ZIIR - Zeitschrift für Informationsrecht

Digitalisierung im Bankwesen im Fokus aufsichtlicher Anforderungen

Aufsätze · Gerald Ganzger , Levente Nagy · ZIIR 2019, 261 · Heft 3 v. 1.9.2019

In einer Welt in der immer mehr Menschen digital bezahlen und Geld transferieren, ist das Thema IT-Sicherheit ein relevantes Thema für das Bankwesen geworden. Die Informationstechnik ist für Kreditinstitute mittlerweile nicht nur mehr Nebenbedingung um Erträge zu generieren, sondern Basisinfrastruktur für sämtliche bankfachlichen sowie auch für alle nichtbankfachlichen Prozesse geworden. Aufgrund der tiefgreifenden Auswirkungen von Digitalisierung auf das Bankwesen mussten sich bereits nationale als auch europäische Aufsichtsbehörden mit den Risiken der innovativen Entwicklungen auseinandersetzen.
Dieser Beitrag beschäftigt sich mit den jüngsten aufsichtlichen Anforderungen an die IT mit einem Fokus auf dem neuesten Leitfaden der österreichischen Finanzmarktaufsichtsbehörde (FMA)[1].
Deskriptoren: Digitalisierung im Bankwesen; Robo-Advisor; IKT-Risiko; Leitfaden für IT-Sicherheit; IT-Strategie; Notfallmanagement; IT-Governance; Schwachstellenmanagement; Benutzerberechtigungsmanagement; E-Geldinstitute Sicherheitsmanagement; Auslagerung.

Normen: § 39 BWG, § 25 BWG, Kreditinstitute-Risikomanagementverordnung - KI-RMV

DOI: https://doi.org/10.33196/ziir201903026101

1. Entwicklung der Anwendung von IT

Im Bankwesen erfolgte eine ausgeprägtere Anwendung von IT zunächst bereichsspezifisch in den kapitalmarktorientierten Kernprozessen. Im Kapitalmarkt wird Informationstechnik nämlich bereits seit Jahrzehnten häufiger und umfänglicher genutzt, da dort seit vielen Jahren große Datenbestände und Algorithmen für Trading verwendet werden.[2]
Mittlerweile entspricht es allerdings auch für die herkömmliche Finanzdienstleistungsbranche der Normalität, wenn kognitive Systeme Berater bei ihrer Arbeit unterstützten.
Es ist sogar auch möglich, dass kognitive Systeme als Robo-Advisors völlig autonom agieren. Via Algorithmen werden über wenige Fragen und ohne menschliche Interaktion Risikobereitschaft, finanzielle Lage und Anlagebedürfnisse des Kunden so ermittelt, dass anschließend komplexe Anlageprodukte oder Anlagestrategien mit verschiedenen Finanzmarktprodukten angeboten werden können.[3] Festzuhalten ist auch, dass Banken ihre IT-Entwicklungsprojekte auch massiv verändert haben: So haben sieben von zehn Banken ihre IT-Entwicklungsprojekte in den vergangenen drei Jahren von klassisch auf agil umgestellt.[4]
Neben den marktdominanten Kreditinstituten tummeln sich vermehrt auch junge, technologieorientierte Startups mit spezifischen Funktionen (Fintechs/Insurtechs/Regtechs/Legaltechs) sowie große, global agierende Technologieunternehmen (Bigtechs) im Wettbewerb um digitale Technologien. Kognitive Systeme, selbstlernende Algorithmen oder Peer-to-Peer-Mechanismen sind Beispiele solcher digitalen Technologien, mit denen bereits in unterschiedlicher Intensität experimentiert wird.[5]

