Protokoll

Sonderfachgremium Cloud zum Thema „Zertifikate“ am 07.10.2021

Videokonferenz

Sonderfachgremium Cloud am 07.10.2021, 10:00 – 15:00 Uhr per Videokonferenz
Deutsche Bundesbank und BaFin begrüßen die Teilnehmerinnen und Teilnehmer. Die Aufsicht erläutert, es gebe heute keine schriftliche Agenda, da für dieses Sonderfachgremium ausschließlich eine Diskussion zum Thema „Zertifikate“ auf Basis der Ergebnisse der Praxisarbeitsgruppe Cloud der Banken vorgesehen sei. Auf die Frage an die Teilnehmerinnen und Teilnehmer, ob weitere Besprechungsinhalte gewünscht seien, werden keine Themen vorgebracht.

Die Praxisarbeitsgruppe Cloud der Banken stellt ihre Zusammensetzung vor. Die Arbeitsgruppe bestehe aus vierzehn tätigen Personen. Vertreten seien zentrale IT-Dienstleister, Verbände, sechs Banken sowie deren Unterstützer. Anlass für das Mandat und die Gründung der Arbeitsgruppe sei gewesen, ein gemeinsames und ganzheitliches Verständnis mit der Bankenaufsicht für die praktische Anwendung der gängigen aufsichtsrechtlichen Anforderungen (insbes. MaRisk/BAIT) an Cloud Services (CS) bei den großen Hyperscalern zu entwickeln.

Das erste Vertiefungsthema war der „Umgang mit Zertifikaten der Cloud Service Provider (CSP)“.

Die Aufsicht führt aus, dass sie weder eine generelle Freigabe für die Verwendung von Zertifikaten erteile, noch die Ergebnisse der „Praxisarbeitsgruppe Cloud“ abnehme. Sie könne lediglich Hinweise geben, welche Aussagen und Ergebnisse ihr fraglich erscheinen. Die Möglichkeit der Institute, Zertifikate für die Beurteilung und Kontrolle von Clouddiensten und Clouddienstleistern zu nutzen, sei zwar grundsätzlich gegeben, müsse jedoch im konkreten Einzelfall bewertet werden.

Zertifikate/testate/Prüfberichte
Die Arbeitsgruppe hat zunächst ihre erarbeiteten Ergebnisse vorgestellt.
Begonnen wurde mit einer Darstellung zur Vielzahl der Zertifikate am Markt, Kriterien zu ihrer Verwertbarkeit und einer möglichen Gruppierung von Zertifikaten/ Testaten (Z/T). Die Aufsicht stimmt zu, dass Kriterien für den Anwendungsfall spezifisch zu prüfen seien. Selbst wenn in einer Vorauswahl unterschieden wird, müsse das Institut das Z/T dennoch in Abhängigkeit des individuellen Risikos bewerten und die Frage klären, ob es der Sicherheit der auszulagernden Daten und Prozesse genüge oder ob das Z/T nicht vielmehr nur den Betrieb der Clouddienste selbst betreffe.

Anschließend hat die Arbeitsgruppe einen möglichen Prozess zur Analyse und Verwertung von Z/T im Institut dargestellt, der die Phasen Scoping, Vereinbarung, Analyse, Verwertung umfasst.

Die Aufsicht macht darauf aufmerksam, dass in bestimmten Bereichen eine Cloudnutzung jedoch auch unmöglich sein könne, solange Mechanismen, die eine zuverlässige Einschätzung der CS bzw. CSP ermöglichten, nicht, bzw. noch nicht vorhanden seien.

Darüber hinaus hat die Arbeitsgruppe die Inhalte auf drei konkreten Praxisbeispielen unterschiedlicher Komplexität / Risikogehalt angewendet und eine mögliche Aufgabenteilung der 3 Lines of Defence dargestellt.

Die Aufsicht weist darauf hin, dass die Prüfungspflichten der Internen Revision gemäß MaRisk, einschließlich der in der MaRisk enthaltenen Erleichterungen, davon unberührt blieben.

Diskussionsergebnisse

A. Umgang mit Zertifikaten und Testaten nebst dazu gehörender Prüfberichte

Im Anschluss an den Austausch über den Umgang mit Zertifikaten/Prüfberichten hat sich das Sonderfachgremium auf die folgenden risikoorientiert abzustufenden Lösungsansätze geeinigt.

1. Wenn Zertifikate und Testate nebst dazu gehörender Prüfberichte als maßgeblicher Nachweis für die Überwachung eines CSP herangezogen werden, müssen sie…

   - die für den spezifischen Leistungsbezug des auslagernden Instituts relevanten IKS-Bestandteile des Instituts („Controls“) abdecken,

   - werthaltig sein, das bedeutet, sie müssen bzgl. der Kriterien (Anforderungen an Akkreditierung, Prüforganisation und Prüfer, Umfang und Dokumentation der Prüfungshandlungen, Aktualität, Unabhängigkeit und Eignung des Prüfers etc.) den Anforderungen des auslagernden Instituts genügen,

   - im auslagernden Institut angemessen und nachvollziehbar analysiert, bewertet und verwertet werden (inkl. zusätzlicher Steuerungsmaßnahmen bei GAPs).

