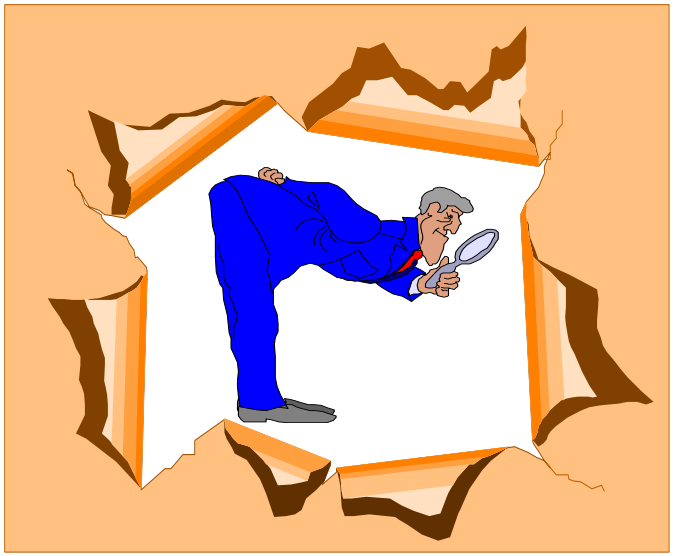
verinice.XP

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Best Practice Umsetzung nach ISO 27001 auf Basis BSI IT-Grundschutz



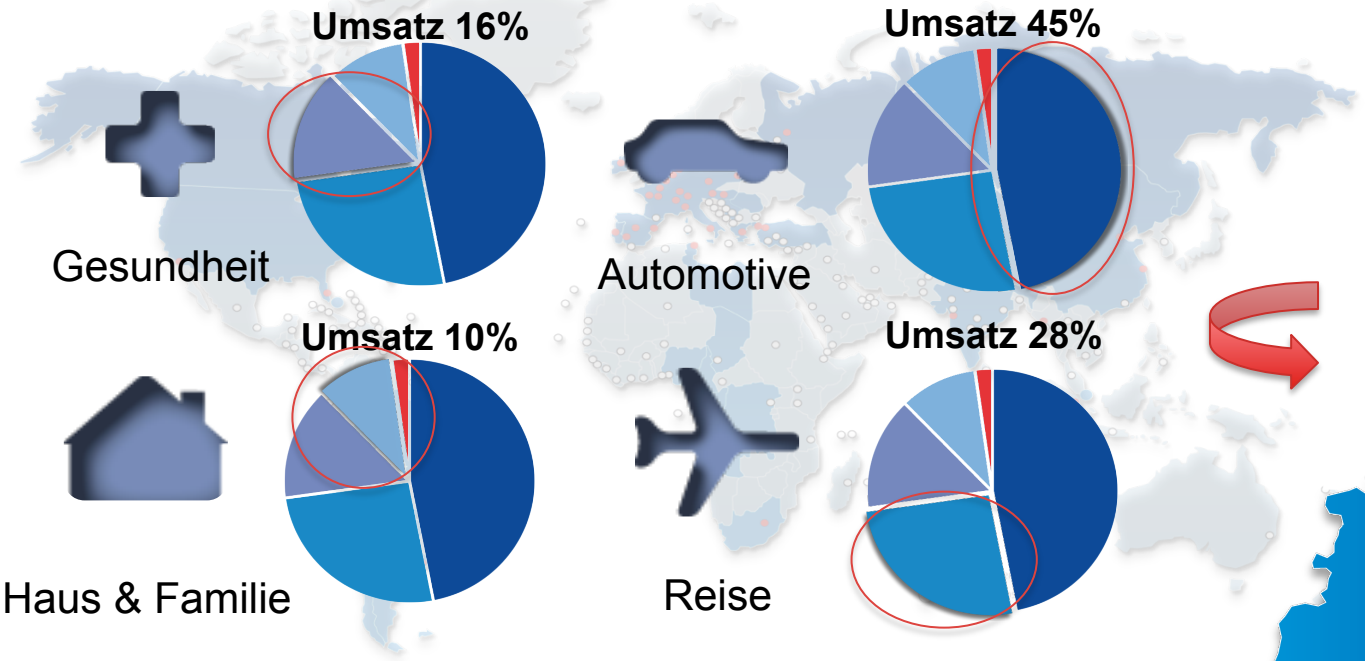
Holger Schellhaas
Management Consulting & Training
Partner der TCI Transformation Consulting International GmbH
Interims-CISO MerckFinck Privatbankiers

Berlin, 06. Februar 2017

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Weltweite Präsenz der EA-Gruppe in vier strategischen Geschäftsfeldern

Mission Statement: « Den Alltag der Menschen erleichtern und ihre Mobilität sichern - weltweit. Durch individuell bereitgestellte Lösungen rund um die Uhr »



Mitarbeiter
< 300

IT-Mitarbeiter
z.Zt. 14

Bearb. Anrufe p.a.
> 400 000

Rund 8 300 Mitarbeiter

Rund 40 Niederlassungen in 33 Ländern

Rund 1,3 Mrd. €
konsolidierter Umsatz 2014

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Aufgrund der zunehmenden Anfragen von Großkunden im Bereich der gesetzlichen Krankenversicherungen, begann Europ Assistance Deutschland, 2013 ein Informations-Sicherheits-Management-System (ISMS) einzuführen.

Kunden-anforderungen

- Die Kunden fordern von uns eine angemessene Informationssicherheit
- zuverlässige Serviceleistungen
- Sicherer Umgang mit Kundendaten
- Ausrichtung an Standards (ISO und BSI-Grundschutz)

Rechtliche Vorgaben

- Anforderungen der „Mutter“ GENERALI
- Datenschutz (BDSG)
- Das neue IT-Sicherheitsgesetz
- Haftungsfragen
- Compliance (z.B. Solvency II, MaRisk)
- Patientenschutz

Eigen-interesse

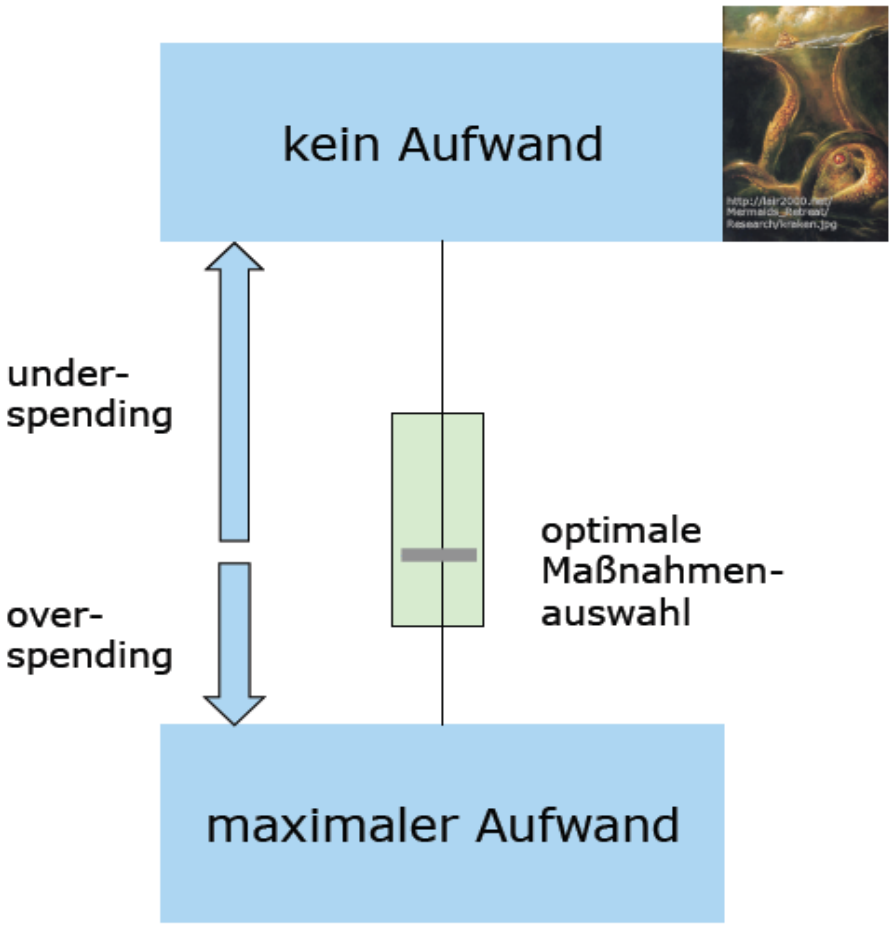
- Schutz von Informationen und Wissen (Know How)
- Schutz der IT-Infrastruktur
- Kooperation mit Wett-bewerbern
- Image in der Öffentlichkeit
- Schutz der Mitarbeiter

