SAP
sapp02	26.03.2013	14:03:14	ZHR_AZUBI	ZUV10356	PA30	ZSVBRIEF	Download 1358 Bytes to File C:\Users\aknarf\AppData\Local\Temp\Datasource_tab.SAP
sapp02	26.03.2013	14:03:14	ZHR_AZUBI	ZUV10356	PA30	ZSVBRIEF	Download 0 Bytes to File C:\Users\aknarf\AppData\Local\Temp\Error_tab.SAP
sapp02	26.03.2013	14:03:14	ZHR_AZUBI	ZUV10356	PA30	ZSVBRIEF	Download 2218 Bytes to File C:\Users\aknarf\AppData\Local\Temp\Explanation_tab.SAP
sapp03	26.03.2013	13:10:37	BETTINAB	TSFUB15	SESSION_MANAGER	SAPMSYST	Password check failed for user BETTINAB in client 101
sapp03	26.03.2013	13:10:37	BETTINAB	TSFUB15	SESSION_MANAGER	SAPMSYST	Logon Failed (Reason = 1, Type = A)
sapp03	26.03.2013	13:21:12	MOENKE	ZUV9243	FDTA	SAPMFDTA	Logical file name FI_DME_DOWNLOAD_FILE not configured. Physical file name Y:\SAP\BB132 nc
sapp03	26.03.2013	13:21:12	MOENKE	ZUV9243	FDTA	SAPMFDTA	Download 487552 Bytes to File Y:\SAP\BB132
sapp03	26.03.2013	13:25:34	MOENKE	ZUV9243	FDTA	SAPMFDTA	Logical file name FI_DME_DOWNLOAD_FILE not configured. Physical file name Y:\SAP\AUE132 r
sapp03	26.03.2013	13:25:34	MOENKE	ZUV9243	FDTA	SAPMFDTA	Download 1280 Bytes to File Y:\SAP\AUE132
sapp03	26.03.2013	13:25:45	MOENKE	ZUV9243	FDTA	SAPMFDTA	Logical file name FI_DME_DOWNLOAD_FILE not configured. Physical file name Y:\SAP\AU5132 r
sapp03	26.03.2013	13:25:45	MOENKE	ZUV9243	FDTA	SAPMFDTA	Download 7424 Bytes to File Y:\SAP\AU5132
sapp03	26.03.2013	13:32:16	BETTINAB	TSFUB15	SESSION_MANAGER	SAPMSYST	Password check failed for user BETTINAB in client 101
sapp03	26.03.2013	13:32:16	BETTINAB	TSFUB15	SESSION_MANAGER	SAPMSYST	Logon Failed (Reason = 1, Type = A)
sapp03	26.03.2013	13:35:33	ANNEM	ZUV9154	FMRP_RFFMEP1AX	RFFMEPGAX	Download 5920 Bytes to File C:\Users\annem\Desktop\RL
sapp03	26.03.2013	13:36:19	ANNEM	ZUV9154	FMRP_RFFMEP1AX	RFFMEPGAX	Download 40 Bytes to File Excel file
sapp03	26.03.2013	13:44:56	FRENZELF	ZUV6417	SESSION_MANAGER	SAPMSYST	Password check failed for user FRENZELF in client 101
sapp03	26.03.2013	13:44:56	FRENZELF	ZUV6417	SESSION_MANAGER	SAPMSYST	Logon Failed (Reason = 1, Type = A)
sapp03	26.03.2013	13:48:18	BRIESI	ZUV621	SESSION_MANAGER	SAPMSYST	Password check failed for user BRIESI in client 101
sapp03	26.03.2013	13:48:18	BRIESI	ZUV621	SESSION_MANAGER	SAPMSYST	Logon Failed (Reason = 1, Type = A)
sapp03	26.03.2013	13:52:52	SAP*			SAPMSSY1	RFC/CPIC Logon Successful (Type = F)
sapp03	26.03.2013	13:52:52	SAP*			SAPMSSY1	Successful RFC Call SALC_GET_MT_LIST_BY_MTCLASS (Function Group = SALC)
sapp03	26.03.2013	13:52:52	SAP*			SAPMSSY1	RFC/CPIC Logon Successful (Type = F)
sapp03	26.03.2013	13:52:52	SAP*			SAPMSSY1	Successful RFC Call SALC_GET_MT_LIST_BY_MTCLASS (Function Group = SALC)

The SOS Report

The ***SAP Security Optimization Service*** is a comprehensive support service that identifies security risks for your SAP system and helps you to determine the appropriate measures to protect it from these risks.

