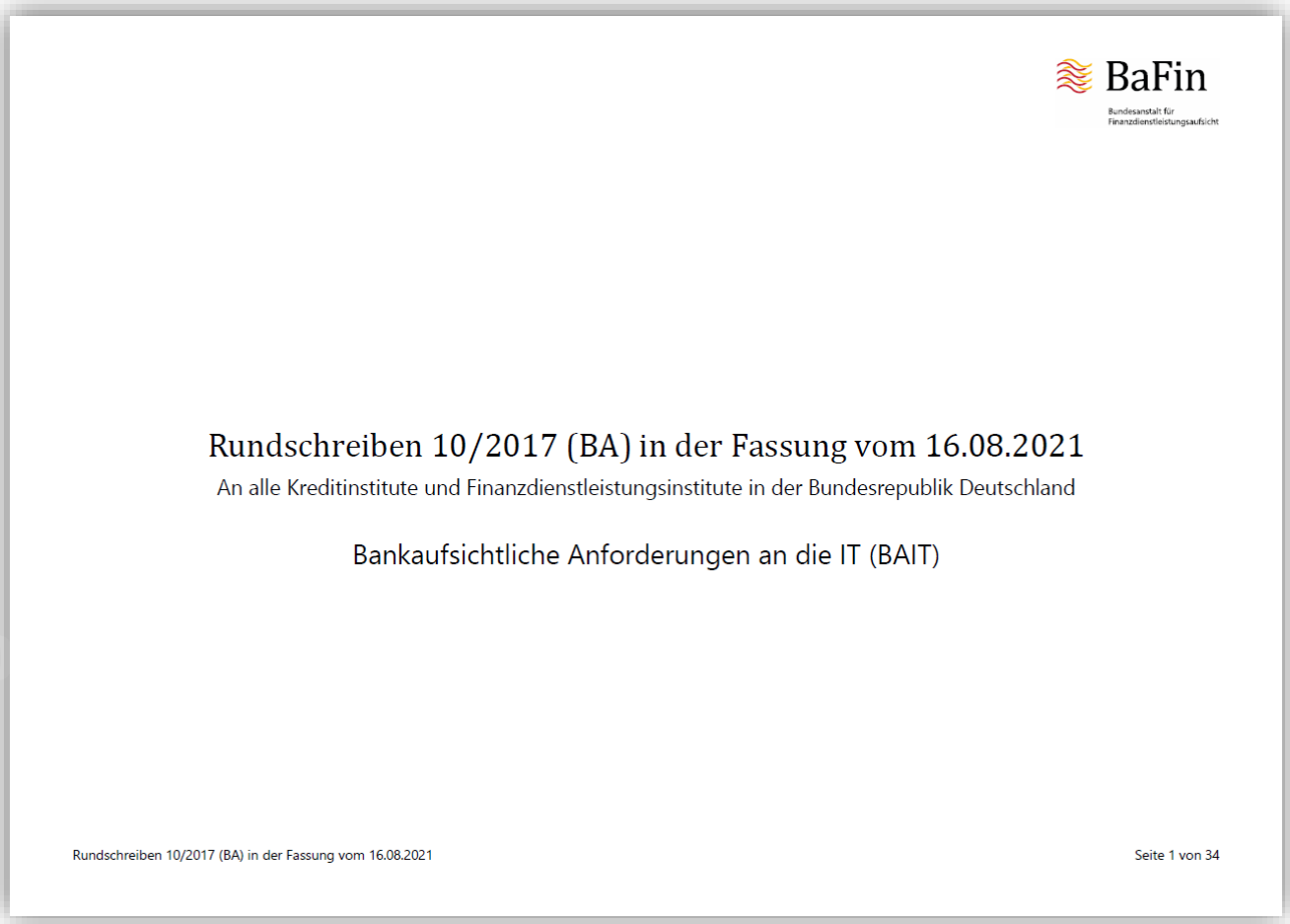
ISACA
Trust in, and value from, information systems
Germany Chapter

BAIT in der Praxis

Presented by: Axel Dors

BAIT

Bankaufsichtliche Anforderungen an die IT (BAIT)



BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

Rundschreiben 10/2017 (BA) in der Fassung vom 16.08.2021

An alle Kreditinstitute und Finanzdienstleistungsinstitute in der Bundesrepublik Deutschland

Bankaufsichtliche Anforderungen an die IT (BAIT)

Rundschreiben 10/2017 (BA) in der Fassung vom 16.08.2021 Seite 1 von 34

BAIT

Motivation der BaFin zur BAIT

„In einer globalisierten Finanzwelt, in der immer mehr Menschen digital bezahlen bzw. Geld transferieren und in der viele Anleger ihre Geldanlage online bestreiten, sind

IT-Governance und Informationssicherheit
keine Randthemen

mehr, sondern haben auch für die Aufsicht inzwischen

den gleichen Stellenwert, wie die Ausstattung
der Institute mit Kapital und Liquidität.“

* Quelle: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1710_BAIT_anschreiben.html

BAIT

Motivation der BaFin zur BAIT

interpretieren gesetzliche Anforderungen (§25 a/b KWG)

sind der zentrale Baustein für die IT-Aufsicht im Bankensektor in Deutschland

sind keine neuen Anforderungen, sondern lediglich Klarstellungen

konkretisieren die MaRisk

sind nicht abschließender Natur

* Quelle: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1710_BAIT_anschreiben.html

BAIT

Hintergründe

- Präzisierung IT-Vorschriften der MaRisk
- Rundschreiben 10/2017 (BA) vom 06.11.2017
- Ergänzt am 14.09.2018 wegen Kritischer Infrastrukturen
- Aktualisiert und ergänzt am 16.08.2021
- Gültigkeit mit Veröffentlichung → keine Übergangsfristen
- Entwurfsfassung wurde bereits als Prüfungsgrundlage bei IT-Risikoprüfungen der Bankenaufsicht verwendet.

Link: https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.html

BAIT

Bankaufsichtliche Anforderungen an die IT (BAIT)

