PRAXISBERICHT

VERINICE.PRO

Technische Migration von BSI 100 auf BSI 200

verinice.XP - Die Konferenz!
am 26. Februar 2020 in Berlin

Informationssicherheit

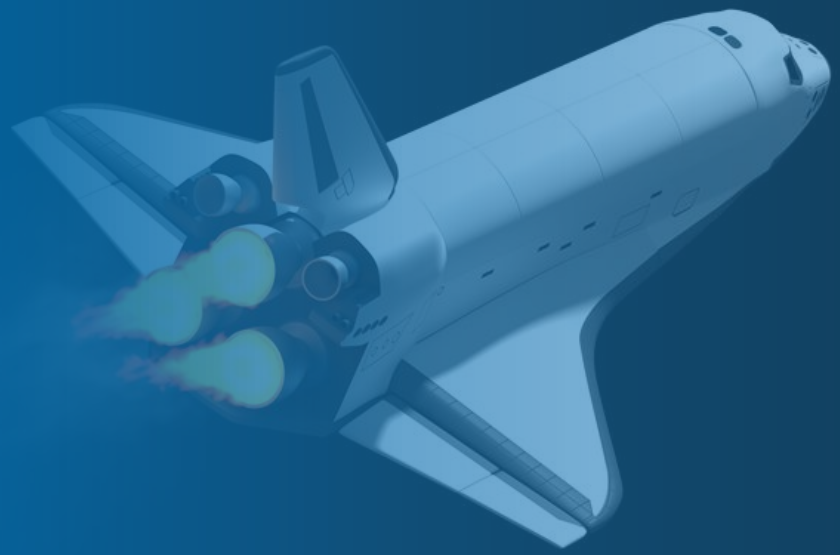
Angemessen
Nutzerfreundlich
Kreativ

SEC2DO

In Zusammenarbeit mit

SONOXO

Lernen Sie ...



1. Wie die Migration technisch umsetzbar ist
2. Welche Funktionen verinice für die Migration bereitstellt
3. Welche Hilfsmittel des BSI relevant sind
4. Welche Nacharbeiten von Hand erfolgen müssen

Martin Peters

Über 11 Jahre Erfahrung bei der Einführung von Informationssicherheits-Managementsystemen (ISMS)

martin.peters@sec2do.com

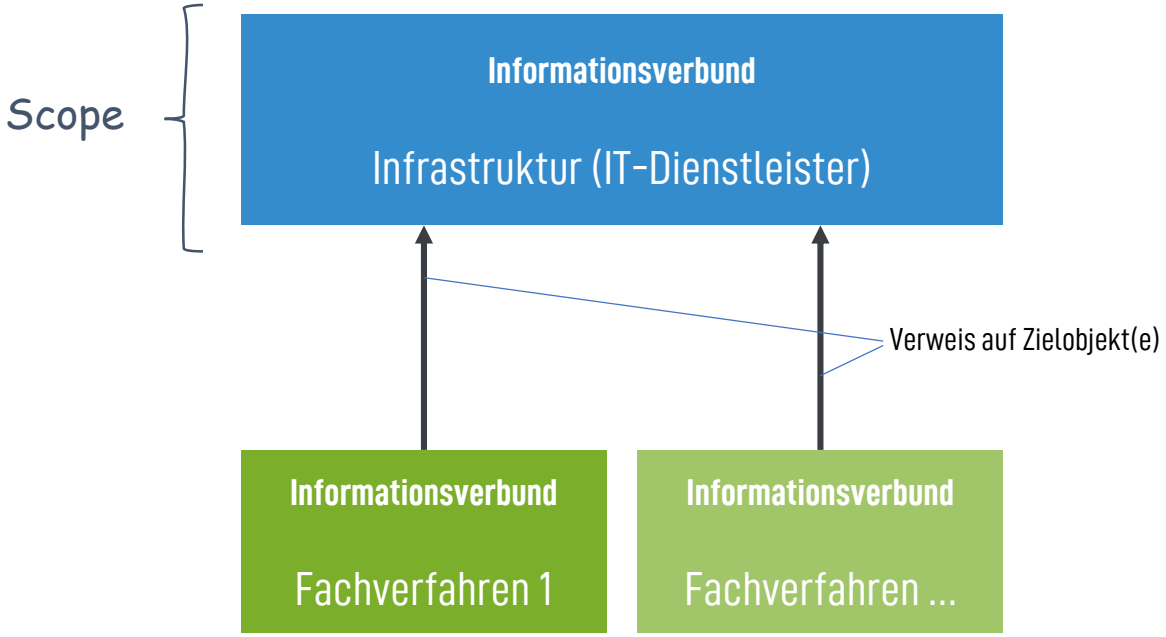
QUALIFIKATIONEN

- Dipl. Wirtschaftsinformatiker (FH)
- Geprüfter ISO 27001 Auditor (SGS TÜV)
- Prüfverfahrenskompetenz §8a (3) BSIG - IT-Sicherheitsaudits bei KRITIS-Betreiber (BSI)
- Geprüfter IT-Sicherheitsbeauftragter (SGS TÜV)
- Geprüfter Datenschutzbeauftragter (SGS TÜV)
- COBIT Practitioner (ISACA)
- Foundation in IT Service Management (TÜV SÜD)
- ITEMO FitSM Foundation 2013 (ICO)
- PRINCE2 Foundation (APM Group)

SCHWERPUNKTE DER BERATUNG

- Design und Einführung von Informationssicherheits-Managementsystemen (ISMS) nach ISO 27001 oder BSI IT-Grundschutz
- Informations-Risikomanagement z.B. nach ISO 27005, BSI 200-3 oder MaRisk/BAIT
- Informationssicherheit in der agilen Software-Entwicklung (DevOps) gemäß MaRisk, BAIT, PCI DSS
- Security Awareness
- Projektmanagement

Ausgangslage im Projekt

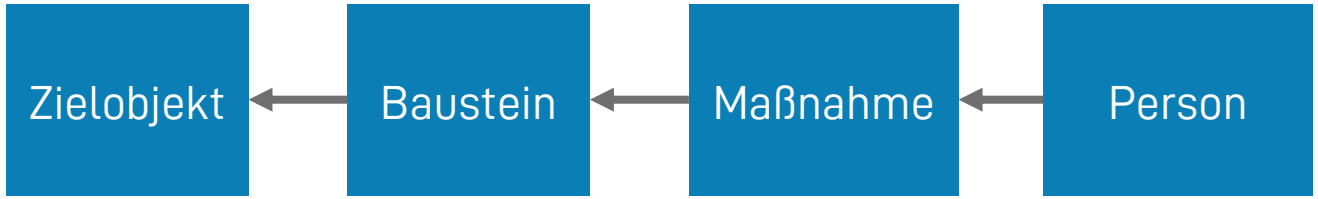


- Verinice und verinice.PRO
  (Version 1.18.1)
- Über 7.500 Maßnahmen

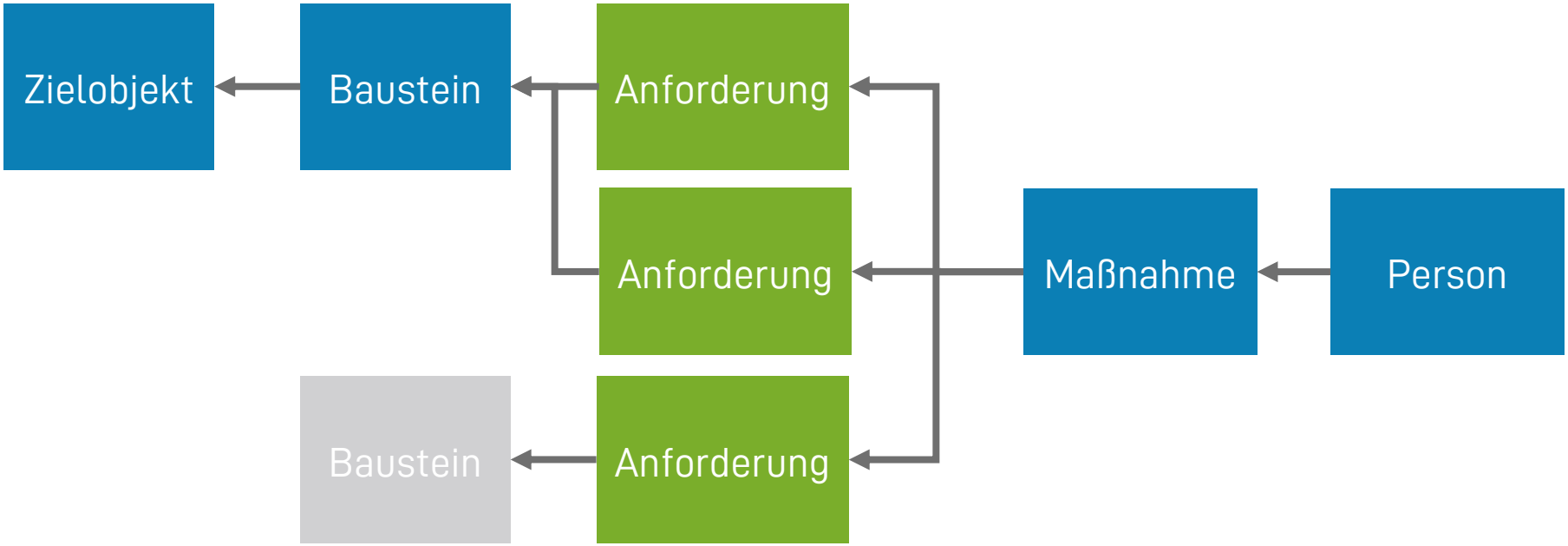
- Fachverfahren werden durch Kunden in separaten Informationsverbünden selbst verwaltet

Sec2do GmbH • Uhlandstraße 28 • 10719 Berlin

Bisheriges Datenmodell in verinice.