The security checks of SAP Security Optimization are performed for the following security aspects:

- **Availability:** ensuring that a system is operational and functional at any given moment
- **Integrity:** ensuring that data is valid and cannot be compromised
- **Authenticity:** ensuring that users are the persons they claim to be
- **Confidentiality:** ensuring that information is not accessed by unauthorized persons
- **Compliance:** ensuring that the system security set-up is in accordance with established guidelines

サービス レポート

SAP Security Optimization Self-Service

SAP システム ID

SAP コンポーネント

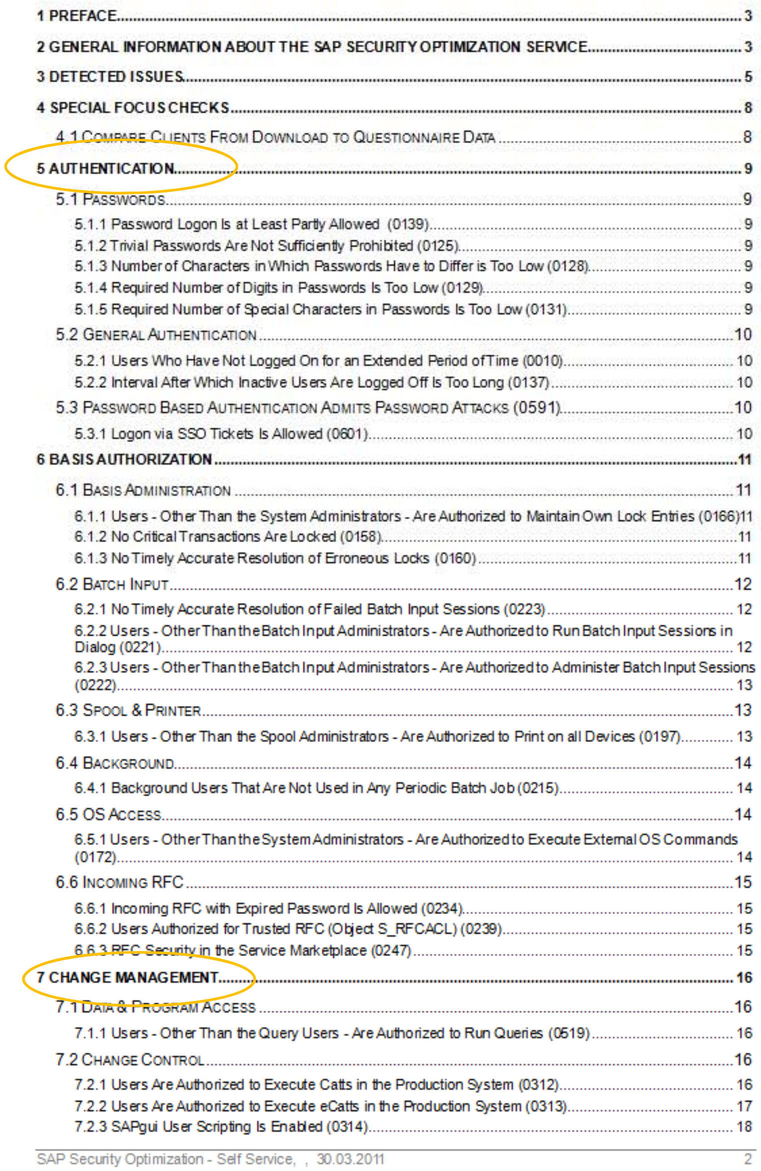
リリース

DB システム

御社名

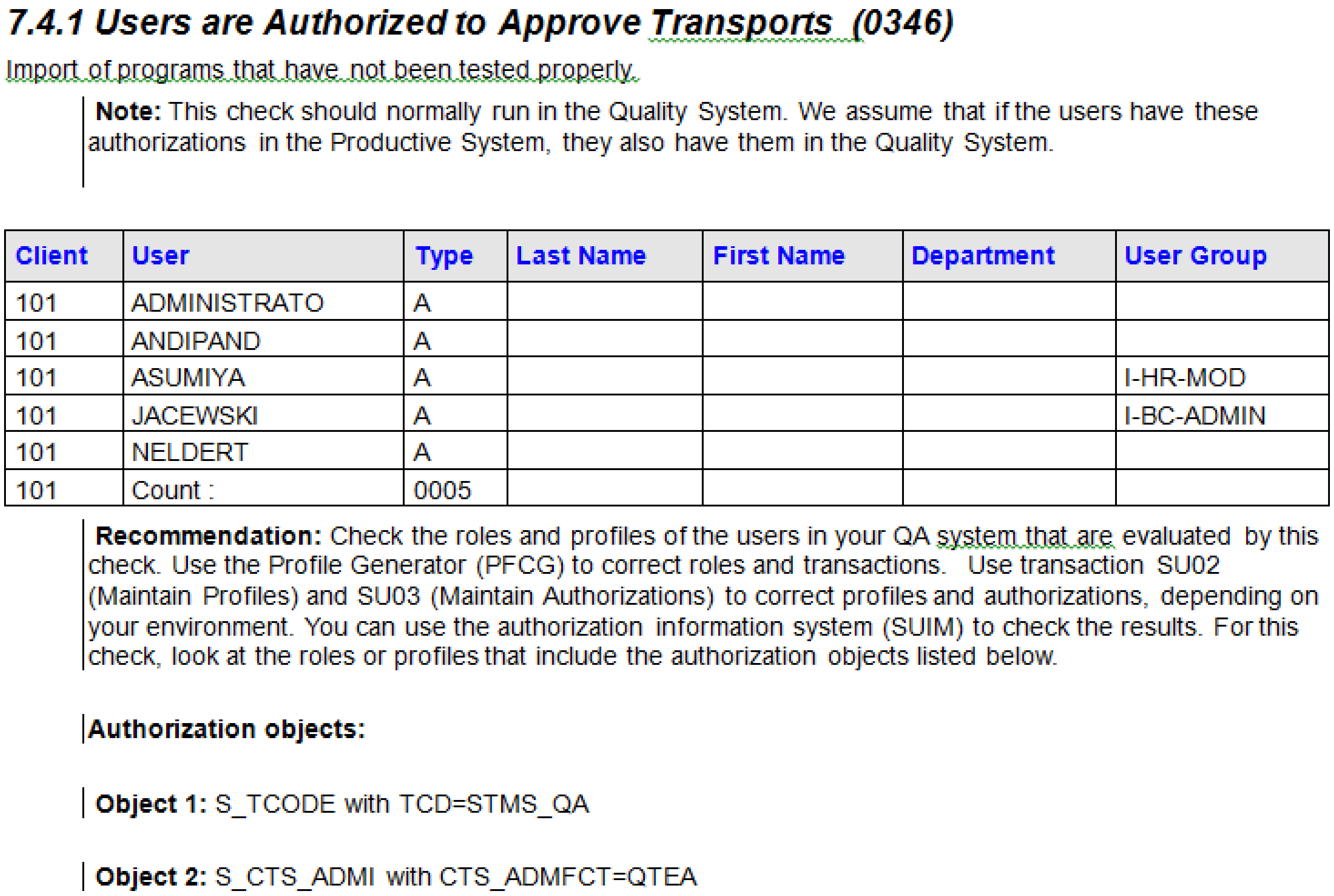
サービスセンター
電話番号
Fax番号

セッション開始日	30.03.2011	Session No.	1010000004372
レポート提出日	15.08.2011	Installation No.	0120058874
作成者	Tatjana Ruhland Freie Universität Berlin	Customer No.	



SAP Security Optimization - Self Service, , 30.03.2011 2

Risks are pointed out



7.4.1 Users are Authorized to Approve Transports (0346)

Import of programs that have not been tested properly.

