Deloitte.

Auswirkungen der Zahlungsdiensteaufsichtlichen Anforderungen an die IT von Zahlungs- und E-Geld-Instituten (ZAIT)

Am 12. April 2021 hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) die im Rahmen der Konsultation der Bankaufsichtlichen Anforderungen an die IT (BAIT) avisierten Zahlungsdiensteaufsichtlichen Anforderungen an die IT von Zahlungs- und E-Geld-Instituten (ZAIT) zur Konsultation, die am 14. Mai 2021 endete, veröffentlicht.

Mit den ZAIT werden im Wesentlichen die „EBA-Leitlinien für das Management von IKT[1] und Sicherheitsrisiken" (EBA-Leitlinie 2019/04), in welcher die „EBA-Leitlinien zu Sicherheitsmaßnahmen bezüglich der operationellen und sicherheitsrelevanten Risiken von Zahlungsdiensten gemäß der Richtlinie (EU) 2015/2366 (PSD2)" aufgingen, sowie die „EBA-Leitlinien zu Auslagerungen" (EBA-Leitlinie 2019/02) in die laufende Aufsicht von Zahlungsinstituten überführt.

[1] Informations- und Kommunikationstechnik.

Der Aufbau sowie die adressierten Themenfelder der ZAIT zeigen einen hohen Deckungsgrad mit den BAIT, was unter Berücksichtigung der durch die BaFin zur laufenden Aufsicht von Zahlungsinstituten empfohlenen Orientierung an den Mindestanforderungen an das Risikomanagement (MaRisk) zur Erfüllung der Anforderungen an eine ordnungsgemäße Geschäftsorganisation gemäß § 27 Zahlungsdiensteaufsichtsgesetz (ZAG)[2] nicht überraschend ist.

Wie bereits bei den MaRisk in Verbindung mit den BAIT ist die Umsetzung der sich aus den ZAIT ergebenden Anforderungen an die Informationstechnologie an das Proportionalitätsprinzip gekoppelt. Hierdurch haben die Maßnahmen zur Unternehmenssteuerung, Kontrollmechanismen und Verfahren gemäß § 27 ZAG der individuellen Risikosituation des Zahlungsinstituts Rechnung zu tragen. Indikatoren sind hierbei Art und Umfang der erbrachten Zahlungsdienste und die damit einhergehenden Risiken sowie die Institutsgröße.

Anwendungsbereich der ZAIT

Die ZAIT sind durch Zahlungsinstitute sowie E-Geld-Institute umzusetzen. Nach § 1 Abs. 1 Satz 1 ZAG sind Zahlungsinstitute Unternehmen, die gewerbsmäßig oder in einem Umfang, der einen in kaufmännischer Weise eingerichteten Geschäftsbetrieb erfordert, Zahlungsdienste erbringen.

E-Geld-Institute sind gemäß § 1 Abs. 2 Satz 1 ZAG Unternehmen, die das E-Geld-Geschäft betreiben.

Von der Definition des Zahlungs- und E-Geld-Instituts nicht umfasst sind u.a. CRR-Kreditinstitute, die Europäische Zentralbank, die Deutsche Bundesbank sowie andere Zentralbanken der Europäischen Union. Für CRR-Kreditinstitute, die Zahlungsdienstleister im Sinne des § 1 Abs. 1 Satz 1 Nr. 3 ZAG sind, sind die ZAIT mit Ausnahme von Kapitel 11 „Management der Beziehungen mit Zahlungsdienstnutzern“[3], welches über Kapitel 11 der BAIT für CRR-Kreditinstitute geregelt ist, nicht anzuwenden. Diese haben als KWG-Institute weiterhin die sich aus den Mindestanforderungen an das Risikomanagement (MaRisk) in Verbindung mit den BAIT ergebenden Anforderungen an eine ordnungsgemäße Geschäftsorganisation gemäß § 25a Abs. 1 Kredwesengesetz (KWG) umzusetzen.