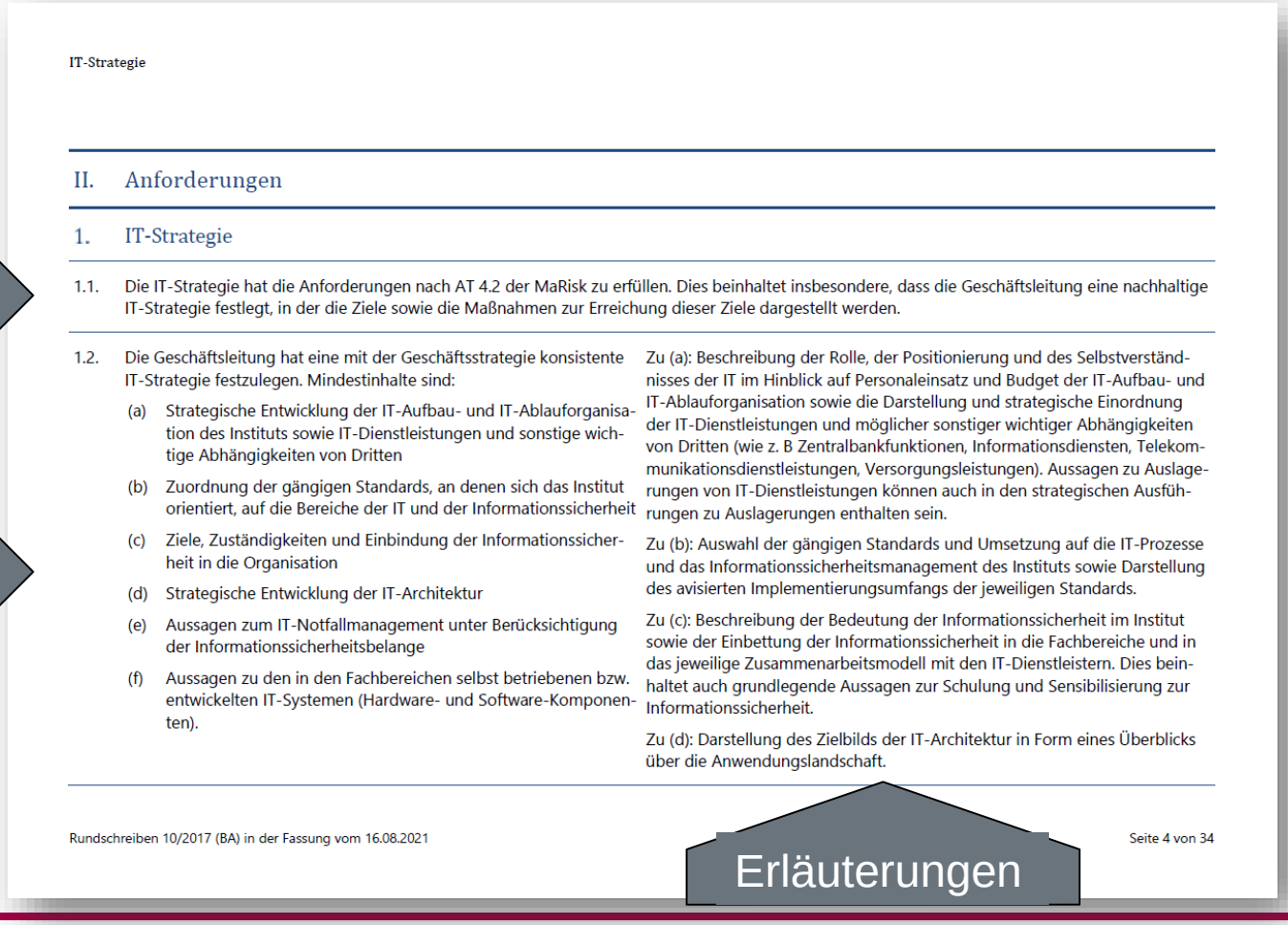
Inhalt

BAIT

Aufbau der Anforderungen

MaRisk Bezug

Anforderungen



IT-Strategie

II. Anforderungen

1. IT-Strategie

1.1. Die IT-Strategie hat die Anforderungen nach AT 4.2 der MaRisk zu erfüllen. Dies beinhaltet insbesondere, dass die Geschäftsleitung eine nachhaltige IT-Strategie festlegt, in der die Ziele sowie die Maßnahmen zur Erreichung dieser Ziele dargestellt werden.

1.2. Die Geschäftsleitung hat eine mit der Geschäftsstrategie konsistente IT-Strategie festzulegen. Mindestinhalte sind:

(a) Strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation des Instituts sowie IT-Dienstleistungen und sonstige wichtige Abhängigkeiten von Dritten

(b) Zuordnung der gängigen Standards, an denen sich das Institut orientiert, auf die Bereiche der IT und der Informationssicherheit

(c) Ziele, Zuständigkeiten und Einbindung der Informationssicherheit in die Organisation

(d) Strategische Entwicklung der IT-Architektur

(e) Aussagen zum IT-Notfallmanagement unter Berücksichtigung der Informationssicherheitsbelange

(f) Aussagen zu den in den Fachbereichen selbst betriebenen bzw. entwickelten IT-Systemen (Hardware- und Software-Komponenten).

Zu (a): Beschreibung der Rolle, der Positionierung und des Selbstverständnisses der IT im Hinblick auf Personaleinsatz und Budget der IT-Aufbau- und IT-Ablauforganisation sowie die Darstellung und strategische Einordnung der IT-Dienstleistungen und möglicher sonstiger wichtiger Abhängigkeiten von Dritten (wie z. B Zentralbankfunktionen, Informationsdiensten, Telekommunikationsdienstleistungen, Versorgungsleistungen). Aussagen zu Auslagerungen von IT-Dienstleistungen können auch in den strategischen Ausführungen zu Auslagerungen enthalten sein.

Zu (b): Auswahl der gängigen Standards und Umsetzung auf die IT-Prozesse und das Informationssicherheitsmanagement des Instituts sowie Darstellung des avisierten Implementierungsumfangs der jeweiligen Standards.

Zu (c): Beschreibung der Bedeutung der Informationssicherheit im Institut sowie der Einbettung der Informationssicherheit in die Fachbereiche und in das jeweilige Zusammenarbeitsmodell mit den IT-Dienstleistern. Dies beinhaltet auch grundlegende Aussagen zur Schulung und Sensibilisierung zur Informationssicherheit.