2. Für „Standard“-Themen (IKS-Bestandteile mit geringer Komplexität, z.B. Aspekte der physischen Sicherheit wie Löschanlage im Rechenzentrum) kann die Nutzung von Zertifikaten und Testaten nebst dazu gehörender Prüfberichte als alleinige Überwachungshandlung ausreichend sein.

3. Für nicht durch Prüfberichte, Zertifikate und Testate nebst dazu gehörender Prüfberichte abgedeckte IKS-Bestandteile ist im Institut zu prüfen, wie Informationen zu diesen nicht abgedeckten IKS-Bestand- teilen einzuholen sind.

4. Arten und Umfang der ergänzenden Prüfungshandlungen nehmen bei höherer Komplexität sowie höherem Risiko der ausgelagerten Leistung typischerweise zu.

5. Sind in Einzelfällen keine hinreichenden Informationen verfügbar, sind die hieraus resultierenden Risiken vom Institut zu bewerten, in das Risi- komanagement zu überführen und entweder durch das Institut zu miti-gieren, oder zu akzeptieren oder der Cloud-Leistungsbezug ist anzupassen oder einzuschränken.

6. Die Überwachungshandlungen sind durch die 1st und 2nd LoD durchzuführen. Sie können dabei auch Ergebnisse der 3rd LoD berücksichtigen.

Die Aufsicht betont, dass die beschriebenen Lösungsansätze auf alle Z/T angewendet werden sollten und nicht nur auf solche, die „maßgeblich“ (vgl.1.) für die Überwachung eines CSP sind.

B. Bedarf zur Weiterentwicklung von Zertifikaten und Testaten nebst dazu gehörender Prüfberichte

Es besteht das gemeinsame Verständnis, dass es für den vollständigen Nachweis eines funktionierenden und den Anforderungen der Finanzindustrie genügenden IKS für die CSP mittelfristigen Ergänzungs- bzw. Weiterentwicklungsbedarf gibt. Die Zielsetzung sollte insbesondere eine deutliche Verbesserung der Qualität/Werthaltigkeit, (ggfs. branchenübergreifende) Vereinheitlichung und somit Komplexitätsreduzierung sein.

Dies kann als Optionen z. B. die Ergänzung/Entwicklung von „Banken- oder Finanzindustrie-Standards“ für Anforderungen an Zertifikate der CSP, bis hin zu gemeinschaftlich von mehreren Unternehmen der Finanzbranche durchgeführten bzw. beauftragten Zertifizierungen oder die perspektivische direkte Beaufsichtigung (z. B. DORA) umfassen.

Teilnehmer*innen Sonderfachgremium Cloud am 07.10.2021

Behrends, Tino	Verband der Regionen e.V.
Böse, Stefan	DZ Bank AG
Burckhardt, Michael	Commerzbank AG
Dr. Kunze, Christoph	Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V.
Fichelscher, Andreas	KfW Bankengruppe
Gärtner, Heino	NordLB
Gropengiesser, Uwe	Deutsche Bank
Hoenes, Frank	Landesbank Baden-Würtemberg
Hug, Jochen	Verband Deutscher Bürgschaftsbanken e.V.
Kastl, Andreas	Verband der Auslandsbanken
Koen, Oliver	Atruvia AG
Michelsen, Heiko	ING
Muster, Holger	Finanz Informatik GmbH & Co KG
Runkel, Dirk	Bausparkasse Mainz
Saller, Christian	Bayerische Landesbank
Scheidl, Marcus	Bundesverbandes Öffentlicher Banken Deutschlands
Schimm, Berit	Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V.
Schwaab, Philipp	Landesbank Hessen-Thüringen
Somma, Michael	Bankenfachverband e.V.
Steuber, Martin	UniCredit
Trojahn, Frank	Deutscher Sparkassen- und Giroverband e.V.
Wagenknecht, Daniel	KPMG
Weltermann, Christian	Commerzbank AG
Wilop, Karsten	PWC
Wüpper, Martin	Hamburg Commercial Bank

Bretz, Jörg	Deutsche Bundesbank
Dr. Janlewing, Rainer	Deutsche Bundesbank
Dr. Paust, Michael	Deutsche Bundesbank
Englisch, Rainer	Deutsche Bundesbank
Rest, Matthias	Deutsche Bundesbank
Schäfer, Dominik	Deutsche Bundesbank
Dr. Beekmann, Frank	Bundesanstalt für Finanzdienstleistungsaufsicht
Dr. Gampe, Jens	Bundesanstalt für Finanzdienstleistungsaufsicht
Kiefer, Jan	Bundesanstalt für Finanzdienstleistungsaufsicht
Kosche-Steinbrecher, Ira	Bundesanstalt für Finanzdienstleistungsaufsicht
Rebmann, Mark	Bundesanstalt für Finanzdienstleistungsaufsicht
Sämisch, Thorsten	Bundesanstalt für Finanzdienstleistungsaufsicht