Note: This check should normally run in the Quality System. We assume that if the users have these authorizations in the Productive System, they also have them in the Quality System.

Client	User	Type	Last Name	First Name	Department	User Group
101	ADMINISTRATO	A				
101	ANDIPAND	A				
101	ASUMIYA	A				I-HR-MOD
101	JACEWSKI	A				I-BC-ADMIN
101	NELDERT	A				
101	Count :	0005				

Recommendation: Check the roles and profiles of the users in your QA system that are evaluated by this check. Use the Profile Generator (PFCG) to correct roles and transactions. Use transaction SU02 (Maintain Profiles) and SU03 (Maintain Authorizations) to correct profiles and authorizations, depending on your environment. You can use the authorization information system (SUIM) to check the results. For this check, look at the roles or profiles that include the authorization objects listed below.

Authorization objects:

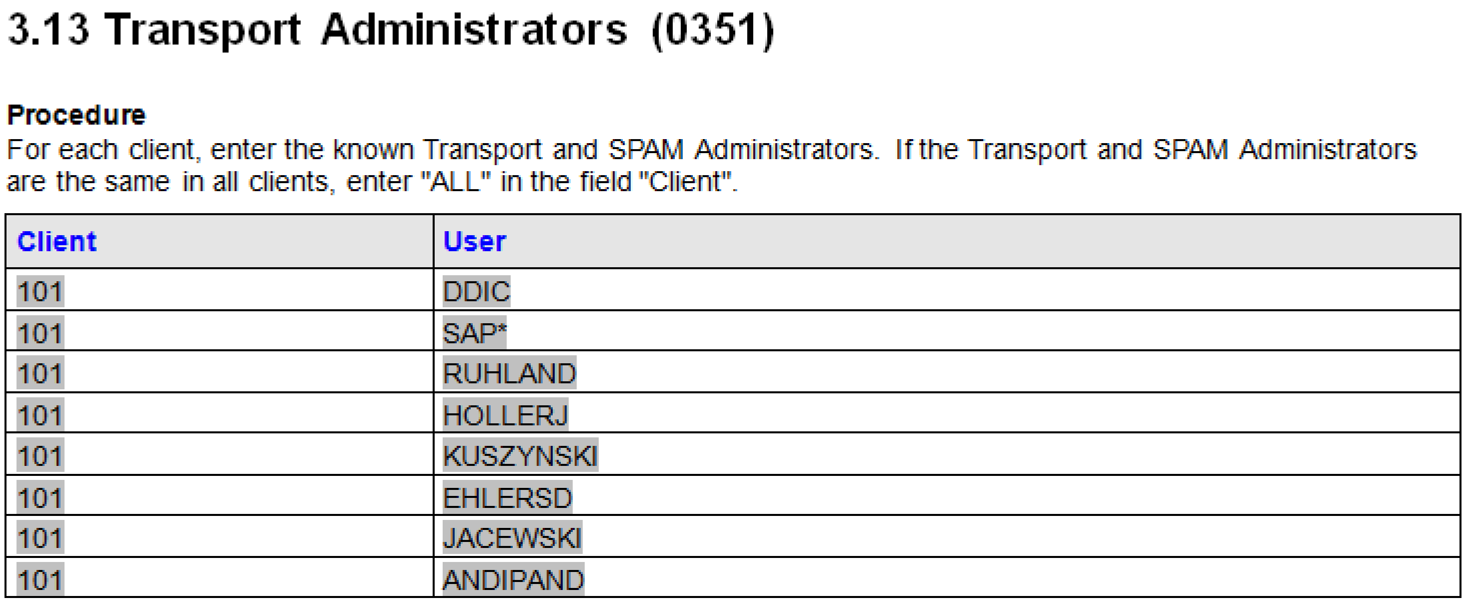
Object 1: S_TCODE with TCD=STMS_QA

Object 2: S_CTS_ADMI with CTS_ADMFCT=QTEA

Es ist o.k. – diese User wurden in Questionary aufgenommen.

