Prüfungsbericht nach IDW PS 880, IDW PS 951 und OPDV-Stellungnahme Nr. 1/2015

LORA Mobile in der Version: 1.4.115.5 für LORA Mobile (live) und 2.6.29.4 für LORA Mobile NG App

(**Abschlussergebnis**)

Dokumentversion 7.0[1] vom 29.01.2020 08:32 [IDW PS 951, Tz121]

Dieser Prüfungsbericht ist nur gültig, wenn er komplett weitergegeben wird, also alle Seiten vom Deckblatt bis zur Unterschriftenseite enthält.
Unvollständig weitergegebene Dokumente sind ungültig!

Eine erste Übersicht der im Rahmen der hier dokumentierten Prüfung behandelten Standards resepektive die genutzten Kriterien finden sich im Abschnitt 2.2.

Auflagen finden sich im Abschnitt 6.3.

[1] Die Versionsnummer bezieht sich auf die Dokumentvorlage, das Datum auf den konkreten Dokumentinhalt

Inhaltsverzeichnis

Versionsführung der Vorlage für den Prüfungsbericht (Checkliste - Prüfungen nach OPDV 1/2015):

Wer	Wann/ Version	Was
Hr. König	V190410 V6.2	▪ IDW PH 9.860.1 integriert
Hr. König	V190709 V6.3	▪ IDW PS 525 integriert
Hr. König	V190814 V6.4	▪ Update der BAIT auf die Version 2018. ▪ Umstellung von [VO1/2006] auf [IDW QS 1] ▪ [MaRiskCloudMerkblatt] integriert
Hr. König	V190906 V7.0	▪ Prüfberichtsstruktur näher an der inhaltlichen Struktur des IDW PS 880 .

Kursive Texte kennzeichnen Originalzitate aus anderen Dokumenten oder Vorgaben.

Rot und fett dargestellte Abschnitte außerhalb der Überschriften stellen Auflagen dar.

Die zur Programmfreigabe nach 1/2015 erforderlichen weiteren Schritte werden im Abschnitt *6.1 Verantwortung des Auftraggebers der Prüfung* beschrieben.

Prüfungsgegenstand

Identifikation des Prüfungsgegenstandes

Im Rahmen der hier dokumentierten Prüfung [IDW PS 860, Tz17] ist die erstellte IT-Anwendung *LORA Mobile* in der Version

- 1.4.115.5 LORA Mobile (live) und
- 2.6.29.4 LORA Mobile NG App

[IDW PS 880, Tz8] und deren Herstellungsprozess bei der NT Neue Technologie AG[2] zu untersuchen und zu bewerten.

Hersteller von *LORA Mobile* ist die NT Neue Technologie AG. Die Entwicklung hat in Erfurt stattgefunden.

Lieferant von *LORA Mobile* ist die on-geo GmbH.

Der Betrieb der IT-Anwendung erfolgt durch die *on-geo GmbH*.

1.2 Zugesagte Eigenschaften des Prüfungsgegenstandes

Gegenstand der Prüfung ist ein Softwaresystem namens *LORA Mobile*. *LORA Mobile* ist eine Dokumentationssoftware für die Mitarbeiter, die Immobilienbesichtigungen durchführen [1021, B.6 Dokumentation Mandantifizierung der Daten und Passwortschutz, 1. Ausgangslage und Anforderungen]. *LORA Mobile* dient dabei der Internen Beauftragung eines Besichtigers und stellt ihm Dokumentationsmöglichkeiten und bis zur Berichtserfassung und dessen Abgabe zur Verfügung Die Kernfunktionalität der *LORA Mobile*-Anwendung besteht hinsichtlich [1022, 1. LORA Suite: LORA Mobile] aus:

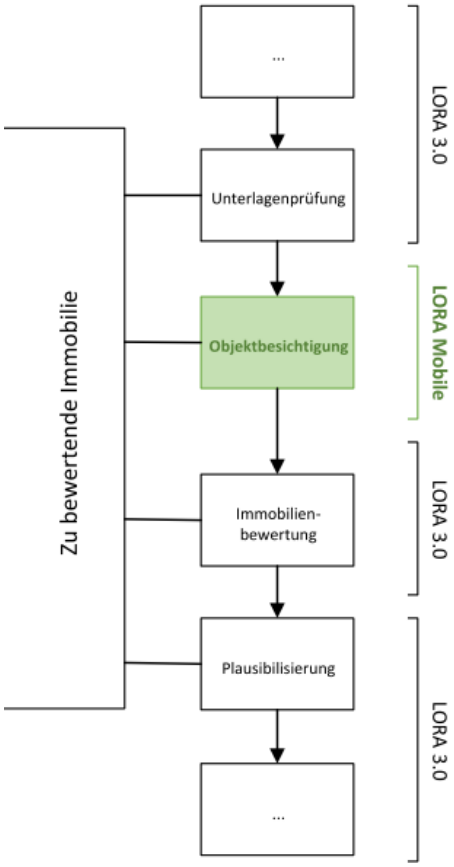
[2] Nachfolgend mit Hersteller bzw. Lieferant abgekürzt.

- *Auftragsübersicht* und
- *Auftragseinzelansicht*. Hier sind Erfassung von Beobachtungen und Fotos sowie die Berichtserstellung möglich.
- Beide Funktionen stehen je nach Berechtigung sowohl der Rolle Besichtigungsbüro und der Rolle Besichtiger/Sachverständiger zur Verfügung [1022, 3. Web-/Browseranwendung].

Die folgenden Dokumente sind vor Vertragsunterschrift als Produktbeschreibung zu konsultieren, da sie wesentliche und für den Betrieb erforderliche Informationen beinhalten:

- Ergänzungsangebot zu LORA [1017]
- Handbuch „*LORA Mobile Dokumentation: Benutzerhandbuch*“ [1022].
- LORA Mobile Organisatorische Voraussetzungen [1020] enthält sowohl organisatorische als auch technische Voraussetzungen.

Folgende fachliche Schnittstellen im Geschäftsprozess sind vorhanden:



[1021, A.5 Arbeitsanweisung Schnittstellentest, 2. Skizze Bewertungsprozess]

Schnittstellen zu den Komponenten handelsplattform und Geoport beziehen sich nur auf LORA, nicht aber auf LORA Mobile.

In dieser Abbildung ist rechts neben die beiden Oberflächenvarianten der Nutzer zu ergänzen.

1.3 Technische Struktur des Prüfungsgegenstandes

Technisch ist *LORA Mobile* eine in verschiedenen Sprachen implementierte Webanwendung bzw. App. *LORA Mobile* wird auf einem Immobilien-Besichtiger-Arbeitsplatz als grafische

Oberfläche zu einem im Hintergrund laufenden Server und potenziell auch offline ausgeführt.

Das Softwaresystem ist in mehrere Komponenten gegliedert. Für eine nähere Beschreibung siehe die entsprechenden Handbücher.

Die Prüfaussage dieses Prüfungsberichtes bezieht sich auf die folgenden Systemkomponenten (Kernbestandteile) von *LORA Mobile*:

- eine Web-/Browseranwendung [1022, 1. LORA Suite: LORA Mobile]
- LORA Mobile NG App [1022, 1. LORA Suite: LORA Mobile].

Der Prüfer nutzt keine eigene Testumgebung [IDW PS 880,Tz86]. Weder eine Rechnungslegung noch ein spezieller Schutzbedarf liegen vor, insofern ist diese Entscheidung vertretbar.

Die physisch übergebenen Bestandteile [BAIT,Tz10] sind Dokumentationen, siehe hierzu die Abschnitte *1.2 Zugesagte Eigenschaften des Prüfungsgegenstandes* und *10.1 Literaturverzeichnis*, und bei Nutzung der App die im während der Prüfung hierzu zu korrigierenden Handbuch [1022, 4.1 Installation und Anmeldung] benannten Downloadlinks zur Installation auf einem Smartphone.

2 Kriterien

2.1 Kriterien des Herstellers/Lieferanten (A)

Unternehmensinterne Kriterien

Vorgelegt wurden weder die Arbeitsanweisungen, die den PS951 abdecken noch Belege, dass im PS951 geforderte Vorgaben eingehalten werden. Solange das Institut hier keine Auslagerung erkennen kann, könnte diese Feststellung ohne Folgen bleiben

Als Kriterien [IDW PS 951, Tz11] wurden aus einer ISO stammende Qualitätsmerkmale festgelegt [1021, A.4 Arbeitsanweisung Qualitätssicherung der Softwareentwicklungsprozesse, 2. Qualitätssicherung]. Die Festlegung wurde während des Prüfungsverlaufes vervollständigt.

Eine Festlegung zum Umgang mit der Qualitätsverantwortung bei Subdienstleistern [IDW PS 951, Tz27] wurde nicht vorgelegt. Neben der fehlenden Auslagerungseigenschaft bei der Softwarebereitstellung, siehe Abschnitt *4.8.1 AT9 (Auslagerungen)*, ist hier auch kein Subdienstleister im Prüfungsverlauf deutlich geworden.

Zur Umsetzung der angewiesenen Qualitätsmerkmale und dem bei Auslagerungen erforderlichen Wirksamkeitsbeleg [IDW PS 951, Tz76] siehe Abschnitt *7.1.8 inhaltliche Testabdeckung in Testprotokollen*.

Die IT-Strategie [BAIT,Tz2] wurde nicht vorgelegt, ist bei fehlendem Auslagerungssachverhalt aber auch verzichtbar.

2.1.2 Vom Hersteller/Lieferanten für die IT-Anwendung festgelegte Kriterien

Zur Umsetzung der geforderten Sollmaßnahmen [BAIT,Tz7], [BAIT,Tz33] definiert der Hersteller aus der ISO-stammende Qualitätsmerkmale, die im Verlauf der Prüfung zu komplettieren waren. Die Prozessbeschreibung legt folgende Merkmale fest [1021, A.2 LORA Mobile - Projektmanagement, Softwareentwicklung und Qualitätssicherung, 4.2 Testablauf nach ISTQB]: *Funktionalität, Zuverlässigkeit und Robustheit, Benutzbarkeit, Effizienz, Änderbarkeit, Übertragbarkeit und Integrität*.

Die beim Nutzer umzusetzenden organisatorischen Voraussetzungen wurden während des Prüfungsverlaufes in einem entsprechenden Dokument [1020] ergänzt. Aus Sicht des Prüfers ist dieses Dokument als Produktbeschreibung zu werten und damit im Abschnitt *1.2 Zugesagte Eigenschaften des Prüfungsgegenstandes* als solches benannt.

Die in der Gesamtdokumentation benannten Schritte werden dabei angesprochen und ergänzend erklärt [1020, 2.2 Prozessablauf zur Einsatzfreigabe], dass die dabei entstehenden Konfigurationsdaten dann vom Support hinterlegt werden müssen.

Das Ergänzungsangebot [1017] enthält elektronische Kontaktdaten zur Kontaktaufnahme mit dem Support.

2.2 Prüfungskriterien

Die folgenden Fakten besitzen eine gravierende Auswirkung auf Vorgaben an die IT-Anwendung respektive Bereitstellung sowie die Prüfungshandlungen und werden daher bereits hier zusammenfassend genannt:

Anforderungen an ...	**... sind für den Prüfer nicht sichtbar.**	**... könnten vorliegen.**	**... sind sichtbar.**
Die zur Umsetzung des festgestellten Schutzbedarfes umzusetzenden Maßnahmen, Details siehe projektspezifisch zu ermittelnden Schutzbedarf			X
Revisionssicherheit / gesetzliche Aufbewahrungspflichten	X		
Umsetzung GoBD / Rechnungslegung	X		
Umsetzung PCI DSS wegen Kreditkartendaten	X		
Auslagerungssachverhalte[3]		X (siehe Abschnitt 4.8.1)	
Schutz für personenbezogene Daten		X (siehe Abschnitt 4.2)	
Schutz zur „*Verarbeitung besonderer Kategorien personenbezogener Daten*“[4]	X		
Anwendung im IT-Sicherheitsmanagement, d. h. der IT-Anwendung obliegt der Schutz finanzieller Werte	X		

[3] [MaRisk, AT9]
Eine Auslagerung liegt vor, wenn
1) Die IT-Anwendung nicht im Finanzinstitut sondern in einem wo auch immer liegenden RZ betrieben wird, hierbei wird aber zwischen wesentlichen und unwesentlichen Auslagerungen unterschieden. Zu betrachten ist das reale Verhältnis zwischen diesem Rechenzentrum und dem Finanzinstitut. Üblicherweise werden damit Beschaffungen einer Sparkasse, die dann in einem von der Sparkasse separat beauftragten RZ betrieben werden, im Prüfungsumfeld ausgeklammert.
2) Die Beschaffung von IT-Anwendungen mit bankfachlichen Standardfunktionen oder zur Risikosteuerung, beginnend bei dessen Erfassung, bedeuten nach [MaRisk] das Vorliegen einer Auslagerung.

[4] [BDSG , §22 Verarbeitung besonderer Kategorien personenbezogener Daten (1)]

Für Qualitätsmanagement und Qualitätssicherung gibt es zwar viele Standards, es ist aber nicht standardübergreifend festgelegt, welcher dieser Standards dabei einzuhalten ist und auch nicht, wie verbindlich die in den jeweiligen Standards erkennbaren Anforderungen sind. Da eine ausreichende Qualität der IT-Anwendung zentral davon abhängt, wie diese Vorgaben umgesetzt sind, wird dargestellt, welche Themen geprüft werden (Sollmaßnahmenkatalog):

- Ein wesentlicher Teil der Prüfungsergebnisse setzt auf bereitgestellten Testprotokollen auf. Diese Testprotokolle besitzen dabei zwar einen Belegcharakter, der für die Prüfung erforderliche Nachweischarakter ist aber erst zu untersuchen.
- Bei einer normalen Qualitätssicherung, ggf. auch Test genannt, wird die IT-Anwendung an ihren Schnittstellen einschließlich der Schnittstelle zum Anwender hinterfragt. Das Betrachten von Abläufen innerhalb der IT-Anwendung (sogenannte WhiteBox-Tests) werden dabei oft vernachlässigt. Der Prüfungsbericht widmet sich daher diesem Thema in den s Entwicklertests und ergänzt bei der Vollständigkeit weitere Aussagen.
- Die sogenannten BlackBox-Tests (normale Qualitätssicherung) müssen für die IT-Anwendung als Ganzes ausreichend vollständig sein. D. h. es sind jeweils vollständige Testmaßnahmen in folgenden Bereichen erforderlich:
  Sogenannte Positivtests sollen belegen, dass erforderliche Eigenschaften auch vorhanden sind, dabei sind gesetzliche respektive normative Vorgaben, von der Institution des Herstellers definierte Vorgaben als auch die produktspezifischen Vorgaben zu betrachten.
  Sogenannte Negativtests sollen belegen, dass die von der IT-Anwendung ausgehenden Risiken ausreichend behandelt werden.
  Der Erwartungstest soll belegen, dass im Projektverlauf beginnend mit der Festlegung von Anforderungen über Design und Programmierung bis zum Test die wesentlichen Nutzbarkeitsanforderungen zumindest umgesetzt sind, sprich die IT-Anwendung tatsächlich zur Lösung des von ihr zu bearbeitenden Problems beiträgt. Diese Aspekte werden im Abschnitt zur Vollständigkeit behandelt.
- Sowohl die normale Softwareerstellung als auch die Bereitstellung von Hotfixes bedingen die Wiederholung bestimmter Testbereiche wegen neuer Zwischenversionen. Hierbei ist relevant, dass i.d.R. nach einer neuen Version keine Tests aller Aspekte stattfinden, sondern nur auszugsweise getestet wird. Die Prüfung hinterfragt deshalb, inwieweit diese verkürzten Schritte die notwendigen Regressionstests vollständig abdecken.
- Die Verantwortung der Unternehmensleitung für das Testverfahren und auch entsprechende Festlegungen werden behandelt.

Prüfungskriterien aus externen Vorgaben

Die Prüfung erfolgt auf der Grundlage von:

[5] Es gibt verschiedene DIN- bzw. ISO-Normen, die dies erfüllen, siehe auch die vom SIZ bereitgestellten Zusatzdokumente.

[6] Dem Prüfer sind keine Projekte bekannt, die komplett ohne Auflagen abgeschlossen wurden. Ohne Auflagen hieße auch, die IT-Anwendung bedarf keinerlei organisatorischer Maßnahmen. Dabei gilt als Rahmenbedingung, dass IT-Anwendungen ohne Risiko respektive Schutzbedarf nicht der Freigabepflicht unterliegen würden, d. h. umgekehrt, dass jede zu prüfende IT-Anwendung ein Risiko darstellt, und dieses i. d. R. nicht ausschließlich technisch reduziert wird.

- Fachausschuss Ordnungsmäßigkeit und Prüfung der Datenverarbeitung (OPDV) Stellungnahme Nr. 1/2015 Anforderungen an ein ordnungsgemäßes Programmeinsatzverfahren, Stand Februar 2015.

Die Prüfung erfolgte unter Hinzuziehen der folgenden Checkliste:

- Checkliste - Prüfungen nach OPDV 1/2015, Version vom 08.08.2019, SIZ GmbH [IDW PS 860, Tz41].

Im Rahmen der Prüfung wird vor Prüfungsbeginn kontrolliert, ob die in der Checkliste abgebildeten Standards für den konkreten Prüfling ausreichend sind. Bei Bedarf werden weitere Standards aufgenommen [IDW PS 850, Tz 89]. Der Prüfer geht davon aus, dass im Rahmen der mit dem Prüfungsbericht dokumentierten Prüfung alle relevanten Standards ausreichend betrachtet wurden. Die Standards, die im Prüfling tatsächlich zu betrachten waren, finden sich an folgenden Stellen:

Einzelne[7] Fälle

[7] Die genannten Gesetze, Standards und sonstigen Regulatorien sind unter dem Index detaillierter angegeben.

Versions- und Herkunftsangaben zu externen Vorgaben

[AH OPDV94] Arbeitshilfe für die Beurteilung von Qualitätseigenschaften bei Fremdsoftware, Veröffentlicht im Handbuch OPDV und in den Fachmitteilungen Nr. 7 vom 31.3.1999

[AO] Abgabenordnung (AO), zuletzt geändert durch Art.9 G v. 21.07.2012 I 1566

[B3S] Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG, BSI-Entwurf Version 0.9.01, Stand: 05.10.2016

[BAIT] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Rundschreiben 10/2017 (BA) in der Fassung vom 14.09.2018, Bankaufsichtliche Anforderungen an die IT (BAIT)

[BDSG] BUNDESDATENSCHUTZGESETZ (BDSG-NEU) IN DER VOM DEUTSCHEN BUNDESTAG AM 27. APRIL 2017 UND DEM DEUTSCHEN BUNDESRAT AM 12. MAI 2017 BESCHLOSSENEN FASSUNG

[BetrVG] Betriebsverfassungsgesetz, zuletzt geändert durch Art. 3 G v. 21.2.2017 I 258

[BSI-GS] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kompendium, Final Draft, Datum 27.10.2017
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_FD.html

[COBIT] ISACA COBIT 5, Rahmenwerk für Governance und Management der Unternehmens-IT, ISBN 978-1-60420-245-8, © 2012 ISACA

[DSGVO] VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

[EN ISO 9000] Die Qualitätsmanagementnorm beschreibt, welchen Anforderungen das Managementsystem eines Unternehmens genügen muss, um einem bestimmten Standard bei der Umsetzung des Qualitätsmanagements zu entsprechen. Details zur Version der Norm und deren Umsetzung siehe im entsprechenden Abschnitt.

[FAIT1] IDW-Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1); (Stand: 24.09.2002): Verabschiedet vom Hauptfachausschuss (HFA) am 24.09.2002

[FARR18] FARR-Checkliste Nr. 18, Checkliste für die Durchführung von IT-Systemprüfungen bei kleinen und mittelgroßen Unternehmen (KMU), Stand 01.05.2017, ISBN 978-3-8021-2130-2

[GoBD] Bundesministerium der Finanzen, 14.11.2014, Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)

[GPSG] Gesetz über technische Arbeitsmittel und Verbraucherprodukte (Geräte- und Produktsicherheitsgesetz - GPSG) GPSG - Ausfertigungsdatum: 06.01.2004

[HGB] Handelsgesetzbuch, zuletzt geändert am 01.03.2011

[IDW PH 9.330.1] IDW Prüfungshinweis: Checkliste zur Abschlussprüfung bei Einsatz von Informationstechnologie (IDW PH 9.330.1) (Stand: 01.07.2002), verabschiedet vom Hauptfachausschuss (HFA) am 01.07.2002.

[IDW PH 9.860.1] IDW Prüfungshinweis: Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz (IDW PH 9.860.1) Stand: 19.06.2018, Verabschiedet vom Fachausschuss für Informationstechnologie (FAIT) am 17.05.2018. Billigende Kenntnisnahme durch den Hauptfachausschuss (HFA) am 19.06.2018.

[IDW PS 860] IDW Prüfungsstandard: IT-Prüfung außerhalb der Abschlussprüfung (IDW PS 860), Stand: 02.03.2018, Verabschiedet vom Fachausschuss für Informationstechnologie (FAIT) am 14.02.2018. Billigende Kenntnisnahme durch den Hauptfachausschuss (HFA) am 02.03.2018.

[IDW PS 850] IDW Prüfungsstandard: Projektbegleitende Prüfung bei Einsatz von Informationstechnologie (Stand: 02.09.2008)

[IDW PS 880] IDW Prüfungsstandard: Die Prüfung von Softwareprodukten (IDW PS 880), (Stand: 11.03.2010), Verabschiedet vom Hauptfachausschuss (HFA) am 11.03.2010.

[IDW PS 951] IDW Prüfungsstandard: Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen (IDW PS 951 n. F.), (Stand: 16.10.2013), Verabschiedet vom Hauptfachausschuss (HFA) am 19.09.2007. Redaktionelle Änderung durch den HFA am 02.09.2008 in Tz.38. Änderungen durch den HFA zur Anpassung an die im Rahmen des Clarity-Projekts des lAASB überarbeiteten international Standards on Auditing (ISA) am 09.09.2010 in Tz.3, 62. Grundlegende Überarbeitung vorbereitet vom Fachausschuss für Informationstechnologie (FAlT), verabschiedet vom H FA am 16.10.2013.

[IDW PS 980] IDW Prüfungsstandard: Grundsätze ordnungsmäßiger Prüfung von Compliance Management Systemen (IDW PS 980) (Stand: 11.03.2011)

[IDW QS 1] IDW Qualitätssicherungsstandard: Anforderungen an die Qualitätssicherung in der Wirtschaftsprüferpraxis (IDW QS 1), Stand: 09.06.2017, Vorbereitet vom Arbeitskreis „Prüfungsqualität“, verabschiedet vom Hauptfachausschuss (HFA) am 09.06.2017.

[ISO IEC 27001] Die internationale Norm ISO/IEC 27001 spezifiziert die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung des Kontexts einer Organisation.

[KWG] Gesetz über das Kreditwesen (Kreditwesengesetz – KWG), zuletzt geändert durch Art. 1G v. 21.07.2010 | 950

[MaRisk] BaFin Rundschreiben 09/2017 (BA) vom 27.10.2017, Mindestanforderungen an das Risikomanagement - MaRisk
englische Übersetzung auf: https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/rs_1709_MaRisk_english.html .

[MCREV] IT-Revision, Schriftlicher Lehrgang in 10 Lektionen, Management Circle Edition, 1. Auflage (2007)

[OPDV 1/2015] Fachausschuss Ordnungsmäßigkeit und Prüfung der Datenverarbeitung (OPDV), Stellungnahme Nr. 1/2015, Anforderungen an ein ordnungsgemäßes Programmeinsatzverfahren, Stellungnahme_1_2015_OPDV_20150211.docx

[OSPLUS-GRL7] OSPlus-Portal Gestaltungsrichtlinien 7.0, Stand 01.09.2008, http://www.s-web.de/handbuecher/ikk/style/index.htm

[OWiG] Gesetz über Ordnungswidrigkeiten (OWiG); zuletzt geändert durch Art. 2 G v. 29.7.2009 I 2353

[PrüfbV] Verordnung über die Prüfung der Jahresabschlüsse der Kreditinstitute und Finanzdienstleistungsinstitute sowie über die darüber zu erstellenden Berichte (Prüfungsberichtsverordnung - PrüfbV), Ausfertigungsdatum: 11.06.2015, Zuletzt geändert durch Art. 1 V v. 16.01.2018 I 134

[SITB] im Unternehmen des Prüfers die Kurzform für [SIZ-SITB].

[SIZ-SITB] Sicherer IT-Betrieb, SIZ GmbH, Version 15.0 vom 18.11.2016

[TÜVIT2005] Von der TÜViT im Rahmen der Überarbeitung der Checkliste für das Projekt TRAVIC Jan 2005 genannte Aspekte aus den Trusted Process.

