

Protokoll

Fachgremium IT am 13.12.2022 13:00 – 15:00

Videokonferenz

Fachgremium IT (FG IT) am 13.12.2022, 13:00 – 15:00 Uhr per Videokonferenz

Im Anschluss an die offizielle Begrüßung durch Vertreterinnen und Vertreter der Aufsicht wird die vorab per Mail versendete Agenda vorgestellt.

TOP 1 Verabschiedung der bisherigen Protokolle (Fachgremium IT vom 09.06.2022 sowie Sonderfachgremium IT vom 20.09.2022)

Die Protokollentwürfe des Fachgremiums IT vom 09.06.2022 sowie des Sonderfachgremiums IT zum Thema Cloud (SFGIT-Cloud) vom 20.09.2022 wurden im Vorfeld der Sitzung an die Teilnehmerinnen und Teilnehmern verteilt. Auf Nachfrage gibt es hierzu keine weiteren Anmerkungen. Die Protokolle werden einstimmig angenommen.

TOP 2 ICT SREP

Ein Vertreter der Aufsicht skizziert die ersten Ergebnisse der Auswertung des ICT SREP anhand eines den Teilnehmerinnen und Teilnehmern zur Verfügung gestellten Foliensatzes. Es wird zunächst ein Überblick über die Methodik und die befragten Institute gegeben. Im Rahmen der Untersuchung wurden 662 Fragebögen ausgewertet und für diese entsprechende Risikolevel und Risikokontrollkategorien dargestellt. Es handelt sich dabei um eine Selbsteinschätzung der Institute, die auf vorgegebenen Multiple-Choice-Antworten und Freitextfeldern basiert.

Es wird ein Überblick darüber gegeben, welche Risikokontrollen den schwächsten Reifegrad (nach BAIT-Modulen) aufweisen. Im Rahmen dessen wird auf Verbesserungspotentiale beim Sollmaßnahmenkatalog hingewiesen. Dieser ist ein wichtiger Bestandteil im Informationsrisikomanagement, sodass ein mangelhafter oder fehlender Sollmaßnahmenkatalog sich negativ auf den gesamten Informationsrisikomanagementprozess (bspw. Soll-Ist-Abgleich) auswirken kann. Die Erwartungshaltung der Aufsicht ist eine Verbesserung in folgenden SREP Durchläufen.

Vertreter der Industrie merken an, dass der Sollmaßnahmenkatalog bei gewissen Dienstleistern aufgrund der hohen Menge an nutzenden Kunden, schwierig umzusetzen sei. Weiterhin würden bestimmte Verträge noch Restlaufzeiten aufweisen und würden erst im Rahmen eines Neuvertrages angepasst.

Weitere Auffälligkeiten liegen im Bereich der operativen Informationssicherheit vor. Hier gebe es laut Vertretern der Aufsicht ebenfalls noch Verbesserungspotential. Auch die Häufigkeit und Schwere von Prüfungsfeststellungen bestätige dies.

Weiterhin weist der Vertreter der Aufsicht auf Auffälligkeiten hinsichtlich des Informationssicherheitsbeauftragten (ISB) hin. Eine Vielzahl der Institute hält diesen, wie durch die BAIT grundsätzlich gefordert, im eigenen Haus vor. Jedoch halten einige Institute diesen nicht im

eigenen Haus vor. Dies führe teilweise zu Prüfungsfeststellungen, da häufig nicht alle Kriterien des Ausnahmetatbestandes (Tz. 4.6 BAIT) erfüllt sind.

Auf Nachfrage erläutern Vertreter der Aufsicht, dass die Auslagerung des ISBs kein grundsätzliches Problem darstelle, jedoch im Rahmen von Prüfungen teilweise festgestellt werde, dass die notwendigen Kriterien für eine Auslagerung des ISBs nicht vorliegen. Zu beachten sei dabei insbesondere, dass die Kriterien aus Tz. 4.6 BAIT kumulativ zu erfüllen seien.

Auf Nachfrage erläutern Vertreter der Aufsicht das geplante Vorgehen für künftige Abfragen. Es sei geplant die Struktur beizubehalten, wenngleich nicht jede Frage übernommen werde. Weiterhin sei nicht geplant alle Institute jedes Jahr abzufragen, dies werde gem. des Risikogehaltes der Institute angepasst.

TOP 3 Update zu DORA

Eine Vertreterin der Aufsicht gibt einen Überblick über die bisherigen Arbeiten am Digital Operational Resilience Act (DORA) und erläutert den aktuellen Stand des Verordnungsvorhabens. Ziel sei ein europaweit harmonisierter Rahmen für den Umgang mit Risiken der IKT. Hierbei geht sie insbesondere auf die abgeschlossene Trilogverhandlung zwischen dem EU Rat, der Europäischen Kommission und dem Europäischen Parlament ein. Sie führt weiter aus, dass die finale Fassung zeitnah erwartet werde. Anfang 2023 werde das Inkrafttreten erwartet, die Anwendung erfolge dann entsprechend 24 Monate später.

Sie erklärt darüber hinaus, dass die Ausarbeitung der technischen Regulierungsstandards (Regulatory Technical Standards – RTS) sowie der technischen Durchführungsstandards (Implementing Technical Standards – ITS) abhängig von der genauen Frist 12 bis 18 Monate dauern würden. Im europäischen Unterausschuss für Digital Operational Resilience (JC SC DOR), der eingerichtet wurde, um die Mandate der ESAs für DORA zu erstellen, seien die BaFin und die Bundesbank jeweils durch eine Person vertreten.

Auf Nachfrage führt die Vertreterin der Aufsicht aus, dass bis zur Anwendung von DORA ab 2025 noch die BAIT gelte.