Questionnaire

SAP Security Optimization Self-Service

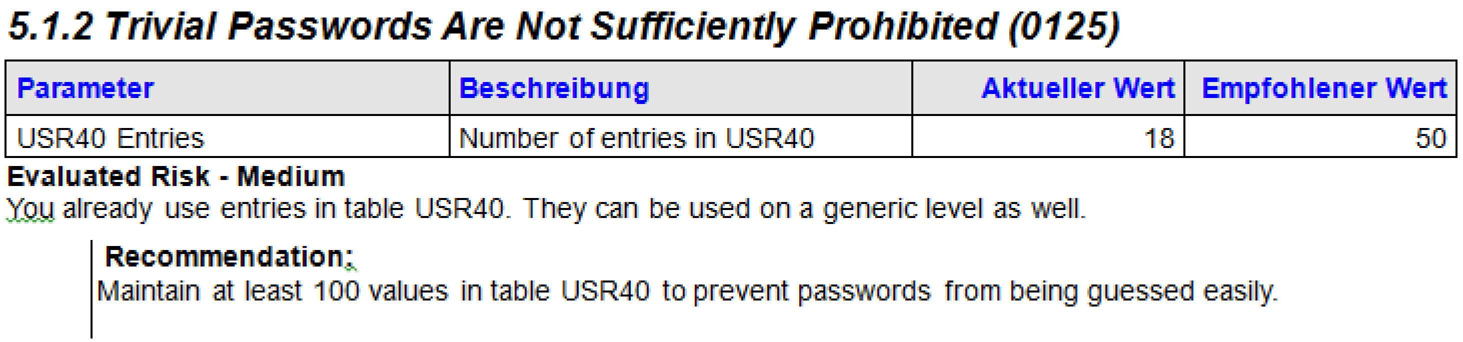


3.13 Transport Administrators (0351)

Procedure
For each client, enter the known Transport and SPAM Administrators. If the Transport and SPAM Administrators are the same in all clients, enter "ALL" in the field "Client".

Client	User
101	DDIC
101	SAP*
101	RUHLAND
101	HOLLERJ
101	KUSZYNSKI
101	EHLERSD
101	JACEWSKI
101	ANDIPAND

Examples for Authentification Alerts



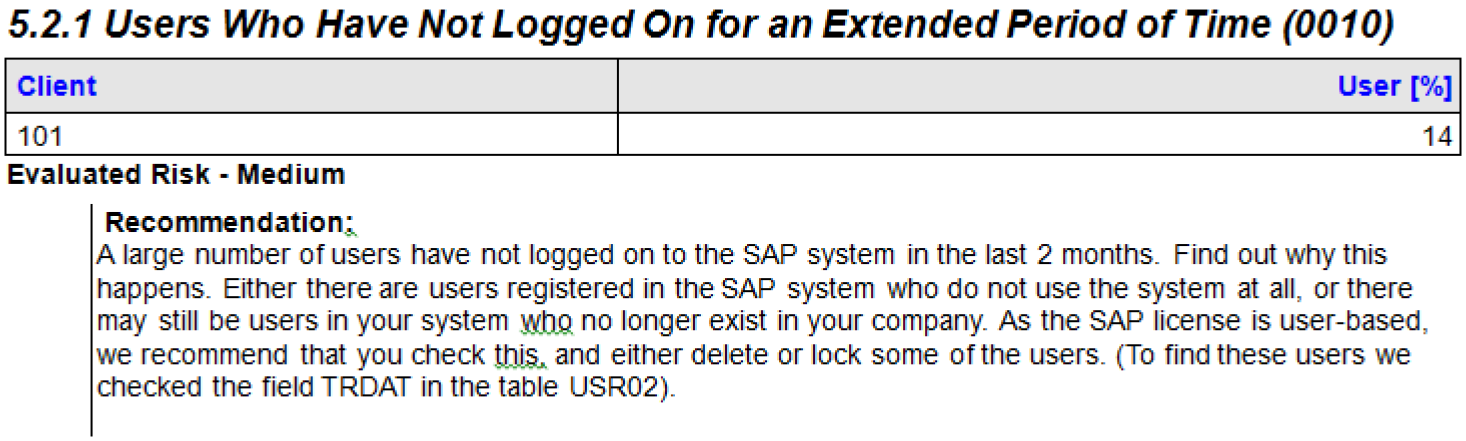
5.1.2 Trivial Passwords Are Not Sufficiently Prohibited (0125)

Parameter	Beschreibung	Aktueller Wert	Empfohlener Wert
USR40 Entries	Number of entries in USR40	18	50

Evaluated Risk - Medium

You already use entries in table USR40. They can be used on a generic level as well.

> **Recommendation:**
> Maintain at least 100 values in table USR40 to prevent passwords from being guessed easily.