[UrhG] Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz), Zuletzt geändert durch Art. 1 G v. 1.9.2017 I 3346

[V BATH08] Kongress: Testing & Finance 2008, 2.+3. Juni 2008, Frankfurt mit geschlossenem VÖB-Service-Kongress, Graham Bath, Performance Testing as a Life-Cycle activity

[ZPO] Zivilprozessordnung ZPO, zuletzt geändert durch Art. 1 G v. 31.1.2019 I 54

2.2.2 Prüfungskriterien aus dem Schutzbedarf

***LORA Mobile* in der auf dem Deckblatt genannten Version stellt nach OPDV Stellungnahme 1/2015 eine IT-Anwendung mit mittlerem bis hohen Schutzbedarf dar[8].**

***LORA Mobile* in der auf dem Deckblatt genannten Version stellt nach der in diesem Dokument beschriebenen Risikobeurteilung eine IT-Anwendung mit niedrigen bis mittleren Risiko dar und entspricht dabei den Vorgaben der Risikostufe C bis B der OPDV-Stellungnahme Nr. 1/2006.**

LORA Mobile wird von Sparkassen mit maximal mittel bewertet, LORA selbst aber auch mit hoch. Die Systemdokumentation [1021, A.1. Immobilienbewertungsprozess, 4.2 Risikoabschätzung aus Sicht der Informationssicherheit] benennt einen umgesetzten hohen Schutzbedarf bei Verfügbarkeit und Vertraulichkeit und einen nur normalen bei der Integrität, weitere Details aus Sicht des Herstellers siehe Abschnitt *10.2 Schutzbedarfsanalyse durch den Hersteller respektive Lieferanten*.

Die Schutzbedarfsfeststellung seitens Prüfer wird für folgende IT-Anwendung erstellt und ist im Ergebnis in Folge dokumentiert:

Anwendungsname	LORA Mobile
Release (optional)	Siehe Abschnitt 1.1 Identifikation des Prüfungsgegenstandes

Die folgende Bewertung der IT-Anwendung wurde durch den Prüferdurchgeführt.

Die Schutzbedarfsfeststellung wurde aus folgenden Gründen durchgeführt:

	Erstversion	
X	Fortschreibung wegen Änderung von	
		gesetzlichen, vertraglichen, aufsichtsrechtlichen oder unternehmensinternen Vorgaben
	X	Geschäftsprozessen/fachlichen Aufgaben/Funktionalität der IT-Anwendung
		Datentypen/Datenstrukturen

[8] Während der Prüfung wird von dem hohen Schutzbedarf ausgegangen, auch wenn seitens Sparkassen eher ein mittlerer Schutzbedarf angenommen werden kann.

		Schnittstellen zu anderen IT-Anwendungen
	Neubewertung im Rahmen der turnusmäßigen Überprüfung	

Die Anwendung unterstützt folgende Geschäftsprozesse:

Immobilienbesichtigung

Die Anwendung wird für folgende fachliche Aufgaben genutzt:

Erstellung eines Besichtigungsberichtes

Es werden folgende Arten von Daten verarbeitet:

X	Personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes, siehe Abschnitt *4.2 BDSG/DSGVO*.	
		darunter besondere personenbezogene Daten im Sinne [DSGVO, Art.9]
?[9]	Nach [HGB], Steuerrecht (inkl. [GoBD]) oder aus sonstigen Gründen archivierungspflichtige Daten, siehe Abschnitt *3.1.3.1 K020 Aufbewahrung und Archivierung*.	

Bei den folgenden Bewertungsspalten gilt:
<leer>: für den Prüfer nicht sichtbar,
„?“: könnte nach Meinung des Prüfers zutreffen und
„X“: trifft nach Meinung des Prüfers zu.
Die Verantwortung für die im Institut gewählte Belegung trifft das Institut, insofern darf im Institut von der folgenden Darstellung abgewichen werden. Die Prüfung orientiert sich an den höchsten hier dargestellten Werten.

Schutzbedarf in Bezug auf die **Verfügbarkeit** **Beurteilungskriterium**	normal	hoch	sehr hoch	**Begründung**
Wirtschaftliche (finanzielle) Auswirkungen	X			
Beeinträchtigung der Aufgabenerfüllung	X			
Image-Schäden	X			
Verstoß gegen Gesetze/Vorschriften/Verträge	X			
Beeinträchtigung des informationellen Selbstbestimmungsrechts	X			
Mindestwert aufgrund von abhängigen Anwendungen	X			

Schutzbedarf in Bezug auf die **Integrität** **Beurteilungskriterium**	normal	hoch	sehr hoch	**Begründung**
Wirtschaftliche (finanzielle) Auswirkungen	X			

[9] Siehe die Ausgrenzungen im Handelsrecht, die im Prüfungsbericht auftauchen.

Beeinträchtigung der Aufgabenerfüllung	X			
Image-Schäden	X			
Verstoß gegen Gesetze/Vorschriften/Verträge		?		
Beeinträchtigung des informationellen Selbstbestimmungsrechts	X			
Mindestwert aufgrund von abhängigen Anwendungen		X		

Schutzbedarf in Bezug auf die **Vertraulichkeit** **Beurteilungskriterium**	normal	hoch	sehr hoch	**Begründung**
Wirtschaftliche (finanzielle) Auswirkungen	X			
Beeinträchtigung der Aufgabenerfüllung	X			
Image-Schäden	X			
Verstoß gegen Gesetze/Vorschriften/Verträge	X			
Beeinträchtigung des informationellen Selbstbestimmungsrechts	X			
Mindestwert aufgrund von abhängigen Anwendungen	X			

Darstellung des **Gesamtschutzbedarfs** **Beurteilungskriterium**	normal	hoch	sehr hoch	**Begründung des Kriteriums mit dem höchsten Wert**
Vertraulichkeit	X	?		
Integrität	?	X		
Verfügbarkeit	X	?		

Im K-Fall gelten folgende Festlegungen:

X	K-Fall-Vorsorge ist nicht erforderlich.	
	K-Fall-Vorsorge ist erforderlich	
		Muss innerhalb von 2 Tagen wieder zur Verfügung stehen.
		Muss innerhalb von 7 Tagen wieder zur Verfügung stehen.
		Muss innerhalb von 30 Tagen wieder zur Verfügung stehen.

3 Ordnungsmäßigkeit und Sicherheit der Programmfunktionen

3.1 Ordnungsmäßigkeit nach GoBD/HGB (A+F)

Der Musterbesichtigungsbericht [1023] enthält keine Beträge, nennt aber Fakten, die später zu Beträgen werden können, wie z. B. die *Anzahl Zimmer*. Die Angaben sind aber wertmäßig zu ergänzen, die Grundstücksgröße ist z. B. im Bericht nicht enthalten.

Die Systemdokumentation [1021, B.3 Dokumentation: Abrechnung, 1 Auftragseinstellung] stellt klar, dass für die vorliegende IT-Anwendung die [GoBD Tz6] nicht relevant ist und erläutert weiter: „*Die Einstellung der Aufträge in LORA Mobile zur internen Bearbeitung durch den Auftraggeber*“, abrechnungsrelevante Tätigkeiten sind danach unzulässig.

Die Systemdokumentation [1021, B.3. LORA Mobile - Dokumentation: Abrechnung] stellt im Fließtext dar, dass es bei Abrechnungen um Aufträge *zur internen Bearbeitung durch den Auftraggeber* geht, die typischer Weise nicht der GoBD unterliegen. **Im Einsatzfreigabeverfahren müssen sowohl Auftraggeber der Besichtigung als auch die durchführende Person dem gleichen Institut bzw. Unternehmen angehören**.

3.1.1 Handbücher

Ein Benutzerhandbuch wurde vorgelegt [1022], Besichtiger benötigen die fachliche Kenntnis Ihres Fachgebietes, die IT-Anwendung selber ist sehr einfach gehalten [IDW PS 850, Tz 80]. Zu kritischen Funktionen siehe Abschnitt *4.6 GPSG / ProdSichG*.

3.1.2 GoBD-Verfahrensdokumentation / Dokumentation

Eine Bereitstellung des Quellcodes [AH OPDV94, 2.5.5], [FAIT1 (63)] oder einer GoBD-Verfahrensdokumentation ist nicht vorgesehen, wegen fehlender Rechnungslegung aber auch nicht erforderlich.

3.1.3 Integrität (Zugriffskontrollen, Archivierung)

3.1.3.1 K020 Aufbewahrung und Archivierung

Eine handelsrechtlich relevante Archivfunktion ist nicht vorhanden. Solange tatsächlich nur interne Auftragsvergaben stattfinden, kann darauf nach Auffassung des Prüfers auch verzichtet werden. **Das Institut hat andernfalls sicherzustellen, dass die handelsrechtlichen Vorgaben zu Aufbewahrungsfristen eingehalten werden**.

Der Prüfungsbericht weist darauf hin, dass nach [MaRisk, AT 6 Dokumentation (1)] *Kontroll- und Überwachungsunterlagen …, vorbehaltlich gesetzlicher Regelungen, grundsätzlich fünf Jahre aufzubewahren* sind.

K115 Zugriffsberechtigung

Identity Management

In der IT-Anwendung wird kein Identity-Management angeboten, für die eindeutige Zuordnung zwischen Accountdaten und handelnden Mitarbeitern [BAIT,Tz25] ist damit allein das Institut verantwortlich.

3.1.3.2.2 Objekte des Berechtigungskonzeptes

Der Schutz der Accountdaten des genutzten technischen Users vor unzulässiger Einsichtnahme obliegt dem durchführenden Rechenzentrum.

Für reale Nutzer beschreibt die Systemdokumentation [1021, B.6 LORA Mobile - Dokumentation Mandantifizierung der Daten und Passwortschutz, 3. Passwortschutz] einen Hash mit Salt und die Ablage des Ergebnisses in der Datenbank. Als kritisch zu bewertende Rückrechnungen sind damit kaum möglich.

3.1.3.2.3 Verfahren im Berechtigungskonzept

Die Prüfung der Berechtigungsverfahren ergibt folgende zusammenfassende Ergebnisse, die nur zusammen bewertet werden können:

- Die Accountdaten des normalen Nutzers müssen zwecks späterer Authentisierung des Nutzers in anwendungsspezifischen Tabellen in der Datenbank hinterlegt werden. Damit diese Hinterlegung bei einer Kompromittierung der Datenbank nicht zu lesbaren Passworten führt, werden die Passworte nach Systemdokumentation [1021, B.6 LORA Mobile - Dokumentation Mandantifizierung der Daten und Passwortschutz, 3. Passwortschutz] verhasht und mit „Salt“ abgelegt, letzteres soll verhindern dass die Passwortdaten verschiedenen Nutzer ausgetauscht werden können.
- Auf dem Smartphone liegende Kopien der Daten werden erst nach Abmeldung gelöscht. Der Nutzer wird im Fließtext darauf hingewiesen, dass damit ein Datenverlust beim Abmelden verbunden ist und dies insbesondere in Gegenden mit schlechter Netzabdeckung dazu führen kann, dass die Sitzung innerhalb der hier geprüften IT-Anwendung nicht beendet werden sollte.
- Smartphones besitzen typischer Weise sogenannte SSD-Speicher, bei denen ein Löschvorgang durch Öffnen der Chips und entsprechende Zusatzgeräte aufgehoben werden kann.
- Die IT-Anwendung selber benutzt einen sogenannten technischen User zum Zugriff auf die Datenbank. Der Vertraulichkeitsschutz der Accountdaten dieses technischen Users obliegt dem betreibenden Rechenzentrum, das eine ISO27001-Zertifizierung besitzt.
- Der Schutzbedarf der Daten sollte nur mit maximal hoch bewertet werden, insofern müssten diese obigen Einzelfaktoren zum Schutz als ausreichend eingestuft werden können,

Zur Legitimation von Veränderungen bei Benutzerkennungen und Berechtigungen fordert das Ergänzungsangebot [1017, Anlage B, 5. Weisungsberechtigte Personen beim Auftraggeber] die Liste der Ansprechpartner im Institut ein.

Zum Verfahren bei Initialpasswörten [FARR18, Checkliste IT-Berechtigungskonzept] erklärt die Systemdokumentation [1021, B.6 Dokumentation Mandantifizierung der Daten und Passwortschutz in LORA Mobile, 3. Passwortschutz]: *Bei dem zur Verfügung gestellten Initialkennwort handelt es sich um ein anwendungsseitig automatisch generiertes Zufallspasswort für die Erstanmeldung des spezifischen Nutzers. Dabei erzeugt ein in der Anwendung implementierter Algorithmus nach Zufallsprinzip eine ebenfalls der Passwortrichtlinie entsprechende Zeichenkette. Im Zuge der Erstanmeldung ist der Nutzer gezwungen, das Initialkennwort zu ändern und ein eigenes, der Passwortrichtlinie entsprechendes, Kennwort zu vergeben.*

Eine vorübergehende Sperrung [BSI-GS, ORP.4.A5 Vergabe von Zutrittsberechtigungen] ist nicht dokumentiert, hier aber verzichtbar.

Das Handbuch [1022, 2. Zugang] beschreibt einheitliche Kennwortanforderungen mit Mindestlänge, Zeichentypmix, Wechselturnus, nicht mit dem Account identisch und eine Kennwortchronik.

3.1.3.2.4 Funktionstrennungen

Eine Funktionstrennung von Aufgaben und damit der Verhinderung einer Personalunion [BAIT,Tz6] ist, sofern erforderlich, durch das nutzende Institut entsprechend zu beauftragen. Die Systemdokumentation [1021, B.5 Organisatorische Voraussetzungen, 2.2 Prozessablauf zur Einsatzfreigabe] legt dar, dass Berechtigungen über den Provider zu beantragen und von ihm in der IT-Anwendung zu hinterlegen sind.

3.1.3.2.5 Mandantentrennung

Die Systemdokumentation [1021, B.6 Dokumentation: Mandantifizierung der Daten und Passwortschutz in LORA Mobile, 2. Duale Systematik zur Mandantentrennung] wird beschrieben, dass Datensätze immer mit dem Schlüsselpaar aus Auftraggeber und Besichtiger gehalten werden und ein Zugriff nur möglich ist, wenn es hier eine Übereinstimmung gibt [SIZ-SITB, K115]. Für Revisoren werden spezielle Accounts zur Verfügung gestellt, die dann auf alle Institutsseitigen Datensätze lesend zugreifen können, dieses Verfahren wird aber nur in separat beauftragten Einzelfällen umgesetzt und ist nicht dokumentiert.

3.1.4 Kontrollmaßnahmen / IKS

Zur Durchführung der Kontrolle des Zugriffsschutzes (Berechtigungsrezertifizierung) [AH OPDV94, 3.1], [BAIT,Tz29] verweist der Hersteller auf die Möglichkeit, entsprechende Listen beim Support anzufordern.

Erfassungs- und Eingabekontrollen sind in der IT-Anwendung nicht explizit vorgesehen. Die erstellten Berichte sind aber institutsintern an die nutzenden Mitarbeiter zu übergeben.

Technische Plausibilisierungen von Eingaben sind nur marginal umgesetzt, das Handbuch [1022, 3.2.2.3 Besichtigungsbericht] beschreibt sie mit „*Die Anwendung kontrolliert automatisch Datumsfelder auf Dateneingaben und Zahlenfelder auf Zahleneingaben*“.

Das Dokument der organisatorischen Voraussetzungen [1020] benennt die Notwendigkeit, die Berichtsvorlage an Institutsvorgaben anpassen zu lassen, hierzu ist die Einbindung der Supportabteilung erforderlich.

Berichte werden nach Dokumentation nur eine kurze Zeit vorgehalten, eine Kontrolle der Verarbeitung muss organisatorisch und außerhalb der hier betrachteten IT-Anwendung stattfinden.

3.2 Sicherheit (A+F)

Die Einhaltung sicherheitsrelevanter Themen des Betriebes [SIZ-SITB, RQ0003] wird durch zwei vorgelegte Zertifikate belegt:

- [1002, Zertifikat - Geprüftes Verbundrechenzentrum hochverfügbar Stufe 3 tekPlus] stellt ein ISO 27002-Zertifikat für die Verfügbarkeit des vom Lieferanten angemieteten Rechenzentrums dar.
- [1002, ISO 27001-Zertifikat auf der Basis von IT-Grundschutz] stellt ein vom BSI ausgestellten ISO 27001-Zertifikat dar.

3.2.1 K107 Datenablage

Das Handbuch [1022, 4.2. Entsperrcode/Passcode (Zugriffsschutz)] nennt die Existenz einer Verschlüsselung [SIZ-SITB, L53.15a] von Daten auf dem Mobilgerät mit Löschung bei zu vielen Fehlversuchen. Die Systemdokumentation [1021, B.5 LORA Mobile Organisatorische Voraussetzungen, 2.4 Hinweise zur digitalen Informationsvorhaltung] beschreibt diese Löschvorgänge und es wird deutlich, dass nur innerhalb der IT-Anwendung gelöscht wird.

Der Prüfer weist darauf hin, dass Löschvorgänge auf den in Smartphones verbauten oder einsetzbaren Speichermodulen technisch aufwändig rückgängig gemacht werden können. Eine dies verhindernde sichere Löschung ist nicht dokumentiert. Der Hersteller verweist hierzu auch darauf, dass die Daten dann trotzdem verschlüsselt sind.

3.2.2 K110 Protokollierung

In der vorgelegten Dokumentation finden sich keine Hinweise auf Protokollierungsfunktionen.

3.2.3 K113 Schutz vor Schadsoftware

Der Einsatz eines Virenscanners wird dem nutzenden Institut empfohlen. Die Systemdokumentation [1021, B.2 LORA Mobile Dokumentation: Betrieb und IT-Sicherheit, 3 Sicherheitsmaßnahmen] ergänzt: *Zum Schutz der Daten vor Virenbefall, erfolgt der einheitliche Einsatz der Antivirenlösung von avast! Die auf den Servern installierten AV clients, werden zentral gemanaged. Die Identifikation eines Virus zieht eine Benachrichtigung per E-Mail an die Administration nach sich. Der Fund wird automatisch isoliert. Die Aktualisierung des Virenscanners erfolgt zyklisch in einem automatisierten Vorgang, indem Updates aus dem Internet vom Hersteller bezogen und verteilt werden (tägliches Update).*

3.2.4 K126 Erkennbarkeit von Angriffen

Eine Erkennung von Einbruchsversuchen [BSI-GS, DER.1.A1 Erstellung einer Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen] ist nicht angeboten.

3.2.5 K311 Compliance-...

Die dem Prüfer sichtbaren Funktionen innerhalb der IT-Anwendung beschränken sich auf die Berichterstellung und eine interne Kommunikation mit Kollegen, eine externe und dem [OWiG, §130] unterliegende Kommunikation wird dabei nicht sichtbar. Die Systemdokumentation bietet darüber hinaus [1021] an: *Für Revisionszwecke kann auf Anfrage bei on-geo durch die LORA Mobile Administration ein Revisions- bzw. Kontrollaccount angelegt werden. Der Account kann so konfiguriert werden, dass eine Einsichtnahme in alle Besichtigungen und Vorgänge des zu prüfenden Instituts innerhalb der LORA Mobile Anwendung möglich ist. Für die Anlage dieses Accounts muss eine entsprechende Legitimation vorliegen.*

3.2.6 K341 Penetrationstest

Die IT-Anwendung besitzt einen durch das Rechenzentrum abzublockenden Internetzugang. Die Systemdokumentation wurde im Verlauf der Prüfung durch ein etwa fünf Jahre altes Penetrationstestprotokoll ergänzt [1021, A.8 Testprotokolle, Testprotokolle Last- und Penetrationstest]. Es benennt das Testergebnis des Penetrationstests auf der Version 1.4.37.11490. Als Tool wird das Standardtool OpenVAS-7 und Fiddler Web Debugger, Version 4.4.5.9 genannt. Der Test wurde im Oktober 2014 durchgeführt, und lieferte angeblich ein zu 100% positives Ergebnis, dabei wurde nur eine herstellereigene Zusammenfassung bereitgestellt, nicht aber die Originalergebnisse der Prüftools. Ergänzend erklärt der Hersteller [1016]: Es *wurde ein Protokoll eines automatisierten Pentests den Unterlagen beigefügt. Ferner ist zu erwähnen, dass SQL-Injection durch das eingesetzte Datenbank-Framework (Entity Framework) nicht möglich ist. Das Einschleusen bspw. von HTML/Javascript Code wird darüber hinaus vom .NET Framework standardmäßig verhindert.*

4 weitere Gesetze, Verordnungen, Standards … mit IT-Bezug

BAIT (Bankaufsichtliche Anforderungen an …)

Die BaFin hat mit der [BAIT] eine Verordnung definiert. Diese Verordnung umfasst unterschiedlichste Bereiche der IT. Eine Zuordnung, welche Teilbereiche durch den Prüfungsbericht neben den potenziell folgenden abgedeckt werden, kann entweder durch eine Suche nach BAIT im Prüfungsbericht oder durch den entsprechenden Abschnitt im Index erreicht werden.

4.2 BDSG/DSGVO

Die im Institut erforderlichen Maßnahmen zur Umsetzung von Löschfristen [DSGVO, Art.5 (1)] sind als solche beschrieben [1020, 2.4 Hinweise zur digitalen Informationsvorhaltung].

Der Musterbesichtigungsbericht [1023] kennt teilnehmende Rollen, aber keine Personen. Kritisch aus Sicht des Prüfers ist die optionale Erfassung von Ansprechpartnern (Nachbarn und andere unbeteiligte Personen). Das Handbuch [1022, 3.2.2.1 Stammdaten] benennt die potenziell zu erfassenden Daten mit: *im Bereich Auftrag erhält der Nutzer detaillierte Informationen zum Auftrag. Zu diesen gehören unter anderem der Auftraggeber/Einsteller, die Auftragsart und der Ansprechpartner.*

4.2.1 BDSG/DSGVO (Ergänzung für Provider und Supportdienstleister)

Das LORA-Angebot [1018, Anlage 3] enthält TOMs und geht in §6 auf Subunternehmer [DSGVO, Art.28 Auftragsverarbeiter (2)] ein, dem Auftraggeber wird dabei eine Widerspruchsmöglichkeit eingeräumt.

In der Dokumentation auftauchende Subunternehmer sind in der im Abschnitt *10.5 Informationen für den Datenschutzbeauftragten* wiedergegebenen Liste weitgehend benannt.

Zur nicht dort auftauchenden euNetworks GmbH erklärt der Hersteller [1021, Hinweis zu Unterlage C.2 TÜV-Zertifikat (NT.AG)]: *In der im Rechenzentrum der euNetworks GmbH angemieteten Rechenzentrumsfläche, Juri-Gagarin-Ring 88, werden jedoch keine Systeme/Server der on-geo GmbH betrieben. Die LORA Mobile IT-Infrastruktur wird ausschließlich im Rechenzentrum in der Peterstraße 3 betrieben.*

Das externe Firmenprofil [1011] benennt einen aus Deutschland kommenden Gesellschafter / Eigentümer des Herstellers, ein weiteres [1012] benennt einen aus Deutschland kommenden Gesellschafter / Eigentümer des Lieferanten on-geo GmbH.

Die Systemdokumentation [1021, Anlage on-geo TOM] enthält die TOMs [DSGVO, Art.28 Auftragsverarbeiter (3)], die aber wegen ursprünglich fehlender Versionsführung und jetzt einer ggf. nicht an Sparkassen ausgelieferten Variante im Abschnitt *10.6 Anlage on-geo TOM (Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO)* dargestellt werden.

Unabhängig von der Feststellung, ob eine rechtlich relevante Auslagerung vorliegt oder nicht, stellt die Tatsache, dass der Betrieb der Anwendung nicht durch das Institut selbst sondern durch ein Rechenzentrum betrieben wird, eine nach [BDSG] relevante Auftragsdatenverarbeitung dar.

Final zu bewerten ist nicht ein potenziell existierender Mustervertrag, sondern der tatsächlich zwischen einsetzendem Institut und Betreiber vereinbarte Vertrag, insofern haben die folgenden Aussagen nur vorläufigen Charakter. **Das einsetzende Institut muss prüfen, ob alle Belange ausreichend erfüllt sind**.

4.2.1.1 Umsetzung der IDW PH 9.860.1

Die dem Prüfer bereitgestellten Dokumente enthalten weder die Festlegungen noch Umsetzungsbelege der in [IDW PH 9.860.1, Tz19] erwarteten Datenschutzprozesse.

4.3 BelWertV (Beleihungswertermittlungsverordnung)

Die IT-Anwendung dient der Umsetzung von [BelWertV § 4 (1) S. 3]: „*Das zu bewertende Objekt ist im Rahmen der Wertermittlung zu besichtigen.*“ Weitere Konkretisierungen enthält die Verordnung nicht. Ein Musterbesichtigungsbericht wurde vorgelegt [1023].

