Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

BSI Technische Richtlinie 03138 Ersetzendes Scannen

Bezeichnung:	Ersetzendes Scannen (RESISCAN)
	Anlage P – Prüfspezifikation
Kürzel:	BSI TR-03138-P
Version:	1.5
Datum:	21.11.2024

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: resiscan@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Anlage P – Prüfspezifikation (normativ)

P.1 Grundlegendes zur Konformitätsprüfung

Im Rahmen der Konformitätsprüfung für die vorliegende Richtlinie wird verifiziert, ob die in [BSI-TR03138] (Abschnitte 3, 4 und 5)[1] definierten Anforderungen vom betrachteten Scansystem erfüllt werden. Hierzu wird sowohl die Verfahrensdokumentation als auch das implementierte Scansystem mit den praktizierten Prozessen geprüft.

P.1.1 Konkretisierung des Prüfgegenstandes

Prüfgrundlage für Konformitätsprüfungen und Audits nach [BSI-TR03138] ist ausschließlich die BSI TR-03138 mit der zugehörigen Prüfspezifikation Anlage P. Ein TR-RESISCAN-Audit umfasst ausschließlich die Prüfung der Testfälle gemäß Anlage P (Basismodule + Aufbaumodule in Abhängigkeit des ermittelten Schutzbedarfs)[2]: Eine Zertifizierung gemäß [ISO/IEC 27001] nativ oder BSI-Grundschutz ist keine Voraussetzung oder Erfordernis für eine Zertifizierung nach [BSI-TR03138][3]: Auch die Anwendung der Vorgehensweise nach BSI-Grundschutz oder die Nutzung bzw. Umsetzung von BSI-Grundschutz oder anderer BSI-Standards ist keine Voraussetzung für eine Zertifizierung nach [BSI-TR03138].

P.1.2 Verweis auf Referenzdokumente

Um den Prozess der Prüfung und Zertifizierung effizient zu gestalten, SOLL der Antragsteller im Rahmen der Beantragung der Zertifizierung das Dokument „Nachweise für die Konformitätsprüfung gemäß BSI TR-03138 Ersetzendes Scannen“ ausgefüllt einreichen.

1 Abschnitt 5 ist optional zu berücksichtigen, wenn das mobile Scannen betrachtet werden soll im Rahmen der Zertifizierung

2 Alle übrigen formalen Verfahrensgrundlagen zur Zertifizierung nach Technischen Richtlinien (allgemein) - d.h. Verfahrensbeschreibung etc. - sind unter https://www.bsi.bund.de/zertifizierungtr veröffentlicht.

3 Disclaimer: Aus Gründen der Übersichtlichkeit und Lesbarkeit wird im Folgenden nur vom BSI-Grundschutz gesprochen. Alle diesbezüglichen Ausführungen gelten synonym auch für die Nutzung von ISO/IEC 27001 (inkl. ISO/IEC 27002 ff.) nativ oder BSI-Grundschutz.

P.2 Basismodul

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
01	15	3.1	-	**Strukturanalyse**				
				Die Strukturanalyse identifiziert die relevanten				
				a Datenobjekte	MUSS			
				b IT-Systeme und Anwendungen	MUSS			
				c Kommunikationsverbindungen (Netze)	MUSS			
				Netzplan liegt vor.	MUSS			
02	19	4.2.1.2	A.G.2	**Schutzbedarfsanalyse**				
				Der Schutzbedarf der weiteren Datenobjekte ergibt sich aus dem Schutzbedarf der Papieroriginale.				
				Der Schutzbedarf der Datenobjekte muss hinsichtlich der Schutzziele Integrität, Vertraulichkeit und Verfügbarkeit bestimmt werden.	MUSS			

P.2.1 Grundlegende Anforderungen

Nr	Seite	Kapitel	ID		Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
03	18	4.2.1.1	A.G.1		**Verfahrensdokumentation**				
					Die Verfahrensdokumentation muss die folgenden Aspekte umfassen:				
				a	Art der verarbeiteten Dokumente	MUSS			
					Regelungen für nicht verarbeitete Dokumente				
					Festlegung der Verantwortlichkeiten im Scanprozess				
					Festlegung der Abläufe im Scanprozess				
					Festlegung der Aufgaben im Scanprozess				
				b	Festlegung von Maßnahmen zur Qualifizierung und Sensibilisierung der Mitarbeiterinnen und Mitarbeiter	MUSS			
				c	Beschreibung der dem Schutzbedarf entsprechender Anforderungen an Räume, IT-Systeme, Anwendungen und Sicherungsmittel	MUSS			
				d	Regelungen für die Administration und Wartung der IT-Systeme und Anwendungen	MUSS			
				e	Festlegung von Sicherheitsanforderungen für IT-Systeme, Netze und Anwendungen	SOLLTE			
				f	Beschreibung der Umsetzung der Sicherheitsmaßnahmen entsprechend dem definierten Schutzbedarf anhand des tatsächlich implementierten Scanprozesses	MUSS			
				g	Verfahrensanweisung, für die am Scanprozess beteiligten Personen	MUSS			

P.2.2 Organisatorische Maßnahmen

Nr	Seite	Kapitel	ID		Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis
04	19	4.2.2.1	A.O.1		**Festlegung von Verantwortlichkeiten, Abläufen und Aufgaben im Scanprozess**			
					Verantwortlichkeiten, Abläufe und Aufgaben müssen festgelegt sein. Dies umfasst insbesondere:			
				a	Welche Schritte werden durch wen ausgeführt und wie ist dabei im Einzelnen vorzugehen?	MUSS		
				b	Welche Dokumente werden gescannt und welche Daten werden hierbei erzeugt?	MUSS		
				c	Welche Qualitätskontrollen werden durch wen in welchen Zeitabständen und nach welchen Kriterien durchgeführt?	MUSS		
				d	Welche Sicherungsdaten oder Sicherungssysteme sind für den Schutz der Integrität dieser Daten vorgesehen?	MUSS		
				e	Qualitätskontrollen müssen mindestens stichprobenartig erfolgen.	MUSS		
					Qualitätskontrollen sollten regelmäßig durch Mitarbeiterinnen und Mitarbeiter durchgeführt werden, die nicht mit der operativen Durchführung des zu kontrollierenden Arbeitsschritts betraut sind.	SOLLTE		
				f	Für die in den Scanprozess involvierten Datenobjekte sowie die genutzten IT-Systeme und Anwendungen sollten Verantwortliche benannt werden.	SOLLTE		
				g	Bei der Zuweisung des Personals zu den operativen Aufgaben im Scanprozess müssen potenzielle Interessenkonflikte berücksichtigt werden.	MUSS		

Nr	Seite	Kapitel	ID	Anforderung		M / S	Referenzen / Bemerkungen	Ergebnis
					Bei der Zuweisung des Personals zu den operativen Aufgaben im Scanprozess sollten potenzielle Interessenkonflikte nach Möglichkeit vermieden werden.	SOLLTE		
				h	Typische Fehlerquellen müssen berücksichtigt werden.	MUSS		
					Für typische Fehlerquellen sollten entsprechende Vorsichtsmaßnahmen festgelegt werden.	SOLLTE		
				i	Es muss festgelegt werden, unter welchen Umständen und ab welchem Zeitpunkt das Originaldokument vernichtet werden darf.	MUSS		
				j	Es muss ein Verfahren zur Klärung von „Zweifelsfragen“ etabliert werden.	MUSS		
05	20	4.2.2.2	A.O.2	**Regelungen für Wartungs- und Reparaturarbeiten**				
				Es sollten Regelungen für die Wartung und die Reparatur der eingesetzten IT-Systeme und Anwendungen getroffen werden. Dies umfasst insbesondere:				
				a	Festlegung der Verantwortlichkeit für die Beauftragung, Durchführung und Kontrolle von Wartungs- und Reparaturarbeiten	SOLLTE		
				b	Verfahren für die regelmäßige Bereitstellung und Anwendung von sicherheitsrelevanten Updates	SOLLTE		
				c	Regelung zur Authentisierung und zum Nachweis der Autorisierung des Wartungspersonals	SOLLTE		
				d	Regelungen zum Schutz personenbezogener oder anderweitig besonders schützenswerter Daten (z. B. Betriebsgeheimnisse) auf den zu wartenden IT-Systemen	SOLLTE		

Nr	Seite	Kapitel	ID	Anforderung		M / S	Referenzen / Bemerkungen	Ergebnis	
				e	Dokumentation von sicherheitsrelevanten Veränderungen an den involvierten IT-Systemen und Anwendungen	SOLLTE			
				f	Dokumentation der erfolgreichen Durchführung der Maßnahmen zur Qualitätskontrolle und Freigabe vor Wiederaufnahme des regulären Betriebs	SOLLTE			
06	20	4.2.2.3	A.O.3	**Abnahme- und Freigabe-Verfahren für Hardware und Software**					
				Es muss ein Verfahren für die Abnahme und Freigabe der eingesetzten Hard- und Software etabliert werden; dies umfasst Scanner, Scan-Workstation und Scan-Cache.		MUSS			
				Neben der initialen Inbetriebnahme ist dieses Abnahmeverfahren auch bei der Wiederaufnahme des Betriebs nach Wartungs- und Reparaturarbeiten durchzuführen.		MUSS			
07	21	4.2.2.4	A.O.4	**Aufrechterhaltung der Informationssicherheit**					
				In angemessenen zeitlichen Abständen muss eine Überprüfung der Wirksamkeit und Vollständigkeit der für die Informationssicherheit beim ersetzenden Scannen vorgesehenen Maßnahmen durchgeführt werden.		MUSS			
				In diesen Audits muss geprüft werden:					
				a	Ob Prozesse und Sicherheitsmaßnahmen korrekt implementiert wurden und wirksam sind.	MUSS			
				b	Ob die Sicherheitsmaßnahmen ausreichend vor den potenziellen Bedrohungen schützen oder ob zusätzliche oder korrigierte Sicherheitsmaßnahmen notwendig sind.	MUSS			
				Audits sollten von unabhängigen Personen durchgeführt werden.		SOLLTE			

