more security. usd

BAIT IN DER PRAXIS

Konsequenzen in der Zusammenarbeit zwischen Fachbereichen und IT

BAIT in der Praxis

Die „Bankaufsichtliche Anforderungen an die IT“ (BAIT) regeln seit 2017 unter anderem die Anforderungen an die IT in den regulierten Finanzinstituten.

Abhängig von der bisherigen Zusammenarbeit zwischen Fachbereichen und IT kann die Umsetzung dieser Anforderungen signifikante Änderungen im Zusammenarbeitsmodell mit sich bringen.

Für eine effiziente Umsetzung der BAIT müssen die Zusammenarbeitsprozesse zwischen IT und Fachbereichen überprüft und ggf. angepasst werden.

Welche Aspekte müssen besonders betrachtet werden?

Relevante Aspekte der BAIT für das Zusammen-arbeitsmodell zwischen Fachbereich und IT

Welche Themengebiete adressiert die BAIT?

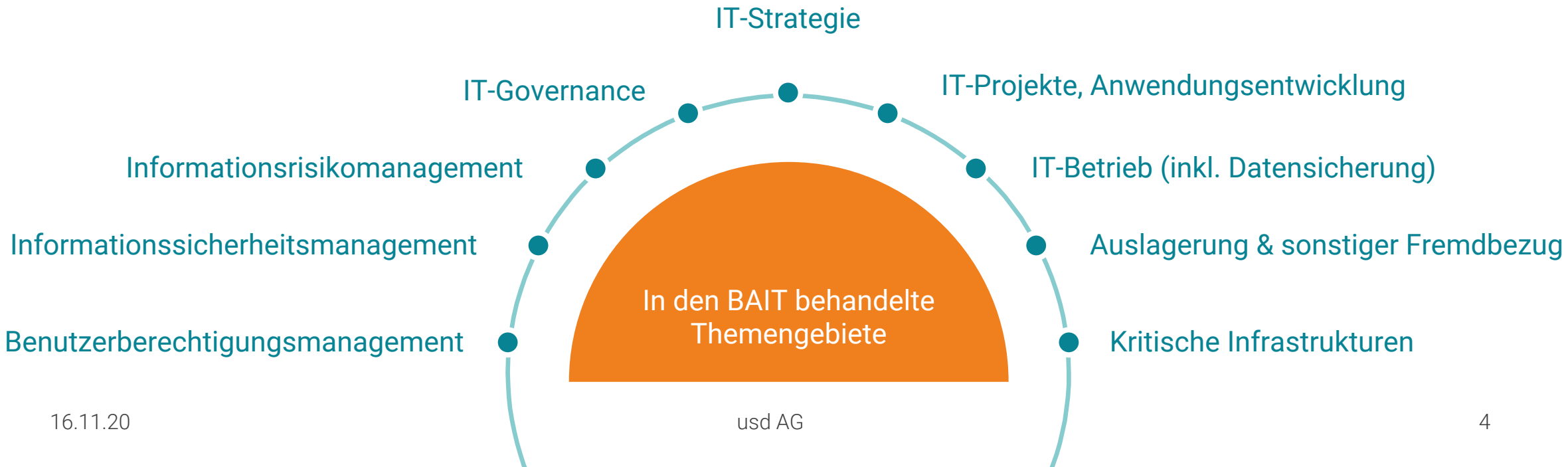
Welche Anforderungen sind für die Zusammenarbeit von Fachbereichen und IT relevant?

Welche Komponenten sollten Zusammenarbeitsmodelle von Fachbereich und IT enthalten?

Welche Änderungen ergeben sich aus der Konsultationsfassung vom 26. Oktober 2020?

Die BAIT stellen generelle Anforderungen an die Nutzung von IT in Finanzinstituten dar

- Die BAIT konkretisieren die Anforderungen der MaRisk um Anforderungen an die Nutzung von IT.
- Die initiale Fassung vom 3. November 2017 wurde am 14. September 2018 um Anforderungen für kritische Infrastruktur erweitert.