Zu (d): Darstellung des Zielbilds der IT-Architektur in Form eines Überblicks über die Anwendungslandschaft.

Rundschreiben 10/2017 (BA) in der Fassung vom 16.08.2021

Seite 4 von 34

Erläuterungen

BAIT

Vorbemerkungen

Verpflichtung jenseits der Konkretisierungen in diesem Rundschreiben gemäß § 25a Abs. 1 Satz 3 Nr. 4 KWG i. V. m. AT 7.2 Tz. 2 MaRisk:

Ausgestaltung der IT-Systeme und der IT-Prozesse nach gängigen Standards, z. B.:

- der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik
- internationalen Sicherheitsstandards ISO/IEC 270XX der International Organization for Standardization.

BAIT

1. IT-Strategie

- Definition von Mindestinhalten

(a) Strategische Entwicklung der IT-Aufbau- und IT-Ablauforganisation des Instituts sowie IT-Dienstleistungen und sonstige wichtige Abhängigkeiten von Dritten

(b) Zuordnung der gängigen Standards, an denen sich das Institut orientiert, auf die Bereiche der IT und der Informationssicherheit

(c) Ziele, Zuständigkeiten und Einbindung der Informationssicherheit in die Organisation

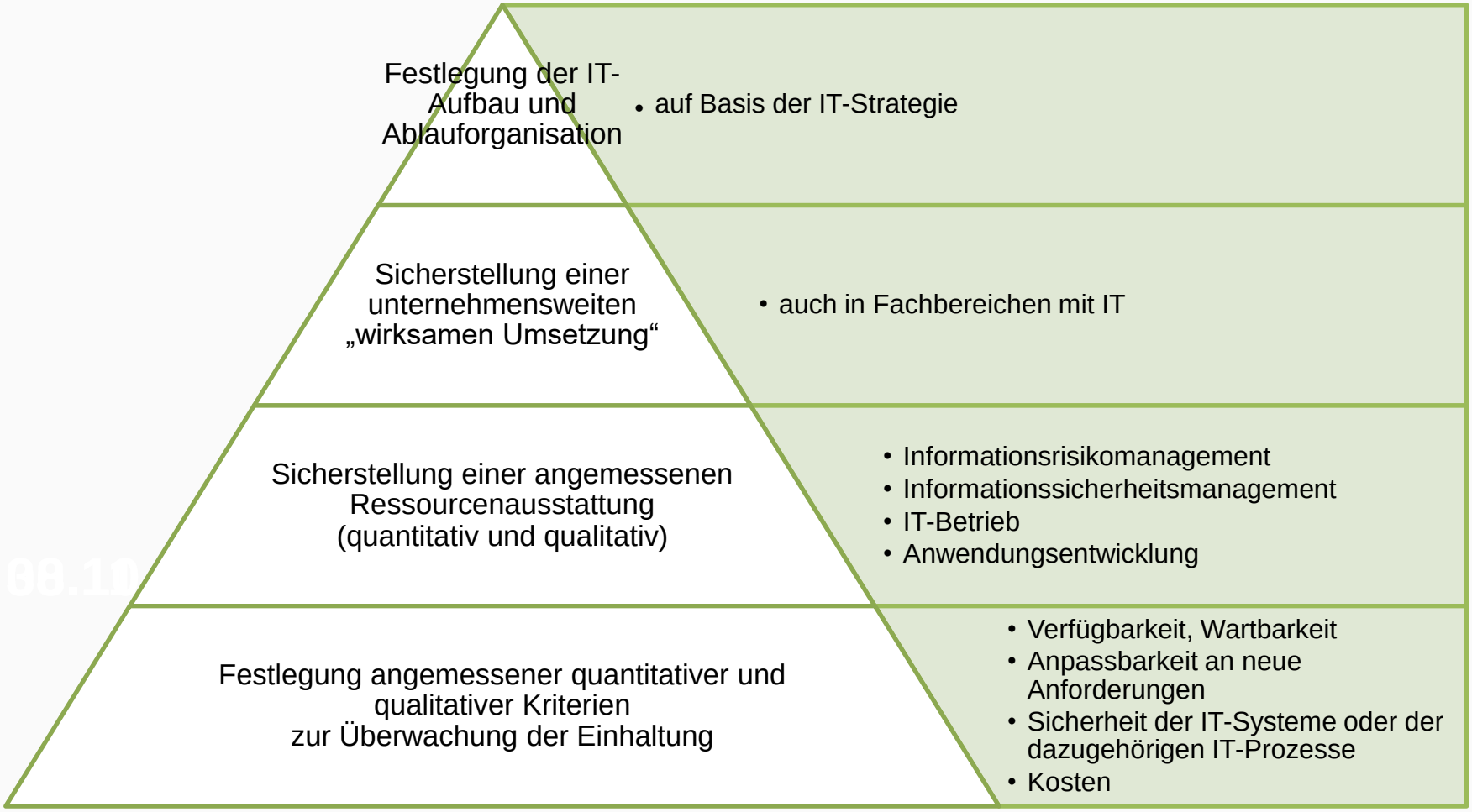
(d) Strategische Entwicklung der IT-Architektur