TOP 4 Orientierungshilfe Cloud

Ein Vertreter der Aufsicht stellt den aktuellen Stand zur Orientierungshilfe zu Auslagerungen an Cloud-Anbieter vor. Diese befinde sich gerade in der Überarbeitung, da sich seit 2018 einige neue Entwicklungen ergeben hätten und das Merkblatt die Fortentwicklung der Aufsichtspraxis widerspiegeln soll. Man werde am bestehenden Inhalt der Orientierungshilfe nur notwendige Änderungen vornehmen und neue Themen ergänzen.

Es handele sich hierbei um einen Entwurf, der aktuell noch BaFin intern und mit der Bundesbank abgestimmt wird und dann auch im Fachgremium vorgestellt werden könne. Die Orientierungshilfe sei nicht verbindlich, sondern biete, wie es der Name sagt, eine Hilfe zur Orientierung. Daher werde diese nicht formal konsultiert.

Erkenntnisse aus den Sonderfachgremien Cloud seien eingeflossen und werden aber aufgrund der Detailfülle nicht in Gänze wiedergegeben, sondern an die Struktur des Dokuments angepasst. Weiterer Anpassungsbedarf aufgrund von DORA ist möglich.

Die aktuellen Inhalte der Orientierungshilfe, die eher die Einführung und Governance der Cloud abbilden, sollen im Merkblatt verbleiben, es sollen aber zwei Bereiche hinzukommen. Diese sollen den weiteren Lebenszyklus einer Auslagerung in die Cloud abdecken, zum einen mit Hinweisen zur Architektur von Cloud-Anwendungen und zum sicheren Cloud-Betrieb sowie zum anderen mit Erläuterungen zur Überwachung und Kontrolle von Cloud-Auslagerungen.

Die Vertreterinnen und Vertreter der Aufsicht bedanken sich für das offene Feedback und ggf. weiteres Feedback im Nachgang der Sitzung per E-Mail.

Auf Nachfrage führt ein Vertreter der Aufsicht aus, dass die in der Orientierungshilfe angeführte „Qualifikation“ auf verschiedene Art und Weise, wie bspw. durch Praxiserfahrung oder Fortbildungen, erworben werden könne.

Auf Nachfrage führt ein Vertreter der Aufsicht weiterhin aus, dass die Orientierungshilfe alle Arten von Cloudservices, wie bspw. IaaS, PaaS oder SaaS umfasse.

Weiterhin führt ein Vertreter der Aufsicht auf Nachfrage aus, dass die Protokolle im Rahmen des Fachgremiums weiterhin bestehen sollen. Diese seien deutlich detaillierter und greifen einzelne konkrete Problemstellungen auf. Die Orientierungshilfe nähert sich hingegen eher auf grundsätzliche Art und Weise dem Thema.

TOP 5 Sonstiges / Organisatorisches (insb. Termine 2023)

Eine Vertreterin der Aufsicht stellt die geplanten Termine für 2023 dar. Es gibt zu diesen keine Rückmeldungen.

Die Vertreterinnen und Vertreter der Aufsicht bedanken sich bei allen Teilnehmerinnen und Teilnehmern für ihre Mitwirkung an der Onlinesitzung, wünschen eine besinnliche Weihnachtszeit und beenden die Veranstaltung um 15:00 Uhr.

Teilnehmerinnen und Teilnehmer Fachgremium IT am 13.12.2022

Bigeschi, Marco	Raiffeisenbank Aidlingen eG
Böse, Stefan	DZ BANK AG Deutsche Zentral-Genossenschaftsbank
Burckhardt, Michael	Commerzbank AG
Delfs, Christian	Verband Deutscher Bürgschaftsbanken e.V.
Dickhoff, Andreas	Atruvia
Dierks, Christian	Deutsche Bank AG
Fichelscher, Andreas	Kreditanstalt für Wiederaufbau Anstalt des öff. Rechts
Hidasi, Annette	Boerse Stuttgart GmbH
Kastl, Andreas	Verband der Auslandsbanken in Deutschland e.V.
Koen, Oliver	Atruvia AG
Melina, Pfisterer	Landesbank Hessen-Thüringen Girozentrale Anstalt des öff. Rechts
Muster, Holger	Finanz Informatik GmbH & Co KG
Nash, Andre	Bundesverband deutscher Banken e.V.
Penther, Brigitte	Hamburg Commercial Bank AG
Rosenberg, Holger	IKB Deutsche Industriebank AG
Scheidl, Marcus	Bundesverbandes Öffentlicher Banken Deutschlands
Schimm, Berit	Bundesverband VR Banken
Semmler, Oliver	Boerse Stuttgart GmbH
Somma, Michael	Bankenfachverband e. V.
Steuber, Martin	UniCredit Bank AG
Stichter, Thorsten	VR Bank Main-Kinzig-Büdingen eG
Trojahn, Frank	DSGV
Zimmermann, Karin	BKM - Bausparkasse Mainz AG

Paust, Dr. Michael	Deutsche Bundesbank
Bretz, Jörg	Deutsche Bundesbank
Habicht, Anke	Deutsche Bundesbank
Janlewing, Dr. Rainer	Deutsche Bundesbank
Mußleack, Markus	Deutsche Bundesbank
Schäfer, Dominik	Deutsche Bundesbank
Schnack, Bjarne	Deutsche Bundesbank
Vogel, Andreas	Deutsche Bundesbank
Kosche-Steinbrecher, Ira	Bundesanstalt für Finanzdienstleistungsaufsicht
Fechler, Dr. Katharina	Bundesanstalt für Finanzdienstleistungsaufsicht
Pohl, Markus	Bundesanstalt für Finanzdienstleistungsaufsicht
Kleinknecht-Dennart, Dr. Sven	Bundesanstalt für Finanzdienstleistungsaufsicht