Nr	Seite	Kapitel	ID		Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
					Die Ergebnisse der Audits sollten schriftlich dokumentiert werden.	SOLLTE			
					Aus identifizierten Sicherheitslücken oder Probleme müssen Korrekturmaßnahmen abgeleitet werden.	MUSS			
					Für die Umsetzung von Korrekturmaßnahmen muss ein Zeitplan mit Verantwortlichkeiten definiert werden.	MUSS			
					Die Umsetzung der Maßnahmen muss durch die Verantwortlichen verfolgt und überprüft werden.	MUSS			
08	21	4.2.2.5	A.O.5		**Anforderungen beim Outsourcing des Scanprozesses**				
					Wird der Scanprozess von spezialisierten Scandienstleistern durchgeführt, sind die Anforderungen der TR-RESISCAN umzusetzen.	MUSS			
					Darüber hinaus gelten folgende Anforderungen:				
				a	Organisatorische und technische Schnittstellen zwischen Auftraggebenden und Auftragnehmenden müssen in der Verfahrensdokumentation explizit dargestellt werden. (Übertragungswege, Datenablageorte, beteiligte Akteure, Rückfallverfahren, Maßnahmen zur Integritäts- und Vollständigkeitskontrolle etc.)	MUSS			
				b	Der Auftragnehmende muss zur Einhaltung der vom Auftraggebenden definierten Sicherheitsmaßnahmen verpflichtet werden.	MUSS			
				c	Es sollte eine Analyse der durch die Aufgabenteilung zusätzlich entstehenden Risiken erfolgen.	SOLLTE			
				d	Zusätzlich zur regelmäßigen Auditierung sollten unangemeldete Stichproben durchgeführt werden.	SOLLTE			

P.2.3 Personelle Maßnahmen

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis
				Verpflichtung der Mitarbeiter zur Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen und der Verfahrensanweisung			
09	22	4.2.3.1	A.P.1.	Die im Rahmen der Schutzbedarfsanalyse identifizierten rechtlichen Rahmenbedingungen sollten den Mitarbeiterinnen und Mitarbeitern zur Kenntnis gebracht werden.	SOLLTE		
				Mitarbeiterinnen und Mitarbeitern sollten zur Einhaltung der einschlägigen Gesetze, Vorschriften, Regelungen und der Verfahrensanweisung verpflichtet werden.	SOLLTE		
				Einweisung zur ordnungsgemäßen Bedienung des Scansystems			
				Mitarbeiterinnen und Mitarbeiter, die den Scanvorgang durchführen, müssen hinsichtlich der eingesetzten Geräte, Anwendungen und Abläufe geschult werden. Dies umfasst insbesondere:			
10	22	4.2.3.2	A.P.2	a Die grundsätzlichen Abläufe im Scanprozess einschließlich der Dokumentenvorbereitung, dem Scannen, der Indexierung, der zulässigen Nachbearbeitung, und der Integritätssicherung	MUSS		
				b Die Konfiguration und Nutzung des Scanners und der Scan-Workstation	MUSS		
				c Die Anforderungen hinsichtlich der Qualitätssicherung	MUSS		
				d Die Abläufe und Anforderungen beider Erstellung des Transfervermerks	MUSS		
				e Die Konfiguration und Nutzung der Systeme zur Integritätssicherung	MUSS		
				f Das Verhalten im Fehlerfall	MUSS		
11	22	4.2.3.3	A.P.3	**Schulung zu Sicherheitsmaßnahmen im Scanprozess**			

Nr	Seite	Kapitel	ID	Anforderung		M / S	Referenzen / Bemerkungen	Ergebnis
				Mitarbeiterinnen und Mitarbeiter, die den Scanprozess durchführen oder verantworten, müssen hinsichtlich der umzusetzenden sowie der implementierten Sicherheitsmaßnahmen geschult werden. Dies umfasst insbesondere:				
				a	Die grundsätzliche Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für Informationssicherheit	MUSS		
				b	Personenbezogene Sicherheitsmaßnahmen im Scanprozess	MUSS		
				c	Systembezogene Sicherheitsmaßnahmen im Scanprozess	MUSS		
				d	Verhalten beim Auftreten von Schadsoftware	MUSS		
				e	Bedeutung der Datensicherung und deren Durchführung	MUSS		
				f	Umgang mit personenbezogenen und anderen sensiblen Daten	MUSS		
				g	Einweisung in Notfallmaßnahmen	MUSS		
12	23	4.2.3.4	A.P.4	**Schulung des Wartungs- und Administrationspersonals**				
				Das Wartungs- und Administrationspersonal sollte soweit geschult werden, dass:				
				a	Alltägliche Administrationsaufgaben selbst durchgeführt werden können.	SOLLTE		
				b	Einfache Fehler selbst erkannt und behoben werden können.	SOLLTE		
				c	Datensicherungen regelmäßig selbsttätig durchgeführt werden können.	SOLLTE		
				d	Eingriffe von externem Wartungspersonal nachvollzogen werden können.	SOLLTE		
				e	Manipulationsversuche oder unbefugte Zugriffe auf die Systeme erkannt und zügig behoben werden können.	SOLLTE		

P.2.4 Technische Maßnahmen

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis
				Grundlegende Sicherheitsmaßnahmen für IT-Systeme im Scanprozess			
13	23	4.2.4.1	A.T.1	Basierend auf den Ergebnissen der Schutzbedarfs-/Strukturanalyse müssen für ALLE in den Scanprozess involvierten IT-Systeme (z.B. Client-, Server- und Netzwerkkomponenten) die relevanten Sicherheitsanforderungen (Bausteine) aus dem BSI Grundschutz-Kompendium [BSI-GSK] oder entsprechende äquivalente Maßnahmen auf Basis [ISO27001] [ISO27002] umgesetzt werden. Für die Prüfung nach BSI Grundschutz-Kompendium [BSI-GSK] sind vom Auditor hiervon fünf Bausteine Risiko-orientiert auszuwählen; in begründeten Fällen kann der Auditor den Prüfumfang auf zusätzliche Bausteine ausweiten. Der Prüfumfang ist vor dem Audit mit dem BSI abzustimmen. Eine bestehende Zertifizierung nach IT-Grundschutz oder [ISO/IEC 27001] nativ, deren Geltungsbereich den zu zertifizierenden Scanprozess abdeckt, kann die Bausteinprüfung ersetzen. Die Gültigkeit des jeweiligen Zertifikates muss hierbei mindestens noch 12 Monate betragen.[4]	MUSS		
14	23	4.2.4.2	A.T.2	**Festlegung der zulässigen Kommunikationsverbindungen**			

[4] Für den Abgleich des Geltungsbereiches ist dem Auditor Einsicht in die entsprechenden Auditberichte/ -ergebnisse zu gewähren. Fällt der zu zertifizierende Scanprozess nicht in den Geltungsbereich der bestehenden Zertifizierung, muss die Bausteinprüfung erfolgen.

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				Sofern die für das Scannen eingesetzten IT-Systeme über ein Netzwerk verbunden sind, müssen in diesem Netzwerk sowie auf den IT-Systemen selbst die zulässigen Kommunikationsverbindungen effektiv vor Zugriffen außerhalb des Netzwerks geschützt werden (Firewall). Bei der Festlegung der zulässigen Kommunikationsverbindungen müssen die jeweiligen Anforderungen der [TR-02102-1] bezogen auf das eingesetzte und in der Strukturanalyse beschriebene Scansystem beachtet werden. Dies kann durch eine zugehörige Erklärung der Organisation sichergestellt werden.	MUSS			
15	24	4.2.4.3	A.T.3	**Schutz vor Schadprogrammen**				
				Zum Schutz vor Schadprogrammen MÜSSEN für alle relevanten IT-Systeme folgende Maßnahmen umgesetzt werden:				
				a Auswahl eines geeigneten Viren-Schutzprogramms	MUSS			
				b Meldung von Schadprogramm-Infektionen	MUSS			
				c Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen	MUSS			
				d Regelmäßige Datensicherung.	MUSS			
16	24	4.2.4.4	A.T.4	**Zuverlässige Speicherung**				
				Die für die beweiswerterhaltende Aufbewahrung der Scanprodukte und Metadaten verwendeten Speichermedien, Verfahren (z. B. zur Datensicherung) und Konfigurationen müssen für die notwendige Aufbewahrungsdauer bzw. bis zur zuverlässigen Übergabe an einen geeigneten Langzeitspeicher eine Verfügbarkeit gewährleisten, die dem Schutzbedarf der Datenobjekte angemessen ist.	MUSS			