2. Fokus des aufsichtlichen Handelns

Die zunehmende Digitalisierung birgt – neben vielen Vorteilen – neue Gefahren und Risiken, denen sowohl Banken als auch ihre Kunden[6] ausgesetzt sind. Insbesondere die jüngsten Angriffe auf IT-Systeme von Zahlungsdienstleister

haben deutlich gemacht wie verwundbar IT-Infrastrukturen sein können. Diese Verschärfung der Risikolage wurde auch von den relevanten Aufsichtsbehörden erkannt.
So ist die Thematik der IT-Aufsicht mehr und mehr in den Fokus des aufsichtlichen Handelns gerückt.[7] Für die Aufsicht sind mittlerweile alle technischen Mittel eine hohe Relevanz beizumessen, die der Verarbeitung oder Übertragung von Informationen dienen. Dazu gehören die Erhebung, die Erfassung, die Nutzung, die Speicherung, die Übermittlung, die programmgesteuerte Verarbeitung, die interne Darstellung und die Ausgabe von Informationen. Darunter ist auch Informations- und Kommunikationstechnologie zu verstehen. Generell lässt sich festhalten, dass das Ziel der aufsichtlichen Anforderungen ist, sich mit dem IT-Risiko auf allen Ebenen des betreffenden Unternehmens auseinanderzusetzen. Um dies erreichen zu können, müsste das IT-Risikobewusstsein in den Unternehmen insbesondere auf den Führungsebenen geschärft werden.
Neben den „soft laws" der Aufsichtsbehörden haben sich diverse Organisationen mit der Thematik der IT-Sicherheit befasst und etablierte Standards entwickelt auf welche betroffene Unternehmen ebenfalls zurückgreifen können:

- IT Infrastructure Library (ITIL)[8];
- BSI-Grundschutz[9];
- Rahmenwerk Control Objectives for Information and related Technology (CobiT)[10];
- ISO 27001[11];
- Österreichisches Informationssicherheitshandbuch[12].

3. Leitlinien für die Informations- und Kommunikationstechnologie-Risikobewertung
Im Jahr 2018 hat die Europäische Bankaufsichtsbehörde (EBA) umfassende Leitlinien für die Informations- und Kommunikationstechnologie (IKT)-Risikobewertung erlassen. Die Leitlinien legten fest welche Aufsichtspraktiken hinsichtlich der IKT-Risikobewertung nach Ansicht der EBA als angemessen zu betrachten sind.
IKT-Risiko ist nach Ansicht der EBA als „*das bestehende oder künftige Risiko von Verlusten aufgrund der Unzweckmäßigkeit oder des Versagens der Hard- und Software technischer Infrastrukturen, welche die Verfügbarkeit, Integrität, Zugänglichkeit und Sicherheit dieser Infrastrukturen oder von Daten beeinträchtigen können*"[13], zu definieren.
Das IT-Risiko erfasst daher auch das Risiko aus IT-Dienstleistungen, IT-Verfügbarkeit und -Kontinuität, IT-Sicherheit, IT-Änderungen, IT-Datenintegrität und IT-Auslagerungen.

4. Umgang mit dem IKT-Risiko in Österreich
Auch in Österreich messen die Aufsichtsbehörden dem Umgang mit dem IKT-Risiko eine enorme Relevanz bei. So wird der Umgang des jeweiligen Bankeninstituts mit dem IKT-Risiko im Rahmen des jährlichen aufsichtlichen Überprüfungs- und Bewertungsprozesses (Supervisory Review and Evaluation Process, SREP) einer Beurteilung unterzogen. Dabei wird insbesondere bewertet, ob der allgemeine Governance-Rahmen und der interne Kontrollrahmen des jeweiligen Instituts die IKT-Systeme und die damit verbundenen Risiken ordnungsgemäß abdecken und ob das Leitungsgremium diese Aspekte angemessen angeht und verwaltet. Dabei konzentriert sich die Bewertung auf folgende Elemente:

- IKT-Strategie – ob das Institut über eine IKT-Strategie verfügt die hinreichend geregelt ist und mit der Geschäftsstrategie des Instituts in Einklang steht;
- interne Governance – ob die internen Governance-Regelungen des Instituts in Bezug auf die IKT-Systeme des Instituts angemessen sind; und
- IKT-Risiko innerhalb des Risikomanagementrahmens – ob der Risikomanagementrahmen und der interne Kontrollrahmen des Instituts die IKT-Systeme des Instituts angemessen sichern.

Die Überprüfung erfolgt durch die OeNB in Zusammenarbeit mit FMA und EZB. Das Ergebnis der Analyse wird dem Proportionalitätsprinzip folgend unter Berücksichtigung der Größe und Komplexität der jeweiligen Bank zu einer Gesamtbeurteilung zusammengeführt, welche die Grundlage für aufsichtliche Maßnahmen durch die zuständigen Behörden darstellt.