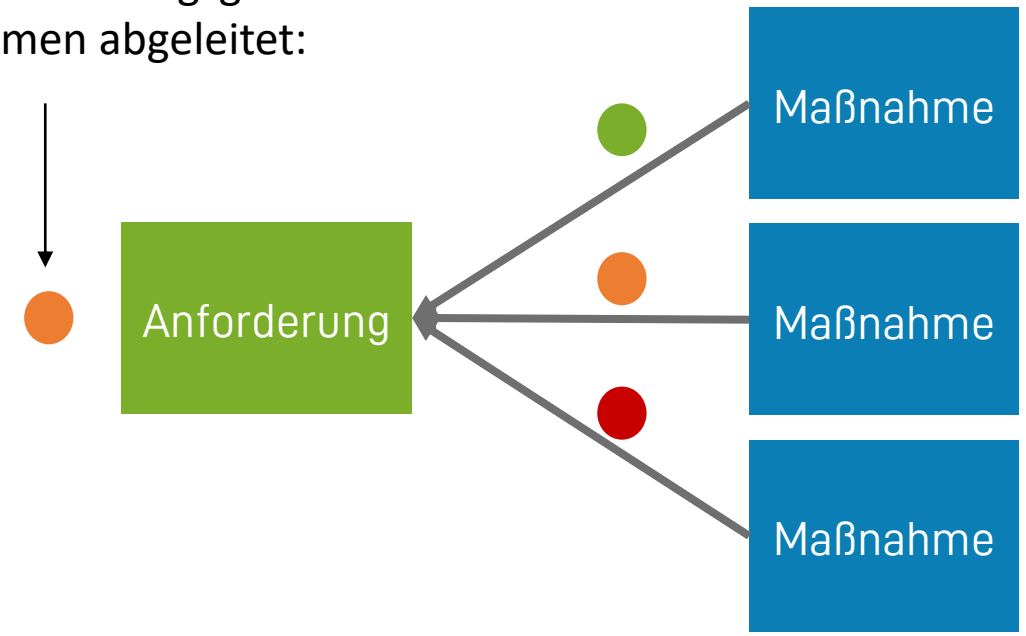


Neues Datenmodell in der Perspektive modernisierter Grundschutz



Status der Umsetzung von Anforderungen

Der Status der Anforderungen
wird aus den Status der Umsetzungsgüte
der verknüpften Maßnahmen abgeleitet:



Fehlende Attribute zu den Maßnahmen

In der genutzten Version (1.18.1) fehlen die Felder:

- Letzte Revision am,
- Revision - Bemerkungen
- Nächste Revision am
- Umsetzung bis

ANPASSUNG ERFOLGT ÜBER

SNCA.XML

Auskunft von SerNet:

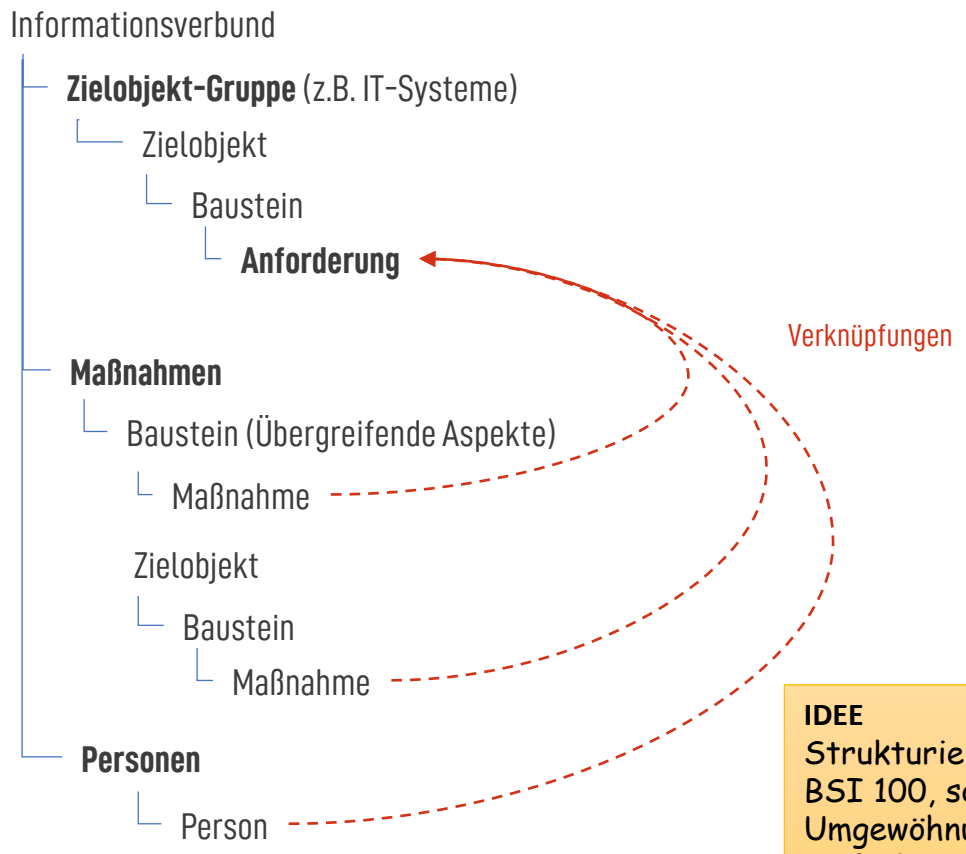
„Die fehlenden Felder werden ab Version 1.20 und in allen zukünftigen Versionen enthalten sein“

Zielbild

Alte Struktur

Informationsverbund
- Baustein (Übergreifende Aspekte)
  - Maßnahme
- Zielobjekt
  - Baustein
    - Maßnahme

Neue Struktur



IDEE
Strukturierung nach BSI 100, so dass Umgewöhnung einfacher ist

Migrationstabellen des BSI (Beispiel)

Für jeden veröffentlichten BSI 200-Baustein
ist eine Migrationstabelle verfügbar

Link: *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Migrationstabellen_FD.html*

Herausforderung:

- → Migriert wird stets aus Sicht der neuen Bausteine
- → Welche alten Maßnahmen sind zu migrieren, wenn kein neuer Baustein diese als Quelle referenziert?
- → Was ist, wenn Maßnahmen aus Bausteinen referenziert werden, die in der Modellierung anderen Zielobjekten zugeordnet wurden?