P.2.5 Sicherheitsmaßnahmen bei der Dokumentenvorbereitung

Nr	Seite	Kapitel	ID	Anforderung		M / S	Referenzen / Bemerkungen	Ergebnis
17	24	4.2.5.1	A.DV.1	**Sorgfältige Vorbereitung der Papierdokumente**				
				Um eine zuverlässige und sorgfältige Erfassung zu gewährleisten, müssen Papierdokumente sorgfältig auf das Scannen vorbereitet werden. Dies umfasst folgende Aspekte:				
				a	Sorgfältige Brieföffnung (bei Bedarf das Aufbringen von Posteingangsnachweisen, z.B. Durch QR-Code auf Trennblättern etc.)	SOLLTE		
					Prüfung, ob das Dokument offensichtlich manipuliert wurde oder es sich um eine Kopie handelt.	SOLLTE		
					Zuordnung zu einer bestimmten Dokumentenklasse, um die entsprechende Vorsortierung zu ermöglichen.	SOLLTE		
					Prüfung, ob die Dokumente grundsätzlich für die Erfassung vorgesehen sind.	MUSS		
				b	Prüfung, dass die zu scannenden Dokumente geeignet sind, mit den beim Scannen verwendeten Geräten, Verfahren und Einstellungen fehlerfrei verarbeitet werden zu können.	SOLLTE		
				c	Maßnahmen für die Bewahrung des logischen Kontextes der zu erfassenden Dokumente	SOLLTE		
					Bewahrung der Zugehörigkeit der eingescannten Seiten zu einem Dokument	SOLLTE		

Nr	Seite	Kapitel	ID	Anforderung		M / S	Referenzen / Bemerkungen	Ergebnis	
				d	Die korrekte Orientierung der erfassten Blätter muss erhalten bleiben (Drehung, leere Rückseite) Ist dies nicht möglich, muss beidseitig erfasst werden.	MUSS			
				e	Bewahrung der korrekten Reihenfolge von Blättern bei mehrseitigen Dokumenten	SOLLTE			
				f	Zuverlässige Trennung von unabhängigen Dokumenten	SOLLTE			
				g	Entfernen von Klammern, Knicken und nicht relevanten Klebezetteln	SOLLTE			
					Sofern der Inhalt eines Klebezettels relevant ist, muss dieser in geeigneter Weise gescannt werden.	MUSS			
				h	Sofern im Rahmen des Scanprozesses ein Umkopieren notwendig ist, ist darauf zu achten, dass die Kopie alle relevanten Informationen enthält.	MUSS			
18	25	4.2.5.2	A.DV.2	**Vorbereitung der Vollständigkeitsprüfung**					
				Bei automatisierter Erfassung müssen geeignete Maßnahmen für die Sicherstellung der Vollständigkeit getroffen werden.		MUSS			
				Damit eine Vollständigkeitsprüfung im Rahmen der Nachbereitung durchgeführt werden kann, sollten entsprechende Vorbereitungen getroffen werden (bei Bedarf).		SOLLTE			

P.2.6 Sicherheitsmaßnahmen beim Scannen

Nr	Seite	Kapitel	ID	Anforderung		M / S	Referenzen / Bemerkungen	Ergebnis
19	26	4.2.6.1	A.SC.1	**Auswahl und Beschaffung geeigneter Scanner**				
				Bei der Auswahl und Beschaffung geeigneter Scanner sollten folgende Kriterien auf ihre Relevanz geprüft und berücksichtigt werden:				
				a	Ausreichender Durchsatz	SOLLTE		
				b	Unterstützung geeigneter Datenformate	SOLLTE		
				c	Unterstützung von Patch- und/oder Barcodes zur Dokumententrennung und Übergabe von Meta-Informationen	SOLLTE		
				d	Ausreichende Qualität der Scanprodukte	SOLLTE		
				e	Ausreichende Flexibilität der Konfiguration	SOLLTE		
				f	Zuverlässiger und leistungsfähiger automatischer Seiteneinzug	SOLLTE		
				g	Möglichkeit zum Scannen gebundener Dokumente, Überlängen, zum Scannen von Farbe oder von Durchlichtdokumenten (bei Bedarf)	SOLLTE		
				h	Geeignete Schnittstellen für die Übermittlung des Scanprodukts in DMS/VBS/Archive/Fachanwendungen	SOLLTE		
				i	Möglichkeit der Absicherung der Administrationsschnittstelle	SOLLTE		
				j	Nutzung eines internen Datenspeichers	SOLLTE		
				k	Möglichkeit zum sicheren Löschen oder verschlüsselter Speicherung von Scanprodukten auf dem internen Datenspeicher	SOLLTE		

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				l Ausreichender Support	SOLLTE			
20	27	4.2.6.2	A.SC.2	**Zugangs- und Zugriffskontrollen für Scanner**				
				Es muss sichergestellt werden, dass Personen, die keinen Zugriff auf Originale, Scanprodukte und Scansystem haben dürfen, keinen unbeaufsichtigten Zugang zum Scansystem erhalten.	MUSS			
				Es müssen geeignete Zugangskontrollen und Besucherregelungen vorgesehen werden.	MUSS			
				Um einen hohen Schutz gegen Manipulationen des Scannen bzw. der Konfigurationen, der Dokumente beim Scannen, oder gegen das nachträgliche Auslesen von Scanprodukten vom internen Datenträger des Scanners zu erreichen, muss der Zugang zum Scanner generell auf ein Minimum beschränkt werden.	MUSS			
				Die Administration des Scanners bzw. die Konfiguration der Kommunikationsschnittstellen bei netzwerkfähigen Scannern muss durch ein geeignetes Authentisierungsverfahren geschützt werden.	MUSS			
				Der Zugriff auf die Administrationsschnittstelle muss durch eine geeignete Netzwerk-Konfiguration auf die notwendigen Systeme eingeschränkt werden.	MUSS			
21	27	4.2.6.3	A.SC.3	**Änderung voreingestellte Passwörter**				
				Voreingestellte Passwörter müssen nach der Installation des Scanners/Scansystems geändert werden.	MUSS			
				Basis für die Passwortvergabe sollten explizit formulierte interne Sicherheitsrichtlinien unter Berücksichtigung der Empfehlungen aus dem [BSI-GSK] in seiner aktuellsten Fassung sein.	SOLLTE			

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis
22	27	4.2.6.4	A.SC.4	**Sorgfältige Durchführung von Konfigurationsänderungen**			
				Bei der Durchführung von Konfigurationsänderungen muss sorgfältig vorgegangen werden.	MUSS		
				Die alte Konfiguration sollte zuvor gesichert werden.	SOLLTE		
				Änderungen sollten von einem Kollegen überprüft werden, bevor diese in den Echtbetrieb übernommen werden.	SOLLTE		
23	27	4.2.6.5	A.SC.5	**Geeignete Benutzung des Scanners**			
				Der eingesetzte Scanner muss gemäß den Vorgaben des Herstellers gepflegt werden.	MUSS		
				Die Dokumente müssen entsprechend den Vorgaben der Produkthandbücher und gemäß der physikalischen Struktur de Dokumente dem Scanner übergeben werden.	MUSS		
				Für Dokumente, die nicht für den automatischen Einzug geeignet sind, müssen in der Verfahrensdokumentation geeignete Verfahren beschrieben werden.	MUSS		
24	27	4.2.6.6	A.SC.6	**Geeignete Scan-Einstellungen**			
				Die Scan-Einstellungen müssen für die jeweiligen Dokumente geeignet gewählt werden.	MUSS		
				Für die Dokumententypen sollten geeignete Profile definiert, getestet und freigegeben werden.	SOLLTE		
				Spätestens beim Scannen sollte geprüft werden, dass geeignete Scan-Einstellungen genutzt werden.	SOLLTE		

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis
25	28	4.2.6.7	A.SC.7	**Geeignete Erfassung von Metainformationen**			
				Index- und Metadaten sollten in geeigneter Weise übergeben werden.	SOLLTE		
				Hierbei sollte eine zuverlässige Konfiguration der Applikation bzgl. der Erkennung und Gültigkeit der ausgelesenen Werte sowie eine sorgfältige manuelle Qualitätssicherung und Nachbearbeitung erfolgen.	SOLLTE		
26	28	4.2.6.8	A.SC.8	**Qualitätssicherung der Scanprodukte**			
				Zur Erkennung mangelhafter Scanvorgänge muss eine geeignete Qualitätskontrolle erfolgen.	MUSS		
				Die Ausgestaltung der Qualitätssicherung sollte sich am Scan-Durchsatz und dem Schutzbedarf der verarbeiteten Dokumente orientieren.	SOLLTE		
				Die Größe der Stichprobe muss abhängig vom Schutzbedarf der Dokumente und der Zuverlässigkeit des Scansystems bestimmt werden.	MUSS		
				Bei automatisierten Qualitätskontrollen sollte eine manuelle Prüfung der automatisch identifizierten Probleme erfolgen.	SOLLTE		
				Die Vernichtung der Originaldokumente darf nicht vor Abschluss der Qualitätskontrolle erfolgen.	MUSS		
27	28	4.2.6.9	A.SC.9	**Sichere Außerbetriebnahme von Scannern**			
				Bei Außerbetriebnahme müssen alle sicherheitsrelevanten Informationen von den Geräten gelöscht werden.	MUSS		
				Authentisierungsinformationen und gespeicherte Informationen im Scan-Cache müssen gelöscht werden.	MUSS		