Eine Auswahl von Anforderungen mit Fokus auf die Zusammenarbeit von Fachbereichen und IT

- Alle Anforderungen der BAIT haben Einfluss auf die Nutzung von IT und beeinflussen somit die Zusammenarbeit von Fachbereichen und IT.
- In der Praxis haben sich einige Anforderungskomplexe als besonders herausfordernd erwiesen.

Strategiegerechte Nutzung von Auslagerungen

Interessenkonflikte in der IT-Aufbau- und IT-Ablauforganisation

Schnitt des Informationsrisiko-managements

Adäquate Anforderungserhebung

Strategiegerechte Nutzung von Auslagerungen

Anforderung nach Teilziffer 2

Die IT-Strategie muss mit der Geschäftsstrategie konsistent gewählt werden.

Die IT-Strategie muss Aussagen zur Auslagerung von IT-Dienstleistungen enthalten.

Konsequenzen der Anforderung

Die Durchführung von Auslagerungen bzw. Nutzung von Cloud-Diensten[1] muss im Kontext der IT- und Geschäfts-strategie erfolgen.

Beschaffung oder Betrieb von Cloud-Dienstleistungen durch Fachbereiche oder die IT sollte zentral gesteuert oder über-wacht werden.

1. Im Sinne der BaFin „*Orientierungshilfe zu Auslagerungen an Cloud-Anbieter*“ im Allgemeinen als Auslagerung zu betrachten.

Umgang mit Interessenkonflikte
in der IT-Aufbau- und IT-Ablauforganisation

Anforderungen nach Teilziffer 6

Interessenkonflikte und unvereinbare Tätigkeiten in der IT-Aufbau- und IT-Ablauf-organisation sind zu vermeiden.

Insbesondere Interessen-konflikte im Zusammenhang mit der Entwicklung und dem Betrieb sind zu betrachten.

Konsequenzen der Anforderung

Aktivitäten zur Entwicklung, zum Betrieb und zum Test sind mindestens durch Rollen-definitionen zu trennen.

Berechtigungen für Systeme, Daten und Aktivitäten sind festzulegen, durchzusetzen und zu überwachen.

Schnitt des Informationsrisikomanagements

Anforderungen nach Teilziffer 9

Das Informationsrisiko-management muss kompetenz-gerecht und frei von Interessen-konflikten erfolgen.

Die Fachbereiche müssen als Informationseigentümer einbezogen werden.

Konsequenzen der Anforderung

Risiken müssen von den Fachbereichen bewertet, akzeptiert und ggf. getragen werden.

Die Fachbereiche müssen, ggf. unterstützt von Domänen-experten, befähigt werden, die Risikobewertung durch-zuführen.

Adäquate Anforderungserhebung

Anforderungen nach Teilziffer 12

Für Anwendungen müssen funktionale und nicht-funktionale Anforderungen erhoben werden.

Die Verantwortung für die Erhebung der Anforderungen liegt in den Fachbereichen.

Konsequenzen der Anforderung

Die Fachbereiche müssen aktiv in das Anforderungs-management einbezogen sein.

Die Anforderungen müssen technische und Sicherheits-aspekte umfassen.

Beispielhafte Komponenten eines effizienten und BAIT-konformen Zusammenarbeitsmodells

- Die Anforderungen der BAIT beeinflussen die Finanzinstitute ganzheitlich.
- Durch das geeignete Design zentraler Komponenten des Zusammenarbeitsmodells können die Anforderungen erfüllt und das Finanzinstitut effizienter und sicherer gemacht werden.