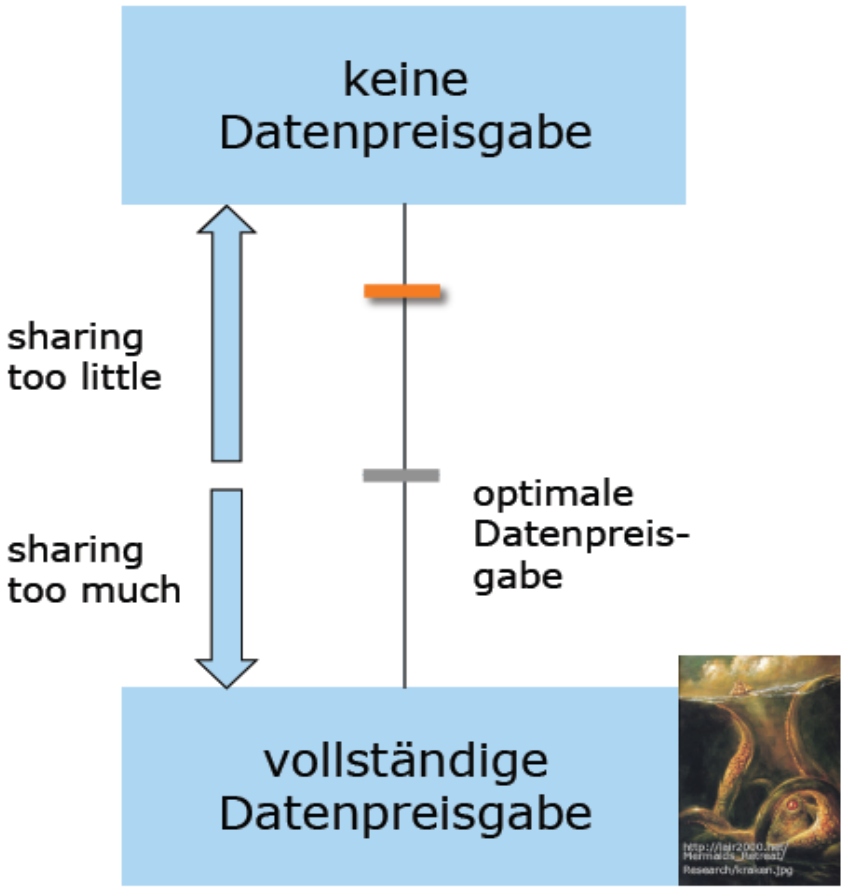
Entscheidung der Leitungsebene

Ziel war und ist, in kleinen „verdaubaren“ Schritten die Zertifizierungsfähigkeit nach ISO 27001 auf Basis BSI IT-Grundschutz zu erlangen.

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

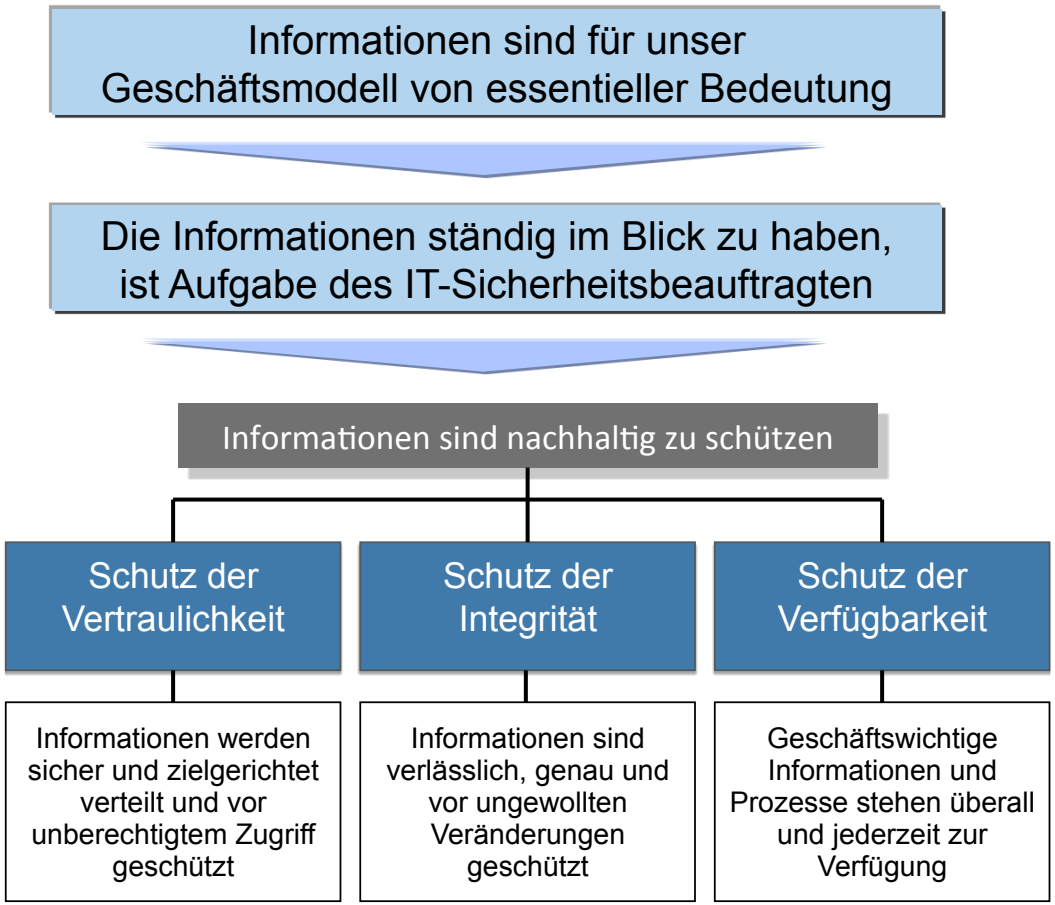
Auftrag der GL: IT-Sicherheitskonzept umsetzen - angemessenes Sicherheitsniveau mit den Fachbereichen festlegen - Akzeptanz und Zertifizierungsfähigkeit schaffen





Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Die Rolle des IT-Sicherheitsbeauftragten wird durch den IT-Leiter übernommen



Der IT-Sicherheitsbeauftragte etabliert, koordiniert und überwacht die IT-Sicherheit der Europe Assistance Deutschland, d.h.