Beispieldarstellung

Anforderungen

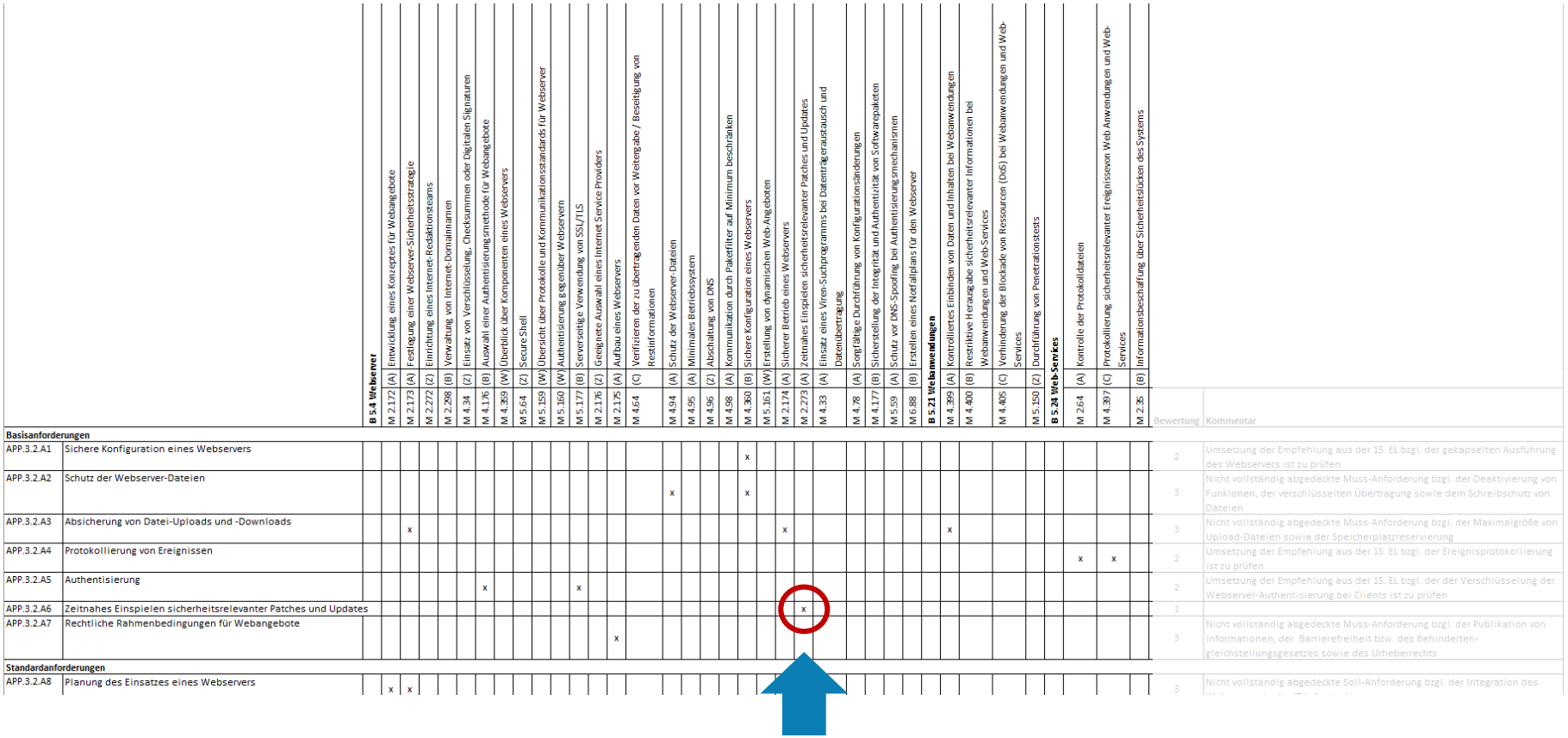
		B 5.4 Webserver	M 2.172 (A) Entwicklung eines Konzeptes für Webangebote	M 2.173 (A) Festlegung einer Webserver-Sicherheitsstrategie	M 2.272 (2) Einrichtung eines Internet-Redaktionsteams	M 2.298 (B) Verwaltung von Internet-Domainnamen	M 4.34 (2) Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen	M 4.176 (B) Auswahl einer Authentisierungsmethode für Webangebote	M 4.393 (W) Überblick über Komponenten eines Webservers	M 5.64 (2) Secure Shell	M 5.159 (W) Übersicht über Protokolle und Kommunikationsstandards für Webserver	M 5.160 (W) Authentisierung gegenüber Webservern	M 5.177 (B) Serverseitige Verwendung von SSL/TLS	M 2.176 (2) Geeignete Auswahl eines Internet Service Providers	M 2.175 (A) Aufbau eines Webservers	M 4.64 (C) Verifizieren der zu übertragenden Daten vor Weitergabe / Bestätigung von Restinformationen	M 4.94 (A) Schutz der Webserver-Dateien	M 4.95 (A) Minimales Betriebssystem	M 4.96 (2) Abschaltung von DNS	M 4.98 (A) Kommunikation durch Paketfilter auf Minimum beschränken	M 4.300 (B) Sichere Konfiguration eines Webservers	M 5.161 (W) Erstellung von dynamischen Web-Angeboten	M 2.174 (A) Sicherer Betrieb eines Webservers	M 2.273 (A) Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates	M 4.33 (A) Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung	M 4.78 (A) Sorgfältige Durchführung von Konfigurationsänderungen	M 4.177 (B) Sicherstellung der Integrität und Authentizität von Softwarepaketen	M 5.59 (A) Schutz vor DNS-Spoofing bei Authentisierungsmechanismen	M 6.88 (B) Erstellen eines Notfallplans für den Webserver	**B 5.21 Webanwendungen**	M 4.399 (A) Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen	M 4.400 (B) Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services	M 4.405 (C) Verhinderung der Blockade von Ressourcen (DoS) bei Webanwendungen und Web-Services	M 5.150 (2) Durchführung von Penetrationstests	**B 5.23 Web-Services**	M 2.64 (A) Kontrolle der Protokolldateien	M 4.397 (C) Protokollierung sicherheitsrelevanter Ereignisse von Web Anwendungen und Web-Services	M 2.35 (B) Informationsbeschaffung über Sicherheitslücken des Systems	Bewertung	Kommentar
Basisanforderungen																																												
APP.3.2.A1	Sichere Konfiguration eines Webservers																					x																						2	Umsetzung der Empfehlung aus der 15. EL bzgl. der gekapselten Ausführung des Webservers ist zu prüfen
APP.3.2.A2	Schutz der Webserver-Dateien																	x				x																						3	Nicht vollständig abgedeckte Muss-Anforderung bzgl. der Deaktivierung von Funktionen, der verschlüsselten Übertragung sowie dem Schreibschutz von Dateien
APP.3.2.A3	Absicherung von Datei-Uploads und -Downloads			x																					x																		3	Nicht vollständig abgedeckte Muss-Anforderung bzgl. der Maximalgröße von Upload-Dateien sowie der Speicherplatzreservierung
APP.3.2.A4	Protokollierung von Ereignissen																														x												2	Umsetzung der Empfehlung aus der 15. EL bzgl. der Ereignisprotokollierung ist zu prüfen
APP.3.2.A5	Authentisierung							x					x																														2	Umsetzung der Empfehlung aus der 15. EL bzgl. der der Verschlüsselung der Webserver-Authentisierung bei Clients ist zu prüfen
APP.3.2.A6	Zeitnahes Einspielen sicherheitsrelevanter Patches und Update																								x																		1	
APP.3.2.A7	Rechtliche Rahmenbedingungen für Webangebote															x																											3	Nicht vollständig abgedeckte Muss-Anforderung bzgl. der Publikation von Informationen, der Barrierefreiheit bzw. des Behinderten-gleichstellungsgesetzes sowie des Urheberrechts
Standardanforderungen																																												
APP.3.2.A8	Planung des Einsatzes eines Webservers		x	x																																							3	Nicht vollständig abgedeckte Soll-Anforderung bzgl. der Integration des