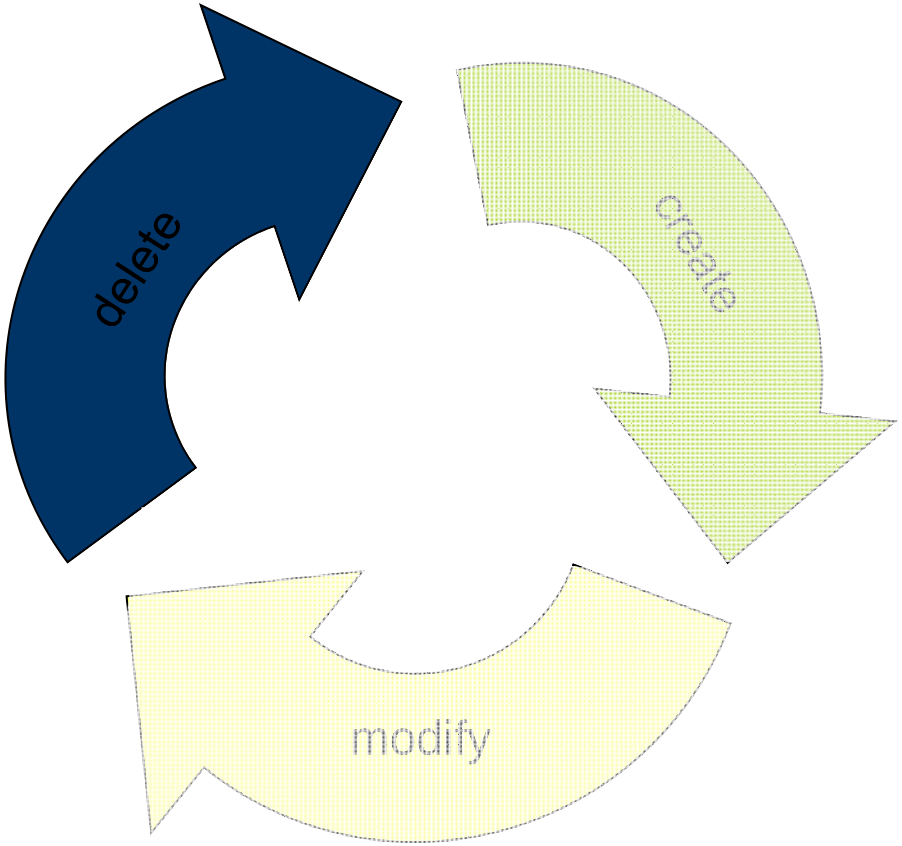
5.2.1 Users Who Have Not Logged On for an Extended Period of Time (0010)

