Konformitätsbericht

2018/19 ISMS ReAudit (2018/19_2_ISMS_INT)

08.10.2018 - 30.06.2019

Inhaltsverzeichis

2018/19 ISMS ReAudit (2018/19_2_ISMS_INT)

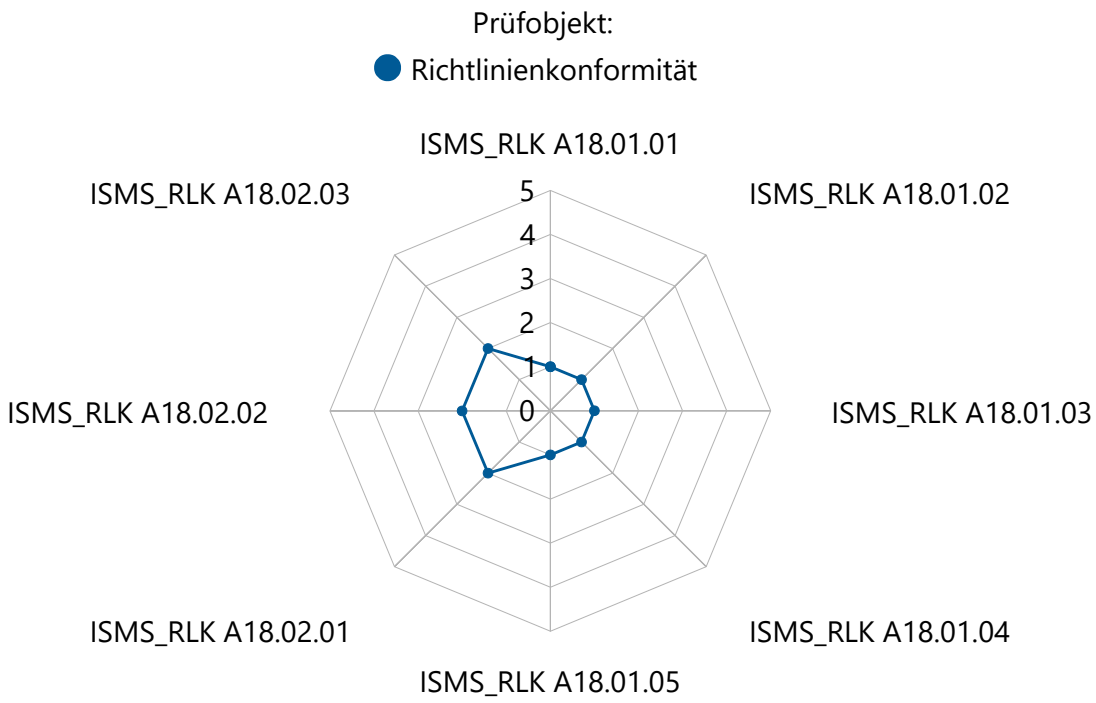
Auditprogramm:	ISM Auditprogramm 2018/19 (ISM 2018/19)	Status:	In Nachbearbeitung
OrgEH:	TogetherSecure Holding AG	Beginn:	08.10.2018
Typ:	Neubewertung Extern: ☐	Ende:	30.06.2019
Hauptprüfer:	Charlotte Hammer		
CoPrüfer:	Lisa Musterfrau, Susi Musterfrau		
Verantwortlich(e):	Daniel Mustermann		
Beschreibung:	Erstbefragungen und Neubewertungen		

Agenda

Bezeichnung	Typ	Beginn	Ende	Status
BIA der Vertriebsabteilung	SBA	08.10.2018 08:00	12.10.2018 10:00	Geschlossen
BIA Kontaktdatenverwaltung	SBA	08.10.2018 08:00	12.10.2018 10:00	Geschlossen
BIA mit der HR	SBA	08.10.2018 08:00	12.10.2018 10:00	Geschlossen
BIA Pflegeheim Eferding	SBA	08.10.2018 08:00	12.10.2018 10:00	Geschlossen
BSI - Virtualisierung	AA	08.10.2018 08:00	12.10.2018 10:00	Angefordert
Pers_AD_BIA	SBA	08.10.2018 08:00	12.10.2018 10:00	Geschlossen
Physische Sicherheitsbegehung	AA	08.10.2018 08:00	12.10.2018 10:00	Geschlossen
ReAudit BIA Pflegeheim Eferding	SBA	08.10.2018 08:00	12.10.2018 10:00	Angefordert
ReAudit Richtlinienkonformität	AA	13.02.2019 08:00	13.02.2019 10:00	Geschlossen
Wirtschaftsprüfungsaudit 2018	PE	04.03.2019 08:00	05.03.2018 17:00	Geschlossen
BSI - Windows Server 2012	AA	10.06.2019 08:00	12.06.2019 10:00	Geschlossen
BSI - Bewertung Relationale Datenbanken	AA	01.07.2019 08:00	03.07.2019 10:00	Geschlossen

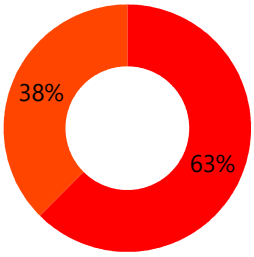
1. ReAudit Richtlinienkonformität

OrgEH:	TogetherSecure Holding AG	Status:	Geschlossen
Audit:	2018/19 ISMS ReAudit (2018/19_2_ISMS_INT)	Beginn:	13.02.2019
Hauptprüfer:	Charlotte Hammer	Ende:	13.02.2019
CoPrüfer:	Lisa Musterfrau, Susi Musterfrau		
Interviewpartner:	Daniel Mustermann		
Beschreibung:	Neuerliche Befragung		


Prüfobjekt:
Richtlinienkonformität
ISMS_RLK A18.01.01
ISMS_RLK A18.01.02
ISMS_RLK A18.01.03
ISMS_RLK A18.01.04
ISMS_RLK A18.01.05
ISMS_RLK A18.02.01
ISMS_RLK A18.02.02
ISMS_RLK A18.02.03
5
4
3
2
1
0

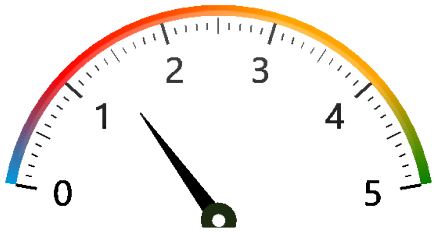
Richtlinienkonformität (RLK)

Verantwortlich(e):	Max Mustermann
Wissensdatenbank:	DEMO: Informationssicherheitsmanagement nach ISO/IEC 27001:2013, Version: 1
Zuletzt geändert:	13.02.2019



Antworten:
- Reifegrad 1: initial (5/8)
- Reifegrad 2: gemanaged (3/8)

Durchschnittlicher Reifegrad



Prüffrage(n):

ISMS_RLK A18.01:	**Einhaltung von gesetzlichen und vertraglichen Anforderungen**	**Strukturfrage**
Frage:	Gibt es Vorkehrungen um zu vermeiden, dass gegen gesetzliche, amtliche oder vertragliche Verpflichtungen im Zusammenhang mit Informationssicherheit oder sonstige Sicherheitsanforderungen verstoßen wird?	
Beschreibung:	Dazu müssen folgende Aspekte im Sinne der Compliance positiv Beachtung finden: - Ist bekannt welche unternehmensinternen und - externen Anforderungen hinsichtlich ISMS gelten? - Ist sichergestellt dass das geistige Eigentum gewahrt wird? - Werden Aufzeichnungen nach gesetzlichen, vertraglichen und geschäftlichen Gesichtspunkten geschützt? - Werden personenbezogene Daten ausreichen geschützt? - Ist sichergestellt, dass die Anforderungen an kryptographische Verfahren und Techniken gesetzeskonform, auch im Umgang mit Drittländern, eingehalten werden?	
Antwort:	Reifegrad 1: initial	
Begründung:	haben wir noch nicht	
Schutzziel(e):	Vertraulichkeit	

ISMS_RLK A18.01.01:	**Ermittlung anwendbarer gesetzlicher und vertraglicher Anforderungen**	**Teilfrage**
Frage:	Ist bekannt welche unternehmensinterne sowie -externe Anforderungen im Sinne der Informationssicherheit gelten?	
Beschreibung:	Werden dabei alle relevanten gesetzlichen, amtlichen und vertraglichen Anforderungen wie beispielsweise die Folgenden bedacht: - Gesetze - Verordnungen - Vorschriften - Normen - Industriestandards - Interne Vorschriften (Anweisungen, Betriebsvereinbarungen) - Vertragliche Vereinbarungen	

Antwort:	**Reifegrad 1: initial**
Schutzziel(e):	Vertraulichkeit

ISMS_RLK A18.01.02:	**Rechte am geistigen Eigentum**	**Teilfrage**
Frage:	Stellen Sie sicher, dass die Beachtung des geistigen Eigentums bei Ihnen im Unternehmen eingehalten wird?	
Beschreibung:	Die Rechte des geistigen Eigentums müssen beachtet werden. Dies sollten Sie in folgenden Bereichen bzw. zu folgenden Themen in Ihrem Unternehmen sichergestellt haben: - Sowohl beim Gebrauch, als auch erst Recht bei der Veröffentlichung ist es Wesentlich Copyrights sowie Warenzeichen zu beachten. - Die Einhaltung von Lizenzbestimmungen insbesondere bei Software ist zu beachten. - Regelungen in Kauf-, Miet- und Leasingverträgen sowie in Wartungsverträgen sind zu beachten.	
Antwort:	**Reifegrad 1: initial**	
Schutzziel(e):	Vertraulichkeit	

ISMS_RLK A18.01.03:	**Schutz von Aufzeichnungen**	**Teilfrage**
Frage:	Sind Aufzeichnung nach gesetzlichen, vertraglichen und geschäftlichen Anforderung vor Verlust, Zerstörung, Fälschung etc. geschützt?	
Beschreibung:	Zur Beantwortung dieser Fragestellung sollten folgende Faktoren berücksichtigt werden: - der Schutzwürdigkeit der Aufzeichnungen (Klassifikation der Daten) - die verwendeten Speichermedien und ihrer Lebensdauer - die Zugriffsrechte auf die Aufzeichnungen - der festgelegten Aufbewahrungs- bzw. Löschfristen	
Antwort:	**Reifegrad 1: initial**	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

ISMS_RLK A18.01.04:	**Privatsphäre und Schutz von personenbezogenen Informationen**	**Teilfrage**
Frage:	Ist sichergestellt, dass der Schutz von personenbezogenen Daten entsprechend der relevanten Gesetze, Vorschriften und Vertragsbedingungen erfolgt?	
Beschreibung:	Dabei sind folgende Vorgaben zu beachten: - Einhaltung der relevanten Datenschutzgesetze bzw. der Datenschutz-Grundverordnung sowie Einhaltung von etwaigen bereichsspezifischen Gesetzen und Verordnungen zum personenbezogenen Datenschutz - Einhaltung von internen Vereinbarungen (Betriebsvereinbarungen, Dienstvereinbarungen, ...) - Einhaltung von Vertragsbedingungen	
Antwort:	**Reifegrad 1: initial**	
Schutzziel(e):	Vertraulichkeit Integrität	

ISMS_RLK	**Regulierung kryptographischer**	**Teilfrage**

A18.01.05:	**Kontrollmaßnahmen**
Frage:	Werden kryptographische Kontrollmaßnahmen angewandt?
Beschreibung:	Um diese Frage beantworten zu können ist auf folgende Aspekte zu hinterfragen: - Gibt es nationale Gesetze zum Import/Export von kryptographischer Hard- und Software und werden diese eingehalten? - Gibt es nationalen Gesetze bei der Anwendung von kryptographischen Verfahren und werden diese eingehalten? - Werden Gesetze anderer Staaten bei grenzübergreifenden Aktivitäten berücksichtigt bzw. eingehalten?
Antwort:	**Reifegrad 1: initial**
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

ISMS_RLK A18.02:	**Informationssicherheitsprüfungen**	**Strukturfrage**
Frage:	Wird sichergestellt, dass die Informationssicherheit im Unternehmen entsprechend der Informationssicherheitspolitik sowie anderen etwaigen Richtlinien, Standards und Verfahren der Organisation implementiert und angewandt wird?	
Beschreibung:	Dazu müssen folgende Aspekte im Sinne der Compliance positiv Beachtung finden: - regelmäßige Überprüfungen des Informationssicherheitsmanagements sind vorgesehen - diese Überprüfung erfolgen durch eine unabhängige Stelle - eine Überprüfung der Technik hinsichtlich der Einhaltung der Informationssicherheitsvorgaben ist vorgesehen	
Antwort:	Reifegrad 2: gemanaged	
Begründung:	hier sind wir definitiv schon weiter als letztes Mal -> Reifegrad 2	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

ISMS_RLK A18.02.01:	**Unabhängige Prüfung der Informationssicherheit**	**Teilfrage**
Frage:	Werden regelmäßige Überprüfungen der Regelungen zur Informationssicherheit bzw. deren Umsetzung durch unabhängige Stellen durchgeführt?	
Beschreibung:	Um diese Frage positiv zu beantworten sollten folgende Aufgaben wahrgenommen werden: - Initiierung unabhängiger Prüfungen durch das Management - Aufzeichnung der Prüfergebnisse - Berichterstattung an das Management - Identifizierung der Möglichkeiten zur Verbesserung und Ergreifen korrigierender Aktionen	
Antwort:	**Reifegrad 2: gemanaged**	
Begründung:	erstmalig gemacht	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

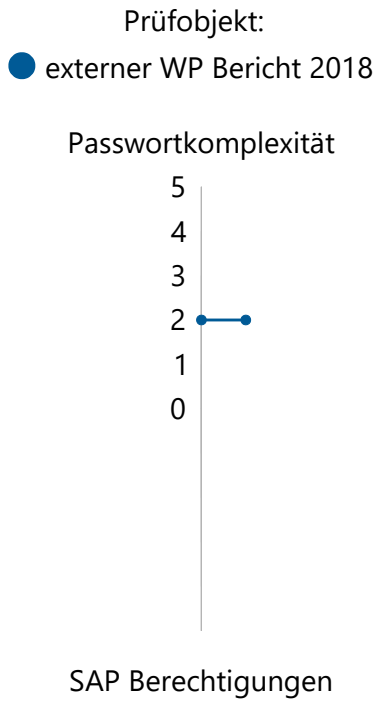
ISMS_RLK A18.02.02:	**Einhaltung der Unternehmensvorgaben zur Informationssicherheit**	**Teilfrage**

