ZAIT – Vergleich zur BAIT

Von 12 Kapiteln 6 inhaltsgleich, 5 erheblich und 1 umfangreich erweitert

Dr. Waldemar Grudzien
Liubov Khomutovskaya

Dezember 2021
Blogpost

Key Facts

- Kapitel 9 zu Auslagerungen wurde stark erweitert
- Die weiteren Änderungen in fünf Kapiteln sind mittlerer Natur und sollten technologieaffine, veränderungsfähige Institute vor keine größeren Herausforderungen stellen
- BaFin trägt damit dem Trend zur Auslagerung von IT-Infrastruktur und dem White-Labelling von Bank-Lizenzen Rechnung
- ZAIT führt zusätzliche feingranulare Vorgaben ein, aus einem Rahmenwerk mit Zielformulierungen und der Freiheit der Umsetzung mit angemessenen Maßnahmen wird zunehmend ein Maßnahmenkatalog
- Die weitere Technologisierung des Bankgeschäfts und die Reaktion des Gesetzgebers hierauf zeigen die Vorteile eines vorhandenen funktionsfähigen ISMS auf, da die meisten Anforderungen der ZAIT bereits durch ein umfängliches ISMS nach gängigen Standards adressiert werden.

Einleitung

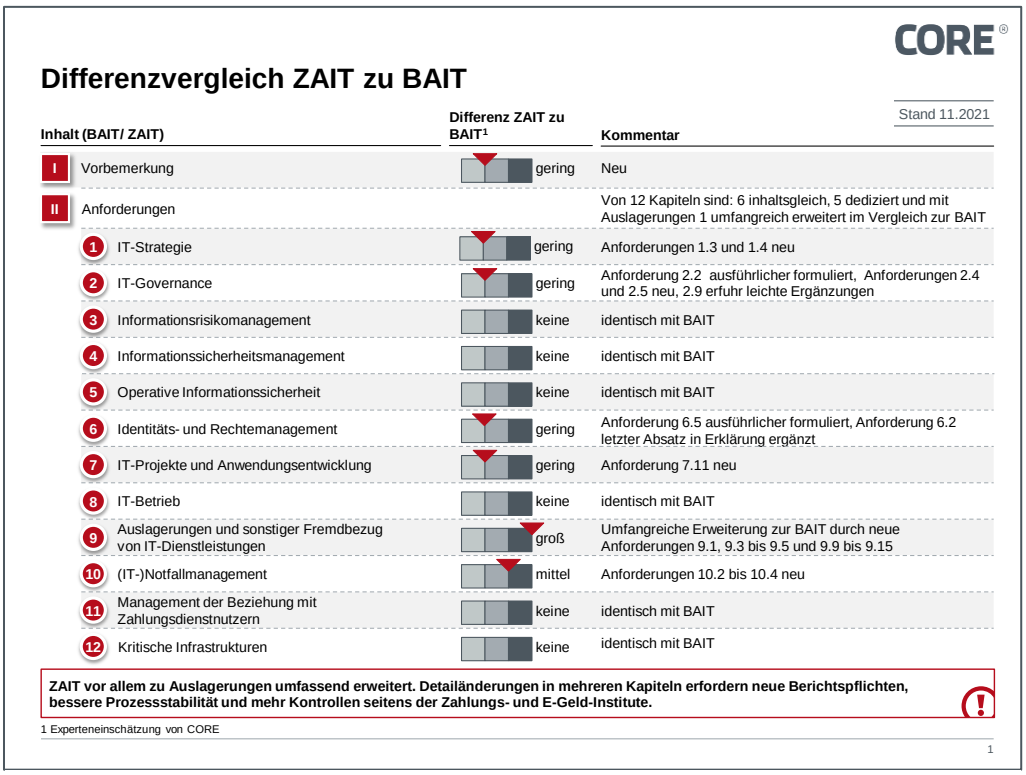
Taggleich mit der Aktualisierung der BAIT hat die BaFin Mitte August 2021 auch die „Zahlungsdiensteaufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld-Instituten – ZAIT“ veröffentlicht. Mit dem Rundschreiben werden die IT-Anforderungen speziell für diese Institute konkretisiert. Die Anforderungen orientieren sich sehr nah an den bereits existierenden IT-Anforderungen für Banken (BAIT) und beinhalten insbesondere die EBA Anforderungen aus den EBA-Leitlinien für IKT und Sicherheitsrisikomanagement (GL/2017/17) sowie den EBA-Leitlinien zu Auslagerungen (GL/2019/02). Von den 12 Kapiteln sind sechs inhaltsgleich zur BAIT geblieben:

- Informationsrisikomanagement,
- Informationssicherheitsmanagement,
- Operative Informationssicherheit,
- IT-Betrieb,
- Management der Beziehungen mit Zahlungsdienstnutzern sowie
- Kritische Infrastrukturen.

Fünf Kapitel erfuhren geringfügige bis mittlere Erweiterungen:

- IT-Strategie,
- IT-Governance,
- Identitäts- und Rechtemanagement,
- IT-Projekte und Anwendungsentwicklung sowie
- IT-Notfallmanagement.

Das Kapitel „9. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistung“ erfuhr sehr umfangreiche Erweiterungen im Vergleich zur BAIT. Eine zusammengefasste Differenzbetrachtung liefert die folgende Abbildung.



Differenzvergleich ZAIT zu BAIT

Stand 11.2021

Inhalt (BAIT/ ZAIT)	Differenz ZAIT zu BAIT[1]	Kommentar
I Vorbemerkung	gering	Neu
II Anforderungen		Von 12 Kapiteln sind: 6 inhaltsgleich, 5 dediziert und mit Auslagerungen 1 umfangreich erweitert im Vergleich zur BAIT
1 IT-Strategie	gering	Anforderungen 1.3 und 1.4 neu
2 IT-Governance	gering	Anforderung 2.2 ausführlicher formuliert, Anforderungen 2.4 und 2.5 neu, 2.9 erfuhr leichte Ergänzungen
3 Informationsrisikomanagement	keine	identisch mit BAIT
4 Informationssicherheitsmanagement	keine	identisch mit BAIT
5 Operative Informationssicherheit	keine	identisch mit BAIT
6 Identitäts- und Rechtemanagement	gering	Anforderung 6.5 ausführlicher formuliert, Anforderung 6.2 letzter Absatz in Erklärung ergänzt
7 IT-Projekte und Anwendungsentwicklung	gering	Anforderung 7.11 neu
8 IT-Betrieb	keine	identisch mit BAIT
9 Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen	groß	Umfangreiche Erweiterung zur BAIT durch neue Anforderungen 9.1, 9.3 bis 9.5 und 9.9 bis 9.15
10 (IT-)Notfallmanagement	mittel	Anforderungen 10.2 bis 10.4 neu
11 Management der Beziehung mit Zahlungsdienstnutzern	keine	identisch mit BAIT
12 Kritische Infrastrukturen	keine	identisch mit BAIT

ZAIT vor allem zu Auslagerungen umfassend erweitert. Detailänderungen in mehreren Kapiteln erfordern neue Berichtspflichten, bessere Prozessstabilität und mehr Kontrollen seitens der Zahlungs- und E-Geld-Institute.

1 Experteneinschätzung von CORE

1

Abbildung 1: Differenzvergleich ZAIT zu BAIT

Einzelbetrachtung Kapitel mit geringen bis mittleren Änderungen

- Vorbemerkung
- Kapitel 1: IT-Strategie,
- Kapitel 2: IT-Governance,
- Kapitel 6: Identitäts- und Rechtemanagement,
- Kapitel 7: IT-Projekte und Anwendungsentwicklung sowie
- Kapitel 10: IT-Notfallmanagement.

Die Vorbemerkungen von BAIT (4 Vorbemerkungen) und ZAIT (5 Vorbemerkungen) gleichen sich in ihren Kernaussagen, indem sie den jeweiligen Anwenderkreis festlegen, den gesetzlichen Rahmen aufspannen, sich auf das Proportionalitätsprinzip verpflichten und bei der Ausgestaltung der IT-Systeme und der dazugehörigen IT-Prozesse grundsätzlich auf gängige Standards abstellen.