5. FMA: Leitfaden für IT-Sicherheit

Entsprechend dem Leitfaden der EBA erließ die österreichische Finanzmarktaufsichtsbehörde (FMA) im Jahr 2018 einen Leitfaden für IT-Sicherheit. Der Leitfaden

richtet sich primär an Kreditinstitute im Sinne des § 1 Abs 1 BWG, ist jedoch auch für Zahlungsinstitute, E-Geldinstitute und Sonderkreditinstitute relevant. Mit diesem Leitfaden hat die FMA versucht den Instituten auf der Grundlage von § 39 Abs 2b Z 5 und Abs 4 BWG[14] iVm § 11 KI-RMV (operationelles Risiko) einen Überblick über Ausgestaltung, Anforderungen und Vorkehrungen betreffend den Umgang mit IKT-Risiko als Orientierungshilfe zur Verfügung zu stellen.[15] Der Leitfaden weist keine normative Wirkung auf.[16]

Die in dem Leitfaden der FMA enthaltenen Anforderungen bieten konkrete Anhaltspunkte dafür welche Methoden, Systeme und Prozesse in Bezug auf die IT-Sicherheit unter dem Grundsatz der Proportionalität angemessen sind.

Adressaten dieser Sorgfaltspflichten ist die Geschäftsleitung und daher insbesondere diejenigen natürlichen Personen, die nach dem Gesetz oder der Satzung zur Führung der Geschäfte insbesondere zur Festlegung der Strategie, Ziele und der Gesamtpolitik, sowie zur organschaftlichen Vertretung des Kredit- oder Finanzinstitutes nach außen vorgesehen sind.[17]

6. IT-Strategie

An erster Stelle ist die von der FMA betonte Relevanz einer funktionierenden IT-Strategie hervorzuheben.[18] Hierbei steht die Anforderung im Vordergrund, dass sich die Geschäftsleitung regelmäßig mit den strategischen Implikationen der verschiedenen Aspekte der IT für die Geschäftsstrategie auseinandersetzt.

Als Beginn müssten Geschäftsleiter von Instituten eine mit der Geschäftsstrategie übereinstimmenden IT-Strategie entwickeln, welche allerdings auch die Art, den Umfang und die Komplexität der IT-Tätigkeiten mitberücksichtigen sollte. Bei der Erstellung der jeweiligen IT-Strategie ist darauf Bedacht zu nehmen, dass die IT-Strategie primär das Geschäftsmodell zu unterstützen hat.

Inhaltlich müssen in der IT-Strategie die vorgesehene strategische Entwicklung der IT, der IT-Aufbau- und Ablauforganisation inklusive der dazugehörigen Prozesse festgelegt werden. In der Praxis sollte eine adäquate IT-Strategie folgende Punkte abdecken:

- Entwicklung einer IT-Zielarchitektur mit einem Überblick über die Anwendungslandschaft;
- Festlegung von Zuständigkeiten, Rollen und Aufgaben für einen systemischen Informationssicherheitsprozess;

- Berücksichtigung von Auslagerungsaspekten;
- Festlegung eines Notfallmanagements;
- Aussagen zu den in den Fachbereichen selbst betriebenen bzw. entwickelten IT-Systemen (Hard- und Software) und
- Festlegung der Grundsätze eines Lebenszyklus-Managements von Hard- und Software.[19]

Nachdem die IT-Strategie verfasst wurde, ist darauf Bedacht zu nehmen, dass diese der Genehmigung und Aufsicht durch die Geschäftsführung unterliegt. Es empfiehlt sich daher, dass die Geschäftsführung die IT-Strategie in regelmäßigen Abständen sowie anlassbezogen auf ihre Aktualität überprüft und gegebenenfalls (orientiert an den Geschäftszielen) anpasst, wobei im Falle einer Änderung der Geschäftsstrategie stets die IT-Strategie überarbeitet werden muss.[20]

7. IT-Governance

Die Geschäftsleitung hat auch sicherzustellen, dass angemessene interne Governance-Regelungen in Bezug auf die IKT-Systeme des Instituts bestehen. Zweck der IT-Governance sollte die Steuerung und Überwachung des Betriebs und der Weiterentwicklung der im Institut verwendeten IT-Systeme samt der dazugehörigen IT-Prozesse sein.
Nach Meinung der FMA setzt sich eine angemessene IT-Governance ua aus folgenden wesentlichen Elementen zusammen:

- Governance-Prozesse (zB Organisationsvorgaben, Prozessstrukturen, Fortschritts- und Haushaltsüberwachung und -berichterstattung) und
- relevante Stellen (zB ein Projektmanagementbüro, eine IKT-Lenkungsgruppe oder ähnliches).