Client	User [%]
101	14

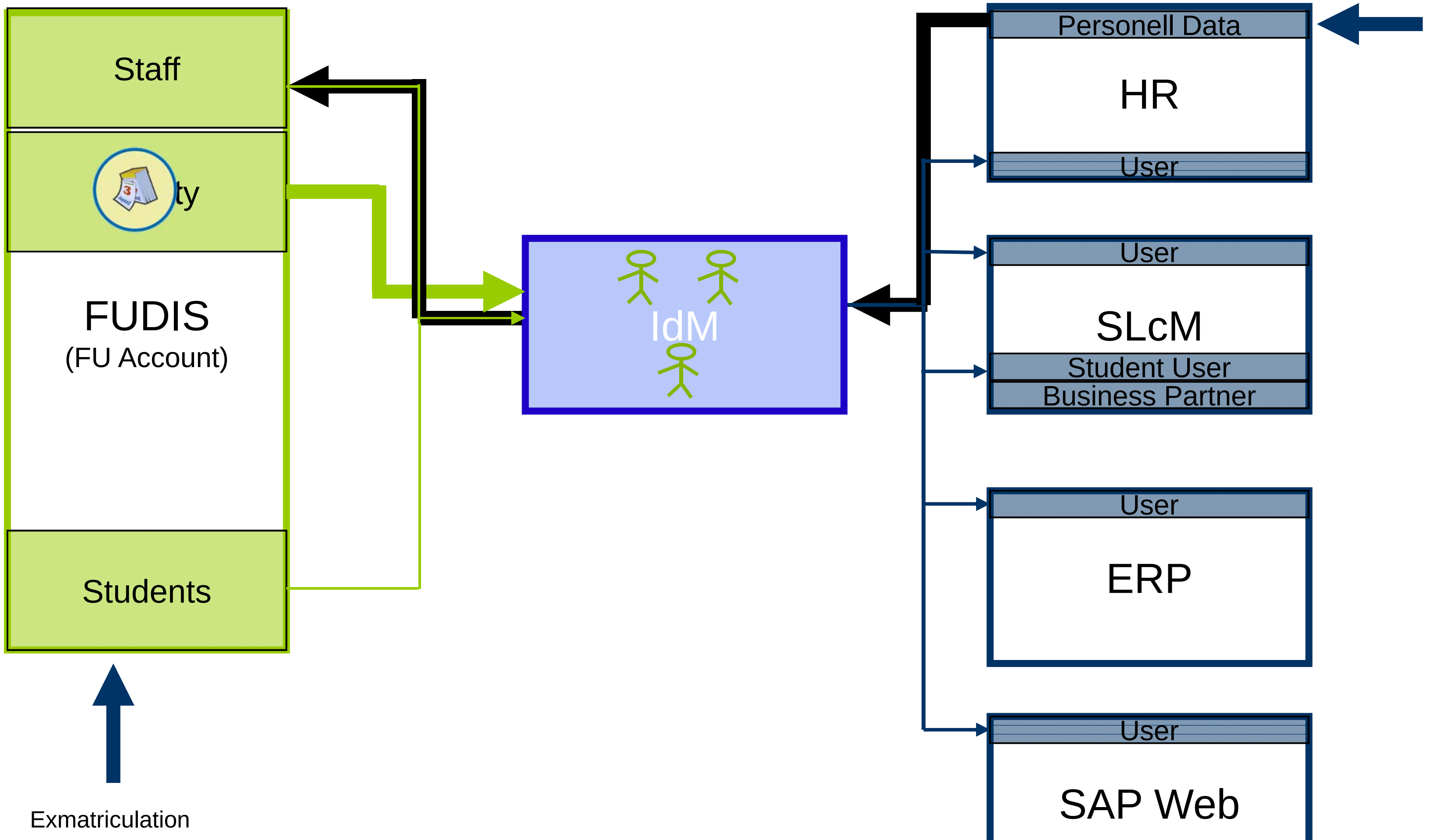
Evaluated Risk - Medium

> **Recommendation:**
> A large number of users have not logged on to the SAP system in the last 2 months. Find out why this happens. Either there are users registered in the SAP system who do not use the system at all, or there may still be users in your system who no longer exist in your company. As the SAP license is user-based, we recommend that you check this, and either delete or lock some of the users. (To find these users we checked the field TRDAT in the table USR02).

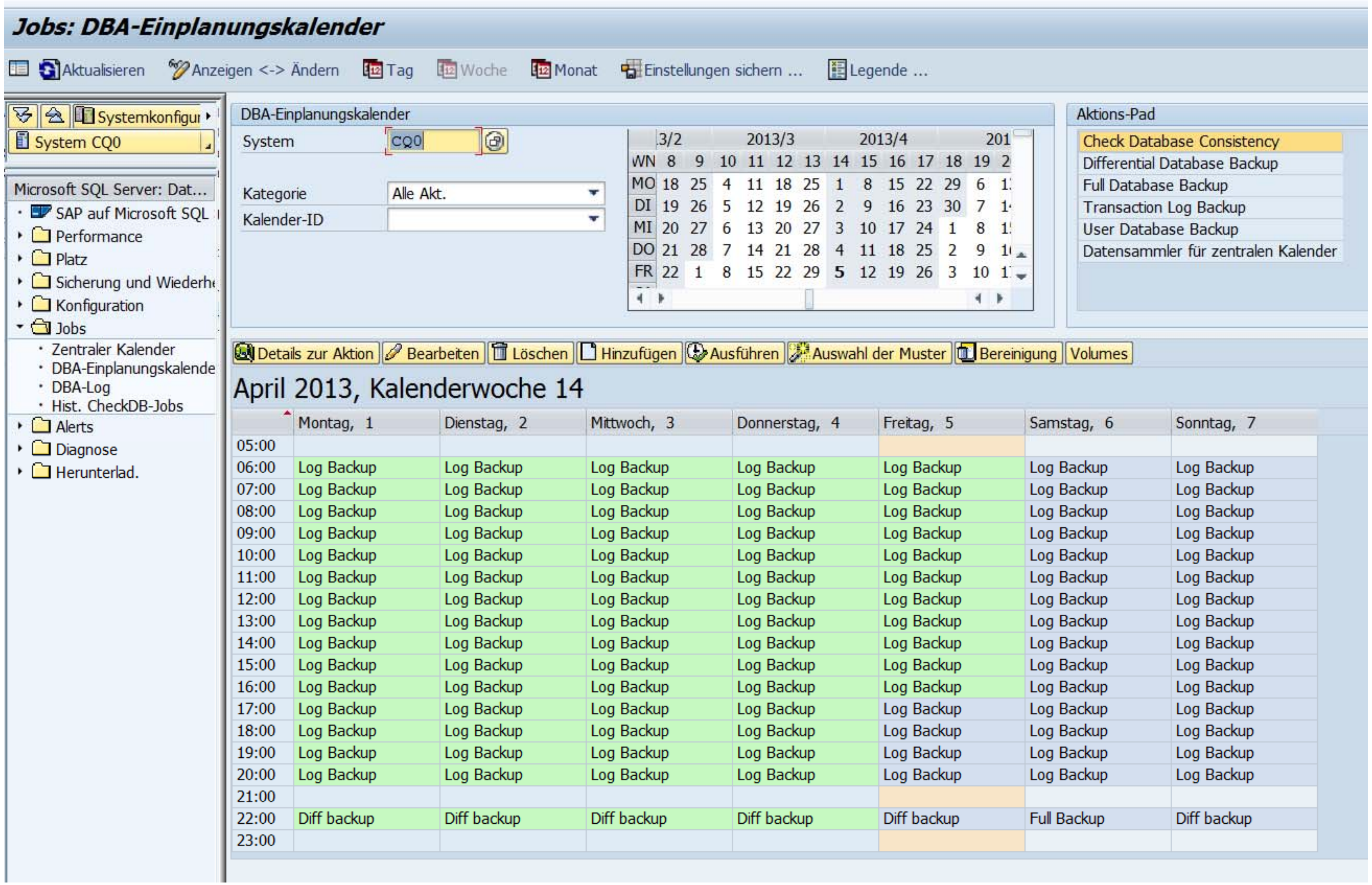
User Lifecycle Management: Deactivation



Deactivation of Users



Business continuity:
Backup and restore support



DBA-Einplanungskalender

System CQ0

Kategorie Alle Akt.