4.4 BetrVG (zu Kontrollmöglichkeiten über Institutsmitarbeiter)

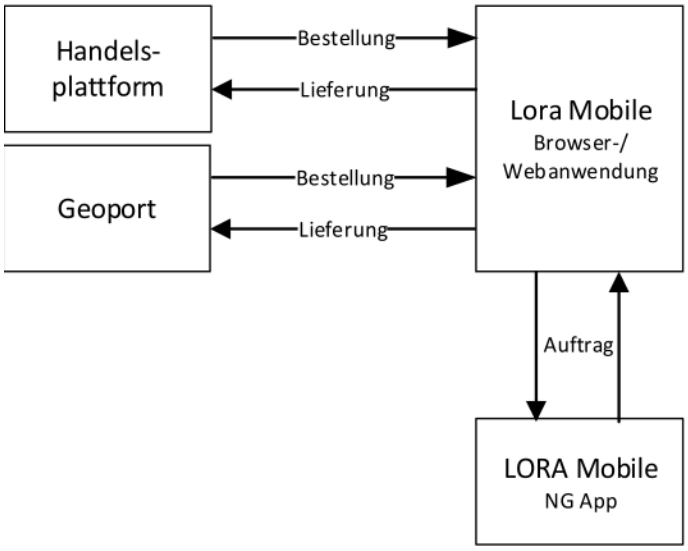
Kontrollmaßnahmen als solche [BetrVG] kann der Prüfer nicht erkennen, Kandidaten könnten sein:

- Im internen Forum ist für weitere Mitarbeiter der Autor und Zeitpunkt von Veröffentlichungen transparent.
- Die Systemdokumentation [1021] enthält den Hinweis auf potenzielle Revisionsrollen, mit denen *eine Einsichtnahme in alle Besichtigungen und Vorgänge des zu prüfenden Instituts innerhalb der LORA Mobile Anwendung möglich ist.*

4.5 BGB (u. a. Vertragsrecht)

Die Beauftragung von Besichtigung und deren Auftragsannahme sind mit dem vorliegenden Prüfungsbericht ausschließlich für die Fälle legitimiert, in denen beide Parteien zum gleichen Institut gehören. Eine handelsrechtliche Auftragserteilung ist explizit nicht Prüfungsumfang.

Die nur für internen Austausch legitimierte Handelstätigkeit gilt auch für folgende in Unterlagen vorgefundene Grafik:



[1002, A.5 Arbeitsanweisung Schnittstellentest, 2. Schnittstellen]

4.6 GPSG / ProdSichG

Der Prüfer hat während der Prüfung auf einer Nennung von Risiken [GPSG, §5] bestanden, die von ihm erkannten sind entweder in der Herstellerdokumentation oder im Prüfungsbericht explizit benannt.

Aus Sicht der Sicherheit muss auch auf folgendes hingewiesen werden: Besichtigungsdaten verbleiben mindestens solange auf dem Smartphone, bis eine Abmeldung erfolgt, die lt. Handbuch aber nicht jederzeit möglich ist. Das Handbuch enthält dazu ohne eigentlich erwarteten Warncharakter und nur im Fließtext folgende Erklärung [1022, 4.8. Abmelden]: *Zur*

[10] Geräte- und Produktsicherheitsgesetz

Ausführung des Abmeldevorgangs (Synchronisierung und Ausloggen) ist eine ausreichend schnelle Internetverbindung notwendig. Ist dies nicht gegeben, wird der Nutzer darauf hingewiesen, den Abmeldevorgang bei bestehender Internetverbindung zu wiederholen.

4.7 HGB

4.7.1 Handelsbriefe

Aufzeichnungen nach [HGB, §239 Abs. 3] und deren Fristen nach [HGB, §257] werden im Abschnitt *3.1.3.1 K020 Aufbewahrung und Archivierung* behandelt.

Verträge mit Provider

Die vertragliche Grundlage zur Auftragsdatenverarbeitung [IDW PH 9.330.1, 4.1.3] ergibt sich durch den Hauptvertrag zwischen dem Lieferanten und dem Institut, der hier nicht Prüfungsumfang ist und der Weitergabe an den Hersteller, die im Rahmen der Prüfung zumindest konsultiert wird. Der Hauptvertrag [1018, Anlage3, §6] geht auf Subunternehmer ein, dem Auftraggeber / Institut wird dabei eine Widerspruchsmöglichkeit eingeräumt.

Die Vererbung der Vertragsanforderungen [SIZ-SITB, V01.15d] auch für Subunternehmer (hier den Hersteller) ergibt sich aus dem Hauptvertrag durch [1018, Anlage3, 6.3] *Der Auftragnehmer wird mit dem Unterauftragnehmer die in diesem AVV getroffenen Regelungen inhaltsgleich vereinbaren. Insbesondere müssen die mit dem Unterauftragnehmer zu vereinbaren-den technischen und organisatorischen Maßnahmen mindestens dasselbe Schutzniveau aufweisen.*

Ein Notfallmanagement [SIZ-SITB, V17.15] wird im Rahmenvertrag, der außerhalb der Prüfung hier erwähnt wird, angesprochen.

Sicherheitsreports oder –berichte seitens Lieferant [BAIT,Tz55], [BAIT,Tz50] sind im Rahmenvertrag [1018] sichtbar.

Zu Meldungen über ungeplante Abweichungen [BAIT,Tz50] konnten in den Verträgen keine Zusagen identifiziert werden.

Der Rahmenvertrag [1018, Anlage 1] geht auf Pflegebedingungen ein, nennt aber keine Behebungszeiten [SIZ-SITB, K302]. Solange kein sehr hoher Schutzbedarf angenommen wird, stellt diese Einschränkung keinen Widerspruch dar.

Bei wesentlichen Auslagerungen geben die [MaRisk, AT9] auch Anforderungen vor, siehe Abschnitt *4.8.1 AT9 (Auslagerungen)*.

Im Rahmen des Prüfungsauftrages ist die Einhaltung der maßgeblichen gesetzlichen Vorschriften und der sie ergänzenden Vorschriften geprüft worden. Zur Vollständigkeitserklärung [IDW PS 880, Tz39], IDW PS 303, [IDW PS 951, Tz91], [IDW PS 951, Tz92], [IDW PS 951, Tz93] siehe Abschnitt *10.3 Bestätigung der gesetzlichen Vertreter*.

KWG

Bei der hier dokumentierten Prüfung werden ausschließlich sparkassenübliche Situationen [KWG, §10 Anforderungen an die Eigenmittelausstattung von Instituten, Institutsgruppen und Finanzholding-Gruppen (2a)] berücksichtigt.

MaRisk (Mindestanforderungen an das Risikomanagement)

4.8.1 AT9 (Auslagerungen)

Die BaFin erklärt in der Erläuterung zu [MaRisk, AT 9]:

Der isolierte Bezug von Software ist in der Regel als sonstiger Fremdbezug einzustufen. Hierzu gehören unter anderem auch die folgenden Unterstützungsleistungen:

- *die Anpassung der Software an die Erfordernisse des Kreditinstituts,*
- *die entwicklungstechnische Umsetzung von Änderungswünschen (Programmierung),*
- *das Testen, die Freigabe und die Implementierung der Software in die Produktionsprozesse beim erstmaligen Einsatz und bei wesentlichen Veränderungen insbesondere von programmtechnischen Vorgaben,*
- *Fehlerbehebungen (Wartung) gemäß der Anforderungs- /Fehlerbeschreibung des Auftraggebers oder Herstellers,*
- *sonstige Unterstützungsleistungen, die über die reine Beratung hinausgehen.*

Dies gilt nicht für Software, die zur Identifizierung, Beurteilung, Steuerung, Überwachung und Kommunikation der Risiken eingesetzt wird oder die für die Durchführung von bankgeschäftlichen Aufgaben von wesentlicher Bedeutung ist; bei dieser Software sind Unterstützungsleistungen als Auslagerung einzustufen. Ferner gilt der Betrieb der Software durch einen externen Dritten als Auslagerung.

Das BSI ergänzt: *Der* [B3S, Tz3.2] *stellt klar, dass bei Outsourcing o. Ä. die volle Verantwortung für eine geeignete Risikobehandlung beim Betreiber verbleibt.*

Software zur Immobilienkreditbewertung könnte als Auslagerung [MaRisk, AT 9] bewertet werden, im vorliegenden Fall geht es aber nur um die in diesem Zusammenhang zu erstellenden Besichtigungsreports und damit eines strukturierten und medienbruchfreien Notizzettels, für den der Prüfer damit keine Auslagerung erkennen kann. Seitens Hersteller wurden dazu keine Festlegungen vorgelegt.

4.9 UrhG

In der IT-Anwendung wird nach den Erkenntnissen des Prüfers [1010] auch Open-Source-Software dergestalt genutzt, dass beim Nutzenden Institut zumindest die Lizenztexte für die Komponenten „***FileUploader***“ und „***jQuery***“ vorliegen müssen [UrhG]. Eine Unterstützung durch den Lieferanten ist nicht sichtbar, insofern ist es **Aufgabe des nutzenden Institutes, diese Lizenztexte zu besorgen**[11]. Der Hersteller erklärt seine Bereitschaft, diese Lizenzen auf Nachfrage ebenfalls bereitzustellen.

Gleiches gilt auch für die Lizenz zu **LIBSODIUM** [1021, B.7 Dokumentation Sicherheit - LORA Mobile NG Applikation]. Die Anbieterseite https://libsodium.gitbook.io/doc/#license bekräftigt die Notwendigkeit der hierzu erforderlichen „ISC-license“.

Die Lizenzweitergabe vom Hersteller an den Lieferanten ist dokumentiert, [1002, D.2 Kooperationsvereinbarung zwischen on-geo und NT.AG] erklärt vertragsrelevant, dass die on-geo das Vertriebsrecht der hier geprüften IT-Anwendung besitzt und damit das Rest hat, auch den Sparkassen die dort benötigten Lizenzen einzuräumen.

weitere spezifische Branchen- und Industriestandards

5.1 COBIT (Governance und Management der Unternehmens-IT)

Im Rahmen der hier dokumentierten Prüfung werden aus dem COBIT-5-Standard nur einzelne ausgewählte Themen betrachtet, es findet keine vollständige Prüfung auf Einhaltung der COBIT statt. Nicht betrachtete Themen sind u. a. alle beim Hersteller nur Vor-Ort ermittelbaren Zustände.

[11] Siehe auch aktuell Zeitschrift Computer und Recht 10-2019 ab S.697.

COSO (Commitee of Sponsoring Organizations of the Treadway Commission)

Zur Reduktion des Betrugsrisikos erklärt der Hersteller [1016]: *Die Funktion zur Änderung des Benutzernamens wurde im Rahmen eines Hotfixes aus der Applikation entfernt. Der Nutzer hat im Bereich Einstellungen nur noch die Möglichkeit sein Passwort zu ändern.*

IDW PS 860 (IT-Prüfung außerhalb der Abschlussprüfung)

Der Prüfer bestätigt die Einhaltung der nach [IDW PS 860, Tz2] geltenden allgemeinen Berufspflichten der Unabhängigkeit, Verschwiegenheit, Eigenverantwortlichkeit und Gewissenhaftigkeit.

Der hier vorliegende Prüfungsbericht berücksichtigt die involvierten Parteien [IDW PS 860, Tz5] dadurch, dass er explizit auch den weiteren vorgesehenen Nutzern –hier insbesondere Sparkassen und deren Mitarbeiter– zur Verfügung gestellt werden und damit deren Fragen beantworten soll. Siehe auch Abschnitt *6 Auftragsannahme und Prüfungsplanung*.

Beauftragt ist eine *direkte IT-Prüfung* [IDW PS 860, Tz6].

Der Prüfer ergänzt die vom Auftraggeber genannten Kriterien immer um die von ihm für relevant gehaltenen Kriterien [IDW PS 860, Tz33] seiner eigenen Prüfung.

Die Prüfungsplanung [IDW PS 860, Tz41] deckt immer nur den nächsten Teilschritt ab, sobald hierzu entweder die relevanten Dokumente eingereicht wurden oder kostenpflichtige Reservierungen vorliegen.

Neben dem Prüfungsbericht wird beim Prüfer auch eine komplette Aufstellung aller Detailergebnisse und Bewertungen (Prüfungsakte) geführt [IDW PS 860, Tz52], die nur unter einer Einzelvereinbarung einem ebenfalls im Prüfungsprozess involvierten Wirtschaftsprüfer bereitgestellt wird.

Während der Prüfung wurden vom Prüfer hinsichtlich besonderer Risiken auffällige Fakten, insbesondere potenzielle Verstöße gegen Kriterien [IDW PS 860, Tz57], in der Prüfungsakte dokumentiert und durch passende Detailprüfungen hinterfragt.

Wurden Verstöße gegen Kriterien [IDW PS 860, Tz59] während der Prüfung festgestellt, wurden vom Prüfer behebende Maßnahmen gefordert. Der Prüfungsbericht geht in Summe auf das dabei vorgefundene Endergebnis ein. Auf Zwischenzustände wird nur eingegangen, wenn dies zum Verständnis des Gesamtergebnisses vom Prüfer für erforderlich gehalten wird.

Strukturvorgabe nach [IDW PS 860, Tz105**]**	**Abschnittnummer im Prüfungsbericht**
a) Überschrift: Angabe, dass es sich um den Prüfungsvermerk eines unabhängigen Prüfers handelt	6.2
b) Berichtsadressaten	Primär Sparkassen und deren Prüfer
c) Prüfungsauftrag einschließlich einer Angabe des zu prüfenden Zeitraums bzw. des zu prüfenden Zeitpunkts	6
d) Beschreibung des geprüften IT-Systems	1
e) Beschreibung der Verantwortlichkeiten der gesetzlichen Vertreter	6.1
f) Darstellung der oder Bezugnahme auf die vom Unternehmen verwendeten Kriterien; sofern bei der Beurteilung des Prüfungsobjekts Kriterien verwendet wurden, die nur einem eingeschränkten Nutzerkreis zugänglich sein sollen (z.B. Vertragsdaten, Preise), ist auf diesen Umstand im Prüfungsvermerk hinzuweisen. Ferner ist darauf hinzuweisen, wenn die verwendeten Kriterien für einen speziellen Zweck entwickelt wurden und dementsprechend die Erklärung der gesetzlichen Vertreter zum IT-System (Prüfung einer Erklärung zum	2.1

IT-System) bzw. die Darstellung des geprüften IT-Systems (direkte IT-Prüfung) für andere Zwecke möglicherweise nicht geeignet ist.	
g) Beschreibung der Verantwortlichkeiten des Prüfers	6.2
h) Gegenstand, Art und Umfang der Prüfung einschließlich einer Aussage, dass es sich um einen Auftrag zur Erlangung hinreichender Sicherheit handelt	6
i) Aussage, dass die Prüfung in Übereinstimmung mit diesem IDW Prüfungsstandard durchgeführt wurde; der Prüfer darf nicht die Einhaltung dieses IDW Prüfungsstandards erklären, wenn er nicht sämtliche einschlägigen Anforderungen beachtet hat	6.2
j) Aussage, dass bei der Prüfung die Berufspflichten der WPO und der Berufssatzung WP/vBP, einschließlich der Anforderungen an die Unabhängigkeit, eingehalten werden und dass die WP-Praxis die Anforderungen an die Qualitätssicherung anwendet	6.2 (sofern relevant)
k) Prüfungsurteil	6.1
l) Aussage über die inhärenten Grenzen des geprüften IT-Systems und zum Risiko, die Feststellungen zum geprüften IT-System auf die Zukunft zu übertragen	6.3
m) falls relevant, bei einer Prüfung einer Erklärung zum IT-System ggf. Hinweis auf nicht geprüfte sonstige Angaben in der Erklärung der gesetzlichen Vertreter zum IT-System	entfällt
n) Aussage, dass der Auftrag für einen bestimmten Zweck bzw. Adressatenkreis durchgeführt wurde und deshalb die Verwendung der Ergebnisse für andere Zwecke möglicherweise nicht geeignet ist	entfällt
o) Datum des Prüfungsvermerks: Das Datum darf nicht vor dem Datum liegen, an dem der Prüfer ausreichende geeignete Prüfungsnachweise als Grundlage für das Prüfungsurteil über das IT-System erlangt hat	11
p) Unterschrift, Name und Ort des Prüfers.	11

Der Prüfungsgegenstand [IDW PS 860, Tz111] wird im Abschnitt *1 Prüfungsgegenstand* genauer beschrieben.

5.4 IDW PS 951

Zur Umsetzung des [IDW PS 951] siehe Abschnitte *2.1.1 Unternehmensinterne Kriterien* und *7.1.8 inhaltliche Testabdeckung in Testprotokollen.*

6 Auftragsannahme und Prüfungsplanung

Im Rahmen der in diesem Dokument beschriebenen Prüfungsmaßnahmen hat die SIZ GmbH am 13.08.2019 den generellen Prüfauftrag erhalten (siehe [IDW EPS 460nF, Tz14ff], [IDW PS 860, TzA60], [IDW PS 951, Tz105]). Die Prüfung wurde beauftragt von NT Neue Technologie AG [IDW PS 951, Tz105].

Das dem Prüfungsauftrag zugrundeliegende Prüfungsangebot enthält auch eine Haftung.

Das Ziel der Prüfung [IDW PS 880, Tz42] ist die Erteilung einer Programmfreigabe nach OPDV 1/2015. Kriterien der Softwareprüfung, Art und Umfang der hierzu erforderlichen Prüfungen werden ausschließlich durch den Prüfer und in dessen Verantwortung auf Basis der hierzu genutzten SIZ-Checkliste festgelegt und werden nicht mit dem Auftraggeber verhan-

delt. Eine vom Auftraggeber bereitgestellte Aufstellung von Kriterien wird damit zwar berücksichtigt [IDW PS 860, Tz5] aber auf jeden Fall durch die vom Prüfer angelegten Kriterien ergänzt.

Beauftragt ist eine *direkte IT-Prüfung* [IDW PS 860, Tz6]. Sie wird ausschließlich als *Angemessenheitsprüfung durchgeführt* [IDW PS 860, Tz20]. Eine ex-post-Prüfung zur Erkennung früherer Zustände [IDW PS 860, Tz22] wird nicht durchgeführt.

Die Prüfungstätigkeiten sind so konzipiert, dass jeweils Belege erforderlich sind. Diese Belege werden im Prüfungsbericht dann benannt. Sofern der Prüfer eine nicht belegte Situation auch selber bewerten kann, kann auf Belege verzichtet werden. Eine abschließende Bewertung des Prüfungsergebnisses obliegt dem Leser [IDW PS 850, Tz 36].

Eine separate Auftragsbestätigung wird nur auf expliziten Wunsch des Auftraggebers ausgestellt [IDW PS 850, Tz 37].

Vor Inbetriebnahme eines IT-Systems innerhalb der Sparkassen-Finanzgruppe ist eine Programmfreigabe nach OPDV 1/2015 erforderlich. In diese Freigabeerklärung fließen die Ergebnisse aller am Abnahmeprozess Beteiligten ein. Als Vorbereitung auf die Freigabe analysiert und bewertet vorliegender, von einem unabhängigen Mitarbeiter der SIZ GmbH erstellter Prüfungsbericht den Verlauf und die jeweiligen Arbeitsergebnisse der Herstellung durch NT Neue Technologie AG.

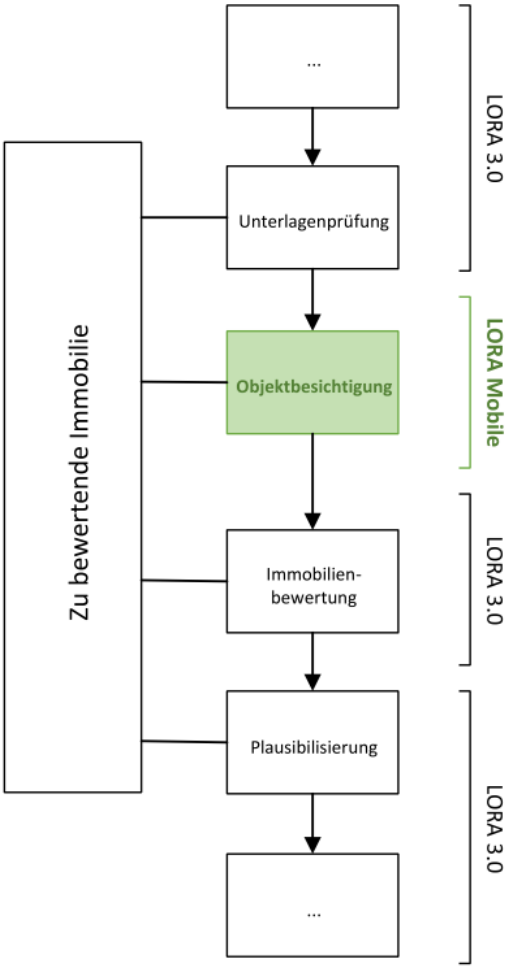
Das Ziel der Prüfung ist die Bewertung, inwieweit die Anforderungen der OPDV 1/2015 eingehalten sind, d. h. es wird im Prüfungsbericht eine Aussage zur Ordnungsmäßigkeit der Verarbeitung des IT-Systems getroffen.

Als Besonderheit bezieht sich das konkrete Prüfungsverfahren der SIZ GmbH für *LORA Mobile* lediglich auf die Frage, ob im vorliegenden Fall der Hersteller respektive Lieferant selber eine „Programmfreigabe“ erteilen darf. Vor einem tatsächlichen Einsatz von *LORA Mobile* innerhalb der Sparkassen-Finanzgruppe ist zusätzlich ein Institutsspezifisches Einsatzfreigabeverfahren zu durchlaufen. Dies muss den örtlichen Gegebenheiten des Betreibers Rechnung tragen und den Integrationsprozess berücksichtigen. Insbesondere sind seine infrastrukturellen, organisations- und bundeslandspezifischen Vorschriften und Regelungen bzw. Gesetze einzubeziehen.

6.1 Verantwortung des Auftraggebers der Prüfung

Die folgenden mit dem Produktumfang ebenfalls ausgelieferten oder auslieferbaren Systemkomponenten sind nicht Bestandteil der Überprüfung [IDW PS 860, Tz25]. Allgemeine Aussagen der vorliegenden Prüfungsdokumentation gelten daher nur dann auch für diese Systemkomponenten, wenn explizit darauf hingewiesen wird:

- Ausschließlich der im folgenden Geschäftsprozessbild grün markierte Bestandteil des Immobilienbewertungsprozesses wird hier geprüft, die anderen Teile nicht:



[1002, A.1. Immobilienbewertungsprozess, 2. Skizze Bewertungsprozess]

- Der vorliegende Prüfungsbericht stellt nur einen Soll-Ist-Vergleich der zu prüfenden IT-Anwendung dar. Aus Sicht des IDW PS 951 deckt er damit maximal eine Stufe 1 ab. Alle Themen, die sich mit Stufe 2 des IDW PS 951 befassen[12] oder andere Standards, die sich mit dem Betriebsablauf einer Software befassen, sind nur dann Thema des vorliegenden Prüfungsberichtes, wenn diese Themen in Einzelfällen explizit angegeben werden. Das gleiche gilt für Datenanalysen.
- Der Prüfungsbericht befasst sich nicht mit Bestandsgefährdungen [IDW PS 400] in den Unternehmen des Herstellers oder Lieferanten.
- Der vorliegende Prüfungsbericht grenzt wirtschaftlichen Verhältnisse des Herstellers oder Lieferanten [PrüfbV, §9 Darstellung der rechtlichen, wirtschaftlichen und organisatorischen Grundlagen] komplett aus.
- Grundsätzlich haben die Betreiber wie auch der Prüfer das Vertrauen in den Hersteller, dass er seine Kompetenzen nach bestem Wissen und Gewissen einsetzt. Damit mögliche Fehler vermieden oder zumindest erkannt und beseitigt werden können, gewährte der Hersteller dem Prüfer einen umfassenden und detaillierten Einblick in seine internen Abläufe. Dies beinhaltet seine Prozesse, Verfahren, Methoden und Dokumente. Hierdurch wird das Vertrauen in die Produkte des Herstellers gestärkt. Die

[12] Typ 2 wird in folgenden Einzelaspekten angesprochen: [IDW PS 951, Tz11], [IDW PS 951, Tz16], [IDW PS 951, Tz18], [IDW PS 951, Tz21], [IDW PS 951, Tz23], [IDW PS 951, Tz56], [IDW PS 951, Tz61], [IDW PS 951, Tz64], [IDW PS 951, Tz73], [IDW PS 951, Tz75], [IDW PS 951, Tz105], [IDW PS 951, Tz107], [IDW PS 951, Tz110], [IDW PS 951, Tz111], [IDW PS 951, Tz113] und [IDW PS 951, Tz114].