- IT-Sicherheitskonzept entwickeln
  Abstimmung im Unternehmen
  Freigabe bei GF (Vorstand) einholen
  Umsetzung initiieren
- IT-Sicherheitsrichtlinien erstellen
  Einhaltung überwachen
- Erstellen einer vollständigen Übersicht über vorhandene IT-Systeme
- Reporting an GF
- Permanente Anpassung des Sicherheitskonzeptes
- Regelmäßige Schulung und Sensibilisierung aller Beteiligten

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Die Entscheidung für BSI IT-Grundschutz schafft spürbaren Nutzen - angepasst durch unseren Healthcheck Informationssicherheit: IT-Compliance mit BSI IT-Grundschutz

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

- **Scoping / Zielbild erarbeiten**
- **Dokumenten-analyse**
- **Prüfungs-aktivitäten planen**
- **Gesprächspartner festlegen**

Vorgehen:

- „Zielbild erarbeiten“: Workshop zur Definition der Anforderung an mit klaren Aussagen, wie das Management BSI IT-Grundschutz angemessen in den nächsten drei Jahren umsetzen will
- Anforderungsdefinition: Erwartungen aller beteiligten Bereiche an ein effektives Managementsystem zur Informationssicherheit
- „Burning Plattform“ entwickeln:
  - ✓ Welche Business-Probleme stehen hinter der geplanten Veränderung des Mindestlevels zur Informationssicherheit?
  - ✓ Ist die IT reif, aus Veränderungen nachhaltigen Nutzen zu ziehen?
- **Passendes Tool auswählen: Klare Entscheidung der EA für verinice**

Erwartete Ergebnisse:

- Mögliche Szenarien zur Steuerung der Anforderungen der Nutzer
- Kenntnis der Rahmenbedingungen
- Beurteilung der Erfolgschancen von Änderungen

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Die Entscheidung für BSI IT-Grundschutz schafft spürbaren Nutzen - auch im Mittelstand

Für die Umsetzung haben wir den modernisierten Ansatz bereits vorweg genommen: Sinnvolles Vorgehen, um das angestrebte angemessene Sicherheitsniveau zu erreichen

„Bonsai-ISMS“ der Basis-Absicherung

Erstellung einer Leitlinie zur Informationssicherheit

Organisation des Sicherheitsprozesses

- Rollen und Aufgaben festlegen
- Informationssicherheit in Abläufe und Prozesse integrieren
- Umsetzung überwachen

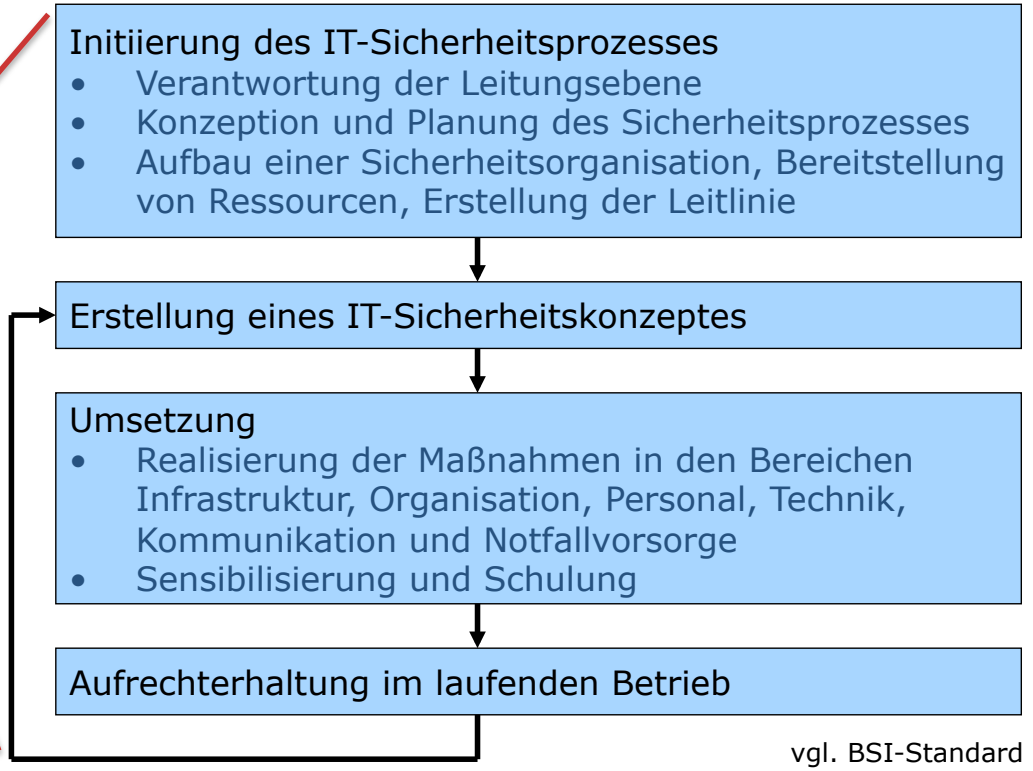
Bereitstellung von Ressourcen

- Angemessen und wirtschaftlich, aber Informationssicherheit kostet Geld!

Einbindung aller Mitarbeiter in den Sicherheitsprozess

Auswahl und Anpassung von Bausteinen

- Umsetzungsreihenfolge der Bausteine

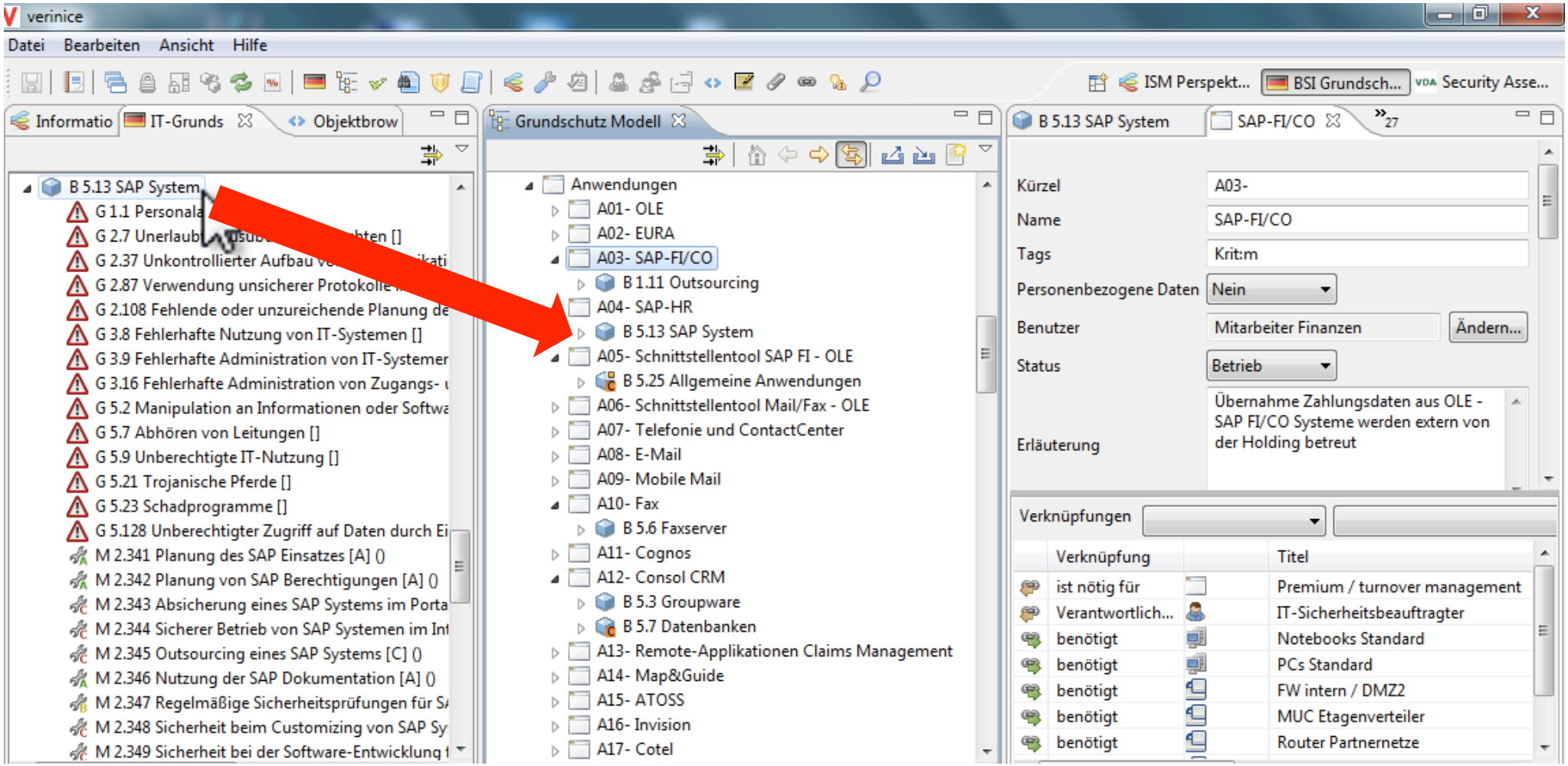


vgl. BSI-Standard 100-2

Quelle: 2. IT-Grundschutz-Tag 2016
Modernisierung des IT-Grundschutzes
Vortrag Holger Schildt