In Kapitel „1. IT-Strategie“ wurden die zwei Anforderungen 1.3 und 1.4 neu aufgenommen. In 1.3 schreibt die BaFin einen PDCA-Zyklus für Strategieprozesse vor, Anforderung 1.4 trägt dem Institut Weitergabe und Erörterung der IT-Strategie mit dem Aufsichtsorgan auf, und zwar nicht nur einmalig, sondern auch bei Anpassungen. Bei den beiden Anforderung 1.1 und 1.2 wurde die Konsistenz der IT-Strategie mit der Geschäftsstrategie von 1.2 bei der BAIT in 1.1 bei der ZAIT verschoben, sonst sind beide Anforderungen inhaltsgleich geblieben.

Im Kapitel „2. IT-Governance“ ist die Anforderung 2.2 ausführlicher formuliert, die Anforderungen 2.4 und 2.5 sind neu, Anforderung 2.9 erfuhr leichte Ergänzungen. Anforderung 2.2 wurde erweitert um die Pflicht, Prozesse aus der IT-Aufbau- und IT-Ablauforganisation wirksam umzusetzen. Neu sind nur die beiden Anforderungen 2.4 (Sicherstellung Qualitätsniveau der Mitarbeiter) und 2.5 (fehlende Mitarbeiter dürfen den Betriebsablauf nicht stören). Anforderung 2.9 wurde um den letzten Satz ergänzt (Eignung der IT-Systeme und IT-Prozesse die Schutzziele zu erreichen ist von den fachlich und technisch zuständigen Mitarbeitern zu überprüfen). Die Bemerkungen zu 2.9 wurden in den Standards zur Ausgestaltung der IT-Systeme um PCI-DSS erweitert. Alle anderen Anforderungen zu IT-Governance der ZAIT können auf verschiedene Anforderungen und Erklärungen zum gleichnamigen Kapitel in der BAIT zurückgeführt werden.

Das „Identitäts- und Rechtemanagement“ (Kapitel 6) weist zwei Änderungen zur BAIT auf: Bei Anforderung 6.2 wurde in der Erklärung der letzte Absatz hinzugefügt. Dieser lässt sich zusammenfassen zu „Berechtigungen müssen den organisatorischen Zuordnung entsprechen“. Die zweite Änderung betrifft die nun ausführlicher formulierte Anforderung 6.5 und lässt sich mit zwei zentralen Aussagen zusammenfassen:

- Berechtigungen sind zeitnah anzupassen
- Rezertifizierungen müssen erfolgen mindestens
    - halbjährlich: besonders kritische Berechtigungen wie z.B. von Administratoren
    - jährlich: wesentliche Berechtigungen
    - alle drei Jahre: alle anderen

Kapitel 7 „IT-Projekte und Anwendungsentwicklung“ weist mit Anforderung 7.11 in einzige Änderung auf. Demnach müssen IT-Systeme vor dem erstmaligen Einsatz und nach wesentlichen Änderungen (wobei in der Erklärung ein Hinweis zur Beurteilung der Wesentlichkeit der Veränderung gegeben wird) getestet und abgenommen werden. Hierfür muss ein Regelprozess etabliert werden; die obligatorische Trennung von Produktions- und Testumgebung wird ebenfalls eingefordert. In den Erklärungen wird ein wertvoller Hinweis zu Testaten Dritter wie bspw. Zertifizierungen gegeben; demnach ersetzen diese die eigene Abnahme nicht vollständig. Ein Institut muss weitere eigene Expertise in die Beurteilung der Eignung und Angemessenheit der IT-Systeme einfließen lassen.