Offenlegung dieser betriebsinternen Informationen erfolgt im wechselseitigen Vertrauen auf die Einhaltung üblicher Vertraulichkeitsregelungen. In den Prüfungsbericht fließen ausschließlich Informationen, die für die Analyse und Bewertung nach OPDV 1/2015 erforderlich sind.

6.2 Verantwortung des Prüfungsinstitutes

Im Rahmen des Prüfungsauftrages ist die Einhaltung der maßgeblichen gesetzlichen Vorschriften und der sie ergänzenden Vorschriften geprüft worden. Zur Vollständigkeitserklärung [IDW PS 880, Tz39], [IDW PS 303], [IDW PS951, Tz91], [IDW PS951, Tz92], [IDW PS951, Tz93] siehe Abschnitt *.10.3 Bestätigung der gesetzlichen Vertreter*.

Die Prüfung wurde von *König, Bernhard*, Mitarbeiter(in) der SIZ GmbH, Bonn durchgeführt. Die Prüfung wird unabhängig vom Projektteam [IDW PS 951, Tz105] dokumentiert.

Nach [Art. 13 Verordnung (EU) 537/2014] ist von der prüfenden Organisation ein Transparenzbericht zu veröffentlichen. Die SIZ GmbH ist keine Wirtschaftsprüfungsorganisation, insofern lassen sich nicht alle WPO-Themen umsetzen. Folgende Themen sind umgesetzt, Duplikate in den Vorgaben werden nur einfach genannt:

- Die SIZ GmbH besitzt Eigentümer, die im Wesentlichen aus der Sparkassenfinanzgruppe stammen. Es wird versucht, bei Ausscheiden eines Eigentümers einen gleichwertigen Ersatz zu schaffen. Es wird weiterhin versucht ca. 20 Eigentümer mit möglichst gleichen Anteilen zu bedienen und diese Anteile ohne signifikante Unterschiede zwischen den Anteilseignern zu verteilen [WPO, §28].

- Die SIZ GmbH und damit auch die Prüfer fühlen sich der Sparkassenfinanzgruppe gegenüber verpflichtet. Hieraus entsteht auch und insbesondere bei Auftragsvergaben durch Softwarehäuser eine große Unabhängigkeit von diesen Softwarehäusern [WPO, §55c], [IDW PS 850, Tz 32ff], [IDW PS 860, Tz2].
  Der Prüfer bestätigt gemäß [HGB, §321 Abs. 4a], dass bei unserer Prüfung die anwendbaren Vorschriften zur Unabhängigkeit beachtet wurden.

- Die SIZ GmbH führt keine Abschlussprüfungen für Unternehmen durch [IDW PS 860, Tz29].

- Das Gehalt der SIZ-Mitarbeiter sowie zusätzliche Sonderzahlungen und damit auch der Prüfer unterliegt spezifischen Regelungen und besitzt insofern keinen direkten Bezug zur Durchführung von Prüfungsaufträgen. Eine entsprechende Abhängigkeit und damit das Risiko einer unzulässigen Beinflussung des Prüfers (z.B. nach [IDW QS 1, Tz36] und [WPO, §55]) kann somit nicht gesehen werden.

- Der Prüfungsprozess ist von der Akquise an, über die eigentliche Prüfung bis zu erforderlichen Nacharbeiten in einer Verfahrensbeschreibung festgelegt [IDW QS 1, Tz185], [IDW PS 460] und mit Beteiligten abgestimmt [IDW PS 850, Tz 35], [IDW PS 860, Tz52], [IDW PS 860, Tz53]. Auch die Dokumentationsverfahren sind festgelegt [IDW PS 860, Tz97], [IDW PS 860, Tz98], [IDW PS 860, Tz99], [IDW PS 860, TzA56]. Wesentlicher Bestandteil der Dokumentenprüfung ist die Feststellung passender Dokumentversionen [IDW PS 951, Tz69].

- Der Umgang mit Angeboten und Aufträgen ist in der SIZ GmbH per separater Arbeitsanweisung festgelegt und unterliegt auch der Innenrevision. Angebotsinhalte zu den hier dokumentierten Prüfungen sind festgelegt [IDW PS 860, Tz37]. Fragen im Umfeld einer Befangenheit (z. B. nach [IDW QS 1, Tz47]) sind dabei nicht explizit festgelegt.

- Der Prüfer soll eine kritische Grundhaltung nach [WPO, §43 Abs. 4] und [IDW QS 1, Tz55] einhalten, angewiesen ist dieses Verhalten in der SIZ nicht.

- Prüfungen bestehen aus einer optionalen Vorbesprechung, aus den ggf. widerholten Bereitstellungen von Unterlagen mit folgender Analyse und Ergebnismeldung und der abschließenden Erstellung eines Prüfungsberichtes. Ein Vor-Ort-Audit wird ggf. im Rahmen der Vorbesprechung durchgeführt und ansonsten nur dann der Prüfungsberichtserstellung vorgelagert, wenn dem Prüfer die erlangten Belege und Nachweise hinsichtlich ihrer Glaubwürdigkeit als nicht ausreichend erscheinen. Im Falle einer Prozesszertifizierung wird das Vor-Ort-Audit zwingend durchgeführt. Eine Beteiligung an Projektsitzungen durch den Prüfer erfolgen im Regelfall nicht [IDW PS 850, Tz 34]. Prüfungsaufträge für die SIZ werden durch die erforderlichen Abstimmungssitzungen begleitet.

- *Die Erklärung der gesetzlichen Vertreter zum IT-System hat zumindest im Entwurf zu Beginn der Prüfung vorzuliegen und ist bis zum Abschluss der Prüfung von den gesetzlichen Vertretern fertigzustellen* [IDW PS 860, Tz26]. Der Auftraggeber erhält dazu am Beginn der Prüfung ein Muster, die final abgegebene Erklärung wird als Anlage im Prüfungsbericht dargestellt, sofern sie übergeben wurde.

- Die SIZ GmbH verfügt intern über diverse Mitarbeiter in IT-relevanten Berufsgruppen, die der Prüfer bei *Fragen konsultieren* kann [IDW PS 850, Tz 91], [IDW PS 860, Tz42], [IDW PS 860, Tz63], [IDW PS 860, Tz64]. Dazu gehören u. a. Sicherheitsexperten in diversen Themengebieten, Datenschutzbeauftragte und IT-Juristen [IDW QS 1, Tz140]. Der Fachvorgesetze ist zur *Lösung von Meinungsverschiedenheiten* einzubeziehen [IDW QS 1, Tz181].

- Themen der Verschwiegenheit werden in der SIZ GmbH auch durch deren Datenschutzbeauftragten geschult und kontrolliert [IDW QS 1, Tz58] und [WPO, §43 Abs. 1 Satz 1]. Verschwiegenheitserklärungen sind abgegeben und bei der Personalstelle hinterlegt. Im weiteren hat der Prüfer [IDW QS 1, Tz5] nach [WPO, §43 Abs. 1 Satz 1] seinen *Beruf unabhängig, gewissenhaft, verschwiegen und eigenverantwortlich auszuüben*. Explizite Anweisungen, wie sie für echte Prüfer nach [HGB, §323], [WPO, §55b Abs. 1 Satz 1] und [IDW QS 1, Tz37] erforderlich wären, sind in der SIZ aber nicht vorhanden.

- Zur Aufrechterhaltung der Fachkunde konsultiert der Prüfer Fachzeitschriften aus den Bereichen IT und Jura [IDW QS 1, Tz91], und nimmt an spezifisch ausgewählten Weiterbildungsmaßnahmen teil. Zur Einbeziehung von Sparkassenwissen werden in der Sparkassen Finanzgruppe verfügbare Informationsmedien genutzt und auch Seminare mit Teilnehmern aus Sparkassen in leitender Funktion durchgeführt [IDW QS 1, Tz90]. Festlegungen hierzu (z. B. nach [IDW QS 1, Tz29]) sind nicht vorhanden.

- Eine Delegation von Prüfungen nach dem im vorliegenden Prüfungsbericht beschriebenen Verfahren erfolgt [IDW QS 1, Tz15] durch die Gruppenleitung an die ihr dazu geeignet erscheinenden Mitarbeiter. Auslagerungen der Prüfungsleistung [IDW QS 1, Tz200] oder Teams sind dabei nicht vorgesehen. Festlegungen hierzu (z. B. nach [IDW QS 1, Tz21]) oder Rotation (z. B. nach [IDW QS 1, Tz52]) sind nicht vorhanden.

- Ein Angebot zu der dokumentierten Prüfung ist ergebnisoffen, d. h. bei ausreichender Einhaltung der Vorgaben wird ein Prüfungsbericht erstellt, andernfalls kann der Auftraggeber den Prozess dann ohne Prüfungsbericht beenden [IDW PS 951, Tz117] oder die Einhaltung der Vorgaben nachliefern [IDW PS 860, Tz38], [IDW PS 860, Tz59]. Prüfungen *sind mit einer kritischen Grundhaltung und mit dem Bewusstsein durchzuführen, dass Umstände bestehen können, die dazu führen, dass das zu prüfende IT-System in Bezug auf die verwendeten Kriterien zu dem zu prüfenden Zeitpunkt bzw. in dem zu prüfenden Zeitraum nicht angemessen bzw. wirksam war* [IDW PS 860, Tz43], [IDW PS 951, Tz53].

- Die bei den Prüfungen als Grundlage genutzte Checkliste spricht potenziell relevante Themen an und wird bei Bedarf ergänzt und benennt grundsätzlich nachzuweisende Eigenschaften der zu prüfenden IT-Anwendung. Im Rahmen der Prüfung sind in jeder

Analysephase als auch bei der Prüfungsberichtserstellung sämtliche inhaltlich relevanten Abschnitte der Checkliste zu bearbeiten. Im Rahmen der Prüfung sind dazu durch den Auftraggeber entsprechende Nachweise, respektive Belege oder andere Dokumente zu liefern [IDW PS 850, Tz 41], aus denen sich der Umsetzungsgrad der jeweiligen Anforderungen ergibt [IDW PS 850, Tz 74].

- Im Rahmen der Prüfungsdurchführung ist der Prüfer angehalten, nicht nur explizit übergebene Unterlagen zur Prüfung heranzuziehen sondern sowohl weitere Unterlagen des Auftraggebers als auch andere Unterlagen über den Auftraggeber oder die IT-Anwendung [IDW PS 860, Tz40]. Der Prüfer muss sich seines Urteils sicher sein, notfalls werden im Prüfungsverlauf weitere Unterlagen angefordert [IDW PS 860, Tz84]. Widersprüchliche Unterlagen stellen einen Formfehler dar und werden im Prüfungsbericht benannt, dabei ist eine Wesentlichkeitsschwelle zu berücksichtigen [IDW PS 860, Tz85].
- Zu Beginn und auch während einer Prüfung wird durch den Prüfer hinterfragt, ob die Liste der einzuhaltenden Normen, Regularien und Gesetze vollständig ist und diese ggf. ergänzt [IDW PS 860, Tz30], weitere Details siehe Abschnitt *1.4 Prüfkriterien*.
- Der Prüfer notiert in der Prüfungsdokumentation [IDW PS 850, Tz 92] die von ihm als relevant angenommenen Risiken, wobei auch anzugeben ist, wo das Risiko im Prüfungsbericht behandelt wird. Hierzu werden mindestens die Grundzüge einer sogenannten FMEA durchgeführt, die für Risiken und deren Berücksichtigung eine Standardmethode darstellt [IDW PS 850, Tz 38]. Je nach Projektverlauf werden diese Risiken dann in den jeweils passenden Abschnitten des Prüfungsberichtes angesprochen.
- Der Auftraggeber wird während der Prüfung über Abweichungen informiert [IDW PS 850, Tz 94f], [IDW QS 1, Tz104].
- Dokumente, einschließlich der dem Prüfer zur Verfügung gestellten Dokumente, unterliegen einem festzulegenden Schutzbedarf. Die in der SIZ hierzu vorhandene Leitlinie definiert darüber hinaus auch die auf diesen Dokumenten durchführbaren Aktionen. Festlegungen zur Aufbewahrungspflicht der Prüfungsdokumente (wie z.B. nach [IDW QS 1, Tz31]) bestehen in der SIZ nicht.
- Die Sicherheit aller Dokumente [IDW QS 1, Tz190] und hier damit sowohl der von Kunden übergebenen Dokumente als auch der Arbeitspapiere des Prüfers, unterliegt in der SIZ den vom Informationssicherheitsbeauftragten verantworteten Regelungen, der sich dabei am [SIZ-SITB] orientiert. Die Erkennbarkeit von rein lesenden Zugriffen auf Dokumente oder handelsrechtliche Aufbewahrungsfristen [IDW QS 1, Tz196] sind dabei nicht umgesetzt.
- Übergreifende Planungsaktivitäten [IDW QS 1, Tz99] finden nur für die jeweils n Folgewochen statt, für die tatsächlich Prüfungsaktivitäten vorliegen oder explizit reserviert sind.
- Tätigkeiten während einer Prüfung werden durch einen in den Prüfungsunterlegen integrierten Laufzettel koordiniert, der insbesondere das Übersehen wichtiger Schritte verhindern soll.
- Für die Qualitätssicherung ist der Fachvorgesetzte verantwortlich, der die erfolgreiche Wahrnehmung seiner Qualitätssicherung im Abschnitt *9* durch seine Unterschrift zu bestätigen hat. Als Higl-Level-Control steht ihm dabei auch die in der SIZ-Struktur verankerte Mitarbeiterführung über Ziele zur Verfügung [IDW QS 1, Tz94]. Welche Maßnahmen dabei in welchem Umfand zur Qualitätssicherung genutzt werden, ist nicht festgelegt. Ein ausformuliertes Qualitätsmanagement, wie z. B. von [IDW QS 1, Tz6] und [WPO, §55b Abs. 1 Satz 2] gefordert, besteht somit nicht. Das gilt sinngemäß auch für die Bereiche einer Nachschau [IDW QS 1, Tz205], einer Berichts-kritik [IDW QS 1, Tz148] und des Beschwerdemanagements [IDW QS 1, Tz102].

- Die ausgestellten Prüfungsberichte sind im Abschnitt *9* vom Prüfer zu unterschrieben [IDW QS 1, Tz111]. Dazu gehört immer auch die Unterschrift des Fachvorgesetzten zur Bestätigung der Qualitätssicherung. Eine Prüfung ist erst mit der Unterschrift beendet, alle vorigen Ereignisse können Auswirkungen auf das Prüfungsergebnis haben [IDW PS 860, Tz70].

Im Rahmen der hier dokumentierten Prüfung im Rahmen einer Programmfreigabe nach OPDV wird die Innenrevision der bereitstellenden Organisation nicht überprüft, mithin die Aspekte [IDW PS 951, Tz84], [IDW PS 951, Tz85], [IDW PS 951, Tz86] und [IDW PS 951, Tz87] nicht hinterfragt. Aussagen der Innenrevision werden bei Bedarf zitiert und ggf. durch Stellungsnahmen des Prüfers ergänzt.

Verantwortung des Finanzinstitutes (Auflagen)

Dieser Prüfungsbericht ist thematisch sehr umfassend angelegt, so dass erwartet werden kann, dass alle IT-technischen Aspekte der Programmfreigabe nach OPDV 1/2015 abgedeckt sind. Seine Grenzen werden hier konkretisiert.

- Dieser Prüfungsbericht betrachtet ausschließlich die in direktem Zusammenhang mit der Informationstechnologie stehenden Aspekte, die zur erfolgreichen Projektabwicklung bzw. System- und Produktentwicklung gehören. Dies schließt sämtliche zugehörigen organisatorischen wie technischen Themen ein. Bspw. gehört das Projektmanagement ebenso zu den Aspekten wie Dokumentation, Entwicklung, Herstellertests, Abnahmetests sowie IT-Qualität und IT-Sicherheit. Nur bedingt betrachtet werden dedizierte juristische oder betriebswirtschaftliche Aspekte. Auch sind Aspekte wie die Analyse des Kundenbedarfs an anderer Stelle zu betrachten.

- Die Überprüfung erfolgt immer gegen die Produktspezifikation, deren inhaltliche Korrektheit und Vollständigkeit ausschließlich in der Verantwortung des Herstellers liegt. Die Spezifikation wird lediglich darauf hin überprüft, ob sie ausreichend vollständig und in sich schlüssig ist.

- Anforderungsdefinitionen bzw. zu Grunde gelegte Standards werden grundsätzlich nicht hinterfragt, es sei denn, dass sie offensichtlich unvollständig oder unangemessen sind.

- Insbesondere nicht enthalten ist eine Detailanalyse des IT-Systems bzw. Produkts bspw. im Rahmen eines Codereview. Solche tiefgehenden Analysen erforderten das Anwenden bspw. von IT-Sicherheitskriterien wie den „Common Criteria“ (ISO 15408) oder des SIZ-Produktes „Sicherer IT-Betrieb“, was inhaltlich sowie im Umfang ausdrücklich außerhalb dieser Prüfung liegt.

- Der vorliegende Prüfungsbericht greift der Einsatzfreigabe nach OPDV 1/2015 durch das einsetzende Institut nicht vor. Diese Freigabe bleibt exklusiv dem jeweiligen Institut vorbehalten.

- Grundsätzlich muss jeder Betreiber vor Einsatz des Produktes sein eigenes Freigabeverfahren durchführen, welches die konkreten Gegebenheiten des Betreibers berücksichtigt. Dabei ist es empfohlen und gewollt, die aus der Programmfreigabe gewonnenen Erkenntnisse in die eigene Analyse einzubinden.

- Hinsichtlich der geforderten eigenen Testfälle des Prüfers [IDW PS 850, Tz 75] wird im Rahmen der hier dokumentierten Prüfung überprüft, ob in den vorgelegten Testprotokollen auch die Prüffälle enthalten sind, die aus Sicht des Prüfers durchgeführt werden müssten. Hierzu werden sowohl Prüfungen auf in der Software erwartete Eigenschaften als auch Prüfungen auf nicht in der Software zugelassene Eigenschaften herangezogen und dabei alle potentiellen Störquellen betrachtet. Einem vorgelegten Testprotokoll wird dabei nicht blind vertraut, es wird seitens des Prüfers hier immer ein Nachweis über die Korrektheit des Testprotokolls verlangt.

Eine Checkliste zur generelle Funktionsbestätigung [1020, 2. Checkliste Einsatzfreigabe] liegt vor und beschreibt Schritte. Wesentlich ist aus Sicht des Prüfers die im folgenden Abschnitt der bereitgestellten Unterlage [1020, 2.2 Prozessablauf zur Einsatzfreigabe] dargestellte Liste von erforderlichen Kontrollmaßnahmen. Das Thema Einsatzfreigabe selbst ist dabei wie immer nach den Regeln des freigebenden Institutes durchzuführen und dabei auch die dabei angeforderten Schritte umzusetzen und Vorgabekonform zu dokumentieren.

Der Prüfer ergänzt die Liste um folgende Auflagen:

- **Die Kenntnis der Produktbeschreibung**, mithin aller Dokumente, die die Eigenschaften der IT-Anwendung beschreiben, **wird** als verbindliche Vorgabe **vorausgesetzt**. Eine Aufstellung dieser Dokumente findet sich im Abschnitt *1.2 Zugesagte Eigenschaften des Prüfungsgegenstandes*. Weiterhin wird darauf hingewiesen, dass sich der in diesem Prüfungsbericht beschriebene Sachverhalt nur auf eine „Programmfreigabe des Herstellers gemäß OPDV 1/2015“ beziehen kann, **das Institut ist** damit **für die Durchführung der Einsatzfreigabe gemäß OPDV 1/2015 verantwortlich**.
    - Bei Festlegungen zur Konfiguration sind **Systemparameter mit dem erlaubten Funktionsbereich der IT-Anwendung abzugleichen**, siehe Abschnitte *3.1 Ordnungsmäßigkeit nach GoBD/HGB (A+F)* und *3.1.3.1 K020 Aufbewahrung und Archivierung*.
- **Einzelne Fremdlizenzen,** mindestens zu FileUploader, jQuery und Libsodium **sind durch das Institut zu besorgen**, Details siehe Abschnitt *4.9 UrhG*.
- Die BaFin weist in den Erläuterungen zu [MaRisk, AT7.2] darauf hin, dass der vorliegende Prüfungsbericht *bei der Abnahme berücksichtigt* werden kann, dabei aber die **eigene *Abnahme*** *nicht vollständig ersetzen* kann.

Sofern in dieser Liste Auflagen enthalten sind, die im Institut weder technisch noch organisatorisch umgesetzt werden können, liegen zu tragende Risiken vor. **Bei diesen Risiken sind seitens des Instituts neben der Bereitstellung ausreichender finanzieller Risikotragfähigkeit auch** mindestens die **gesetzlichen Vorgaben umzusetzen** [BAIT, Tz14], [BAIT, Tz35]. [B3S, Tz3.2] begrenzt die Möglichkeiten des Risikotragens für Institute[13], die der KritisV unterliegen mit: *Der B3S stellt klar, dass bzgl. relevanter Risiken für die kDL eine eigenständige dauerhafte Risikoakzeptanz durch den Betreiber in der Regel keine zulässige Option im Sinne des BSIG ist. Ähnliches gilt für die Versicherung gegen solche Risiken. Ggf. weist der B3S darauf hin, in welchem Rahmen eine Risikoakzeptanz z. B. aufgrund regulatorischer Vorgaben oder expliziter Beschränkung der Anforderungen an die Qualität oder Quantität der kDL[14] denkbar sind. Der B3S stellt klar, dass bei Outsourcing o. Ä. die volle Verantwortung für eine geeignete Risikobehandlung beim Betreiber verbleibt.*

7 organisatorische und technologische Entwicklungsrahmenbedingungen

Auch wenn in den Vorgaben an die Geschäftsführungsverantwortung in den externen Quellen von IT-Strategie, Leitlinien, Richtlinien, Arbeitsanweisungen oder einfach nur von Verantwortung gesprochen wird, so werden im Detail diese Dokumentformen im Rahmen der Prüfung nur dahingehend unterschieden, ob sie durch die Geschäftsführung legitimiert wurden oder nicht.

Zur Testumgebung [IDW PS 880,Tz55] weist die Systemdokumentation [1021, A.2 LORA Mobile Projektmanagement, Softwareentwicklung und Qualitätssicherung, 4.2.3 Systemtest]

[13] Siehe auch [SIZ-SITB, RQ0099].

[14] kDL = kritische Dienstleistung

einen Test *in einer der Produktivumgebung ähnelnden Testumgebung* an. Belege (z. B. durch die dabei entstehenden Testprotokolle) für das Verfahren wurden nicht vorgelegt.

7.1 K346, K341 Anwendungsentwicklung bis Freigabe

Die Systemdokumentation geht als Entwicklungsstandard mit von SCRUM aus und [1021, A.3 Arbeitsanweisung Atlassian Suite Anwendung des Projektmanagement- und Entwicklungsprozesses von der Anforderung bis zur Veröffentlichung, 2. Programmiereransicht] weist mit Lehrbuchmaterial die Führung eines Backlogs an. Zur ebenfalls relevanten „Definition of Done“ wird eine dynamisch zu definierende Definition of Done angewiesen [1021, A.2 LORA Mobile Projektmanagement, Softwareentwicklung und Qualitätssicherung, 3.2.4 Source Code]. Weder Backlog noch die projektspezifische Definition of Done wurden vorgelegt.

Anforderungsmanagement im Bereitstellungsprozess (A)

Berücksichtigung von Fremdkomponenten

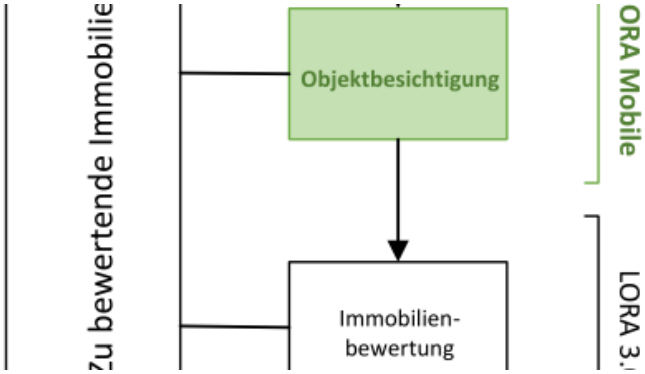
Schnittstellen zu anderen Produkten [AH OPDV94, 1.1.2.6] siehe unterhalb von Abschnitt *1 Prüfungsgegenstand*.

Es gibt eine Art Betriebshandbuch [1002, B.2. LORA Mobile - Dokumentation: Betrieb], dass seitens des Herstellers für den Lieferanten bzw. Provider erstellt wurde und damit für Sparkassen keine direkte Bedeutung besitzt und daher weitgehend während der Prüfung ignoriert wird.

Die NT Neue Technologie AG ist Hersteller der Software und „Housing-Provider“ für den Softwarelieferanten on-geo GmbH.