Beispieldarstellung

Maßnahmen

		B 5.4 Webserver	M 2.172 (A) Entwicklung eines Konzeptes für Webangebote	M 2.173 (A) Festlegung einer Webserver-Sicherheitsstrategie	M 2.272 (Z) Einrichtung eines Internet-Redaktionsteams	M 2.298 (B) Verwaltung von Internet-Domainnamen	M 4.34 (Z) Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen	M 4.176 (B) Auswahl einer Authentisierungsmethode für Webangebote	M 4.359 (W) Überblick über Komponenten eines Webservers	M 5.64 (Z) Secure Shell	M 5.159 (W) Übersicht über Protokolle und Kommunikationsstandards für Webserver	M 5.160 (W) Authentisierung gegenüber Webservern	M 5.177 (B) Serverseitige Verwendung von SSL/TLS	M 2.176 (Z) Geeignete Auswahl eines Internet Service Providers	M 2.175 (A) Aufbau eines Webservers	M 4.64 (C) Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen	M 4.94 (A) Schutz der Webserver-Dateien	M 4.95 (A) Minimales Betriebssystem	M 4.96 (Z) Abschaltung von DNS	M 4.98 (A) Kommunikation durch Paketfilter auf Minimum beschränken	M 4.360 (B) Sichere Konfiguration eines Webservers	M 5.161 (W) Erstellung von dynamischen Web-Angeboten	M 2.174 (A) Sicherer Betrieb eines Webservers	M 2.273 (A) Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates	M 4.33 (A) Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung	M 4.78 (A) Sorgfältige Durchführung von Konfigurationsänderungen	M 4.177 (B) Sicherstellung der Integrität und Authentizität von Softwarepaketen	M 5.59 (A) Schutz vor DNS-Spoofing bei Authentisierungsmechanismen	M 6.88 (B) Erstellen eines Notfallplans für den Webserver	B 5.21 Webanwendungen	M 4.399 (A) Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen	M 4.400 (B) Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services	M 4.405 (C) Verhinderung der Blockade von Ressourcen (DoS) bei Webanwendungen und Web-Services	M 5.150 (Z) Durchführung von Penetrationstests	B 5.24 Web-Services	M 2.64 (A) Kontrolle der Protokolldateien	M 4.397 (C) Protokollierung sicherheitsrelevanter Ereignisse von Web Anwendungen und Web-Services	M 2.35 (B) Informationsbeschaffung über Sicherheitslücken des Systems	Bewertung	Kommentar
Basisanforderungen																																								
APP.3.2.A1	Sichere Konfiguration eines Webservers																				x																		2	Umsetzung der Empfehlung aus der 15. EL bzgl. der gekapselten Ausführung des Webservers ist zu prüfen
APP.3.2.A2	Schutz der Webserver-Dateien																x				x																		3	Nicht vollständig abgedeckte Muss-Anforderung bzgl. der Deaktivierung von Funkionen, der verschlüsselten Übertragung sowie dem Schreibschutz von Dateien
APP.3.2.A3	Absicherung von Datei-Uploads und -Downloads			x																			x							x									3	Nicht vollständig abgedeckte Muss-Anforderung bzgl. der Maximalgröße von Upload-Dateien sowie der Speicherplatzreservierung
APP.3.2.A4	Protokollierung von Ereignissen																																			x	x		2	Umsetzung der Empfehlung aus der 15. EL bzgl. der Ereignisprotokollierung ist zu prüfen
APP.3.2.A5	Authentisierung							x					x																										2	Umsetzung der Empfehlung aus der 15. EL bzgl. der der Verschlüsselung der Webserver-Authentisierung bei Clients ist zu prüfen
APP.3.2.A6	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates																							x															1	
APP.3.2.A7	Rechtliche Rahmenbedingungen für Webangebote													x																									3	Nicht vollständig abgedeckte Muss-Anforderung bzgl. der Publikation von Informationen, der Barrierefreiheit bzw. des Behinderten-gleichstellungsgesetzes sowie des Urheberrechts
Standardanforderungen																																								
APP.3.2.A8	Planung des Einsatzes eines Webservers		x	x																																			3	Nicht vollständig abgedeckte Soll-Anforderung bzgl. der Integration des

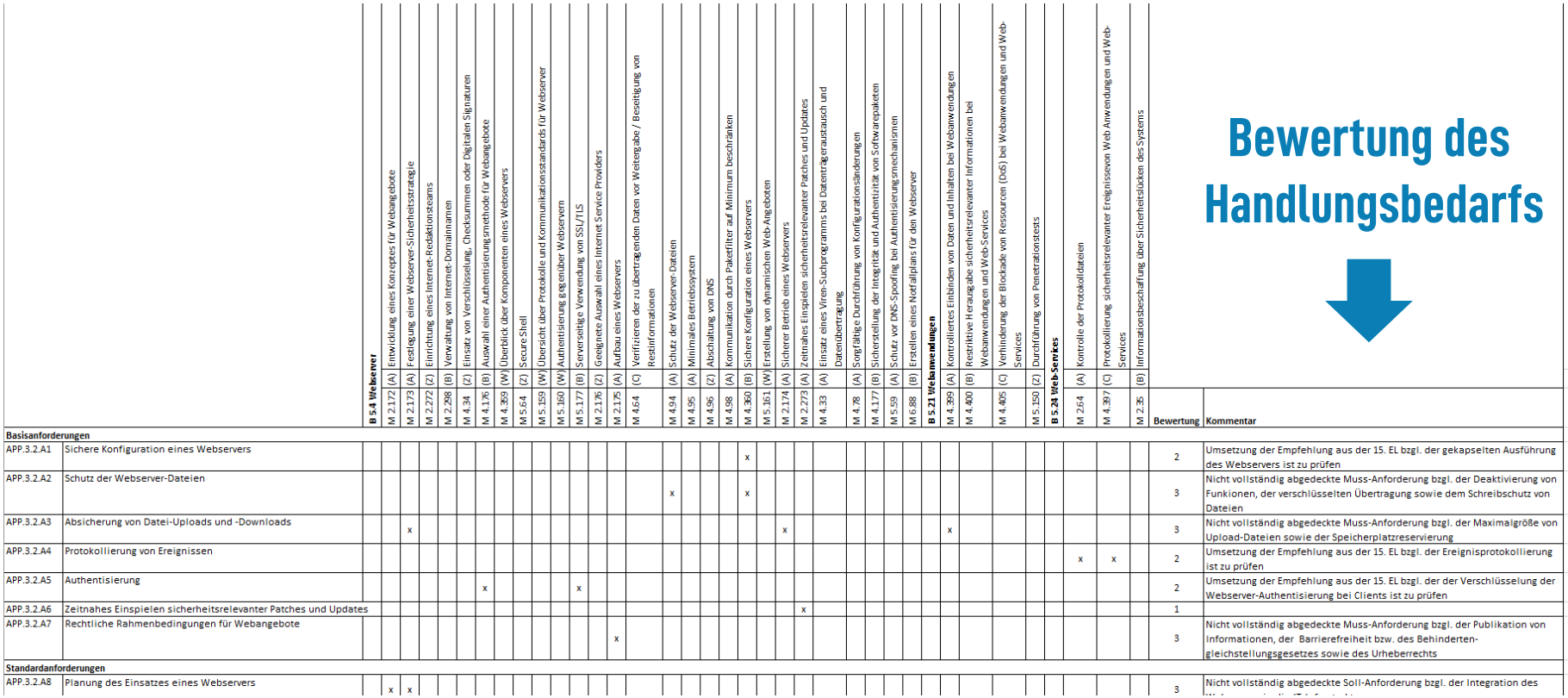
Beispieldarstellung



		B 5.4 Webserver		M 2.172 (A) Entwicklung eines Konzeptes für Webangebote	M 2.173 (A) Festlegung einer Webserver-Sicherheitsstrategie	M 2.272 (Z) Einrichtung eines Internet-Redaktionsteams	M 2.298 (B) Verwaltung von Internet-Domainnamen	M 4.34 (Z) Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen	M 4.176 (B) Auswahl einer Authentisierungsmethode für Webangebote	M 4.369 (W) Überblick über Komponenten eines Webservers	M 5.64 (Z) Secure Shell	M 5.159 (W) Übersicht über Protokolle und Kommunikationsstandards für Webserver	M 5.160 (W) Authentisierung gegenüber Webservern	M 5.177 (B) Serverseitige Verwendung von SSL/TLS	M 2.176 (Z) Geeignete Auswahl eines Internet Service Providers	M 2.175 (A) Aufbau eines Webservers	M 4.64 (C) Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen	B 5.21 Webanwendungen	M 4.94 (A) Schutz der Webserver-Dateien	M 4.95 (A) Minimales Betriebssystem	M 4.96 (Z) Abschaltung von DNS	M 4.98 (A) Kommunikation durch Paketfilter auf Minimum beschränken	M 4.360 (B) Sichere Konfiguration eines Webservers	M 5.161 (W) Erstellung von dynamischen Web-Angeboten	M 2.174 (A) Sicherer Betrieb eines Webservers	M 2.273 (A) Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates	M 4.33 (A) Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung	M 4.78 (A) Sorgfältige Durchführung von Konfigurationsänderungen	M 4.177 (B) Sicherstellung der Integrität und Authentizität von Softwarepaketen	M 5.59 (A) Schutz vor DNS-Spoofing bei Authentisierungsmechanismen	M 6.88 (B) Erstellen eines Notfallplans für den Webserver	B 5.21 Webanwendungen	M 4.369 (A) Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen	M 4.400 (B) Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services	M 4.405 (C) Verhinderung der Blockade von Ressourcen (DoS) bei Webanwendungen und Web-Services	M 5.150 (Z) Durchführung von Penetrationstests	B 5.24 Web-Services	M 2.64 (A) Kontrolle der Protokolldateien	M 4.367 (C) Protokollierung sicherheitsrelevanter Ereignissevon Web Anwendungen und Web-Services	M 2.35 (B) Informationsbeschaffung über Sicherheitslücken des Systems	Bewertung	Kommentar
Basisanforderungen																																														
APP.3.2.A1	Sichere Konfiguration eines Webservers																							x																						2	Umsetzung der Empfehlung aus der 15. EL bzgl. der gekapselten Ausführung des Webservers ist zu prüfen
APP.3.2.A2	Schutz der Webserver-Dateien																		x					x																						3	Nicht vollständig abgedeckte Muss-Anforderung bzgl. der Deaktivierung von Funktionen, der verschlüsselten Übertragung sowie dem Schreibschutz von Dateien
APP.3.2.A3	Absicherung von Datei-Uploads und -Downloads				x																						x																	3	Nicht vollständig abgedeckte Muss-Anforderung bzgl. der Maximalgröße von Upload-Dateien sowie der Speicherplatzreservierung
APP.3.2.A4	Protokollierung von Ereignissen																																x											2	Umsetzung der Empfehlung aus der 15. EL bzgl. der Ereignisprotokollierung ist zu prüfen
APP.3.2.A5	Authentisierung								x					x																														2	Umsetzung der Empfehlung aus der 15. EL bzgl. der der Verschlüsselung der Webserver-Authentisierung bei Clients ist zu prüfen
APP.3.2.A6	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates																										x																	1	
APP.3.2.A7	Rechtliche Rahmenbedingungen für Webangebote																x																												3	Nicht vollständig abgedeckte Muss-Anforderung bzgl. der Publikation von Informationen, der Barrierefreiheit bzw. des Behinderten-gleichstellungsgesetzes sowie des Urheberrechts
Standardanforderungen																																													
APP.3.2.A8	Planung des Einsatzes eines Webservers			x	x																																						3	Nicht vollständig abgedeckte Soll-Anforderung bzgl. der Integration des