Kongruenz zwischen ZAIT und BAIT

Auf den ersten Blick sind die ZAIT identisch zu den BAIT und umfassen nachfolgende Themengebiete:

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

Wie im Anschreiben zu den ZAIT seitens der BaFin dargelegt, „orientieren sich die ZAIT sehr nah an den bereits existierenden IT-Anforderungen für Banken“[4]. Mit der Formulierung „sehr nah“ bringt die BaFin implizit zum Ausdruck, dass die ZAIT im Vergleich zur BAIT[5] dennoch Unterschiede aufweisen. Dabei handelt es sich um weiterführende Ergänzungen in den Themengebieten:

- Kapitel 1 „IT-Strategie“
- Kapitel 2 „IT-Governance“
- Kapitel 6 „Identitäts- und Rechtemanagement“
- Kapitel 9 „Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen“
- Kapitel 10 „Notfallmanagement“
- Kapitel 11 „Management der Beziehungen mit Zahlungsdienstnutzern“

Mit Ausnahme von Kapitel 5 „Operative Informationssicherheit“ und Kapitel 11 „Management der Beziehungen mit Zahlungsdienstnutzern“ handelt es sich bei den Themengebieten und Ergänzungen der ZAIT um keine neuen, in die laufende Aufsichtspraxis übernommenen aufsichtsrechtlichen Anforderungen. Bei den in den ZAIT über die BAIT hinausgehenden Ergänzungen handelt es sich um Anforderungen aus den MaRisk, welche durch CRR-Kreditinstitute bereits umzusetzen sind und daher nicht in den BAIT nochmals aufgenommen wurden. Da die MaRisk für Zahlungs- und E-Geld-Institute keine Anwendung finden, wurden diese als Konkretisierung in die ZAIT überführt. Eine Übersicht der aus den MaRisk in die ZAIT überführten Anforderungen wird zum Schluss in der „Übersicht von MaRisk-Anforderungen in der ZAIT“ dargestellt.

[2] Vgl. https://www.bafin.de/DE/Aufsicht/ZahlungsdienstePSD2/ZulassungsverfahrenundLaufendeAufsicht/ZulassungsverfahrenundLaufendeAufsicht_node.html.
[3] Vgl. Entwurf zum BaFin-Rundschreiben 13/2020 Bankfachliche Anforderungen an die IT (BAIT), Kapitel 11.
[4] Vgl. Anschreiben zur ZAIT.
[5] Vgl. BaFin-Rundschreiben 13/2020 Bankfachliche Anforderungen an die IT (BAIT).

Management der Beziehungen mit Zahlungsdienstnutzern

Mit Kapitel 11 der ZAIT werden sowohl für Zahlungsinstitute als auch für CRR-Kreditinstitute, die Zahlungsdienste erbringen, die sich aus der Umsetzung der Zweiten Zahlungsdiensterichtlinie (PSD2) ergebenden Anforderungen aus der „EBA-Leitlinie 2017/17 Leitlinien zu Sicherheitsmaßnahmen bezüglich der operationellen und sicherheitsrelevanten Risiken von Zahlungsdiensten gemäß der Richtlinie (EU) 2015/2366 (PSD2)“ bzw. aus der „EBA-Leitlinie 2019/04 Management von IKT- und Sicherheitsrisiken“ hinsichtlich der Kundenbeziehungen mit Zahlungsdienstnutzern neu in die laufende Aufsichtspraxis überführt.

Insbesondere wird § 53 ZAG „Beherrschung operationeller und sicherheitsrelevanter Risiken“ durch Kapitel 11 ZAIT dahingehend konkretisiert, dass Prozesse zur Reduzierung von Risiken, denen Zahlungsdienstnutzer ausgesetzt sind, im Zusammenhang mit Zahlungsdiensten zu implementieren sind.

Die zu implementierenden Prozesse umfassen zum einen die Bereitstellung von Informationen, die Unterstützung und Beratung von Zahlungsdienstnutzern in Bezug auf sicherheitsrelevante Risiken wie Cyber-Angriffe (Phishing und Social Engineering), Sicherheit (Passwort- und Virenschutz sowie Durchführung von Updates) sowie Betrugsversuche und zum anderen Prozesse zur Aktivierung oder Deaktivierung von Produktfunktionalitäten wie Sperrung von Überweisungen außerhalb des SEPA-Raums, Anpassung von Betragsobergrenzen für die Durchführung von Überweisungen oder Bargeldverfügungen.

Ziel ist es, durch ein angemessenes Management von Kundenbeziehungen den Zahlungsdienstnutzer über aktuelle Risiken im Zusammenhang mit Zahlungsdiensten angemessen zu informieren und bei Bedarf den Zahlungsdienstnutzer zu unterstützen, sodass dieser angemessen auf Risiken reagieren kann. Die Informationsbereitstellung sowie die Unterstützung können hierbei online über eine Web-Seite des Zahlungsdienstleisters, im Rahmen individueller Beratung oder in schriftlicher Form erfolgen. Hierbei ist zu beachten, dass die Informationsbereitstellung nicht einmalig wie z.B. mit Bereitstellung einer Kundenbroschüre bei Vertragsabschluss erfolgt, sondern die Kommunikationskanäle eine kontinuierliche Informationsbereitstellung, Unterstützung und Beratung sicherstellen.