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Die Entscheidung für BSI IT-Grundschutz schafft spürbaren Nutzen - ohne passenden Tool-Einsatz nicht sinnvoll durchführbar => verinice eingeführt und Team überzeugt



Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Die Entscheidung für BSI IT-Grundschutz schafft spürbaren Nutzen - angepasst durch unseren Healthcheck Informationssicherheit: IT-Compliance mit BSI IT-Grundschutz

- Checklisten, Interviews, Workshops
- Stärken-/ Schwächen-analyse
- Reifegrad-Ampel
- Empfehlungen für Sofort-maßnahmen

Vorgehen:

- Gestützt auf das Zielbild bewerten wir mit einem Soll-/Ist-Vergleich das „Gap“ zwischen vorhandenem Sicherheitsniveau und BSI
- **Wesentliche Kriterien, u.a.:**
  - ✓Positionierung der IT, Richtlinien und Verantwortlichkeiten
  - ✓Organisation der IT und der Informationssicherheit
  - ✓Qualität der IT-Prozesse, speziell zu IT-Security & Datenschutz
  - ✓Zugriffskontrollen und Berechtigungskonzepte
- Einsatz bewährter Checklisten - auf Basis von ISO-Standards und Best Practices (ISO/IEC 27001, BSI Grundschutz, COBIT, Prüfstandard IDW)

Erwartete Ergebnisse:

- Reifegrad und IT-Compliance bzgl. der Bewertungsdimensionen
- Einbeziehung aller betroffenen Bereiche („Awareness“ schaffen)
- Identifikation des Transformationsbedarfs (Schwerpunkte)

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Die Entscheidung für BSI IT-Grundschutz schafft spürbaren Nutzen - endlich Struktur

Erfolgsfaktor Individuelles Reporting

Zuordnung IT-Anwendungen zu IT-Systemen

Informationsverbund:	Europ Assistance
Organisation:	Europ Assistance
Mitarbeiter:	300
Geltungsbereich:	Definierter IT-Verbund
Datum:	14.07.15 17:08
Autor:	Kay Romeis
Version:	SerNet verinice 1.10 - BSI IT-Grundschutz EL13
Freigabe:	Andreas Kelz

Anwendung	zugehöriger Prozess	Pers.-bez. Daten	IT-System Server	IT-System-Clients	IT-System Netz/TK
A01- OLE	Case / claims management Management of client Premium / turnover management	X	S01- Datenbank-Cluster S11- Terminalserver	C01- PCs Standard C02- Thin Clients C03- Notebooks Standard	ITS02- Switches VLAN:NFS ITS07- MUC Etagenverteiler ITS08- HRO Etagenverteiler ITS13- Router MPLS MUC ITS14- Router MPLS HRO
A02- EURA	Premium / turnover Underwriting B2C contracts	X	S01- Datenbank-Cluster	C01- PCs Standard C03- Notebooks Standard	ITS02- Switches VLAN:NFS ITS07- MUC Etagenverteiler ITS13- Router MPLS MUC ITS14- Router MPLS HRO TK04- Netzdrucker
A03- SAP-FI/CO	Premium / turnover management			C01- PCs Standard C03- Notebooks Standard	ITS01- Switches VLAN:LAN ITS04- Switches FW Fortinet ITS07- MUC Etagenverteiler ITS09- FW intern / DMZ2 ITS12- Router Partnernetze
A04- SAP-HR	HR management	X	S06- SAP-Server	C01- PCs Standard C03- Notebooks Standard	ITS01- Switches VLAN:LAN ITS07- MUC Etagenverteiler

Individuelles Reporting - Zuordnung der IT-Anwendungen zu IT-Systemen

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Die Entscheidung für BSI IT-Grundschutz schafft spürbaren Nutzen - endlich Struktur
Aggregierte Übersicht über Maßnahmen => Workflow mit dem IT-Sicherheitsteam

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 – sortiert nach Maßnahmen

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Die Entscheidung für BSI IT-Grundschutz schafft spürbaren Nutzen
Basissicherheitscheck Report (A.4) aus verinice ergänzt durch „sprechende“ Übersicht *

Outsourcing	M 2.221	Änderungsmanagemen					Change Management Prozess ist vorhanden I:\Docs_Richtlinien\EA_IT_Liste_gueltiger_Dokumente.doc
Datensicherungskonzept	M 6.32	Regelmäßige Datensicherung					- Regelungen und Vorgehen bei der Datensicherung siehe I:\Docs\Server_Services\Backup\Backup_Recover.doc - Es werden regelmässig Notfalltests durchgeführt. Darunter befinden sich auch Wiederherstellungen von Datensicherungen. I:\Docs__NOTFALLKONZEPT\Not
Datensicherungskonzept	M 6.36	Festlegung des Minimaldatensicherungskonzeptes					Datensicherung ist im Rahmen des IT-Sicherheitshandbuchs geregelt (Aktualität und Vollständigkeit wird regelmäßig überprüft)
Datensicherungskonzept	M 6.37	Dokumentation der Datensicherung					- Wie Daten wiederhergestellt werden ist im Notfallkonzept und Backup_Recover-Dokument beschrieben: I:\Docs\Server_Services\Backup\Backup_Recover.doc I:\Docs__NOTFALLKONZEPT
Behandlung von Sicherheitsvorfällen	M 6.59	Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen					Aufgaben und Kompetenzen bei Sicherheitsvorfällen sind als als Teil des Incident Management Prozesses festgelegt
Mobiler Arbeitsplatz	M 2.309	Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung	A	Ja	- Sicherheitsrichtlinie zur mobilen IT-Nutzung erstellen.	30.04.14	# Benutzerrichtlinie regelt die mobile Nutzung von IT-Systemen und wird im Intranet bereitgestellt. # Teil der Schulungen zu Sicherheitsmaßnahmen # Eine Sicherheitsrichtlinie existiert nicht, die Inhalte werden aber in der "Richtlinie mobile IT-Systeme" ab
Mobiler Arbeitsplatz	M 1.15	Geschlossene Fenster und Türen	A	Teilweise	# Orgahandbuch ist allerdings nicht aktuell. # Wird darauf geachtet, dass Brand- und Rauchschutztüren tatsächlich geschlossen werden?	11.09.15	Verschluss ist geregelt im Orgahandbuch. Orgahandbuch ist allerdings nicht aktuell. # Eine regelmäßige Prüfung findet statt (IT-156478).

B 3.405	Smartphones, Tablets und PDAs
Erfasst am:	Mi, 25.02.2015
Erfasst durch:	
Gesprächspartner:	
Erläuterung:	
M 1.33	Geeignete Aufbewahrung tragbarer IT-	# Prüfen, ob eine Regelung
Umsetzung:	Umsetzung bis:	Umsetzung durch:
Teilweise	Mo, 30.11.2015	
M 2.218	Regelung der Mitnahme von	B- und C-Maßnahmen erst
Umsetzung:	Umsetzung bis:	Umsetzung durch:
Nein	Sa, 31.12.2016	IT-Sicherheitsbeauftragter
M 2.303	Festlegung einer Strategie für den	# Dokument verlinken aus de
Umsetzung:	Umsetzung bis:	Umsetzung durch:
Teilweise	Mo, 30.11.2015	
M 2.304	Sicherheitsrichtlinien und Regelungen für	# Prüfen, welche in M 2.304
Umsetzung:	Umsetzung bis:	Umsetzung durch:
Teilweise	Mo, 30.11.2015	
M 2.305	Geeignete Auswahl von Smartphones,	B- und C-Maßnahmen erst
Umsetzung:	Umsetzung bis:	Umsetzung durch:
Nein	Sa, 31.12.2016	IT-Sicherheitsbeauftragter
M 2.306	Verlustmeldung	
Umsetzung:	Umsetzung bis:	Umsetzung durch:
Ja	Do, 05.11.2015	
M 2.558	Sensibilisierung der Mitarbeiter zur	
Umsetzung:	Umsetzung bis:	Umsetzung durch:
	Mo, 18.04.2016	