Kapitel 10 „Notfallmanagement“ erfuhr mehr Anpassungen: Anforderung 10.1 ist gegenüber 10.1 der BAIT verkürzt, die „fehlenden“ Anteile wurden in der ZAIT auf weitere Anforderungen in Kapitel 10 verteilt. Anforderung 10.2 schreibt für die Identifizierung von Zeitkritikalitäten die Durchführung von Auswirkungsanalysen und Risikoanalysen vor. Die erstgenannte Analyse untersucht beeinträchtigte Aktivitäten und Prozesse hinsichtlich ihrer Auswirkungen auf den Geschäftsbetrieb, die Risikoanalyse untersucht als zeitkritisch identifizierte Aktivitäten und Prozesse hinsichtlich ihrer Beeinträchtigung von Geschäftsprozessen.

Anforderung 10.3 schreibt für das Notfallkonzept sowohl Geschäftsfortführungs- als auch Wiederherstellungspläne vor. Damit wird ebenso wie bei der BAIT als eins von drei möglichen BCMS-Modellen des BSI-Standards 200-4 einzig das Standard-BCMS bevorzugt. Bei Auslagerungen

müssen die Notfallkonzepte aufeinander abgestimmt sein. Der deskriptive Teil der Anforderung schreibt mindestens die folgenden Szenarien zur Berücksichtigung im Notfallkonzept vor:

- (Teil-)Ausfall eines Standorts
- erheblicher Ausfall von IT-Systemen oder Kommunikationsinfrastruktur
- Ausfall einer kritischen Anzahl von Mitarbeitern
- Ausfall von Dienstleistern

Anforderung 10.4 schreibt die regelmäßige Überprüfung der Wirksamkeit und Angemessenheit des Notfallkonzepts vor. Regelmäßig für zeitkritische Aktivitäten und Prozesse bedeutet mindestens jährlich[1] und anlassbezogen nachzuweisen. Die Überprüfungen müssen u.a. beinhalten:

- Test der technischen Vorsorgemaßnahmen
- Kommunikations-, Krisenstabs- und Alarmierungsübungen
- Ernstfall- oder Vollübungen

Beschreibung der Änderungen im Kapitel 9 zu Auslagerungen und sonstigem IT-Bezug

Grundsätzlich verweist die BAIT bei Auslagerungen auf AT.9 MaRisk und macht nur Vorgaben für sonstigen Fremdbezug. Die ZAIT adressiert immer Auslagerungen und sonstigen Fremdbezug bei Verzicht auf den Verweis auf eigene separate Mindestanforderungen.

Die ZAIT kodifiziert Kapitel 9 in großen Teilen neu. Vier Anforderungen der BAIT finden sich auch in der ZAIT wieder:

- ZAIT 9.2 entspricht BAIT 9.1
- ZAIT 9.6 entspricht BAIT 9.5
- ZAIT 9.7 entspricht BAIT 9.3
- ZAIT 9.8 entspricht BAIT 9.4

Die Anforderungen 9.1, 9.3 bis 9.5 und 9.9 bis 9.15 sind neu und werden im Folgenden kursorisch in ihren wichtigsten Aussagen dargestellt:

Anforderung 9.1:

- hebt bei der Auslagerung den Verbleib der Verantwortung beim Institut hervor
- Leitungsaufgaben der Geschäftsleitung sind nicht auslagerbar
- Bei Auslagerung außerhalb EWR muss die Aufsicht des Auslagerungsunternehmens durch die zuständigen Aufsichtsbehörden im Drittstatt sichergestellt sein. Das auslagernde Institut muss sicherstellen, dass eine Kooperationsvereinbarung zwischen den für die Beaufsichtigung des Instituts zuständigen Aufsichtsbehörden und den für die Beaufsichtigung des Auslagerungsunternehmens zuständigen Aufsichtsbehörden besteht.

[1] und anlassbezogen (das wird hier nur ein einziges Mal erwähnt, da jegliche Dokumente bei gegebenem Anlass zu aktualisieren sind)

Letzte Ergänzung ist gänzlich neu und könnte Institute vor ein Fragezeichen und mindestens zeitliche Verzögerungen stellen, zumindest solange keine standardisierten und bereits zahlreich unter Behörden abgeschlossenen Kooperationsvereinbarungen bestehen.