Frage:	Erfolgt regelmäßig eine Überprüfung hinsichtlich der Einhaltung der Vorgaben im Unternehmen zum Thema Informationssicherheit die z.B. über Leitlinien, Sicherheitsleitlinien und -normen geregelt sein können?
Beschreibung:	Dabei ist auf Folgendes zu achten: - Wird regelmäßige überprüft ob, die Sicherheitsrichtlinien und Standards eingehalten werden? - Und sofern man zur Erkenntnis gelangt, dass sie nicht eingehalten werden, wird dann überprüft welche Gründe es für die Nichteinhaltung gibt bzw. werden diesbzgl. korrigierende Maßnahmen abgeleitet?
Antwort:	**Reifegrad 2: gemanaged**
Begründung:	erstmalig gemacht
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

ISMS_RLK A18.02.03:	**Inspektion der Technik auf Richtlinienkonformität**	**Teilfrage**
Frage:	Erfolgt eine Prüfung der Informationssysteme auf technische Konformität mit ISMS-Leitlinien und -normen?	
Beschreibung:	Dazu sind folgende Aspekte zu hinterfragen, sowohl im Zuge einer Anschaffung als auch im Betrieb in regelmäßigen Abständen: - Erfolgt eine Prüfung der Erfüllung der technischen Standards und Richtlinien? - Erfolgt die Prüfung durch kompetentes und autorisiertes Personal? - Werden die Prüfungen geplant und wird eine Dokumentation der Prüfungen erstellt?	
Antwort:	**Reifegrad 2: gemanaged**	
Begründung:	erstmalig gemacht	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

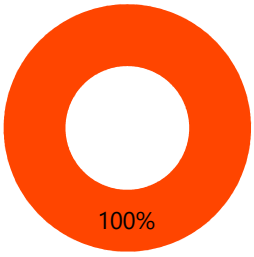
2. Wirtschaftsprüfungsaudit 2018

OrgEH:	TogetherSecure Holding AG	Status:	Geschlossen
Audit:	2018/19 ISMS ReAudit (2018/19_2_ISMS_INT)	Beginn:	04.03.2019
Hauptprüfer:	Charlotte Hammer	Ende:	05.03.2018
CoPrüfer:	Lisa Musterfrau, Susi Musterfrau		
Interviewpartner:	Daniel Mustermann		
Beschreibung:	externes Audit des Wirtschaftsprüfers KPMG		


Prüfobjekt:
externer WP Bericht 2018
Passwortkomplexität
5
4
3
2
1
0
SAP Berechtigungen

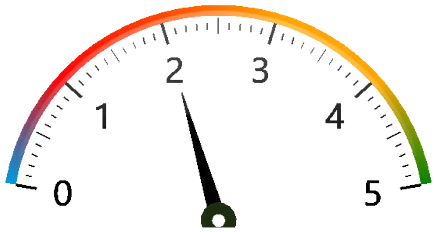
externer WP Bericht 2018 (EXT_WP_2018)

Verantwortlich(e):	Charlotte Hammer
Zuletzt geändert:	04.03.2019



Antworten:
- Reifegrad 2: gemanaged (2/2)

Durchschnittlicher Reifegrad



Prüfergebnisse:

Passwortkomplexität

Kurzbeschreibung	Die Passwortkomplexität ist nicht ausreichend gegeben.
Antwort:	**Reifegrad 2: gemanaged**
Beschreibung:	Die Passwortkomplexität muss erhöht werden. Längere Passwörter sind jedenfalls empfehlenswert!
Schutzziel(e):	Vertraulichkeit Integrität

SAP Berechtigungen

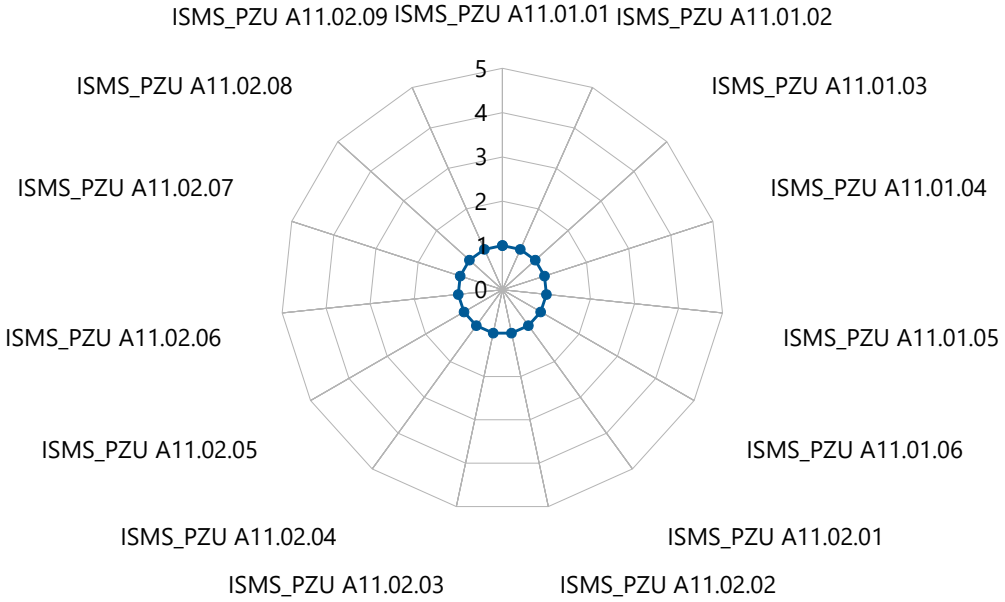
Kurzbeschreibung	Die SAP Berechtigungen müssen häufiger ausgewertet und freigegeben werden.
Antwort:	**Reifegrad 2: gemanaged**
Beschreibung:	SAP Berechtigungen werden 1x im Jahr ausgewertet und freigegeben. Das ist nicht sehr oft: eine halbjährliche Auswertung und Freigabe wird empfohlen.
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

3. Physische Sicherheitsbegehung

OrgEH:	TogetherSecure Holding AG	Status:	Geschlossen
Audit:	2018/19 ISMS ReAudit (2018/19_2_ISMS_INT)	Beginn:	08.10.2018
Hauptprüfer:	Charlotte Hammer	Ende:	12.10.2018
CoPrüfer:	Lisa Musterfrau, Susi Musterfrau		
Interviewpartner:	Daniel Mustermann		

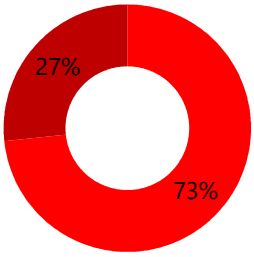
Prüfobjekt:

DEMO: Schutz vor physischem Zugang und Umwelteinflüssen



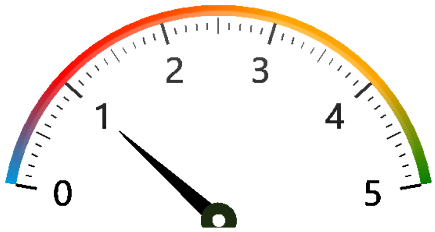
DEMO: Schutz vor physischem Zugang und Umwelteinflüssen (PHY_Sicherheit)

Verantwortlich(e):	Daniel Mustermann
Wissensdatenbank:	DEMO: Informationssicherheitsmanagement nach ISO/IEC 27001:2013, Version: 1
Zuletzt geändert:	04.03.2019



Antworten:
- Nein (11/15)
- Reifegrad 1: initial (4/15)

Durchschnittlicher Reifegrad



Prüffrage(n):

ISMS_PZU A11.01:	**Sicherheitsbereiche** **Strukturfrage**
Frage:	Wird der unautorisierte physische Zugriff auf die Informationen und informationsverarbeitenden Einrichtungen der Organisation sowie deren Beschädigung und Beeinträchtigung verhindert?
Beschreibung:	Werden Maßnahmen wie die folgenden ergriffen: - Einrichtung physischer Sicherheitszonen - Physische Zugangskontrolle - Sicherung von Zweigstellen, Räumen und Anlagen - Schutzmaßnahmen vor externen und umweltbedingten Bedrohungen - Maßnahmen zu Arbeiten im Sicherheitsbereich - Maßnahmen zur Absicherung von Anlieferungs- und Ladezonen
Antwort:	Nein
Begründung:	nein, leider fehlt uns da noch sehr viel!
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

ISMS_PZU A11.01.01:	**Physische Sicherheitszone** **Teilfrage**
Frage:	Wurden Sicherheitszonen zum Schutz von vertraulichen bzw. betriebswichtigen Informationen oder Systemen eingerichtet?
Beschreibung:	Dazu sollten folgenden Aspekte bejaht werden können: - Einrichtung von physischen Sicherheitszonen in abgestufter Form abgeleitet aus den Sicherheitsanforderungen - Maßnahmen zur Kontrolle und Verhinderung von unberechtigtem Zutritt - Schutz gegen Feuer und Einbruch
Antwort:	**Nein**

Schutzziel(e):	Vertraulichkeit	
	Verfügbarkeit	
	Integrität	

ISMS_PZU A11.01.02:	**Physische Zugangskontrolle**	**Teilfrage**
Frage:	Ist ein Schutz der Sicherheitszonen durch angemessene Zugangskontrollen gewährleistet?	
Beschreibung:	Dazu sollten folgende Aspekte bejaht werden können: - Einrichtung von Zutrittskontrollen, die nur berechtigten Personen Zutritt erlauben - Regelungen für den Zutritt von Betriebsfremden (Besuchern, Lieferanten, ...) - Protokollierung von Zutritten - Sichtbares Tragen von Kennungen für Firmenangehörige und Besucher	
Antwort:	**Reifegrad 1: initial**	
Schutzziel(e):	Vertraulichkeit	
	Verfügbarkeit	
	Integrität	

ISMS_PZU A11.01.03:	**Sicherung von Zweigstellen, Räumen und Anlagen**	**Teilfrage**
Frage:	Ist die Implementierung von physischen Sicherheitsvorkehrungen für Zweigstellen, Räume und Anlagen sichergestellt?	
Beschreibung:	Folgende Aspekte sollten bejaht werden können: - Festlegung von physischen Maßnahmen zur Sicherung von Zweigstellen, Räumen und Einrichtungen - Berücksichtigung relevanter Standards für die Gesundheit von Mitarbeitern - Minimierung des öffentlichen Zutritts und Zugangs zu Informationen	
Antwort:	**Reifegrad 1: initial**	
Schutzziel(e):	Vertraulichkeit	
	Verfügbarkeit	
	Integrität	

ISMS_PZU A11.01.04:	**Schutz vor externen und umweltbedingten Bedrohungen**	**Teilfrage**
Frage:	Ist die Implementierung von physischen Schutzvorkehrungen gegen Naturkatastrophen, vorsätzliche Angriffe oder Unfälle vorgesehen?	
Beschreibung:	Dabei sollten folgende Aspekte bejahrt werden können: - Schutz vor Feuer, Wasser, Explosion, etc. und anderen Formen von Katastrophen - Getrennte Lagerung von gefährlichen und brennbaren Materialien - Geeignet Lagerung von BackUp-Datenträgern - Geeignete Anordnung von Fallback-Einrichtungen	
Antwort:	**Nein**	
Schutzziel(e):	Vertraulichkeit	
	Verfügbarkeit	
	Integrität	

ISMS_PZU A11.01.05:	**Arbeit in Sicherheitsbereichen**	**Teilfrage**
Frage:	Ist die Implementierung von physischen Schutzvorkehrungen und Richtlinien für die Arbeit in Sicherheitsbereichen vorgesehen?	
Beschreibung:	Diesbezüglich sollten folgende Aspekte bejaht werden können: - Beschränkung des Wissens über Sicherheitsbereiche auf notwendige Personen - Vermeidung von nicht-überwachten Aktivitäten in Sicherheitsbereichen - Strikte Beschränkung des Erstellen von Fotos, Videos, Sprachaufzeichnungen usw. - Regelungen für externes Personal, das in Sicherheitsbereichen arbeitet	
Antwort:	**Reifegrad 1: initial**	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

ISMS_PZU A11.01.06:	**Anlieferungs- und Ladezonen**	**Teilfrage**
Frage:	Ist die Kontrolle von Punkten für An- und Ablieferungen vor unautorisiertem Zutritten geschützt?	
Beschreibung:	Diesbezüglich sollten folgende Aspekte bejaht werden können: - Einrichtung von Liefer- und Ladezonen mit kontrollierten Zutrittswegen - Maßnahmen, um öffentlichen Zutritt durch Liefer- und Ladezonen zu verhindern - Durchführung von Wareneingangsprüfungen und Aktualisierung des Werte-Inventars	
Antwort:	**Reifegrad 1: initial**	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

ISMS_PZU A11.02:	**Betriebsmittel**	**Strukturfrage**
Frage:	Wird dem Verlust, der Beschädigung, dem Diebstahl oder der Beeinträchtigung von Werten und Unterbrechungen der Betriebstätigkeit der Organisation vorgebeugt?	
Beschreibung:	@ToDo	
Antwort:	Nein	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

ISMS_PZU A11.02.01:	**Platzierung und Schutz von Betriebsmitteln**	**Teilfrage**
Frage:	Wird auf den Schutz von Betriebsmitteln vor Risiken durch Umweltbedrohungen, Gefährdungen und unautorisiertem Zugriff geachtet?	