Kalender-ID

	3/2		2013/3				2013/4					201	
WN	8	9	10	11	12	13	14	15	16	17	18	19	2
MO	18	25	4	11	18	25	1	8	15	22	29	6	1
DI	19	26	5	12	19	26	2	9	16	23	30	7	1
MI	20	27	6	13	20	27	3	10	17	24	1	8	1
DO	21	28	7	14	21	28	4	11	18	25	2	9	1
FR	22	1	8	15	22	29	5	12	19	26	3	10	1

Aktions-Pad

- Check Database Consistency
- Differential Database Backup
- Full Database Backup
- Transaction Log Backup
- User Database Backup
- Datensammler für zentralen Kalender

April 2013, Kalenderwoche 14

	Montag, 1	Dienstag, 2	Mittwoch, 3	Donnerstag, 4	Freitag, 5	Samstag, 6	Sonntag, 7
05:00							
06:00	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup
07:00	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup
08:00	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup
09:00	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup
10:00	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup
11:00	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup
12:00	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup
13:00	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup
14:00	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup
15:00	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup
16:00	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup
17:00	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup
18:00	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup
19:00	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup
20:00	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup	Log Backup
21:00							
22:00	Diff backup	Diff backup	Diff backup	Diff backup	Diff backup	Full Backup	Diff backup
23:00							

IT-Security-Management-System reloaded

Governance

Risk assessment or analysis: A risk analysis provides information on the probability of the occurrence of a damaging event and what negative consequences the damage would have.

Security policy: In a security policy the security objectives and general security safeguards are formulated in the sense of the *official regulations of a company* or a public authority. Detailed security safeguards are contained in a more comprehensive security concept.

Technical

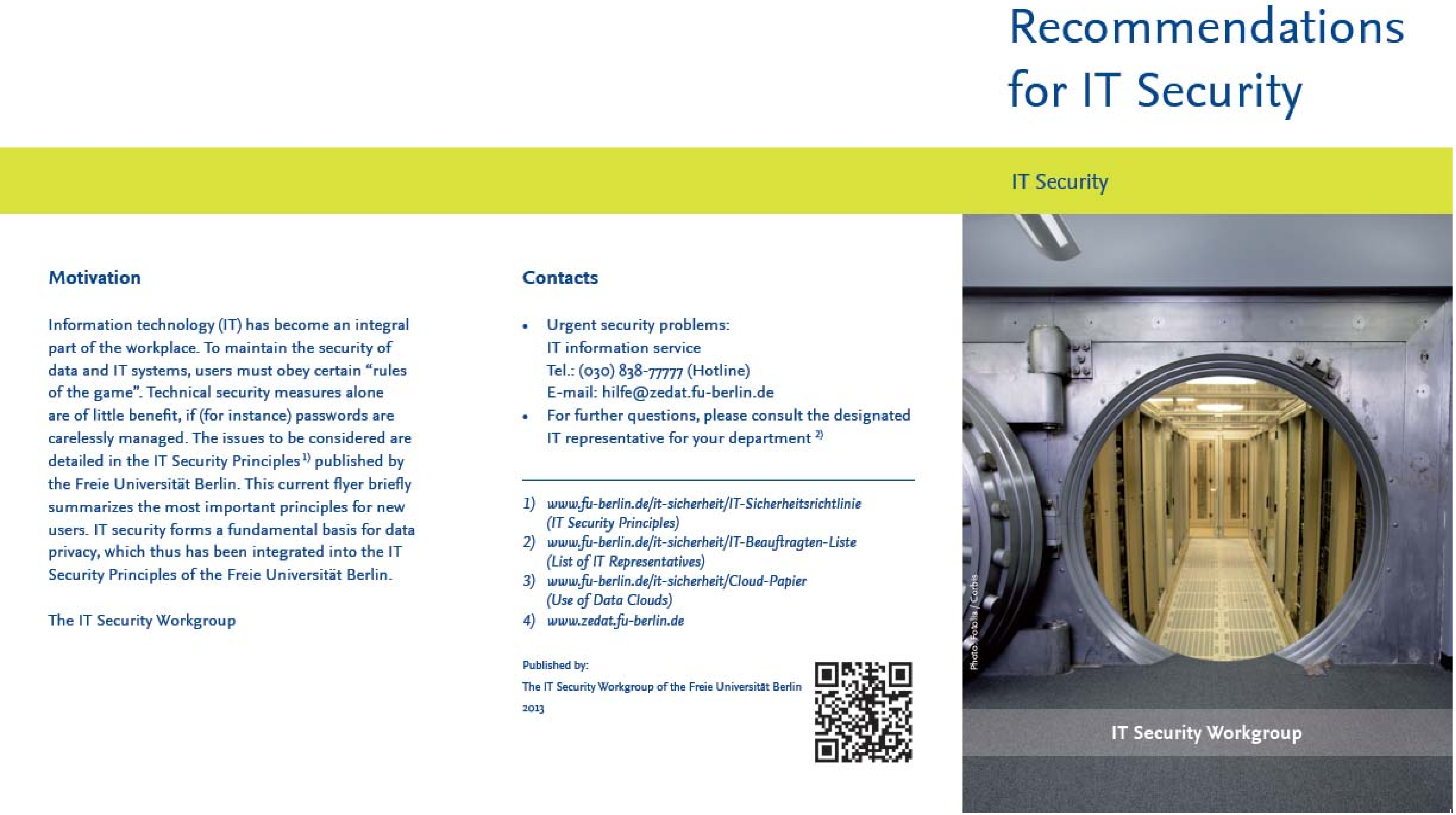
Authentication: When a person logs in on a system, the system runs a check in an authentication process to verify the identity of the person. The term is also used when the identity of IT components or applications is tested.