Design im Bereitstellungsprozess (A)

Die IT-Anwendung beliefert eine „Folgeanwendung“ mit Daten, siehe folgende Grafik:



[1002, A.1. Immobilienbewertungsprozess, 2. Skizze Bewertungsprozess]

Im Rahmen der Prüfung wurde die Dokumentation um die Vollständigkeitskontrolle der Datenübertragung ergänzt. Sie [1021, B.8 LORA Mobile Dokumentation: Datenaustausch] beschreibt das Zieldokument als Base64 codiert. Das Format hat die Eigenschaft, dass unvollständige Daten erkannt werden. Inhaltliche Fehler bei der Übertragung sind durch eine Verschlüsselung ausgeschlossen, die sich im Fehlerfall nicht wieder entschlüsseln ließe.

[15] Produktbeschreibung ist im Prüfungsumfeld definiert als die Gesamtheit aller VOR Vertragsschluss dem Nutzer bereitgestellter Artefakte, darunter können je nach Festlegung des Lieferanten Flyer, Broschüren, Verträge, Produktbeschreibungen, Handbücher oder Demoversionen gehören. Vorsicht: Für die Vollständigkeit ist nach deutscher Rechtsprechung der Lieferant verantwortlich und es gibt Normen, die Minimalangaben benennen.

7.1.3 Programmierung im Bereitstellungsprozess (A)

Programmierkonventionen [FARR18, E. Checkliste zur IT-Systemprüfung, 58.] liegen vor [1002, A.2 LORA Mobile - Projektmanagement, Softwareentwicklung und Qualitätssicherung, 3.2.4 Source Code]. Darin enthalten sind die Ergänzung der Programmiersprachen um C#, Schichtenmodelle, Namensregelungen, Zulässigkeit bestimmter Komponenten, Versionsführung, Fehlerbehandlungen und kommentierter sowie übersichtlicher Programmcode.

Dokumentierte Entwicklertests wurden vorgelegt. [1002, A.8 Testprotokolle, Testprotokoll LORA Mobile] bestätigt die erfolgreiche Durchführung der Entwicklertests auf der Web-Variante. [1002, A.8 Testprotokolle, Testprotokoll LORA Mobile NG] bestätigt die erfolgreiche Durchführung der Entwicklertests auf der App.

7.1.4 Testen im Bereitstellungsprozess (A)

Geforderte Whitebox-Tests sind als Entwicklertests dokumentiert, siehe Abschnitt *7.1.3 Programmierung im Bereitstellungsprozess (A)*.

Ein Testprotokoll zur Abdeckung der Funktionalität [IDW PS 880,Tz68] liegt vor [1002], enthält kurze Testprotokolle, aus Sicht des Risikos ist die Kürze aber vertretbar.

Der Umgang mit den von der IT-Anwendung ausgehenden Risiken [IDW PS 880, Tz49], [IDW PS 880,Tz68], [SIZ-SITB, RQ0091] ist durch Testprotokolle belegt [1002, A.8 Testprotokolle, Testlog: Unit-Test (der App)], sie enthalten Negativtests zur Passwortpolicy, zur falschen Berechtigung, Datenvalidierungsfehler und zur Entschlüsselungsverweigerung.

Die festgelegten Sollmaßnahmen sollten belegt werden [BAIT,Tz13]. Definiert sind als Sollmaßnahmen sogenannte Qualitätsmerkmale [1002, A.2 LORA Mobile - Projektmanagement, Softwareentwicklung und Qualitätssicherung, 4.2 Testablauf nach ISTQB]. Die vorgelegten Testprotokolle stellen zwar dar, dass es Tests der neuen Funktionen gibt, lassen zu den Qualitätsmaßnahmen bzw. deren Erreichung keine Aussage zu.

Die fachliche Nutzbarkeit von Vorversionen mit vergleichbare Funktionalität ist nachgewiesen, siehe Abschnitt *8 Nachweise von Dritten*.

Geänderte Komponenten können einem verkürzten Test, einem sogenannten Regressionstest, unterzogen werden, wenn ein vollständiger Test für Vorversionen dokumentiert ist. Die Systemdokumentation [1002, A.4 Arbeitsanweisung - Qualitätssicherung der Softwareentwicklungsprozesse, 3. Anwendung der Testverfahren] beschreibt das Verfahren von Regressionstests, nennt sie aber nicht so. Grundsätzlicher Inhalt sind damit die sogenannten Unit-Tests, die in die Gruppe Entwicklertests fallen.

7.1.4.1 Lasttest

Ein Lasttestprotokoll 1021, A.8 Testprotokolle, Testprotokolle Last- und Penetrationstest] benennt die auf einer undokumentierten Softwareversion durchgeführten Lasttests mit bis zu 50 parallelen Nutzern und gibt dazu Screenshots eines Auswertungstools wieder. Es wird sichtbar, dass der Test vor rund fünf Jahren durchgeführt wurde und der Hersteller gibt an, dass neue Tests wegen fehlender signifikanter Änderungen nicht wiederholt wurden. Das Testergebnis ist glaubhaft.

7.1.5 Risikomanagement und Projektleitung

Der Hersteller gibt als Projektmanagementverfahren [1021, A.2 LORA Mobile - Projektmanagement, Softwareentwicklung und Qualitätssicherung, 2. Projektmanagement] das amerikanische POSDCORB-Modell[16] als Projektmanagementstandard an. Der Prüfer sieht keine Veranlassung, das im Detail zu hinterfragen. Insbesondere sind hier als interner Auftraggeber on-geo und als Hersteller die NT AG und damit zwei unterschiedliche Unternehmen involviert.

Als Koordinations-Tool wird das Standard-Tool Atlassian-Suite angegeben [1021, A.2 LORA Mobile - Projektmanagement, Softwareentwicklung und Qualitätssicherung, 2.3 Koordination].

Die Prüfung behandelt die Projektsicht aus der Sicht eines einsetzenden Institutes. Themen, die zwar für den Hersteller oder den Lieferanten der IT-Anwendung im Rahmen des Projektmanagements relevant sind, nicht aber auf ein nutzenden Institut durchschlagen, werden im Rahmen der Prüfung ignoriert.

7.1.6 Versionsverwaltung und Identifikation der IT-Anwendung

Die Systemdokumentation [1021, A.6 Richtlinie für die Versionierung von Anwendungen] beschreibt die aus 4 Stellen bestehende Versionsnummer der Web-Anwendung und stellt klar, dass die letzte Zahl automatisch ermittelt wird und lediglich der eindeutigen Identifizierung dient, aber weder aufsteigend noch garantiert sondern nur sehr wahrscheinlich eindeutig ist. Für die App gilt ein ähnliches Verfahren, hier ist die letzte Stelle aber manuell gebildet und damit eher aufsteigend aber hinsichtlich ihrer Eindeutigkeit von manuellen Aktionen abhängig.

7.1.6.1 Version der Produktbeschreibung, Pflichtenheft oder Releasenotes

Als Prüfungsergebnis wird die Produktbeschreibung jetzt versioniert und enthält die Softwareversion und eine eigene Stand-Angabe.

Wartungs- und Supportmaßnahmen

Wartungs- und Supportmaßnahmen richten sich nach dem Vertrag zwischen Lieferant und Nutzer, der hier vorliegt aber nicht Prüfungsthema ist.

7.1.8 inhaltliche Testabdeckung in Testprotokollen

Oben wurde schon darauf hingewiesen, dass die vom Hersteller definierten Qualitätsmerkmale nicht umfassend durch Testprotokolle belegt sind. Mit Hinblick auf den Schutzbedarf kann diese Situation hingenommen werden.

7.1.9 formale Testdokumentation

Von der Testdokumentation wird die Einhaltung der [BAIT,Tz41] erwartet, die Herstellerseitigen Festlegungen und die darauf basierenden Protokolle sind aber formal nicht so detailliert. Auch hier ist der relativ überschaubare Schutzbedarf als Legitimation möglich.

Als Qualitätsstandart nennt die Systemdokumentation [1021, A.2 LORA Mobile - Projektmanagement, Softwareentwicklung und Qualitätssicherung, 4.2 Testablauf nach ISTQB]: „*Softwarequalitätsmanagement in Anlehnung an das ISTQB*“.

[16] Lt. Gabler Wirtschaftslexikon: *von der amerik. Management Process School entwickeltes Akronym für die wichtigsten Aufgaben des Managements: Planning (P), Organizing (O), Staffing (S), Directing (D), Coordinating (C), Reporting (R), Budgeting (B).*

Die Systemdokumentation [1021, A.7 Herstellerfreigaben] enthält eine Vorstandslegitimation an Herrn Kotlinsky mit der Erlaubnis, Freigaben zu erteilen. Folgende Freigabeerklärungen wurden dem Prüfer vorgelegt:

- [1021, A.7 Herstellerfreigaben, Freigabe für LORA Mobile (live)] enthält eine Herstellerfreigabe für „LORA Mobile (live)“ in der Version 1.4.115.5.
- [1021, A.7 Herstellerfreigaben, Freigabe für LORA Mobile NG App] enthält eine Herstellerfreigabe für „LORA Mobile NG App“ in der Version 2.6.29.4.

8 Nachweise von Dritten

Die Programmfreigabe nach OPDV 1/2015 ist durch den Hersteller respektive Lieferanten oder Provider vorzulegen. Diese Freigabeerklärung ist dem nutzenden Institut zusammen mit dem fertigen Prüfungsbericht zu übergeben.

- [1002, Zertifikat - Geprüftes Verbundrechenzentrum hochverfügbar Stufe 3 tekPlus] stellt ein ISO 27002-Zertifikat für die Verfügbarkeit des vom Lieferanten angemieteten Rechenzentrums dar.
- [1002, ISO 27001-Zertifikat auf der Basis von IT-Grundschutz] stellt ein vom BSI ausgestellten ISO 27001-Zertifikat dar.

Eine separate Prüfung auf die [ISO IEC 27001] wird nicht durchgeführt, für den Prüfer sind die Themen ausreichend im [SIZ-SITB] behandelt.

Eine separate Prüfung auf die [EN ISO 9000] wird nicht durchgeführt.

Der Abschnitt *7.1.9 formale Testdokumentation* enthält Zertifikate von Prüfungsorganisationen.

Die Systemdokumentation [1021, C.1 Auszug Referenzliste Sparkassen, C.1 Auszug Referenzliste Sparkassen] enthält eine Referenzliste von Sparkassen.

9 Folgeprüfungen

9.1 Prüfungsergebnisse der Version LoraMobile 1.4.54, gehört zu Lora 3.0

9.1.1 Detailbewertung der Bereitstellungs- und Wartungsprozesse (Projektverantwortung)

Der Prüfbericht zur IT-Anwendung *LORA* beschreibt Themen, die zu großen Teilen auch in der hier geprüften Zusatzkomponente zu *LORA* relevant sind, hier aber nur wiederholt werden, wenn explizit Aussagen zu *LORA Mobile* getroffen werden.

9.1.1.1 Nachvollziehbares Projektmanagement

Zum Projektmanagement erklärt der Hersteller [324, 2. Projektmanagement]: *Das Projektmanagement umfasst in Anlehnung an das POSDCORB-Modell (amerik. Management Process School) die Aufgaben Planning (P), Organizing (O), Staffing (S), Directing (D), Coordinating (C), Reporting (R), Budgeting (B).* Ein Planungsstandard ist damit vorgesehen.

Der Hersteller hat ein Dokument vorgelegt [324, Legitimation zur Freigabe von Anwendungen und Entwicklungen der NT.AG Juni 2016], in dem per Vorstandsunterschrift sowohl der Vorstand in Vertretung als auch Herr Kotlinsky und Herr Lamprecht berechtigt werden, Herstellerfreigaben zu erteilen.

Die von aufgestellte Forderung, „*Bedeutende Schadensfälle sind unverzüglich hinsichtlich ihrer Ursachen zu analysieren*“, ist wegen fehlender Zusage einer Umsetzung durch den Lieferanten zu hinterfragen. Der Prüfer kann keine Gefahr bedeutender Schadensfälle für das Institut ausmachen, insofern wäre eine Umsetzung durch den Lieferanten formal verzichtbar. Ein Institut könnte von dieser Bewertung abweichen, müsste dann aber in die Vertragsverhandlungen mit dem Lieferanten eintreten oder andere Analysen umsetzen.

Zu Wartung und Support enthält das vorgelegte Vertragsmuster [327, 3.2 Sıcherheit, Supportleistungen und Serviceverfügbarkeit] in der aktuellen Version Reaktionszeiten und Behebungsziele. Aus Prüfungssicht sind folgende Teilaspekte zu kombinieren:

- Die Anwendung unterstützt weder handelsrechtlich relevante noch rechnungslegungsrelevante Geschäftsprozesse, insofern ist dem Institut aus externer Sicht freigestellt, ob Wartung und Support zu regeln sind oder nicht. Zu institutseigenen Vorgaben kann der Prüfer keine Aussage treffen.
- Im Vergleich zu früheren Versionen des Vertragsmusters ist in der aktuellen Version kein implizieter Ausschluss von Rechtsmängeln mehr enthalten, diese sind in der vorgelegten Version insofern mit abgedeckt.
- Es wird in der höchsten Priorität zwar neben einer Reaktionszeit auch ein Problembehebungsziel benannt, dieses wird juristisch aber dadurch unverbindlich, da es nicht eingehalten werden muss sondern nur eingehalten werden „*soll*“.
- Das Institut ist bei einer fremdgehosteten IT-Anwendung, wie sie durch LORA Mobile dargestellt wird, bei beliebigen technischen Problemen nicht in der Lage ohne Support eine Behebung des Problems durchzuführen, es besteht insofern eine Abhängigkeit von der Supportbereitschaft.
- Zusammenfassend ist es sinnvoll, einen ausreichenden Support abzufordern, eine Detailbewertung muss aber durch das Institut erfolgen.

Die vorgelegte Herstellerfreigabe [324, Freigabe für LORA Mobile (live) Juni 2015] umfasst die ausreichend legitimierte Freigabe für LORA Mobile (live) in der Version 1.4.54.

9.1.1.1.1 Projektleitung

Zum Projektmanagement gibt der Hersteller an [315, 2. Projektmanagement] einen an das POSDCORB-Modell angelehnten Projektmanagementprozess anzuwenden. Wegen fehlender Risiken für ein nutzendes Institut wird diese Aussage nicht weiter hinterfragt.

Zur technischen Unterstützung seiner Entwicklungstätigkeiten benennt der Hersteller diverse Tools bzw. Standardvorgehen:

- *Abstimmung vom LORA Mobile Projektleiter mit dem NT.AG-Entwicklungsleiter* [324, 2.2 Ressourcen und Entscheidungen].
- *Das Projektberichtswesen fußt auf dem Einsatz der Atlassian-Suite* [324, 2.4 Reporting].
- *Als IDE (integrated Development Enviroment) wird das Microsoft Visual Studio 2012 verwendet* [324, 3.2.1 Browseranwendung].
- *Nutzung von etablierten Softwarebibliotheken wie log4net, Microsoft Entity Framework oder jQuery sowie die Verwendung von allgemein anerkannten Entwurfsmustern für das Design der Softwaremodule* [324, 3.2.1 Browseranwendung].
- *Die Programmierung der iPad App erfolgt(e) gemäß dem Apple SDK (Software Development Kit, aktuell Version 8.1) in der Apple-Entwicklungsumgebung Xcode (aktuell Version 6.1) mittels der Sprache Objective-C. Über die Apple-Entwick-*

lungssprache hinaus werden gleichfalls etablierte Softwarebibliotheken mitverwendet (u.a. CoreData.framework, MapKit.framework und Security.framework). Es handelt sich hierbei um eine native App für das Apple-Tablet iPad [324, 3.2.2 iPad App].

- *Für Serviceorientierte Anwendungen findet zusätzlich das SOA-Security-Kompendium des BSI (Version 2.01 aus 2009) Anwendung* [324, 3.2.4 Source Code].
- *Der Source Code wird in der Source Code-Verwaltung Microsoft Team Foundation Server (TFS) gehalten. TFS ist direkt in die IDE Visual Studio 2012 der Entwickler integriert und stellt ein professionelles Management des gesamten LORA Mobile-Source Codes von der Implementierung bis zum Release Management sowie der Versionierung und Archivierung Sicher* [324, Quellcode-Verwaltung].
- *Die NT.AG orientiert das Softwarequalitätsmanagement in Anlehnung an das ISTQB (International Software Testing Qualification Board) unter besonderer Berücksichtigung der agilen Vorgehensweise in der Entwicklung* [324, 4.2 Testablauf nach ISTQB].

9.1.1.1.2 Spezialprojekte

9.1.1.1.2.1 Elektronische Archivierung und Dokumentenmanagementsysteme

Rechtlich erforderliche Aufbewahrungsmaßnahmen sind weder umgesetzt noch als erforderlich sichtbar.

9.1.1.2 Fehlerfreie Herstellung der IT-Anwendung

In der IT-Anwendung werden diverse Datenstrukturen verarbeitet, dazu gehören Accountinformationen, Immobilienbeschreibung sowie Planungsinformationen zu den durchzuführenden Besichtigungsprojekten. Inhaltlich sensibel sind dabei die Accountinformationen, die nur soweit konkretisiert sind, dass die Zuordnung zwischen Mitarbeiter und seinen Daten transparent wird.

Der vom Hersteller mit „*POSDCORB-Modell*“ angegebene Standardprojektmanagementprozess [324, 2. Projektmanagement] müsste nach Auffassung des Prüfers die bei der vorliegenden Implementierungskritikalität die erforderlichen Schritte abdecken, es ist insofern nicht erforderlich, hier konkretere oder höhere Entwicklungsstandards zu fordern.

9.1.1.2.1 Anforderungserfassung (AE)

Eine mögliche Anforderung an einen Wartungs- und Supportvertrag deckt der Lieferant durch den bereitgestellten SaaS-Vertrag [327] ab.

Der Lieferant gibt an, dass alle Verträge, die nicht als SaaS-Vertrag [327] gestaltet sind, veraltet sind.

Die IT-Anwendung deckt mit ihren Funktionen ausschließlich den Geschäftsprozessteil ab, der den Immobilienbesichtigungsbericht zum Ziel ab.

Der Hersteller gibt an [315, 4.2 Testablauf nach ISTQB], dass im Test gegen folgende generellen Kriterien: *Funktionalität, Zuverlässigkeit, Benutzbarkeit, Effizienz, Änderbarkeit und Übertragbarkeit* getestet werden soll. Da keines dieser Qualitätsmerkmale im konkreten Anwendungskontext ein signifikantes Risiko darstellt, hält der Prüfer eine Überprüfung diese Aussage für verzichtbar.

9.1.1.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM)

9.1.1.2.2.1 Architektur und Betriebssicherheit

Diverse Gesetze und Verordnungen fordern eine ausreichende Berücksichtigung des Themas Sicherheit. Nach Herstellerangaben wird die Sicherheit durch den beim Hersteller mit „Last- und Penetrationstest“ benannten Test abgedeckt. Für die hier zu prüfende Softwareversion gibt das entsprechende Testprotokoll [328] an, dass entsprechend interner Regelungen auf diesen Test verzichtet wurde. Im Rahmen der Prüfung wurden auch Testprotokolle einer vorangegangenen Version 1.4.47 vorgelegt [314], in dem dieser Sicherheitstest als erfolgreich durchgeführt dokumentiert wurde. Grundsätzlich ist der hier erfolgte Verzicht auf eine Wiederholung im Rahmen eines sogenannten „Regressionstests“ als zulässig zu bezeichnen. Wegen der niedrigen Kritikalität kann dieses Verfahren akzeptiert werden.

Auch bei Komplettausfall der ITZ-Anwendung kann das Ergebnis, hier der Besichtigungsbericht, mit überschaubarem Zusatzaufwand durch Kamera und Standard-Office-Methoden ersetzt werden.

Zur Unterstützung der Designdurchführung beschreibt das Prozesshandbuch des Herstellers [301, 3.1.1. Basis] die Architekturvorgaben mit Standardmodellen für die jeweiligen Umgebungen. Diese Schritte kennt der Prüfer als Implementierungsunterstützung insbesondere für Entwicklungsprozesse für Mobilgeräte und sieht deren Nutzung damit als ausreichend nachgewiesen an.

9.1.1.2.2.2 Schnittstellen und sicherer Datenaustausch

Für ein Zwischenrelease wurden Lasttestprotokolle vorgelegt [300, 5. Lasttests], die über Schnittstellen kommunizieren.

Die im konkreten Einsatzumfeld erforderliche Verfügbarkeit wird durch den Prüfer mit relativ gering angenommen, bei Ausfällen steht dem Institut eine Kontaktaufnahme mit dem Provider zur Verfügung. Weitere Maßnahmen wären insofern vielleicht positiv, sind aber nicht erforderlich und werden damit auch nicht weiter geprüft.

Die Kommunikation zwischen Handgerät beim Besichtiger und Server funktioniert Web-basiert, ein Penetrationstest ist insofern erforderlich. Für ein Zwischenrelease wurde ein rein automatischer Penetrationstest dokumentiert [300, 4. Penetrationstests].

9.1.1.2.2.3 Integration in den Geschäftsprozess

Im Nutzungsumfeld der IT-Anwendung erfolgen die Anwendungskontrollen durch diejenigen Mitarbeiter, denen der Besuchsbericht zugeleitet wird. Das Handbuch weist ohne Sicherheitshinweise auf diese Aufgabe hin [318, 3. Web-/Browseranwendung].

9.1.1.2.3 Einhaltung von Programmierkonventionen

Zum erforderlichen Programmierungsinhalt sind durch den Hersteller Programmierkonventionen festzulegen, diese liegen formal vor [315, 3.2 Programmierung]. Die definierten Programmierkonventionen beschränken sich auf Lesbarkeit und Benennungen. Die vom BSI in definierten Programmierkonventionen sind nicht direkt angewiesen. Die Implementierung beschreibt der Hersteller [324, 3.2.1 Browseranwendung] unter Nutzung von Komponenten[17], die hier eine Risikoreduktion darstellen. Der verbleibende Mangel wird vom Prüfer wegen der geringen Kritikalität und dem vorgelegten Penetrationstestergebnis als ausreichend akzeptiert.

[17] Der Hersteller [324, 3.2.1 Browseranwendung] benennt technische Standards bei der Implementierung mit: Dot-Net Frameworks, Microsoft Visual Studio 2012, objektorientierten mehrschichtigen Softwarearchitektur mit Kapselung der Komponenten, etablierten Softwarebibliotheken wie log4net, Microsoft Entity Framework oder jQuery, Apple-Entwicklungsumgebung Xcode.

Weiter risikoreduzierend erklärt der Hersteller [324, 3.2.4. Source Code]: *Um eine hohe Qualität des Quellcodes sicherzustellen, wurden projektweite Programmierkonventionen vereinbart. Diese wurden auf der Basis allgemein anerkannter Programmierstandards, dem Microsoft C#-Programmierhandbuch sowie in Anlehnung an ausgewählte IT-Grundschutz-Kataloge erstellt. Für Serviceorientierte Anwendungen findet zusätzlich das SOA-Security-Kompendium des BSI (Version 2.01 aus 2009) Anwendung.*

Zum Versionsverwaltungssystem erklärt der Hersteller [324, 3.2.4. Source Code]: *Der Source Code wird in der Source Code-Verwaltung Microsoft Team Foundation Server (TFS) gehalten. TFS ist direkt in die IDE Visual Studio 2012 der Entwickler integriert und stellt ein professionelles Management des gesamten LORA Mobile-Source Codes von der Implementierung bis zum Release Management sowie der Versionierung und Archivierung sicher.*

9.1.1.2.4 Programm- bzw. Systemdokumentation

Die Beschreibung der Quellcode-Verwaltung [324, Quellcode-Verwaltung] umfasst auch Angaben zur Lage der Module in der Qualcode-Verwaltung.

9.1.1.2.5 Durchführung und Dokumentation der Entwicklertests

Die Forderung nach dokumentierten Entwicklertests wird durch den Hersteller dadurch umgesetzt, dass im Testprotokoll die erfolgreiche Durchführung von „*146 Unit-Tests*“ ohne weitere Angaben dokumentiert wird. Da technisch bei Unit-Tests das Protokoll ein oder ausgeschaltet werden kann und auf Grund der geringen Kritikalität der Entwicklertests akzeptiert der Prüfer diese Sachlage als ausreichend.

9.1.1.3 Nachweis einer vollumfänglichen Qualitätssicherung

9.1.1.3.1 Nachweischarakter von Testergebnissen

Qualitätssicherungsunterlagen müssen nicht nur Belegfunktion sondern auch eine Nachweisfunktion besitzen, die grundsätzlich einer ausreichenden Unabhängigkeit bedarf. Der Hersteller liefert als Nachweis einer Qualitätssicherung eine Referenzliste von Nutzern [326]. Diesen Nachweis akzeptiert der Prüfer, da die damit dokumentierten Abnahmen durch andere Marktteilnehmer eine existierende Qualitätssicherung voraussetzen. Wichtig: Es geht bei diesem Nachweis nur um das Vorhandensein, nicht um den Inhalt.

