Protokoll

Fachgremium IT am 09.06.2022

Videokonferenz

Fachgremium IT (FG IT) am 09.06.2022, 10:00 – 13:00 Uhr per Videokonferenz
Im Anschluss an die offizielle Begrüßung durch Vertreter*innen der Aufsicht wird die vorab per Mail versendete Agenda vorgestellt und um Ergänzungen gebeten (keine Ergänzungen).

TOP 1 Protokoll des Fachgremiums IT vom 02.12.2021
Der Protokollentwurf des Fachgremiums IT vom 02.12.2021 wurde im Vorfeld der Sitzung an die Teilnehmer*innen verteilt. Die Rückmeldungen wurden im Änderungsmodus eingearbeitet. Auf Nachfrage gibt es hierzu keine weiteren Anmerkungen. Das Protokoll wird einstimmig angenommen.

TOP 2 Protokoll des Sonderfachgremiums IT Cloud/CMDB 01.03.2022
Der Protokollentwurf des Sonderfachgremiums IT Cloud/CMDB 01.03.2022 wurde im Vorfeld der Sitzung an die Teilnehmer*innen verteilt. Die Rückmeldungen wurden im Änderungsmodus eingearbeitet. Es wird sich darauf geeinigt, den Begriff Sourcing Mechanismen, anstatt Beschaffungsmechanismen zu verwenden, damit es bei Veröffentlichung zu keinen Missverständnissen kommt. Das Protokoll wird einstimmig angenommen.

TOP 3 Update zu DORA
Eine Vertreterin der Aufsicht gibt zu den Verhandlungen zum Digital Operational Resilience Act (DORA) ein Update. Am 10. Mai erzielten der Europäische Rat, das Europäische Parlament und die Europäische Kommission im Trilog eine vorläufige politische Einigung zu DORA. Es würde erwartet, dass DORA noch in diesem Monat im EU Rat finalisiert wird. Die vorläufige Einigung beinhalte folgende Punkte: Wirtschaftsprüfer und –gesellschaften stehen nicht mehr im Anwendungsbereich, aber DORA werde vsl. eine Revisionsklausel enthalten. Weiter sollen kritische IKT-Drittdienstleister eine „Subsidiary“ in der EU gründen. Ebenfalls beim Überwachungsrahmenwerk ist die Etablierung eines sog. Joint Oversight Network zur Koordination zwischen den Europäischen Aufsichtsbehörden vorgesehen. Bei TLPT sollen nunmehr, unter sehr engen Voraussetzungen, interne Tester möglich sein. Und hinsichtlich der Interaktion mit der NIS 2.0 bleibt die lex-specialis Klausel bestehen.
Ein Vertreter der Industrie erfragt die genaue Zeitschiene, ab welchem Zeitpunkt DORA zum Tragen komme, ob es einen Zeitplan für die Entwicklung der RTS gebe und ob seitens der Industrie an diesen mitgearbeitet werden könne. Eine Vertreterin der Aufsicht beantwortet, dass die konkrete Zeitplanung noch Gegenstand der Verhandlungen sei. Lege man das Ratsmandat zu Grunde, wird DORA vsl. Ende 2022 in Kraft treten und dann zwei Jahre später, Ende 2024, Anwendung finden; für die Erstellung der technischen Regulierungsstandards (RTS) und technischen Durchführungsstandards (ITS) sowie der Leitlinien seien im Ratsmandat 18 Monate vorgesehen. Bei der Erstellung der Leitlinien und technischen Standards (RTS/ITS) sei eine öffentliche Konsultation im Rahmen des Erstellungsprozesses vorgesehen. Diese ermöglicht der Industrie als auch allen anderen Stakeholdern sich einzubringen.

Ein Vertreter der Industrie erfragt, ob sich evtl. Dopplungen mit der Richtlinie über die Netz- und Informationssicherheit (NIS) ergeben würden. Eine Vertreterin der Aufsicht antwortet, dass NIS weiterhin gelte. Beinhalte aber DORA gleichartige oder auch spezifischere Regelungen als die NIS, also Überschneidungen, greife die lex-specialis Klausel, die DORA enthalten wird. Ein Vertreter der Industrie bringt ein, dass auch die xAIT in diesem Zusammenhang angeschaut werden und ggfs. Anpassungen erforderlich seien. Dies werde getan, sei aber laut Aufsicht erst nach Erarbeitung der entsprechenden RTS möglich.
Auf Nachfrage der Industrie wird von Seiten der Aufsicht erklärt, dass aktuell noch offen sei, ob Förderbanken im Anwendungsbereich stehen werden.

