verinice.XP

Erfolgsstory Europ Assistance - vom erfolgreichen Aufbau mit verinice zur Aufrechterhaltung des erreichten Sicherheits-Levels

Holger Schellhaas
Management Consulting & Training
verinice.PARTNER und Partner der TCI
Transformation Consulting International GmbH
Interim-CISO Haspa-Direkt

Berlin, 23. März 2018

verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Europ Assistance (EA) ist eine Tochter der GENERALI; in Deutschland gehört EA zum Mittelstand. Trotzdem haben wir uns bewusst für BSI IT-Grundschutz entschieden.

Weltweite Präsenz in 33 Ländern für Gesundheit, Automotive, Reise und Haus & Familie; Mission Statement: « Den Alltag der Menschen erleichtern und ihre Mobilität sichern»

Gegründet in
1 9 8 0

Mitarbeiter
< 300 (Welt: 8.000)

IT-Mitarbeiter
z.Zt. 14

Bearb. Anrufe p.a.
> 400 000

Einsätze p.a.
~ 250 000

verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Auftrag der GL: IT-Sicherheitskonzept und angemessenen Sicherheits-Level umsetzen
Akzeptanz der Fachbereiche und der IT durch kleine „verdaubare“ Schritte schaffen

Wir haben das Standardvorgehen an die Anforderungen der EA angepasst

- **1.Schritt: Etablierung der Sicherheitsorganisation und IT-Struktur (nach BSI)**
  - ✓ Definition des IT-Verbunds: Erfassung aller infrastrukturellen, organisatorischen, personellen und technischen Komponenten zur Aufgabenerfüllung
- **2.Schritt: Festlegung des angemessenen Sicherheitslevels**
  - ✓ Leitlinie zur Informationssicherheit und passende Sicherheitsrichtlinien
  - ✓ Bewertung des Schutzbedarfs der Prozesse und Informationen
- **3.Schritt: Soll-/Ist-Vergleich zur Ermittlung des Umsetzungsstatus der Maßnahmen**
  - ✓ Umsetzung der Maßnahmen; Restrisiko-Übernahme durch die Geschäftsführung
  - ✓ Awareness-Initiativen und regelmäßige Schulungen
- **4.Schritt: Aufrechterhaltung des erreichten Sicherheits-Levels**
  - ✓ Regelmäßige externe und interne Audits auf Basis von IT-Grundschutz
  - ✓ Anpassung der technischen und organisatorischen Maßnahmen an EU-DSGVO
- **5.Schritt: Neuausrichtung des IT-Verbunds an der IT-Strategie: Cloud-Migration**

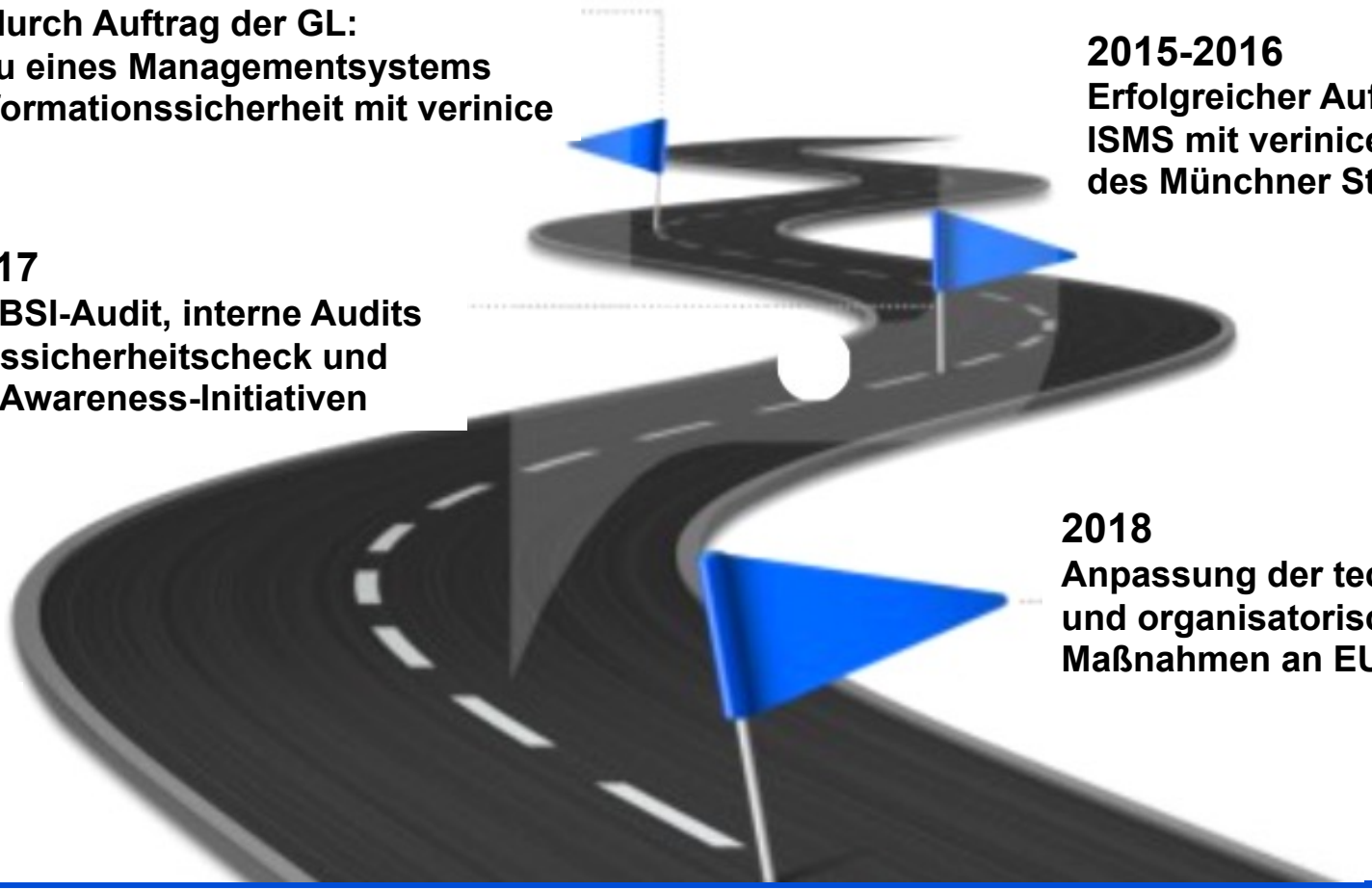
verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Auftrag der GL: IT-Sicherheitskonzept und angemessenen Sicherheits-Level umsetzen
Unsere Roadmap - „Agenda 2020“ - zur Aufrechterhaltung des erreichten Levels

2013-2014
Start durch Auftrag der GL:
Aufbau eines Managementsystems zur Informationssicherheit mit verinice

2015-2016
Erfolgreicher Aufbau des ISMS mit verinice (mit Umzug des Münchner Standorts)