Beschreibung:	Diesbezüglich sollten folgende Aspekte bejaht werden können: - Schutzmaßnahmen gegen Diebstahl, Feuer, Sprengstoff, Rauch, Wasser, Staub, Schwingungen, chemische Einflüsse, elektromagnetische Störungen, ... - Schutz vor unberechtigtem Zugang zu vertraulichen Informationen - Schutz der Betriebsmittel vor umgebungsbedingten Bedrohungen und unberechtigtem Zugang bei Aufstellung und Gebrauch
Antwort:	**Nein**
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

ISMS_PZU A11.02.02:	**Versorgungseinrichtungen**	**Teilfrage**
Frage:	Ist ein Schutz der Betriebsmittel vor Stromausfällen und Betriebsunterbrechungen vorgesehen?	
Beschreibung:	Diesbezüglich sollten folgende Aspekte bejaht werden können: - Schutz vor Stromausfall und anderen Fehlern von Versorgungseinrichtungen - Sicherstellung der Stromversorgung bei Netzausfällen (Mehrfacheinspeisung, mehrere Lieferanten, USV, Stromgenerator, ...) - Regelmäßige Prüfung aller Versorgungseinrichtungen (Strom, Wasser, Klimaanlage, etc.)	
Antwort:	**Nein**	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

ISMS_PZU A11.02.03:	**Sicherheit der Verkabelung**	**Teilfrage**
Frage:	Ist der Schutz von Stromversorgungs- und Kommunikationskabel vor Abfangen, Beeinträchtigung oder Beschädigung vorgesehen?	
Beschreibung:	Diesbezüglich sollten folgende Aspekte bejaht werden können: - Schutz aller Kabel vor Schaden und Abfangen von Nachrichten - Sichere Führung von Stromkabeln - Sichere Führung von Telekommunikationskabeln/ Netzwerkverkabelung - Getrennte Verlegung von Strom- und Telekommunikationskabeln - Gesicherte Schalteinrichtungen	
Antwort:	**Nein**	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

ISMS_PZU A11.02.04:	**Instandhaltung von Gerätschaften**	**Teilfrage**
Frage:	Ist die ordnungsgemäße Instandhaltung von Gerätschaften sichergestellt?	
Beschreibung:	Diesbezüglich sollten folgende Aspekte bejaht werden können: - Wartung in vorgesehenen Intervallen - Wartung nur durch autorisiertes Personal, eventuell unter Aufsicht - Führung von Aufzeichnungen über durchgeführte Wartungsarbeiten	

	- Durchführung von Kontrollen bei Verschicken von Anlagen/Ausrüstung zur Wartung außer Haus - Einhaltung von Auflagen in Versicherungspolicen
Antwort:	**Nein**
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

ISMS_PZU A11.02.05:	**Entfernung von Werten**	**Teilfrage**
Frage:	Dürfen Ausstattung, Informationen oder Software nur nach Autorisierung entfernt werden?	
Beschreibung:	Diesbezüglich sollten folgende Aspekte bejaht werden können: - Verfahren zum Entfernen von Werten von dem Firmengelände (Autorisierung und Dokumentation) - Schutz vor unberechtigtem Entfernen von Werten und Durchführung von Kontrollen	
Antwort:	**Nein**	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

ISMS_PZU A11.02.06:	**Sicherheit von Betriebsmitteln und Werten außerhalb der Betriebsgebäude**	**Teilfrage**
Frage:	Ist die Anwendung von Sicherheitsvorkehrungen bei Arbeiten außerhalb der Betriebsgebäude sichergestellt?	
Beschreibung:	Diesbezüglich sollten folgende Aspekte bejaht werden können: - Regelungen für den Einsatz von Betriebsmittel und Werten außerhalb der Betriebsgebäude - Durchführung einer Risikoanalyse bei dem Einsatz außerhalb der Betriebsgebäude, z.B. bei der Telearbeit - Versicherungsschutz vereinbaren	
Antwort:	**Nein**	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

ISMS_PZU A11.02.07:	**Sichere Entsorgung oder Wiederverwendung von Betriebsmitteln**	**Teilfrage**
Frage:	Ist die Überprüfung aller Geräte mit Speichermedien vor ihrer Entsorgung oder Wiederverwendung bzgl. der Löschung von vertraulichen Daten oder lizensierter Software sichergestellt?	
Beschreibung:	Diesbezüglich sollten folgende Aspekte bejaht werden können: - Verfahren zur sicheren Entsorgung von Datenträgern - Verfahren zum sicheren Löschen von Informationen - Regelungen zur Wiederverwendung von Speichermedien	
Antwort:	**Nein**	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit	

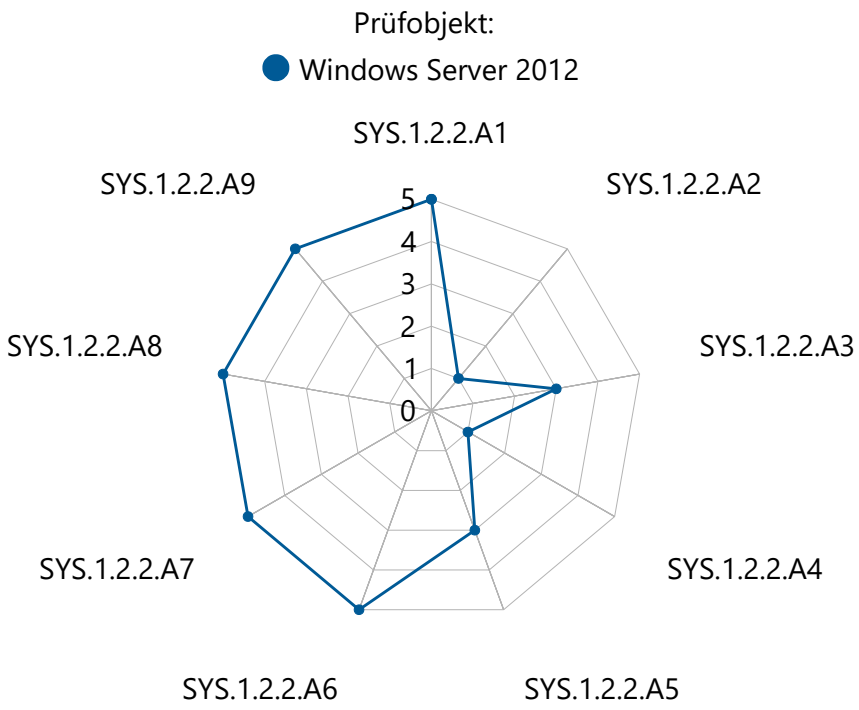
	Integrität	

ISMS_PZU A11.02.08:	**Unbeaufsichtigte Benutzerausstattung**	**Teilfrage**
Frage:	Ist der Schutz von unbeaufsichtigten Benutzerausstattungen gewährleistet?	
Beschreibung:	Diesbezüglich sollten folgende Aspekte bejaht werden können: - Ausschalten des informationsverarbeitenden Gerätes - Einschalten eines passwortgeschützten Bildschirmschoners - Beendigung von Anwendungen - Abmeldung aus Betriebssystemen	
Antwort:	**Nein**	
Schutzziel(e):	Vertraulichkeit  Verfügbarkeit Integrität 	

ISMS_PZU A11.02.09:	**Der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms**	**Teilfrage**
Frage:	Wird der Grundsatz des aufgeräumten Schreibtisches sowie des leeren Bildschirms befolgt?	
Beschreibung:	Diesbezüglich sollten folgende Aspekte bejaht werden können: - Wegräumen/Verschließen von Dokumenten - Wegräumen/Verschließen von tragbaren Speichermedien - Ausschalten des Computers (Mobile Devices) oder Löschen des Bildschirms zusammen mit Passwortschutz beim Verlassen des Arbeitsplatzes - Ausdrucke an offen zugänglichen Druckern/Kopierer und den Gebrauch von reproduzierenden Geräten überwachen	
Antwort:	**Nein**	
Schutzziel(e):	Vertraulichkeit  Verfügbarkeit  Integrität	

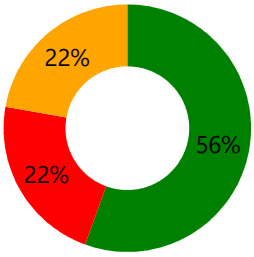
4. BSI - Windows Server 2012

OrgEH:	TogetherSecure Holding AG	Status:	Geschlossen
Audit:	2018/19 ISMS ReAudit (2018/19_2_ISMS_INT)	Beginn:	10.06.2019
Hauptprüfer:	Charlotte Hammer	Ende:	12.06.2019
CoPrüfer:	Lisa Musterfrau, Susi Musterfrau		
Interviewpartner:	Daniel Mustermann		
Beschreibung:	Bewertung der Windows Server 2012 nach BSI Grundschutz Kompendium		


Prüfobjekt:
Windows Server 2012
SYS.1.2.2.A1
SYS.1.2.2.A2
SYS.1.2.2.A3
SYS.1.2.2.A4
SYS.1.2.2.A5
SYS.1.2.2.A6
SYS.1.2.2.A7
SYS.1.2.2.A8
SYS.1.2.2.A9
5
4
3
2
1
0

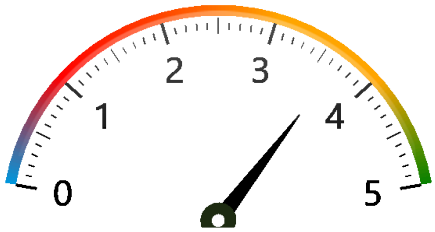
Windows Server 2012 (SYS.1.2.2 (2))

Verantwortlich(e):	Daniel Mustermann
Wissensdatenbank:	© IT-Grundschutz-Kompendium - Edition 2019, Version: 15
Zuletzt geändert:	04.04.2020



Antworten:
- Ja (5/9)
- Nein (2/9)
- Teilweise (2/9)

Durchschnittlicher Reifegrad



Prüffrage(n):

SYS.1.2.2.A1:	**Planung von Windows Server 2012**
Frage:	Wurde die Thematik "SYS.1.2.2.A1 Planung von Windows Server 2012" umgesetzt?
Beschreibung:	Der Einsatz von Windows Server 2012 (R2) MUSS vor der Installation sorgfältig geplant werden. Die Anforderungen an die Hardware MÜSSEN vor der Beschaffung geprüft werden. Es MUSS eine begründete und dokumentierte Entscheidung für eine geeignete Edition des Windows Server 2012 (R2) getroffen werden. Der Einsatzzweck des Servers MUSS dabei spezifiziert werden, inkl. einer geplanten Einbindung ins Active Directory. Die Nutzung von ins Betriebssystem integrierten Cloud-Diensten MUSS grundsätzlich abgewogen und geplant werden. Wenn nicht benötigt, MUSS die Einrichtung von Microsoft-Konten auf dem Server blockiert werden.
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

SYS.1.2.2.A2:	**Sichere Installation von Windows Server 2012**
Frage:	Wurde die Thematik "SYS.1.2.2.A2 Sichere Installation von Windows Server 2012" umgesetzt?
Beschreibung:	Das Installationsmedium MUSS aus einer nachweislich integren Quelle bezogen werden. Es DÜRFEN KEINE anderen als die benötigten Serverrollen und Features bzw. Funktionen installiert werden. Wenn vom Funktionsumfang her ausreichend, MUSS die Server-Core-Variante installiert werden. Andernfalls MUSS begründet werden, warum die Server-Core-Variante nicht genügt. Der Server MUSS im Rahmen der Installation zunächst auf einen aktuellen Patch-Stand gebracht werden.
Antwort:	**Nein**
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

Zugeteilte Gefährdungslage:	**Risiko Windows Server 2012 (Srv2012_Risk)**

SYS.1.2.2.A3:	**Sichere Administration von Windows Server 2012**
Frage:	Wurde die Thematik "SYS.1.2.2.A3 Sichere Administration von Windows Server 2012" umgesetzt?
Beschreibung:	Lokale Administrationskonten MÜSSEN einzigartige, sichere Passwörter besitzen. Alle Administratoren, die für das Serversystem zuständig sind, MÜSSEN in den sicherheitsrelevanten Aspekten der Administration von Windows Server 2012 bzw. R2 geschult sein. Sie DÜRFEN administrative Rechte NICHT einsetzen, wo diese nicht zwingend erforderlich sind. Browser auf dem Server DÜRFEN NICHT zum Surfen im Web verwendet werden.
Antwort:	**Teilweise**
Begründung:	Hier müssen wir uns noch abklären wie es wirklich genau aussieht und überlegen ob wir eine Maßnahme dazu planen sollen
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

Zugeteilte Gefährdungslage:	**Risiko Windows Server 2012 (Srv2012_Risk)**

SYS.1.2.2_STD:	**Standard-Anforderungen**	**Strukturfrage**
Frage:	Sollen weitere Anforderungen für den Baustein "SYS.1.2.2 Windows Server 2012" zur Absicherung des Stands der Technik überprüft werden?	
Beschreibung:	Die folgenden Standard-Anforderungen sollten für diese Thematik erfüllt sein um ein Sicherheitsmaß entsprechend Stand der Technik gewährleisten zu können.	
Antwort:	Ja	

SYS.1.2.2.A4:	**Sichere Konfiguration von Windows Server 2012**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.2.2.A4 Sichere Konfiguration von Windows Server 2012" umgesetzt?	
Beschreibung:	Es SOLLTEN NICHT mehrere wesentliche Funktionen bzw. Rollen durch einen einzigen Server erfüllt werden. Vor Inbetriebnahme SOLLTE das System grundlegend gehärtet werden. Dafür SOLLTEN funktionsspezifische institutionsweite Sicherheitsvorlagen erstellt und gepflegt werden, die auf die Serversysteme ausgerollt werden. Die Einstellungen SOLLTEN anfangs und bei Änderungen vor Inbetriebnahme getestet werden. Der Internet Explorer SOLLTE auf dem Server nur in der Enhanced Security Configuration und im Enhanced Protected Mode genutzt werden.	
Antwort:	**Nein**	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

SYS.1.2.2.A5:	**Schutz vor Schadsoftware**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.2.2.A5 Schutz vor Schadsoftware" umgesetzt?	
Beschreibung:	Außer bei IT-Systemen mit Windows Server 2012, die als Stand-alone- Gerät ohne Netzanschluss und Wechselmedien betrieben werden, SOLLTE vor dem ersten Verbinden mit dem Netz oder Wechselmedien ein	

	Virenschutzprogramm installiert werden. Die Signaturen SOLLTEN regelmäßig aktualisiert werden. Zudem SOLLTEN regelmäßig alle Festplatten vollständig gescannt werden. Es SOLLTEN Alarme für die zuständigen Administratoren bei Virenfunden konfiguriert sein.
Antwort:	**Teilweise**
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