Als weiterer Nachweis erfolgreicher Tätigkeiten im Bereich Qualitätssicherung wird das vorgelegte ISO27001 Zertifikat [309] akzeptiert, in dem für das RZ u. a. die Einhaltung „*organisatorischer Anforderungen*“ bestätigt wird.

9.1.1.3.2 Vollständige Qualitätssicherung

Aussagen zu Whitebox-Tests siehe oben unter Entwicklertests.

Zur Bestätigung der Qualitätssicherung wurden eine Beschreibung der beim Hersteller laufenden Qualitätssicherungsprozesse [315, 4.2 Testablauf nach ISTQB], das Testprotokoll [328] sowie die resultierende Herstellerfreigabe [317] vorgelegt.

Da im Betrieb auch mit Störungen zu rechnen ist, sind auch diese durch Tests abzudecken. Testprotokolle dazu [300], [328] wurden vorgelegt.

Die vollständige fachliche Prüfung definiert der Hersteller [315, 4.2.4 Abnahmetest] mit Tests auf Akzeptanz des Auftraggebers, konkrete des Softwarelieferanten und unter Einbeziehung von Pilotkunden. Auf Grund der fachlichen Verantwortung des Lieferanten –hier ongeo–, der organisatorisch nicht mit dem Hersteller –hier die NT– identisch ist, geht der Prüfer von einer ausreichenden Verantwortungsübernahme und Tests aus. Weiterhin sind in der oben bereit benannten Referenzliste nicht nur Pilotkunden sondern auch Echtkunden enthalten.

9.1.1.3.3 Lasttest

Lasttestergebnisse sind dokumentiert [316] und enthalten zusammenfassende Aussagen zu Tests, die als durchschnittliche Antwortzeiten 3,5 Sekunden unterschreiten.

Der sogenannte Überlasttest, also die Wiederherstellung nach technischen Problemen, wird durch das vorgelegte ISO27001-Zertifikat verzichtbar.

9.1.1.3.4 Qualitätsmanagement

Als Qualitätssicherungsstandard gibt der Hersteller eine teilweise Einhaltung des ISTQB-Standards an [324, 4.2 Testablauf nach ISTQB]. Genauere Prüfungen hierzu hält der Prüfer wegen der geringen Anwendungskritikalität für nicht erforderlich.

9.1.1.4 Bereitstellung und Identifikation des Liefergegenstandes sowie seiner Quellen

9.1.1.4.1 Versionsverwaltung und Identifikation

9.1.1.4.1.1 Produktbeschreibung, Pflichtenheft oder Releasenotes

Der Abschnitt zur Produktbeschreibung beschreibt die Funktionen auch aus Sicht der Abgrenzung detailliert genug, so dass die fehlende Versionierung einzelner referenzierter Teildokumente zwar unschön, aber nicht als kritisch zu werten ist.

9.1.1.4.1.2 Systemdokumentation, Programmdokumentation, Softwaredesigndokumente

Der Hersteller wurde aufgefordert, zur Version passende Dokumente zu liefern. Ein Versionskonflikt wurde dabei nicht festgestellt. Eine Risikoübertragung aus potenziell unpassender Versionierung auf die konkrete IT-Anwendung kann der Prüfer aber nicht erkennen.

9.1.2 Detailbewertung aus Sicht der Benutzer bzw. Fachbereiche

Der Prüfbericht zur IT-Anwendung *LORA* beschreibt Themen, die zu großen Teilen auch in der hier geprüften Zusatzkomponente zu *LORA* relevant sind, hier aber nur wiederholt werden, wenn explizit Aussagen zu *LORA Mobile* getroffen werden.

9.1.2.1 Sicherstellung der Vollständigkeit von fachlichen Anforderungen

In der Produktdokumentation wird eine implementierte „*Tourenoptimierung*“ benannt [304, Optionale Leistungen]. Das Handbuch weist ohne Warnhinweis darauf hin [318, Handbuch, 3.2.3 Planung (optional)], dass diese Funktion durch den Nutzer durch manuelles Umsortieren von zu besichtigenden Adressen umgesetzt werden muss und keine technisch darüber hinausgehende Unterstützung angeboten wird.

Das Institut wird vom Provider / Lieferanten Abrechnungen über die spezifische Nutzung der IT-Anwendung erhalten, die vom Institut kontrolliert werden sollten.

Die Nutzung der IT-Anwendung umfasst auch Geschäftsprozesse zur Einhaltung von Verordnungen, wie z. B. der Beleihungswertverordnung (BelWertV). Auf das hier erforderliche Spezialwissen – sprich die Nennung von spezifischen Kenntnissen – geht die Produktdokumentation nicht ein. Da die entsprechende Kenntnissicherstellung auch vom nutzenden Institut verantwortet wird, bleibt es bei diesem aus Sicht der Prüfung damit ansonsten folgenlosen Hinweis.

Zur Verhinderung unerlaubter bietet die IT-Anwendung die Möglichkeit, Nutzerberechtigungen festzulegen. Der Prüfer ergänzt hier, dass die vergebenen Nutzerrechte automatisch die Berechtigung erhalten, Kosten durch Nutzung der IT-Anwendung zu erzeugen während die vom Lieferanten benannten Voraussetzungen auf institutsinterne Kontrollprozesse nicht

eingehen. Das Institut sollte damit darüber nachdenken, in welcher Form die Rechnungskontrolle umgesetzt werden soll, die sich auf Basis der Nutzung der IT-Anwendung ergibt. Die Kostenverursachung selbst muss vertraglich mit dem Institut vereinbart werden, insofern ist eine Auflage im Rahmen der Prüfung hier verzichtbar.

Zur Sicherstellung einer datenschutzkonformen Nutzung ist der enthaltene automatisierte E-Mail-Versand entsprechend zu konfigurieren.

9.1.2.2 Fachliche Berücksichtigung von gesetzlichen oder normativen Vorgaben

9.1.2.2.1 BGB

Im Rahmen der Prüfung wurde deutlich, dass seitens des Lieferanten unterschiedliche Produkte mit unterschiedlichen Vertragsinhalten vertrieben werden. Es ist insofern im Rahmen der Prüfung darauf hinzuweisen, dass ausschließlich der „Software as a Service Vertrag Lora Mobile, 1.Januar 2015“ im Rahmen der Prüfung zu hinterfragen ist.

Die Anwendung stellt keine handelsrechtlich ausreichende Beauftragung fremder Besichtiger zur Verfügung. **Die Nennung von „Auftraggeber einer Besichtigung“ und die „Besichtigung durchführender Sachbearbeiter“ bezieht sich auf Mitarbeiter eines Unternehmens bzw. Institutes**. Insbesondere eine Fremdbeauftragung ist nicht legitimiert.

9.1.2.2.2 BDSG

Die von der IT-Anwendung bearbeiteten personenbezogenen Daten werden zum Teil und an unterschiedlichen Stellen der Produktbeschreibung und Handbücher genannt. Der Prüfbericht fasst diese Stellen wie folgt zusammen:

- Die Anwendung kennt Anmeldedaten des Mitarbeiters für das Login.
- Der Prüfer weist darauf hin, dass potenziell auch Immobilienmieter durch den Besichtiger erfasst werden könnten.
- Alle erfassten Daten werden durch das nutzende Institut erfasst, viele der dabei zu benennenden Personen besitzen keine Vertragsbeziehung zum Institut. Eine zwingende Voraussetzung unzulässige Daten zu erfassen, wird aber nicht sichtbar. **Es ist Aufgabe des Institutes, festzulegen, welche personenbezogenen Daten wie zu erfassen sind und diese Festlegung umzusetzen**.

Insbesondere für die grundsätzlich mögliche **Erfassung von Mieternamen in Besichtigungsberichten hat das Institut eine gesetzlich zulässige Form** [BDSG] **zu wählen**.

9.1.2.2.3 HGB

9.1.2.2.3.1 Handelsbriefe [HGB, §37a]

Die Übermittlung von Aufträgen an organisatorisch ausreichend abgegrenzte Organisationen (z. B. andere Unternehmen oder Institute) stellt einen Handelsbrief dar. Dieser Handelsbrief muss festgelegte Eigenschaften erfüllen, die durch die IT-Anwendung LORA Mobile nicht abgedeckt werden. **Die Nutzung der** enthaltenen **Beauftragungsfunktion ist** insofern **ausschließlich für Institutsmitarbeiter** bzw. Mitarbeiter des beauftragenden Unternehmens **zugelassen**. **Es ist sicherzustellen, dass** der Sachverhalt „**Auftragsvergabe**“ **keinerlei handelsrechtliche Implikationen besitzt**.

9.1.2.2.4 StGB

§303a Datenveränderung stellt potenziell die Kombination privater E-Mails mit Spam-Filtern unter Strafe. In der hier betrachteten IT-Anwendung kommt eine E-Mail-Kommunikation

zum Einsatz. Der Hersteller erklärt hierzu [314]: *Der Versand der fertiggestellten Besichtigungsberichte (es handelt sich nicht um Gutachten) erfolgt durch die Handelsplattform an den jeweiligen Einsteller des Auftrages.* In LORA ist nach Aussage des Herstellers kein Virenscanner enthalten. Dessen Notwendigkeit kann aus Sicht von LORA Mobile auch nicht angenommen werden, insofern kann der Prüfer keinen Konflikt sehen.

9.1.2.2.5 TKG & TMG

In wie weit der Provider dem TKG und TMG unterliegt, fällt nicht in den Prüfungsumfang. Für ein Institut ist keine Relevanz dieser Gesetze sichtbar.

9.1.2.2.6 UrhG

Die Nutzungsrechtsübertragung an das nutzende Institut erfolgt im Falle der Nutzung des AppStores [327, 2.1. Nutzungsrecht] durch diesen Store.

Für die rechtlich zulässige Nutzung der App ist nach Aussagen des Herstellers eine vorherige Registrierung zum Erhalt der Anmeldedaten erforderlich.

Die Software wird von einem Hersteller entwickelt und vom Lieferanten dem einsetzenden Institut zur Verfügung gestellt. Damit das Institut eine gültige Nutzungserlaubnis erhalten kann, muss der Lizenzgeber, hier der Lieferant on-geo das dazu passende Nutzungsrecht erworben haben. Im vorgelegten Kooperationsvertragsauszug zwischen Hersteller und Lieferant [327, 2. Gegenstand der Vereinbarung] wird dabei die on-geo explizit mit der Vermarktung der hier betrachteten Softwarelösungen beauftragt. Eine ausreichende Erlaubnis liegt damit nach Auffassung des Prüfers vor.

Die Urheberschaft für eine Software ist nicht handelbar, d. h. für die von der NT AG erstellte Software verbleibt sie bei der NT AG bzw. dessen Rechtsnachfolger. Aussagen zu einer angeblichen Urheberschaft der on-geo sind in diesem Zusammenhang ungültig aber vorhanden [311, 11.7]. Negative Folgen sind aus dieser Feststellung für ein Institut nicht ableitbar.

9.1.2.2.7 AO (Abgabenordnung und Aufbewahrungsfristen), GoBD und Verarbeitung buchungsrelevanter Geschäftstransaktionen

In der Produktdokumentation werden Abrechnungen benannt. Der Hersteller stellt in internen Dokumenten [319, 2 AUFTRAGSABRECHNUNG] klar, dass Abrechnungen seitens des Lieferanten erfolgen und diese per Rechnung bzw. Rechnungsanhang an das nutzende Institut erfolgen. Seitens Institut besteht damit in LORA Mobile keine GoBD-Relevanz. **Eine Abrechnung gegenüber Institutskunden ist durch LORA Mobile nicht legitimiert**.

9.1.2.2.8 BelWertV (Beleihungswertermittlungsverordnung)

Die Produktunterlagen grenzen hier wie folgt gegen [BelWertV, § 4 (1) S. 3] ab: „*Das zu bewertende Objekt ist im Rahmen der Wertermittlung zu besichtigen*“ und „*Die Browser-/Webanwendung LORA Mobile und die LORA Mobile iPad App beziehen sich ausschließlich auf den Prozessschritt der Objektbesichtigung*“.

9.1.2.2.9 ZPO (Zivil-Prozess-Ordnung)

Die IT-Anwendung stellt keine Protokolle mit Nachweischarakter zur Verfügung.

9.1.2.2.10 ISO/IEC 27001:2005

Für das Rechenzentrum des Unternehmens „NT Neue Technologie AG, Peterstraße 1, 99084 Erfurt“ liegt ein bis zum 31. Juli 2016 gültiges Zertifikat mit der Aussage „*Geprüftes Rechenzentrum*“ vor [326]. Dieses Zertifikat bestätigt eine „*erfolgreichen Sicherheitsüberprüfung in Anlehnung an BS|-Grundschutz und ISO 27002*“.

9.1.2.3 Fachliche Administration der IT-Anwendung

Konfigurationsmaßnahmen sind nach Aussage des Herstellers durch den Lieferanten / Provider umzusetzen und können angeblich nicht durch das Institut vorgenommen werden.

9.1.3 Detailbewertung aus Sicht des Betreibers

Der Prüfbericht zur IT-Anwendung *LORA* beschreibt Themen, die zu großen Teilen auch in der hier geprüften Zusatzkomponente zu *LORA* relevant sind, hier aber nur wiederholt werden, wenn explizit Aussagen zu *LORA Mobile* getroffen werden.

9.1.3.1 Betriebsbereitschaft in einer Sparkasse oder deren VRZ

9.1.3.1.1 Betrieb und Abrechnung

Abzurechnende Rechenleistungen müssen ausreichend **transparent** sein. Der SaaS-Vertrag sollte dazu die anfallenden Kosten nennen, das dem Prüfer vorgelegte Muster enthielt hier keinen Wert. Da Kosten nur bei vorliegender vertraglicher Vereinbarung zu erstatten sind, sieht der Prüfer hier keinen Mangel.

9.1.3.2 Sicherstellung eines sicheren IT-Betriebes

9.1.3.2.1 IT-Dokumentation (K015)

Wesentlich für die technische Sicherheit sind die genutzten Verfahren. Der Hersteller dokumentiert für den Penetrationstest die Nutzung des „*Open Vulnerability Assessment System (OpenVAS), Version OpenVAS-7*“. Das Ergebnisprotokoll liefert die bestandenen Sicherheitstests ohne Mängel.

9.1.3.2.2 Archivierungsmedien, -fristen (K020)

Sofern die IT-Anwendung zur Erteilung von Fremdbeauftragungen genutzt würde, was formal aus dem Prüfungsumfang ausgeklammert ist, würde als eine der ersten Institutsaufgaben die Klärung der handelsrechtlichen Aufbewahrung der entsprechenden Beauftragungen und Ergebnisse zu klären sein.

9.1.3.2.3 Identifikation / Authentisierung (K101)

Der Schutzbedarf der IT-Anwendung wird vom Prüfer mit maximal hoch bewertet, insofern stellen die folgenden Informationen immer noch eine ausreichende Umsetzung dar:

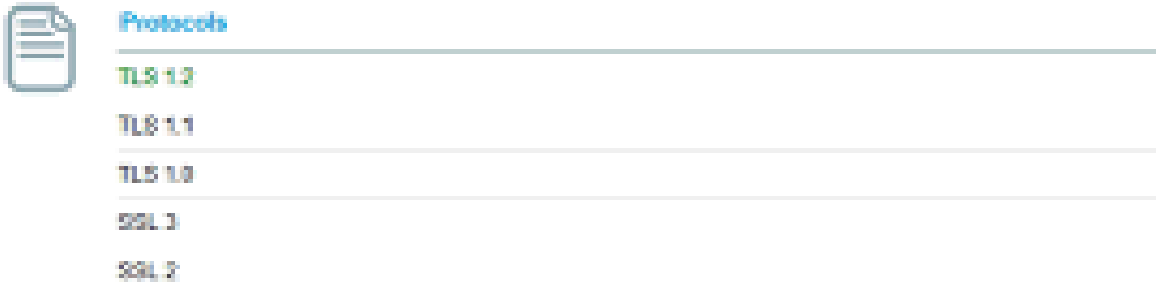
- Eine automatische Sperre der Anmeldung nach x Fehlversuchen ist nicht dokumentiert.
  Der Hersteller erklärt ergänzend: *Nach fünf Fehleingaben wird der Benutzeraccount gesperrt und kann nur durch Versand eines neuen Einmalpassworts an die beim Nutzer hinterlegte E-Mail-Adresse wieder freigeschaltet werden. Dieser Versand kann nur über die Administration ausgelöst werden. Dies gilt sowohl für die Webanwendung als auch für die iPad-App.*
- Eine potenziell erfolgte Sperrung müsste durch den Provider / Lieferanten aufgehoben werden.
- Ein nach Timeout wirksames Logout ist nicht dokumentiert.
  Der Hersteller ergänzt hierzu: *In der App gibt es kein direktes Timeout für den Login, da es sich um eine Offline-Anwendung handelt und der Nutzer nie dauerhaft auf einem Server eingeloggt ist. Eine Verbindung zum Server wird nur beim Datenaustausch aufgebaut, wobei kein Login, sondern eine Token benutzt wird. Jedoch gibt es ein lokales an das Timeout angelehntes Verfahren der App. Beim Öffnen*

der App muss der Nutzer jeweils den von ihm definierten Passcode, welcher stellvertretend für den Login anzusehen ist, eingeben. Insofern muss der Nutzer mit jeder neuen App-Sitzung seine Identität bestätigen. Als Öffnen der App gilt auch das Erwachen des Geräts aus dem Standby.

- In der Webanwendung ist der Login entweder nur während der aktuellen Browser-Sitzung gültig (bis Browser geschlossen wird) oder solange bis der Nutzer sich aktiv ausloggt. Welche Variante genutzt wird, entscheidet der Nutzer:
- (siehe Funktion „Ich möchte auf diesem Computer angemeldet bleiben“).
- Nutzer können lt. Handbuch ihr Passwort und ihren Namen beliebig ändern, weitere Einschränkungen zur Passwortnutzung waren in der Produktdokumentation nicht aufzufinden.

9.1.3.2.4 Vertrauenswürdige Kanäle (K106)

Der Hersteller gibt an [318, 4.5 Synchronisation]: *Zur Sicherheit zwischen dem Server und dem iPad, werden alle Daten über eine verschlüsselte SSL-Verbindung (HTTPS) übertragen.* Hinsichtlich der Sicherheitsfrage zu SSL bzw. TLS ergänzt der Hersteller: *Es wird eine TLS-Verschlüsselung genutzt. SSL wird nur genannt, da dies oft synonym für TLS benutzt wird. Der eingesetzte IIS unterstützt nur noch TLS.*



Welche TLS-Version eingesetzt wird, hängt vom Client ab (App: abhängig vom benutzten Framework; Web: abhängig vom Browser).

9.1.3.2.5 Verschlüsselte Datenablage (K107)

Zur Datenablage liefert das Sicherheitskonzept des Herstellers folgende Details [314, Sicherheit, Datenablage]: *Die mit der Tabletanwendung einhergehende Anforderung der Offlinearbeitsfähigkeit (z.B. Erfassen von Besichtigungsinformationen außerhalb bestehender Internetverbindungen) bedingt die Haltung von Daten auf dem Endgerät. Hierbei wurden zwei Aspekte verfolgt – zum einen Absicherung der abgelegten Daten und zum anderen Begrenzung des Datenumfangs. Hinsichtlich der auf das Gerät übertragenen Daten werden ausschließlich die aktiven Aufträge genau eines Sachverständigen bzw. Nutzers zur Verfügung gestellt. Nach Abschluss eines Besichtigungsauftrages erfolgt die umgehende physische Löschung. Die iPad-Applikation verwendet zur Datenablage einen eignen von den allgemeinen Daten getrennten Container. Hierin werden die jeweiligen Auftragsdaten verschlüsselt gespeichert (AES256, ausgenommen Forum, Bildbezeichner und erfasste Kubatur/Wohnfläche), so dass bei einem eventuellen Abhandenkommen des Geräts kein Zugriff durch unbefugte Dritte (z.B. Auslesen der auf dem Gerät gespeicherten Daten mittels Drittsoftware) erfolgen kann. Die Ver- und Entschlüsselung der Daten findet zur Laufzeit der Applikation auf dem iPad statt (Hardware Encryption). Auftragsbezogene und insofern sensible Daten werden zu keiner Zeit unverschlüsselt dauerhaft auf dem Gerät gespeichert. Die zum Einsatz kommende Technologie wurde seit iOS 4.0 in den offiziellen Frameworks von Apple integriert.*

9.1.3.2.6 Key- Management (K108)

Zum Speicherungsverfahren der Passworte erklärt der Hersteller [314]: *Die Passwörter werden in der Datenbank grundsätzlich nicht umkehrbar verschlüsselt ("Hash") hinterlegt. Um die Sicherheit zusätzlich zu erhöhen, werden vor der Verschlüsselung zufällig generierte Werte an das Passwort angehangen („Salt“). Der Datenaustausch zwischen der LORA Mobile Webanwendung und der Datenbank erfolgt über einen "technischen" Datenbanknutzer. Die Datensätze sind dabei durch die technische Infrastruktur geschützt, sodass der Anwender über die Benutzeroberfläche keinen direkten Zugriff auf die Datenbank hat.* Die technische Infrastruktur wurde extern zertifiziert [309].

9.1.3.2.7 Sicherer E-Mail-Verkehr (K109)

Zur IT-Anwendung gehört auch die Übermittlung von potenziell sensiblen Auftragsinformationen per E-Mail. Der Hersteller gibt hierzu an [314]: „… *haben wir folgende personenbezogene Daten in den E-Mails aus LORA Mobile identifiziert: Die E-Mail-Vorlage einer Unterstützungsanfrage enthält die vollständige Objektadresse sowie den Namen und die Telefonnummer des Ansprechpartners der Besichtigung. Bei einer Zuweisung eines Auftrages an einen Sachverständigen erhält dieser den Kundennamen und die Kundennummer. Weitere in der E-Mail-Vorlage enthaltenen Daten, wie die Auftragsnummer oder unvollständige Adressangaben (ohne Hausnummer) fallen nicht unter personenbezogene Daten. Es besteht die Möglichkeit, die E-Mail-Vorlagen auftraggeberindividuell zu konfigurieren, sodass auf Wunsch auf bestimmte Daten in den versendeten E-Mails verzichtet werden kann“*. **Im Institut ist** damit **sicherzustellen, dass zu den Konfigurationsmöglichkeiten der E-Mails auch Datenschutzaspekte ausreichend umgesetzt werden**.

Der Versand von E-Mails, die im Inhalt Weblinks enthalten, bei denen man sich erst einloggen muss, entspricht im Kern dem Versand von Phishing-E-Mails und sollte daher -soweit möglich- vermieden werden. Wird jedoch kein anklickbarer Link angegeben, muss der Empfänger, hier dann ein Institutsmitarbeiter, diesen Link extern und z. B. über seine eigenen Lesezeichen aufrufen. Ein solcher Versand von gefährdenden E-Mails entspricht der Standardkonfiguration der IT-Anwendung. **Das Institut hat** insofern **festzulegen, ob in den vom System versandten E-Mails direkt der Link auf das Zielsystem**, z. B. http://www.loramobile.de, **enthalten sein soll oder nicht und diese Entscheidung durch den Lieferanten umsetzen zu lassen**.

9.1.3.2.8 Protokollierung (K110)

Protokollfunktionalitäten wurden während der Prüfung nicht identifiziert. Eine Notwendigkeit dazu kann der Prüfer nicht sehen.

9.1.3.2.9 Härtung der Systeme (K112)

Der Hersteller gibt an [314]: *Die Verantwortlichkeit für die Härtung der mobilen Endgeräte liegt beim Institut. Ein Hinweis dazu befindet sich im Handbuch im Kapitel "2. Zugang".*

9.1.3.2.10 Datensicherung (K318)

Das Institut ist auf eine ausreichende Datensicherung angewiesen, die im vorliegenden Geschäftsprozess zwischen der institutsinternen Beauftragung eines Kollegen bis zur Bereitstellung des Besuchsberichtes an die nachgelagerten Geschäftsprozessbearbeiter angelegt sein muss. Der Sicherungszeitraum innerhalb des von der IT-Anwendung abgedeckten Geschäftsprozesses ist damit als relativ kurz anzunehmen. Unter dieser Rahmenbedingung sieht es der Prüfer für ausreichend an, dass das betreibende Rechenzentrum zwar eine allgemeine Datensicherungspflicht besitzt und bestimmt auch umsetzt, juristisch die Verantwortung dafür aber beim nutzenden Institut zu sehen ist. Der Hersteller, der dabei kein Vertragspartner wird, wiederspricht zwar, aber aus Sicht des Prüfers stellen folgende Aussagen des SaaS-Vertrages [327, 10.3] ausreichend klar, dass nicht das RZ sondern das nutzende

Institut für die Datensicherung verantwortlich ist: *Für die Wiederbeschaffung von Daten haftet der Auftragnehmer im Übrigen nur dann, wenn der Auftraggeber sichergestellt hat, dass diese Daten aus in maschinenlesbarer Form bereitgehaltene Datenbeständen mit vertretbarem Aufwand reproduzierbar sind.*

9.1.4 Detailbewertung bei ganz oder teilweise ausgelagertem Betrieb

9.1.4.1 Gesetzliche und normative Vorgaben

9.1.4.1.1 §11 BDSG, §§241,311 BGB - Datenschutz

Sowohl die nach BDSG erforderliche Benennung der „**technisch organisatorischen Maßnahmen**“ als auch der Beleg über ein erfolgreich durch die Schufa durchgeführtes Datenschutzaudit liegen vor [326]. Bei diesen Dokumenten ist aber eine **Einbindung in den Vertrag** mit dem jeweiligen Institut nicht sichtbar und insofern **durch das Institut sicherzustellen**.