Authorisation: Authorisation is the process of checking whether a person, an IT component or an application is authorised to perform a specific action.

Data protection: Data protection refers to the protection of personal data against misuse by third parties.

Data backup: Data backup involves making copies of existing data to prevent its loss.

Information policy



Recommendations for IT Security

IT Security

Motivation

Information technology (IT) has become an integral part of the workplace. To maintain the security of data and IT systems, users must obey certain “rules of the game”. Technical security measures alone are of little benefit, if (for instance) passwords are carelessly managed. The issues to be considered are detailed in the IT Security Principles [1] published by the Freie Universität Berlin. This current flyer briefly summarizes the most important principles for new users. IT security forms a fundamental basis for data privacy, which thus has been integrated into the IT Security Principles of the Freie Universität Berlin.

The IT Security Workgroup

Contacts

- Urgent security problems:
  IT information service
  Tel.: (030) 838-77777 (Hotline)
  E-mail: hilfe@zedat.fu-berlin.de
- For further questions, please consult the designated IT representative for your department [2]

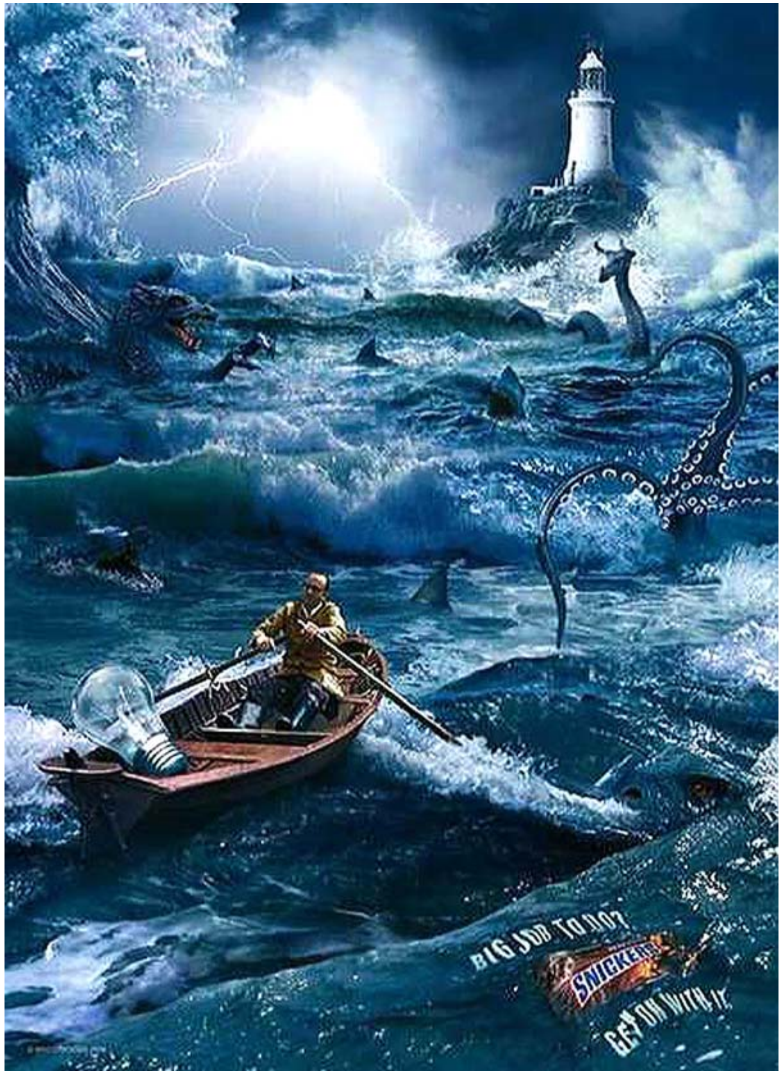
1) *www.fu-berlin.de/it-sicherheit/IT-Sicherheitsrichtlinie (IT Security Principles)*
2) *www.fu-berlin.de/it-sicherheit/IT-Beauftragten-Liste (List of IT Representatives)*
3) *www.fu-berlin.de/it-sicherheit/Cloud-Papier (Use of Data Clouds)*
4) *www.zedat.fu-berlin.de*

Published by:
The IT Security Workgroup of the Freie Universität Berlin
2013

Photo: Fotolia / Curtis

IT Security Workgroup

Big job to do ?



Get on with it !

eAS

elektronische Administration und Services

Dr. Christoph Wall
Boltzmannstr. 18
14195 Berlin
Germany

Christoph.wall@fu-berlin.de
+49 30 838 58000