SYS.1.2.2.A6:	**Sichere Authentisierung und Autorisierung in Windows Server 2012**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.2.2.A6 Sichere Authentisierung und Autorisierung in Windows Server 2012" umgesetzt?	
Beschreibung:	In Windows Server 2012 R2 SOLLTEN alle Benutzer Mitglieder der Sicherheitsgruppe "Geschützte Nutzer" sein. Konten für Dienste und Computer SOLLTEN NICHT Mitglied von "Geschützte Nutzer" sein. Dienste-Konten in Windows Server 2012 (R2) SOLLTEN Mitglieder der Gruppe "Managed Service Account" sein, damit die Passwörter der Dienste regelmäßig und vollautomatisch gemäß der AD-Richtlinien gewechselt werden. Der PPL-Schutz des Local Credential Store LSA SOLLTE aktiviert werden. Der Einsatz dynamischer Zugriffsregeln auf Ressourcen SOLLTE bevorzugt werden. Die Administratoren von Windows Server 2012 (R2) SOLLTEN auf ihren eigenen Clients mit beschränkten Rechten arbeiten.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

SYS.1.2.2.A7:	**Sicherheitsprüfung von Windows Server 2012**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.2.2.A7 Sicherheitsprüfung von Windows Server 2012" umgesetzt?	
Beschreibung:	Die Sicherheitskonfiguration von Windows Server 2012 (R2) SOLLTE mittels geeigneter Tools regelmäßig überprüft, dokumentiert und verbessert werden.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

SYS.1.2.2.A8:	**Schutz der Systemintegrität**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.2.2.A8 Schutz der Systemintegrität" umgesetzt?	
Beschreibung:	Secure Boot SOLLTE aktiv sein. AppLocker SOLLTE aktiviert und möglichst strikt konfiguriert sein. Die Auswirkungen von Änderungen SOLLTEN vorab getestet werden.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

SYS.1.2.2.A9:	**Lokale Kommunikationsfilterung**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.2.2.A9 Lokale Kommunikationsfilterung" umgesetzt?	
Beschreibung:	Die lokale Firewall SOLLTE für eingehenden und ausgehenden Netzverkehr aktiviert und möglichst strikt eingestellt sein. Die Identität von Remote-Systemen und die Integrität der Verbindungen mit diesen SOLLTE kryptografisch abgesichert sein.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

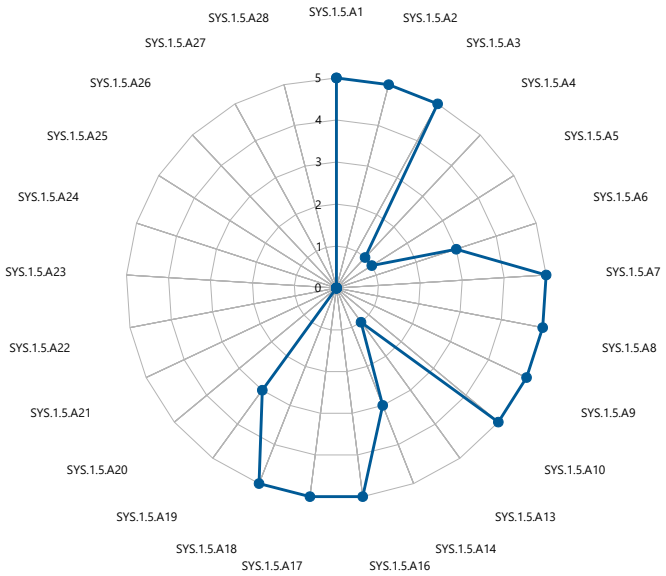
SYS.1.2.2_SBA:	**Anforderungen bei erhöhtem Schutzbedarf**	**Strukturfrage**
Frage:	Sollen weitere Anforderungen bei erhöhtem Schutzbedarf für den Baustein "SYS.1.2.2 Windows Server 2012" überprüft werden?	
Beschreibung:	Die folgenden Anforderungen sollten für diese Thematik erfüllt sein um bei erhöhten Sicherheitsanforderungen ein ausreichendes Sicherheitsausmaß gewährleisten zu können.	
Antwort:	Nein	

5. BSI - Virtualisierung

OrgEH:	TogetherSecure Holding AG	Status:	Angefordert
Audit:	2018/19 ISMS ReAudit (2018/19_2_ISMS_INT)	Beginn:	08.10.2018
Hauptprüfer:	Charlotte Hammer	Ende:	12.10.2018
CoPrüfer:	Lisa Musterfrau, Susi Musterfrau		
Interviewpartner:	Daniel Mustermann		
Beschreibung:	Bewertung der Virtualisierungsumgebung nach BSI Grundschutz Kompendium		

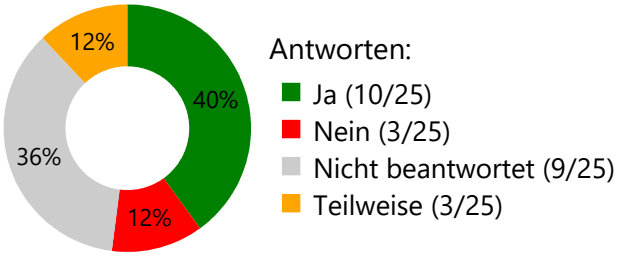
Prüfobjekt:

Virtualisierung

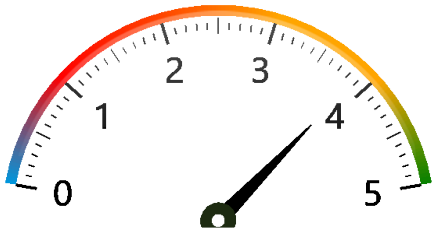


Virtualisierung (SYS.1.5)

Verantwortlich(e):	Daniel Mustermann
Wissensdatenbank:	© IT-Grundschutz-Kompendium - Edition 2019, Version: 15
Zuletzt geändert:	02.12.2019



Durchschnittlicher Reifegrad



Prüffrage(n):

SYS.1.5.A1:	**Einspielen von Aktualisierungen und Sicherheitsupdates**
Frage:	Wurde die Thematik "SYS.1.5.A1 Einspielen von Aktualisierungen und Sicherheitsupdates" umgesetzt?
Beschreibung:	Host-Betriebssystem, Management-Software und Hardware-Firmware MÜSSEN regelmäßig aktualisiert werden. Vorhandene Sicherheitsupdates MÜSSEN zeitnah eingespielt werden. Vorab MUSS auf einem Testsystem überprüft werden, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen.
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

SYS.1.5.A2:	**Sicherer Einsatz virtueller IT-Systeme**
Frage:	Wurde die Thematik "SYS.1.5.A2 Sicherer Einsatz virtueller IT-Systeme" umgesetzt?
Beschreibung:	Jeder Administrator von virtuellen IT-Systemen MUSS wissen, wie sich eine Virtualisierung auf die betriebenen IT-Systeme und Anwendungen auswirkt. Die Zugriffsrechte für Administratoren auf virtuelle IT-Systeme MÜSSEN auf das tatsächlich notwendige Maß reduziert sein. Es MUSS gewährleistet sein, dass die für die virtuellen IT-Systeme notwendigen Netzverbindungen in der virtuellen Infrastruktur verfügbar sind. Auch MUSS geprüft werden, ob die Anforderungen an die Isolation und Kapselung der virtuellen IT-Systeme sowie der darauf betriebenen Anwendungen hinreichend erfüllt sind. Weiterhin MÜSSEN die eingesetzten virtuellen IT-Systeme den Anforderungen an die Verfügbarkeit und den Datendurchsatz genügen. Im laufenden Betrieb MUSS die Performance der virtuellen IT-Systeme überwacht werden.
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

SYS.1.5.A3:	**Sichere Konfiguration virtueller IT-Systeme**
Frage:	Wurde die Thematik "SYS.1.5.A3 Sichere Konfiguration virtueller IT-Systeme" umgesetzt?
Beschreibung:	Gast-Systeme DÜRFEN NICHT auf Geräte und Schnittstellen des Virtualisierungsservers zugreifen. Ist eine solche Verbindung jedoch notwendig, MUSS diese exklusiv und nur für die notwendige Dauer vom Administrator des Host-Systems hergestellt werden. Dafür MÜSSEN verbindliche Regelungen festgelegt werden. Virtuelle IT-Systeme SOLLTEN nach den Sicherheitsrichtlinien der Institution konfiguriert und geschützt werden (siehe dazu die jeweils passenden Bausteine der Schicht SYS *IT-Systeme*).
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

SYS.1.5.A4:	**Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen**
Frage:	Wurde die Thematik "SYS.1.5.A4 Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen" umgesetzt?
Beschreibung:	Es MUSS sichergestellt werden, dass bestehende Sicherheitsmechanismen (z. B. Firewalls) und Monitoring-Systeme nicht durch virtuelle Netze umgangen werden können. Auch MUSS ausgeschlossen sein, dass über virtuelle IT-Systeme, die mit mehreren Netzen verbunden sind, unerwünschte Netzverbindungen aufgebaut werden können. Netzverbindungen zwischen virtuellen IT-Systemen und physischen IT-Systemen sowie für virtuelle Sicherheitsgateways SOLLTEN gemäß den Sicherheitsrichtlinien der Institution konfiguriert werden.
Antwort:	**Nein**
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität
Zugeteilte Gefährdungslage:	**Gefährdungslage Virtualisierung (VM_Risk)**

SYS.1.5.A5:	**Schutz der Administrationsschnittstellen**
Frage:	Wurde die Thematik "SYS.1.5.A5 Schutz der Administrationsschnittstellen" umgesetzt?
Beschreibung:	Alle Administrations- und Management-Zugänge zum Management-System und zu den Host-Systemen MÜSSEN eingeschränkt werden. Es MUSS sichergestellt sein, dass aus nicht-vertrauenswürdigen Netzen heraus nicht auf die Administrationsschnittstellen zugegriffen werden kann. Um die Virtualisierungsserver oder die Management-Systeme zu administrieren bzw. zu überwachen, SOLLTEN ausreichend verschlüsselte Protokolle eingesetzt werden. Sollte dennoch auf unverschlüsselte und damit unsichere Protokolle zurückgegriffen werden, MUSS für die Administration ein eigenes Administrationsnetz genutzt werden.
Antwort:	**Nein**
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

Zugeteilte Gefährdungslage:	**Gefährdungslage Virtualisierung (VM_Risk)**

SYS.1.5.A6:	**Protokollierung in der virtuellen Infrastruktur**
Frage:	Wurde die Thematik "SYS.1.5.A6 Protokollierung in der virtuellen Infrastruktur" umgesetzt?
Beschreibung:	Betriebszustand, Auslastung und Netzanbindungen der virtuellen Infrastruktur MÜSSEN laufend protokolliert werden. Werden Kapazitätsgrenzen erreicht, SOLLTEN virtuelle Maschinen verschoben und eventuell die Hardware erweitert werden. Die Protokollierungsdaten SOLLTEN regelmäßig ausgewertet werden.
Antwort:	**Teilweise**
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

Zugeteilte Gefährdungslage:	**Gefährdungslage Virtualisierung (VM_Risk)**

SYS.1.5.A7:	**Zeitsynchronisation in virtuellen IT-Systemen**
Frage:	Wurde die Thematik "SYS.1.5.A7 Zeitsynchronisation in virtuellen IT-Systemen" umgesetzt?
Beschreibung:	Die Systemzeit aller produktiv eingesetzten IT-Systeme MUSS immer synchron sein (siehe auch OPS.1.1.5 *Protokollierung*).
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

SYS.1.5_STD:	**Standard-Anforderungen** **Strukturfrage**
Frage:	Sollen weitere Anforderungen für den Baustein "SYS.1.5 Virtualisierung" zur Absicherung des Stands der Technik überprüft werden?
Beschreibung:	Die folgenden Standard-Anforderungen sollten für diese Thematik erfüllt sein um ein Sicherheitsmaß entsprechend Stand der Technik gewährleisten zu können.
Antwort:	Ja

SYS.1.5.A8:	**Planung einer virtuellen Infrastruktur** **Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A8 Planung einer virtuellen Infrastruktur" umgesetzt?
Beschreibung:	Der Aufbau der virtuellen Infrastruktur SOLLTE detailliert geplant werden. Dabei SOLLTEN die geltenden Regelungen und Richtlinien für den Betrieb von IT-Systemen, Anwendungen, Netzen und Speichernetzen berücksichtigt werden. Wenn mehrere virtuelle IT-Systeme auf einem Virtualisierungsserver betrieben werden, SOLLTEN keine Konflikte hinsichtlich des Schutzbedarfs der IT-Systeme auftreten. Weiterhin SOLLTEN die Aufgaben der einzelnen Administratorengruppen festgelegt und klar voneinander abgegrenzt werden. Es SOLLTE auch geregelt werden, welcher Mitarbeiter für den Betrieb welcher Komponente verantwortlich ist. Die Administratoren SOLLTEN ausreichend qualifiziert sein.
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit

	Verfügbarkeit ● ● Integrität ● ●

SYS.1.5.A9:	**Netzplanung für virtuelle Infrastrukturen**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A9 Netzplanung für virtuelle Infrastrukturen" umgesetzt?	
Beschreibung:	Der Aufbau des Netzes für virtuelle Infrastrukturen SOLLTE detailliert geplant werden. Dafür SOLLTE der Baustein NET.1.1 *Netzarchitektur und -design* berücksichtigt werden. Auch SOLLTE geprüft werden, ob für bestimmte Virtualisierungsfunktionen (wie z. B. die Live Migration) ein eigenes Netz aufgebaut und genutzt werden muss. Es SOLLTE geplant werden, welche Netzsegmente aufgebaut werden müssen (z. B. Managementnetz, Speichernetz) und wie sie sich sicher voneinander trennen und schützen lassen. Dabei SOLLTE sichergestellt werden, dass das produktive Netz vom Managementnetz getrennt ist (siehe SYS.1.5.A11 *Administration der Virtualisierungsinfrastruktur über ein gesondertes Managementnetz*). Auch die Verfügbarkeitsanforderungen an das Netz SOLLTEN beachtet und erfüllt werden.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit ● ● Verfügbarkeit ● ● Integrität ● ●	