Nr	Seite	Kapitel	ID		Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
					Spezifische Konfigurationsinformationen, die Rückschlüsse auf die Netzwerkstrukturen liefern können, sollten gelöscht werden.	SOLLTE			
28	29	4.2.6.10	A.SC.10		**Informationsschutz und Zugriffsbeschränkung bei netzwerkfähigen Scannern**				
					Bei Scannern, die über ein Netzwerk angesprochen werden, sollten geeignete Maßnahmen zur Zugriffsbeschränkung und für den Schutz der über das Netzwerk übertragenen Informationen vorgesehen werden.	SOLLTE			
					Werden Netzlaufwerke für die Ablage von Zwischenergebnissen oder Scanprodukten genutzt, muss der Zugriff auf diese Netzlaufwerke auf das notwendige Minimum eingeschränkt werden.	MUSS			
					Bei Multifunktionsgeräten, die Scan2Mail oder Scan2Fax unterstützen, muss der Versand an ungewünschte Empfängerkreise verhindert werden.	MUSS			
29	29	4.2.6.11	A.SC.11		**Protokollierung beim Scannen**				
					Für die Sicherstellung der Nachvollziehbarkeit des Scanprozesses soll eine geeignete und in der Verfahrensanweisung näher geregelte Protokollierung erfolgen. Dies sollte insbesondere folgende Punkte umfassen:				
				a	Änderung von kritischen Konfigurationsparametern sowie Authentisierungs- und Berechtigungsfunktionen	SOLLTE			
				b	Informationen, wer das Scansystem wann und in welcher Weise genutzt hat.	SOLLTE			
				c	Informationen, ob eine manuelle Nachbearbeitung des Scanprodukts stattgefunden hat.	SOLLTE			
				d	Fehlgeschlagene Authentisierungsvorgänge und sonstige aufgetretene Fehler	SOLLTE			

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				Protokolldaten müssen gemäß den geltenden datenschutzrechtlichen Bestimmungen verarbeitet und vor unautorisiertem Zugriff geschützt werden.	MUSS			
30	29	4.2.6.12	A.SC.12	**Auswahl geeigneter Bildkompressionsverfahren**				
				Es muss auf die Auswahl geeigneter Bildkompressionsverfahren geachtet werden.	MUSS			
				Verfahren, die zur Bildkompression - das sog. „Symbol Coding“ verwenden, dürfen nicht eingesetzt werden.	DARF NICHT			

P.2.7 Sicherheitsmaßnahmen bei der Nachbearbeitung

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis
31	30	4.2.7.1	A.NB.1	**Geeignete und nachvollziehbare Nachbearbeitung**			
				Die Nachbearbeitung des Scanproduktes (z. B. Veränderung des Kontrastes/Helligkeit, Farbreduktion, Beschneiden, Rauschunterdrückung) darf nicht erfolgen, außer sie zielt auf die Erhöhung der Lesbarkeit ab.	MUSS		
				Die Nachbearbeitung muss sorgfältig durchgeführt werden, damit keine potenziell relevanten Informationen zerstört werden.	MUSS		
				Es muss ausgeschlossen werden (z. B. Protokollierung), dass Inhalte unbemerkt verfälscht werden können.	MUSS		
				Welche Form der Nachbearbeitung in welchen Fällen zulässig ist, sollte in der Verfahrensanweisung geregelt werden.	SOLLTE		
32	30	4.2.7.2	A.NB.2	**Qualitätssicherung der nachbearbeiteten Scanprodukte**			
				Sofern eine Nachbearbeitung erfolgt, muss für die durchgeführten Operationen eine Qualitätssicherung erfolgen.	MUSS		
				Die ursprünglichen Scanprodukte dürfen nicht vor Abschluss der Qualitätssicherung gelöscht werden.	MUSS		
33	30	4.2.7.3	A.NB.3	**Durchführung der Vollständigkeitsprüfung**			

Nr	Seite	Kapitel	ID		Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
					In einem automatisierten Prozess müssen geeignete Maßnahmen zur Sicherstellung der Vollständigkeit getroffen werden. Im Rahmen des Audits werden die getroffenen Maßnahmen zur Vollständigkeits-prüfung erfasst und vom Auditor hinsichtlich der Eignung bewertet. Die Vollständigkeitsprüfung muss die bildliche und inhaltliche Übereinstimmung von Originaldokument und Scanprodukt auf geeignete Weise prüfen und im Transfervermerk dokumentieren. Hierzu muss die Sachbearbeitung die Ergebnisse der Vollständigkeitsprüfung an die Scanstelle weitergeben.	MUSS			
					Die Größe der Stichprobe sollte abhängig vom Schutzbedarf der gescannten Dokumente, der Zuverlässigkeit des Scansystems und den Ergebnissen vorhergehender Stichproben bestimmt werden.	SOLLTE			
34	30	4.2.7.4	A.NB.4		**Transfervermerk**				
					Für jedes Scanprodukt muss ein Transfervermerk erstellt werden.	MUSS			
					Der Transfervermerk soll insbesondere folgende Aspekte dokumentieren				
				a	Ersteller des Scanprodukts	MUSS			
				a	Die ausschließliche Angabe der Organisation darf nicht erfolgen	DARF NICHT			
				b	Technisches und organisatorisches Umfeld des Erfassungsvorgangs	MUSS			
				c	Etwaige Auffälligkeiten während des Scanprozesses	MUSS			

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				d Zeitpunkt der Erfassung	MUSS			
				e Ergebnis der Qualitätssicherung	MUSS			
				f Die Tatsache, dass es sich um ein Scanprodukt handelt, das bildlich und inhaltlich mit dem Papierdokument übereinstimmt.	MUSS			
				Der Transfervermerk muss mit dem Scanprodukt logisch verknüpft oder in das Scanprodukt integriert werden.	MUSS			
				Die Integrität des Transfervermerks muss entsprechend dem Schutzbedarf der verarbeiteten Dokumente geschützt werden.	MUSS			
				Besteht der Transfervermerk ganz oder teilweise aus entsprechenden Protokollinformationen, muss die Integrität derselben entsprechend geschützt werden.	MUSS			

P.2.8 Sicherheitsmaßnahmen bei der Integritätssicherung

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				Nutzung geeigneter Dienste und Systeme für den Integritätsschutz				
35	31	4.2.8.1	A.IS.1	Um eine unerkannte nachträgliche Manipulation der während des Scanprozesses entstehenden Datenobjekte (Scanprodukt, Transfervermerk, Index- und Metadaten, Protokolldaten, ...) zu verhindern, müssen geeignete Mechanismen zum Schutz deren Integrität eingesetzt werden.	MUSS			
				Die Widerstandsfähigkeit der Mechanismen muss sich am Schutzbedarf (hinsichtlich der Integrität) der verarbeiteten Datenobjekte orientieren.	MUSS			

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				Bei der Verarbeitung von Dokumenten mit Schutzbedarf „normal“ bezüglich der	SOLLTE			
				Integrität, sollten geeignete kryptographische Mechanismen in Form von fortgeschrittenen elektronischen Signaturen oder fortgeschrittenen elektronischen Siegeln verwendet werden.	SOLLTE			
				Andernfalls muss ein schriftlicher Nachweis erbracht werden, dass der für den Integritätsschutz eingesetzte Mechanismus im Sinne der obigen Festlegung ausreichend widerstandsfähig ist.	MUSS			
				Zum Schutz der Datenobjekte gegen zufällige Änderungen oder aufgrund von Systemfehlern sollten diese jedoch mit einem geeigneten Datensicherungsverfahren gesichert werden.	SOLLTE			

P.3 Aufbaumodule

P.3.1 Generelle Maßnahmen bei erhöhtem Schutzbedarf

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
36	32	4.3.1.1	A.AM.G.1	**Beschränkung des Zugriffs auf sensible Papierdokumente**				
				Bei der Verarbeitung von Dokumenten mit Schutzbedarf von zumindest „hoch“ bezüglich der Integrität, Vertraulichkeit oder Verfügbarkeit sollten während des Scanvorgangs keine unbefugten Personen Zugriff auf die Papierdokumente erhalten.	SOLLTE			
				Es müssen geeignete Maßnahmen für die Beschränkung des Zugriffs auf die sensiblen Papierdokumente getroffen werden. Dies umfasst:				

Nr	Seite	Kapitel	ID	Anforderung		M / S	Referenzen / Bemerkungen	Ergebnis	
				a	Zugangsbeschränkung zu den Räumlichkeiten, in denen die Dokumente verarbeitet werden.	MUSS			
				b	Eine Aufbewahrung, die Schutz vor unbefugtem Zugriff, Einsichtnahme oder Beschädigung bietet.	MUSS			
				c	Die Verpflichtung der Mitarbeiter zur sorgfältigen Handhabung der Dokumente (z. B. kein unbeaufsichtigtes Liegenlassen, keine Weitergabe ohne Prüfung der Autorisierung)	MUSS			
				Sofern nicht bereits generelle Regelungen für den Zugriff auf sensible Papierdokumente existieren, müssen im Rahmen des ersetzenden Scannens entsprechende Regelungen geschaffen werden.		MUSS			
37	33	4.3.1.2	A.AM.G.2	**Pflicht zur Protokollierung beim Scannen**					
				Die in A.SC.11 empfohlene Protokollierung muss erfolgen.		MUSS			
38	33	4.3.1.3	A.AM.G.3	**Pflicht zur regelmäßigen Auditierung**					
				Die in A.O.4 empfohlene Überprüfung der Wirksamkeit und Vollständigkeit, der für die Informationssicherheit beim ersetzenden Scannen vorgesehenen Maßnahmen, muss mindestens alle drei Jahre erfolgen.		MUSS			