TOP 4 Umfrage zu Log4J
Ein Vertreter der Bundesbank präsentiert die wesentlichen Erkenntnisse einer Adhoc-Abfrage der Aufsicht bei Finanzunternehmen zum Umgang mit der am 10.12.2021 durch das BSI bekannt gegebenen Sicherheitslücke in der Java-Bibliothek Log4J. Es wurde diskutiert, wodurch die langen Reaktionszeiträume seitens der Industrie zwischen Meldung durch das BSI und dem Ergreifen erster Maßnahmen und dem vollständigen Patchen aller betroffenen IT Systeme zu begründen seien. Dies wird von Vertretern der Industrie mit der Lage des Zeitpunkts kurz vor Weihnachten und der Intensität des Vorfalls begründet. Es seien unzählige IT Systeme jeglicher Art innerhalb der Unternehmen betroffen gewesen und die Komplexität der Faktoren hätten die Prozesse verlangsamt. Durch den Vortragenden wurde betont, dass nur der entsprechende Patch aus Sicht der Aufsicht das Risiko final adressiert.
Vom Vortragenden wird die Frage in das Fachgremium gestellt, was aus diesem Vorfall gelernt wurde, bzw. was bei einem erneuten Vorfall in dem eine Bibliothek betroffen sein könnte anders gemacht werden könnte. Dazu gibt es keine Rückmeldungen.
Außerdem wird vom Vortragenden nachgefragt, wie zukünftige Abfragen optimiert werden könnten. Ein Vertreter der Industrie regt an, detailliertere und dezidierte Abfragen durchzuführen.. Es wird seitens der Industrie der Vorschlag geäußert, dass aus einem Fragebogen klarer die Zuständigkeit für die Beantwortung sowohl bei den Unternehmen als auch bei deren Dienstleistern hervorgehen solle. Zudem solle es eine klare Kennzeichnung im Fragebogen geben, wo Meldungen aufgrund von Meldungen durch Mehrmandantendienstleister nicht erforderlich seien.

TOP 5 Einsatz Künstlicher Intelligenz
Eine Vertreterin der Industrie hält einen Gastvortrag zum Thema „Risikomanagement und Model Governance beim Einsatz von Künstlicher Intelligenz und Maschinellem Lernen“. Im Anschluss findet eine Round-Table Diskussion mit dem Fachgremium IT statt. Die Vortragende bestätigt auf Nachfrage, dass beim Einsatz von KI in ihrem Haus nach dem „Human in the Loop Prinzip“ bei allen Vorgängen menschliche Interaktionen zur Durchführung von relevanten Prozessen erforderlich seien und sich nach Stand heute der Kunde noch nicht in einer vollautomatisierten Betreuung/Beratung befinde. Das gäbe auch die Einhaltung der EU-Datenschutz-Grundverordnung nicht her.
Von einem Vertreter der Industrie kommt die Frage auf, wie beim Einsatz von KI die die Regelkonformität bei der Dokumentation der Vorgänge eingehalten werden könne. Wie müsse inventarisiert werden um die Wirtschaftsprüfung zu bestehen? Dies kann nicht beantwortet werden, die Informationen würden von der Vortragenden aber im Nachgang zur Sitzung nachgereicht werden.
Die Nachfrage, ob für das Thema KI bestehende „second lines of defense“ als Risikomanagementfunktionen erweitert oder neue eingeführt werden müssten wird verneint. Dies sei bis zum heutigen Stand nicht angedacht.

Ein Vertreter der Aufsicht fragt in wie weit KI heute in den Unternehmen eingesetzt wird, welche Anwendungen bereits etabliert seien, welche Herausforderungen damit verbunden seien und welche neuen Entwicklungen gerade entstehen würden. Einzelne Vertreter der Industrie nennen Beispiele zum heutigen Einsatz von KI im laufenden Geschäft, wie bspw. die Nutzung von Spracherkennung oder den Einsatz von Fotoüberweisungen. Die meisten Anwendungen würden von externen Dienstleistern angeboten und umgesetzt. Ein Vertreter der Industrie berichtet, dass KI für Kreditvergabeentscheidungen eingesetzt wird. Einige Vertreter der Industrie erwähnen, dass KI insbesondere zur internen Prozessoptimierung eingesetzt wird.
Es wird von einem Vertreter der Aufsicht angeregt, dass es zukünftig einen fortlaufenden Austausch zum Thema KI-Verordnung geben solle. Dabei sollen folgende Aspekte betrachtet werden: Welche Bereiche der Institute betroffen seien, welche KI-Systeme in die Kategorien „low-“ oder „high-risk“ fallen, welche darüberhinausgehenden Anforderungen die KI Verordnung in der finalen Fassung an die Institute stellt und was davon in der Auslegung konkretisiert werden müsste.