Standard-Report

Individuelles Reporting - für Soll-Ist-Vergleich

Die durchgeführten Maßnahmen werden hier neben den „ToDos“ dokumentiert

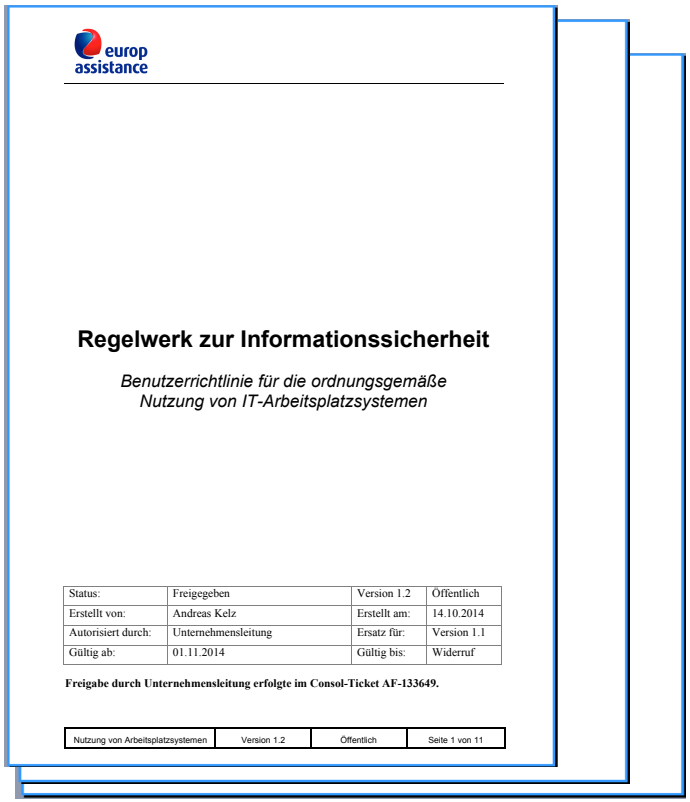
** Auftrag an Support-Team für individuelle Report-Templates; alternativ in verinice-PRO: Eigenentwicklung über vDesigner*

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Die Entscheidung für BSI IT-Grundschutz schafft spürbaren Nutzen
Erstes Handlungsfeld: Schrittweise zu den „Top 10“ aktueller Richtlinien und Regeln

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

- Leitlinie zur Informationssicherheit
- Richtlinie für den Umgang mit sicherheitsrelevanten Ereignissen (Incidents) in der IT
- Benutzerrichtlinie für die ordnungsgemäße Nutzung von IT-Arbeitsplatzsystemen
- IT-Sicherheitshandbuch
- Richtlinie zur Zusammenarbeit mit Geschäftspartnern
- Handbuch über Ordnung und Verhalten im Betrieb (Organisationshandbuch)
- Richtlinie zum Passwortgebrauch
- Benutzerrichtlinie für E-Mail
- Hausordnung Standort Adenauerring


europ assistance

Regelwerk zur Informationssicherheit

Benutzerrichtlinie für die ordnungsgemäße Nutzung von IT-Arbeitsplatzsystemen

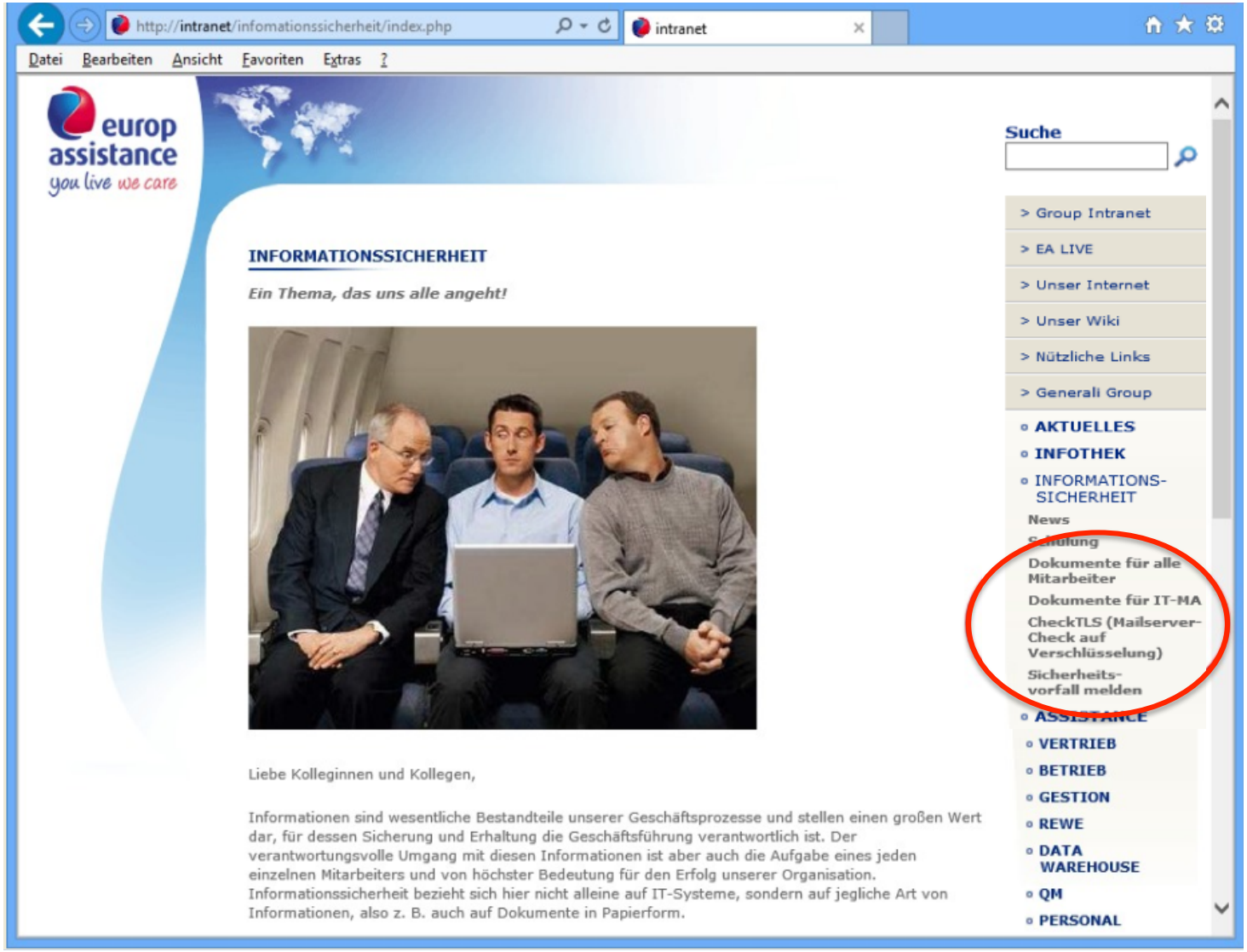
Status:	Freigegeben	Version 1.2	Öffentlich
Erstellt von:	Andreas Kelz	Erstellt am:	14.10.2014
Autorisiert durch:	Unternehmensleitung	Ersatz für:	Version 1.1
Gültig ab:	01.11.2014	Gültig bis:	Widerruf

Freigabe durch Unternehmensleitung erfolgte im Consol-Ticket AF-133649.

