Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Nachweise für die Konformitätsprüfung gemäß BSI TR-03138 Ersetzendes Scannen

enthält Testcases der	BSI TR-03138 Anlage P
in der Version:	1.4.1
09.09.2021	

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.0	23.04.2020	BSI	Finale Fassung
1.1	09.09.2021	BSI	Umstellung auf MS Word,

Tabelle 1: Änderungshistorie

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

Inhalt

Nachweise für die Konformitätsprüfung gemäß BSI TR-03138 Ersetzendes Scannen

P.1 Grundlegendes

Bei Beantragung der Zertifizierung gemäß BSI TR-03138 „Ersetzendes Scannen“ (RESISCAN), ist dieses Dokument ausgefüllt einzureichen. Dies dient dazu, den Prozess der Prüfung und Zertifizierung effizient zu gestalten.

Antragsteller SOLLEN bei jedem Prüfkriterium in der Spalte „Referenzen / Umsetzung“ die Umsetzung beschreiben bzw. auf das/die Referenzdokument/e (inkl. Dokumenten-bezeichnung, Kapitel, Seite und ggf. Abschnitt) verweisen.

Reicht der Platz innerhalb der Spalte „Referenzen/Umsetzung“ nicht aus, so können bei Bedarf die Seiten 34 bis 38 für weitere Ausführungen genutzt werden.

P.2 Basismodul

ID	*Anforderung*		*M / S*	*Referenzen / Umsetzung*
-	*Strukturanalyse*			
	Die Strukturanalyse identifiziert die relevanten			
	a	Datenobjekte	MUSS	
	b	IT-Systeme und Anwendungen	MUSS	
	c	Kommunikationsverbindungen (Netze)	MUSS	
	Bereinigter Netzplan liegt vor		MUSS	
-	*Schutzbedarfsanalyse*			
	Der Schutzbedarf der weiteren Datenobjekte ergibt sich aus dem Schutzbedarf der			

ID	Anforderung	M / S	Referenzen / Umsetzung
	Papieroriginale.		
	Der Schutzbedarf der Datenobjekte muss hinsichtlich der Grundwerte Integrität, Vertraulichkeit und Verfügbarkeit bestimmt werden.	MUSS	
	Bei der Bestimmung des Schutzbedarfs empfiehlt sich die Klassifizierung und Zusammenfassung gleichartiger Dokumente.	SOLL	

P.2.1 Grundlegende Anforderungen

ID		Anforderung	M / S	Referenzen / Umsetzung
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		MUSS	

ID	Anforderung		M / S	Referenzen / Umsetzung
		Festlegung von Maßnahmen zur Qualifizierung und Sensibilisierung der Mitarbeiter		
	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	MUSS	

P.2.2 Organisatorische Maßnahmen

ID	Anforderung		M / S	Referenzen / Umsetzung
A.O.1	*Festlegung von Verantwortlichkeiten, Abläufen und Aufgaben im Scanprozess*			
	Verantwortlichkeiten, Abläufen 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	

ID	Anforderung		M / S	Referenzen / Umsetzung
	e	Qualitätskontrollen müssen mindestens stichprobenartig erfolgen.	MUSS	
		Qualitätskontrollen sollen regelmäßig durch Mitarbeiter durchgeführt werden, die nicht mit der operativen Durchführung des zu kontrollierenden Arbeitsschritts betraut sind.	SOLL	
	f	Für die in den Scanprozess involvierten Datenobjekte sowie die genutzten IT-Systeme und Anwendungen sollen Verantwortliche benannt werden.	SOLL	
	g	Bei der Zuweisung des Personals zu den operativen Aufgaben im Scanprozess müssen potenzielle Interessenkonflikte berücksichtigt werden.	MUSS	
		Bei der Zuweisung des Personals zu den operativen Aufgaben im Scanprozess sollen potenzielle Interessenkonflikte nach Möglichkeit vermieden werden	SOLL	
	h	Typische Fehlerquellen müssen berücksichtigt werden.	MUSS	
		Für typische Fehlerquellen sollen entsprechende Vorsichtsmaßnahmen festgelegt werden.	SOLL	
	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	

ID		Anforderung	M / S	Referenzen / Umsetzung
	k	Es wird empfohlen das Scannen vor der Vorgangsbearbeitung durchzuführen (frühes Scannen).	SOLL	
A.O.2		*Regelungen für Wartungs- und Reparaturarbeiten*		
		Es sollen 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	SOLL	
	b	Verfahren für die regelmäßige Bereitstellung und Anwendung von sicherheitsrelevanten Updates	SOLL	
	c	Regelung zur Authentisierung und zum Nachweis der Autorisierung des Wartungspersonals	SOLL	
	d	Regelungen zum Schutz personenbezogener oder anderweitig besonders schützenswerter Daten (z. B. Betriebsgeheimnisse) auf den zu wartenden IT-Systemen	SOLL	
	e	Dokumentation von sicherheitsrelevanten Veränderungen an den involvierten IT-Systemen und Anwendungen	SOLL	
	f	Dokumentation der erfolgreichen Durchführung der Maßnahmen zur Qualitätskontrolle und Freigabe vor Wiederaufnahme des regulären Betriebs	SOLL	

ID	Anforderung	M / S	Referenzen / Umsetzung
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	
A.O.4	*Aufrechterhaltung der Informationssicherheit*		
	In angemessenen Abständen soll eine Überprüfung der Wirksamkeit und Vollständigkeit der für die Informationssicherheit beim ersetzenden Scannen vorgesehenen Maßnahmen durchgeführt werden (in Bundesbehörden min. alle drei Jahre).	SOLL	
	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 sollen von unabhängigen Personen durchgeführt werden.	SOLL	
	Die Ergebnisse der Audits sollen schriftlich dokumentiert werden.	SOLL	

ID		Anforderung	M / S	Referenzen / Umsetzung
		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	
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 Auftraggeber und Auftragnehmer müssen in der Verfahrensdokumentation explizit dargestellt werden. (Übertragungswege, Datenablageorte, beteiligte Akteure, Rückfallverfahren, Maßnahmen zur Integritäts- und Vollständigkeitskontrolle etc.)	MUSS	
	b	Der Auftragnehmer muss zur Einhaltung der vom Auftraggeber definierten Sicherheitsmaßnahmen verpflichtet werden.	MUSS	
	c	Es soll eine Analyse der durch die Aufgabenteilung zusätzlich entstehenden Risiken erfolgen.	SOLL	

ID		Anforderung	M / S	Referenzen / Umsetzung
	d	Zusätzlich zur regelmäßigen Auditierung sollen unangemeldete Stichproben durchgeführt werden.	SOLL	

P.2.3 Personelle Maßnahmen

ID		Anforderung	M / S	Referenzen / Umsetzung
A.P.1		*Sensibilisierung der Mitarbeiter für Informationssicherheit*		
		Mitarbeiter sollen bzgl. der Sicherheitsmaßnahmen und der sicherheitsbewussten Handhabung von Dokumenten, Daten und IT-Systemen sowie der ergreifenden Vorsichtsmaßnahmen sensibilisiert werden.	SOLL	
A.P.2		*Verpflichtung der Mitarbeiter zur Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen und der Verfahrensanweisung*		
		Die im Rahmen der Schutzbedarfsanalyse identifizierten rechtlichen Rahmenbedingungen sollen den Mitarbeitern zur Kenntnis gebracht werden.	SOLL	
		Mitarbeiter sollen zur Einhaltung der einschlägigen Gesetze, Vorschriften, Regelungen und der Verfahrensanweisung verpflichtet werden.	SOLL	
A.P.3		*Einweisung zur ordnungsgemäßen Bedienung des Scansystems*		
		Mitarbeiter, die den Scanvorgang durchführen, müssen hinsichtlich der eingesetzten Geräte, Anwendungen und Abläufe geschult werden. Dies umfasst insbesondere:		
	a	die grundsätzlichen Abläufe im Scanprozess einschließlich der Dokumentenvorbereitung,	MUSS	

ID		Anforderung	M / S	Referenzen / Umsetzung
		dem Scannen, der Indexierung, der zulässigen Nachbearbeitung, und der Integritätssicherung		
	b	die Konfiguration und Nutzung des Scanners und der Scan-Workstation	MUSS	
	c	die Anforderungen hinsichtlich der Qualitätssicherung	MUSS	
	d	die Abläufe und Anforderungen bei der Erstellung des Transfervermerks	MUSS	
	e	die Konfiguration und Nutzung der Systeme zur Integritätssicherung	MUSS	
	f	das Verhalten im Fehlerfall	MUSS	
A.P.4	*Schulung zu Sicherheitsmaßnahmen im Scanprozess*			
	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 Mitarbeiter für Informationssicherheit	MUSS	
	b	Personenbezogene Sicherheitsmaßnahmen im Scanprozess	MUSS	
	c	System-bezogene Sicherheitsmaßnahmen im Scanprozess	MUSS	
	d	Verhalten beim Auftreten von Schadsoftware	MUSS	
	e	Bedeutung der Datensicherung und deren Durchführung	MUSS	

ID		Anforderung	M / S	Referenzen / Umsetzung
	f	Umgang mit personenbezogenen und anderen sensiblen Daten	MUSS	
	g	Einweisung in Notfallmaßnahmen	MUSS	
A.P.5	*Schulung des Wartungs- und Administrationspersonals*			
	Das Wartungs- und Administrationspersonal soll soweit geschult werden, dass:			
	a	alltägliche Administrationsaufgaben selbst durchgeführt werden können.	SOLL	
	b	einfache Fehler selbst erkannt und behoben werden können.	SOLL	
	c	Datensicherungen regelmäßig selbsttätig durchgeführt werden können.	SOLL	
	d	Eingriffe von externem Wartungspersonal nachvollzogen werden können.	SOLL	
	e	Manipulationsversuche oder unbefugte Zugriffe auf die Systeme erkannt und zügig behoben werden können.	SOLL	

P.2.4 Technische Maßnahmen

ID	Anforderung	M / S	Referenzen / Umsetzung
A.T.1	*Grundlegende Sicherheitsmaßnahmen für IT-Systeme im Scanprozess*		

ID	Anforderung	M / S	Referenzen / Umsetzung
	Basierend auf den Ergebnissen der Schutzbedarfs-/Strukturanalyse SOLLEN 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] umgesetzt werden. Für die Prüfung 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.[1] Die Gültigkeit des jeweiligen Zertifikates MUSS hierbei mindestens noch 12 Monate betragen.	SOLL	
A.T.2	*Festlegung der zulässigen Kommunikationsverbindungen*		
	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).	MUSS	

1Für 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.

ID		Anforderung	M / S	Referenzen / Umsetzung
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	
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

ID	Anforderung	M / S	Referenzen / Umsetzung
A.DV.1	*Sorgfältige Vorbereitung der Papierdokumente*		

ID	Anforderung		M / S	Referenzen / Umsetzung
	Um eine zuverlässige und sorgfältige Erfassung zu gewährleisten, müssen Papierdokumente sorgfältig auf das Scannen vorbereitet werden. Dies umfasst folgende Aspekte:			
	a	Sorgfältige Brieföffnung	MUSS	
		Prüfung, ob das Dokument offensichtlich manipuliert wurde oder es sich um eine Kopie handelt.	MUSS	
		Zuordnung zu einer bestimmten Dokumentenklasse, um die entsprechende Vorsortierung zu ermöglichen.	MUSS	
		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.	SOLL	
	c	Maßnahmen für die Bewahrung des logischen Kontextes der zu erfassenden Dokumente	MUSS	
		Bewahrung der Zugehörigkeit der eingescannten Seiten zu einem Dokument	MUSS	
	d	Die korrekte Orientierung der erfassten Blätter muss erhalten bleiben (Drehung, leere Rückseite)	MUSS	

ID	Anforderung		M / S	Referenzen / Umsetzung
		Ist dies nicht möglich, muss beidseitig erfasst werden.	MUSS	
	e	Bewahrung der korrekten Reihenfolge von Blättern bei mehrseitigen Dokumenten	MUSS	
	f	Zuverlässige Trennung von unabhängigen Dokumenten	MUSS	
	g	Entfernen von Klammern, Knicken und nicht relevanten Klebezetteln	MUSS	
		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	
A.DV.2	*Vorbereitung der Vollständigkeitsprüfung*			
	Bei automatisierter Erfassung müssen Maßnahmen für die Sicherstellung der Vollständigkeit getroffen werden.		MUSS	
	Damit eine Vollständigkeitsprüfung im Rahmen der Nachbereitung durchgeführt werden kann, sollen entsprechende Vorbereitungen getroffen werden (bei Bedarf).		SOLL	

P.2.6 Sicherheitsmaßnahmen beim Scannen

ID	*Anforderung*		*M / S*	*Referenzen / Umsetzung*
A.SC.1	*Auswahl und Beschaffung geeigneter Scanner*			
	Bei der Auswahl und Beschaffung geeigneter Scanner sollen folgende Kriterien auf ihre Relevanz geprüft und berücksichtigt werden:			
	a	ausreichender Durchsatz	SOLL	
	b	Unterstützung geeigneter Datenformate	SOLL	
	c	Unterstützung von Patch- und/oder Barcodes zur Dokumententrennung und Übergabe von Meta-Informationen	SOLL	
	d	ausreichende Qualität der Scanprodukte	SOLL	
	e	ausreichende Flexibilität der Konfiguration	SOLL	
	f	Zuverlässiger und leistungsfähiger automatischer Seiteneinzug	SOLL	
	g	Möglichkeit zum Scannen gebundener Dokumente, Überlängen, zum Scannen von Farbe oder von Durchlichtdokumenten (bei Bedarf)	SOLL	
	h	Geeignete Schnittstellen für die Übermittlung des Scanprodukts in DMS/VBS/Archive/Fachanwendungen	SOLL	
	i	Möglichkeit der Absicherung der Administrationsschnittstelle	SOLL	
	j	Nutzung eines internen Datenspeichers	SOLL	

ID	Anforderung		M / S	Referenzen / Umsetzung
	k	Möglichkeit zum sicheren Löschen oder verschlüsselter Speicherung von Scanprodukten auf dem internen Datenspeicher	SOLL	
	l	ausreichender Support	SOLL	
A.SC.2	*Zugangs- und Zugriffskontrollen für Scanner*			
	Personen, die keinen Zugriff auf Originale, Scanpro-dukte und Scansystem haben dürfen, sollen keinen unbeaufsichtigten Zugang zum Scansystem erhalten.		SOLL	
	Es sollen geeignete Zugangskontrollen und Besucherregelungen vorgesehen werden.		SOLL	
	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, soll der Zugang zum Scanner generell auf ein Minimum beschränkt werden.		SOLL	
	Die Administration des Scanners bzw. die Konfiguration der Kommunikationsschnittstellen bei netzwerkfähigen Scannern soll durch ein geeignetes Authentisierungsverfahren geschützt werden.		SOLL	
	Der Zugriff auf die Administrationsschnittstelle soll durch eine geeignete Netzwerk-		SOLL	

ID	Anforderung	M / S	Referenzen / Umsetzung
	Konfiguration auf die notwendigen Systeme eingeschränkt werden.		
A.SC.3	*Änderung voreingestellte Passwörter*		
	Voreingestellte Passwörter müssen nach der Installation des Scanners/Scansystems geändert werden.	MUSS	
	Basis für die Vergabe der Passwörter SOLLEN explizit formulierte interne Sicherheitsrichtlinien unter Berücksichtigung der Empfehlungen aus BSI-Grundschutz (siehe ORP.4.A8) sein.	SOLL	
A.SC.4	*Sorgfältige Durchführung von Konfigurationsänderungen*		
	Bei der Durchführung von Konfigurationsänderungen muss sorgfältig vorgegangen werden.	MUSS	
	Die alte Konfiguration soll zuvor gesichert werden.	SOLL	
	Änderungen sollen von einem Kollegen überprüft werden, bevor diese in den Echtbetrieb übernommen werden.	SOLL	
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	

ID	Anforderung	M / S	Referenzen / Umsetzung
	Für Dokumente, die nicht für den automatischen Einzug geeignet sind, müssen in der Verfahrensdokumentation geeignete Verfahren beschrieben werden.	MUSS	
A.SC.6	*Geeignete Scan-Einstellungen*		
	Die Scan-Einstellungen müssen für die jeweiligen Dokumente geeignet gewählt werden.	MUSS	
	Für die Dokumententypen sollen geeignete Profile definiert, getestet und freigegeben werden.	SOLL	
	Spätestens beim Scannen soll geprüft werden, dass geeignete Scan-Einstellungen genutzt werden.	SOLL	
A.SC.7	*Geeignete Erfassung von Metainformationen*		
	Index- und Metadaten sollen in geeigneter Weise übergeben werden.	SOLL	
	Hierbei soll eine zuverlässige Konfiguration der Applikation bzgl. der Erkennung und Gültigkeit der ausgelesenen Werte sowie eine sorgfältige manuelle Qualitätssicherung und Nachbearbeitung erfolgen.	SOLL	
A.SC.8	*Qualitätssicherung der Scanprodukte*		
	Zur Erkennung mangelhafter Scanvorgänge muss eine geeignete Qualitätskontrolle erfolgen.	MUSS	
	Die Ausgestaltung der Qualitätssicherung soll sich am Scan-Durchsatz und dem Schutzbedarf der verarbeiteten Dokumente orientieren.	SOLL	

ID	Anforderung	M / S	Referenzen / Umsetzung
	Die Größe der Stichprobe soll abhängig vom Schutzbedarf der Dokumente und der Zuverlässigkeit des Scansystems bestimmt werden.	SOLL	
	Bei automatisierten Qualitätskontrollen soll eine manuelle Prüfung der automatisch identifizierten Probleme erfolgen.	SOLL	
	Die Vernichtung der Originaldokumente darf nicht vor Abschluss der Qualitätskontrolle erfolgen.	MUSS	
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	
	Spezifische Konfigurationsinformationen, die Rückschlüsse auf die Netzwerkstrukturen liefern können, sollen gelöscht werden.	SOLL	
A.SC.10	*Informationsschutz und Zugriffsbeschränkung bei netzwerkfähigen Scannern*		
	Bei Scannern, die über ein Netzwerk angesprochen werden, sollen geeignete Maßnahmen zur Zugriffsbeschränkung und für den Schutz der über das Netzwerk übertragenen Informationen vorgesehen werden.	SOLL	

ID		Anforderung	M / S	Referenzen / Umsetzung
		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	
		Sofern Dokumente mit Schutzbedarf „sehr hoch“ verarbeitet werden, sollen geeignete kryptographische Mechanismen gemäß BSI TR-02102 oder BSI TR-03116 für die gesicherte Übertragung der Informationen und die Realisierung des Zugriffsschutzes eingesetzt werden.	SOLL	
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 soll insbesondere folgende Punkte umfassen:		
	a	Änderung von kritischen Konfigurationsparametern sowie Authentisierungs- und Berechtigungsfunktionen	SOLL	

ID		Anforderung	M / S	Referenzen / Umsetzung
	b	Informationen wer das Scansystem wann und in welcher Weise genutzt hat	SOLL	
	c	Informationen ob eine manuelle Nachbearbeitung des Scanprodukts stattgefunden hat	SOLL	
	d	Fehlgeschlagene Authentisierungsvorgänge und sonstige aufgetretene Fehler	SOLL	
	Protokolldaten müssen gemäß den geltenden datenschutzrechtlichen Bestimmungen verarbeitet und vor unautorisiertem Zugriff geschützt werden.		MUSS	
A.SC.12	*Auswahl geeigneter Bildkompressionsverfahren*			
	Es muss auf die Auswahl geeigneter Bildkompressionsverfahren geachtet werden.		MUSS	

P.2.7 Sicherheitsmaßnahmen bei der Nachbearbeitung

ID	Anforderung	M / S	Referenzen / Umsetzung
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	

ID	Anforderung	M / S	Referenzen / Umsetzung
	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, soll in der Verfahrensanweisung geregelt werden.	SOLL	
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	
A.NB.3	*Durchführung der Vollständigkeitsprüfung*		
	In einem automatisierten Prozess müssen geeignete Maßnahmen zur Sicherstellung der Vollständigkeit getroffen werden. Im Rahmen des Audits werden die getroffenen Maßnahmen zur Vollständigkeitsprüfung erfasst und vom Auditor hinsichtlich der Eignung bewertet.	MUSS	
A.NB.4	*Transfervermerk*		
	Für jedes Scanprodukt soll ein Transfervermerk erstellt werden.	SOLL	

ID	Anforderung		M / S	Referenzen / Umsetzung
	Der Transfervermerk soll insbesondere folgende Aspekte dokumentieren			
	a	Ersteller des Scanprodukts	SOLL	
	b	Technisches und organisatorisches Umfeld des Erfassungsvorgangs	SOLL	
	c	Etwaige Auffälligkeiten während des Scanprozesses	SOLL	
	d	Zeitpunkt der Erfassung	SOLL	
	e	Ergebnis der Qualitätssicherung	SOLL	
	f	die Tatsache, dass es sich um ein Scanprodukt handelt, das bildlich und inhaltlich mit dem Papierdokument übereinstimmt.	SOLL	
	Der Transfervermerk muss mit dem Scanprodukt logisch verknüpft oder in das Scanprodukt integriert werden.		MUSS	
	Der Transfervermerk muss entsprechend dem Schutzbedarf der verarbeiteten Dokumente geschützt werden.		MUSS	

P.2.8 Sicherheitsmaßnahmen bei der Integritätssicherung

ID	Anforderung	M / S	Referenzen / Umsetzung
A.IS.1	*Nutzung geeigneter Dienste und Systeme für den Integritätsschutz*		
	Um eine unerkannte nachträgliche Manipulation der während des Scanprozesses entstehenden Datenobjekte (Scanprodukt, Transfervermerk,	MUSS	

ID	Anforderung	M / S	Referenzen / Umsetzung
	Index- und Metadaten, Protokolldaten, ...) zu verhindern, müssen geeignete Mechanismen zum Schutz deren Integrität eingesetzt werden.		
	Die Widerstandsfähigkeit der Mechanismen muss sich am Schutzbedarf (hinsichtlich der Integrität) der verarbeiteten Datenobjekte orientieren.	MUSS	
	Zum Schutz der Datenobjekte gegen zufällige Änderungen oder aufgrund von Systemfehlern sollen diese jedoch mit einem geeigneten Datensicherungsverfahren gesichert werden.	SOLL	

P.3 Aufbaumodule

P.3.1 Generelle Maßnahmen bei erhöhtem Schutzbedarf

ID	Anforderung	M / S	Referenzen / Umsetzung
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 sollen während des Scanvorgangs keine unbefugten Personen Zugriff auf die Papierdokumente erhalten.	SOLL	
	Es sollen geeignete Maßnahmen für die Beschränkung des Zugriffs auf die sensiblen Papierdokumente getroffen werden. Dies umfasst:		
	a Zugangsbeschränkung zu den Räumlichkeiten in denen die Dokumente verarbeitet werden.	SOLL	

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

P.3.2 Zusätzliche Maßnahmen bei hohen Integritätsanforderungen

ID	Anforderung	M / S	Referenzen / Umsetzung
A.AM.IN.H.1	*Einsatz kryptographischer Mechanismen zum Integritätsschutz*		
	Bei der Verarbeitung von Dokumenten mit Schutzbedarf von zumindest „hoch“	SOLL	

ID	Anforderung	M / S	Referenzen / Umsetzung
	bezüglich der Integrität sollen geeignete kryptographische Mechanismen in Form von fortgeschrittenen elektronischen Signaturen, fortgeschrittenen elektronischen Siegeln und/ oder elektronischen Zeitstempeln zum Einsatz kommen.		
	Sofern keine kryptographischen Mechanismen in Form von fortgeschrittenen elektronischen Signaturen, fortgeschrittenen elektronischen Siegeln und/oder elektronischen Zeitstempeln eingesetzt werden, Andernfalls muss ein schriftlicher Nachweis erbracht werden, dass der für den Integritätsschutz eingesetzte Mechanismus ausreichend widerstandsfähig (siehe Fußnote 31 in A.IS.1) ist.	MUSS	
	Für den Integritätsschutz des dokumentierten Zeitpunktes des Scan-Vorgangs (als Meta-Datum) sollen (qualifizierte) Zeitstempel (Art. 3 Nr. 34 eIDAS) verwendet werden.	SOLL	
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		

ID	Anforderung		M / S	Referenzen / Umsetzung
	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 sollen 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.		SOLL	
A.AM.IN.H.3	*Auswahl eines geeigneten kryptographischen Verfahrens*			
	Sofern kryptographische Verfahren eingesetzt werden, müssen diese für den jeweiligen Zweck geeignet sein.		MUSS	
	Hierbei sollen Verfahren gemäß BSI TR-02102 oder BSI TR-03116 eingesetzt werden.		SOLL	
	Sofern andere kryptographische Verfahren eingesetzt werden, Andernfalls muss ein schriftlicher Nachweis erbracht werden, dass der eingesetzte Mechanismus		MUSS	

ID	Anforderung	M / S	Referenzen / Umsetzung
	ausreichend widerstandsfähig (siehe Fußnote 31 in A.IS.1) ist.		
A.AM.IN.H.4	*Auswahl eines geeigneten kryptographischen Produktes*		
	Zur Integritätssicherung müssen geeignete Produkte hinsichtlich Funktionalität (insb. Stärke und Widerstandsfähigkeit der Sicherheitsmechanismen) und Vertrauenswürdigkeit (z. B. Einsatz veröffentlichter Algorithmen, Prüfung nach anerkannten Sicherheitsstandards wie CC, FIPS-140) eingesetzt werden.	MUSS	
	Da sich die Sicherheitseignung der kryptographischen Algorithmen ändern kann, soll auf eine leichte Austauschbarkeit der entsprechenden Komponenten geachtet werden.	SOLL	
	Um eine sichere Nutzung der kryptographischen Produkte zu gewährleisten, müssen die notwendigen Einsatzbedingungen und sonstigen Empfehlungen des Herstellers berücksichtigt werden.	MUSS	
A.AM.IN.H.5	*Langfristige Datensicherung bei Einsatz kryptographischer Verfahren*		
	Für die eingesetzten kryptographischen Verfahren soll die Eignung der verwendeten Algorithmen und Parameter regelmäßig evaluiert werden.	SOLL	
	Sofern der Beweiswert von qualifiziert signierten, gesiegelten oder	MUSS	

ID	Anforderung	M / S	Referenzen / Umsetzung
	zeitgestempelten Daten über längere Zeiträume erhalten bleiben soll, muss rechtzeitig vor Ablauf der Eignung der kryptographischen Verfahren eine Nachsignatur erfolgen.		
	Für den Erhalt der Beweiskraft kryptographisch signierter Daten wird der Einsatz der in der BSI TR-03125 spezifizierten Verfahren empfohlen.	SOLL	
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 Netzwerk-segment darf nur entkoppelt (Proxy/Gateway) und nur bei Initiierung von innen möglich sein.	MUSS	

P.3.3 Zusätzliche Maßnahmen bei sehr hohen Integritätsanforderungen

ID	Anforderung	M / S	Referenzen / Umsetzung
A.AM.IN.SH.1	*4-Augen-Prinzip*		
	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	MUSS	

ID	Anforderung	M / S	Referenzen / Umsetzung
	durchgeführt werden. ein 4-Augen-Prinzip umgesetzt werden.		
A.AM.IN.SH.2	*Einsatz qualifizierter elektronischer Signaturen oder Siegel und Zeitstempel*		
	Sofern Datenobjekte mit einem Schutzbedarf von „sehr hoch“ bzgl. der Integrität verarbeitet werden, für Datenobjekte die Verkehrsfähigkeit gefordert ist und die im Rahmen des Scanprozesses entstandenen Datenobjekte (Scanprodukt, Transfervermerk, Index- und Metadaten, Protokolldaten) voraussichtlich als Beweismittel genutzt werden, sollen für die Integritätssicherung des Scanproduktes bzw. des Transfervermerks qualifizierte elektronische Signaturen oder qualifizierte elektronische Siegel und qualifizierte Zeitstempel eingesetzt werden.	SOLL	
	Sofern in diesem Fall andere Sicherheitsmechanismen für die Integritätssicherung eingesetzt werden, Andernfalls muss ein schriftlicher Nachweis erbracht werden, dass der für den Integritätsschutz eingesetzte Mechanismus ausreichend widerstandsfähig (siehe Fußnote 31 in A.IS.1) ist.	MUSS	
A.AM.IN.SH.3	*Eigenständiges Netzsegment*		

ID	Anforderung	M / S	Referenzen / Umsetzung
	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	
A.AM.IN.SH.4	*Kennzeichnung der Dokumente bzgl. Sensitivität*		
	Dokumente, die einen Schutzbedarf von „sehr hoch“ bzgl. der Integrität besitzen, sollen als solche gekennzeichnet werden.	SOLL	
	Die Kennzeichnung soll deutlich sichtbar angebracht werden.	SOLL	

P.3.4 Zusätzliche Maßnahmen bei hohen Vertraulichkeitsanforderungen

ID	Anforderung	M / S	Referenzen / Umsetzung
A.AM.VT.H.1	*Sensibilisierung und Verpflichtung der Mitarbeiter*		
	Bei der Verarbeitung von Dokumenten mit einem Schutzbedarf hinsichtlich der Vertraulichkeit von zumindest „hoch“ müssen die Mitarbeiter bzgl. der Sicherheitsmaßnahmen und der sicherheitsbewussten Handhabung von	MUSS	

ID	Anforderung	M / S	Referenzen / Umsetzung
	Dokumenten, Daten und IT-Systemen und der zu ergreifenden Vorsichtsmaßnahmen sensibilisiert und geschult werden.		
	Mitarbeiter müssen durch eine explizite Verfahrensanweisung auf die Einhaltung der einschlägigen Gesetze, Vorschriften und Regelungen verpflichtet werden.	MUSS	
A.AM.VT.H.2	*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	
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

ID	*Anforderung*	*M / S*	*Referenzen / Umsetzung*
-	Bei der Verarbeitung von Verschlusssachen müssen die Anforderungen der VSA berücksichtigt werden.	MUSS	
A.AM.VT.SH.1	*Kennzeichnung der Dokumente bzgl. Sensitivität*		
	Dokumente, die einen Schutzbedarf von „sehr hoch“ bzgl. der Vertraulichkeit besitzen, sollen als solche gekennzeichnet werden.	SOLL	
	Die Kennzeichnung soll deutlich sichtbar angebracht werden.	SOLL	
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 soll der Datenträger ausgebaut und mit einem geeigneten Verfahren zuverlässig gelöscht oder zerstört werden.	SOLL	
	Kryptographische Schlüssel, die im zu entsorgenden Scanner vorgehalten werden, müssen zuverlässig gelöscht oder deaktiviert werden.	MUSS	
A.AM.VT.SH.3	*Besondere Zuverlässigkeit und Vertrauenswürdigkeit der Mitarbeiter*		

ID	Anforderung	M / S	Referenzen / Umsetzung
	Sofern Dokumente gescannt werden, deren Schutzbedarf hinsichtlich der Vertraulichkeit „sehr hoch“ ist, soll sichergestellt werden, dass die Mitarbeiter, die für den Scanprozess verantwortlich sind und den Prozess durchführen besonders zuverlässig und vertrauenswürdig sind.	SOLL	
A.AM.VT.SH.4	*Verschlüsselte Datenübertragung innerhalb des Scansystems*		
	Bei der Verarbeitung von Datenobjekten mit einem Schutzbedarf von „sehr hoch“ bzgl. der Vertraulichkeit soll die Datenübertragung zwischen Scanner, Scan-Workstation, Scan-Cache und anderen damit zusammenhängenden Systemen durch geeignete Verschlüsselungsverfahren gemäß BSI TR-02102 oder BSI TR-03116 erfolgen.	SOLL	
	Andernfalls muss ein geeigneter Nachweis erbracht werden, dass diese Kommunikationsverbindungen durch alternative Maßnahmen ausreichend geschützt sind.	MUSS	

P.3.6 Zusätzliche Maßnahmen bei hohen Verfügbarkeitsanforderungen

ID	Anforderung	M / S	Referenzen / Umsetzung
A.AM.VF.H.1	*Erweiterte Qualitätssicherung der Scanprodukte*		
	Bei einem Schutzbedarf der Datenobjekte von „hoch“ bezüglich der Verfügbarkeit soll	SOLL	

ID	Anforderung	M / S	Referenzen / Umsetzung
	die Qualitätskontrolle der Scanprodukte durch eine vollständige Sichtkontrolle erfolgen. 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. In regelmäßigen zeitlichen Abständen MUSS die Qualitätssicherung durch eine vollständige Sichtkontrolle erfolgen		
	Falls keine vollständige Sichtkontrolle realisiert wird, SOLLEN automatische Mechanismen zur Qualitätskontrolle eingesetzt werden, wie z.B. eine automatische Erkennung von Leerseiten, von unzureichender Bildqualität oder die Prüfung der Seitenzahl (z.B. gegen die auf Vorblättern angegebenen Meta-Daten).	SOLL	
	Beim Einsatz automatisierter Mechanismen MUSS eine manuelle Prüfung der identifizierten Probleme und Auffälligkeiten erfolgen.	MUSS	
A.AM.VF.H.2	*Fehlertolerante Protokolle und redundante Datenhaltung*		
	Bei Schutzbedarf „hoch“ bzgl. der Verfügbarkeit wird die Verwendung eines fehlertoleranten Übertragungsprotokolls sowie eine redundante Datenhaltung empfohlen.	SOLL	

P.3.7 Zusätzliche Maßnahmen bei sehr hohen Verfügbarkeitsanforderungen

ID	*Anforderung*	*M / S*	*Referenzen / Umsetzung*
A.AM.VF.SH.1	*Vollständige Sichtkontrolle zur Qualitätssicherung der Scanprodukte*		
	Bei einem Schutzbedarf der Datenobjekte von „sehr hoch“ bzgl. der Verfügbarkeit soll die Qualitätskontrolle der Scanprodukte durch eine vollständige Sichtkontrolle erfolgen.	SOLL	
A.AM.VF.SH.2	*Test der Geräte und Einstellungen mit ähnlichen Dokumenten*		
	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	

P4. Weitere Ausführungen

Literaturverzeichnis

[BSI-TR03138] Bundesamt für Sicherheit in der Informationstechnik (BSI): Ersetzendes Scannen, Technische Richtlinie (TR) des BSI Nr. 03138 (TR RESISCAN), Version 1.4, 2019

[BSI-TR03138-R] Bundesamt für Sicherheit in der Informationstechnik (BSI): Ersetzendes Scannen - Anwendungshinweis R: Unverbindliche rechtliche Hinweise, Anwendungshinweis R, Version 1.2, 2018, Technische Richtlinie (TR) des BSI Nr. 03138 (TR RESISCAN), Version 1.2, 2018