Unabhängig von der Feststellung, ob eine rechtlich relevante Auslagerung vorliegt oder nicht, stellt die Tatsache, dass der Betrieb der Anwendung nicht durch das Institut selbst sondern durch ein Rechenzentrum betrieben wird, eine nach BDSG relevante Auftragsdatenverarbeitung dar.

Final zu bewerten ist nicht ein potenziell existierender Mustervertrag, sondern der tatsächlich zwischen einsetzendem Institut und Betreiber vereinbarte Vertrag, insofern haben die folgenden Aussagen nur vorläufigen Charakter. **Das einsetzende Institut muss prüfen, ob alle Belange ausreichend erfüllt sind**.

gesetzliche Vorgabe an den Vertragsinhalt nach BDSG §11 Abs. 2 (BDSG-Novelle II: In Kraft getreten am 1. September 2009 zum Thema Auftragsdatenverarbeitung)	**Hinweis auf Behandlung im Mustervertrag**
eventuelle Erlaubnis gegenüber dem Auftragnehmer zur Einschaltung von Subunternehmern	[313, 4. Rechte und Pflichten] stellt die zwischen Institut und on-geo geltenden Regeln auch im Subunternehmerverhältnis zur NT AG her. [327] dito. Die NT AG hat RZ-Dienstleistungen in einem weiteren RZ beauftragt.

10 Anlagen

Literaturverzeichnis

Bei der Prüfung wurden folgende Artefakte[18] vollständig berücksichtigt, im Dokument selbst werden weitere Referenzen durch eckige Klammern gekennzeichnet und dabei jeweils die

[18] Berücksichtigte Artefakte (SW-Teile und Dokumente) werden in den Prüfungsdokumenten mit abkürzender Notation der Quelle hier mit [<lit-nr>] bezeichnet, wenn dieses Artefakt im Literaturverzeichnis auftaucht. Konkrete Inhalte innerhalb dieser Quelle werden dabei möglichst auch detaillierter angegeben:
[<lit-nr>, <Abschnitt>] Der Abschnitt kann dabei auch aus der Abschnittsnummer gebildet werden
[<lit-nr>, S.<Seitennummer>] Als Seitenangabe im Dokument
[<lit-nr>, XYZ] wenn XYZ in der speziellen Dokumentenform eine Stelle eindeutig kennzeichnet, bei Tabellenkalkulationsprogrammen z. B. die Zellennummern.

ID-Nummer des Dokumentes angegeben, Prüfungsvorgaben sind durch Kurzbezeichnungen gekennzeichnet, die im Abschnitt *2.2.1 Prüfungskriterien aus externen Vorgaben* aufgelistet werden.

[300] LORA Mobile Dokumente für Testierung nach OPDV durch SIZ, Oktober 2014

[301] 1. Prozessdokumentationen; LORA Mobile - Projektmanagement, Softwareentwicklung und Qualitätssicherung, (Stand Aug. 2014)

[304] 2. Soll-Beschreibung der IT-Anwendung; LORA Mobile Überblick (Stand Nov. 2013)

[309] 3. Nachweise; TÜV-Zertifikat NT.AG (Stand Aug. 2014)

[311] 4. Verträge; Angebot LORA Mobile an die Mustersparkasse - Anlage 1: Allgemeine Bestimmungen zur Softwareüberlassung für die LORA-Immobilienplattform, LORA-Gutachterlösung, LORA-Besichtigerlösung und LORA-Wertschätzerlösung (Stand 01.03.2010)

[313] 4. Verträge; Kooperationsvereinbarung on-geo GmbH <-> NT AG vom 14.12.11

[314] LORA Mobile Dokumente für Testierung nach OPDV durch SIZ, Januar 2015

[315] LORA Mobile – Projektmanagement, Softwareentwicklung und Qualitätssicherung (Stand Jan. 2015)

[316] Testprotokolle (Stand Jan. 2015)

[317] Herstellerfreigabe (Stand Jan. 2015)

[318] Vertragsanlage / Handbücher

[319] Dokumentation Mandantifizierung der Daten in LORA Mobile (Stand Jan. 2015)

[324] 1. Prozessdokumentation

[326] 3. Nachweise

[327] 4. Verträge
- Software as a Service Vertrag Lora Mobile, 1.Januar 2015

[328] Testprotokolle

[1002] LORA Mobile Dokumente für Testierung nach OPDV durch SIZ, Juli 2019
13.08.2019 13:18 8.945.984 /190813 E Komplettdokument/LORA Mobile - Unterlagen für Testierung nach OPDV.pdf

[1010] 19.08.2019 14:08 56.756 /190819 P Webabruf/https _www.loramobile.de_Content_Site.css _=1.4.117.2.css

[1011] 20.08.2019 16:20 134.544 /190820 P Eigentümerstrukturen/190820_Vorschau Firmenprofil NT Neue Technologie Aktiengesellschaft.pdf

[1012] 20.08.2019 16:28 414.558 /190820 P Eigentümerstrukturen/8170601474_Firmenprofil.pdf

[1016] LORA Mobile Dokumente für Testierung nach OPDV durch SIZ, ohne interne Versionierung
27.09.2019 17:57 234.275 /190927 zweite Einreichung/2019-09-27 Erläuterungen Befundliste.pdf

[1017] Ergänzungsangebot LORA Mobile, 19. September 2019
19.09.2019 10:39 216.434 /190927 zweite Einreichung/Ergänzungsangebot_LORA Mobile.pdf

[1018] Angebot LORA, 13. September 2019
13.09.2019 15:20 476.106 /190927 zweite Einreichung/Hauptvertrag_LORA SPK Muster.pdf

[1020] LORA Mobile Organisatorische Voraussetzungen, Stand: August 2019
27.09.2019 16:56 231.842 /190927 zweite Einreichung/LORA Mobile - Organisatorische Voraussetzungen.pdf

[1021] LORA Mobile Dokumente für Testierung nach OPDV durch SIZ, Juli 2019
27.09.2019 17:57 11.814.751 /190927 zweite Einreichung/LORA Mobile - Unterlagen OPDV_2.Einreichung09_2019.pdf

[1022] Benutzerhandbuch LORA Mobile / LORA Mobile NG App, Stand: September 2019
27.09.2019 16:59 2.381.492 /190927 zweite Einreichung/LORA Mobile Dokumentation Benutzerhandbuch.pdf

[1023] Musterbesichtigungsbericht (Außen- u. Innenbesichtigung), Standard 2018
27.09.2019 16:52 565.583 /190927 zweite Einreichung/Muster_Besichtigungsbericht.pdf

10.2 Schutzbedarfsanalyse durch den Hersteller respektive Lieferanten

Die Systemdokumentation [1021, A.1. Immobilienbewertungsprozess, 4.2 Risikoabschätzung aus Sicht der Informationssicherheit] benennt den vom Hersteller umgesetzten Schutzbedarf [BAIT,Tz43] mit:

- Vertraulichkeit hoch
- Integrität normal
- Verfügbarkeit hoch.

10.3 Bestätigung der gesetzlichen Vertreter

Wurde nicht vorgelegt.

Vorschlag einer Freigabeerklärung durch den Lieferanten oder Hersteller

Als Hilfe wird folgender Vorschlag übergeben, der ggf. anzupassen ist:

> Betreff: Programmfreigabe nach OPDV 1/2015 für die IT-Anwendung LORA Mobile
>
> Hiermit erteilt die NT Neue Technologie AG als Hersteller / on-geo GmbH als Lieferant die Programmfreigabe nach OPDV 1/2015 für die IT-Anwendung LORA Mobile.
>
> Details zur Versionierung der IT-Anwendung, deren Herstellungsprozess und Eigenschaften, sowie der Legitimation zu dieser Programmfreigabe ergeben sich aus dem beigefügten Prüfungsbericht der SIZ GmbH. Dieser Prüfungsbericht ist Bestandteil der Freigabeerklärung.
>
> Der Unterzeichnende bestätigt die Einhaltung der im Prüfungsbericht benannten Standards und der kaufmännischen Sorgfalt und bestätigt die aus seiner Sicht korrekte Darstellung der Sachverhalte im Prüfungsbericht.
>
> Das bei uns definierte Verfahren zur qualitätsgesicherten Erstellung von Programmen wurde in allen Punkten eingehalten. Alle Maßnahmen, Abstimmungen und Regelungen, die zur Organisation des ordnungsgemäßen Programmeinsatzes erforderlich sind, wurden getroffen und dokumentiert. Das Programm erfüllt die gestellten Anforderungen hinsichtlich der geplanten Integration in die bestehenden Systemumgebungen der Institute sowie des Datenschutzes.
>
> Das Programm erfüllt aus fachlicher und technischer Sicht die gestellten Anforderungen. Von der Funktionsfähigkeit haben wir uns überzeugt und die durchgeführten Tests entsprechend unseren Vorgaben dokumentiert. Im Programm zu hinterlegende Parameter (Konditionen, Zinssätze, Zugriffsrechte, Institutsparameter, etc.) wurden benannt, deren Erfassungs- und Kontrollmöglichkeiten sind in Handbüchern beschrieben. Zur Anwendung des Programms

erforderliche Schulungsunterlagen sind bereitgestellt. Anwender-Handbücher bzw. Arbeitshilfen sind vorhanden.

Kompetenzgerechte Unterschriften …

Informationen für den Datenschutzbeauftragten

Bereitgestellt als [1021, B.4 LORA Mobile - Auflistung personenbezogener Daten].

1. Einleitung

Laut Datenschutzgrundverordnung Art. 4 sind personenbezogene Daten folgendermaßen definiert:

„Personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Die Speicherung und Verarbeitung personenbezogener Daten sind für die Bearbeitung und Durchführung des Besichtigungsauftrages erforderlich. Die eindeutige Identifizierung des Objektes und des dazugehörigen Kunden, für den der Auftrag erbracht werden soll, können nur unter Verwendung personenbezogener Daten erfolgen.

Die Entscheidung, welche personenbezogenen Daten bei der Einstellung eines Besichtigungsauftrages zur Verarbeitung an LORA Mobile übertragen werden obliegt dem Einsteller/Besteller des Instituts. Das Institut muss für sich festlegen, ob der Besichtiger des Instituts alle angebotenen Informationen zur Erledigung des Besichtigungsauftrages in LORA Mobile benötigt.

LORA Mobile bietet die folgenden Datenfelder mit Personenbezug an, die durch Eingabe über das Bestellsystem in der Anwendung verarbeitet und gespeichert werden können aber nicht müssen.

2. Webanwendung

- *Auftraggeber/Einsteller*
  - *Name, Vorname*
  - *E-Mailadresse*
  - *Telefonnummer (für Rückfragen)*
- *Ansprechpartner für die Besichtigung/Terminvereinbarung*
  - *Name, Vorname*
  - *Telefonnummer (für Rückfragen)*
  - *E-Mailadresse*
- *Kunde des Instituts (nur wenn Kunde ungleich Ansprechpartner)*
  - *Name, Vorname*
- *Objekt*
  - *Straße, Hausnummer*
  - *PLZ, Ort*

3. Lora Mobile NG App

- *Auftraggeber/Einsteller*
  - *Name, Vorname*
  - *E-Mailadresse*
  - *Telefonnummer (für Rückfragen)*
- *Ansprechpartner für die Besichtigung/Terminvereinbarung*
  - *Name, Vorname*
  - *Telefonnummer (für Rückfragen)*
  - *E-Mailadresse*
- *Kunde des Instituts (nur wenn Kunde ungleich Ansprechpartner)*
  - *Name, Vorname*
- *Objekt*
  - *Straße, Hausnummer*
  - *PLZ, Ort*

4. Besichtigungsbogen (abhängig v. auftraggeberspez. Konfiguration)

- *Ansprechpartner für die Besichtigung/Terminvereinbarung*
  - *Name, Vorname*
  - *Telefonnummer (für Rückfragen)*
  - *E-Mailadresse*
- *Objekt*
  - *Straße, Hausnummer*
  - *PLZ, Ort*
  - *Fotoaufnahmen*
  - *Wesentliche Einträge im Besichtigungsbericht, die auf persönliche Verhältnisse Rückschlüsse zulassen.*

10.6 Anlage on-geo TOM (Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO)

(Bereitgestellt als [1021, Anlage on-geo TOM], hier abgebildet, da das Bereitstellungsdokument nicht ausreichend versioniert ist.)

Anlage on-geo TOM

(Sicherheit der Verarbeitung gemäß Artikel 32 DSGVO)

Präambel

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, konkretisiert diese Anlage nach Artikel 32 EU-Datenschutzgrundverordnung („DSGVO"), die getroffenen technischen und organisatorischen Schutzmaßnahmen, die sich aus dem oben genannten Vertrag in seinen Einzelheiten beschriebenen Datenverarbeitung ergeben, um ein dem Risiko angemessenes Datenschutzniveau zu gewährleisten

Diese Anlage findet Anwendung auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragsverarbeiters (Auftragnehmer) oder durch den Auftragsverarbeiter weiter beauftragte Auftragsverarbeiter (Subunternehmer) mit personenbezogenen oder sonstigen Daten des Verantwortlichen (Auftraggeber) in Berührung kommen können.

Darüber hinaus werden Subunternehmer, deren Einsatz zur Durchführung des vereinbarten Auftrages bei Abschluss der Vereinbarung bereits gebilligt sind, in dieser Anlage sowie der Datenschutzbeauftragte bzw. die für den Datenschutz verantwortliche Person des Auftragsverarbeiters, benannt.

Der Verantwortliche ist nach Artikel 5 Abs. 2 und Artikel 28 Abs. 3h DSGVO dafür verantwortlich, dass er sich bei Auftragserteilung und sodann regelmäßig von der Zuverlässigkeit des Auftragsverarbeiters hinsichtlich der hier getroffenen technischen und organisatorischen Schutzmaßnahmen überzeugt.

§ 1 Getroffene technische und organisatorische Sicherheitsmaßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus

(1a) Maßnahmen zur **Pseudonymisierung und Anonymisierung** personenbezogener Daten:
Performance Auswertungen in den Anwendungen werden anonym durchgeführt. WebServer Analytic Tools auf öffentlichen on-geo Webseiten protokollieren nur nach expliziter Einwilligung durch den Betroffenen. Für LORA 3 gibt es optional ein Anonymisierungs Modul, womit anwenderseitig nachträgliche Anonymisierung von gewählten Datensätzen durchgeführt werden kann. Für LORA mobile kann auf Weisung des Auftraggebers durch on-geo über manuelle Schritte eine Anonymisierung von einzelnen Datensätzen durchgeführt werden. An Stellen, bei der keine Anonymisierung/Pseudonomisierung möglich ist, wird Verschlüsselung verwendet.

Erläuterung:
Pseudonymisierung ist die Verarbeitung personenbezogene Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Existieren solche zusätzlichen Informationen nicht oder werden sie unwiderruflich gelöscht, so handelt es sich um eine Anonymisierung.
Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(1b) Maßnahmen zur **Verschlüsselung** personenbezogener Daten:
E-Mails werden per Default mit dem TLS Verfahren auf der Wegstrecke verschlüsselt. Die on-geo E-Mail Server haben das Feature TLS standardmäßig aktiv. Unterstützt der Sende/Empfangs Server auf der Gegenseite ebenfalls TLS, werden die Nachrichten automatisch via TLS verschlüsselt. Darüber hinaus ist auch das S/MIME Verschlüsselungsverfahren optional möglich. Alle Webseiten und WebServices (API) sind mit HTTPS/TLS geschützt. Sensible Daten werden nach vorheriger Absprache mit dem Empfänger/Sender per einzelner Nachricht mit einer verschlüsselten ZIP Datei ausgetauscht. USB-Sticks, externe Festplatten, optische Datenträger mit schützenswerten Inhalt werden verschlüsselt. Der Transport von Datenträgern wird protokolliert.

Erläuterung:
Verschlüsselung personenbezogener Daten ist eine gängige Möglichkeit diese gegen die Kenntnisnahme durch Unbefugte zu schützen.
Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(1c) Maßnahmen zur **Sicherstellung der Vertraulichkeit auf Dauer**:
Sofern technisch möglich und soweit die Praktikabilität in Prozessen nicht maßgeblich davon behindert wird, ist Verschlüsselung im Einsatz. Falls technisch oder prozessbedingt keine Verschlüsselung möglich ist, wird durch sowohl technische als auch organisatorische Sicherheitsmaßnahmen der bestmögliche Schutz erreicht um die Vertraulichkeit der Daten sicherzustellen. Dazu gehören insbesondere: - Berechtigungskonzepte mit Need to know Prinzip - Regelmäßige interne und externe Sicherheitsaudits - Aktive Überwachung von Security-Key-Elementen (Monitoring mit Event Trigger) - Schutz der IT-Infrastruktur mit Anti Virus, Firewalls, Loadbalancer, gehärtete Systeme

Erläuterung:
Damit sind Maßnahmen gemeint, die eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, einschließlich Schutz von unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Diese Maßnahmen müssen so ausgelegt sein, dass sie die Vertraulichkeit auf Dauer gewährleisten.
Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(1d) Maßnahmen zur **Sicherstellung der Integrität auf Dauer**:
Zum Schutz vor unrechtmäßiger Veränderung bzw. Löschung von Daten wird vorrangig ein effektives Berechtigungskonzept auf Applikations- und Betriebssystemebene eingesetzt. Den äußeren Schutz bilden Anti-Virus und Firewall. Sofern technisch und prozessbedingt möglich, werden die Daten des Weiteren durch Verschlüsselung geschützt. Zugriffe auf Daten und IT-Systeme werden protokolliert. Es finden zyklische Datensicherungen (Backups) statt.

Erläuterung:
Damit sind Maßnahmen gemeint, die eine angemessene Sicherheit der personenbezogenen Daten gewährleisten, einschließlich Schutz von unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung sowie unbefugter Änderung. Diese Maßnahmen müssen so ausgelegt sein, dass sie die Integrität auf Dauer gewährleisten.
Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(1e) Maßnahmen zur **Sicherstellung der Verfügbarkeit auf Dauer**:
Alle Systeme werden permanent über zentrale Monitoring Schnittstellen überwacht. Unerwartetes Verhalten und Probleme lösen eine automatische Mitteilung aus, welche die Mitarbeiter der IT-Administration sofort informiert. Die IT-Architektur ist redundant aufgebaut. Mit Hilfe von Hardware Loadbalacern wird die Last auf mehrere Systeme verteilt. Im Notfall kann das Ausweichsystem die Arbeit übernehmen. Des Weiteren ist im Rahmen des Continuity Managements die Wiederaufnahme und Fortführung des Betriebes über Rücksicherung von Daten möglich. (Desaster Recovery). Ein physisch abgetrenntes Ausweich-Rechenzentrum (CoLocation) kann im Bedarfsfall die Aufgaben des Hauptrechenzentrums übernehmen. Als präventive Maßnahme sind sowohl physische Schutzmaßnahmen für die Standorte der Datenverarbeitung als auch IT-basierte Schutzmechanismen im aktiven Einsatz. Dazu zählen insbesondere: - Anti Virus - Firewalls - Zugangs- und Zugriffsschutz durch Berechtigungskonzepte

Erläuterung:
Damit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Diese Maßnahmen müssen so ausgelegt sein, dass sie die Verfügbarkeit auf Dauer gewährleisten.
Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(1f) Maßnahmen zur **Sicherstellung der Belastbarkeit der Systeme und Dienste auf Dauer**:
Alle IT-Systeme werden aktiv über mehrere Ebenen überwacht. Dazu gehört insbesondere das Monitoring auf Hardware Ebene, auf Betriebssystemebene und auf Applikationsebene. Definierte Events lösen eine Benachrichtigung an die verantwortlichen Stellen aus. Für die IT-Systeme stehen rund um die Uhr (24/7) professionelle interne IT-Administratoren zur Verfügung. Die IT-Architektur ist redundant aufgebaut. Mit Hilfe von Hardware Loadbalacern wird die Last auf mehrere Systeme verteilt. Im Rahmen des Continuity Managements wird u.a. mit Hilfe von Last Tests die Belastbarkeit von den IT-Systemen verprobt. In festgelegten Zyklen wird die vorhandene Hardware durch neue Hardware ersetzt um stets neue Technik mit verbesserter Effektivität und Effizienz im aktiven Einsatz zu haben.

Erläuterung:
Hierzu gehören beispielsweise Maßnahmen, die schon in der Phase vor Durchführung der Datenverarbeitung durch den Verantwortlichen und den Auftragsverarbeiter zu ergreifen sind (vgl. 2i). Aber auch eine kontinuierliche Überwachung der Systeme kann erforderlich sein.
Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(1g) Maßnahmen zur raschen **Wiederherstellung der Verfügbarkeit bei einem physischem oder technischem Zwischenfall**:
Die IT-Systeme sind redundant aufgebaut und können sich bei einem technischen Zwischenfall gegenseitig ersetzen. Für alle Systeme wird eine regelmäßige Datensicherung durchgeführt. Die Wiederherstellung der Sicherung wird regelmäßig geprüft. Im Rahmen des Continuity Managements werden zudem zusätzlich noch Desaster Recovery Tests durchgeführt. Es existiert ein Notfallkonzept, in welchem definierte Prozesse für den Wiederanlauf, den Notbetrieb und die Überführung in den Regelbetrieb beschrieben sind. Für vorhandene IT-Systeme bestehen Garantie, Service und Wartungsverträge. Bei Störungen / Defekten wird innerhalb kürzester Zeit eine Reparatur bzw. Austausch garantiert.

Erläuterung:
Zur Sicherstellung der Wiederherstellbarkeit erscheinen einerseits ausreichende Sicherungen denkbar, wie aber auch Maßnahmenpläne, die im Sinne von Katastrophen-Fall-Szenarien (ggf. auch Basis der Sicherungen) den laufenden Betrieb wiederherstellen können.
Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(1h) Maßnahmen zur **regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen**:
Es werden regelmäßig koordinierte, interne Schwachstellen Scans gegen die IT-Systeme durchgeführt. Darüber hinaus finden Penetrations Tests durch unabhängige Dritte (Spezialfirmen), vornehmlich für LORA 3, statt. Mehrmals im Jahr werden externe Audits von Revisionen der Auftraggeber bei on-geo durchgeführt. Die Ergebnisse der vorgenannten internen und externen Prüfungen und der ggf. daraus abzuleitenden problembehebenden bzw. -verringernden Maßnahmen werden entsprechend umgesetzt um den bestmöglichen Schutz der IT-Systeme und Daten gewährleisten zu können. Die Umsetzung der Maßnahmen wird durch die on-geo eigene interne Revision und die externen Revisionen (IR der AG) verfolgt.

Erläuterung:
Maßnahmen, um insbesondere die hier geregelten Maßnahmen zur Datensicherheit laufend aktuell zu halten.
Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

§ 2 Weitere getroffene technische und organisatorische Sicherheitsmaßnahmen soweit nicht unter § 1 genannt

(2a) Maßnahmen zur **Verwehrung des Zutritts zu Datenverarbeitungsanlagen für Unbefugte** (Zutrittskontrolle durch physischen Sicherheitsmaßnahmen):
Die Zutrittskontrolle den on-geo Räumlichkeiten erfolgt über ein Transponder-System. Einzelne Räume sind zusätzlich mit einem Schlüsselsystem gesichert. Es besteht eine abgeschlossene Personalliste mit den Zutrittsberechtigungen. Mit jedem Mitarbeiter auf dieser Liste wurde eine gesonderte Vertraulichkeitsvereinbarung abgeschlossen. Darüber hinaus ist der Zugang den Räumen so angelegt, dass Unbefugte zuvor in das gesicherte Hauptgebäude und danach noch in weitere Sicherheitszonen eindringen müssten um den Sicherheitsbereich zu gefährden. Auf Lagehinweise wurde explizit verzichtet. Das Rechenzentrum (RZ) wird durch die Zutrittskontrolle des Housing Partners geschützt. Die Räume des RZ sind durch ein Transponder-System gesichert. Nur Personal des Housing Partners ist im Besitz einzeln geschalteter, personalisierter Transponder-Karten. Der Zutritt muss vorher angemeldet werden und ist nur möglich in Begleitung von Personal des Housing Partners. Der Aufenthalt wird protokolliert inkl. des Namens der Begleitperson. Die RZ-Räumlichkeiten können nur durch einen videoüberwachten Schleusenraum betreten werden. Der Zutritt ist hierbei im 4Augen Prinzip gesichert. Der Zutritt vom Schleusenraum in die RZ-Stellflächen muss von der Leitstelle mittels Videoaufschaltung autorisiert werden. Die Co-Location, in der Funktion des alternativen RZ, ist gesondert gesichert. Der Zutritt ist nur für dediziertes on-geo Personal nach vorheriger schriftlicher Anmeldung möglich. Die Co-Lo ist mit einem Transponder-System, Gegensprechanlage und Videoüberwachung gesichert.