SYS.1.5.A10:	**Einführung von Verwaltungsprozessen für virtuelle IT-Systeme**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A10 Einführung von Verwaltungsprozessen für virtuelle IT-Systeme" umgesetzt?	
Beschreibung:	Für Virtualisierungsserver und virtuelle IT-Systeme SOLLTEN Prozesse für die Inbetriebnahme, die Inventarisierung, den Betrieb und die Außerbetriebnahme definiert und etabliert werden. Die Prozesse SOLLTEN dokumentiert und regelmäßig aktualisiert werden. Wenn der Einsatz geplant wird, SOLLTE festgelegt werden, welche Virtualisierungsfunktionen die virtuellen IT-Systeme benutzen dürfen. Bevor ein virtuelles IT-System betrieben wird, SOLLTE in einer Test- und Entwicklungsumgebung geprüft werden, ob es für den Produktiveinsatz geeignet ist. Test- und Entwicklungsumgebungen SOLLTEN NICHT auf demselben Virtualisierungsserver betrieben werden wie produktive virtuelle IT-Systeme.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit ● ● Verfügbarkeit ● ● Integrität ● ●	

SYS.1.5.A13:	**Auswahl geeigneter Hardware für Virtualisierungsumgebungen**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A13 Auswahl geeigneter Hardware für Virtualisierungsumgebungen" umgesetzt?	
Beschreibung:	Die verwendete Hardware SOLLTE kompatibel zur eingesetzten Virtualisierungslösung sein. Dabei SOLLTE darauf geachtet werden, dass der Hersteller der Virtualisierungslösung über den geplanten Einsatzzeitraum auch Support für die betriebene Hardware anbietet.	
Antwort:	**Nein**	

Schutzziel(e):	Vertraulichkeit	
	Verfügbarkeit	
	Integrität	

SYS.1.5.A14:	**Einheitliche Konfigurationsstandards für virtuelle IT-Systeme**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A14 Einheitliche Konfigurationsstandards für virtuelle IT-Systeme" umgesetzt?	
Beschreibung:	Für die eingesetzten virtuellen IT-Systeme SOLLTEN einheitliche Konfigurationsstandards definiert werden. Die virtuellen IT-Systeme SOLLTEN nach diesen Standards konfiguriert werden. Die Konfigurationsstandards SOLLTEN regelmäßig überprüft und, falls erforderlich, angepasst werden.	
Antwort:	**Teilweise**	
Schutzziel(e):	Vertraulichkeit	
	Verfügbarkeit	
	Integrität	

SYS.1.5.A16:	**Kapselung der virtuellen Maschinen**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A16 Kapselung der virtuellen Maschinen" umgesetzt?	
Beschreibung:	Die Funktionen "Kopieren" und "Einfügen" von Informationen zwischen virtuellen Maschinen SOLLTEN deaktiviert sein.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit	
	Verfügbarkeit	
	Integrität	

SYS.1.5.A17:	**Überwachung des Betriebszustands und der Konfiguration der virtuellen Infrastruktur**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A17 Überwachung des Betriebszustands und der Konfiguration der virtuellen Infrastruktur" umgesetzt?	
Beschreibung:	Der Betriebszustand der virtuellen Infrastruktur SOLLTE überwacht werden. Dabei SOLLTE z. B. geprüft werden, ob noch ausreichend Ressourcen verfügbar sind und ob es eventuell Konflikte bei gemeinsam benutzten Ressourcen eines Virtualisierungsservers gibt. Weiterhin SOLLTEN die Konfigurationsdateien der virtuellen IT-Systeme regelmäßig auf unautorisierte Änderungen überprüft werden. Auch SOLLTE überwacht werden, ob die virtuellen Netze den jeweiligen virtuellen IT-Systemen korrekt zugeordnet sind. Werden Konfigurationsänderungen an der Virtualisierungsinfrastruktur vorgenommen, SOLLTEN diese geprüft bzw. getestet werden, bevor sie umgesetzt werden.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit	
	Verfügbarkeit	
	Integrität	

SYS.1.5.A18:	**Schulung der Administratoren virtueller Umgebungen**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A18 Schulung der Administratoren virtueller Umgebungen" umgesetzt?	
Beschreibung:	Alle Administratoren der virtuellen Umgebung SOLLTEN ausreichend geschult werden. In der Schulung SOLLTE vermittelt werden, wie virtuelle Infrastrukturen sicher aufgebaut und betrieben werden können.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

SYS.1.5.A19:	**Regelmäßige Audits der Virtualisierungsinfrastruktur**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A19 Regelmäßige Audits der Virtualisierungsinfrastruktur" umgesetzt?	
Beschreibung:	Es SOLLTE regelmäßig auditiert werden, ob der Ist-Zustand der virtuellen Infrastruktur dem in der Planung festgelegten Zustand entspricht und ob die Konfiguration der virtuellen Komponenten die vorgegebene Standardkonfiguration einhält. Die Auditergebnisse SOLLTEN nachvollziehbar dokumentiert werden. Abweichungen SOLLTEN behoben werden.	
Antwort:	**Teilweise**	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

SYS.1.5_SBA:	**Anforderungen bei erhöhtem Schutzbedarf**	**Strukturfrage**
Frage:	Sollen weitere Anforderungen bei erhöhtem Schutzbedarf für den Baustein "SYS.1.5 Virtualisierung" überprüft werden?	
Beschreibung:	Die folgenden Anforderungen sollten für diese Thematik erfüllt sein um bei erhöhten Sicherheitsanforderungen ein ausreichendes Sicherheitsausmaß gewährleisten zu können.	
Antwort:	Nicht beantwortet	

SYS.1.5.A20:	**Verwendung von hochverfügbaren Architekturen**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A20 Verwendung von hochverfügbaren Architekturen" umgesetzt?	
Beschreibung:	Die virtuelle Infrastruktur SOLLTE hochverfügbar ausgelegt werden. Alle Virtualisierungsserver SOLLTEN in Clustern zusammengeschlossen werden.	
Antwort:	Nicht beantwortet	
Schutzziel(e):	Verfügbarkeit	

SYS.1.5.A21:	**Sichere Konfiguration virtueller IT-Systeme bei erhöhtem Schutzbedarf**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A21 Sichere Konfiguration virtueller IT-Systeme bei	

	erhöhtem Schutzbedarf" umgesetzt?
Beschreibung:	Für virtuelle IT-Systeme SOLLTEN Überbuchungsfunktionen für Ressourcen deaktiviert werden.
Antwort:	Nicht beantwortet
Schutzziel(e):	Verfügbarkeit Integrität

SYS.1.5.A22:	**Härtung des Virtualisierungsservers**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A22 Härtung des Virtualisierungsservers" umgesetzt?	
Beschreibung:	Der Virtualisierungsserver SOLLTE gehärtet werden. Um virtuelle IT-Systeme voreinander und gegenüber dem Virtualsierungsserver zusätzlich zu isolieren und zu kapseln, SOLLTEN Mandatory Access Controls eingesetzt werden. Ebenso SOLLTE das IT-System gehärtet werden, auf dem die Management-Software installiert ist.	
Antwort:	Nicht beantwortet	
Schutzziel(e):	Vertraulichkeit Integrität	

SYS.1.5.A23:	**Rechte-Einschränkung der virtuellen Maschinen**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A23 Rechte-Einschränkung der virtuellen Maschinen" umgesetzt?	
Beschreibung:	Alle Schnittstellen und Kommunikationskanäle, die es einem virtuellen IT-System erlauben, Informationen über das Host-System auszulesen und abzufragen, SOLLTEN deaktiviert sein oder unterbunden werden. Weiterhin SOLLTE ausschließlich der Virtualisierungsserver auf seine Ressourcen zugreifen können. Außerdem SOLLTE es NICHT möglich sein, dass sich virtuelle IT-Systeme sogenannte *Pages* des Arbeitsspeichers teilen.	
Antwort:	Nicht beantwortet	
Schutzziel(e):	Vertraulichkeit Integrität	

SYS.1.5.A24:	**Deaktivierung von Snapshots virtueller IT-Systeme**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A24 Deaktivierung von Snapshots virtueller IT-Systeme" umgesetzt?	
Beschreibung:	Für alle virtuellen IT-Systeme SOLLTE die Snapshot-Funktion deaktiviert werden.	
Antwort:	Nicht beantwortet	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

SYS.1.5.A25:	**Minimale Nutzung von Konsolenzugriffen auf virtuelle IT-Systeme**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A25 Minimale Nutzung von Konsolenzugriffen auf virtuelle IT-Systeme" umgesetzt?	
Beschreibung:	Direkte Zugriffe auf die emulierten Konsolen virtueller IT-Systeme SOLLTEN auf ein Mindestmaß reduziert werden. Die virtuellen Systeme SOLLTEN möglichst über das Netz gesteuert werden.	

Antwort:	Nicht beantwortet
Schutzziel(e):	Verfügbarkeit

SYS.1.5.A26:	**Einsatz einer PKI**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A26 Einsatz einer PKI" umgesetzt?	
Beschreibung:	Da die Kommunikation zwischen den Komponenten der IT-Infrastruktur häufig mithilfe von Zertifikaten abgesichert wird, SOLLTE eine Public-Key-Infrastruktur (PKI) eingesetzt werden.	
Antwort:	Nicht beantwortet	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

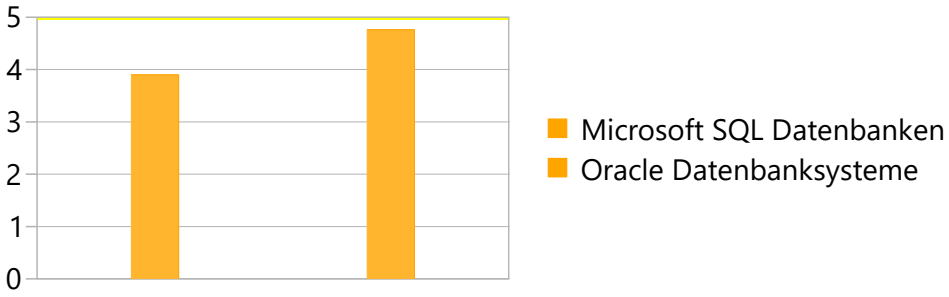
SYS.1.5.A27:	**Einsatz zertifizierter Virtualisierungssoftware**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A27 Einsatz zertifizierter Virtualisierungssoftware" umgesetzt?	
Beschreibung:	Es SOLLTE zertifizierte Virtualisierungssoftware der Stufe EAL 4 oder höher eingesetzt werden.	
Antwort:	Nicht beantwortet	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

SYS.1.5.A28:	**Verschlüsselung von virtuellen IT-Systemen**	**Teilfrage**
Frage:	Wurde die Thematik "SYS.1.5.A28 Verschlüsselung von virtuellen IT-Systemen" umgesetzt?	
Beschreibung:	Alle virtuellen IT-Systeme SOLLTEN verschlüsselt werden.	
Antwort:	Nicht beantwortet	
Schutzziel(e):	Vertraulichkeit Integrität	

6. BSI - Bewertung Relationale Datenbanken

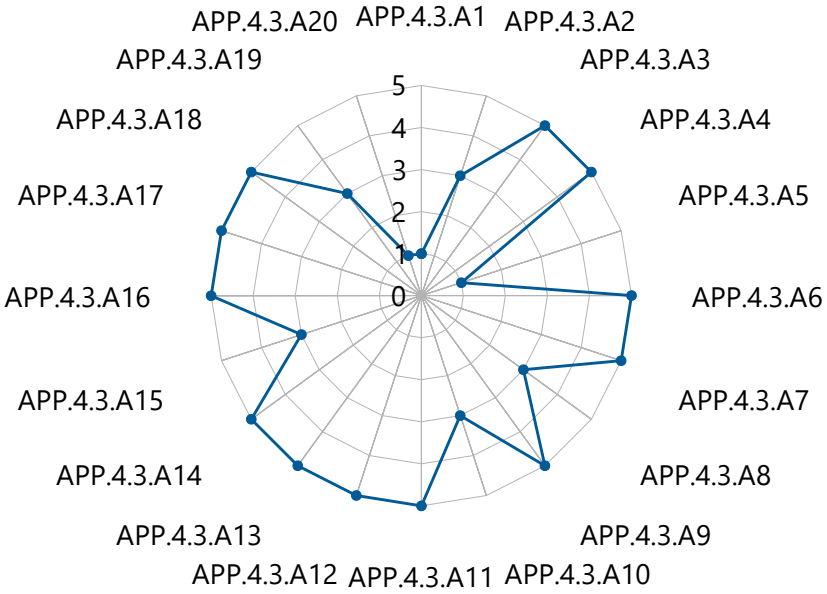
OrgEH:	TogetherSecure Holding AG	Status:	Geschlossen
Audit:	2018/19 ISMS ReAudit (2018/19_2_ISMS_INT)	Beginn:	01.07.2019
Hauptprüfer:	Charlotte Hammer	Ende:	03.07.2019
CoPrüfer:	Lisa Musterfrau, Susi Musterfrau		
Interviewpartner:	Daniel Mustermann		
Beschreibung:	Abweichungsanalyse für SQL DBs und ORACLE DBs nach BSI		

Durchschnittlicher Reifegrad der Prüfobjekte



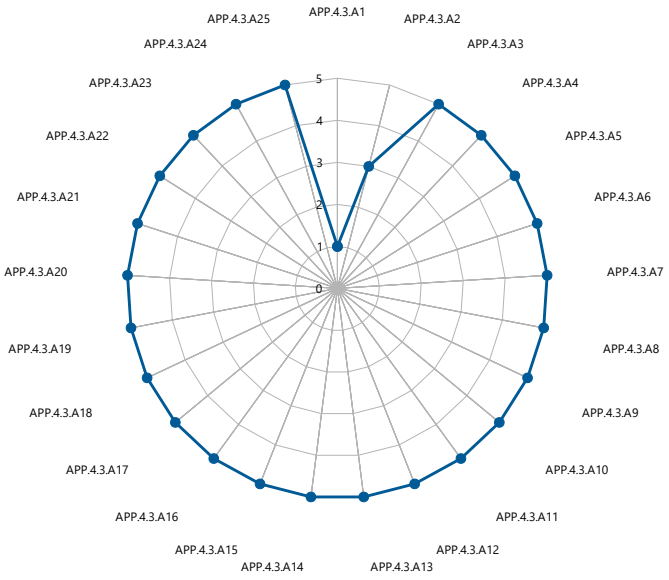
Prüfobjekt:

Microsoft SQL Datenbanken



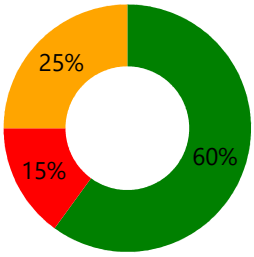
Prüfobjekt:

Oracle Datenbanksysteme



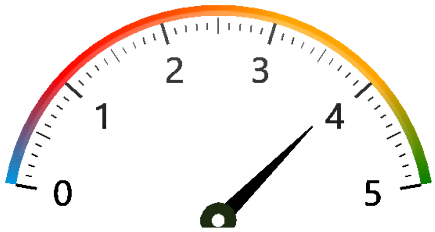
Microsoft SQL Datenbanken (SQL_DB)

Verantwortlich(e):	Daniel Mustermann
Wissensdatenbank:	© IT-Grundschutz-Kompendium - Edition 2019, Version: 15
Zuletzt geändert:	04.04.2020



Antworten:
- Ja (12/20)
- Nein (3/20)
- Teilweise (5/20)

Durchschnittlicher Reifegrad



Prüffrage(n):

APP.4.3.A1:	**Erstellung einer Sicherheitsrichtlinie für Datenbanksysteme**
Frage:	Wurde die Thematik "APP.4.3.A1 Erstellung einer Sicherheitsrichtlinie für Datenbanksysteme" umgesetzt?
Beschreibung:	Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für Datenbanksysteme erstellt werden, in der nachvollziehbar Anforderungen und Vorgaben beschrieben sind, wie Datenbanksysteme sicher betrieben werden können. Die Richtlinie MUSS allen im Bereich Datenbanksysteme verantwortlichen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit dem ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse MÜSSEN sinnvoll dokumentiert werden.
Antwort:	**Nein**
Begründung:	fehlt derzeit
Schutzziel(e):	Vertraulichkeit ● ● ● ● Verfügbarkeit ● ● ● ● Integrität ● ● ● ●

Zugeteilte Gefährdungslage:	**Gefährdungslage Microsoft SQL Datenbanken (SQL_DB)**

APP.4.3.A2:	**Installation des Datenbankmanagementsystems**
Frage:	Wurde die Thematik "APP.4.3.A2 Installation des Datenbankmanagementsystems" umgesetzt?
Beschreibung:	Es MUSS sichergestellt sein, dass die Installationspakete des Datenbankmanagementsystems aus sicheren Quellen stammen. Bereits veröffentlichte Patches MÜSSEN eingespielt werden, bevor das DBMS betrieben wird.
Antwort:	**Teilweise**
Begründung:	es gibt dazu kein niedergeschriebenes Vorgehen, auch wenn es idR so erfolgt

Schutzziel(e):	Vertraulichkeit	● ● ● ●
	Verfügbarkeit	● ● ● ●
	Integrität	● ● ● ●

Zugeteilte Gefährdungslage:	**Gefährdungslage Microsoft SQL Datenbanken (SQL_DB)**

APP.4.3.A3:	**Basishärtung des Datenbankmanagementsystems**	
Frage:	Wurde die Thematik "APP.4.3.A3 Basishärtung des Datenbankmanagementsystems" umgesetzt?	
Beschreibung:	Das Datenbankmanagementsystem MUSS gehärtet werden. Hierfür MUSS eine Checkliste mit den durchzuführenden Schritten zusammengestellt und abgearbeitet werden. Auch MÜSSEN alle Passwörter entsprechend den internen Anforderungen der Institution geändert werden. Alle Passwörter MÜSSEN verschlüsselt gespeichert werden. Die Basishärtung MUSS regelmäßig überprüft und falls erforderlich angepasst werden.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit	● ● ● ●
	Verfügbarkeit	● ● ● ●
	Integrität	● ● ● ●

APP.4.3.A4:	**Geregeltes Anlegen neuer Datenbanken**	
Frage:	Wurde die Thematik "APP.4.3.A4 Geregeltes Anlegen neuer Datenbanken" umgesetzt?	
Beschreibung:	Neue Datenbanken MÜSSEN nach einem definierten Prozess angelegt werden. Wenn eine neue Datenbank angelegt wird, MÜSSEN Grundinformationen zur Datenbank nachvollziehbar dokumentiert werden.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit	● ● ● ●
	Verfügbarkeit	● ● ● ●
	Integrität	● ● ● ●

APP.4.3.A5:	**Benutzer- und Berechtigungskonzept**	
Frage:	Wurde die Thematik "APP.4.3.A5 Benutzer- und Berechtigungskonzept" umgesetzt?	
Beschreibung:	Das Benutzer- und Berechtigungskonzept (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*) der Institution MUSS um die für Datenbankmanagementsysteme notwendigen Berechtigungen für Rollen, Profile und Benutzergruppen erweitert werden. Es MUSS ein Prozess etabliert werden, der regelt, wie Datenbankbenutzer und deren Berechtigungen angelegt, genehmigt, eingerichtet, modifiziert und wieder entzogen bzw. gelöscht werden. Dabei DÜRFEN immer NUR so viele Zugriffsrechte vergeben werden, wie für die jeweiligen Aufgaben erforderlich sind (Need-to-know-Prinzip). Alle Änderungen SOLLTEN dokumentiert werden. Die eingerichteten Benutzer und die ihnen zugeordneten Berechtigungen MÜSSEN regelmäßig überprüft und, falls erforderlich, angepasst werden.	
Antwort:	**Nein**	
Begründung:	derzeit gibt es hier zu viele Zuriffsrechte	
Schutzziel(e):	Vertraulichkeit	● ● ● ●
	Verfügbarkeit	● ● ● ●
	Integrität	● ● ● ●

Zugeteilte Gefährdungslage:	**Gefährdungslage Microsoft SQL Datenbanken (SQL_DB)**

APP.4.3.A6:	**Passwortänderung**
Frage:	Wurde die Thematik "APP.4.3.A6 Passwortänderung" umgesetzt?
Beschreibung:	Alle Passwörter der Datenbankbenutzer MÜSSEN der Passwortrichtlinie der Institution entsprechen (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*). Es MUSS gewährleistet sein, dass die Passwörter beim geringsten Verdacht eines diesbezüglichen Sicherheitsvorfalles geändert werden. Insbesondere bei privilegierten Datenbankaccounts und Dienstkonten SOLLTE ein Passwortwechsel sorgfältig geplant und gegebenenfalls mit den Anwendungsverantwortlichen abgestimmt werden.
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

APP.4.3.A7:	**Zeitnahes Einspielen von Sicherheitsupdates**
Frage:	Wurde die Thematik "APP.4.3.A7 Zeitnahes Einspielen von Sicherheitsupdates" umgesetzt?
Beschreibung:	Vorhandene Sicherheitsupdates für das Datenbankmanagementsystem und das Betriebssystem MÜSSEN zeitnah installiert werden. Vorab MUSS auf einem Testsystem überprüft werden, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen. Bevor ein Patch eingespielt wird, MUSS das Datenbanksystem gesichert werden (siehe APP.4.3.A9 *Datensicherung eines Datenbanksystems*). Zusätzlich MUSS eine verantwortliche Rolle definiert werden, die dafür zuständig ist, sich regelmäßig über bekannte Sicherheitslücken des Datenbankmanagementsystems sowie über verfügbare Sicherheitsupdates zu informieren. Des Weiteren MUSS geprüft werden, ob die Update-Intervalle des Datenbankmanagementsystems auf die Update-Zyklen des Herstellers abgestimmt werden können. Das Ergebnis SOLLTE nachvollziehbar dokumentiert werden.
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

APP.4.3.A8:	**Datenbank-Protokollierung**
Frage:	Wurde die Thematik "APP.4.3.A8 Datenbank-Protokollierung" umgesetzt?
Beschreibung:	Sicherheitsrelevante Ereignisse des Datenbanksystems MÜSSEN mit einem eindeutigen Zeitstempel protokolliert werden. Dabei MÜSSEN sich Art und Umfang der Protokollierung am Schutzbedarf der zu verarbeitenden Informationen orientieren. Zusätzlich MUSS geprüft werden, ob die Protokollierung der Fachanwendungen zusammen mit der Protokollierung der Datenbank alle erforderlichen Informationen abdeckt, um betriebs- und sicherheitsrelevante Veränderungen an der Datenbankinfrastruktur und den Anwendungen zu erkennen. Es SOLLTE so protokolliert werden, dass die Protokolldateien nicht nachträglich veränderbar sind. Vertiefende Informationen sind in OPS.1.1.5 *Protokollierung* zu finden.
Antwort:	**Teilweise**
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

Zugeteilte Gefährdungslage:	**Gefährdungslage Microsoft SQL Datenbanken (SQL_DB)**

APP.4.3.A9:	**Datensicherung eines Datenbanksystems**
Frage:	Wurde die Thematik "APP.4.3.A9 Datensicherung eines Datenbanksystems" umgesetzt?
Beschreibung:	Es MÜSSEN regelmäßig Systemsicherungen des DBMS und der Daten durchgeführt werden. Auch bevor eine Datenbank neu erzeugt wird, MUSS das Datenbanksystem gesichert werden. Hierfür SOLLTEN die dafür zulässigen Dienstprogramme benutzt werden. Alle Transaktionen SOLLTEN so gesichert werden, dass sie jederzeit wiederherstellbar sind. Sofern die Datensicherung die verfügbaren Kapazitäten übersteigt, SOLLTE ein erweitertes Konzept (z. B. inkrementelle Sicherung) erstellt werden, um die Datenbank zu sichern. Abhängig vom Schutzbedarf der Daten SOLLTEN die Wiederherstellungsparameter vorgegeben werden (siehe CON.3 *Datensicherungskonzept)*.
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

APP.4.3_STD:	**Standard-Anforderungen** **Strukturfrage**
Frage:	Sollen weitere Anforderungen für den Baustein "APP.4.3 Relationale Datenbanksysteme" zur Absicherung des Stands der Technik überprüft werden?
Beschreibung:	Die folgenden Standard-Anforderungen sollten für diese Thematik erfüllt sein um ein Sicherheitsmaß entsprechend Stand der Technik gewährleisten zu können.
Antwort:	Ja

APP.4.3.A10:	**Auswahl geeigneter Datenbankmanagementsysteme** **Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A10 Auswahl geeigneter Datenbankmanagementsysteme" umgesetzt?
Beschreibung:	Bevor Datenbankmanagementsysteme beschafft werden, SOLLTEN Anforderungen an die DBMS definiert und in einem Anforderungskatalog dokumentiert werden. Danach SOLLTEN alle infrage kommenden Datenbankmanagementsysteme anhand des Katalogs bewertet werden. Die Ergebnisse SOLLTEN dokumentiert werden.
Antwort:	**Teilweise**
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

APP.4.3.A11:	**Ausreichende Dimensionierung der Hardware** **Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A11 Ausreichende Dimensionierung der Hardware" umgesetzt?
Beschreibung:	Datenbankmanagementsysteme SOLLTEN auf ausreichend dimensionierter Hardware installiert werden. Die Hardware SOLLTE über genügend Reserven verfügen, um auch eventuell steigenden Anforderungen gerecht zu werden. Zeichnen sich trotzdem während des Betriebs Ressourcenengpässe ab, SOLLTEN diese frühzeitig behoben werden. Wenn die Hardware dimensioniert wird, SOLLTE das erwartete Wachstum für den geplanten Einsatzzeitraum berücksichtigt werden.
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit

	Verfügbarkeit	● ●
	Integrität	● ●

APP.4.3.A12:	**Einheitlicher Konfigurationsstandard von Datenbankmanagementsystemen**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A12 Einheitlicher Konfigurationsstandard von Datenbankmanagementsystemen" umgesetzt?	
Beschreibung:	Für alle eingesetzten Datenbankmanagementsysteme SOLLTE ein einheitlicher Konfigurationsstandard definiert werden. Alle Datenbankmanagementsysteme SOLLTEN nach diesem Standard konfiguriert und einheitlich betrieben werden. Falls es bei einer Installation notwendig ist, vom Konfigurationsstandard abzuweichen, SOLLTEN alle Schritte vom ISB freigegeben und nachvollziehbar dokumentiert werden. Der Konfigurationsstandard SOLLTE regelmäßig überprüft und, falls erforderlich, angepasst werden.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit	● ●
	Verfügbarkeit	● ●
	Integrität	● ●

APP.4.3.A13:	**Restriktive Handhabung von Datenbank-Links**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A13 Restriktive Handhabung von Datenbank-Links" umgesetzt?	
Beschreibung:	Es SOLLTE sichergestellt sein, dass nur Verantwortliche dazu berechtigt sind, Datenbank-Links (DB-Links) anzulegen. Werden solche Links angelegt, MÜSSEN so genannte Private DB-Links vor Public DB-Links bevorzugt angelegt werden. Alle von den Verantwortlichen angelegten DB-Links SOLLTEN dokumentiert und regelmäßig überprüft werden. Zudem SOLLTEN DB-Links mitberücksichtigt werden, wenn das Datenbanksystem gesichert wird (siehe APP.4.3.A9 *Datensicherung eines Datenbanksystems*).	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit	● ● ● ●
	Verfügbarkeit	● ● ● ●
	Integrität	● ● ● ●

APP.4.3.A14:	**Überprüfung der Datensicherung eines Datenbanksystems**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A14 Überprüfung der Datensicherung eines Datenbanksystems" umgesetzt?	
Beschreibung:	Die vorgenommenen Datensicherungen SOLLTEN regelmäßig daraufhin überprüft werden, ob die Integrität der Sicherungsdateien noch gewährleistet ist. Die verantwortlichen Mitarbeiter SOLLTEN zudem regelmäßig üben, wie sich Datenbanken im Notfall schnell wiederherstellen lassen.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit	● ●
	Verfügbarkeit	● ●
	Integrität	● ●