Operative Informationssicherheit und IT-Notfallmanagement

Obwohl über AT 7.2 MaRisk „Technisch-organisatorische Ausstattung“ und AT 7.3 MaRisk „Notfallmanagement“ diese Themenbereiche bereits in die laufende Aufsichtspraxis für Kreditinstitute überführt wurden, wurden in der 2. Novelle der BAIT mit BaFin-Rundschreiben 13/2020 Kapitel 5 „Operative Informationssicherheit“ und Kapitel 10 „IT-Notfallmanagement“ neu aufgenommen, um der Konsistenz zwischen der deutschen Aufsichtspraxis und den europäischen Anforderungen und Rahmenbedingungen gerecht zu werden[6]. Aufgrund der Orientierung der ZAIT an den BAIT haben beide Themenstellungen auch Einzug in die ZAIT erhalten. Insbesondere Kapitel 10 „Notfallmanagement“ konkretisiert § 27 Abs. 1 Nr. 3 ZAG in Bezug auf das Vorliegen angemessener Notfallkonzepte für IT-Systeme.

Operative Informationssicherheit

Die operative Informationssicherheit umfasst sowohl präventive als auch detektivische Maßnahmen zur Reduzierung von Informationsrisiken.

Neu an den Anforderungen ist, dass die BaFin hierbei explizit auf die Datenanalyse für das Erkennen von Korrelationen, Abweichungen und Mustern als präventive Maßnahme zur frühzeitigen Erkennung von Gefährdungen des Informationsverbundes sowie auf die regelbasierte Identifizierung von sicherheitsrelevanten Ereignissen als detektivische Maßnahme abstellt.

Beide Maßnahmen erfordern die systematische Auswertung von Systemprotokollen, um eine Gefährdung des Informationsverbundes sowie sicherheitsrelevante Ereignisse frühzeitig erkennen und Gegenmaßnahmen einleiten zu können. Aufgrund des Umfangs an auszuwertenden Systemprotokollen erfordert dies in der Regel technische Lösungsansätze, da mittels einer manuellen Bearbeitung mögliche Korrelationen und Muster von Ereignissen kaum erkennbar sind und solche Auswertungen zeitintensiv und langwierig sein werden.

Insbesondere die frühzeitige Erkennung von sicherheitsrelevanten Ereignissen erfordert den Einsatz von technischen Lösungen wie z.B. Intrusion-Detection-Systemen in Kombination mit einem Security Information and Event Management (SIEM), um unautorisierte Zugriffsversuche zu erkennen und Gegenmaßnahmen einzuleiten, bevor sie erfolgreich durchgeführt wurden.

[6] Vgl. Anschreiben zur Konsultation 13/2020.

IT-Notfallmanagement

(IT-)Notfallplanung ist ein essenzieller Bestandteil, um in Notfall- und Krisensituationen die wesentlichen Geschäftsaktivitäten aufrechterhalten und die Auswirkungen eines Notfalls oder einer Krise minimieren zu können.

Das IT-Notfallmanagement ist aus aufsichtsrechtlicher Sicht keine neue Anforderung und für Zahlungs- und E-Geld-Institute über § 27 Abs. 1 Nr. 3 ZAG kodifiziert.

Neu ist jedoch, dass die Aufsicht im Zusammenhang mit dem (IT-)Notfallmanagement sowohl in den BAIT als auch in den ZAIT erstmals die vier Szenarien

- (Teil-)Ausfall eines Standortes,
- erheblicher Ausfall von IT-Systemen oder Kommunikationsinfrastruktur,
- Ausfall einer kritischen Anzahl an Mitarbeitern und
- Ausfall von Dienstleistern

benennt, die im Rahmen des (IT-)Notfallmanagements mindestens zu berücksichtigen sind.