P.3.2 Zusätzliche Maßnahmen bei hohen Integritätsanforderungen

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
39	33	4.3.2.1	A.AM.IN.H.1	**Einsatz kryptographischer Mechanismen zum Integritätsschutz**				
				Bei der Verarbeitung von Datenobjekten mit einem Schutzbedarf von zumindest „hoch“ bezüglich der Integrität müssen geeignete	MUSS			

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				kryptographische Mechanismen in Form von qualifizierten elektronischen Signaturen oder qualifizierten elektronischen Siegeln zum Einsatz kommen.				
				Die Vorgaben der [LeitLeSig] müssen eingehalten werden, sofern eine anschließende langfristige Beweiswerterhaltung vorgesehen ist.	MUSS			
				Um die Verkehrsfähigkeit der Datenobjekte und Sicherungsdaten sicherzustellen, müssen standardisierte Formate verwendet werden.	MUSS			
40	34	4.3.2.2	A.AM.IN.H.2	**Geeignetes Schlüsselmanagement**				
				Sofern schlüsselbasierte kryptographische Mechanismen eingesetzt werden, müssen geeignete Verfahren zum Schlüsselmanagement vorgesehen werden.	MUSS			
				Dabei muss insbesondere über den vorgesehenen Aufbewahrungszeitraum der Scanprodukte hin sichergestellt werden, dass				
				a die Vertraulichkeit, Integrität und Authentizität der Schlüssel gewahrt bleibt.	MUSS			
				b private und geheime Schlüssel nicht unbefugt verwendet werden können.	MUSS			
				c die zur Prüfung der Integritätssicherung erforderlichen Schlüssel und Zertifikate verfügbar bleiben.	MUSS			
				Hierbei sollten die einschlägigen Empfehlungen aus dem IT-Grundschutz-Kompendium des BSI (CON.1, Kryptokonzept), [NIST-800-57-1/2], [NIST-800-133] und [BSI TR-03145] bei der Verwaltung des Schlüsselmaterials berücksichtigt oder vertrauenswürdige Dienstleister für das Schlüsselmanagement genutzt werden.	SOLLTE			

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis
				Auswahl eines geeigneten kryptographischen Verfahrens			
41	34	4.3.2.3	A.AM.IN.H.3	Sofern kryptographische Verfahren eingesetzt werden, müssen geeignete kryptographische Verfahren verwendet werden. Hierbei müssen Verfahren gemäß {BSI TR-02102-1], [BSI TR-03116-4] oder [ETSI TS 119 312] eingesetzt werden.	MUSS		
				Auswahl eines geeigneten kryptographischen Produktes			
				Zur Integritätssicherung müssen geeignete (qualifizierte) Vertrauensdienste und Produkte hinsichtlich Funktionalität und Vertrauenswürdigkeit eingesetzt werden. Bei der Funktionalität ist vor allem auf eine ausreichende Stärke und Widerstandsfähigkeit der eingesetzten Sicherheitsmechanismen im Sinne der eIDAS-VO sowie der [LeitLeSig] zu achten.	MUSS		
42	34	4.3.2.4	A.AM.IN.H.4	Hinsichtlich der Vertrauenswürdigkeit sind der Einsatz veröffentlichter und gemeinschaftlich analysierter Algorithmen (siehe A.AM.IN.H.3, oben) und Quellen sowie durchgeführte Prüfungen nach einem anerkannten Sicherheitsstandard wie FIPS-140, Common Criteria oder ITSEC positiv zu bewerten und sollten daher primär herangezogen werden	SOLLTE		
				Da sich die Sicherheitseignung der kryptographischen Algorithmen ändern kann, sollte auf eine leichte Austauschbarkeit der entsprechenden Komponenten geachtet werden.	SOLLTE		
				Um eine sichere Nutzung der kryptographischen Produkte zu gewährleisten, müssen die notwendigen Einsatzbedingungen und sonstigen Empfehlungen des Herstellers berücksichtigt werden.	MUSS		
				Langfristige Datensicherung bei Einsatz kryptographischer Verfahren			
43	35	4.3.2.5	A.AM.IN.H.5	Für die eingesetzten kryptographischen Verfahren, muss die Eignung der verwendeten Algorithmen und Parameter regelmäßig evaluiert werden.	MUSS		

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis
				Sofern Bedarf für eine langfristige Beweiswerterhaltung besteht, sind nach § 15 VDG, qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten durch geeignete Maßnahmen neu zu schützen, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird.	MUSS		
				Sofern Bedarf für eine langfristige Beweiswerterhaltung besteht, muss die neue Sicherung nach dem Stand der Technik erfolgen. Der Stand der Technik wird durch den Einsatz eines (zertifizierten) [BSI TR-03125]-Produktes oder durch den Einsatz eines (qualifizierten) Bewahrungsdienstes gemäß [ETSI TS 119 511] sichergestellt.	MUSS		
44	35	4.3.2.6	A.AM.IN.H.6	**Verhinderung ungesicherter Netzzugänge**			
				Sofern die für das Scannen eingesetzten IT-Systeme über ein Netzwerk verbunden sind, muss ein ungesicherter Zugang zu diesem Netzwerksegment verhindert werden.	MUSS		
				Ein Zugriff aus dem Internet auf dieses Netzwerksegment darf nur entkoppelt (Proxy/Gateway) und nur bei Initiierung von innen möglich sein.	MUSS		
45	35	4.3.2.7	A.AM.IN.H.7	**Erweiterte Qualitätssicherung der Scanprodukte**			
				Bei einem Schutzbedarf der Datenobjekte von „hoch“ bezüglich der Integrität, sollte die Qualitätskontrolle der Scanprodukte (in regelmäßigen zeitlichen Abständen) durch eine vollständige Sichtkontrolle erfolgen.	SOLLTE		
				Bei einem sehr hohen Durchsatz kann die Sichtkontrolle sukzessive auf regelmäßig durchgeführte Stichproben reduziert werden, wobei deren Größe den Stichprobenumfang der Sichtkontrolle des Schutzbedarfs „normal“ deutlich übertreffen muss.	MUSS		

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				Falls keine vollständige Sichtkontrolle realisiert wird, sollten automatische Mechanismen zur Qualitätskontrolle eingesetzt werden, wie z. B. eine automatische Erkennung von Leerseiten, von unzureichender Bildqualität oder die Prüfung der Seitenzahl.	SOLLTE			
				Beim Einsatz automatisierter Mechanismen muss eine manuelle Prüfung der identifizierten Probleme und Auffälligkeiten erfolgen.	MUSS			

P.3.3 Zusätzliche Maßnahmen bei sehr hohen Integritätsanforderungen

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				4-Augen-Prinzip				
46	36	4.3.3.1	A.AM.IN.SH.1	Bei Schutzbedarf „sehr hoch“ hinsichtlich der Integrität muss im Rahmen der Aufgabenteilung (siehe A.O.1) sichergestellt werden, dass die Erstellung und Qualitätssicherung des Scanproduktes von unterschiedlichen Personen durchgeführt wird.	MUSS			
				Einsatz qualifizierter elektronischer Signaturen oder Siegel und Zeitstempel				
47	36	4.3.3.2	A.AM.IN.SH.2	Sofern Datenobjekte mit einem Schutzbedarf von „sehr hoch“ bezüglich der Integrität verarbeitet werden, müssen für die Integritätssicherung des Scanproduktes bzw. des Transfervermerkes qualifizierte elektronische Signaturen oder qualifizierte elektronische Siegel und qualifizierte Zeitstempel eingesetzt werden (vgl. A.AM.IN.H.1).	MUSS			
				Eigenständiges Netzsegment				
48	36	4.3.3.3	A.AM.IN.SH.3	Bei einem Schutzbedarf der Datenobjekte bzgl. Vertraulichkeit oder Integrität von „sehr hoch“, müssen die für das Scannen eingesetzten IT-Systeme in einem eigenständigen Netzsegment eingebunden sein.	MUSS			
				Der Zugriff auf dieses Netzsegment aus anderen Netzsegmenten darf nicht erfolgen, es sei denn die Kommunikation wird über einen Proxy oder ein Gateway vermittelt und der Verbindungsaufbau erfolgt von innen.	MUSS			
				Kennzeichnung der Dokumente bzgl. Sensitivität				
49	36	4.3.3.4	A.AM.IN.SH.4	Dokumente, die einen Schutzbedarf von „sehr hoch“ bzgl. der Integrität besitzen, sollten als solche gekennzeichnet werden, ohne das Original zu manipulieren.	SOLLTE			

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				Die Kennzeichnung sollte deutlich sichtbar angebracht werden.	SOLLTE			
50	36	4.3.3.5	A.AM.IN.SH.5	**Vollständige Sichtkontrolle zur Qualitätssicherung der Scanprodukte**				
				Bei einem Schutzbedarf der Datenobjekte von „sehr hoch“ bezüglich der Integrität, muss die Qualitätskontrolle der Scanprodukte durch eine vollständige Sichtkontrolle erfolgen.	MUSS			