Erläuterung:
Damit sind Maßnahmen gemeint, die Unbefugten den Zutritt zu den Gebäuden und Rechenzentren verwehren in denen personenbezogene Daten verarbeitet werden. Es werden in diesem Zusammenhang Maßnahmen ergriffen, die dafür Sorge tragen, dass nur die Personen Zutritt zu den Gebäuden und Rechenzentren haben, die über eine entsprechende Berechtigung verfügen.
Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(2b) Maßnahmen zur **Verwehrung der Nutzung von Datenverarbeitungssysteme für Unbefugte** (Zugangskontrolle zu Datenverarbeitungssysteme):
Nur befugte Personen haben Zugang zu Datenverarbeitungsanlagen. Zu diesem Zweck sind DV-Anlagen grundsätzlich mittels Zugangskennungen geschützt. Zugangskennungen, d.h. Nutzername und Passwort sind an den jeweiligen Nutzer gebunden und dürfen nicht weiter gegeben werden. Es gilt die folgende Passwortrichtlinie: a) Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Es ist immer ein komplexes Passwort zu verwenden: Buchstaben (groß und klein), Zahlen, Sonderzeichen). b) Die Passwörter sind nach 90 Tagen zu wechseln. (maximales Kennwortalter) c) Das Kennwort darf nicht den Kontonamen des Benutzers oder mehr als zwei Zeichen enthalten, die nacheinander im vollständigen Namen des Benutzers vorkommen. d) Die Kennwortchronik ist aktiv, die letzten 10 Kennwörter können nicht verwendet werden. e) Alle IT-Systeme sind mit einem passwortunterstützten Bildschirmschoner ausgestattet. Diese Funktion kann nicht eigenständig geändert werden. f) sämtliche genannte Funktionen werden elektronisch erzwungen und über die Domänenweite Active Directory GPO Richtlinie gesteuert

Erläuterung:
Damit sind Maßnahmen gemeint, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und –verfahren benutzen. Es werden in diesem Zusammenhang Maßnahmen ergriffen, die dafür Sorge tragen, dass nur Personen auf Anlagen zur Datenverarbeitung zugreifen können, die über eine entsprechende Berechtigung verfügen. Hierzu gehören bspw. geeignete Passwortregeln und Firewallkonfigurationen.
Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(2c) Maßnahmen zur **Verwehrung des Zugriffs auf personenbezogene Daten für Unbefugte** (Zugriffskontrolle durch Berechtigungsmanagement):
Der Zugriff zur Verarbeitung, Nutzung und Speicherung der Daten innerhalb der Datenverarbeitungssysteme ist nur berechtigten Mitarbeitern der on-geo GmbH möglich. Alle Mitarbeiter sind mit einer persönlichen Verpflichtungserklärung zur Verschwiegenheit und Wahrung des Datenschutzes verpflichtet. Die Zugriffskontrolle wird durch differenzierte Berechtigungen erreicht, was das unbefugte Lesen, Verändern oder Löschen von Daten verhindert. Für alle Rechtevergaben in DV-Systemen sind elektronische Antrags Tickets notwendig. Die Genehmigung erfolgt im 4Augen Prinzip. Die Berechtigungen werden im need-to-know Prinzip vergeben. Für HPU (Admin Accounts) findet mindestens 2 x jährlich eine Rezertifizierung der Accounts statt. Es existieren fest im Unternehmen verankerte Regelprozesse für Joiner/Mover/Leaver. Die Personalabteilung initiiert den Prozess auf elektronischer Ebene. Die Accounts des betroffenen Mitarbeiters werden folgend beantragt & genehmigt, verändert oder gesperrt/gelöscht.

Erläuterung:
Damit sind Maßnahmen gemeint, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können. Es werden in diesem Zusammenhang Maßnahmen ergriffen, die dafür Sorge tragen, dass Personen im Rahmen der Datenverarbeitung nur auf die Daten zugreifen können, für die sie über eine entsprechende Berechtigung verfügen und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(2d) Maßnahmen zur **Verwehrung der unbefugten Kenntnisnahme, der Nachvollziehbarkeit und Wahrung der Integrität bei der Datenübertragung** (Weitergabekontrolle durch sichere Übertragung):
Personenbezogene Daten und vertrauliche Informationen werden nur über sichere Kommunikationswege übertragen. Alle elektronischen Übertragungen sind gegen unbefugtes Lesen, Verändern, Kopieren geschützt. Zur Sicherung der Datenübertragung finden Firewall, VPN, Virenschutz, SSL, Passwortschutz einzelner Dokumente und Verschlüsselung ihren Einsatz. Emails, USB-Sticks, externe Festplatten, optische Datenträger mit schützenswerten Inhalt werden verschlüsselt. Der Transport von Datenträgern wird protokolliert.

Erläuterung:
Damit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(2e) Maßnahmen zur **nachträglichen Überprüfung und Nachvollziehbarkeit bei Eingaben, Änderungen und Löschungen** (Eingabekontrolle durch Protokollierung):
Mit Ausnahme vom Lesezugriff werden die Zugriffe auf Datensätze automatisch protokolliert. Die Log-Einträge unterscheiden die Art der Aktivität (z.B. Anlegen eines Datensatzes, Modifizieren eines Datensatzes, Löschen eines Datensatzes). Aufgrund der Nachvollziehbarkeit ist es deshalb unabdinglich dass jeder Benutzer ausschließlich seine eigene Login-Daten verwendet. Die Logs sind vor unberechtigten Zugriff geschützt und werden ausgewertet.

Erläuterung:
Damit sind Maßnahmen gemeint, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungs-Systemen bzw. Anwendungen eingegeben, verändert oder entfernt worden sind.
Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(2f) Maßnahmen zur **Wiederherstellung personenbezogener Daten im Störungsfall** (Verfügbarkeitskontrolle durch Business Continuity Management):
Die IT-Systeme sind redundant aufgebaut und können sich bei einem technischen Zwischenfall gegenseitig ersetzen. Für alle Systeme wird eine regelmäßige Datensicherung durchgeführt. Die Wiederherstellung der Sicherung wird regelmäßig geprüft. Im Rahmen des Continuity Managements werden zudem zusätzlich noch Desaster Recovery Tests durchgeführt. Es existiert ein Notfallkonzept, in welchem definierte Prozesse für den Wiederanlauf, den Notbetrieb und die Überführung in den Regelbetrieb beschrieben sind. Für vorhandene IT-Systeme bestehen Garantie, Service und Wartungsverträge. Bei Störungen / Defekten wird innerhalb kürzester Zeit eine Reparatur bzw. Austausch garantiert.

Erläuterung:
Damit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(2g) Maßnahmen der **Trennung der Verarbeitung für verschiedene Zwecke** erhobene personenbezogene Daten (Trennungskontrolle durch Mandantentrennung und Berechtigungsmanagement):
Daten die bei on-geo zu unterschiedlichen Zwecken erhoben werden, werden auch getrennt gehalten und verarbeitet und nur für den bestimmten Zweck verwendet. Die Mandantentrennung wird durch logische und physische Trennung erreicht. Dadurch wird technisch verhindert, dass Kunden untereinander auf Daten zugreifen können. Zur Funktionstrennung gibt es unterschiedliche Bereiche (Development/Test/Produktiv). Die Bereiche sind durch verschiedene Netze technisch voneinander getrennt und besitzen keine Verbindung untereinander. Je Netzwerk sind nur bestimmte Personen & Gruppen zum jeweiligen Zugriff berechtigt. Es werden keine Produktiv-Daten für die Anwendungsentwicklung oder interne Tests verwendet.

Erläuterung:
Damit sind Maßnahmen gemeint, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(2h) Maßnahmen zur **Datenlöschung und Einschränkung der Verarbeitung**:
LORA Mobile: Eigenständiges Löschkonzept für LORA Mobile - Datenlöschung und –archivierung. **LORA 3 und Auftragsverarbeitung generell:** Sofern vertraglich nicht gesondert vereinbart, findet durch on-geo keine automatische oder manuelle Löschung von Daten statt (Data Lifecycle). Gemäß den gesetzlichen und vertraglichen Bestimmungen verbleibt in der Auftragsverarbeitung der Auftraggeber der Datenherr. on-geo löscht Daten nur nach expliziter Weisung des Auftraggebers.

Erläuterung:
Sind personenbezogene Daten für die Zwecke, für die sie erhoben werden oder auf sonstige Weise verarbeitet wurden nicht mehr notwendig, sind sie, unabhängig von einen entsprechenden Ersuchen der betroffenen Person, zu löschen. Dies gilt insbesondere dann, wenn keine Grundlage für die Datenverarbeitung mehr besteht oder die Grundlage zwischenzeitlich entfallen ist.
In bestimmten Fällen kann oder muss anstatt der vollständigen Löschung eine Einschränkung der Datenverarbeitung erfolgen (bisher Sperrung genannt).
Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(2i) Maßnahmen für **sichere Softwareentwicklung** (optional):
Die Entwicklung ist in verschiedene Phasen eingeteilt: Anforderungsanalyse, Konzeptphase, Systemdesign, Systementwicklung, Test, Inbetriebnahme, Betrieb. Für die einzelnen Phasen gibt es sauber getrennte Umgebungen (siehe – Trennungskontrolle) Für die Entwickler existieren verbindliche Arbeitsanweisungen und Guidelines wie Secure Coding Practises, Style Guides, Programmierrichtlinien etc. Die entwickelten Softwarepakete durchlaufen eine interne QS durch die Entwickler selbst sowie die Tests

durch interne QS Mitarbeiter. Das angewandte Verfahren sowie die Software als solche wird von unabhängigen Dritten (SIZ) geprüft und zertifiziert (OPDV Freigabe für LORA2.4, LORA mobile und LORA3).

Erläuterung:
Ggf. Beschreibung von Maßnahmen zu sicheren Softwareentwicklung (No Spy-Verfahren, wie OWASP). Eine bestehende Dokumentation (z.B. in einem Datenschutz- oder Sicherheitskonzept) kann zudem angegeben werden.

(2j) Ergebnisse eines **Penetrationstests** (optional):
Für Auftraggeber besteht die Möglichkeit, in Absprache mit on-geo, Penetrationstests gegen die eigene (Mandanten-)Umgebung in LORA 3, die Anwendung LORA 2.4 oder LORA mobile) durchzuführen. Der Test ist durch den AG oder durch ihn organisierte Dritte auf eigene Kosten durchzuführen.

§ 3 Datenschutzbeauftragter der on-geo GmbH

Vorname Name:	Kontaktdaten:
Klaus Rathsfeld	Klaus.Rathsfeld@on-geo.de Telefon: + 49 361 / 21 681 2038

§ 4 Auflistung weiterer Auftragsverarbeiter (Subunternehmer)

Hinweis:
Abhängig von dem vertraglich vereinbarten Leistungsumfang sind möglicherweise nicht alle Unterauftragnehmer relevant.

Kurzbeschreibung der Tätigkeit:	Name des Unternehmens:	Sitz der Firma, Ort der Datenverarbeitung:
Datenschutzkonforme Datenentsorgung und -vernichtung	Documentus (ex. Reisswolf) GmbH	Zörbiger Str. 21, 06118 Halle (Saale)
Housing der von on-geo genutzten IT-Infrastruktur (Server) Hinweis: Der Housing Partner stellt lediglich die Rechenzentrums-Stellfläche, Internet, Strom und Klimatisierung. Das Hosting der Daten und die Verwaltung der IT-Infrastruktur wird von on-geo erbracht.	Neue Technologie AG (NT.AG)	Firmensitz: Peterstraße 1, 99084 Erfurt Rechenzentrum: Peterstraße 3, 99084 Erfurt
Immobiliengutachtenerstellung Hinweis 2	onval GmbH	Peterstraße 1, 99084 Erfurt
Organisation von Immobilienbesichtigungen	Instant Service AG (IS AG)	Peterstraße 1, 99084 Erfurt
Durchführung von Immobilienbesichtigungen Hinweis 2	Sachverständigen-Netzwerk	Bundesweit

Hinweis 2:

Grundsätzlich werden alle Besichtiger und Besichtigungsunternehmen aus dem Sachverständigen-Netzwerk der IS AG durch den Auftraggeber freigegeben.
Die Besichtigungsleistung wird in Abhängigkeit von Qualifikation, Auslastung, Nähe zum Objekt als Einzelauftrag durch die IS AG an die jeweiligen Besichtiger/Besichtigungsunternehmen vergeben.

Grundsätzlich werden alle Gutachter aus dem Sachverständigen-Netzwerk der onval GmbH durch den Auftraggeber freigegeben.
Der Auftrag zur Gutachtenerstellung wird in Abhängigkeit von Qualifikation und Auslastung als Einzelauftrag durch die onval GmbH an die jeweiligen Gutachter vergeben.

Eine Weiterverlagerung liegt somit nicht vor. (sonstiger und gelegentlicher Fremdbezug von Leistungen)

Dem Auftraggeber wird jederzeit auf Verlangen eine Aufstellung der relevanten Besichtiger / Gutachter zur Verfügung gestellt. Der Auftraggeber hat das jederzeitige Recht einzelne Besichtiger / Gutachter aus berechtigtem Grund zu sperren.

10.7 GLOSSAR

BEGRIFF	DEFINITION
Abnahmetest	Der Abnahmetest dient dem Ziel, zu zeigen, dass das Vertrauen in das System für den produktiven Einsatz gerechtfertigt ist
Angemessen	Entsprechend [IDW EPS 300, Tz8] stellt in der hier vorliegenden Dokumentation dieser Begriff *die „Angemessenheit" der Prüfungsnach-*

BEGRIFF	DEFINITION
	weise einen qualitativen Maßstab für die eingeholten Prüfungsnachweise, deren Verlässlichkeit und Relevanz für die Prüfung einer Aussage in der Rechnungslegung dar. Siehe auch „ausreichend“. [IDW PS 860, Tz10]: *Die Grundsätze, Verfahren und Maßnahmen des zu prüfenden IT-Systems sind geeignet, mit hinreichender Sicherheit (vgl. Tz. A8) die Kriterien einzuhalten und sie sind implementiert, d.h. wie vorgesehen eingerichtet. Dies schließt ein, dass die Grundsätze, Verfahren und Maßnahmen mit hinreichender Sicherheit geeignet sind, die wesentlichen Risiken für die Einhaltung der Kriterien rechtzeitig zu erkennen, zu bewerten, zu steuern und zu überwachen.*
Arbeitspapiere	[IDW QS 1, Tz12] *Handakten i.S.v.* [WPO, §51b Abs. 1], *die der Berufsangehörige bzw. die Prüfungsorganisation im Zusammenhang mit der Auftragsabwicklung selbst erstellt, sowie alle Schriftstücke und Unterlagen, die der Berufsangehörige bzw. die Prüfungsorganisation von dem Auftraggeber oder von Dritten als Ergänzung seiner eigenen Unterlagen zum Verbleib erhält. Die Arbeitspapiere dürfen in elektronischer Form geführt werden.*
Ausreichend	Entsprechend [IDW EPS 300, Tz8] stellt in der hier vorliegenden Dokumentation dieser Begriff keine Schulnote dar sondern beschreibt lediglich einen quantitativen Maßstab, siehe auch „angemessen“.
Direkte IT-Prüfung	[IDW PS 860, Tz10]: … *Ein Prüfungsauftrag, bei dem der Prüfer das durch die Auftragsvereinbarung abgegrenzte IT-System als Prüfungsobjekt anhand der vereinbarten Kriterien prüft und die daraus resultierenden Sachverhaltsinformationen als Teil seiner Berichterstattung darstellt.*
Erklärung der gesetzlichen Vertreter zum IT-System	[IDW PS 860, Tz10]: *Aussagen der gesetzlichen Vertreter des Unternehmens zum IT-System sowie zur Angemessenheit und – sofern einschlägig – zur Wirksamkeit der zur Einhaltung der Kriterien getroffenen Grundsätze, Verfahren und Maßnahmen in Bezug auf das IT-System in schriftlicher Form* (siehe Abschnitt *10.3 Bestätigung der gesetzlichen Vertreter*).
Hinreichende (Sicherheit)	[IDW PS 860, TzA8]: *Hinreichende Sicherheit bedeutet nicht absolute Sicherheit: Auch ein wirksames IT-System unterliegt systemimmanenten Grenzen, so dass möglicherweise die Kriterien in wesentlichen Belangen nicht eingehalten werden, ohne dass dies systemseitig rechtzeitig erkannt und verhindert bzw. aufgedeckt wird. Diese systemimmanenten Grenzen ergeben sich u.a. aus menschlichen Fehlleistungen (bspw. infolge von Nachlässigkeit, Ablenkungen, Beurteilungsfehlern und Missverstehen von Arbeitsanweisungen), Missbrauch oder Vernachlässigung der Verantwortung durch für bestimmte Maßnahmen verantwortliche Personen, der Umgehung oder Außerkraftsetzung von Kontrollen durch Zusammenwirken zweier oder mehrerer Personen oder dem Verzicht des Unternehmens auf bestimmte Maßnahmen, weil die Kosten dafür höher eingeschätzt werden als der erwartete Nutzen.*
Informationssicherheitsmanagement	[BAIT,Tz15]: *Das Informationssicherheitsmanagement macht Vorgaben zur Informationssicherheit, definiert Prozesse und steuert deren Umsetzung (vgl. AT 7.2 Tz. 2 MaRisk). Das Informationssicherheitsmanagement folgt einem fortlaufenden Prozess, der die Phasen Planung, Umsetzung, Erfolgskontrolle sowie Optimierung und Verbesserung umfasst. Die inhaltlichen Berichtspflichten des Informationssicher-*

BEGRIFF	DEFINITION
	heitsbeauftragten an die Geschäftsleitung sowie der Turnus der Berichterstattung orientieren sich an BT 3.2 Tz. 1 MaRisk [MaRisk, AT 7.2], [MaRisk, BT 3.2].
Kriterien	[IDW PS 860, Tz10]: *Die zur Messung bzw. Beurteilung des zugrunde liegenden Sachverhalts angewandten Maßstäbe. Die „verwendeten Kriterien" sind die Kriterien, die bei einem bestimmten Auftrag zur Anwendung kommen.*
Qualität	DIN ISO 8402 (Entwurf März 1992): "*Die Gesamtheit von Merkmalen einer Einheit (entity in der engl. Fassung) bezüglich ihrer Eignung, festgelegte und vorausgesetzte Erfordernisse zu erfüllen.*" DIN 55350 (Teil 11) : "*Qualität ist die Gesamtheit von Eigenschaften und Merkmalen eines Produkts oder einer Tätigkeit, die sich auf deren Eignung zur Erfüllung gegebener Erfordernisse bezieht.*" Qualität ist kein absoluter Wert, sondern muss immer relativ zu gegebenen Erfordernissen gesehen werden. Qualitätsbewertungen beinhalten also immer einen Vergleich zwischen Qualitätsvorgaben, die aus den gegebenen Erfordernissen abgeleitet werden (Soll-Werte) und den tatsächlich erreichten Ausprägungen der Merkmale (Ist-Werte). Qualität ist ein Maß für die Erfüllung von Anforderungen.
Qualitätssicherung	Alle geplanten und systematischen Tätigkeiten, die innerhalb des Qualitätsmanagementsystems verwirklicht sind und die wie erforderlich dargelegt werden, um angemessenes Vertrauen zu schaffen, dass ein Projekt/Team/Bereich/... die Qualitätsforderung erfüllen wird. Im Bereich der Softwareentwicklung sind dies in erster Linie analytische Maßnahmen wie Reviews oder Tests.
Regressionstest	Der Regressionstest besteht aus der Wiederholung von bereits durchgeführten Testfällen und dient zum Nachweis, dass die bereits vorher enthaltene Funktionalität der Betrachtungseinheit nach wie vor korrekt erbracht wird. Unter einem Regressionstest (v. lat. Regression = Rückschritt) versteht man in der Softwaretechnik die Wiederholung aller oder einer Teilmenge aller Testfälle, um Nebenwirkungen von Modifikationen in bereits getesteten Teilen der Software aufzuspüren. Solche Modifikationen entstehen regelmäßig z. B. aufgrund der Pflege, Änderung und Korrektur von Software. Der Regressionstest gehört zu den dynamischen Testtechniken. Aufgrund des Wiederholungscharakters und der Häufigkeit dieser Wiederholungen eignen sich Regressionstests gut für eine automatisierte Ausführung. In der Praxis steht der Begriff des Regressionstests für die reine Wiederholung von Testfällen. Die Testfälle selbst müssen anhand anderer Techniken spezifiziert und mit einem Soll-Ergebnis versehen sein, welches mit dem Ist-Ergebnis eines Testfalls verglichen wird. Ein direkter Bezug auf die Ergebnisse eines vorherigen Testdurchlaufs findet nicht statt. Im Gegensatz dazu ordnet Liggesmeyer den Regressionstest in die Gruppe der Diversifizierenden Tests ein. Dadurch wird im Unterschied zu Funktionsorientierten Testtechniken die Korrektheit der Testergebnisse nicht anhand der Spezifikation entschieden, sondern

BEGRIFF	DEFINITION
	durch Vergleich der Ausgaben der aktuellen Version mit den Ausgaben des Vorgängers. Ein Testfall gilt beim Regressionstest als erfolgreich absolviert, wenn die Ausgaben identisch sind.
Schutzbedarf	Eine spezifische Voraussetzung der IT-Sicherheit eines bestimmten Systems, also eine notwendige Bedingung zur Sicherung der Integrität und Verfügbarkeit des Systems sowie der Informationsvertraulichkeit innerhalb des Systems. Schutzbedürfnisse sind sehr konkret formulierte Erfordernisse der IT-Sicherheit eines Systems. Sie identifizieren seine Verwundbarkeiten, indem sie das schutzbedürftige Objekt (Subsystem), seinen konkreten Schutzbedarf und (vorzugsweise) die Konsequenzen mangelnden Schutzes nennen. Sie antworten auf die Fragestellung "Welches konkrete Objekt braucht welchen Schutz zur Vermeidung welcher Gefahr?" oder, salopper formuliert, "Was muss im Einzelnen verhindert werden?"
Sicherheit	Die Kombination aus Vertrauenswürdigkeit, Integrität und Verfügbarkeit.
SITB	[SIZ-SITB] Der „Sichere IT-Betrieb der SIZ GmbH“ beschreibt Sicherheit entsprechend aller für Finanzinstitute in Deutschland geltenden Regeln und bietet auch eine Zertifizierung nach SITB an. Viele Sparkassen haben ihr Sicherheitsmanagement entsprechend SITB zertifizieren lassen.
Unternehmen	[IDW PS 860, TzA10]: *Unternehmen i.S. dieses IDW Prüfungsstandards können neben Unternehmen im rechtlichen Sinne auch Gesellschaften bürgerlichen Rechts, rechtsfähige oder nicht rechtsfähige Vereine, Stiftungen, Gebietskörperschaften, sonstige Körperschaften, Eigenbetriebe, Anstalten des öffentlichen Rechts, Gemeinschaften, natürliche Personen oder sonstige wirtschaftlich abgegrenzte Geschäftstätigkeiten (z.B. Standorte, selbstständige Teilbetriebe, Sparten) oder Gruppen dieser Einheiten sein.*
Vorgesehene Nutzer	[IDW PS 860, Tz10]: … *Die natürliche(n) Person(en) oder Organisation(en) oder (eine) Gruppe(n) dieser, von der der Prüfer erwartet, dass sie seine Berichterstattung über die Prüfung verwendet bzw. verwenden. In einigen Fällen kann es weitere als die in der Berichterstattung als Empfänger genannten vorgesehenen Nutzer geben (vgl. Tz. A3).*

10.8 INDEX

Unterschrift

Bonn, Mittwoch, 29. Januar 2020	Dipl. Inform. Bernhard König (Prüfer)	Dr. Thomas Stock (Qualitätssicherung des vorliegenden Prüfungsberichtes)