Darüber hinaus nimmt die Aufsicht explizit Bezug auf die Ausgestaltung von (IT-)Notfalltests, die sowohl den Ausfall einzelner IT-Systeme, ganzer Systemverbünde als auch Prozesse wie das Zutritts- und Zugriffsmanagement aufführt. Demnach ist es z.B. nicht mehr ausreichend, jährlich einen Rechenzentrumsschwenk durchzuführen, sondern auch die Wiederherstellung einzelner IT-Systeme sowie der Ausfall einer kritischen Anzahl an Mitarbeitern z.B. aufgrund von Pandemie oder Lebensmittelvergiftung sind zu verproben.

Des Weiteren sind für alle zeitkritischen Aktivitäten und Prozesse die Angemessenheit und Wirksamkeit des Notfallkonzepts für alle relevanten Szenarien mindestens jährlich und anlassbezogen nachzuweisen.

Mit der ZAIT setzt die BaFin die nach dem Vorbild der BAIT geltenden aufsichtsrechtlichen Anforderungen an die IT nun auch für Zahlungs- und E-Geld-Institute um.

Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen

Gemäß § 26 ZAG „Auslagerungen" haben Zahlungs- und E-Geld-Institute für wesentliche Auslagerungen angemessene Vorkehrungen zu treffen, um übermäßige zusätzliche Risiken zu vermeiden. Des Weiteren darf die Auslagerung zu keiner Delegation der Verantwortung der Geschäftsleitung sowie der für die Führung des Zahlungsdienst- oder E-Geldgeschäfts verantwortlichen Personen führen. Darüber hinaus sind ausgelagerte Aktivitäten und Prozesse angemessen in das Risikomanagement einzubinden sowie die Auskunfts- und Prüfungsrechte sowie die Kontrollmöglichkeiten der Aufsicht und der Prüfer (u.a. Interne Revision, Jahresabschlussprüfer, beauftragte Person für Informationssicherheit) sicherzustellen.

Im Vergleich zu den BAIT umfasst Kapitel 9 „Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen" der ZAIT weitere Konkretisierungen und übernimmt die Anforderungen an das Auslagerungsmanagement gemäß AT 9 MaRisk „Auslagerung" mit der Einschränkung, dass die ZAIT im Zusammenhang mit Auslagerungen explizit nur von IT-Aktivitäten und IT-Prozessen sprechen und nicht wie die MaRisk jegliche Auslagerung von institutsspezifischen Aktivitäten und Prozessen inkludieren.

Durch die Aufnahme der Anforderungen aus AT 9 MaRisk „Auslagerung" in die ZAIT werden die sich aus § 26 ZAG ergebenden Anforderungen weiter präzisiert, die Kongruenz zwischen der Banken- und Zahlungsdienstleisteraufsicht sichergestellt sowie die EBA-Leitlinien zu Auslagerungen in die deutsche Aufsichtspraxis überführt.

Des Weiteren wird sichergestellt, dass die Identifikation, Bewertung und Überwachung von Auslagerungen auf Grundlage von institutsweit bzw. gruppenweit einheitlichen Rahmenvorgaben regelmäßig und anlassbezogen durchgeführt sowie die sich aus einer Auslagerung ergebenden Risiken einheitlich und objektiv ermittelt und angemessen durch das Zahlungs- sowie E-Geld-Institut gesteuert werden.

Warum die Aufsicht in den ZAIT im Zusammenhang mit Auslagerungen nur IT-Aktivitäten und IT-Prozesse berücksichtigt, ist kritisch zu hinterfragen, da hierdurch u.a. fachliche Auslagerungen wie z.B. im Bereich Rechnungswesen, Geldwäsche oder Personal nicht angemessen berücksichtigt werden.

Implikationen der ZAIT auf Zahlungs- und E-Geld-Institute

Zahlungsdienstleister, die gemäß § 1 Abs. 1 Satz 1 Nr. 1 als Zahlungsinstitut oder gemäß § 1 Abs. 1 Satz 1 Nr. 2 als E-Geld-Institut zu klassifizieren sind, bekommen nun ein einheitliches Rahmenwerk, wie § 27 ZAG „Organisationspflichten" auszugestalten ist.

Neben der Bestellung einer beauftragten Person für Informationssicherheit durch die Geschäftsleitung und dem Aufbau, der Aufrechterhaltung und Weiterentwicklung eines Informationsrisikomanagements steigen die Anforderungen an die Dokumentation. Insbesondere sind an dieser Stelle

- die Dokumentation der erstmaligen und wiederkehrenden Durchführung einer Risikoanalyse zur Ermittlung der mit einer Auslagerung von IT-Aktivitäten und IT-Prozessen oder dem Fremdbezug von IT-Dienstleistungen einhergehenden Risiken,
- die Dokumentation von fachlichen und technischen Berechtigungskonzepten für die Steuerung des Zugangs zu IT-Systemen und des Zugriffs auf Daten,
- die Dokumentation der Anwendungen, bestehend aus Anwenderdokumentation, technischer Systemdokumentation und Betriebsdokumentation,
- die Dokumentation der Informationsverbünde sowie
- die Dokumentation von IT-Notfalltests

hervorzuheben.