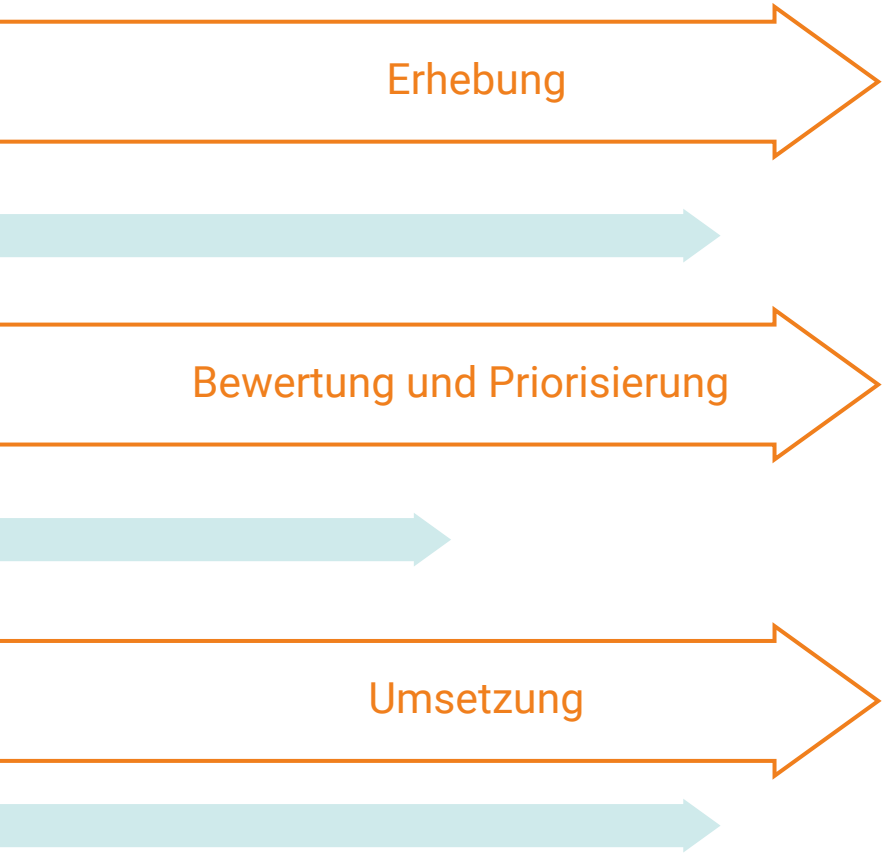
Integriertes Anforderungs-management

Fachlich getriebenes Risikomanagement

Klare Definition von Verantwortlichkeiten

Zusätzliche Komponenten ergeben sich aus dem Kontext des Finanzinstituts.

Integriertes Anforderungsmanagement



- Einheitliche Erhebung von Anforderungen unter Verantwortung der Fachbereiche
- Befähigung der Fachbereiche zur Beachtung von technischen und Sicherheitsanforderungen bei der Anforderungserhebung

- Einbezug von Integrationsaufwänden in die Bewertung
- Betrachtung langfristiger Effizienzgewinne durch Anforderungen, z.B. durch die Reduktion technischer Schuld
- Priorisierung der Anforderungen unter Berücksichtigung von möglichen Ressourcenengpässen bei den umsetzenden Einheiten

- Frühzeitige Beachtung des Sollmaßnahmenkatalogs bei der Umsetzung
- Erstellung und Aktualisierung aller notwendigen Dokumentationen vor der Abnahme