Nutzung von Arbeitsplatzsystemen	Version 1.2	Öffentlich	Seite 1 von 11

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

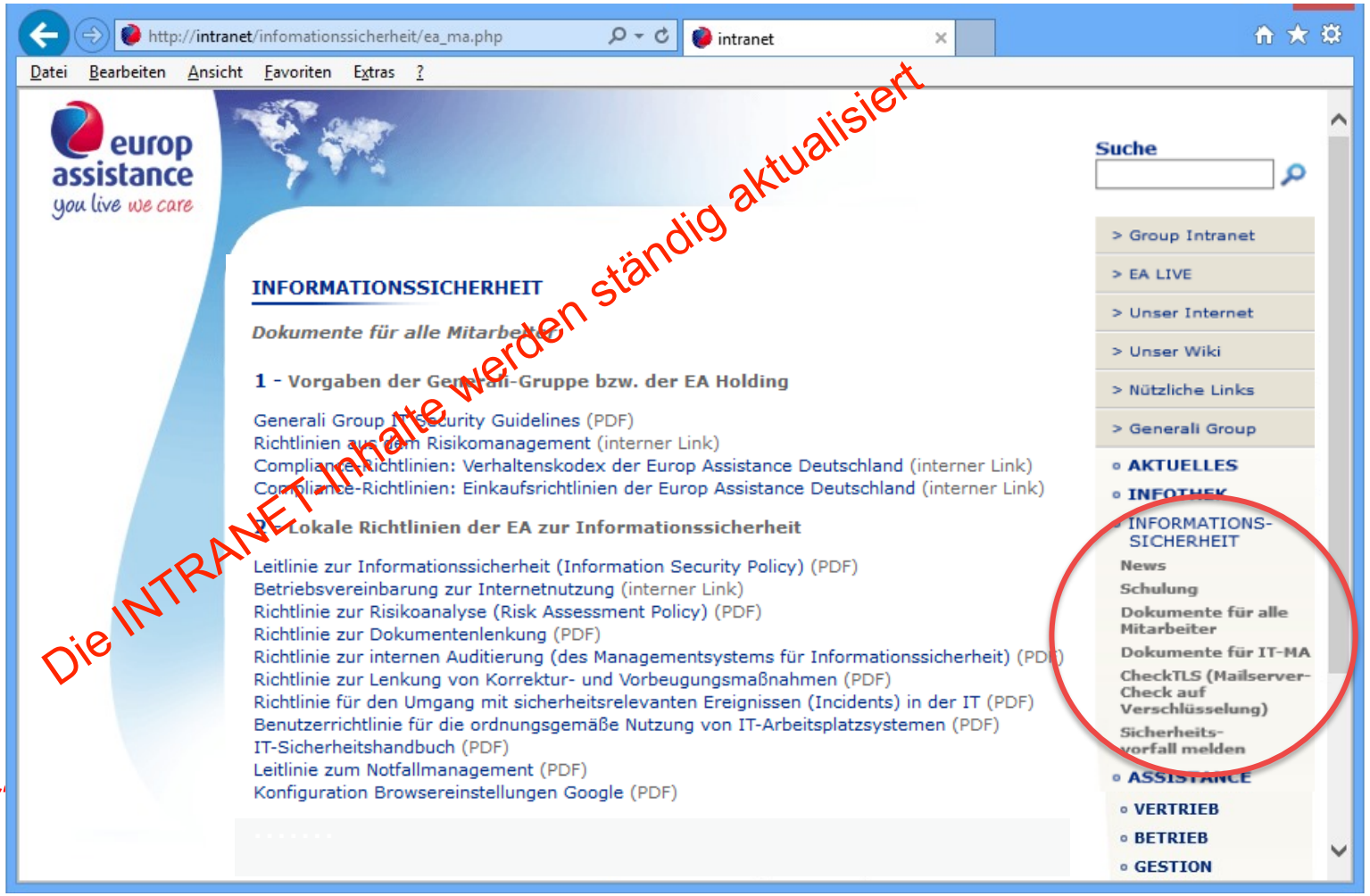
Alle wichtigen Informationen stehen im Intranet



http://intranet/informationssicherheit/index.php

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Alle wichtigen Informationen stehen im Intranet - „mit 3 Klicks zum Dokument“



siehe: „Dokumente für Mitarbeiter“ im Intranet

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Kritischer Erfolgsfaktor für die Risikoanalyse: Verantwortung der Führungskräfte

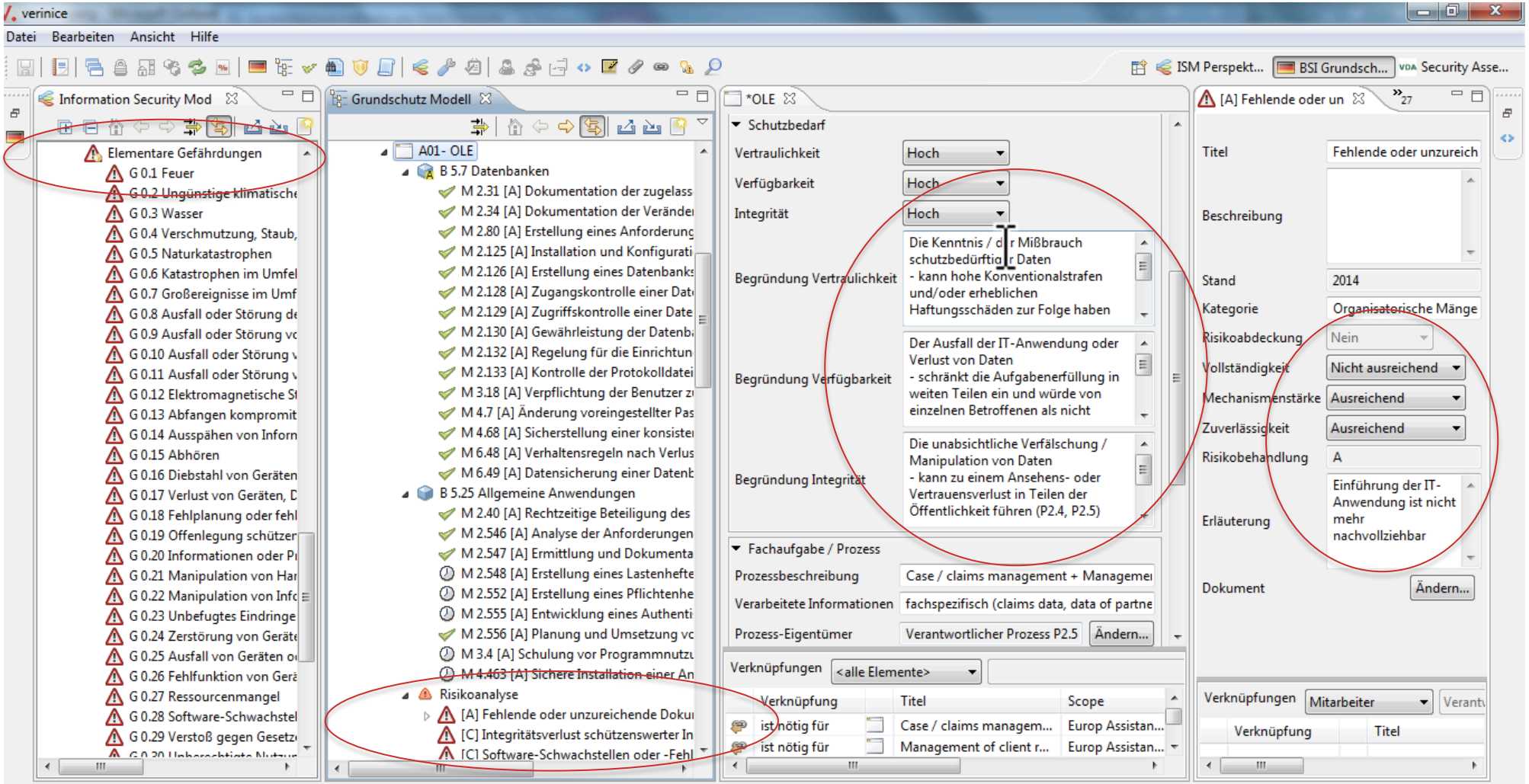
Ermitteln des Schutzbedarfs - Szenarien zum Prozess „Claims/Case Management“

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)

Interviews mit Prozessverantwortlichen

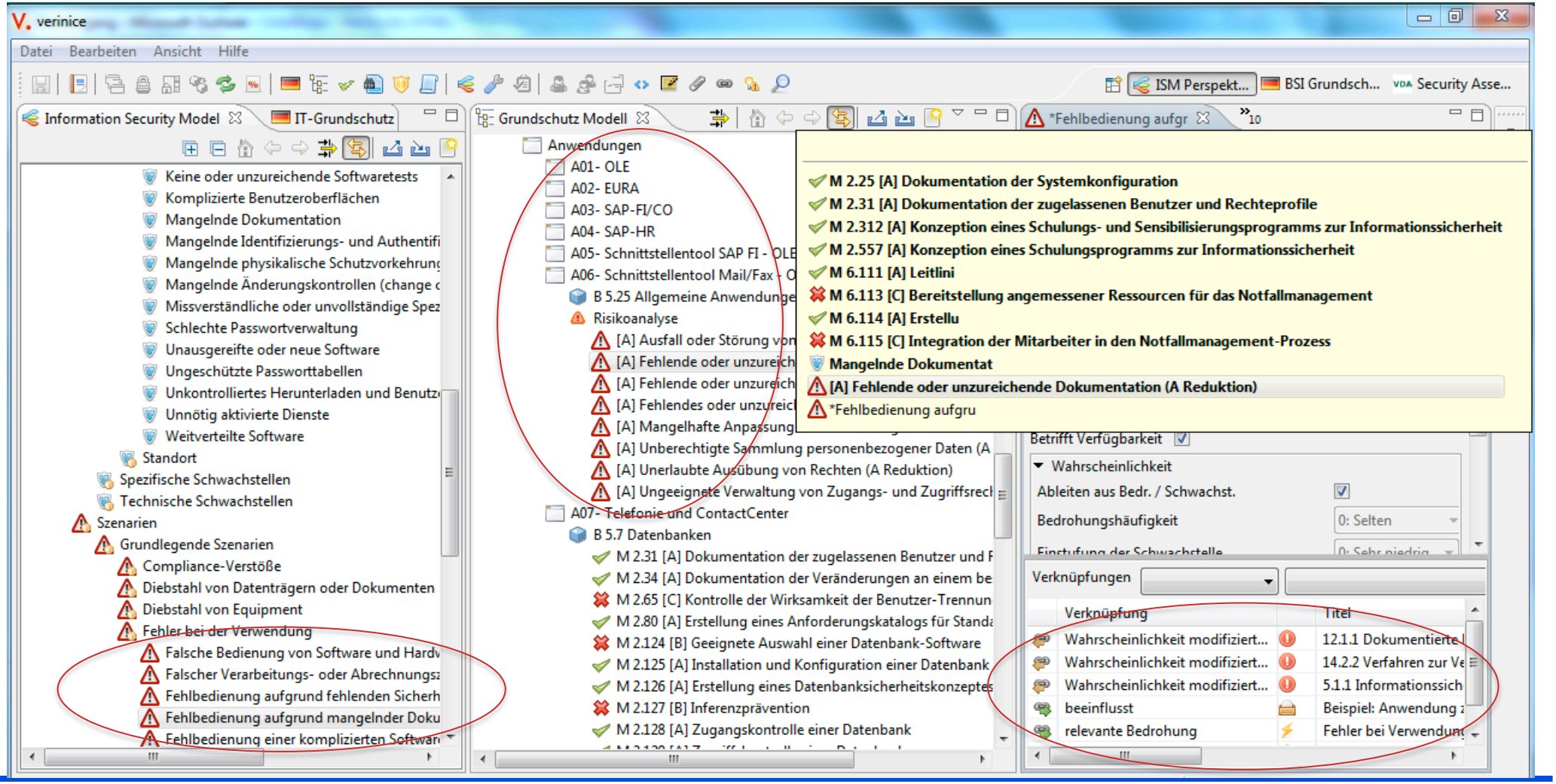
Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Kritischer Erfolgsfaktor für die Risikoanalyse: Verantwortung der Führungskräfte
Der Clou in verinice: Straffes Risikomanagement durch übersichtliche Dokumentation



Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Kritischer Erfolgsfaktor für die Risikoanalyse: Verantwortung der Führungskräfte
Der Clou in verinice: Risikokatalog aus ISO 27005 auch in BSI-Projekten verwendet



Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Kritischer Erfolgsfaktor für die Risikoanalyse: Management-taugliche Berichte

Zielobjekt	Name	Vertraulichkeit	Integrität	Verfügbarkeit
R04-	Serverraum	Hoch	Hoch	Hoch

1. Gefährdungsübersicht

Kap.	Titel	Bewertung: OK?
G 1.4	Feuer	Ja
G 1.5	Wasser	Ja
G 1.7	Unzulässige Temperatur und Luftfeuchte	Ja
G 1.16	Ausfall von Patchfeldern durch Brand	Ja
G 2.1	Fehlende oder unzureichende Regelungen	Ja
G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen	Nein
G 2.27	Fehlende oder unzureichende Dokumentation	Nein
G 4.1	Ausfall der Stromversorgung	Ja
G 4.2	Ausfall interner Versorgungsnetze	Ja
G 4.6	Spannungsschwankungen/Überspannung/Unterspannung	Ja
G 5.1	Manipulation oder Zerstörung von Geräten oder Zubehör	Ja
G 5.2	Manipulation an Informationen oder Software	Ja
G 5.3	Unbefugtes Eindringen in ein Gebäude	Ja
G 5.4	Diebstahl	Ja
G 1.8	Staub, Verschmutzung	Ja
G 2.4	Unzureichende Kontrolle der Sicherheitsmaßnahmen	Nein
G 3.21	Fehlbedienung von Codeschlössern	Ja
G 4.3	Ausfall vorhandener Sicherungseinrichtungen	Ja
G 4.4	Leitungsbeeinträchtigung durch Umfeldfaktoren	Ja
G 5.16	Gefährdung bei Wartungs-/Administrierungsarbeiten	Ja
G 5.53	Bewusste Fehlbedienung von Schutzschränken aus Bequemlichkeit	Ja

Standard-Reporting mit verinice noch nicht wirklich management-tauglich

2. Gefährdungsbewertung

Kap.	Titel	Bewertung: OK?	Vollständigkeit	Zuverlässigkeit	Mechanismenstärke
G 2.4	Unzureichende Kontrolle der Sicherheitsmaßnahmen	Nein	Ausreichend	Nicht ausreichend	Nicht ausreichend
G 2.6	Unbefugter Zutritt zu schutzbedürftigen Räumen	Nein	Nicht ausreichend	Ausreichend	Ausreichend
G 2.27	Fehlende oder unzureichende Dokumentation	Nein	Nicht ausreichend	Ausreichend	Ausreichend

3. Risikobehandlung

Kap.	Titel	Risikobehandlung	Erläuterung
G 2.27	Fehlende oder unzureichende Dokumentation	C	Es existieren Richtlinien, aber die Wirksamkeit ist zu prüfen.

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Kritischer Erfolgsfaktor für die Risikoanalyse: Management-taugliche Berichte

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

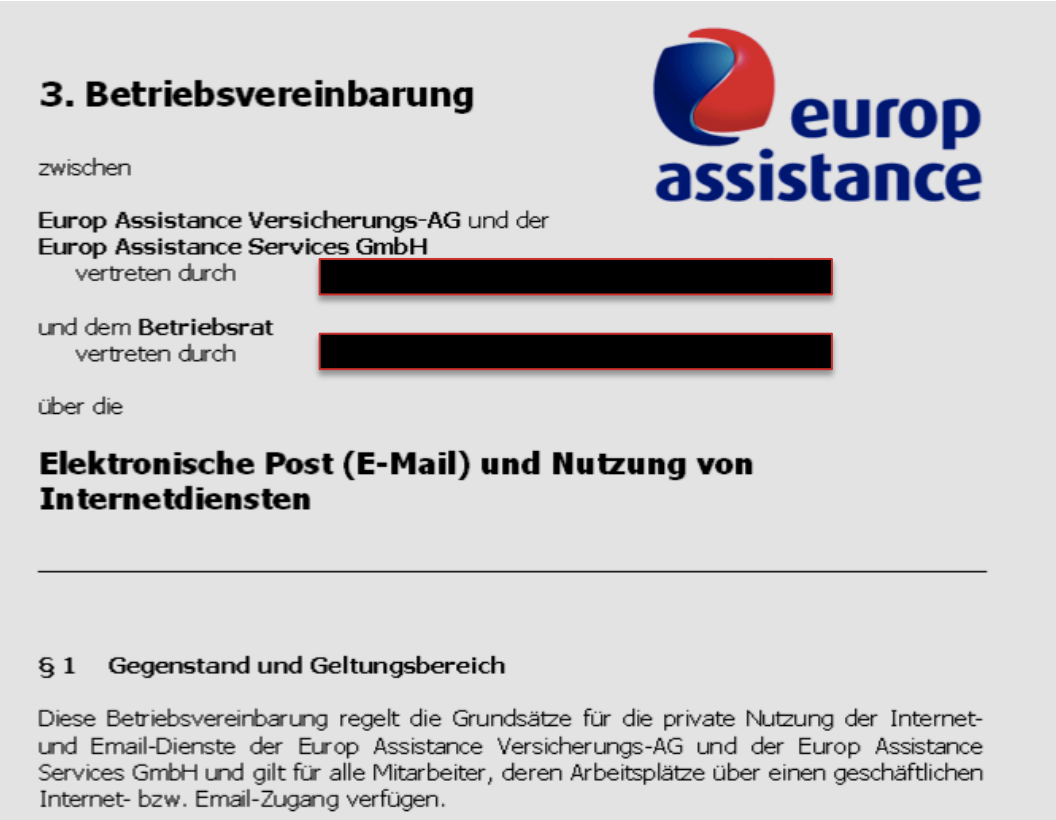
- Es liegt in der Verantwortung der EA-Führungskräfte, welche Maßnahmen in welcher Reihenfolge ergriffen werden und wo Restrisiken verbleiben.
- Bei der Umsetzung der Maßnahmen orientiert sich EA an dem Stellenwert, den die jeweilige Maßnahme im Sicherheitskonzept hat. Sogenannte A-Maßnahmen (A=Einstieg 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.

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Ausblick: „Dreiklang“ zwischen Informationssicherheit, Datenschutz, Compliance - Richtlinien, Prozesse und Betriebsvereinbarungen sind aufeinander abgestimmt

Compliance-Richtlinie:
Verhaltenskodex der EA Deutschland

- „**Vertraulichkeit**: Alle Beschäftigten müssen die Vertraulichkeit der ihnen seitens der Europ Assistance Deutschland, der Europ Assistance Gruppe oder der Geschäftspartner zugänglich gemachten Betriebs- und Geschäftsgeheimnisse wahren ...
... Angelegenheiten und Informationen sind vertraulich zu behandeln, die als solche gekennzeichnet sind .....“
- „**Datenschutz**: Alle Beschäftigten sind verpflichtet, ... aktiv dazu beizutragen, dass personenbezogene Daten zuverlässig gegen unberechtigte Zugriffe gesichert werden ...“



3. Betriebsvereinbarung

europ assistance

zwischen

Europ Assistance Versicherungs-AG und der
Europ Assistance Services GmbH
vertreten durch [redacted]

und dem **Betriebsrat**
vertreten durch [redacted]

über die

Elektronische Post (E-Mail) und Nutzung von Internetdiensten

---

§ 1 Gegenstand und Geltungsbereich

Diese Betriebsvereinbarung regelt die Grundsätze für die private Nutzung der Internet- und Email-Dienste der Europ Assistance Versicherungs-AG und der Europ Assistance Services GmbH und gilt für alle Mitarbeiter, deren Arbeitsplätze über einen geschäftlichen Internet- bzw. Email-Zugang verfügen.

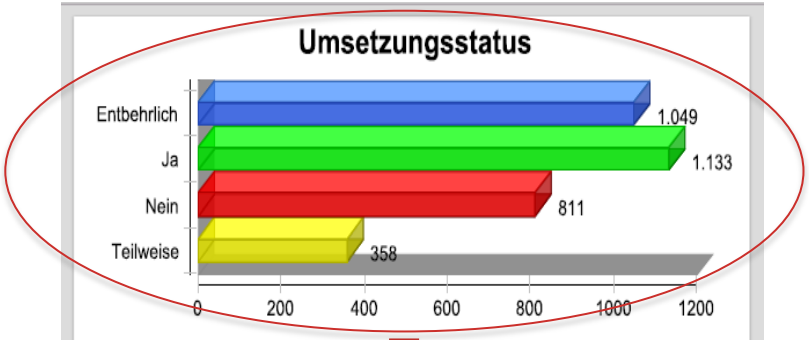
Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

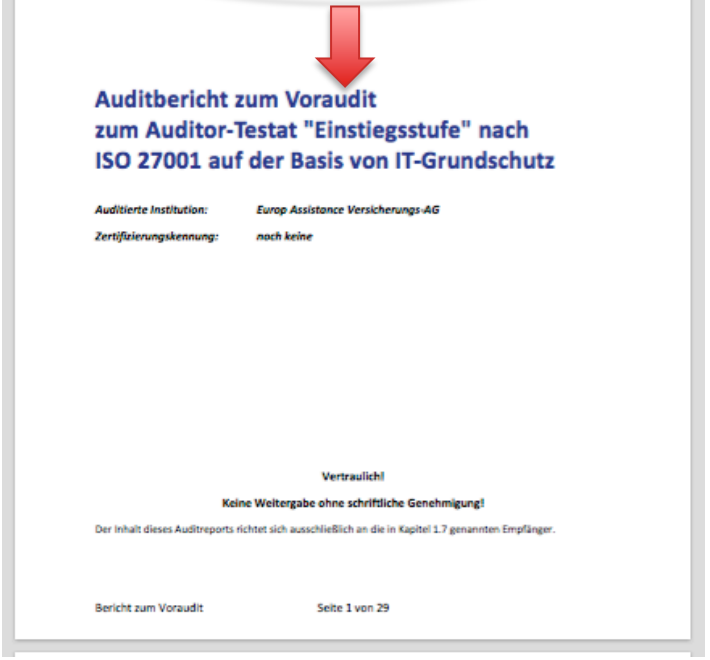
Ausblick: Regelmäßige interne Audits (extern unterstützt) sind etabliert
BSI Vor-Audit durchgeführt - 3 Jahre erfolgreiche Einführung des ISMS bestätigt

Beispiel: Jährliche Schwachstellenanalyse durch Führungskräfte der Europ-Assistance

	ja	nein
1.1.1 Wurden die von Ihnen veranlassten Maßnahmen durchgeführt?		
1.1.2 Haben diese Maßnahmen die beabsichtigte Wirkung erzielt?		
1.1.3 Haben Sie die von Ihnen allein nicht behebbaren Schwachstellen Ihrer Führungskraft sowie dem lokal zuständigen Ansprechpartner für Informationssicherheit gemeldet?		
1.1.4 Liegen für diese gemeldeten, nicht selbst behebbaren Schwachstellen Entscheidungen über die weitere Vorgehensweise vor?		
1.1.5 Sind alle Maßnahmen dokumentiert?		

betrifft Führungskräfte, die bereits eine Schwachstellenanalyse durchgeführt haben




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

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

Ausblick: Alle ziehen an einem Strang - vom Administrator bis zur Geschäftsleitung

Alles geht nur gemeinsam mit allen Führungskräften und Mitarbeitern

Alle Führungskräfte der Europ Assistance haben in Ihrem Verantwortungs-bereich auf die Informationssicherheit entscheidenden Einfluss:

- Erkennen und Beurteilen von Sicherheits-Risiken
- Einführung und Durchsetzung von Maßnahmen zur Informationssicherheit
- Beschaffung und Einsatz von sicheren IT-Systemen
- Sicherheit der Arbeitsräume und Arbeitsmittel
- Einwirkung im Tagesalltag auf das Bewusstsein und Verhalten ihrer Mitarbeiter
- Regelmäßige Information Ihrer Mitarbeiter

Unsere Führungskräfte wissen, dass sie eine Vorbildfunktion haben, sie leben Datenschutz und Informationssicherheit vor.

Beispiel Europ Assistance - verinice als entscheidender Erfolgsfaktor

?? Fragen

Transformation Consulting International

Holger Schellhaas

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