Einen besonderen Stellenwert haben die operative Informationssicherheit und das Management der Beziehungen mit Zahlungsdienstnutzern, da hier durch den Zahlungsdienstleister neue organisatorische, prozessuale sowie technische Änderungen vorzunehmen sind.

Es ist nicht mehr ausreichend, Systemprotokolle entsprechend gesetzlicher und/oder aufsichtsrechtlicher Vorgaben zu archivieren und im Verdachtsfall auszu werten; vielmehr ist eine regelbasierte Near-Time-Analyse von Systemprotokollen zur frühzeitigen Erkennung von Gefährdungen oder sicherheitsrelevanten Ereignissen erforderlich, die zur Bewältigung der Masse an täglich generierten Systemprotokollen eine technische Lösung erfordern.

Neben dem Zahlungs- oder E-Geld-Institut haben des Weiteren auch die Interne Revision sowie der Jahresabschlussprüfer von Zahlungsinstituten ein einheitliches Rahmenwerk, anhand dessen die Prüfungsplanung und -handlungen auszurichten sind.

Insbesondere die Interpretationsmöglichkeiten der sich aus den EBA-Leitlinien für Zahlungs- und E-Geld-Institute ergebenden Anforderungen und deren Umsetzungen werden durch die ZAIT eingeschränkt, sodass der Prüfungsumfang insbesondere im Rahmen von Jahresabschlussprüfungen nicht vom Jahresabschlussprüfer abhängt, sondern durch die ZAIT vorgegeben wird.

Schlussbemerkung

Zahlungsinstitute, die sich entsprechend der Empfehlung der BaFin bereits an den MaRisk und den BAIT orientieren oder wie Leasinggesellschaften aufgrund ihres Geschäftsmodells unter das ZAG gefallen sind und aus einem regulierten Umfeld kommen, sollten mit der Umsetzung der ZAIT mit Ausnahme von Kapitel 5 „Operative Informationssicherheit" und Kapitel 11 „Management der Beziehungen mit Zahlungsdienstnutzern" für die zukünftige Umsetzung der ZAIT gut aufgestellt sein, sodass sich kein signifikanter Mehraufwand ergeben sollte.

Für Zahlungsdienstleister wie Kontoinformations- und Zahlungsauslösedienstleister, die mit der Überführung der PSD2 in deutsches Recht unter die Regulierung fielen und mit der Regulatorik bisher wenig oder keine Berührungspunkte hatten, empfiehlt es sich, eine Gap-Analyse durchzuführen und für identifizierte Schwachstellen eine priorisierte Umsetzungs-Road-Map aufzustellen. Auf Grundlage unserer langjährigen Erfahrung benötigen insbesondere die Umsetzung der Anforderungen an das Berechtigungsmanagement und die Erstellung der erforderlichen Dokumentation der Anwendungen eine angemessene Projektstruktur und ausreichende Kapazitäten bei Mitarbeitern aus dem operativen Betrieb, um die entsprechenden Dokumentationen zu erstellen.

Abschließend bleibt abzuwarten, ob die BaFin für die Umsetzung der sich aus den ZAIT ergebenden Anforderungen eine Übergangsfrist über 2021 hinausgehend zulässt oder eine verpflichtende Umsetzung bis Dezember 2021 erwartet, da die Umsetzungsfrist erheblich die mit der Umsetzung der regulatorischen Anforderungen verbundenen Kosten beeinflusst. Ferner ist abzuwarten, inwieweit im Rahmen der Konsultation die BaFin weitere Änderungen an den ZAIT, insbesondere in Bezug auf mögliche Öffnungsklauseln bzw. Umsetzungserleichterungen, die wiederum Auswirkungen auf die Umsetzungskosten haben werden, umsetzt.