Anforderung 9.3:

- Ein Institut muss weiterhin über genügend Kenntnisse und Erfahrungen verfügen, um eine wirksame Überwachung der erbrachten IT-Dienstleistung zu gewährleisten
- Für den Fall der Beendigung des Auslagerungsverhältnisses oder der Änderung der Gruppenstruktur muss der ordnungsmäßige Betrieb in diesen Bereichen fortgesetzt werden können

Institute sind damit verpflichtet, eigene Ressourcen vorzuhalten, die sowohl fachlich als auch in den wesentlichen Compliance-Bereichen eine hinreichende Bewertung der Leistungen der Dienstleister gewährleisten können. Fraglich ist, ob die Institute den ausgelagerten Bereich im Notfall selbst erbringen können müssen oder ob z.B. eine hinreichend ausführliche Analyse der Anbieterlandschaft und die Möglichkeit eines zügigen Anbieterwechsels genügt. Für die Dienstleistungen mit großer Anbieterauswahl und geringen Migrationskosten ist hier wohl kein Zwang zur Bereithaltung von hinreichend Ressourcen für eine Internalisierung gemeint. Dies würde auch Ziff. 9.9 widersprechen, die bei Fehlen von Handlungsoptionen eine Berücksichtigung in der Notfallplanung fordert, ohne hier spezifischere Vorgaben zu machen.

Anforderung 9.4:

- Definition für Auslagerung, die durch vertragliche Vereinbarungen nicht ausgeschlossen werden kann
- Nennung von Beispielen zur Abgrenzung von Auslagerung und sonstigem Fremdbezug
- Nicht als Auslagerungen einzustufen sich Wartungs- und Software-Unterstützungsleistungen, es sei denn es handelt sich um Software, die zur Identifizierung, Beurteilung, Steuerung, Überwachung und Kommunikation der Risiken eingesetzt wird oder die für die Durchführung von zahlungsdienstegeschäftlichen Aufgaben von wesentlicher Bedeutung ist.

Anforderung 9.5:

- Verpflichtung auf Vorabbewertung einer Auslagerung von IT-Aktivitäten und IT-Prozessen bzw. dem Fremdbezug mittels Risikoanalyse
- Identifikation wesentlicher Auslagerungen auf Basis der Risikoanalysen
- Erstellung von Rahmenvorgaben für Risikoanalyse
- Aus den Erklärungen sind umfangreiche, detaillierte Vorgaben bei Risikoanalyse zu berücksichtigen hinsichtlich Risikobetrachtung, teilnehmenden verantwortlichen Funktionen und
- Bei Auslagerungen von IT-Aktivitäten oder IT-Prozessen mit erheblicher Tragweite ist entsprechend intensiv zu prüfen, ob und wie eine Einbeziehung der ausgelagerten

IT-Aktivitäten und IT-Prozesse in das Risikomanagement sichergestellt werden kann.

Unglücklich ist die Einführung des Begriffs „erhebliche Tragweite“, der neben der „Wesentlichkeit“ nicht zur Vereinfachung beiträgt.

Anforderung 9.9:

- Verpflichtung auf Erstellung einer Ausstiegsstrategie und Ihre regelmäßige Überprüfung
- Existieren keine Handlungsoptionen, so muss die Ausstiegsmöglichkeit im Rahmen der Notfallplanung Berücksichtigung finden

Anforderung 9.10:

- Detaillierte Vorgaben für Mindestinhalte des Auslagerungsvertrages, u.a. „vereinbarte Dienstleistungsgüte mit eindeutig festgelegten Leistungszielen“ und Sicherstellung der Datenschutz-konformen Verarbeitung, Unterstützung des Instituts durch das alte Auslagerungsunternehmen bei Transfer vom alten Auslagerungsunternehmen zum neuen Auslagerungsunternehmen
- Abgrenzung der Pflicht Weisungsrechte zu vereinbaren
- Einräumung von Informations- und Prüfungsrechten für die BaFin bei Auslagerungen

Hilfreich ist der Hinweis, dass auf eine explizite Vereinbarung von Weisungsrechten zugunsten des Instituts verzichtet werden kann, wenn die vom Auslagerungsunternehmen zu erbringende Leistung hinreichend klar im Auslagerungsvertrag spezifiziert ist. Dies stellt häufig einen schwierigen Verhandlungspunkt dar. Ferner kann die Interne Revision des auslagernden Instituts von eigenen Prüfungshandlungen absehen, sofern eine anderweitig durchgeführte Revisionstätigkeit, z. B. in Form von Group-Audits den aufsichtlichen Anforderungen genügt.