APP.4.3.A15:	**Schulung der Datenbankadministratoren**	**Teilfrage**

Frage:	Wurde die Thematik "APP.4.3.A15 Schulung der Datenbankadministratoren" umgesetzt?
Beschreibung:	Es SOLLTE gewährleistet sein, dass nur ausreichend geschulte Mitarbeiter das Datenbankmanagementsystem administrieren. Es SOLLTE ein Schulungsplan erstellt werden, mit dem sichergestellt wird, dass Datenbankverantwortliche rechtzeitig zu Themen der Informationssicherheit (siehe ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*) und Performance sowie zu den Funktionen neuer Versionen des Datenbankmanagementsystems geschult werden.
Antwort:	**Teilweise**
Begründung:	learning by doing / Key User Schulungen
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

APP.4.3.A16:	**Verschlüsselung der Datenbankanbindung**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A16 Verschlüsselung der Datenbankanbindung" umgesetzt?	
Beschreibung:	Das Datenbankmanagementsystem SOLLTE so konfiguriert werden, dass Datenbankverbindungen immer verschlüsselt werden. Die dazu eingesetzten kryptografischen Verfahren und Protokolle SOLLTEN den internen Vorgaben der Institution entsprechen (siehe CON.1 *Kryptokonzept*).	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

APP.4.3.A17:	**Datenübernahme oder Migration**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A17 Datenübernahme oder Migration" umgesetzt?	
Beschreibung:	Falls initial oder regelmäßig Daten in eine Datenbank übernommen werden, SOLLTE vorab definiert werden, wie diese Datenübernahme erfolgen soll. Nachdem Daten übernommen wurden, SOLLTE geprüft werden, ob sie vollständig und unverändert sind.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

APP.4.3.A18:	**Überwachung des Datenbankmanagementsystems**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A18 Überwachung des Datenbankmanagementsystems" umgesetzt?	
Beschreibung:	Es SOLLTEN Parameter, Ereignisse und Betriebszustände des Datenbankmanagementsystems definiert werden, die für den sicheren Betrieb kritisch sind. Diese SOLLTEN mithilfe eines Monitoring-Systems überwacht werden. Für alle kritischen Parameter und Ereignisse SOLLTEN Schwellwerte festgelegt werden. Wenn diese Werte überschritten werden, MUSS geeignet reagiert werden (z. B. müssen die zuständigen Mitarbeiter alarmiert werden). Anwendungsspezifische Parameter, Ereignisse und deren Schwellwerte SOLLTEN mit den Verantwortlichen für die Fachanwendungen abgestimmt werden (siehe auch APP.4.3.A11 *Ausreichende Dimensionierung der Hardware*).	
Antwort:	Ja	

Schutzziel(e):	Vertraulichkeit	
	Verfügbarkeit	
	Integrität	

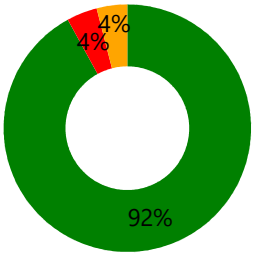
APP.4.3.A19:	**Schutz vor schädlichen Datenbank-Skripten**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A19 Schutz vor schädlichen Datenbank-Skripten" umgesetzt?	
Beschreibung:	Werden Datenbank-Skripte entwickelt, SOLLTEN hierfür verpflichtende Qualitätskriterien definiert werden (siehe CON.8 *Softwareentwicklung*). Datenbank-Skripte SOLLTEN auf gesonderten Testsystemen ausführlichen Funktionstests unterzogen werden, bevor sie produktiv eingesetzt werden. Die Ergebnisse SOLLTEN dokumentiert werden.	
Antwort:	**Teilweise**	
Schutzziel(e):	Vertraulichkeit	
	Verfügbarkeit	
	Integrität	

APP.4.3.A20:	**Regelmäßige Audits**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A20 Regelmäßige Audits" umgesetzt?	
Beschreibung:	Bei allen Komponenten des Datenbanksystems SOLLTE regelmäßig überprüft werden, ob alle festgelegten Sicherheitsmaßnahmen umgesetzt und diese korrekt konfiguriert sind. Dabei SOLLTE geprüft werden, ob der dokumentierte Stand dem Ist-Zustand entspricht, ob die Konfiguration des Datenbankmanagementsystems der dokumentierten Standardkonfiguration entspricht, ob alle Datenbank-Skripte benötigt werden und ob sie dem Qualitätsstandard der Institution genügen. Zusätzlich SOLLTEN die Protokolldateien des Datenbanksystems und des Betriebssystems nach Auffälligkeiten untersucht werden (siehe DER.1 *Detektion von sicherheitsrelevanten Ereignissen*). Die Auditergebnisse SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.	
Antwort:	**Nein**	
Schutzziel(e):	Vertraulichkeit	
	Verfügbarkeit	
	Integrität	

APP.4.3_SBA:	**Anforderungen bei erhöhtem Schutzbedarf**	**Strukturfrage**
Frage:	Sollen weitere Anforderungen bei erhöhtem Schutzbedarf für den Baustein "APP.4.3 Relationale Datenbanksysteme" überprüft werden?	
Beschreibung:	Die folgenden Anforderungen sollten für diese Thematik erfüllt sein um bei erhöhten Sicherheitsanforderungen ein ausreichendes Sicherheitsausmaß gewährleisten zu können.	
Antwort:	Nein	

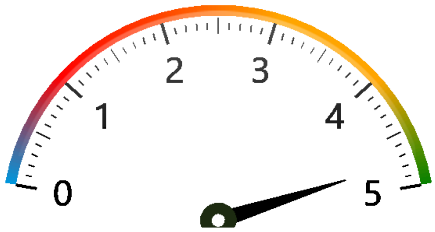
Oracle Datenbanksysteme (ORACLE_DB)

Verantwortlich(e):	Daniel Mustermann
Wissensdatenbank:	© IT-Grundschutz-Kompendium - Edition 2019, Version: 15
Zuletzt geändert:	04.04.2020



Antworten:
- Ja (23/25)
- Nein (1/25)
- Teilweise (1/25)

Durchschnittlicher Reifegrad



Prüffrage(n):

APP.4.3.A1:	**Erstellung einer Sicherheitsrichtlinie für Datenbanksysteme**
Frage:	Wurde die Thematik "APP.4.3.A1 Erstellung einer Sicherheitsrichtlinie für Datenbanksysteme" umgesetzt?
Beschreibung:	Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für Datenbanksysteme erstellt werden, in der nachvollziehbar Anforderungen und Vorgaben beschrieben sind, wie Datenbanksysteme sicher betrieben werden können. Die Richtlinie MUSS allen im Bereich Datenbanksysteme verantwortlichen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit dem ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse MÜSSEN sinnvoll dokumentiert werden.
Antwort:	**Nein**
Begründung:	fehlt derzeit
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität
Zugeteilte Gefährdungslage:	**Gefährdungslage Oracle Datenbanksysteme (ORACLE_DB)**

APP.4.3.A2:	**Installation des Datenbankmanagementsystems**
Frage:	Wurde die Thematik "APP.4.3.A2 Installation des Datenbankmanagementsystems" umgesetzt?
Beschreibung:	Es MUSS sichergestellt sein, dass die Installationspakete des Datenbankmanagementsystems aus sicheren Quellen stammen. Bereits veröffentlichte Patches MÜSSEN eingespielt werden, bevor das DBMS betrieben wird.
Antwort:	**Teilweise**
Begründung:	es gibt dazu kein niedergeschriebenes Vorgehen, auch wenn es idR so erfolgt

Schutzziel(e):	Vertraulichkeit	● ● ● ●
	Verfügbarkeit	● ● ● ●
	Integrität	● ● ● ●

Zugeteilte Gefährdungslage:	**Gefährdungslage Oracle Datenbanksysteme (ORACLE_DB)**

APP.4.3.A3:	**Basishärtung des Datenbankmanagementsystems**
Frage:	Wurde die Thematik "APP.4.3.A3 Basishärtung des Datenbankmanagementsystems" umgesetzt?
Beschreibung:	Das Datenbankmanagementsystem MUSS gehärtet werden. Hierfür MUSS eine Checkliste mit den durchzuführenden Schritten zusammengestellt und abgearbeitet werden. Auch MÜSSEN alle Passwörter entsprechend den internen Anforderungen der Institution geändert werden. Alle Passwörter MÜSSEN verschlüsselt gespeichert werden. Die Basishärtung MUSS regelmäßig überprüft und falls erforderlich angepasst werden.
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit ● ● ● ● Verfügbarkeit ● ● ● ● Integrität ● ● ● ●

APP.4.3.A4:	**Geregeltes Anlegen neuer Datenbanken**
Frage:	Wurde die Thematik "APP.4.3.A4 Geregeltes Anlegen neuer Datenbanken" umgesetzt?
Beschreibung:	Neue Datenbanken MÜSSEN nach einem definierten Prozess angelegt werden. Wenn eine neue Datenbank angelegt wird, MÜSSEN Grundinformationen zur Datenbank nachvollziehbar dokumentiert werden.
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit ● ● ● ● Verfügbarkeit ● ● ● ● Integrität ● ● ● ●

APP.4.3.A5:	**Benutzer- und Berechtigungskonzept**
Frage:	Wurde die Thematik "APP.4.3.A5 Benutzer- und Berechtigungskonzept" umgesetzt?
Beschreibung:	Das Benutzer- und Berechtigungskonzept (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*) der Institution MUSS um die für Datenbankmanagementsysteme notwendigen Berechtigungen für Rollen, Profile und Benutzergruppen erweitert werden. Es MUSS ein Prozess etabliert werden, der regelt, wie Datenbankbenutzer und deren Berechtigungen angelegt, genehmigt, eingerichtet, modifiziert und wieder entzogen bzw. gelöscht werden. Dabei DÜRFEN immer NUR so viele Zugriffsrechte vergeben werden, wie für die jeweiligen Aufgaben erforderlich sind (Need-to-know-Prinzip). Alle Änderungen SOLLTEN dokumentiert werden. Die eingerichteten Benutzer und die ihnen zugeordneten Berechtigungen MÜSSEN regelmäßig überprüft und, falls erforderlich, angepasst werden.
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit ● ● ● ● Verfügbarkeit ● ● ● ● Integrität ● ● ● ●

APP.4.3.A6:	**Passwortänderung**
Frage:	Wurde die Thematik "APP.4.3.A6 Passwortänderung" umgesetzt?
Beschreibung:	Alle Passwörter der Datenbankbenutzer MÜSSEN der Passwortrichtlinie der Institution entsprechen (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*). Es MUSS gewährleistet sein, dass die Passwörter beim geringsten Verdacht eines diesbezüglichen Sicherheitsvorfalles geändert werden. Insbesondere bei privilegierten Datenbankaccounts und Dienstkonten SOLLTE ein Passwortwechsel sorgfältig geplant und gegebenenfalls mit den Anwendungsverantwortlichen abgestimmt werden.
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

APP.4.3.A7:	**Zeitnahes Einspielen von Sicherheitsupdates**
Frage:	Wurde die Thematik "APP.4.3.A7 Zeitnahes Einspielen von Sicherheitsupdates" umgesetzt?
Beschreibung:	Vorhandene Sicherheitsupdates für das Datenbankmanagementsystem und das Betriebssystem MÜSSEN zeitnah installiert werden. Vorab MUSS auf einem Testsystem überprüft werden, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen. Bevor ein Patch eingespielt wird, MUSS das Datenbanksystem gesichert werden (siehe APP.4.3.A9 *Datensicherung eines Datenbanksystems*). Zusätzlich MUSS eine verantwortliche Rolle definiert werden, die dafür zuständig ist, sich regelmäßig über bekannte Sicherheitslücken des Datenbankmanagementsystems sowie über verfügbare Sicherheitsupdates zu informieren. Des Weiteren MUSS geprüft werden, ob die Update-Intervalle des Datenbankmanagementsystems auf die Update-Zyklen des Herstellers abgestimmt werden können. Das Ergebnis SOLLTE nachvollziehbar dokumentiert werden.
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

APP.4.3.A8:	**Datenbank-Protokollierung**
Frage:	Wurde die Thematik "APP.4.3.A8 Datenbank-Protokollierung" umgesetzt?
Beschreibung:	Sicherheitsrelevante Ereignisse des Datenbanksystems MÜSSEN mit einem eindeutigen Zeitstempel protokolliert werden. Dabei MÜSSEN sich Art und Umfang der Protokollierung am Schutzbedarf der zu verarbeitenden Informationen orientieren. Zusätzlich MUSS geprüft werden, ob die Protokollierung der Fachanwendungen zusammen mit der Protokollierung der Datenbank alle erforderlichen Informationen abdeckt, um betriebs- und sicherheitsrelevante Veränderungen an der Datenbankinfrastruktur und den Anwendungen zu erkennen. Es SOLLTE so protokolliert werden, dass die Protokolldateien nicht nachträglich veränderbar sind. Vertiefende Informationen sind in OPS.1.1.5 *Protokollierung* zu finden.
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

APP.4.3.A9:	**Datensicherung eines Datenbanksystems**
Frage:	Wurde die Thematik "APP.4.3.A9 Datensicherung eines Datenbanksystems" umgesetzt?
Beschreibung:	Es MÜSSEN regelmäßig Systemsicherungen des DBMS und der Daten durchgeführt werden. Auch bevor eine

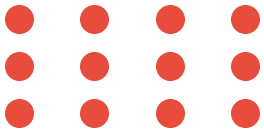
	Datenbank neu erzeugt wird, MUSS das Datenbanksystem gesichert werden. Hierfür SOLLTEN die dafür zulässigen Dienstprogramme benutzt werden. Alle Transaktionen SOLLTEN so gesichert werden, dass sie jederzeit wiederherstellbar sind. Sofern die Datensicherung die verfügbaren Kapazitäten übersteigt, SOLLTE ein erweitertes Konzept (z. B. inkrementelle Sicherung) erstellt werden, um die Datenbank zu sichern. Abhängig vom Schutzbedarf der Daten SOLLTEN die Wiederherstellungsparameter vorgegeben werden (siehe CON.3 *Datensicherungskonzept)*.
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