P.3.4 Zusätzliche Maßnahmen bei hohen Vertraulichkeitsanforderungen

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
51	37	4.3.4.1	A.AM.VT.H.1	**Sensibilisierung und Verpflichtung der Mitarbeiter**				
				Bei der Verarbeitung von Dokumenten mit einem Schutzbedarf bezüglich der Vertraulichkeit von zumindest „hoch“ müssen die Mitarbeiterinnen und Mitarbeiter bzgl. der Sicherheitsmaßnahmen und der sicherheitsbewussten Handhabung von Dokumenten, Daten und IT-Systemen und der zu ergreifenden Vorsichtsmaßnahmen sensibilisiert und geschult werden.	MUSS			
				Mitarbeiter müssen durch eine explizite Verfahrensanweisung auf die Einhaltung der einschlägigen Gesetze, Vorschriften und Regelungen verpflichtet werden.	MUSS			
52	37	4.3.4.2	A.AM.VT.H.2	**Verhinderung ungesicherter Netzzugänge**				
				Siehe A.AM.IN.H.6, Abschnitt 4.3.2.	MUSS			
53	37	4.3.4.3	A.AM.VT.H.3	**Löschen von Zwischenergebnissen**				
				Bei der Verarbeitung von Dokumenten mit einem Schutzbedarf hinsichtlich der Vertraulichkeit von zumindest „hoch“, müssen die in der Verarbeitung entstehenden Zwischenergebnisse (z. B. rohe Scanprodukte, Daten im Scan-Cache) zuverlässig gelöscht werden.	MUSS			

P.3.5 Zusätzliche Maßnahmen bei sehr hohen Vertraulichkeitsanforderungen

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
54	37	4.3.5.1	A.AM.VT.SH.1	**Kennzeichnung der Dokumente bzgl. Sensitivität**				
				Dokumente, die einen Schutzbedarf von „sehr hoch“ bzgl. der Vertraulichkeit besitzen, sollten als solche gekennzeichnet werden, ohne das Original zu manipulieren.	SOLLTE			
				Die Kennzeichnung sollte deutlich sichtbar angebracht werden.	SOLLTE			
55	37	4.3.5.2	A.AM.VT.SH.2	**Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln**				
				Sofern der Scanner einen internen Speicher besitzt und Dokumente gescannt werden, die einen Schutzbedarf bzgl. der Vertraulichkeit von „sehr hoch“ besitzen, muss der Datenträger vor der Entsorgung des Scanners zuverlässig gelöscht werden.	MUSS			
				Sofern möglich, sollte der Datenträger ausgebaut und mit einem geeigneten Verfahren zuverlässig gelöscht oder zerstört werden.	SOLLTE			
				Kryptographische Schlüssel, die im zu entsorgenden Scanner vorgehalten werden, müssen zuverlässig gelöscht oder deaktiviert werden.	MUSS			
				In etwaigen Verträgen mit Dienstleistern ist darauf zu achten, dass ein zuverlässiges und für die Organisation nachvollziehbares Lösch- und Entsorgungsverfahren etabliert wird. Hierbei müssen die Anforderungen nach CON.6 aus dem BSI-Grundschutzkompendium oder [DIN66399] angewendet werden.	MUSS			
56	38	4.3.5.3	A.AM.VT.SH.3	**Besondere Zuverlässigkeit und Vertrauenswürdigkeit der Mitarbeiter**				
				Sofern Dokumente gescannt werden, deren Schutzbedarf hinsichtlich der Vertraulichkeit „sehr hoch“ ist, sollte sichergestellt werden, dass die	SOLLTE			

Nr	Seite	Kapitel	ID		Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
					Mitarbeiter, die für den Scanprozess verantwortlich sind und den Prozess durchführen besonders zuverlässig und vertrauenswürdig sind.				
57	38	4.3.5.4	A.AM.VT.SH.4		**Verschlüsselte Datenübertragung innerhalb des Scansystems**				
					Bei der Verarbeitung von Datenobjekten mit einem Schutzbedarf von „sehr hoch“ bzgl. der Vertraulichkeit sollte die Datenübertragung zwischen Scanner, Scan-Workstation, Scan-Cache und anderen damit zusammenhängenden Systemen durch geeignete Verschlüsselungsverfahren gemäß [BSI TR-02102-1] oder [BSI TR-03116-4] erfolgen.	SOLLTE			
					Andernfalls muss ein geeigneter Nachweis erbracht werden, dass diese Kommunikationsverbindungen durch alternative Maßnahmen ausreichend geschützt sind.	MUSS			
58	39	4.3.5.5	A.AM.VT.SH.5		**Räumlichkeiten des Scan-Systems**				
				a	Die räumliche Absicherung des Scan-Systems muss dem Schutzbedarf des Papieroriginals entsprechen.	MUSS			
				b	Die Räumlichkeiten sollten nur von den vertrauenswürdigen Mitarbeitenden zu betreten sein, in dem dies in einem geeigneten Zutrittskonzept beschrieben ist.	SOLLTE			
				c	Etwaige Fenster müssen mit einem lichtdurchlässigen Sichtschutz versehen sein.	MUSS			

P.3.6 Zusätzliche Maßnahmen bei hohen Verfügbarkeitsanforderungen

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				Fehlertolerante Protokolle und redundante Datenhaltung				
59	39	4.3.6.1	A.AM.VF.H.1	Bei Schutzbedarf „hoch“ bzgl. der Verfügbarkeit sollte ein fehlertolerantes Übertragungsprotokoll sowie eine redundante Auslegung des Scansystems verwendet werden.	SOLLTE			

P.3.7 Zusätzliche Maßnahmen bei sehr hohen Verfügbarkeitsanforderungen

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				Test der Geräte und Einstellungen mit ähnlichen Dokumenten				
60	39	4.3.7.1	A.AM.VF.SH.1	Bei Datenobjekten mit einem Schutzbedarf „sehr hoch“ bzgl. der Verfügbarkeit, muss die Eignung der verwendeten Geräte, Verfahren und Einstellungen vorher mit physikalisch ähnlichen Dokumenten, die selbst keinen hohen Schutzbedarf bzgl. der Verfügbarkeit haben, getestet und das Prüfergebnis dokumentiert werden.	MUSS			

P.4 Besonderheiten beim mobilen ersetzenden Scannen

P.4.1 Einführung in das mobile Scannen

Unter mobilem ersetzendem Scannen wird die ersetzende Digitalisierung von Papieroriginalen unter Nutzung mobiler Endgeräte (beispielsweise Mobiltelefon oder Tablet) unter Nutzung einer ScanApp und Übertragung von Scanprodukt, Metadaten, Transfervermerk etc. an eine zentrale Infrastruktur verstanden. Stationäre Scanstellen an verschiedenen Orten oder solche, die mittels Fahrzeugen an verschiedene Orte verbracht werden können, werden vom mobilen Scannen nicht umfasst.

Im Folgenden werden nur die besonderen Anforderungen an das mobile ersetzende Scannen als Abweichung zum stationären ersetzenden Scannen definiert. Sofern keine Abweichung beschrieben ist, gelten die Anforderungen der TR-RESISCAN für das stationäre ersetzende Scannen (P 2 und P 3). Die spezifischen Anforderungen an das mobile Scannen werden in der Syntax [M.MaßnahmeXY.Nr. der Maßnahme] angegeben:

P.4.2 Basismodul mobiles Scannen

P.4.2.1 Organisatorische Maßnahmen

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis
				Festlegung von Verantwortlichkeiten, Abläufen und Aufgaben im Scanprozess			
61	40	5.2.1.1	M.A.O.1	Abweichend von den organisatorischen Maßnahmen nach A.O.1 müssen beim mobilen Scannen die folgenden Aspekte besonders umgesetzt werden: Zu a) Klare Aufteilung der Verantwortlichkeiten zwischen scannender Mitarbeiterin/scannendem Mitarbeiter und nachbearbeitender Mitarbeiterin/nachbearbeitendem Mitarbeiter	MUSS		
				Zu b) Festlegung der Dokumente, die vom mobilen Scannen eingeschlossen sind und die mobil nur kopierend gescannt werden dürfen.	MUSS		

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				Zu c) und d) • Protokolldaten der scannenden Mitarbeiterinnen und Mitarbeiter zum Prozess und Nachweise zur bildlichen und inhaltlichen Übereinstimmung • Protokolldaten des Mobilgeräts beim Scannen der Dokumente • Nutzung von Hashwerten und kryptografischen Signaturen und Siegeln	MUSS			
				Zu e) • Qualitätssicherung durch scannende Mitarbeiterin / scannendem Mitarbeiter vor dem Upload. • Ergänzende Qualitätssicherung durch organisationsinterne Mitarbeiterin / organisationsinternen Mitarbeiter nach Upload • Festlegung der Maßnahmen zur Qualitätssicherung, ausgerichtet an den Möglichkeiten des Mobilgeräts • Festlegung des Prozesses bei Qualitätsmängeln	MUSS			
				Es sollten Vorgaben zu den nachfolgenden Aspekten in einer organisationsweiten Richtlinie festgehalten, in die bestehenden Prozesse integriert und durch die Mitarbeitenden, die am mobilen Scannen beteiligt sind auf geeignete Weise bestätigt werden: • Schritte zur Dokumentenvorbereitung und Digitalisierung. • Welche Dokumente gescannt und welche Daten hierbei erzeugt werden, respektive wie diese zu scannen sind. • Notwendige Qualitätskontrollen, also z.B. die Prüfung der auf den Scancache gescannte Dokumente durch die scannenden Mitarbeitenden auf logische, inhaltliche und bildliche Übereinstimmung.	SOLLTE			