Fachlich getriebenes Risikomanagement

Rollen

BISO — Fachlich Verantwortlicher und Prozess- bzw. Risikoeigentümer

TISO — Umsetzungsverantwortlicher aus der IT-Organisation

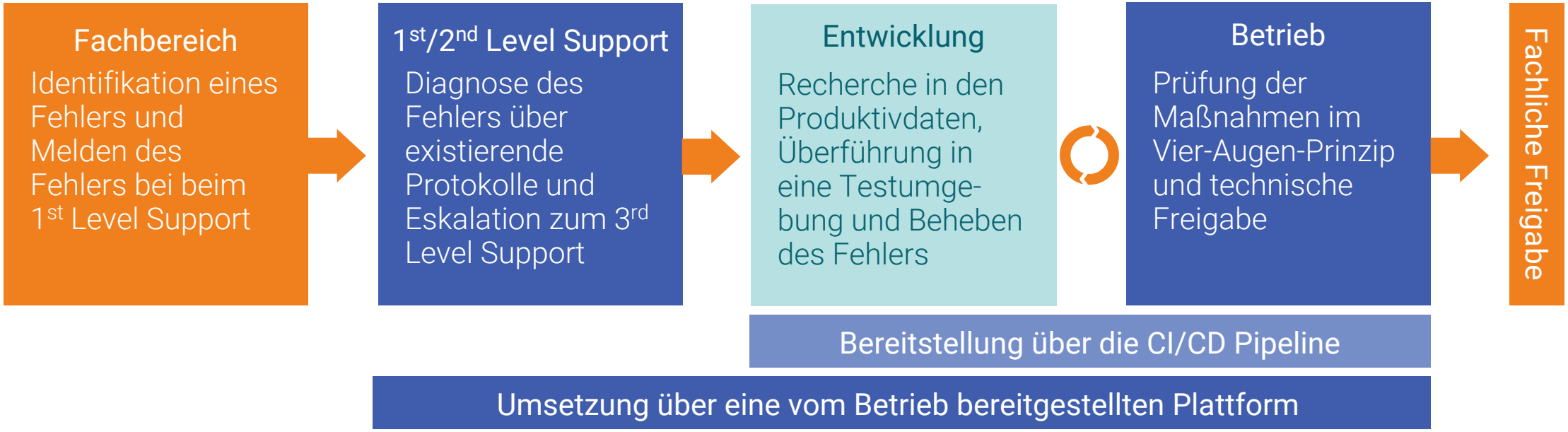
Aktivitäten

BISO	TISO	TISO	BISO	BISO
Beauftragt TISO mit Einführung eines Dienstes	Lässt Dienst durch Mitarbeiter:innen umsetzen	Stellt Abweichungen zum Sollmaß-nahmenkatalog fest und meldet an BISO	Bewertet Risiken mit Unterstützung von Expert:innen	Legt Risiko-behandlung in Abstimmung mit 2nd Line fest

Operative Unterstützung bei der Umsetzung aus den jeweiligen Einheiten

Klare Definition von Verantwortlichkeiten am Beispiel eines Szenarios im 3rd Level Support

- Eine Supportanfrage zu einer Eigenentwicklung kann nicht im 1st / 2nd Level Support behandelt werden.
- Eine Eskalation in den 3rd Level Support ist notwendig.
- Der Fehler kann nicht in Testsystemen nachgestellt werden.



Änderungen in der neuen Konsultationsfassung

- Eine neue Konsultationsfassung der BAIT wurde am 26. Oktober 2020 veröffentlicht, bis zum 23. November können Stellungnahmen an die BaFin eingereicht werden.
- Nach der Bewertung der Stellungnahmen wird eine neue Fassung der BAIT veröffentlicht.

Zusätzliche bzw. umbenannte Themengebiete in der neuen Konsultationsfassung

Operative Informationssicherheit

IT-Notfallmanagement

Kundenbeziehungen mit Zahlungsdienstnutzern

Berechtigungs-management > Identitäts- und Rechtemanagement

Die existierenden – bzw. umbenannten – Themengebieten enthalten zahlreiche neue Anforderungen, welche die Zusammenarbeit von Fachbereichen und IT beeinflussen.

Ausgewählte, ergänzte Anforderungen

mit Einfluss auf die Zusammenarbeit von Fachbereichen und IT

Anforderungen aus Teilziffer 3.7

Risikoanalysen müssen neben Soll-Ist-Vergleichen unter anderem auch Bedrohungen, Schadenspotential und Schadenshäufigkeit betrachten.

Anforderungen aus Teilziffer 5.2

Operativen Informationssicherheitsmaßnahmen sind in Anwendungen, Systemen, Netzen und Gebäuden zu implementieren.

Anforderungen aus Teilziffer 4.4

Befugnisse des Informationssicherheitsbeauftragten werden zur Überwachung und Hinwirkung auf Einhaltung der Informationssicherheit bei Projekten und Beschaffungen ausgeweitet.

Anforderungen aus Teilziffer 7.7

Anforderungen an die Informationssicherheit sind als nicht-funktionale Anforderungen zu definieren und mit Akzeptanz und Testkriterien zu versehen.

Ihr Ansprechpartner

Dr. Christian Schwartz
Managing Consultant
Security Consulting

christian.schwartz@usd.de
Telefon: +49 6102 8631-380
Mobil: +49 151 29268960
Twitter: @ch_schwartz

Wir helfen Ihnen gerne!