APP.4.3_STD:	**Standard-Anforderungen**	**Strukturfrage**
Frage:	Sollen weitere Anforderungen für den Baustein "APP.4.3 Relationale Datenbanksysteme" zur Absicherung des Stands der Technik überprüft werden?	
Beschreibung:	Die folgenden Standard-Anforderungen sollten für diese Thematik erfüllt sein um ein Sicherheitsmaß entsprechend Stand der Technik gewährleisten zu können.	
Antwort:	Ja	

APP.4.3.A10:	**Auswahl geeigneter Datenbankmanagementsysteme**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A10 Auswahl geeigneter Datenbankmanagementsysteme" umgesetzt?	
Beschreibung:	Bevor Datenbankmanagementsysteme beschafft werden, SOLLTEN Anforderungen an die DBMS definiert und in einem Anforderungskatalog dokumentiert werden. Danach SOLLTEN alle infrage kommenden Datenbankmanagementsysteme anhand des Katalogs bewertet werden. Die Ergebnisse SOLLTEN dokumentiert werden.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

APP.4.3.A11:	**Ausreichende Dimensionierung der Hardware**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A11 Ausreichende Dimensionierung der Hardware" umgesetzt?	
Beschreibung:	Datenbankmanagementsysteme SOLLTEN auf ausreichend dimensionierter Hardware installiert werden. Die Hardware SOLLTE über genügend Reserven verfügen, um auch eventuell steigenden Anforderungen gerecht zu werden. Zeichnen sich trotzdem während des Betriebs Ressourcenengpässe ab, SOLLTEN diese frühzeitig behoben werden. Wenn die Hardware dimensioniert wird, SOLLTE das erwartete Wachstum für den geplanten Einsatzzeitraum berücksichtigt werden.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

APP.4.3.A12:	**Einheitlicher Konfigurationsstandard von Datenbankmanagementsystemen**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A12 Einheitlicher Konfigurationsstandard von Datenbankmanagementsystemen" umgesetzt?	
Beschreibung:	Für alle eingesetzten Datenbankmanagementsysteme SOLLTE ein einheitlicher Konfigurationsstandard definiert werden. Alle Datenbankmanagementsysteme SOLLTEN nach diesem Standard konfiguriert und einheitlich betrieben werden. Falls es bei einer Installation notwendig ist, vom Konfigurationsstandard abzuweichen, SOLLTEN alle Schritte vom ISB freigegeben und nachvollziehbar dokumentiert werden. Der Konfigurationsstandard SOLLTE regelmäßig überprüft und, falls erforderlich, angepasst werden.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

APP.4.3.A13:	**Restriktive Handhabung von Datenbank-Links**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A13 Restriktive Handhabung von Datenbank-Links" umgesetzt?	
Beschreibung:	Es SOLLTE sichergestellt sein, dass nur Verantwortliche dazu berechtigt sind, Datenbank-Links (DB-Links) anzulegen. Werden solche Links angelegt, MÜSSEN so genannte Private DB-Links vor Public DB-Links bevorzugt angelegt werden. Alle von den Verantwortlichen angelegten DB-Links SOLLTEN dokumentiert und regelmäßig überprüft werden. Zudem SOLLTEN DB-Links mitberücksichtigt werden, wenn das Datenbanksystem gesichert wird (siehe APP.4.3.A9 *Datensicherung eines Datenbanksystems*).	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

APP.4.3.A14:	**Überprüfung der Datensicherung eines Datenbanksystems**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A14 Überprüfung der Datensicherung eines Datenbanksystems" umgesetzt?	
Beschreibung:	Die vorgenommenen Datensicherungen SOLLTEN regelmäßig daraufhin überprüft werden, ob die Integrität der Sicherungsdateien noch gewährleistet ist. Die verantwortlichen Mitarbeiter SOLLTEN zudem regelmäßig üben, wie sich Datenbanken im Notfall schnell wiederherstellen lassen.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

APP.4.3.A15:	**Schulung der Datenbankadministratoren**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A15 Schulung der Datenbankadministratoren" umgesetzt?	
Beschreibung:	Es SOLLTE gewährleistet sein, dass nur ausreichend geschulte Mitarbeiter das Datenbankmanagementsystem administrieren. Es SOLLTE ein Schulungsplan erstellt werden, mit dem sichergestellt wird, dass	

	Datenbankverantwortliche rechtzeitig zu Themen der Informationssicherheit (siehe ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*) und Performance sowie zu den Funktionen neuer Versionen des Datenbankmanagementsystems geschult werden.
Antwort:	Ja
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität

APP.4.3.A16:	**Verschlüsselung der Datenbankanbindung**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A16 Verschlüsselung der Datenbankanbindung" umgesetzt?	
Beschreibung:	Das Datenbankmanagementsystem SOLLTE so konfiguriert werden, dass Datenbankverbindungen immer verschlüsselt werden. Die dazu eingesetzten kryptografischen Verfahren und Protokolle SOLLTEN den internen Vorgaben der Institution entsprechen (siehe CON.1 *Kryptokonzept*).	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

APP.4.3.A17:	**Datenübernahme oder Migration**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A17 Datenübernahme oder Migration" umgesetzt?	
Beschreibung:	Falls initial oder regelmäßig Daten in eine Datenbank übernommen werden, SOLLTE vorab definiert werden, wie diese Datenübernahme erfolgen soll. Nachdem Daten übernommen wurden, SOLLTE geprüft werden, ob sie vollständig und unverändert sind.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

APP.4.3.A18:	**Überwachung des Datenbankmanagementsystems**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A18 Überwachung des Datenbankmanagementsystems" umgesetzt?	
Beschreibung:	Es SOLLTEN Parameter, Ereignisse und Betriebszustände des Datenbankmanagementsystems definiert werden, die für den sicheren Betrieb kritisch sind. Diese SOLLTEN mithilfe eines Monitoring-Systems überwacht werden. Für alle kritischen Parameter und Ereignisse SOLLTEN Schwellwerte festgelegt werden. Wenn diese Werte überschritten werden, MUSS geeignet reagiert werden (z. B. müssen die zuständigen Mitarbeiter alarmiert werden). Anwendungsspezifische Parameter, Ereignisse und deren Schwellwerte SOLLTEN mit den Verantwortlichen für die Fachanwendungen abgestimmt werden (siehe auch APP.4.3.A11 *Ausreichende Dimensionierung der Hardware*).	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

APP.4.3.A19:	**Schutz vor schädlichen Datenbank-Skripten**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A19 Schutz vor schädlichen Datenbank-Skripten" umgesetzt?	
Beschreibung:	Werden Datenbank-Skripte entwickelt, SOLLTEN hierfür verpflichtende Qualitätskriterien definiert werden (siehe CON.8 *Softwareentwicklung*). Datenbank-Skripte SOLLTEN auf gesonderten Testsystemen ausführlichen Funktionstests unterzogen werden, bevor sie produktiv eingesetzt werden. Die Ergebnisse SOLLTEN dokumentiert werden.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

APP.4.3.A20:	**Regelmäßige Audits**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A20 Regelmäßige Audits" umgesetzt?	
Beschreibung:	Bei allen Komponenten des Datenbanksystems SOLLTE regelmäßig überprüft werden, ob alle festgelegten Sicherheitsmaßnahmen umgesetzt und diese korrekt konfiguriert sind. Dabei SOLLTE geprüft werden, ob der dokumentierte Stand dem Ist-Zustand entspricht, ob die Konfiguration des Datenbankmanagementsystems der dokumentierten Standardkonfiguration entspricht, ob alle Datenbank-Skripte benötigt werden und ob sie dem Qualitätsstandard der Institution genügen. Zusätzlich SOLLTEN die Protokolldateien des Datenbanksystems und des Betriebssystems nach Auffälligkeiten untersucht werden (siehe DER.1 *Detektion von sicherheitsrelevanten Ereignissen*). Die Auditergebnisse SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

APP.4.3_SBA:	**Anforderungen bei erhöhtem Schutzbedarf**	**Strukturfrage**
Frage:	Sollen weitere Anforderungen bei erhöhtem Schutzbedarf für den Baustein "APP.4.3 Relationale Datenbanksysteme" überprüft werden?	
Beschreibung:	Die folgenden Anforderungen sollten für diese Thematik erfüllt sein um bei erhöhten Sicherheitsanforderungen ein ausreichendes Sicherheitsausmaß gewährleisten zu können.	
Antwort:	Ja	

APP.4.3.A21:	**Einsatz von Datenbank Security Tools**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A21 Einsatz von Datenbank Security Tools" umgesetzt?	
Beschreibung:	Es SOLLTEN Informationssicherheitsprodukte für Datenbanken eingesetzt werden. Die eingesetzten Produkte SOLLTEN folgende Funktionen bereitstellen: • Erstellung einer Übersicht über alle Datenbanksysteme, • Erweiterte Konfigurationsmöglichkeiten und Rechtemanagement der Datenbank, • Erkennung und Unterbindung von möglichen Angriffen (z. B. Brute Force Angriffe auf ein Benutzerkonto, SQL-Injection) und • Auditfunktionen (z. B. Überprüfung von Konfigurationsvorgaben).	
Antwort:	Ja	

Schutzziel(e):	Vertraulichkeit Integrität

APP.4.3.A22:	**Notfallvorsorge**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A22 Notfallvorsorge" umgesetzt?	
Beschreibung:	Für das Datenbankmanagementsystem SOLLTE ein Notfallplan erstellt werden, der festlegt, wie ein Notbetrieb realisiert werden kann und welche Ressourcen dafür nötig sind (siehe DER.4 *Notfallmanagement*). Zusätzlich SOLLTE der Notfallplan definieren, wie aus dem Notbetrieb der Regelbetrieb wiederhergestellt werden kann. Der Notfallplan SOLLTE die nötigen Meldewege, Reaktionswege, Ressourcen und Reaktionszeiten der Fachverantwortlichen festlegen, durch die sich ein möglicher Notfall schnell eskalieren lässt. Auf Basis eines Wiederanlaufkoordinationsplanes SOLLTEN alle von der Datenbank abhängigen IT-Systeme vorab ermittelt und berücksichtigt werden.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

APP.4.3.A23:	**Archivierung**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A23 Archivierung" umgesetzt?	
Beschreibung:	Ist es erforderlich, Daten eines Datenbanksystems zu archivieren, SOLLTE ein entsprechendes Archivierungskonzept erstellt werden. Es SOLLTE sichergestellt sein, dass die Datenbestände zu einem späteren Zeitpunkt wieder vollständig und konsistent verfügbar sind. Im Archivierungskonzept SOLLTEN sowohl die Intervalle der Archivierung als auch die Vorhaltefristen der archivierten Daten festgelegt werden. Zusätzlich SOLLTE dokumentiert werden, mit welcher Technik die Datenbanken archiviert wurden. Mit den archivierten Daten SOLLTEN regelmäßig Wiederherstellungstests durchgeführt werden. Die Ergebnisse SOLLTEN dokumentiert werden.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

APP.4.3.A24:	**Datenverschlüsselung in der Datenbank**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A24 Datenverschlüsselung in der Datenbank" umgesetzt?	
Beschreibung:	Die Daten in den Datenbanken SOLLTEN verschlüsselt werden. Dabei SOLLTEN vorher unter anderem folgende Faktoren betrachtet werden: • Einfluss auf die Performance, • Schlüsselverwaltungsprozesse und -verfahren, einschließlich separater Schlüsselaufbewahrung und -sicherung, • Einfluss auf Backup-Recovery-Konzepte, • funktionale Auswirkungen auf die Datenbank, beispielsweise Sortiermöglichkeiten.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit	

APP.4.3.A25:	**Sicherheitsüberprüfungen von Datenbanksystemen**	**Teilfrage**
Frage:	Wurde die Thematik "APP.4.3.A25 Sicherheitsüberprüfungen von Datenbanksystemen" umgesetzt?	
Beschreibung:	Datenbanksysteme SOLLTEN regelmäßig mithilfe von Sicherheitsüberprüfungen überprüft werden. Bei den Sicherheitsüberprüfungen SOLLTEN die systemischen und herstellerspezifischen Aspekte der eingesetzten Datenbank-Infrastruktur (z. B. Verzeichnisdienste) sowie des eingesetzten Datenbankmanagementsystems betrachtet werden.	
Antwort:	Ja	
Schutzziel(e):	Vertraulichkeit Verfügbarkeit Integrität	

Anhang

Im Folgenden wird erläutert welche Arten von Fragen und Antworttypen in den Überprüfungen verwendet werden können und welche Bedeutung diese haben:

Reifegradfragen

Die Reifegradbewertung orientiert sich am Capability Maturity Model Integration (CMMI) Reifegradmodell der ISACA. Der Reifegrad beschreibt ein Entwicklungsniveau eines Prozesses. Die Reifegrade sind:

Reifegrad 1: initial
Diesen Reifegrad hat jedes Prozessgebiet automatisch.

Reifegrad 2: gemanaged
Die Projekte in diesem Prozessgebiet werden geführt. Ähnliche Projekte können dadurch erfolgreich wiederholt werden.

Reifegrad 3: definiert
Die Projekte in diesem Prozessgebiet werden nach einem angepassten Standardprozess durchgeführt und eine organisationsweite kontinuierliche Prozessverbesserung ist vorhanden.

Reifegrad 4: gemessen
Es wird eine statistische Prozesskontrolle durchgeführt.

Reifegrad 5: optimiert
Die Arbeit und die Arbeitsweise werden mit Hilfe der statistischen Prozesskontrolle verbessert.

Technikfragen

Die Bewertung von Technikfragen ist mit den Antwortmöglichkeiten „Ja“, „Nein“, „Teilweise“ möglich.

Weitere Antwortmöglichkeiten

Die Option "Entbehrlich" bedeutet, dass eine Frage im Kontext des Anwendungsbereichs nicht sinnvoll bzw. nicht relevant ist. „Nicht beantwortet“ bedeutet, dass die Frage im Zuge der Überprüfung nicht gestellt wurde.

Strukturfrage / Teilfrage

Die Beantwortung von Strukturfragen steuert die Anzeige bzw. Beantwortung von Teilfragen. Die Beantwortung der Teilfragen ist relevant für die Compliance Auswertungen.