(e) Aussagen zum IT-Notfallmanagement unter Berücksichtigung der Informationssicherheitsbelange

(f) Aussagen zu den in den Fachbereichen selbst betriebenen bzw. entwickelten IT-Systemen (Hardware- und Software-Komponenten).

BAIT

2. IT-Governance



BAIT

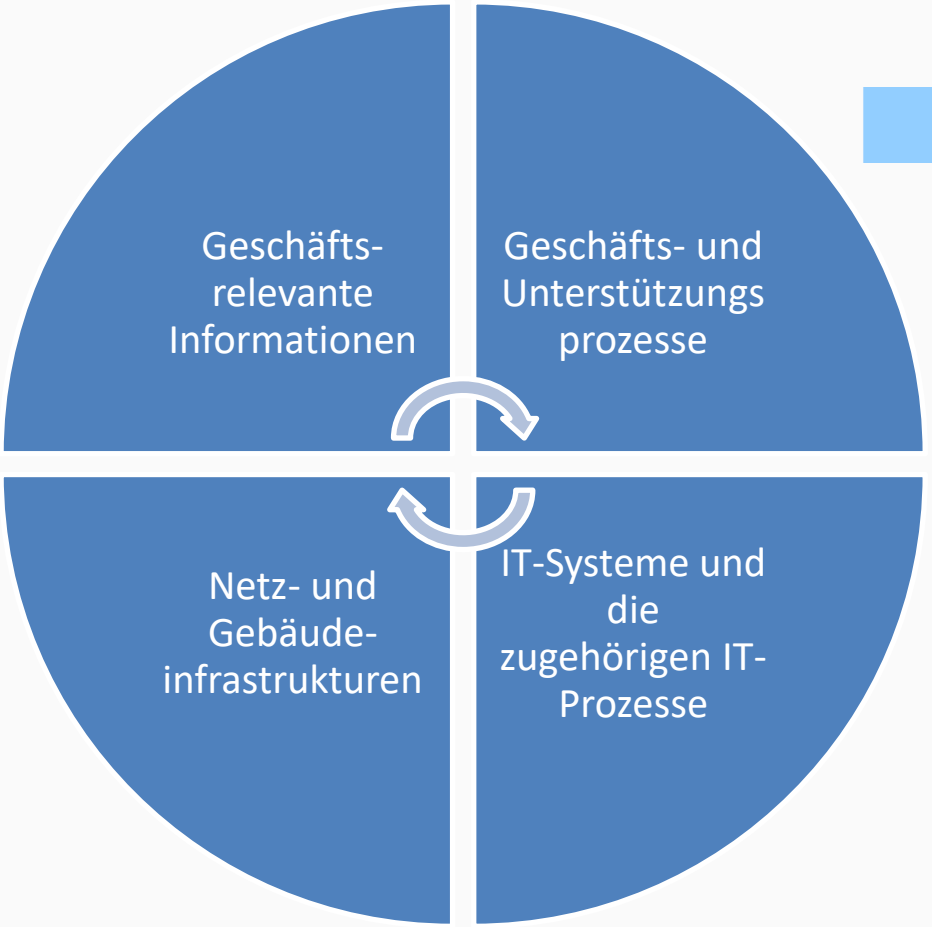
3. Informationsrisikomanagement

- Aufbau eines Systems zum Management der Informationsrisiken
  - Mitwirkung aller maßgeblichen Stellen
  - Kompetenzgerecht
  - Frei von Interessenkonflikten