TOP 7 Sonstiges
Es werden zwei Nachfragen von einem Verbandsvertreter dazu gestellt, wie (1) der aktuelle Sachstand zum Diskussionspapier zu MaRisk und (2) wie weit die Erarbeitung zur Orientierungshilfe zu Cloud vorangeschritten sei. Die Aufsicht erklärt zu (1), dass am 24.06.2022 das Fachgremium MaRisk tage und es danach neue Erkenntnisse geben werde. Bei (2) kommt es aus Kapazitätsgrünen zu Verzögerungen. Sobald der Entwurf der Orientierungshilfe vorliege, würde er hier im FG IT präsentiert.

Die Aufsicht berichtet über die Anfrage eines Finanzunternehmens, in das FG IT aufgenommen zu werden. Diese Anfrage wird von Seiten der Aufsicht unterstützt. Es liegen keine Bedenken der anderen Mitglieder des FG IT vor und es wird der Aufnahme zugestimmt.

Ein Vertreter der Industrie äußert den Wunsch, sich zukünftig im FG IT zum Thema Teams/Cloud Anwendungen, wie hier der Umgang in anderen Unternehmen gehandhabt werde und sich zu best practices auszutauschen.

TOP 8 Termine
Der Termin für ein Sonderfachgremium zum Thema Weiterverlagerung wird auf den 18.08.2022 von 10-13 Uhr festgelegt.

Am 20.09.2022 und am 15.11.2022 finden die nächsten Sonderfachgremien statt.

Das nächste FG IT tagt am 13.12.2022. Nach Abstimmung soll es in Präsenzveranstaltung stattfinden. Sollte dies pandemiebedingt nicht möglich sein, werde kurzfristig auf eine Onlineveranstaltung umdisponiert. Inhaltliche Themen werden im Vorfeld abgestimmt.

Die Vertreter*innen der Aufsicht bedanken sich bei allen Teilnehmer*innen für ihre Mitwirkung an der Onlinesitzung und beenden die Veranstaltung um 13:05 Uhr.

Teilnehmer*innen Fachgremium IT am 09.06.2022

Name	Institut
Böse, Stefan	DZ Bank AG
Buddensiek, Dirk	Bürgschaftsbank Baden-Württemberg GmbH
Burckhardt, Michael	Commerzbank AG
Dickhoff, Andreas	Atruvia
Dierks, Christian	Deutsche Bank
Fichelscher, Andreas	KfW Bankengruppe
Koen, Oliver	Atruvia AG
Kohaut, Thomas	Helaba
Muster, Holger	Finanz Informatik GmbH & Co KG
Nash, Andre	Bundesverband deutscher Banken e.V.
Penther, Brigitte	Hamburg Commercial Bank AG
Saller, Christian	Bayern LB
Scheidl, Marcus	Bundesverbandes Öffentlicher Banken Deutschlands
Schimm, Berit	Bundesverband VR Banken
Simone Heuser	IKB Deutsche Industriebank AG
Somma, Michael	Bankenfachverband e.V.
Sterling, Julia	Commerzbank AG
Steuber, Martin	UniCredit
Stichter, Thorsten	VR-Bank MBK
Trojahn, Frank	DSGV
Vahldiek, Wolfgang	Verband der Auslandsbanken
Zimmermann, Karin	BKM - Bausparkasse Mainz AG
Englisch, Rainer	Deutsche Bundesbank
Habicht, Anke	Deutsche Bundesbank
Paust Dr., Michael	Deutsche Bundesbank
Rest, Matthias	Deutsche Bundesbank
Schäfer, Dominik	Deutsche Bundesbank
Stöllinger, Regina	Deutsche Bundesbank
Brüggemann, Silke	Bundesanstalt für Finanzdienstleistungsaufsicht
Fechler Dr., Katharina	Bundesanstalt für Finanzdienstleistungsaufsicht
Kiefer, Jan	Bundesanstalt für Finanzdienstleistungsaufsicht
Kosche-Steinbrecher, Ira	Bundesanstalt für Finanzdienstleistungsaufsicht
Sämisch, Thorsten	Bundesanstalt für Finanzdienstleistungsaufsicht