Zu internen vorbereitenden Handlungen und zur Dokumentation müssen Überlegungen zum internen Grad der Akzeptanz etwaiger Schlechtleistungen aufgenommen werden.

Anforderung 9.11:

- Einräumung von Informations- und Zustimmungsrechten für das Institut bei Weiterverlagerungen im Auslagerungsvertrag zu hinterlegen
- Weiterverlagerungsvertrag muss Vereinbarungen des originären Auslagerungsvertrags entsprechen
- Institut hat Qualität der ausgelagerten Dienstleistungen regelmäßig zu beurteilen

Anforderung 9.12:

- Pflicht zur Einrichtung der Funktion des zentralen Auslagerungsbeauftragten (zAB), der in Abhängigkeit von Art, Umfang und Komplexität der Auslagerungen durch ein zentrales Auslagerungsmanagement zu unterstützen ist
- Vorgaben zur unmittelbaren Unterstellung des zAB zur Geschäftsleitung
- Vorgaben der Mindestaufgaben des Auslagerungsmanagements

Anforderung 9.13:

- Erstellung eines Berichts über die wesentlichen Auslagerungen mindestens jährlich sowie anlassbezogen (Ausnahme: kleinere, weniger komplexe Institute)
- Ableitung einer Aussage ob Auslagerung fortgeführt werden soll

Anforderung 9.14:

- Erleichterungen für Finanzverbünde wie zum Beispiel
    - Risikomindernde Berücksichtigung von wirksamen Vorkehrungen auf Gruppenebene, insbesondere ein einheitliches und umfassendes Risikomanagement sowie Durchgriffsrechte bei gruppen- und verbundinternen Auslagerungen von IT-Aktivitäten und IT-Prozessen bei der Erstellung und Anpassung der Risikoanalyse
    - Einrichtung eines zentralen Auslagerungsmanagements auf Gruppen- bzw. Verbundebene möglich
    - Verzicht auf die Erstellung von Ausstiegsprozessen und Handlungsoptionen
    - gemeinsame Notfallkonzepte

Anforderung 9.15:

- Vorhaltung eines aktuellen Auslagerungsregisters mit Informationen über alle Auslagerungsvereinbarungen
- inhaltliche Mindestanforderungen an das Auslagerungsregister für alle Auslagerungen in Tz. 54 und für wesentliche Auslagerungen in Tz. 55 der EBA-Leitlinien zu Auslagerungen (EBA/GL/2019/02).
- Das Auslagerungsregister umfasst alle Auslagerungsvereinbarungen, einschließlich der Auslagerungsvereinbarungen mit Auslagerungsunternehmen innerhalb einer Institutsgruppe oder eines Finanzverbunds.
- Bei Weiterverlagerung von wesentlichen Auslagerungen muss auslagerndes Institut festlegen, ob der weiter zu verlagernde Teil wesentlich ist und wesentliche Teile sind im Auslagerungsregister zu erfassen

Verfasser

Waldemar Grudzien ist Expert Director bei CORE. Er wurde in Elektrotechnik promoviert und verfügt über ein Diplom in VWL. Schwerpunkte seiner Arbeit sind Informationssicherheit und Datenschutz – in Theorie und Praxis, inklusive der Tätigkeit als ISB und DSB in verschiedenen Klientenstrukturen.

Mail: waldemar.grudzien@core.se

Liubov Khomutovskaya ist Senior Legal Expert bei CORE. Sie ist Wirtschaftsjuristin und arbeitet schwerpunktmäßig im Bereich Verhandlung und Gestaltung von IT-Verträgen sowie zu Themen der Informationssicherheit.

Mail: liubov.khomutovskaya@core.se

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform Consulting MEA Ltd.
DIFC – 105, Currency
House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633
office@core.se