08.10.2015

BAIT

Informationsverbund gemäß BAIT 3.3, Erläuterungen

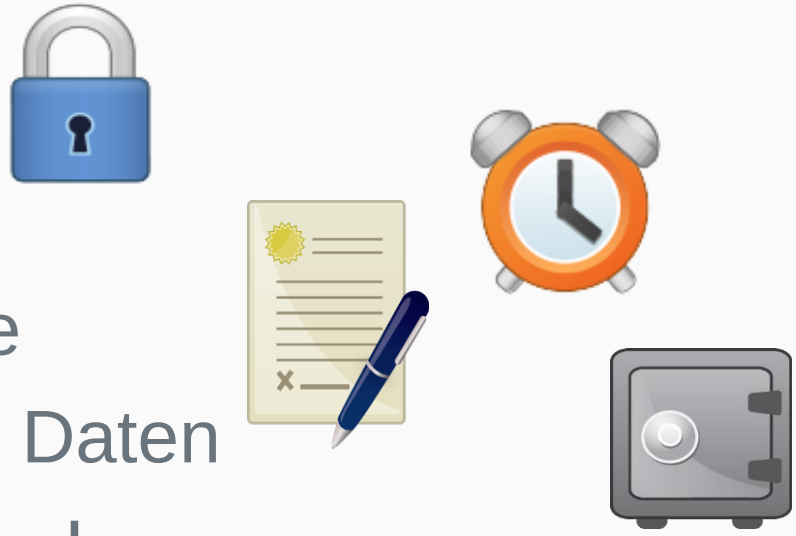


BAIT

3. Informationsrisikomanagement

- Überblick über alle Bestandteile des Informationsverbunds inkl. Abhängigkeiten
- Sicherstellung
  - der Integrität,
  - der Verfügbarkeit,
  - der Authentizität sowie
  - der Vertraulichkeit der Daten

  im Informationsverbund



BAIT

4. Informationssicherheitsmanagement

gefordert werden

- Informationssicherheitsleitlinie
- Informationssicherheitsrichtlinien und -prozesse
- Funktion des IS-Beauftragten
- Analysen und Nachsorgemaßnahmen bei Vorfällen
- Berichterstattung

BAIT

5. Operative Informationssicherheit

- Die operative Informationssicherheit setzt die Anforderungen des Informationssicherheitsmanagements um.
- Überwachungs- und Steuerungsprozesse für IT-Risiken
  - Festlegung von IT-Risikokriterien zur Identifikation von IT-Risiken
  - Festlegung des Schutzbedarfs
  - Abgeleitete Schutzmaßnahmen für den IT-Betrieb
  - Festlegung entsprechender Maßnahmen zur Risikobehandlung und –minderung

BAIT

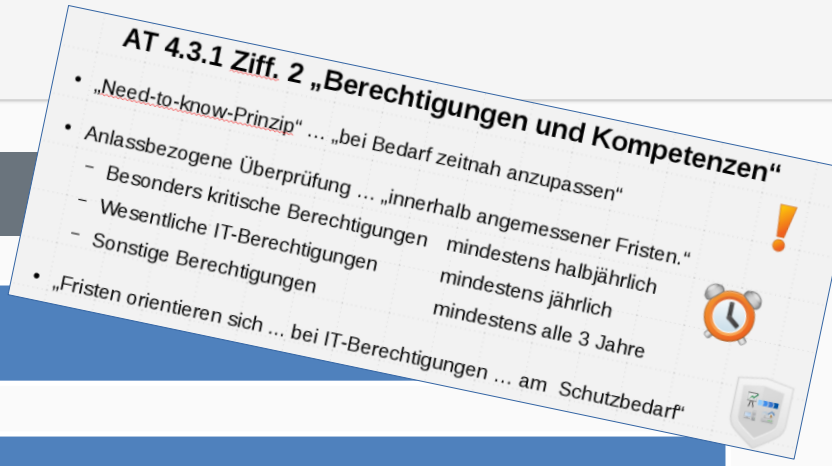
6. Identitäts- und Rechtemanagement (ehem. Berechtigungsmgm.)