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				• Verantwortlichkeit für die Originaldokumente und Scanprodukte bei den scannenden Mitarbeitenden.				
				Die Qualitätskontrolle des Scanprodukts muss in zwei Schritten erfolgen (Erstkontrolle und Freigabe zum Upload durch scannende Mitarbeitende und Zweikontrolle durch Bearbeitende in der Zielinfrastruktur	MUSS			
				Es müssen geeignete Kommunikationsprozesse unter Beachtung der BSI TR-02102-1 zwischen scannenden Mitarbeitenden und Bearbeitenden in der Zielinfrastruktur etabliert werden.	MUSS			
62	42	5.2.1.2	M.A.O.2 M.A.O.3	**Wartungs- und Reparaturarbeiten sowie Abnahme und Freigabeverfahren**				
				Wartung und Reparatur sowie Abnahme und Freigabe der zum mobilen ersetzenden Scannen eingesetzten Geräte darf nur mit in der Organisation geprüften Endgeräten möglich sein.	MUSS			
				Für mobile Endgeräte müssen die Bausteine INF.9, SYS.2.1 und SYS.3.2 des [BSI-GSK] umgesetzt werden.	MUSS			
63	42	5.2.1.3	M.A.O.4	**Aufrechterhaltung der Informationssicherheit**				
				Das mobile ersetzende Scannen muss in der Organisation integriert und entsprechend dokumentiert sein. Die Überprüfung muss in die in der Organisation etablierten Prüfprozesse für die mobilen Endgeräte integriert werden.	MUSS			

P.4.2.2 Personelle Maßnahmen

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				Einweisung zum ordnungsgemäßen Scannen sowie Schulungen und Sensibilisierung zu Sicherheitsmaßnahmen				
64	42	5.2.2.1 5.2.2.2	M.A.P.1 M.A.P.2	Sowohl die Sensibilisierungen zu Sicherheitsmaßnahmen und Einweisungen zum ordnungsgemäßen Scannen als auch Schulungen und können aufgrund der personeller Komplexität durch elektronische Verfahren der Organisation (z.B. Onlinetutorials) erfolgen. Die Teilnahme muss durch die Mitarbeitenden elektronisch bestätigt und von der Organisation überprüfbar nachgehalten werden.	MUSS			

P.4.2.3 Technische Maßnahmen

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				Generelle Sicherheitsmaßnahmen				
65	43	5.2.3.1	M.A.T.1	Entsprechend A.T.1 ist das jeweilige Scansystem zu betrachten. Neben den grundsätzlichen, scanrelevanten Bausteinen des BSI-Grundschutz, müssen beim mobilen Scannen folgende Teile des BSI IT-Grundschutzkompendium mindestens umgesetzt werden oder vergleichbare Maßnahmen nach [ISO 27001] getroffen werden: • APP.1.2 (Webbrowser) • APP.1.4 (Mobile Anwendungen (Apps)) • SYS.2.1 (Allgemeiner Client) • SYS.3.3 (Mobiltelefon) • SYS.3.2.1 (Allgemeine Smartphones und Tablets) • SYS.3.2.2 (Mobile Device Management (MDM)) • SYS.3.2.3 (iOS for Enterprise)	MUSS			

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				• SYS.4.4 (Allgemeines IoT-Gerät) • INF.9 (Mobiler Arbeitsplatz) • NET.1.1 (Netzarchitektur & -design) • NET.3.3 (VPN)				
66	43	5.2.3.2	M.A.T.2	**Festlegung der zulässigen Kommunikationsverbindungen** Es gelten die Kommunikationsverbindungen nach dem generischen Scansystem mit Ausnahme von K1, siehe BSITR-03138-A. Hinzu kommt die Verbindung mobiles Endgerät zum Scancache. Es müssen beim mobilen Scannen folgende Teile des BSI IT-Grundschutzkompendiums mindestens berücksichtigt werden oder vergleichbare Maßnahmen nach ISO 27001 getroffen werden: • NET.1.1 (Netzarchitektur & -design) • NET.1.2 (Netzmanagement) • NET.3.1 (Router & Switches) • NET.3.2 (Firewall) • INF.9 (Mobiler Arbeitsplatz) • SYS.2.1 (Allgemeiner Client) • SYS.3.2 (Allgemeine Smartphone und Tablets)	MUSS			
67	43	5.2.3.3	M.A.T.3	**Schutz vor Schadprogrammen** • Es müssen beim mobilen Scannen folgende Teile des BSI IT-Grundschutzkompendiums mindestens berücksichtigt werden oder vergleichbare Maßnahmen nach ISO 27001 getroffen werden: • OPS.1.1.4 (Schutz vor Schadprogrammen)	MUSS			

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				• CON (Datensicherungskonzept) • INF.9 (Mobiler Arbeitsplatz) • SYS.2.1 (Allgemeiner Client) • SYS.3.2 (Allgemeine Smartphones und Tablets)				
68	43	5.2.3.4	M.A.T.4	**Zuverlässige Speicherung**				
				Die dauerhafte Speicherung von Scanprodukten auf dem mobilen Endgerät muss technisch ausgeschlossen sein. Eine Speicherung auf dem mobilen Endgerät darf nur temporär erfolgen. Nach Übermittlung an die Zielinfrastruktur muss das Scanprodukt im mobilen Endgerät automatisch gelöscht werden (z.B. Funktion der ScanApp). Eine Speicherung darf nur in der Zielinfrastruktur der Organisation erfolgen.	MUSS			

P.4.2.4 Sicherheitsmaßnahmen zur Dokumentenvorbereitung

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
69	44	5.2.4.1	M.A.DV.1	**Sorgfältige Vorbereitung der Papierdokumente**				
				Hinsichtlich der Bewahrung des logischen Kontexts der zu erfassenden Dokumente sollte beim mobilen Scannen bei den scannenden Mitarbeitenden aus Gründen der Ergonomie nur eine begrenzte Metadatenerfassung erfolgen.	SOLLTE			
				Die Metadaten müssen so vergeben werden können, dass der logische Kontext erhalten bleibt.	MUSS			
70	44	5.2.4.2	M.A.DV.2	**Vorbereitung der Vollständigkeitsprüfung**				

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				Die Vollständigkeitsprüfung in A.NB.3 sollte auf Stichproben reduziert werden.	SOLLTE			

P.4.2.5 Sicherheitsmaßnahmen beim Scannen

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				Auswahl und Beschaffung geeigneter Scanner				
				Als mobiles Endgerät dürfen nur in der Organisation zugelassene Geräte zum Einsatz kommen. Dies muss auf geeignete Weise sichergestellt werden.	MUSS			
				Für mobile Endgeräte müssen die Bausteine INF.9, SYS.2.1 und SYS.3.2 des [BSI IT-GSK] erfüllt werden oder vergleichbare Maßnahmen nach ISO 27001 getroffen werden.	MUSS			
71	44	5.2.5.1	M.A.SC.1	Dabei müssen zudem folgende Kriterien geprüft werden: • Bereitstellung und ausschließliche Nutzung einer in der Organisation zugelassenen ScanApp auf den mobilen Endgeräten • Bereitstellung und Wartung der App auf einem sicheren Weg (z. B. organisationseigener App-Store) • Softwareseitige Verhinderung einer Zwischenspeicherung des Scanprodukts bei Nutzung der ScanApp • Verhinderung eines Zugriffs auf den Scancache ohne Nutzung der zugelassenen ScanApp • Unterstützung geeigneter Datenformate • Unterstützung einer Erfassung von Minimalmetadaten am Mobilgerät • Ausreichende Qualität der Scanprodukte (bzgl. Auflösung, Bildkompressionsverfahren, Helligkeit, Kontrast etc.)	MUSS			

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				• Ausreichende Flexibilität der Konfiguration • Geeignete Schnittstellen zur Übertragung der Scanprodukte an den Scancache (Scannen zum Scancache) sowie zum Zugriff auf eine Integritätssicherungssoftware oder externen Vertrauensdienst • Möglichkeit zur sicheren Bestätigung/Freigabe eines Scanvorgangs unter Anzeige des Scanprodukts • Möglichkeit zum sicheren Löschen oder zur verschlüsselten Speicherung auf dem Scancache • Ausreichender Support				
72	44	5.2.5.2	M.A.SC.2	**Zugangs- und Zugriffskontrollen für Scanner**				
				Es muss eine sichere Authentisierung der scannenden Mitarbeitenden am zugelassenen mobilen Endgerät sowie der zentralen Infrastruktur gewährleistet werden, um Zugriffe durch unbefugte Personen auf das mobile Endgerät zu vermeiden.	MUSS			
				Die Konfiguration und Administration der ScanApp muss durch berechtigtes Administrationspersonal erfolgen.	MUSS			
73	45	5.2.5.3	M.A.SC.6	**Geeignete Scan-Einstellungen**				
				Die Scan-Einstellung muss durch die ScanApp der Organisation vorgegeben und darf von der scannenden Mitarbeiterin / vom scannenden Mitarbeiter nicht verändert werden.	MUSS/ DARF NICHT			
74	45	5.2.5.4	M.A.SC.7	**Geeignete Erfassung von Metadaten**				
				Beim mobilen Scannen muss sichergestellt werden, dass die Erfassung minimaler Metadaten am mobilen Endgerät möglich ist.	MUSS			