2016-2017
Externer BSI-Audit, interne Audits zum Basissicherheitscheck und laufende Awareness-Initiativen



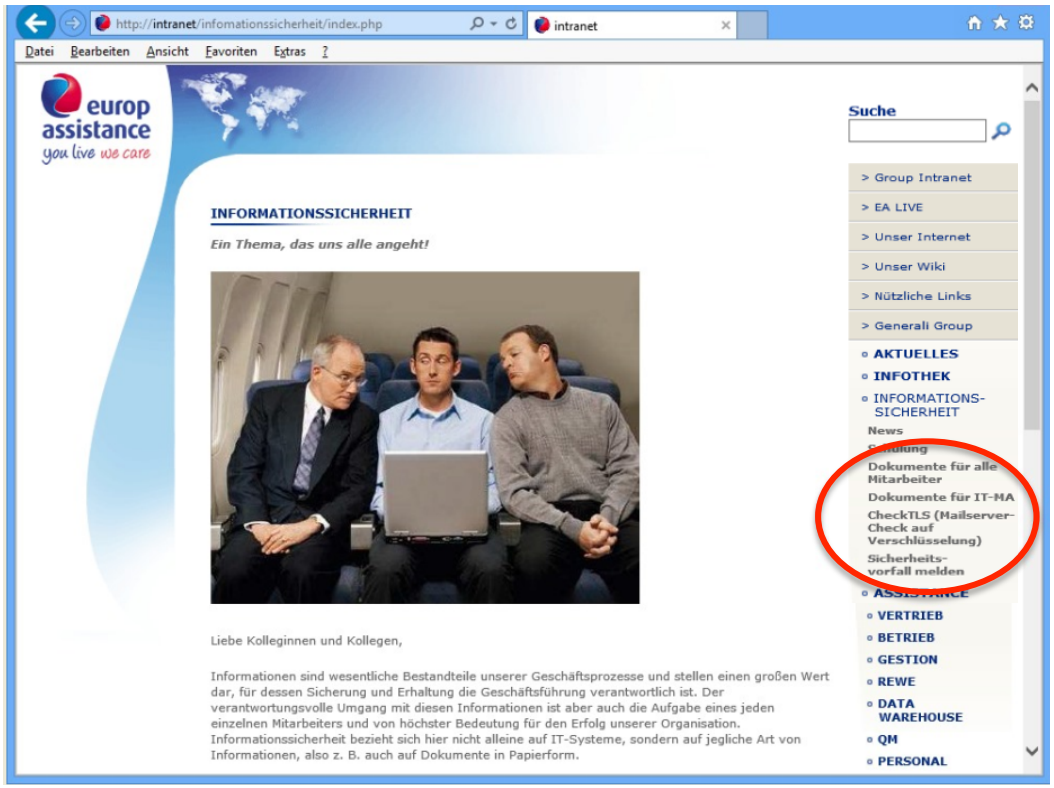
2018
Anpassung der technischen und organisatorischen Maßnahmen an EU-DSGVO

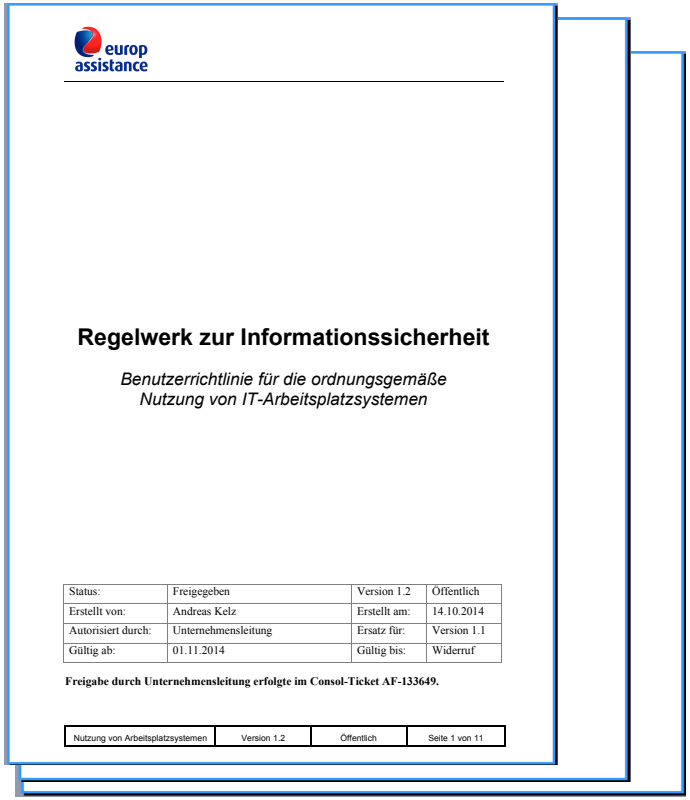
2019-2020
Migration in die Cloud

verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Auftrag der GL: IT-Sicherheitskonzept und angemessenen Sicherheits-Level umsetzen
Erstes Handlungsfeld war: Schrittweise zur Awareness und zu den „Top 10“ Richtlinien