- Ein Identitäts- und Rechtemanagement stellt sicher, dass den Benutzern eingeräumte Berechtigungen so ausgestaltet sind und genutzt werden, wie es den organisatorischen und fachlichen Vorgaben des Instituts entspricht.

- Jegliche Zugriffs-, Zugangs- und Zutrittsrechte auf Bestandteile bzw. zu Bestandteilen des Informationsverbundes sollten standardisierten Prozessen und Kontrollen unterliegen.

BAIT

6. Identitäts- und Rechtemanagement



- Berechtigungskonzepte
- Personalisierte und nicht personalisierte Benutzer, Technische Benutzer
- privilegierte (besonders kritische) Benutzer- und Zutrittsrechte
- Funktionstrennung & Zuordenbarkeit
- Verfahren zur Einrichtung, Änderung, Deaktivierung oder Löschung von Berechtigungen
- Überprüfung / Rezertifizierung

BAIT

7. IT-Projekte und Anwendungsentwicklung

IT-Projekte

- Auswirkungsanalyse
- organisatorische Grundlagen
- Projektsteuerung
- Projektportfoliosteuerung
- Berichterstellung und Risikomanagement

Individuelle Datenverarbeitung

- Schutzbedarfsermittlung
- Vorgaben / Zentrales IDV-Register

Anwendungsentwicklung

- Prozesse der Anwendungsentwicklung
- Anforderungen an Anwendungen
- Maßgabe des Schutzbedarfs
- Schutz vor Manipulation
- Dokumentation
- Testen
- Überwachung

BAIT

8. IT-Betrieb

- Der IT-Betrieb hat die Anforderungen, die sich
  - aus der Umsetzung der Geschäftsstrategie sowie
  - aus den IT-unterstützten Geschäftsprozessen

  ergeben, zu erfüllen.

BAIT

8. IT-Betrieb

- Zum IT-Betrieb gehören

– Verwaltung der IT-Komponenten


– (IT-) Lebens-Zyklus Management


– Prozesse zur Änderung von IT-Systemen


– IT-Änderungsmanagement


– Störungsmanagement


– Datensicherung

BAIT

9. Auslagerungen und sonstiger Fremdbezug von IT-

IT-Dienstleistungen umfassen

alle Ausprägungen des Bezugs von IT:

- Bereitstellung von IT-Systemen
- Projekte/Gewerke
- Personalgestellung

auch über ein Netz bereitgestellte: (Cloud-Dienstleistungen)

- Rechenleistung
- Speicherplatz
- Plattformen
- Software

BAIT

Auslagerung

Anforderungen nach AT 9 MaRisk

- Risikoanalysen
- Kontroll- und Überwachungs-prozesse
- Auslagerungs-management

08.10.2015

Sonstiger Fremdbezug

- Risikobewertung
- Steuerung und Überwachung
- Maßnahmen / Vertragsgestaltung / OpRisk-Management
- Überprüfung

BAIT

10. IT-Notfallmanagement

- Definition von Zielen zum Notfallmanagement
- Ableitung Notfallmanagementprozess
- Erstellung Notfallkonzept
- Wiederherstellungspläne
- Regelmäßige Überprüfung

BAIT

11. Management der Beziehungen mit Zahlungsdienstnutzern

- Wegen ZAG:
  Prozesse zur Verbesserung des Bewusstseins der Zahlungsdienstnutzer über die sicherheitsrelevanten Risiken in Bezug auf die Zahlungsdienste:

Beratung	Unterstützung	technische Funktionen	aktive Information

BAIT

12. Kritische Infrastrukturen

- nur für KRITIS-Betreiber - Dienstleistungen gemäß § 7 BSI-Kritisverordnung
- Beachtung der KRITIS-Schutzziele gem. BAIT-Module 3 und 4
- Nachweiserbringung gemäß § 8a Abs. 3 BSIG bzgl. der Einhaltung der Anforderungen gemäß § 8a Abs. 1 BSIG
- Nachweis erstmalig zum Jahresabschluss 2018

BAIT

12. Kritische Infrastrukturen

- Banken sind KRITIS-relevant, u.a. wenn
- Geldautomaten: > 15.000.000 Transaktionen/Jahr