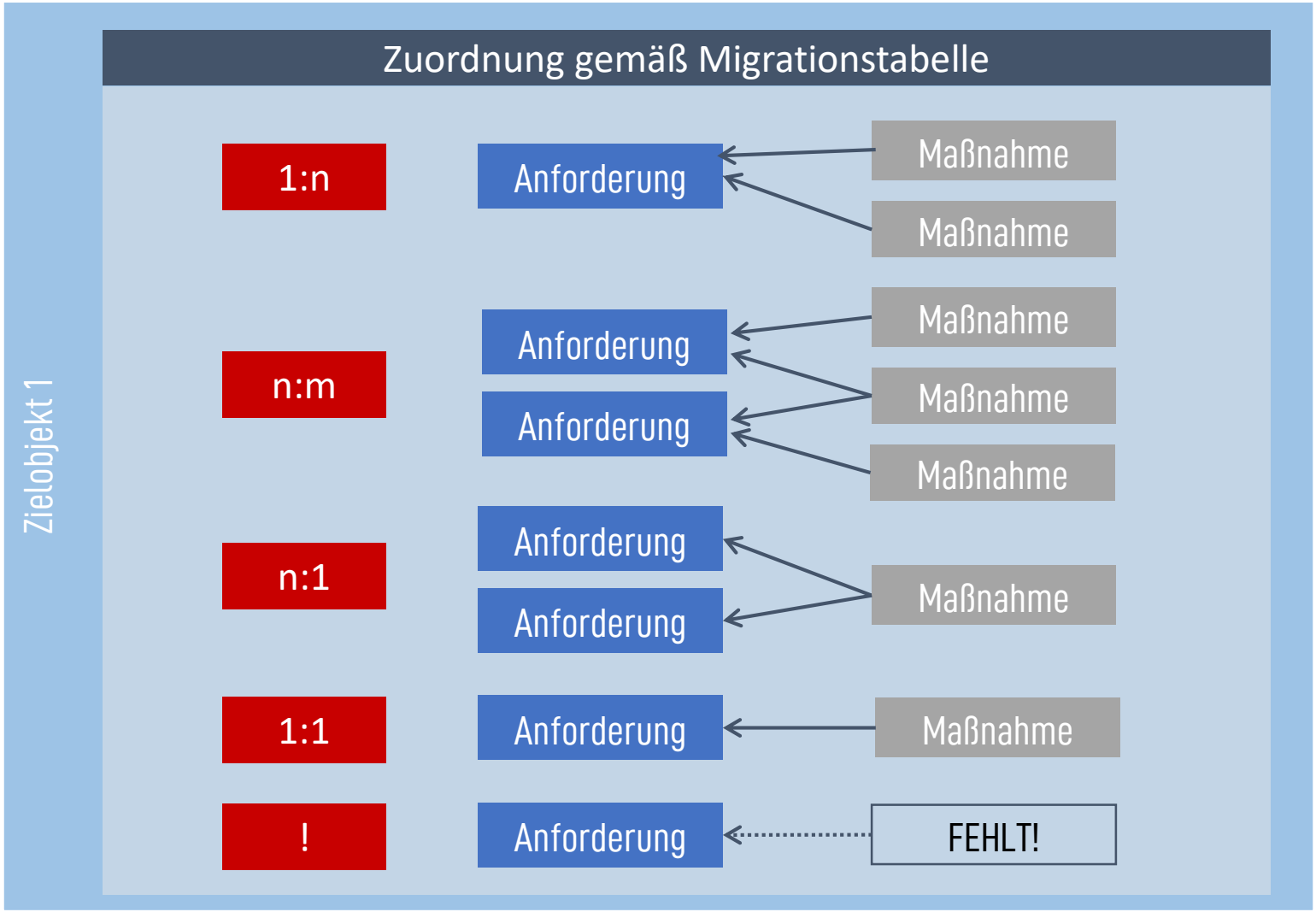
Mögliche Ableitung der Umsetzung der Anforderungen auf Basis der alten Maßnahmen

Beispieldarstellung



		B 5.4 Webserver	M 2.172 (A) Entwicklung eines Konzeptes für Webangebote	M 2.173 (A) Festlegung einer Webserver-Sicherheitsstrategie	M 2.272 (Z) Einrichtung eines Internet-Redaktionsteams	M 2.298 (B) Verwaltung von Internet-Domainnamen	M 4.34 (Z) Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen	M 4.176 (B) Auswahl einer Authentisierungsmethode für Webangebote	M 4.369 (W) Überblick über Komponenten eines Webservers	M 5.64 (Z) Secure Shell	M 5.159 (W) Übersicht über Protokolle und Kommunikationsstandards für Webserver	M 5.160 (W) Authentisierung gegenüber Webservern	M 5.177 (B) Serverseitige Verwendung von SSL/TLS	M 2.176 (Z) Geeignete Auswahl eines Internet Service Providers	M 2.175 (A) Aufbau eines Webservers	M 4.64 (C) Verifizieren der zu übertragenden Daten vor Weitergabe / Beseitigung von Restinformationen	M 4.94 (A) Schutz der Webserver-Dateien	M 4.95 (A) Minimales Betriebssystem	M 4.96 (Z) Abschaltung von DNS	M 4.98 (A) Kommunikation durch Paketfilter auf Minimum beschränken	M 4.360 (B) Sichere Konfiguration eines Webservers	M 5.161 (W) Erstellung von dynamischen Web-Angeboten	M 2.174 (A) Sicherer Betrieb eines Webservers	M 2.273 (A) Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates	M 4.33 (A) Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung	M 4.78 (A) Sorgfältige Durchführung von Konfigurationsänderungen	M 4.177 (B) Sicherstellung der Integrität und Authentizität von Softwarepaketen	M 5.59 (A) Schutz vor DNS-Spoofing bei Authentisierungsmechanismen	M 6.88 (B) Erstellen eines Notfallplans für den Webserver	B 5.21 Webanwendungen	M 4.393 (A) Kontrolliertes Einbinden von Daten und Inhalten bei Webanwendungen	M 4.400 (B) Restriktive Herausgabe sicherheitsrelevanter Informationen bei Webanwendungen und Web-Services	M 4.405 (C) Verhinderung der Blockade von Ressourcen (DoS) bei Webanwendungen und Web-Services	M 5.150 (Z) Durchführung von Penetrationstests	B 5.24 Web-Services	M 2.64 (A) Kontrolle der Protokolldateien	M 4.397 (C) Protokollierung sicherheitsrelevanter Ereignissevon Web Anwendungen und Web-Services	M 2.35 (B) Informationsbeschaffung über Sicherheitslücken des Systems	Bewertung	Kommentar
Basisanforderungen																																									
APP.3.2.A1	Sichere Konfiguration eines Webservers																					x																			2	Umsetzung der Empfehlung aus der 15. EL bzgl. der gekapselten Ausführung des Webservers ist zu prüfen
APP.3.2.A2	Schutz der Webserver-Dateien																	x				x																			3	Nicht vollständig abgedeckte Muss-Anforderung bzgl. der Deaktivierung von Funkionen, der verschlüsselten Übertragung sowie dem Schreibschutz von Dateien
APP.3.2.A3	Absicherung von Datei-Uploads und -Downloads			x																				x																3	Nicht vollständig abgedeckte Muss-Anforderung bzgl. der Maximalgröße von Upload-Dateien sowie der Speicherplatzreservierung
APP.3.2.A4	Protokollierung von Ereignissen																																				x	x		2	Umsetzung der Empfehlung aus der 15. EL bzgl. der Ereignisprotokollierung ist zu prüfen
APP.3.2.A5	Authentisierung							x					x																											2	Umsetzung der Empfehlung aus der 15. EL bzgl. der der Verschlüsselung der Webserver-Authentisierung bei Clients ist zu prüfen
APP.3.2.A6	Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates																								x															1	
APP.3.2.A7	Rechtliche Rahmenbedingungen für Webangebote															x																								3	Nicht vollständig abgedeckte Muss-Anforderung bzgl. der Publikation von Informationen, der Barrierefreiheit bzw. des Behinderten-gleichstellungsgesetzes sowie des Urheberrechts
Standardanforderungen																																									
APP.3.2.A8	Planung des Einsatzes eines Webservers		x	x																																				3	Nicht vollständig abgedeckte Soll-Anforderung bzgl. der Integration des

Fallvarianten bei der Anwendung der Migrationstabellen



Fallvarianten bei der Zuordnung der Maßnahmen

BEWERTUNG

#1 Die Anforderung wird vollständig mit den Maßnahmen aus dem entsprechenden Baustein der 15. EL abgedeckt

#2 Die Anforderung wird vollständig nur unter Berücksichtigung zusätzlicher Maßnahmen aus weiteren Bausteinen abgedeckt.