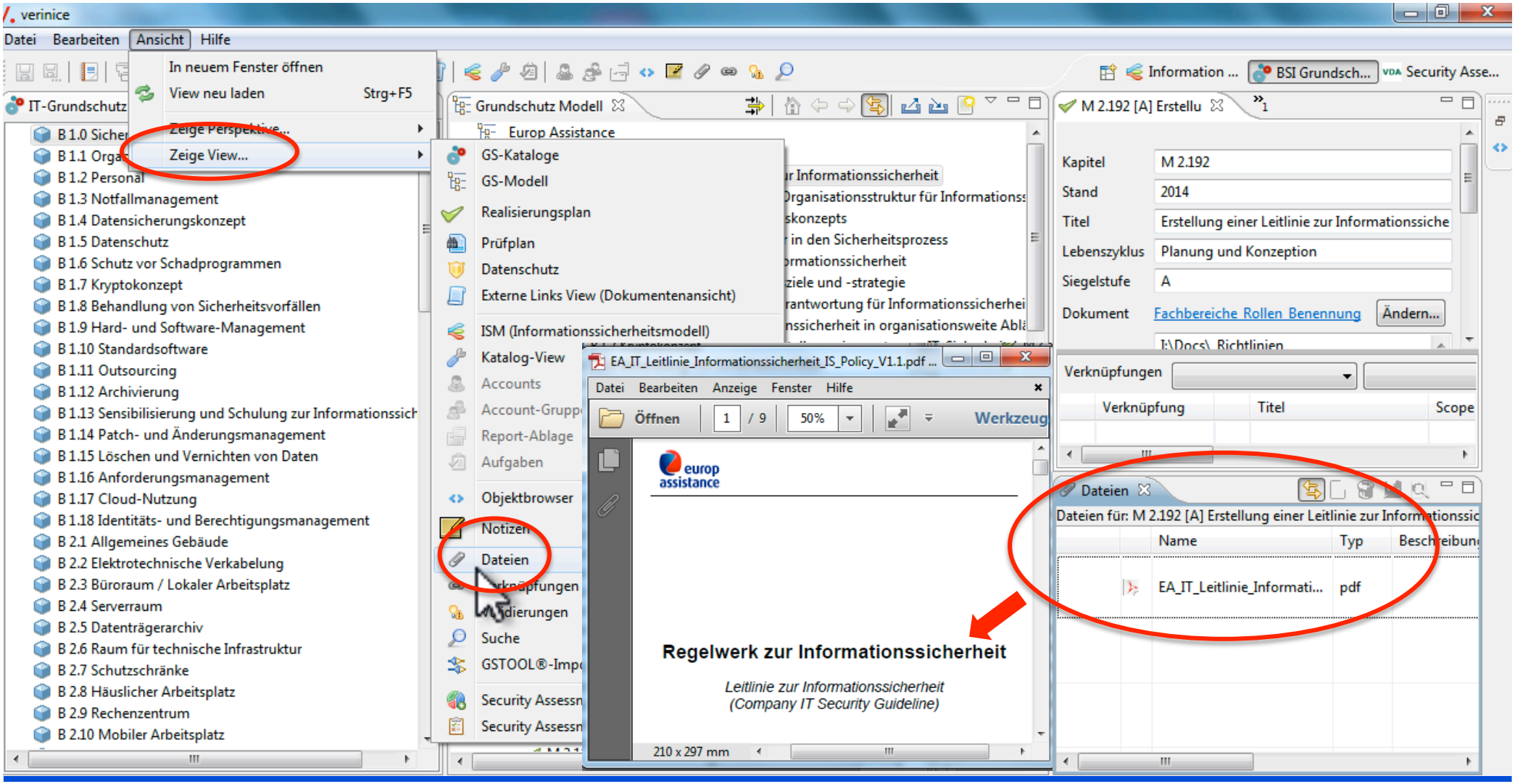
Phase 1 „Set Up“ → **Phase 2** „Gap“-Analyse → **Phase 3** Handlungs-felder → **Phase 4** Risikoanalyse/ Roadmap → **Phase 5** Umsetzungs-Unterstützung





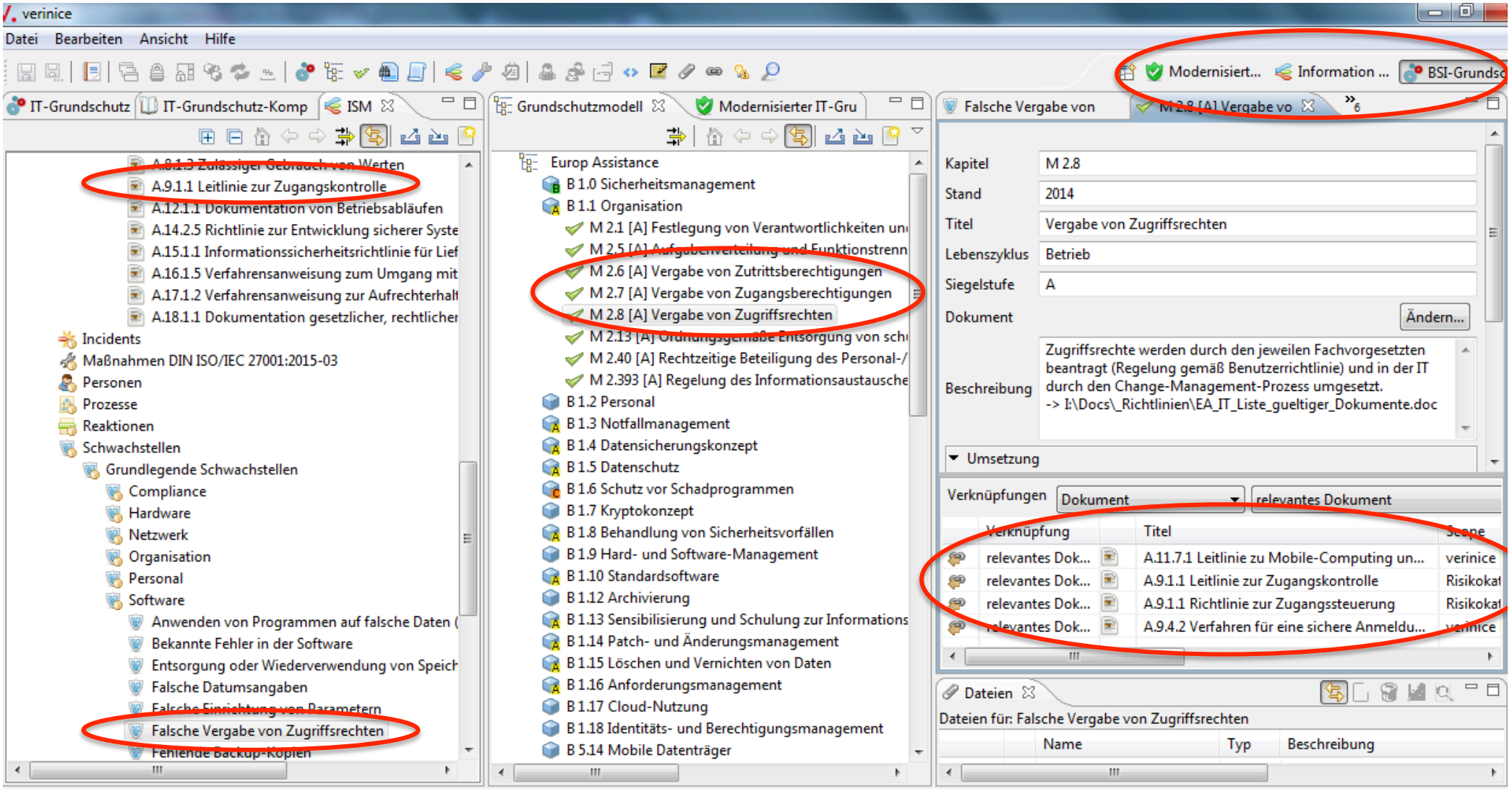
verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Jetzt geht‘s um Transparenz und Komfort mit verinice - Dokumente/Dateien anhängen