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				Die Indexierung und umfassendere Erfassung beschreibender Information sollte durch die Bearbeiterin / den Bearbeiter in der Zielinfrastruktur der Organisation erfolgen.	SOLLTE			
75	45	5.2.5.5	M.A.SC.8	**Qualitätssicherung der Scanprodukte**				
				Die Qualitätskontrolle muss in den folgenden beiden Schritten erfolgen: • Qualitätssicherung durch die scannende Mitarbeiterin / dem scannenden Mitarbeiter am mobilen Endgerät. • Qualitätssicherung durch die Bearbeiterin / den Bearbeiter in der Zielinfrastruktur der Organisation gemäß A.SC.8.	MUSS			
76	45	5.2.5.6	M.A.SC.9	**Sichere Außerbetriebnahme von Scannern**				
				Es müssen die Bausteine INF.9 und SYS.3.2 oder vergleichbare Maßnahmen nach [ISO 27001] umgesetzt werden.	MUSS			
77	45	5.2.5.7	M.A.SC.10	**Informationsschutz und Zugriffsbeschränkung bei netzwerkfähigen Scannern**				
				Es müssen die Bausteine INF.9 und SYS.3.2 oder vergleichbare Maßnahmen nach [ISO 27001] umgesetzt werden.	MUSS			
78	45	5.2.5.8	M.A.SC.11	**Protokollierung beim Scannen**				
				Zusätzlich müssen Maßnahmen nach A.SC.11 auch für die ScanApp umgesetzt werden.	MUSS			

P.4.2.6 Sicherheitsmaßnahmen bei der Nachbearbeitung und Integritätssicherung

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
79	45	5.2.6	M.A.NB/IS.1	**Sicherheitsmaßnahmen bei der Nachbearbeitung und Integritätssicherung**				
				Die Nachbearbeitung, Qualitätssicherung und Vollständigkeitsprüfung müssen in der Zielinfrastruktur der Organisation erfolgen.	MUSS			
				Der Transfervermerk muss in der Zielinfrastruktur erzeugt werden.	MUSS			
				Die Integritätssicherung muss in der Zielinfrastruktur erfolgen.	MUSS			

P.4.3 Aufbaumodule

P.4.3.1 Generelle Maßnahmen bei Schutzbedarf „hoch“

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
80	46	5.3.1.1	M.A.AM.G.1	**Beschränkung des Zugriffs auf sensible Papierdokumente**				
				Das mobile Scannen sensibler Papierdokumente muss durch eine erhöhte Sensibilisierung der Mitarbeitenden zum Umgang und Digitalisierung dieser Dokumente begleitet werden, welche in einer spezifischen internen Richtlinie festgehalten wird und von den Mitarbeitenden nachprüfbar bestätigt wird.	MUSS			
81	46	5.3.1.2	M.A.AM.G.2	**Pflicht zur Protokollierung beim Scannen**				
				Alle technischen Schritte im Scanprozess (ScanApp und Komponenten in der Zielinfrastruktur) müssen gemäß A.AM.G.2 protokolliert werden.	MUSS			
82	46	5.3.1.3	M.A.AM.G.3	**Pflicht zur regelmäßigen Auditierung**				

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
				Die mobilen Endgeräte und deren Nutzung müssen in die periodische Audits ebenso eingebunden werden, wie die Zielinfrastruktur.	MUSS			

P.4.3.2 Zusätzliche Maßnahmen bei hohen Integritätsanforderungen

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
83	46	5.3.2.1	M.A.AM.IN.H.1	**Einsatz kryptografischer Mechanismen zum Integritätsschutz**				
				Der Integritätsschutz muss in der Zielinfrastruktur gemäß den Vorgaben von A.AM.IN.H.1 erfolgen.	MUSS			
84	46	5.3.2.2	M.A.AM.IN.H.2	**Geeignetes Schlüsselmanagement**				
				Das Schlüsselmanagement muss in der Zielinfrastruktur gemäß den Vorgaben von A.AM.IN.H.2 erfolgen.	MUSS			
85	46	5.3.2.3	M.A.AM.IN.H.5	**Langfristige Datensicherung bei Einsatz kryptographischer Vorgaben**				
				Die langfristige Datensicherung muss in der Zielinfrastruktur gemäß den Vorgaben von A.AM.IN.H.5 erfolgen.	MUSS			
86	46	5.3.2.4	M.A.AM.IN.H.6	**Verhinderung ungesicherter Netzzugänge**				
				Es muss ein ungesicherter Zugang zum Netzwerksegment der Zielinfrastruktur unter Beachtung der [BSI TR-02102-1] verhindert werden.	MUSS			
				Ein Zugriff aus dem Internet auf dieses Netzsegment darf nicht erfolgen, es sei denn die Kommunikation wird über einen Proxy oder ein Gateway vermittelt und der Verbindungsaufbau erfolgt von innen.	MUSS			

P.4.3.3 Zusätzliche Maßnahmen bei hohen Vertraulichkeitsanforderungen

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
87	47	5.3.3.1	M.A.AM.VT.H.1	**Sensibilisierung und Verpflichtung der Mitarbeiterinnen und Mitarbeiter**				
				Es muss eine gesonderte Sensibilisierung und nachweisbare Verpflichtungen der Mitarbeitenden für das mobile Scannen erfolgen.	MUSS			
88	47	5.3.3.2	M.A.AM.VT.H.3	**Löschen von Zwischenergebnissen**				
				Es darf keine Speicherung von Zwischenergebnissen auf dem mobilen Endgerät erfolgen.	MUSS			

P.4.3.4 Zusätzliche Maßnahmen bei hohen Verfügbarkeitsanforderungen

Nr	Seite	Kapitel	ID	Anforderung	M / S	Referenzen / Bemerkungen	Ergebnis	
89	48	5.3.4.1	M.A.AM.VF.H.1	**Erweiterte Qualitätssicherung der Scanprodukte**				
				Die Maßgaben von A.AM.VF.H.1 müssen in der Zielinfrastruktur umgesetzt werden.	MUSS			
				Die Rückkopplung zum einscannenden Mitarbeitenden muss dabei berücksichtigt werden.	MUSS			
90	48	5.3.4.2	M.A.AM.VF.H.2	**Fehlertolerante Protokolle und redundante Datenhaltung**				
				Die Maßgaben nach A.AM.VF.H.2 müssen in der Zielinfrastruktur und beim mobilen Endgerät umgesetzt werden.	MUSS			
				Da im mobilen Endgerät keine Datensicherung erfolgt muss die redundante Datenhaltung in der Zielinfrastruktur der Organisation erfolgen.	MUSS			

Referenzen

[BSI-GSK] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz- Kompendium, 2023 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

[BSI TR-02102-1] Bundesamt für Sicherheit in der Informationstechnik (BSI): Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI TR-02102-1, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=10

[BSI TR-03116-4] Bundesamt für Sicherheit in der Informationstechnik (BSI): Kryptographische Vorgaben für Projekte der Bundesregierung, Teil: Kommunikationsverfahren und Anwendungen, BSI TR-03116-4 ,https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.pdf?__blob=publicationFile&v=5

[BSI TR-03125] Bundesamt für Sicherheit in der Informationstechnik (BSI): Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR), BSI TR-03125, https://www.bsi.bund.de/dok/TR-03125

[BSI TR-03138] Bundesamt für Sicherheit in der Informationstechnik (BSI): Ersetzendes Scannen, Technische Richtlinie (TR) des BSI Nr. 03138 (TR RESISCAN)

[BSI TR-03138-R] Bundesamt für Sicherheit in der Informationstechnik (BSI): Ersetzendes Scannen - Anwendungshinweis R: Unverbindliche rechtliche Hinweise, Anwendungshinweis R, Technische Richtlinie (TR) des BSI Nr. 03138 (TR RESISCAN)

[BSI TR-03145] Bundesamt für Sicherheit in der Informationstechnik (BSI): Secure CA operation, BSI TR-03145

[DIN66399] DIN: DIN 66399-1-3 Büro- und Datentechnik - Vernichten von Datenträgern - Teil 1: Grundlagen und Begriffe, Vernichten von Datenträgern - Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern; Vernichten von Datenträgern - Teil 3: Prozess der Datenträgervernichtung. https://www.din.de/de/meta/suche/62730!search?query=66399&submit-btn=Submit

[ETSI TS 119 312] ETSI TS 119 312: Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[ETSI TS 119 511] ETSI TS 119 511: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques

[ISO27001] ISO/IEC, ISO/IEC 27001: Information security, cybersecurity and privacy protection Information security management systems - requirements, International Standard, https://www.iso.org/standard/27001

[ISO27002] ISO/IEC, ISO/IEC 27002: Information security, cybersecurity and privacy protection — Information security controls, International Standard, https://www.iso.org/standard/75652.html

[LeitLeSig] Leitlinie für digitale Signatur-/ Siegel-, Zeitstempelformate sowie technische Beweisdaten (Evidence Record). Bundesamt für Sicherheit in der Informationstechnik.

[NIST-800-57-1] E. Barker: Recommendation for Key Management – Part 1: General, NIST Special Publication 800-57

[NIST-800-57-2] E. Barker, W. Barker, W. Burr, W. Polk, M. Smid: Recommendation for Key Management – Part 2: Best Practices for Key Management Organization, NIST Special Publication 800-57

[NIST-800-133] E. Barker, A. Roginsky: Recommendation for Cryptographic Key Generation, NIST Special Publication 800-133

[VDG] Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist