Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik,
Postfach 20 03 63, 53133 Bonn

Einschreiben mit Rückschein
Ratiodata AG
Herr Frank Holtgrefe
Lyoner Str. 9

60528 Frankfurt a. Main
Deutschland

Christine Hau

HAUSANSCHRIFT
Bundesamt für Sicherheit in
der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL +49 (0) 228 99 9582-5848
FAX +49 (0) 228 99 10 9582-5848

zertifizierung-tr@bsi.bund.de
https://www.bsi.bund.de

Az.: SZ25-720-07-00
Datum: 01. Dezember 2020
Seite 1 von 1

Betreff: **Zertifizierung des Prüfgegenstands „Scan- & Dokumenten-Services der Ratiodata AG“**

Bezug: Ihr Antrag auf Zertifizierung nach Technischen Richtlinien vom 07. September 2018

Anlagen: -5-

Sehr geehrter Herr Holtgrefe,

anbei erhalten Sie die korrigierten Zertifizierungsdokumente wie den Konformitätsbescheid, das Zertifikat nach Technischen Richtlinien sowie den zugehörigen Konformitätsreport zum Zertifizierungsverfahren

BSI-K-TR-0320-2020
Scan- & Dokumentenservice der Ratiodata AG

Bitte senden Sie die beiliegende Empfangsbestätigung unterschrieben an das BSI zurück.

Mit dem beiliegenden Formular (→ Widerspruchsverzicht) können Sie vor Ablauf der Monatsfrist auf Widerspruch verzichten. Der Konformitätsbescheid wird in diesem Fall unmittelbar rechtskräftig und eine Veröffentlichung des Zertifizierungsergebnisses kann unverzüglich erfolgen.

Im Auftrag

Hau

Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53113 Bonn

Ratiodata AG
Lyoner Str. 9

60528 Frankfurt a.M.

Michael Krämer

HAUSANSCHRIFT
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL +49 (0) 228 99 9582-5974
FAX +49 (0) 228 99 9582-5974

zertifizierung-tr@bsi.bund.de
https://www.bsi.bund.de

AZ: SZ25-720-07-00
Datum 31. März 2020

Betreff: **Zertifizierung des Prüfgegenstands „Scan- & Dokumenten-Services“ der Ratiodata AG**

Bezug: Ihr Antrag auf Zertifizierung nach Technischen Richtlinien vom 07. September 2018

Anlagen: Zertifikat nach Technischen Richtlinien
Konformitätsreport

KONFORMITÄTSBESCHEID

Für den Prüfgegenstand „Scan- & Dokumenten-Services“ der Ratiodata AG wird das Zertifikat nach Technischen Richtlinien BSI-K-TR-0320-2020 mit Auflagen erteilt.

Das Zertifikat nach Technischen Richtlinien BSI-K-TR-0320-2020 ist gültig bis zum 30. März 2023 unter der Voraussetzung, dass die nachfolgenden Auflagen fristgerecht erfüllt werden.

Aufgrund der Ergebnisse der Konformitätsprüfung werden folgende Auflagen festgelegt:

1. Für die im Rahmen der Konformitätsprüfung festgestellten Abweichungen sind die in Kapitel 8.2 des Konformitätsreports BSI-K-TR-0320-2020 aufgeführten, erforderlichen Maßnahmen bis zur nächsten Re-Zertifizierung des Prüfgegenstands durchzuführen.

Hinsichtlich der Kosten des Zertifizierungsverfahrens ergeht ein gesonderter Kostenbescheid.

Begründung:

Sie sind Hersteller/Betreiber des Prüfgegenstands „Scan- & Dokumenten-Services“ der Ratiodata AG. Mit Antrag vom 07. September 2018, hier vollständig eingegangen am 11. September 2018, haben Sie beim BSI für diesen Prüfgegenstand eine Zertifizierung nach Technischen Richtlinien beantragt.

Beantragt wurde die Prüfung der Konformität zur Technischen Richtlinie BSI TR-03138 – Technische Richtlinie Ersetzendes Scannen (TR-RESISCAN), Version 1.4.

Die Konformitätsprüfung wurde von dem vom BSI zertifizierten Auditor Dr. Wolfgang Böhmer, Dr. Böhmer Consulting, Am Stiftsberg – Sackgasse 4, 63739 Aschaffenburg durchgeführt.

Die Durchführung der Konformitätsprüfung wurde durch die Zertifizierungsstelle des BSI überwacht.

Auf der Grundlage des vom Auditor vorgelegten Prüfberichts wurden das Zertifikat nach Technischen

Richtlinien und der Konformitätsreport erstellt.

Die Ergebnisse des Zertifizierungsverfahrens sind im Detail im beiliegenden Konformitätsreport enthalten.

Ihrem Antrag auf Erteilung eines Zertifikats nach Technischen Richtlinien konnte mit Auflagen entsprochen werden.

Das Zertifikat ist gemäß § 12 Abs. 2 BSIZertV (BSI-Zertifizierungs- und Anerkennungsverordnung vom 17. Dezember 2014, BGBl. I S. 2231) zu befristen. Die Geltungsdauer eines Zertifikats nach der Technischen Richtlinie BSI TR-03138 beträgt drei Jahre ab Erteilungsdatum. Das Zertifikat BSI-K-TR-0320-2020 ist dementsprechend gültig bis zum 30. März 2023 unter der Voraussetzung, dass die o. g. Auflagen fristgerecht erfüllt werden.

Hinweise:

Dieses Zertifikat gilt nur im Zusammenhang mit dem vollständigen Konformitätsreport und ausschließlich für die geprüfte und im Konformitätsreport angegebene Version bzw. Konfiguration des Prüfgegenstands.

Werden während der Gültigkeitsdauer wesentliche Änderungen am zertifizierten Prüfgegenstand vorgenommen (wie z. B. größere Änderungen am Scan-System/-Prozess, Änderungen im Managementsystem, der Organisation, im Outsourcing, Standortwechsel, ...), sind diese dem BSI schriftlich mitzuteilen. Das BSI entscheidet dann, ggf. unter Einbeziehung der Prüfstelle/des Auditors, ob eine vorzeitige Re-Zertifizierung erforderlich ist.

Dieses Zertifikat ist keine Empfehlung des genannten Prüfgegenstands durch das Bundesamt für Sicherheit in der Informationstechnik. Eine Gewährleistung für den genannten Prüfgegenstand durch das Bundesamt für Sicherheit in der Informationstechnik ist weder enthalten noch zum Ausdruck gebracht.

Darüber hinaus gelten die im zugehörigen Konformitätsreport unter Punkt 3 aufgeführten “Hinweise für den Antragsteller”.

Das Zertifizierungsergebnis, das Zertifikat nach Technischen Richtlinien sowie der zugehörige Konformitätsreport werden durch das BSI veröffentlicht.

Rechtsbehelfsbelehrung:

Gegen diesen Bescheid kann innerhalb eines Monats nach Bekanntgabe Widerspruch erhoben werden. Der Widerspruch ist schriftlich oder zur Niederschrift beim Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189, 53175 Bonn einzulegen.

Im Auftrag

Amendola

Bundesamt
für Sicherheit in der
Informationstechnik

Zertifikat

nach Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik

BSI-K-TR-0320-2020

Scan- & Dokumenten-Services

der	Ratiodata AG
Konformität zu:	**BSI TR-03138** – Technische Richtlinie Ersetzendes Scannen (TR-RESISCAN)
gültig bis:	30. März 2023

Die Konformität des Prüfgegenstands „Scan- & Dokumenten-Services“ der Ratiodata AG zur Technischen Richtlinie BSI TR-03138 wurde von dem vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten Auditor Dr. Wolfgang Böhmer, Dr. Böhmer Consulting überprüft und vom BSI bestätigt.

Als Prüfgrundlage für die Konformitätsprüfung dienten:

BSI TR-03138 – Technische Richtlinie Ersetzendes Scannen
Version 1.4 vom 03. September 2019

BSI TR-03138-P – Technische Richtlinie Ersetzendes Scannen, Anlage P: Prüfspezifikation
Version 1.4 vom 03. September 2019

Der Prüfgegenstand erfüllt die Anforderungen der Technischen Richtlinie BSI TR-03138.

Dieses Zertifikat gilt nur in Verbindung mit dem vollständigen Konformitätsreport BSI-K-TR-0320-2020. Die Gültigkeit ist ausschließlich auf die geprüfte und im Konformitätsreport angegebene Version und Konfiguration des Prüfgegenstands beschränkt.

Das Zertifizierungsverfahren wurde in Übereinstimmung mit den Bestimmungen des BSI-Schemas zur Zertifizierung nach Technischen Richtlinien durchgeführt.

Dieses Zertifikat ist keine Empfehlung des genannten Prüfgegenstands durch das Bundesamt für Sicherheit in der Informationstechnik. Eine Gewährleistung für den genannten Prüfgegenstand durch das Bundesamt für Sicherheit in der Informationstechnik ist weder enthalten noch zum Ausdruck gebracht.

Bonn, den 31. März 2020
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag

Sandro Amendola
Abteilungspräsident

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, D-53175 Bonn • Postfach 20 03 63, D-53113 Bonn
Tel.: +49 (0)228 9582-0 • Fax: +49 (0)228 9582-5400 • Infoline: +49 (0)800 274-1000 • Internet: www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Konformitätsreport

BSI-K-TR-0320-2020

Scan- & Dokumenten-Services

der

Ratiodata AG
Lyoner Str. 9, 60528 Frankfurt a. M., Deutschland

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, D-53175 Bonn ♦ Postfach 20 03 63, D-53113 Bonn
Tel.: +49 (0)228 9582-0 ♦ Fax: +49 (0)228 9582-5400 ♦ Internet: www.bsi.bund.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Vorbemerkung

Die Zertifizierung von IT-Produkten oder -Systemen – im Folgenden Prüfgegenstand genannt – nach Technischen Richtlinien (TR) wird auf Veranlassung des Herstellers – im folgenden Antragsteller genannt – durchgeführt.

Technische Richtlinien, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellt und veröffentlicht werden, bilden die Grundlage für Konformitätsprüfungen. Anhand einer Konformitätsprüfung wird sichergestellt, dass ein Prüfgegenstand die (sicherheits-) technischen, funktionalen und qualitativen Anforderungen einer TR erfüllt.

Konformitätsprüfungen werden von den vom BSI gemäß DIN ISO/IEC 17025 anerkannten Prüfstellen oder zertifizierten Auditoren gemäß den in der jeweiligen TR definierten Prüfspezifikationen und Tests durchgeführt. Die Konformitätsprüfung eines Prüfgegenstands erfolgt in Übereinstimmung mit den Bestimmungen des entsprechenden BSI-Schemas zur Zertifizierung nach Technischen Richtlinien.

Für jedes Zertifizierungsverfahren nach TR führt das BSI eine Prüfbegleitung durch, um einheitliches Vorgehen, einheitliche Interpretation der Kriterienwerke und einheitliche Bewertungen sicherzustellen.

Das Ergebnis eines Zertifizierungsverfahrens nach TR wird in einem abschließenden Konformitätsreport zusammengefasst.

Das im Rahmen einer Zertifizierung nach TR ausgestellte Zertifikat ist keine Empfehlung des Prüfgegenstands durch das Bundesamt für Sicherheit in der Informationstechnik. Eine Gewährleistung für den Prüfgegenstand durch das BSI ist weder enthalten noch zum Ausdruck gebracht.

2 Grundlagen des Zertifizierungsverfahrens

Das Zertifizierungsverfahren wurde vom Bundesamt für Sicherheit in der Informationstechnik nach Maßgabe der folgenden Vorgaben durchgeführt:

- BSI-Gesetz – Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009, Bundesgesetzblatt Teil I Nr. 54, S. 2821, [BSIG]
- BSI-Zertifizierungs- und Anerkennungsverordnung – Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSIZertV), vom 17. Dezember 2014, Bundesgesetzblatt Teil I Nr. 61, S. 2231, [BSIZertV]
- Besondere Gebührenverordnung des Bundesministeriums des Inneren, für Bau und Heimat für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (Besondere Gebührenverordnung BMI, BMIBGebV) vom 02. September 2019, Bundesgesetzblatt I, S. 1359, [BMIBGebV]
- Verfahrensbeschreibung zur Zertifizierung von Produkten, Version 2.4 vom 09. September 2019, [VB-Produkte]
- Anforderungen an Antragsteller zur Zertifizierung von Produkten nach Technischen Richtlinien, Version 1.3 vom 09. September 2019, [TR-Produkte]

3 Hinweise für den Antragsteller

1. Das vom BSI erteilte Zertifikat nach Technischen Richtlinien BSI-K-TR-0320-2020 ist nur in Zusammenhang mit dem vollständigen Konformitätsreport gültig.
2. Die Gültigkeit des Zertifikats erstreckt sich ausschließlich auf die geprüfte Version bzw. Konfiguration des Prüfgegenstands. Alle geprüften Komponenten des Prüfgegenstands und deren Versionsstände sind in Kapitel 7 des Konformitätsreports festgeschrieben.
3. Die Gültigkeit eines Zertifikats nach der Technischen Richtlinie BSI TR-03138 (TR-RESISCAN) beträgt drei Jahre.
4. Werden während der Gültigkeitsdauer wesentliche Änderungen (wie z. B. größere Änderungen am Scan-System/-Prozess, Änderungen am Managementsystem, der Organisation, im Outsourcing, Standortwechsel, ...) am zertifizierten Prüfgegenstand vorgenommen, sind diese dem BSI schriftlich mitzuteilen. Das BSI entscheidet dann, ggf. unter Einbeziehung der Prüfstelle/ des Auditors, ob eine vorzeitige Re-Zertifizierung erforderlich ist.
5. Nur dem Zertifikat entsprechende Ausführungen des Prüfgegenstands dürfen als vom BSI zertifiziert bezeichnet und als solche beworben werden. Stellt das BSI diesbezüglich eine Zuwiderhandlung fest, erfolgt eine Abmahnung des Antragstellers. Daneben ist das BSI berechtigt, den Eintrag des Prüfgegenstands von der Veröffentlichungsliste der nach Technischen Richtlinien erteilten Zertifikate auf der BSI-Webseite zu streichen.
6. Das BSI kann den Antragsteller jederzeit auffordern, ein dem Zertifikat entsprechendes Exemplar des Prüfgegenstands aus der laufenden Produktion zur Überprüfung bereitzustellen. Kommt der Antragsteller der Aufforderung nicht innerhalb einer gesetzten Frist nach, ist das BSI berechtigt, den Eintrag des Prüfgegenstands von der Veröffentlichungsliste der nach Technischen Richtlinien erteilten Zertifikate auf der BSI-Webseite zu streichen.

4 Antrag

Für den in Kapitel 7 genannten Prüfgegenstand wurde von der

Ratiodata AG
Lyoner Str. 9
60528 Frankfurt a. M.

Deutschland

Ansprechpartner:

Herr Frank Holtgrefe (frank.holtgrefe@ratiodata.de)

mit Antragsdatum 07. September 2018 (Eingangsdatum BSI: 11. September 2018) beim BSI eine erstmalige Zertifizierung nach Technischen Richtlinien beantragt.

5 Prüfbereich und Prüfgrundlage

Beantragt wurde eine Zertifizierung nach der Technischen Richtlinie:

BSI TR-03138 – Technische Richtlinie Ersetzendes Scannen

Die Konformitätsprüfung nach der Technischen Richtlinie BSI TR-03138 erfolgte für den Prüfbereich:

BSI TR-03138 – Ersetzendes Scannen (TR-RESISCAN)

Die Prüfgrundlage für Konformitätsprüfungen in diesen Prüfbereichen bildeten folgende Dokumente:

BSI TR-03138 – Technische Richtlinie Ersetzendes Scannen, Version 1.4 vom 03. September 2019, [BSI TR-03138]

BSI TR-03138-P – Technische Richtlinie Ersetzendes Scannen, Anlage P: Prüfspezifikation, Version 1.4 vom 03. September 2019, [BSI TR-03138-P]

6 Prüfstelle

Mit der Durchführung der Konformitätsprüfung wurde folgender Auditor beauftragt:

Dr. Wolfgang Böhmer
Dr. Böhmer Consulting
Am Stiftsberg – Sackgasse 4

63739 Aschaffenburg

E-Mail: mail@wolfgang-boehmer.eu

7 Prüfgegenstand

7.1 Beschreibung des Prüfgegenstands

Prüfgegenstand ist das IT-Produkt/-System:

Scan- & Dokumenten-Services der Ratiodata AG

Bei dem Prüfgegenstand handelt es sich um die spezifischen Prozesse des ersetzenden Scannens von Eingangspost mit z.T. personenbezogenen Daten gemäß BSI TR-03138 (TR-RESISCAN) der Ratiodata AG an den Standorten Münster (Gustav-Stresemann-Weg 29, 48155 Münster) und Duisburg (Dr.-Alfred-Herrhausen-Allee 46, 47228 Duisburg).

7.2 Komponenten des Prüfgegenstands

Die einzelnen Komponenten des Prüfgegenstands (IT-Systeme, Hard-/Software, Kommunikationsverbindungen, Datenobjekte, ...) wurden im Rahmen einer Strukturanalyse identifiziert. Der Prüfbericht (→ Kapitel 9) des Auditors enthält eine vollständige Aufstellung aller Komponenten.

7.3 Implementation Conformance Statement

Das Implementation Conformance Statement (ICS) enthält die für die Durchführung der Konformitätsprüfung benötigten Informationen zum Prüfgegenstand und ist zur Festlegung des Prüfumfangs erforderlich. Im Falle der [BSI TR-03138] ergibt sich der Prüfumfang aus der Schutzbedarfsanalyse des Prüfgegenstands.

Der Schutzbedarf des Prüfgegenstands wurde als „hoch“ hinsichtlich des Schutzziels Vertraulichkeit sowie „normal“ hinsichtlich der Integrität und Verfügbarkeit eingestuft.

Daraus ergibt sich für die Konformitätsprüfung folgender Prüfumfang:

Basismodule	*A.G, A.O, A.P, A.T, A.DV, A.SC, A.NB, A.IS*
Aufbaumodule	*A.AM.G, A.AM.VT.H*

8 Konformitätsprüfung

Die Konformitätsprüfung gemäß [BSI TR-03138-P] wurde im Zeitraum Dezember 2019 bis Januar 2020 von dem beauftragten Auditor durchgeführt.

Im Rahmen der Konformitätsprüfung wurde der Prüfgegenstand gemäß den Prüfvorgaben der [BSI TR-03138-P] untersucht.

Der vom Auditor vorgelegte Prüfbericht enthält detaillierte Beschreibungen der durchgeführten Testfälle, der jeweils zu erfüllenden Anforderungen/Vorgaben sowie eine vollständige Aufstellung der erzielten Prüfergebnisse.

8.1 Konformitätsprüfung gemäß BSI TR-03138, Anlage P

Tabelle 1 enthält eine Zusammenfassung der durchgeführten Testfälle. Für eine detaillierte Beschreibung der Testfälle sei auf [BSI TR-03138-P] verwiesen.

Tabelle 1: Ergebnisse der Konformitätsprüfung gemäß BSI TR-03138-P

Nr	Testfall	Bewertung
Basismodule		
01	Strukturanalyse	Pass
02	Schutzbedarfsanalyse	Pass
Grundlegende Anforderungen		
03	A.G.1	Pass
Organisatorische Anforderungen		
04	A.O.1	Pass
05	A.O.2	Pass
06	A.O.3	Pass
07	A.O.4	Pass
08	A.O.5	Pass
Personelle Anforderungen		
09	A.P.1	Pass
10	A.P.2	Pass
11	A.P.3	Pass
12	A.P.4	Pass
13	A.P.5	Pass

Nr	Testfall	Bewertung
Technische Anforderungen		
14	A.T.1	Pass
15	A.T.2	Pass
16	A.T.3	Pass
17	A.T.4	Pass
Sicherheitsmaßnahmen bei der Dokumentenvorbereitung		
18	A.DV.1	Pass
19	A.DV.2	Pass
Sicherheitsmaßnahmen beim Scannen		
20	A.SC.1	Pass
21	A.SC.2	Pass
22	A.SC.3	Pass
23	A.SC.4	Pass
24	A.SC.5	Pass
25	A.SC.6	Pass
26	A.SC.7	Pass
27	A.SC.8	Pass

Nr	Testfall	Bewertung
28	A.SC.9	Pass
29	A.SC.10	Pass
30	A.SC.11	Pass
31	A.SC.12	Pass
Sicherheitsmaßnahmen bei der Nachbearbeitung		
32	A.NB.1	Pass
33	A.NB.2	Pass
34	A.NB.3	Pass
35	A.NB.4	Pass
Sicherheitsmaßnahmen bei der Integritätssicherung		
36	A.IS.1	Pass
Aufbaumodule		
Generelle Maßnahmen bei erhöhtem Schutzbedarf		
37	A.AM.G.1	Pass
38	A.AM.G.2	Pass
39	A.AM.G.3	Pass
Zusätzliche Maßnahmen bei hohen Integritätsanforderungen		
40	A.AM.IN.H.1	n.a.
41	A.AM.IN.H.2	n.a.
42	A.AM.IN.H.3	n.a.
43	A.AM.IN.H.4	n.a.
44	A.AM.IN.H.5	n.a.
45	A.AM.IN.H.6	n.a.

Nr	Testfall	Bewertung
Zusätzliche Maßnahmen bei sehr hohen Integritätsanforderungen		
46	A.AM.IN.SH.1	n.a.
47	A.AM.IN.SH.2	n.a.
48	A.AM.IN.SH.3	n.a.
49	A.AM.IN.SH.4	n.a.
Zusätzliche Maßnahmen bei hohen Vertraulichkeitsanforderungen		
50	A.AM.VT.H.1	Pass
51	A.AM.VT.H.2	Pass
52	A.AM.VT.H.3	Pass
Zusätzliche Maßnahmen bei sehr hohen Vertraulichkeitsanforderungen		
53	VSA	n.a.
54	A.AM.VT.SH.1	n.a.
55	A.AM.VT.SH.2	n.a.
56	A.AM.VT.SH.3	n.a.
57	A.AM.VT.SH.4	n.a.
Zusätzliche Maßnahmen bei hohen Verfügbarkeitsanforderungen		
58	A.AM.VF.H.1	n.a.
59	A.AM.VF.H.2	n.a.
Zusätzliche Maßnahmen bei sehr hohen Verfügbarkeitsanforderungen		
60	A.AM.VF.SH.1	n.a.
61	A.AM.VF.SH.2	n.a.

H = Hinweis, E = Empfehlung, AG = geringfügige Abweichung,
AS = schwerwiegende Abweichung

8.2 Festgestellte Abweichungen

Sämtliche im Rahmen der Konformitätsprüfung festgestellten Abweichungen und Empfehlungen wurden vom Auditor im Anhang zum Prüfbericht „Liste der Abweichungen und Empfehlungen“ vom 10.01.2020 festgehalten.

8.2.1 Empfehlungen zur Verfahrensdokumentation

Festgestellter Sachverhalt: Es wurden verschiedene Punkte identifiziert, die eine Revision der Verfahrensdokumentation erfordern. Dies betrifft insbesondere die Dokumente bzw. Richtlinien Risikomanagement, Verfahrensanweisung „Ersetzendes Scannen“ gemäß BSI TR-03138, Prozessbeschreibung Dokumentendigitalisierung in folgenden Punkten:

- Auf der Seite 10 in der Richtlinie Risikomanagement wird von drei „Grundgefährdungen“ gesprochen. Es muss „Grundwerte“ heißen. (E-1)
- In allen Dokumenten wird die Bildbeschriftung und Tabellenbeschriftung sehr unterschiedlich geführt. In der Verfahrensanweisung und Risikoanalyse fehlen diese völlig. In den Arbeitsanweisungen sind diese z. T. Vorhanden. (E-2)
- In den Dokumenten Risikomanagement, Verfahrensanweisung und Prozessbeschreibung ist das Layout ist unterschiedlich. Mal ist ein Vorwort vorhanden mal nur eine Einleitung. Mal ist die Einordnung - Kompendium vorhanden mal nicht. (E-3)
- Es sollte in der schriftlich fixierten Ordnung ein Dokumententyp unterhalb der Richtlinie und oberhalb der Prozesse eingeführt werden. Es könnte der Typ Verfahrensanweisung oder Konzeption sein. (E-4)

Bewertung: Empfehlung

Empfohlene Maßnahmen: Es wird empfohlen, die Dokumente entsprechend er o. g. Punkte zu überarbeiten.

8.2.2 Revision der Verfahrensdokumentation

Festgestellter Sachverhalt: Es wurden verschiedene Punkte identifiziert, die eine Revision der Arbeitsanweisungen und Verfahrensdokumentation erfordern:

- Alle Dokumente, z.B. Verfahrensanweisungen werden als Richtlinien betitelt. Die sogenannte Richtlinie enthält keine steuernde Begriffe wie MUSS, KANN, SOLL, DARF, etc. (AG-1)
- Sämtliche Arbeitsanweisungen (AAW) sind aus der jährlichen Revision gelaufen. (AG-6, AG-13)
- Richtlinie Risikomanagement: Eine eindeutige Zuweisung der EW (Eintrittswahrscheinlichkeit (niedrig, mittel, hoch, sehr hoch) zu den Ziffern 1,2,3,4 ist nicht gegeben. (AG-7)

- Richtlinie Risikomanagement: Kapitel 3.2 Kontext definieren. Der Kontext zu dem Geschäftsprozess Dokumentendigitalisierung" ist nicht nachvollziehbar. (AG-8)
- Richtlinie Risikomanagement: Es ist nicht nachvollziehbar wie das Risikomanagement und seine Vorgehensweise mit der Verfahrensanweisung, Kapitel 2.4.3 bis 2.4.6 in Beziehung steht. (AG-9)
- Richtlinie Risikomanagement: Es werden Begriffe höchst unterschiedlich verwendet wie z.B. Gefährdungsanalyse, Grundgefährdung, Schutzbedarfsanalyse, Risikobeurteilung, Risikobewertung, IS-Risikobeurteilung, Gefährdungen, Risiko, Risikoanalyse, Risikobehandlung. (AG-10)
- Richtlinie Risikomanagement: Die Risikobehandlung im Kapitel 3.3 ist lediglich aufgeführt, jedoch sind keine Schwellwerte angegeben. (AG-11)
- Richtlinie Risikomanagement: Im Kapitel 3.5 wird das Monitor und Überwachung der Maßnahmenumsetzung beschrieben, es ist jedoch nicht nachvollziehbar, wie diese zu dem SoA der ISO27001 steht. (AG-12)

Bewertung: geringfügige Abweichung(en)

Erforderliche Maßnahmen: Verfahrensdokumente und Arbeitsanweisungen sind entsprechend der o. g. Punkte zu überarbeiten und einer jährlichen Revision zu unterziehen.

9 Ergebnis der Konformitätsprüfung

Die vollständigen Ergebnisse der Konformitätsprüfung sind in folgendem Prüfbericht und seinen zugehörigen Anlagen enthalten:

Bericht im Rahmen de Zertifizierung nach TR-03138
Auditierte Institution: Ratiodata AG
Standort Münster und Duisburg

Zertifizierungskennung: BSI-K-TR-0320-2020
Prüfbericht Version 1.0
Erstellungsdatum: 25. März 2020

Die Vollständigkeit und Widerspruchsfreiheit des vorgelegten Prüfberichts wurde durch das Bundesamt für Sicherheit in der Informationstechnik verifiziert und bestätigt.

Die im Rahmen der Konformitätsprüfung erzielten Ergebnisse lassen sich wie folgt zusammenfassen:

- im Rahmen der Konformitätsprüfung der Basismodule gemäß BSI TR-03138 wurden
  - alle untersuchten, relevanten Testfälle des Moduls A.G mit „Pass“ bewertet
  - alle untersuchten, relevanten Testfälle des Moduls A.O mit „Pass“ bewertet
  - alle untersuchten, relevanten Testfälle des Moduls A.P mit „Pass“ bewertet
  - alle untersuchten, relevanten Testfälle des Moduls A.T mit „Pass“ bewertet
  - alle untersuchten, relevanten Testfälle des Moduls A.DV mit „Pass“ bewertet
  - alle untersuchten, relevanten Testfälle des Moduls A.SC mit „Pass“ bewertet
  - alle untersuchten, relevanten Testfälle des Moduls A.NB mit „Pass“ bewertet
  - alle untersuchten, relevanten Testfälle des Moduls A.IS mit „Pass“ bewertet.
- im Rahmen der Konformitätsprüfung der Aufbaumodule gemäß BSI TR-03138 wurden
  - alle untersuchten, relevanten Testfälle des Moduls A.AM.G mit „Pass“ bewertet;
  - alle untersuchten, relevanten Testfälle des Moduls A.AM.VT.H mit „Pass“ bewertet.

Das erzielte Gesamtergebnis der Konformitätsprüfung ist: Pass (mit Auflagen)

10 Ergebnis des Zertifizierungsverfahrens nach TR

Die Konformität des Prüfgegenstands zur Technischen Richtlinie BSI TR-03138 wird vom Bundesamt für Sicherheit in der Informationstechnik für den untersuchten Prüfbereich mit dem Zertifikat nach Technischen Richtlinien BSI-K-TR-0320-2020 vom 31. März 2020 mit Auflagen bestätigt.

Das Zertifikat nach Technischen Richtlinien BSI-K-TR-0320-2020 ist gültig bis zum 30. März 2023 unter der Voraussetzung, dass die nachfolgenden Auflagen fristgerecht erfüllt werden.

Aufgrund der Ergebnisse der Konformitätsprüfung werden folgende Auflagen festgelegt:

- Für die im Rahmen der Konformitätsprüfung festgestellten Abweichungen sind die in Kapitel 8.2 dieses Konformitätsreports aufgeführten, erforderlichen Maßnahmen bis zur nächsten Re-Zertifizierung des Prüfgegenstands umzusetzen.

Literaturverzeichnis

BSIG	BSI-Gesetz – Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009, Bundesgesetzblatt Teil I Nr. 54, S. 2821
BSIZertV	BSI-Zertifizierungs- und Anerkennungsverordnung – Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSIZertV), vom 17. Dezember 2014, Bundesgesetzblatt Teil I Nr. 61, S. 2231
BMIBGebV	Besondere Gebührenverordnung des Bundesministeriums des Inneren, für Bau und Heimat für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (Besondere Gebührenverordnung BMI, BMIBGebV) vom02. September 2019, Bundesgesetzblatt I, S. 1359
VB-Produkte	Verfahrensbeschreibung zur Zertifizierung von Produkten, Version 2.4 vom 09. September 2019
TR-Produkte	Anforderungen an Antragsteller zur Zertifizierung von Produkten nach Technischen Richtlinien, Version 1.3 vom 09. September 2019
BSI TR-03138	BSI TR-03138 – Technische Richtlinie Ersetzendes Scannen, Version 1.4 vom 03. September 2019
BSI TR-03138-P	BSI TR-03138-P – Technische Richtlinie Ersetzendes Scannen, Anlage P: Prüfspezifikation, Version 1.4 vom 03. September 2019

Bundesamt
für Sicherheit in der
Informationstechnik

Empfangsbestätigung

Hiermit bestätige ich den Empfang des Konformitätsbescheids, des Zertifikats nach Technischen Richtlinien und des Konformitätsreports, erteilt vom Bundesamt für Sicherheit in der Informationstechnik am 31. März 2020, für den Prüfgegenstand 'Scan- & Dokumenten-Services‘ der Ratiodata AG, unter der Verfahrenskennung BSI-K-TR-0320-2020.

Ort, Datum	Unterschrift, Firmenstempel

Bitte senden Sie dieses Schreiben an folgende Adresse zurück:

Bundesamt für Sicherheit in der Informationstechnik
Referat SZ 25
Postfach 20 03 63
53133 Bonn

Bundesamt
für Sicherheit in der
Informationstechnik

Erklärung zum Verzicht auf Widerspruch

Der Konformitätsbescheid zum Verfahren BSI-K-TR-0320-2020 kann unmittelbar rechtskräftig werden, sobald Sie Ihren Verzicht auf Widerspruch dem BSI schriftlich mitteilen. Andernfalls wird der Konformitätsbescheid erst nach Ablauf eines Monats rechtskräftig.

Falls Sie vor Ablauf der Monatsfrist auf Widerspruch verzichten möchten, füllen Sie bitte diesen Vordruck aus und senden Sie ihn an folgende Adresse zurück:

Bundesamt für Sicherheit in der Informationstechnik
Referat SZ 25
Postfach 20 03 63
53133 Bonn

Verzicht auf Widerspruch

Hiermit verzichte ich auf Widerspruch zum Konformitätsbescheid vom 31. März 2020 zum Zertifizierungsverfahren nach Technischen Richtlinien BSI-K-TR-0320-2020 ('Scan- & Dokumenten-Services' der Ratiodata AG) vor Ablauf der Monatsfrist, sodass dieser mit sofortiger Wirkung rechtskräftig werden kann.

Ort, Datum	Unterschrift, Firmenstempel