HANDLUNGSBEDARF

→ i.d.R. nicht erforderlich

→ Wenn Maßnahme nicht vorhanden: Erstellen einer *benutzerdefinierten* Maßnahme

Fallvarianten bei der Zuordnung der Maßnahmen

BEWERTUNG

#3 Die Anforderung wird durch die Maßnahmen der 15. EL nicht vollständig abgedeckt.

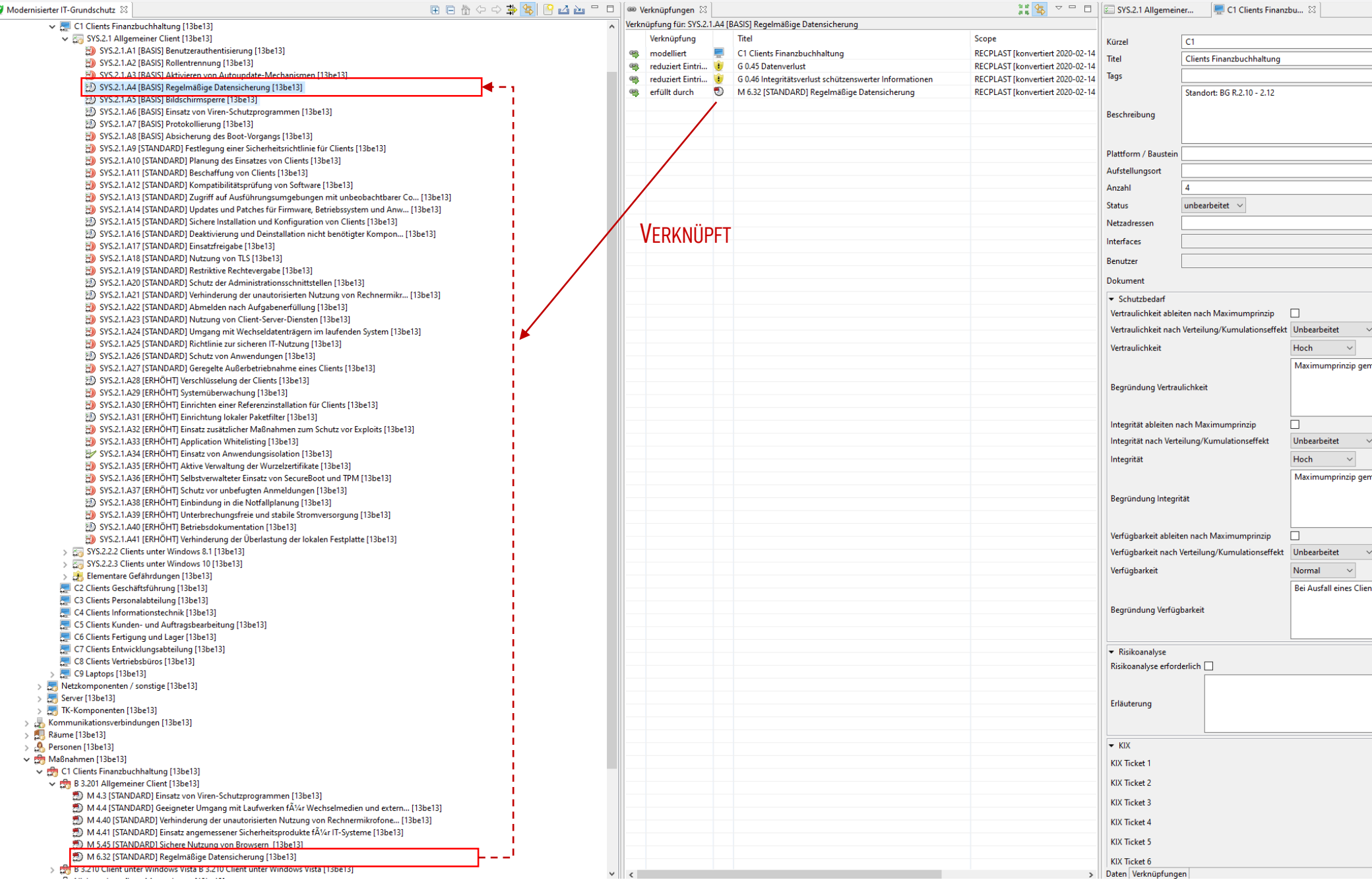
HANDLUNGSBEDARF

→ Für den offenen Handlungsbedarf (Kommentar in der Migrationstabelle) ist immer eine benutzerdefinierte Maßnahme zu erstellen.

→ Wenn Maßnahme nicht vorhanden: Erstellen einer *benutzerdefinierten* Maßnahme

Baumstruktur für Maßnahmen mit Fallunterscheidung

verinice. in Aktion:



Wie die Migration funktioniert

Phase1: Vorbereitung

MODELLIERUNG

- **Konvertierung**
  alten Verbund
  (neue Struktur)
- **Modellierung**
  BSI 200: Bausteine

PROGRAMMIERUNG

- Parsen der benötigten **Migrations-Tabellen** des BSI
- Erstellung und Test der **techn. Lösung**

Phase2: Migration (per API)

BASIS-SICHERHEITSCHECK

- Übernahme Zielobjekte und Bausteine als **Maßnahmen-Gruppen**
- Übernahme von Maßnahmen als **Maßnahmenumsetzung** (gem. festgelegter Varianten!)
- Erstellung **„neue" Maßnahmen-umsetzung** für zusätzlichen Handlungsbedarf gem. BSI Migrationstabellen
- Erstellung **Personen-**Objekte

VERKNÜPFUNGEN

- Verknüpfung Maßnahmen mit Anforderungen
- Verknüpfung Personen mit Maßnahmen

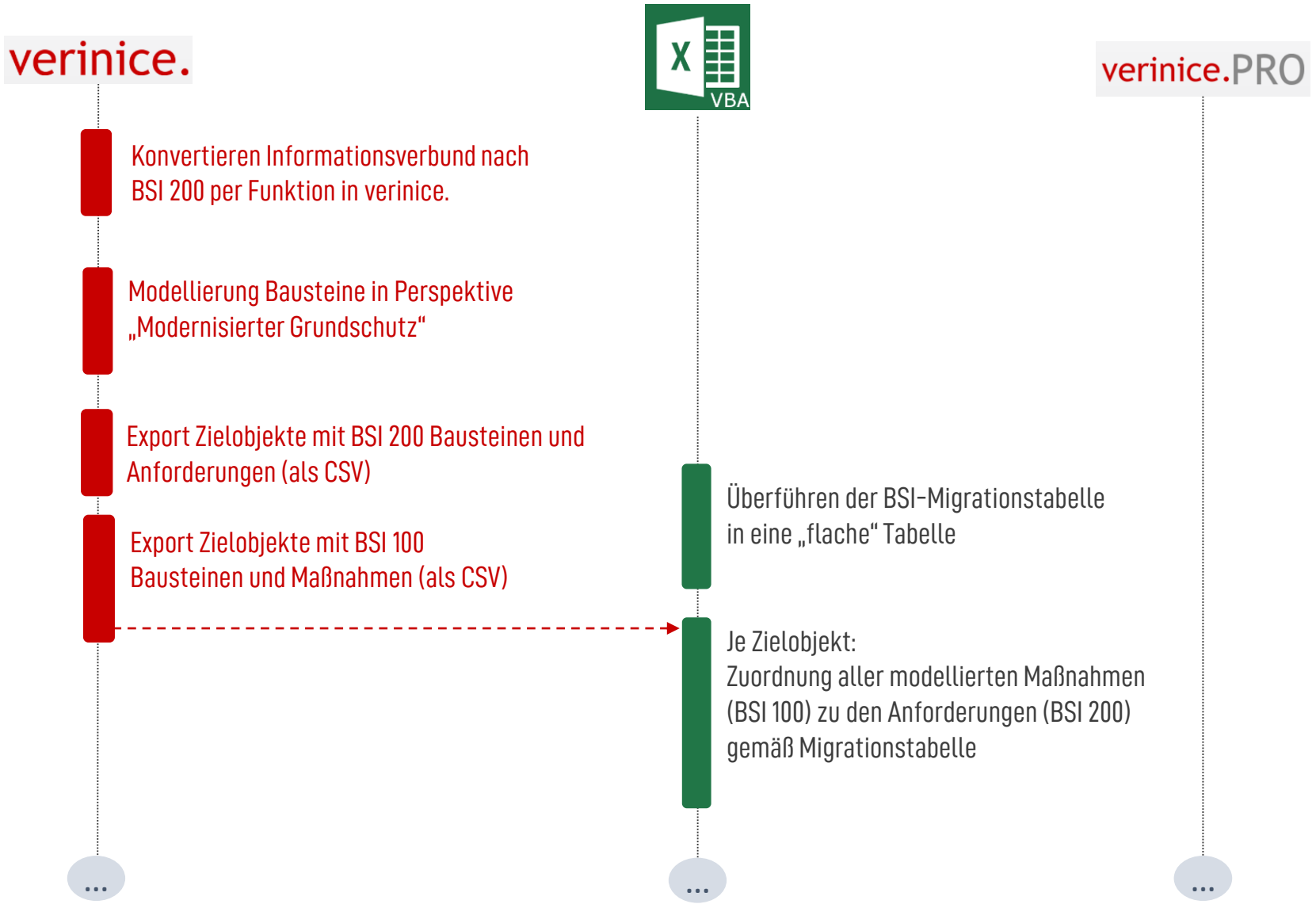
Phase3: Nacharbeiten

KONSOLIDIERUNG

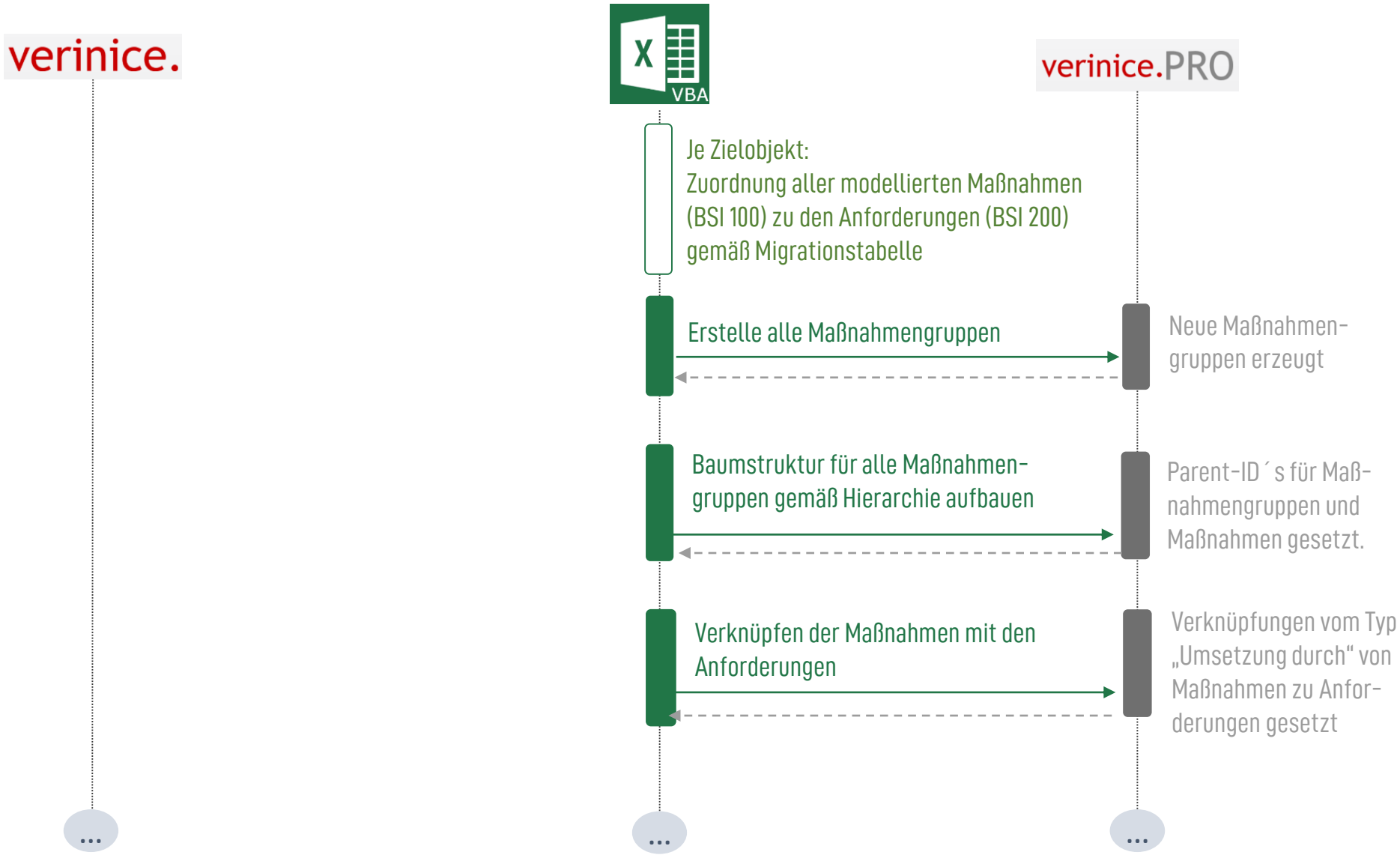
- Durchführung Soll-Ist-Abgleich für BSI 200 – Anforderungen auf Basis verknüpfter Maßnahmen
- Ggf. löschen und überarbeiten der BSI 100-Maßnahmen

Sec2do GmbH • Uhlandstraße 28 • 10719 Berlin

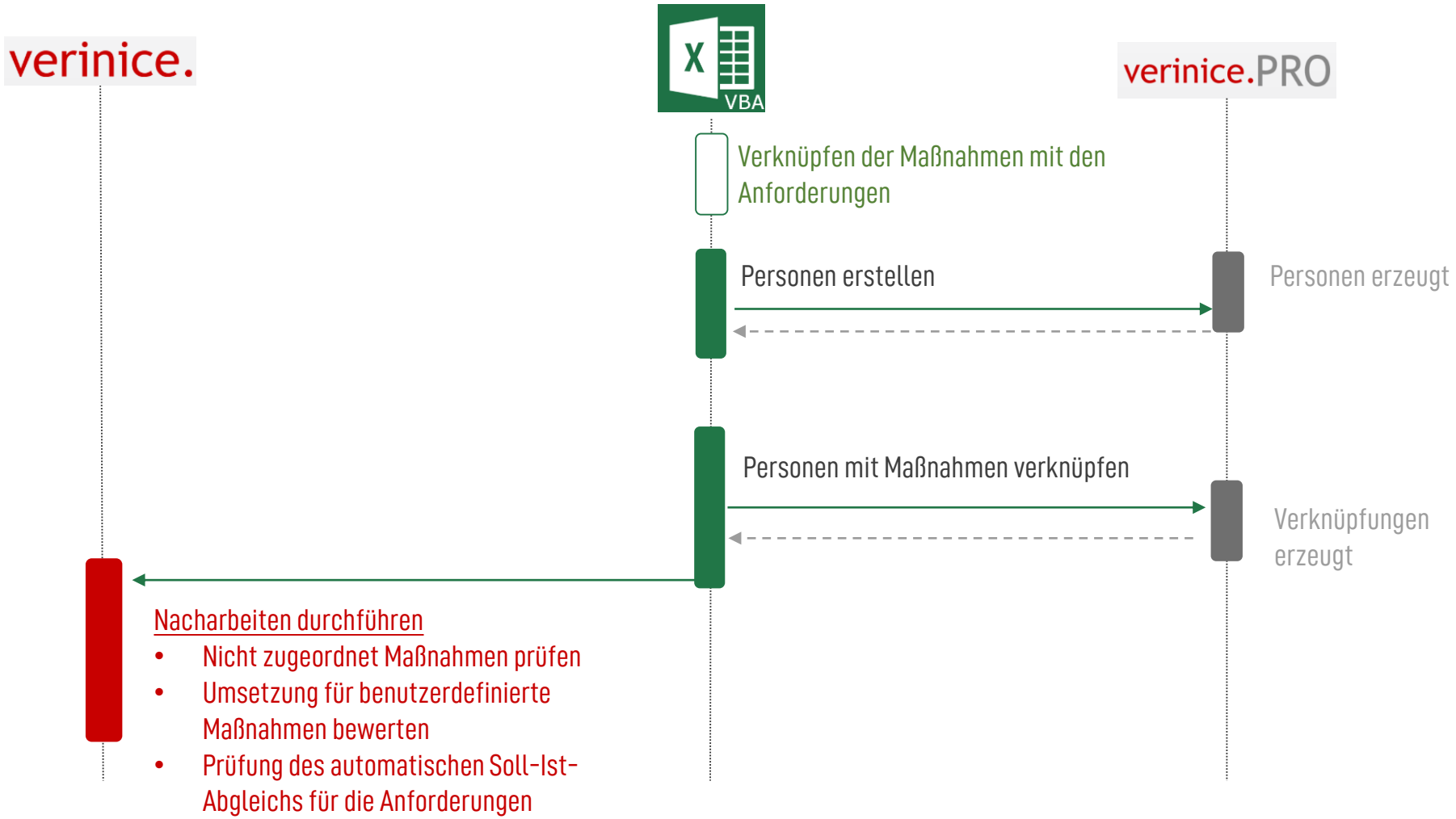
Vorgehen im Detail



Vorgehen im Detail

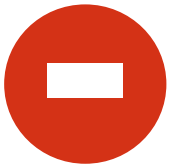


Vorgehen im Detail



Vor- und Nachteile der Lösung

- Vermeidung von Copy & Paste-Fehlern
- Erhalt der BSI-100 Modellierung durch Hybrid-Betrieb
- Reduktion von Zeit und Aufwand
  BEI „GROßEN" VERBÜNDEN



- Einmaliger Aufwand für Erstellung und Test der technischen Umsetzung
- Erfahrung zur Installation und Nutzung der REST-API erforderlich

Vielen Dank
für‘s Mitdenken!

SEC2DO

Informationssicherheit

Angemessen • Nutzerfreundlich • Kreativ

Ihre Informationsrisiken steuern Sie am besten durch erprobte und pragmatische Ansätze, kombiniert mit Verständlichen und leicht nutzbare Lösungen und Tools.

team@sec2do.com
www.sec2do.com

Sec2do GmbH
Uhlandstraße 28
10719 Berlin

Referenzen

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Hella Aglaia

SCHOTT glass made of ideas
ALS UNTERAUFTRAGNEHMER

Bundesamt für Sicherheit in der Informationstechnik
ALS UNTERAUFTRAGNEHMER

Thüringer Aufbaubank
Die Förderbank.

Brandenburgischer IT-Dienstleister

VR Finanz DienstLeistung

sonoxo

T · · Systems ·
ALS UNTERAUFTRAGNEHMER

Kreiskrankenhaus Delitzsch GmbH
KLINIKEN DELITZSCH & EILENBURG

1892

Messe Berlin
ALS UNTERAUFTRAGNEHMER

SENACOR

IHK Potsdam

DKB
Deutsche Kreditbank AG

Schwerpunkte bisheriger Projektarbeit

- Informationssicherheits-Managementsystem (ISO 27001, BSI IT-Grundschutz) etablieren
- Bewertung der Angemessenheit von Sicherheitsmaßnahmen
- Seminare zur Informationssicherheit
- Erstellung der Sicherheitskonzeption im Kontext agiler Softwareentwicklung
- Erstellung eines Branchenspezifischen Sicherheitsstandards (B3S) im Gesundheitsbereich (KRITIS-Umfeld)
- Studien zur IT-Sicherheit, z.B. Erhebung kritischer Systeme in der med. stat. Versorgung in Krankenhäusern (KRITIS-Umfeld)
- Stellung des externen Informations-sicherheitsbeauftragten

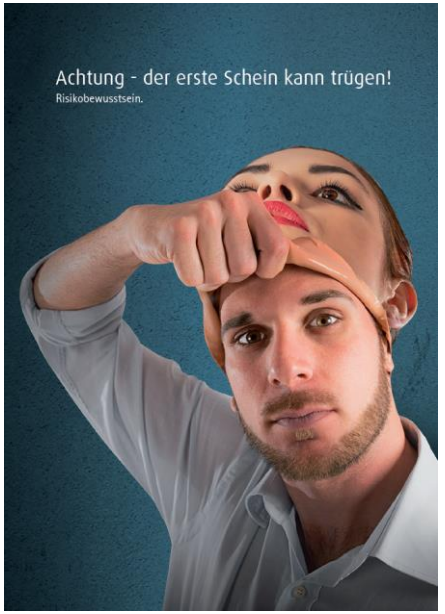
Unsere Leistungen

Schnelltest zur Ermittlung des erreichten Niveaus zur Informationssicherheit

Beratung und Mentoring zum Aufbau und Weiterentwicklung eines passgenauen Informations-sicherheits-Managementsystems

Finden, ausbilden oder stellen des Informationssicherheits-Beauftragten

Ausbildung und Durchführung von Sensibilisierungskampagnen zur Informationssicherheit



Sec2do GmbH • Uhlandstraße 28 • 10719 Berlin

Was Kunden über uns sagen...

An der Zusammenarbeit mit Sec2do schätzen wir neben der fachlichen Expertise vor allem die verbindliche und zuverlässige Arbeitsweise sowie die Flexibilität, auch kurzfristig auf veränderte Rahmenbedingungen reagieren zu können.

DEUTSCHE KRANKENHAUS GESELLSCHAFT DKG

Markus Holzbrecher-Morys
Deutsche Krankenhausgesellschaft e. V.
Stellvertretender Geschäftsführer
(IT, Datenaustausch und eHealth)

Die Firma Sec2do hat sich in der Kooperation mit SONOXO als sehr kompetenter und zuverlässiger Partner erwiesen.

Neben der ausgewiesenen fachlichen Expertise, überzeugen vor allem die Ergebnisqualität, die Projektdurchführung und die methodischen Ansätze.

In der partnerschaftlichen Zusammenarbeit konnte für den Kunden ein besonders hoher Nutzen geschaffen werden, der die initial gestellte Aufgabenstellung übertraf.

SONOXO

Alexander Gutendorf
SONOXO GmbH
Managing Director

Wir standen vor der Herausforderung, unser im Zusammenspiel mit dem Risiko- und Notfallmanagement in kurzer Zeit revisionssicher neu zu gestalten.

Die Zusammenarbeit mit Sec2do hat uns dabei sehr geholfen, die Fülle an Themen und Aufgaben rund um das ISM sowie die Interdependenzen zum Notfall- und Risikomanagement zu verstehen und zu strukturieren.

Insbesondere die Expertise, gepaart mit Flexibilität und Einsatzbereitschaft heben Sec2do von anderen Beratungsgesellschaften im ISM-Umfeld positiv ab. Ohne die Kompetenz und Unterstützung von Sec2do hätten wir es nicht geschafft. Wir danken dem Team sehr für dessen Leistung!

Beauftragter für Informationssicherheit
IT-Dienstleisters im Banksektor

Sec2do GmbH • Uhlandstraße 28 • 10719 Berlin

SONOXO

Die SONOXO GmbH ist ein herstellerunabhängiges Beratungshaus im Bereich IT und Organisation. Das Unternehmen wurde im Mai 2009 von Experten mit langjähriger Führungs- und Projekterfahrung aus dem Umfeld der Betriebsabläufe, des Prozess- und IT-Managements gegründet.

Das SONOXO Portfolio umfasst drei Leistungsblöcke:

- Strategische Beratung
- Projektmanagement
- Sichere Kommunikation

SONOXO Referenzen

SONOXO hat sich als verlässlicher IT-Partner im Bereich der öffentlichen Verwaltung etabliert - auf Bundes, Landes- und Kommunalebene.

SONOXO versteht sich als Beratungs- und Projektmanagementpartner bei Kooperationen mit öffentlich-rechtlichen Rechenzentren, Zweckverbänden und plant die Umsetzung des IT-Betriebs, der IT-Steuerung, der IT-Sicherheit und des IT-Datenschutzes.

IMPRESSUM

Sec2do GmbH
Uhlandstraße 28
10719 Berlin
Deutschland

UID-Nummer:
DE227770516

Geschäftsführer
Martin Peters

Handelsregister:
Berlin (Charlottenburg)
HRB 175859 B

BILDNACHWEIS

123rf.com
© ID 83383390

istockphoto.com
© ID 486902140
© ID 953782574

Fotolia.com
© ID 116655159

DISCLAIMER

Die in Inhalte und Werke dieser Präsentation unterliegen dem deutschen Urheberrecht. Die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung außerhalb der Grenzen des Urheberrechtes bedürfen der schriftlichen Zustimmung der Sec2do GmbH.

Es wird keinerlei Gewähr für die Aktualität, Korrektheit, Vollständigkeit oder Qualität der bereitgestellten Informationen übernommen. Alle Angebote sind freibleibend und unverbindlich.

STAND

Januar 2020

SEC2DO