- Banknoten: > 93.500.000 Banknoten/Jahr

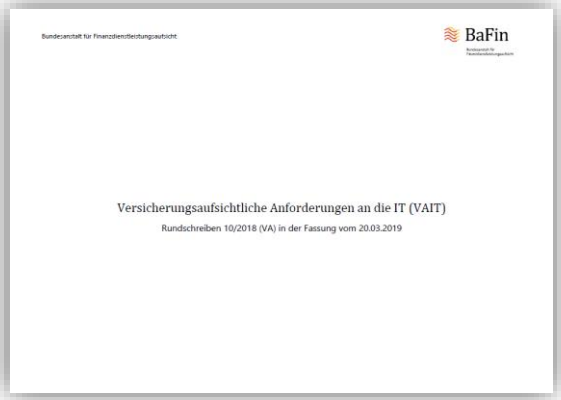
08.10.2015

- Karten-POS: > 18.000.000 Transaktionen/Jahr

Anforderungen an die IT (xAIT)

VAIT

- Versicherungs-aufsichtliche Anforderungen an die IT
- Gesetz: VAG

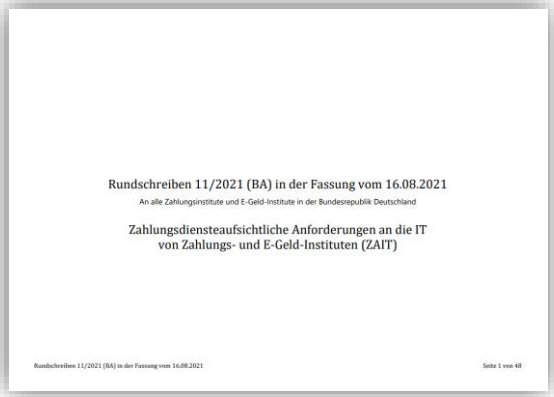


KAIT

- Kapital-verwaltungs-aufsichtliche Anforderungen an die IT
- Gesetz: KAGB

ZAIT

- Zahlungsdienste-aufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld-Instituten
- Gesetz: ZAG



Anforderungen an die IT (xAIT)

VAIT

- 1. IT-Strategie
- 2. IT-Governance
- 3. Informationsrisikomanag.
- 4. Informationssicherheitsm.
- 5. Benutzerberechtigungsm.
- 6. IT-Projekte, Anwendungsentwicklung (inkl. durch Endbenutzer in den Fachbereichen)
- 7. IT-Betrieb (inkl. Datensicherung)
- 8. Ausgliederungen von IT-Dienstleistungen und sonstige Dienstleistungsbeziehungen im Bereich IT-Dienstleistungen; isolierter Bezug von Hard- und/oder Software
- 9. Kritische Infrastrukturen

KAIT

- 1. IT-Strategie
- 2. IT-Governance
- 3. Informationsrisikom.
- 4. Informationssicherheitsm.
- 5. Benutzerberechtigungsm.
- 6. IT-Projekte, Anwendungsentwicklung (inkl. durch Endbenutzer in den Fachbereichen)
- 7. IT-Betrieb (inkl. Datensicherung)
- 8. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen

ZAIT

- 1. IT-Strategie
- 2. IT-Governance
- 3. Informationsrisikom.
- 4. Informationssicherheitsm.
- 5. Operative Informationssicherheit
- 6. Identitäts- und Rechtemanagement
- 7. IT-Projekte und Anwendungsentwicklung
- 8. IT-Betrieb
- 9. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen
- 10. Notfallmanagement
- 11. Management der Beziehungen mit Zahlungsdienstnutzern
- 12. Kritische Infrastrukturen

Gliederung gleicht BAIT

ISACA®
Trust in, and value from, information systems
Germany Chapter

Vielen Dank

Presented by: John Doe

Referent

Axel Dors
CISA, Geschäftsführer

Dors Impuls Deutschland GmbH
Im Windfang 6
41334 Nettetal

Tel.: +49 2153 127 86 88 0
Fax: +49 2153 127 86 88 9
Web: https://dors-impuls.info/de
E-Mail: kontakt.de@dors-impuls.info