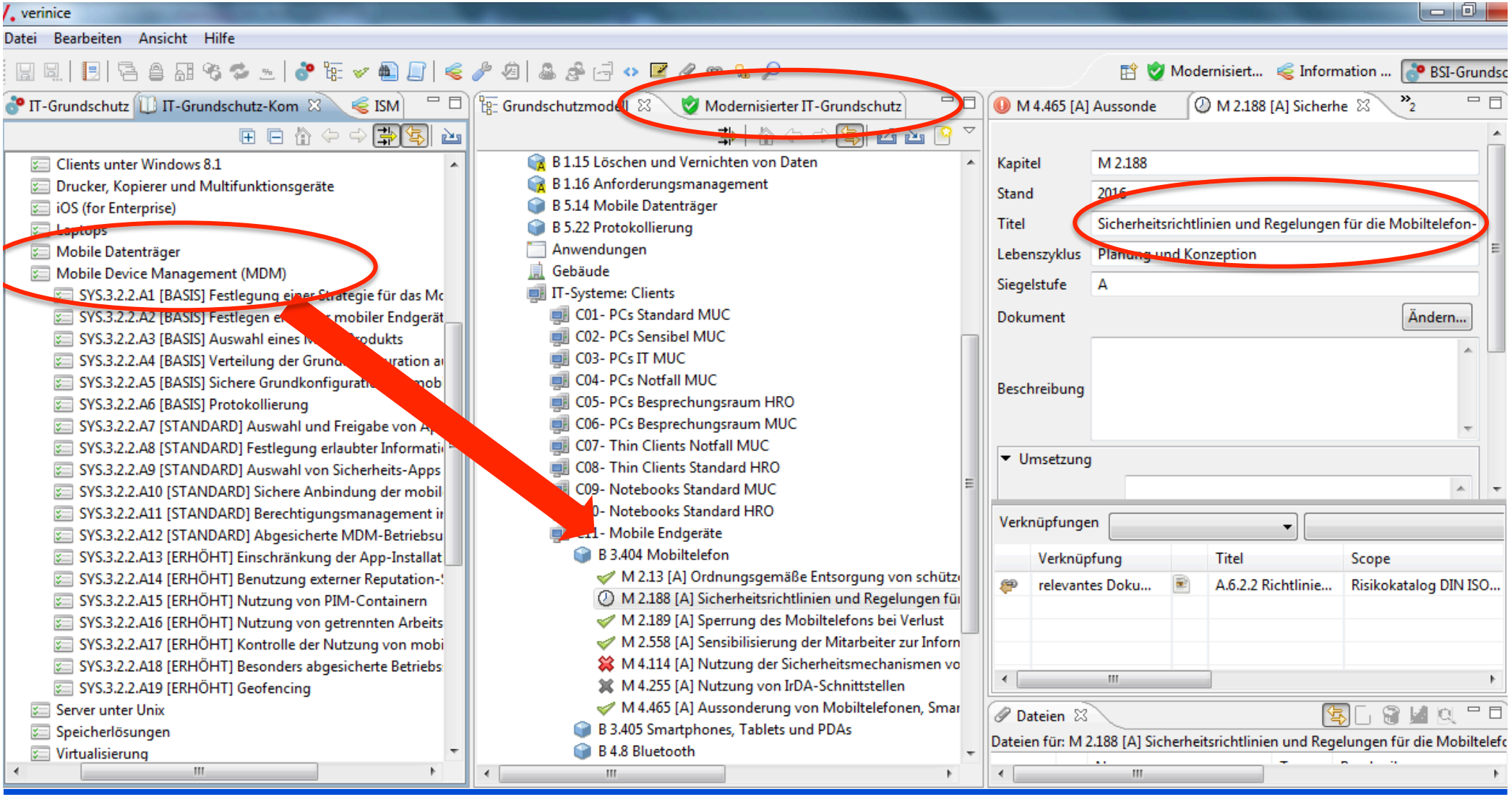
verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Jetzt geht‘s um Transparenz und Komfort mit verinice - Nutzung von BSI plus ISO 27001



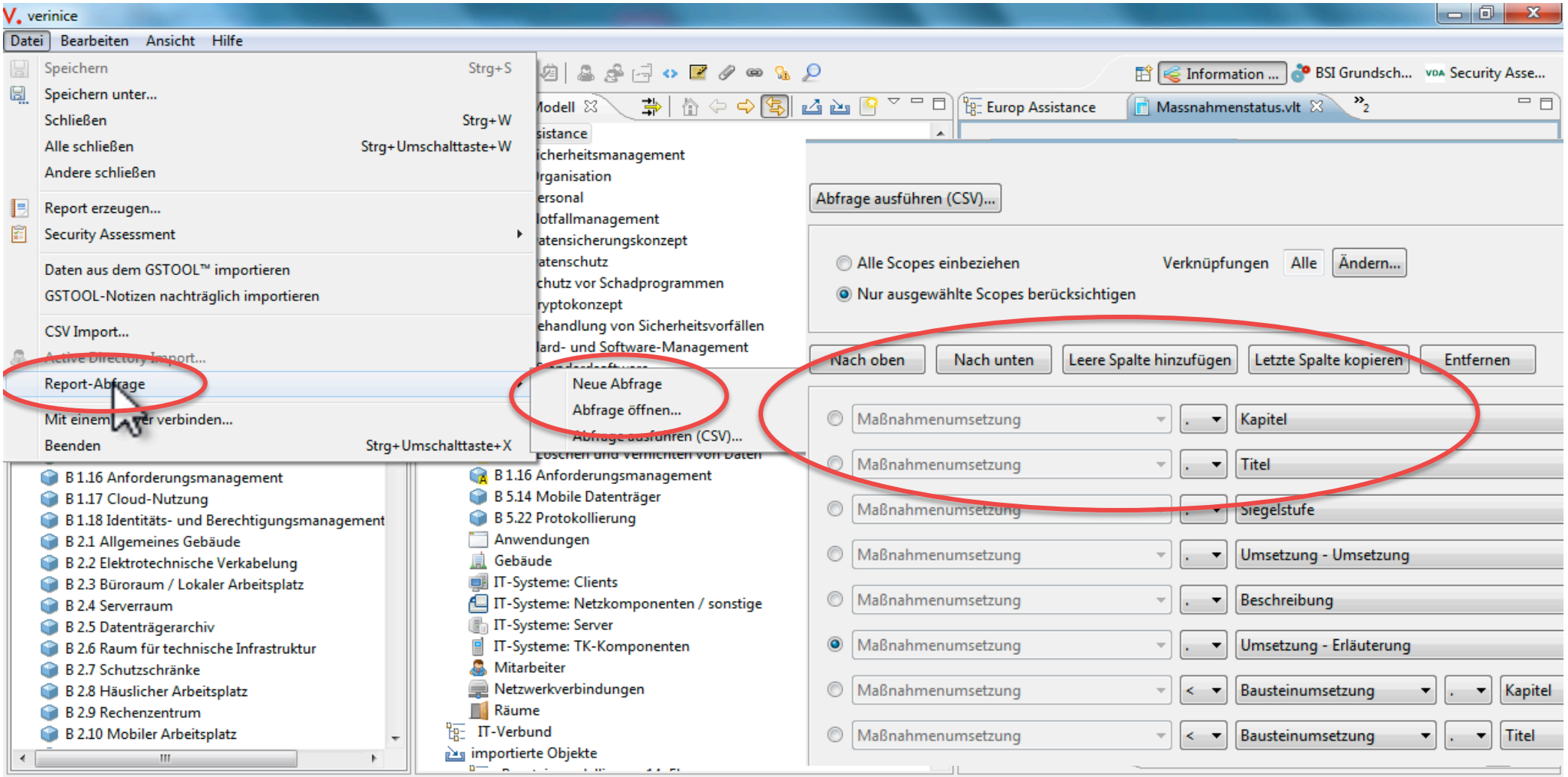
verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Jetzt geht‘s um Transparenz und Komfort mit verinice – „hybride“ Nutzung, z.B. MDM



verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Die Entscheidung für verinice hat für alle Beteiligten spürbaren Nutzen gebracht
Aggregierte Sicht der Maßnahmen => sprechende Übersicht mit Link Table Report LTR



verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Die Entscheidung für verinice hat für alle Beteiligten spürbaren Nutzen gebracht
Aggregierte Sicht der Maßnahmen => sprechende Übersicht mit Link Table Report LTR

Maßnahmen (Stufe A)	Baustein	Umsetzung bis	Lebenszyklus	Umsetzung durch	Initiierung durch	Aufwand (in PT)	Bemerkungen
M 2.193 [A] Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit	B 1.0 Sicherheitsmanagement	28.02.2014	Umsetzung	Leiter IT	IT-Sicherheitsbeauftragter	1	- Sicherheitsbeauftragter ist benannt und bei relevanten Entscheidungen beteiligt; aber Aufgaben und Kompetenzen im Sicherheitsteam sind noch nicht definiert
M 2.335 [A] Festlegung der Sicherheitsziele und -strategie	B 1.0 Sicherheitsmanagement	28.02.2014	Planung und Konzeption	IT	IT-Sicherheitsbeauftragter	2	- Mitarbeiter sind per Rundschreiben auf die Sicherheitsziele hinzuweisen; der Zugriff auf die Sicherheitsleitlinie ist zu gewährleisten
M 2.1 [A] Festlegung von Verantwortlichkeiten und Regelungen	B 1.1 Organisation	28.02.2014	Planung und Konzeption	Leiter IT	IT-Sicherheitsbeauftragter	1 / Monat	- Verantwortlichkeiten und Befugnisse im IT-Bereich regeln und dokumentieren
M 2.5 [A] Aufgabenverteilung und Funktionstrennung	B 1.1 Organisation	28.02.2014	Planung und Konzeption	Leiter IT	IT-Sicherheitsbeauftragter	1	- Dokument zur Funktionstrennung in der IT liegt vor, ist noch an den EA-Standard zur Dokumentation von Richtlinien anzupassen
M 2.6 [A] Vergabe von Zutrittsberechtigungen	B 1.1 Organisation	28.02.2014	Planung und Konzeption	Leiter IT	IT-Sicherheitsbeauftragter	1	- Schutzbedarf der Räume ist bestimmt; Dokument über den Zugang zum Serverraum noch an den EA-Standard zur Dokumentation von Richtlinien anpassen
M 2.7 [A] Vergabe von Zugangsberechtigungen	B 1.1 Organisation	28.02.2014	Planung und Konzeption	Leiter IT	stv. IT-Sicherheitsbeauftragter	3	- Dokumentation über Vergabe und Entzug von Zugangsberechtigungen erstellen
M 3.3 [A] Vertretungsregelungen	B 1.2 Personal	28.02.2014	Betrieb	Leiter Fachabteilung, Leiter Organisation, Leiter Personal	IT-Sicherheitsbeauftragter	1 / Quartal	- Vertretungsregelungen in allen für die Informationssicherheit relevanten Bereichen verabschieden und kommunizieren
M 6.41 [A] Übungen zur Datenrekonstruktion	B 1.4 Datensicherungskonzept	28.02.2014	Notfallvorsorge	IT	stv. IT-Sicherheitsbeauftragter	1	- Prüfen, ob ein sachverständiger Dritter die Datenrestaurierung anhand vorhandener Dokumentation durchführen kann.
M 2.154 [A] Erstellung eines Sicherheitskonzeptes gegen Schadprogramme	B 1.6 Schutz vor Schadprogrammen	28.02.2014	Planung und Konzeption	IT	stv. IT-Sicherheitsbeauftragter	2	- im Rahmen des IT-Betriebs gewährleistet; IT-Sicherheitshandbuch auf Aktualität und Vollständigkeit überprüfen (ggf. anpassen)
M 2.158 [A] Meldung von Schadprogramm-Infektionen	B 1.6 Schutz vor Schadprogrammen	28.02.2014	Betrieb	Leiter IT	stv. IT-Sicherheitsbeauftragter	1	- Zentrale Meldestelle für Schadprogram-Vorfälle festlegen und kommunizieren - Prüfen, ob Meldepflicht besteht
M 2.34 [A] Dokumentation der Veränderungen an einem bestehenden System	B 1.6 Schutz vor Schadprogrammen B 1.9 Hard- und Software-Management	28.02.2014	Betrieb	IT	stv. IT-Sicherheitsbeauftragter	1	- Die Aufzeichnungen von Veränderungen, die Administratoren am System vornehmen, müssen für alle fachkundigen Personen G5ausreichend und nachvollziehbar sein -> prüfen - Prüfen, ob die Aufzeichnungen im Helpdesktool vor unberechtigtem Zugriff geschützt sind

Individuelles Reporting – auf Basis des LTR-Outputs

verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Erfolgreicher Audit - nicht zuletzt wegen transparenter Dokumentation und Reports

Bundesamt
für Sicherheit in der
Informationstechnik

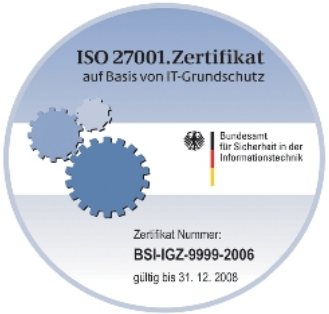
Durchführung eines Vor-Audits – Beschreibung des Iformationsverbunds

Der für das Managementsystem zur Informationssicherheit relevante IT-Verbund der Europ Assistance Deutschland umfasst die beiden rechtlich getrennten Gesellschaften Europ Assistance AG und Europ Assistance Services GmbH an den beiden Standorten Adenauerring 9, 81737 München, und Am Strande 3a, 18055 Rostock.

Beide deutschen Gesellschaften sind Teil der internationalen Europ Assistance, ein Tochterunternehmen der GENERALI-Gruppe, und erbringen mit rund 300 Mitarbeitern an den beiden Standorten München und Rostock (Stand 2016) die folgenden, für das operative Geschäft wesentlichen **Kernprozesse**:

- Festlegung der strategischen Ausrichtung („Commercial strategy")
- Kundenakquisition und Vertrieb ("Implementation & monitoring of contracts")
- Vertragsverwaltung ("Underwriting B2C contracts")
- In-/Exkasso von Prämien und Umsätzen („Premium / turnover management")
- Schadensabwicklung ("Case / claims management ")
- Qualitäts- und Beschwerdemanagement ("Management of client relationship")
- Suche, Auswahl und Monitoring von Dienstleistern („Network monitoring")
- Auswahl und Abrechnung von Rückversicherern („Reinsurance management")

Der IT-Verbund erstreckt sich über diese Kernprozesse mit den Supportprozessen „HR Management" und „IT Management" sowie über alle von der zentralen IT in München (derzeit 14 Mitarbeiter) in Eigenverantwortung bereitgestellten IT-Anwendungen, IT-Services und IT-Komponenten.



activeMind · AG

Auditbericht zum Voraudit
zum Auditor-Testat "Einstiegsstufe" nach
ISO 27001 auf der Basis von IT-Grundschutz

Auditierte Institution: *Europ Assistance Versicherungs-AG*
Zertifizierungskennung: *noch keine*

Vertraulich!
Keine Weitergabe ohne schriftliche Genehmigung!
Der Inhalt dieses Auditreports richtet sich ausschließlich an die in Kapitel 1.7 genannten Empfänger.

Bericht zum Voraudit Seite 1 von 29

verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Aktuelle Herausforderung: Bewertung der Maßnahmen (TOMs) nach EU-DSGVO
Sicherheit in der Verarbeitung nach Artikel 32 EU-DSGVO - Stand der Technik

Phase 1 „Set Up“ → **Phase 2** „Gap“-Analyse → **Phase 3** Handlungs-felder → **Phase 4** Risikoanalyse/ Roadmap → **Phase 5** Umsetzungs-Unterstützung

Allgemein anerkannte Regeln der Technik

- Schriftlich fixierte oder mündlich überlieferte technische **Festlegungen**
- Für Verfahren, Einrichtungen und Betriebsweisen, die nach **herrschender Auffassung von Fachleuten**, Anwendern, Verbrauchern und der öffentlichen Hand die **Eignung besitzen**,
- das **gesetzlich vorgegebene Ziel** zu erreichen und
- die sich in der Praxis **allgemein bewährt** haben bzw. deren Bewährung in naher Zeit bevorsteht

Stand der Technik

- Entwicklungsstand **fortschrittlicher Verfahren**, Einrichtungen und Betriebsweisen,
- der nach **herrschender Auffassung** führender Fachleute das Erreichen des gesetzlich vorgegebenen **Ziels gesichert** erscheinen lässt, wenn sich
- die entsprechenden Verfahren bereits in der Praxis **bewährt haben** oder zumindest aber im Betrieb mit Erfolg **erprobt wurden**

Stand von Wissenschaft und Technik

- Entwicklungsstand **fortschrittlichster Verfahren**
- Nach Auffassung **führender Fachleute** aus Wissenschaft und Technik
- Auf der Grundlage **neuester wissenschaftlich vertretbarer Erkenntnisse** im Hinblick auf das gesetzgeberische Ziel für erforderlich gehalten
- **Zielerreichung** erscheint gesichert

verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Aktuelle Herausforderung: Bewertung der Maßnahmen (TOMs) nach EU-DSGVO
Sicherheit in der Verarbeitung nach Artikel 32 EU-DSGVO - Stand der Technik

verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Aktuelle Herausforderung: Bewertung der Maßnahmen (TOMs) nach EU-DSGVO
Wir müssen wieder in die Betrachtung des konkreten Schutzbedarfes einsteigen

Beispiel

Maßnahmen / TOMs	Stand der Technik	
	Objektiv-technisch	Best Practices
Stand der Technik für Mobile Devices		
Sichere Konfiguration der mobilen Geräte zur Verhinderung einer unerwünschten Kopplung zwischen dem Firmennetz und Internet	Das mobile Gerät muss seine Konfiguration von einem Mobile Device Management System (MDM) entgegen nehmen können und auf sichere Art verwalten - vgl. Mindeststandard des BSI	Benutzerrichtlinie zum Einsatz von Mobile Devices; die Wirksamkeit lässt sich aber nur über MDM prüfen Richtlinie zur Administration von Mobile Devices
Verbieten der Option, dass Daten automatisch in „die Cloud“ synchronisiert werden	Richtlinie für Verhinderung der Installation aus unsicheren Quellen, Einsatz von Mobile-Device-Management-Lösungen	Benutzerrichtlinie zum Einsatz von Mobile Devices; Trennen des Geräts in eine „private“ und eine „Firmen“-Arbeitsumgebung
Stand der Technik zum Berechtigungsmanagement		
Unberechtigten Zugang zu IT-Systemen verhindern	Schwachstellen-Scanner zur Feststellung, wer auf was - ggf. mit falschem Passwort - versucht, zuzugreifen SW-Lösung, die den Prozess end-to-end managen kann	High-Level-Prozess zum Berechtigungsmanagement etablieren (u.a. „Folder“-Owner in den Genehmigungs-Workflow involvieren) Richtlinie um Berechtigungsmanagement (BSI IT-Grundschutz B 1.18)

verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Kritischer Erfolgsfaktor ist und bleibt hier die Verantwortung der Führungskräfte
Ermitteln des Schutzbedarfs der eigenen Prozesse und wesentlicher Verfahren

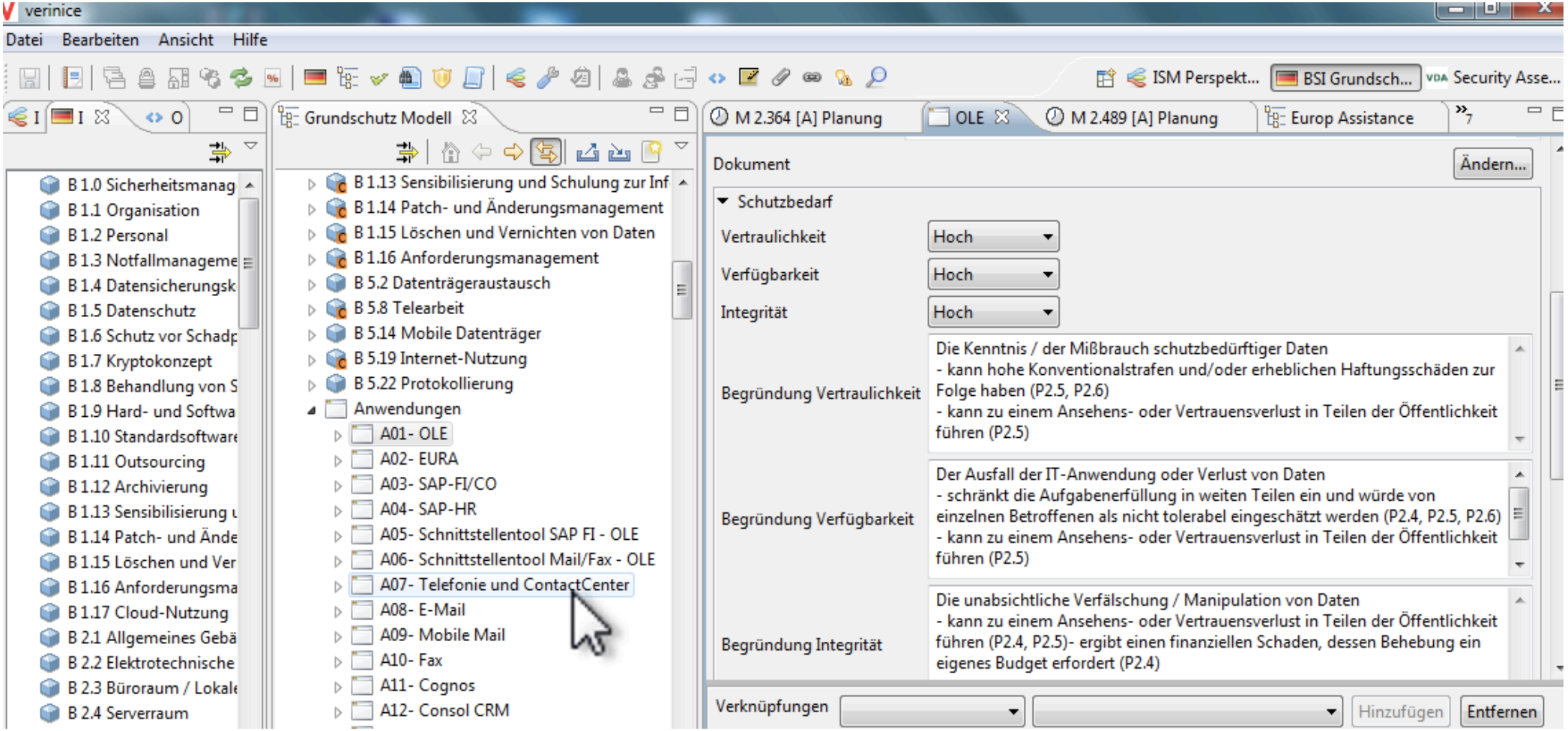
Phase 1 „Set Up“ | **Phase 2 „Gap“-Analyse** | **Phase 3 Handlungs-felder** | **Phase 4 Risikoanalyse/ Roadmap** | **Phase 5 Umsetzungs-Unterstützung**

Interviews mit Prozessverantwortlichen

lfd. Nr.	Wesentliche Verfahren	Mögliches Schadensszenario	Vertrau-lichkeit	Integrität	Verfüg-barkeit	Kommentar
1	OLE	1. Verstoß gegen Gesetze/ Vorschriften/Verträge	hoch	normal	normal	Zahlungen erfolgen
		2. Negative Innen- oder Außenwirkung	hoch	hoch	hoch	über OLE, kein direkter
		3. Finanzielle Auswirkungen	normal	normal	normal	Zugriff auf SAP FI/CO
		4. Beeinträchtigung der Aufgabenerfüllung	normal	normal	hoch	
		5. Beeinträchtigung des informationellen Selbstbestimmungsrechts	normal	normal	normal	
		6. Beeinträchtigung der persönlichen Unversehrtheit	normal	normal	normal	
2	Schnittstellen	1. Verstoß gegen Gesetze/ Vorschriften/Verträge	normal	normal	normal	erzeugt Zahlungsdatei
	OLE - SAP	2. Negative Innen- oder Außenwirkung	normal	normal	normal	für SAP FI aus OLE
		3. Finanzielle Auswirkungen	normal	normal	normal	
		4. Beeinträchtigung der Aufgabenerfüllung	normal	normal	normal	
		5. Beeinträchtigung des informationellen Selbstbestimmungsrechts	normal	normal	normal	
		6. Beeinträchtigung der persönlichen Unversehrtheit	normal	normal	normal	
3	Telefonie/	1. Verstoß gegen Gesetze/ Vorschriften/Verträge	normal	normal	normal	systemimmanente
	Contact Center	2. Negative Innen- oder Außenwirkung	normal	normal	normal	Fallback-Lösung; nur
		3. Finanzielle Auswirkungen	normal	normal	normal	Leitungsausfall kritisch
		4. Beeinträchtigung der Aufgabenerfüllung	normal	normal	hoch	
		5. Beeinträchtigung des informationellen Selbstbestimmungsrechts	normal	normal	normal	
		6. Beeinträchtigung der persönlichen Unversehrtheit	normal	normal	normal	
4	E-Mail	1. Verstoß gegen Gesetze/ Vorschriften/Verträge	normal	normal	normal	Wenn nicht aus OLE,
		2. Negative Innen- oder Außenwirkung	hoch	normal	normal	dann verschlüsselt
		3. Finanzielle Auswirkungen	normal	normal	normal	(Gesundheitsdaten
		4. Beeinträchtigung der Aufgabenerfüllung	normal	normal	normal	nur verschlüsselt)

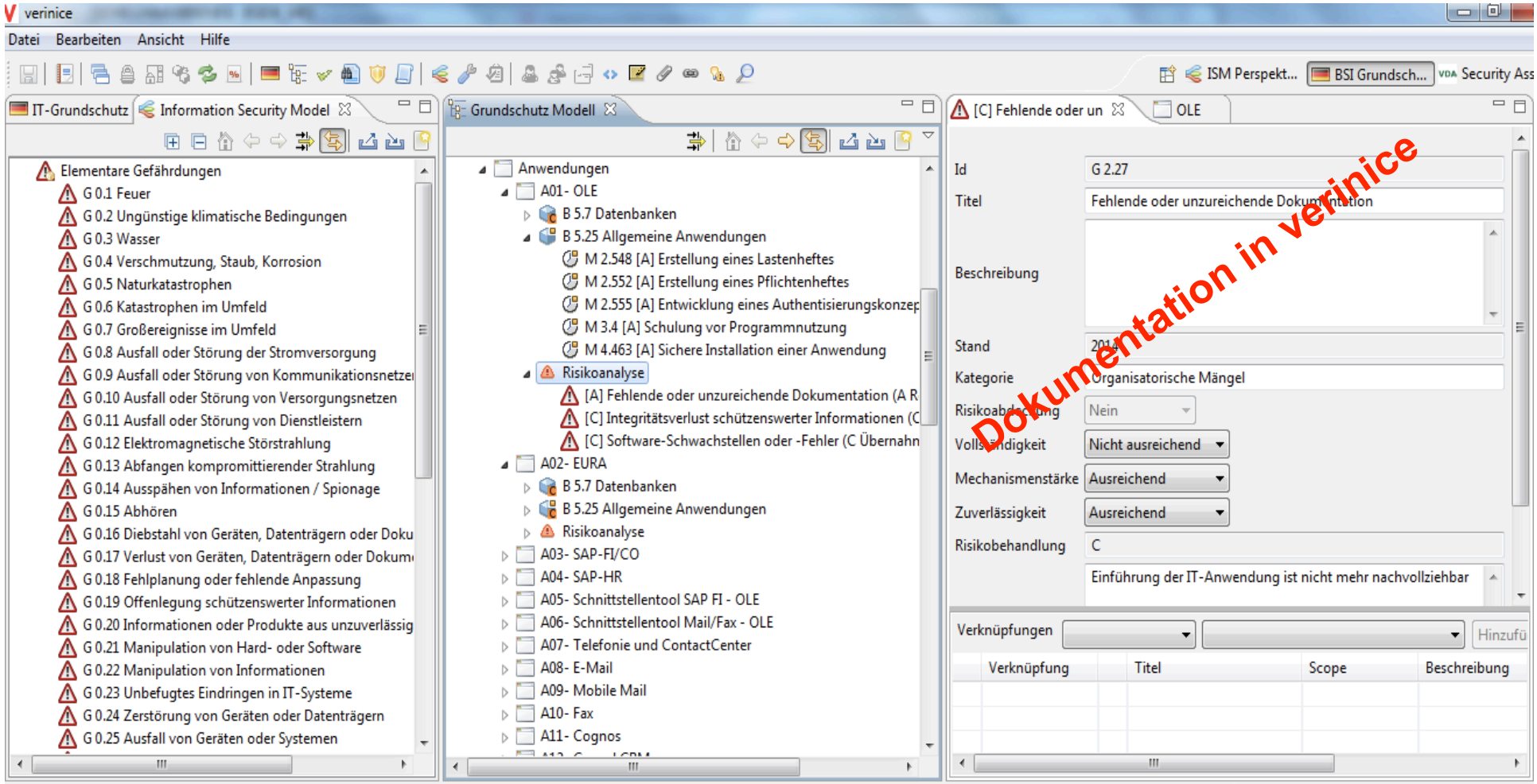
verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Kritischer Erfolgsfaktor ist und bleibt die Verantwortung der Führungskräfte
Hier hilft ungemein die transparente Dokumentation des Schutzbedarfs in verinice



verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Kritischer Erfolgsfaktor ist und bleibt die Verantwortung der Führungskräfte
Der Clou in verinice: Straffes Risikomanagement durch übersichtliche Dokumentation



verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Kritischer Erfolgsfaktor ist und bleibt die Verantwortung der Führungskräfte

Managementsystem für Informationssicherheit
Restrisikobetrachtung

Status:	in Bearbeitung	Version 1.0	INTERN
Erstellt von:	Kay Romeis	Erstellt am:	05.07.16
Autorisiert durch:	Andreas Kelz	Ersatz für:	-
Gültig ab:	xx.xx.xxxx	Gültig bis:	Widerruf

Lfd. Nr. 1	Anforderungen an Anwendungen	Bemerkung
Risikobeschreibung	Verstoß gegen gesetzliche Regelungen	Der Einfluss gesetzlicher Bestimmungen auf Anwendungen muss berücksichtigt werden. Das Controlling-Tool MS Excel ist für den derzeitigen Einsatz nicht geeignet und sollte ersetzt werden.
bisher umgesetzte Maßnahmen	-	
Empfehlung	Auftrag an die zuständige Stelle erteilen	Risikoübernahme bis Erledigung

Lfd. Nr. 2	Dateiberechtigungen	Bemerkung
Risikobeschreibung	Unerlaubte Ausübung von Rechten / Vertraulichkeitsverlust	Zugriffsrechte auf Dateien müssen geregelt sein und regelmässig mit geeigneten Hilfsmitteln überprüft werden.
bisher umgesetzte Maßnahmen	Erstellung eines Berechtigungskonzepts ist in Arbeit.	
Empfehlung	Auftrag an die zuständige Stelle erteilen	Risikoübernahme bis Erledigung

Lfd. Nr. 3	Netz- und Systemmanagement	Bemerkung
Risikobeschreibung	Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement	Die Protokollierung der Netznutzung muss Datenschutzgesetzen genügen, sollte einen ausreichenden Umfang haben und durch entsprechende Analysewerkzeuge unterstützt werden.
bisher umgesetzte Maßnahmen	Einführung Monitoring-Tool	
Empfehlung	Auftrag an die zuständige Stelle erteilen	Risikoübernahme bis Erledigung

- Es liegt in der Verantwortung der EA-Führungskräfte, welche Maßnahmen in welcher Reihenfolge ergriffen werden und wo Restrisiken verbleiben.
- Bei der Umsetzung der Maßnahmen orientiert sich EA an dem Stellenwert, den die jeweilige Maßnahme im Sicherheitskonzept hat. Sogenannte A-Maßnahmen (A=Einstieg entsprechend der BSI-Qualifizierungsstufe) und Maßnahmen, die im Grundschutz der Phase "Planung und Konzeption" zugeordnet sind, werden vorrangig umgesetzt.
- Verbleibt nach Durchführung aller vorgesehenen Sicherheitsmaßnahmen ein Restrisiko, dessen weitere Reduktion technisch nicht möglich oder wirtschaftlich nicht sinnvoll ist, so besteht die Möglichkeit einer bewussten Akzeptanz des Restrisikos.

verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Fazit: Das Management der Informationssicherheit hat 2017 funktioniert. Und nun: „Das einzig Beständige ist der Wandel“ oder „Never change a winning team“?

Was wir tun, um Informationssicherheit immer weiter zu verbessern

- **Voraussetzungen für das Managementsystem nach BSI optimieren**
  - ✓ Richtlinienstandard verbessern („Einer muss immer Aufwand reinstecken - entweder der, der die Richtlinie erstellt, oder der, der sie lesen muss“)
- **Regelungen optimieren, die sich um personenbezogene Daten drehen**
  - ✓ Benutzerrichtlinie; Richtlinie Berechtigungsmanagement; E-Mail-Richtlinie; Umgang mit Sicherheitsvorfällen; mobile IT-Systeme; externe Dienstleister
- **Prozesse zur Identifizierung verdächtiger Mails entwickeln und etablieren**
- **Anforderungen an die geplante Cloud-Migration aus BSI-Sicht durchsetzen**
- **Erfolgreiche Sensibilisierung und Schulung weiter vorantreiben**
  - ✓ Neben Präsenzschulung E-Learning Module für Online-Training anbieten
- **Trotz Empfehlungen des BSI keine schnelle Migration zum modernisierten Grundschutz -> Wir testen das erstmal ausführlich in verinice 1.15**

verinice bei Europ Assistance - Aufrechterhaltung des Sicherheits-Levels

Transformation Consulting International

Holger Schellhaas

Interim-CISO der Haspa-Direkt
Partner der TCI Transformation Consulting International GmbH

mobile +49 (0) 170 240 85 70
holger.schellhaas@tci-partners.com

Persönliche Referenz:
Andreas Kelz
IT-Sicherheitsbeauftragter
Europ Assistance AG