Wie Deloitte Sie unterstützen kann

Zur Beurteilung des Umsetzungsstandes bietet Deloitte einen ZAIT-Compliance-Check an, der unsere bewährte Methodik aus den MaRisk- und BAIT-Compliance-Checks adaptiert. Unser methodischer Ansatz zur Aufdeckung möglicher Handlungsfelder berücksichtigt hierbei neben den aufsichtsrechtlichen Anforderungen insbesondere die institutsspezifische Risikosituation sowie eine Benchmarking-Analyse zur Wahrung des Proportionalitätsprinzips in der Umsetzungsanforderung.

Durch das Aufzeigen möglicher Handlungsfelder werden neben Risiken aus der Nicht-Umsetzung regulatorischer Anforderungen auch operationelle, finanzielle sowie Reputationsrisiken aufgedeckt und transparent dargestellt. Für identifizierte Handlungsfelder definieren wir Umsetzungsmaßnahmen und priorisieren diese anhand einer Umsetzungs-Road-Map, um eine strukturierte sowie effiziente Abarbeitung der Umsetzungsmaßnahmen sicherzustellen und hierdurch die Einhaltung aufsichtsrechtlicher Anforderungen zu gewährleisten.

Auf Wunsch begleiten wir Sie aktiv bei der Umsetzung identifizierter Handlungsbedarfe, sei es als Sparring-Partner oder bei der Definition und Implementierung erforderlicher Prozesse, oder führen nach einer vereinbarten Umsetzungsfrist den ZAIT-Compliance-Check erneut durch, um den Umsetzungsstand sowie den Umsetzungsfortschritt zu bewerten.

Abb. 1 – Übersicht von MaRisk-Anforderungen in der ZAIT

Die „Zahlungsdiensteaufsichtlichen Anforderungen an die IT von Zahlungs- und E-Geld-Instituten (ZAIT)" wurden am 12. April von der BaFin zur Konsultation gestellt und entsprechen erwartungsgemäß im Wesentlichen den BAIT

Erweiterung

IT-Strategie

- IT-Strategieprozess (AT 4.2 Tz. 5)
- Abstimmung der IT-Strategie mit Aufsichtsorgan des Instituts (AT 4.2 Tz. 6)
- Kommunikation der IT-Strategie (AT 4.2 Tz. 7)

IT-Governance

- Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen (AT 4.3.1 Tz. 2)
- Kenntnisse und Erfahrungen von Mitarbeitern (AT 7.1 Tz. 2)
- Ausscheiden von Mitarbeitern (AT 7.1 Tz. 3)
- Technisch-organisatorische Ausstattung (AT 7.2 Tz. 1)
- Ausgestaltung der IT-Systeme und -Prozesse (AT 7.2 Tz. 2)

Identitäts- und Rechtemanagement

- Review von Berechtigungen (AT 4.3.1 Tz. 2)

IT-Projekte und Anwendungsentwicklung

- Testmanagement (AT 7.2 Tz. 3)
- Individuelle Datenverarbeitung (AT 7.2 Tz. 5)

Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen

- Definition Auslagerung (AT 9 Tz. 1)
- Risikoanalyse (AT 9 Tz. 2)
- Umfang zulässiger Auslagerungen (AT 9 Tz. 4 i.V.m Tz. 5)
- Beabsichtigte und unbeabsichtigte Beendigung von Auslagerungen (AT 9 Tz. 6)
- Vertraglicher Mindestinhalt bei wesentlichen Auslagerungen (AT 9 Tz. 7)
- Weiterverlagerung (AT 9 Tz. 8 und AT 9 Tz. 11)
- Risikosteuerung (AT 9 Tz. 9)
- Zentraler Auslagerungsbeauftragter (AT 9 Tz. 12)
- Berichterstattung an die Geschäftsleitung (AT 9 Tz. 13)
- Erleichterungen bei Gruppenauslagerungen (AT 9 Tz. 14*)
- Führen eines Auslagerungsregisters (AT 9 Tz. 15*)

Notfallmanagement

- Business-Impact-Analyse (AT 7.3 Tz. 1)
- Umfang der Notfallkonzepte (AT 7.3 Tz. 2)
- Überprüfung der Notfallkonzepte (AT 7.3 Tz. 3*)

* Neu in die MaRisk aufgenommen

Kontakte

Daniel Hellmann
Director
Risk Advisory | Payments
Tel: +49 (0)30 25468 5879
dhellmann@deloitte.de

Jörg Lang
Senior Manager
Risk Advisory | Payments
Tel: +49 (0)711 16554 7026
jolang@deloitte.de

Deloitte.

Stand 05/2021