Bei der Festsetzung der internen IT-Governance ist darauf Bedacht zu nehmen, dass eine solide und transparente Organisationsstruktur mit klaren Zuständigkeiten in Bezug auf die IKT, einschließlich des Leistungsorgans und seiner Ausschüsse geschaffen wird.
Insbesondere soll sichergestellt werden, dass die wichtigen für IKT verantwortlichen Personen (zB Chief Information Officer „CIO", Chief Operating Officer „COO" oder eine vergleichbare Rolle) sinngemäß über eine angemessene indirekte oder direkte Berichtslinie zu dem

Leitungsorgan verfügen, um sicherzustellen, dass wichtige IKT-bezogene Informationen oder Probleme ordnungsgemäß gemeldet, erörtert und auf Ebene des Leitungsorgans entschieden werden.
Schließlich ist darauf hinzuweisen, dass die Geschäftsleitung für die Umsetzung und die Einhaltung der Regelungen zur IT-Governance institutsintern und gegenüber Dritten verantwortlich ist.

8. IKT-Risiko innerhalb des Risikomanagementrahmens

Neben einer adäquaten IT-Strategie sowie einer adäquaten IT-Governance hat die Geschäftsleitung auch sicherzustellen, dass innerhalb des Bankinstitutes ein angemessener Risikomanagementrahmen vorhanden ist. Der Risikomanagementrahmen hat sich aus folgenden Elementen zusammenzusetzen:

- Informationsrisikomanagement;
- Sicherheitsmanagement;
- Benutzerberechtigungsmanagement;
- Schwachstellenmanagement;

- Notfallmanagement.

Um ein funktionierendes Management sicherzustellen haben Bankinstitute die Funktion eines Informationssicherheitsbeauftragten einzurichten. Dessen zentrale Aufgabe ist die Verantwortung aller Belange der Informationssicherheit innerhalb des Instituts gegenüber Dritten. Zudem unterstützt der Informationssicherheitsbeauftragte auch die Geschäftsleitung bei der Festlegung und Anpassung der Informationssicherheitsrichtlinie und berichtet dieser regelmäßig. Darüber hinaus obliegen ihm die Informationssicherheit betreffend die Durchführung von Schulungsmaßnahmen und die Setzung von Sensibilisierungsmaßnahmen im Institut.[21]
Wichtig ist, dass die Funktion des Informationssicherheitsbeauftragten organisatorisch und prozessual unabhängig ausgestaltet sein muss.

9. Informationsrisikomanagement
Durch ein adäquates Informationsrisikomanagement soll gewährleistet werden, dass die Informationsverarbeitung und Weitergabe innerhalb des Bankinstituts durch angemessene IT-Systeme (Hardware- und Softwarekomponenten) und Prozesse unterstützt werden.[22]
Die Bank hat dabei den Schutzbedarf der relevanten Daten bzw. Informationen zu ermitteln. Auf dieser Grundlage hat dann das Management Soll-Maßnahmen festzulegen und diese mit den wirksam umgesetzten Ist-Maßnahmen zu vergleichen.

10. Sicherheitsmanagement
Banken müssen über einen wirksamen Rahmen zur Ermittlung, Verständnis, Messung und Minderung des IKT-Sicherheitsrisikos verfügen. Dies kann insbesondere durch die Etablierung eines funktionierenden Informationssicherheitsmanagements (zB In-formationssicherheitsrichtlinie), welches Vorgaben zur Informationssicherheit festlegt sowie entsprechende Prozesse definiert und deren Umsetzung steuert, erreicht werden.[23]
Die Informationssicherheitsrichtlinie soll als Ausgangspunkt für konkretisierende Richtlinien und Prozesse für Teilbereiche, wie bspw Netzwerksicherheit, Kryptografie, Authentisierung, Protokollierung, etc dienen.

11. Benutzerberechtigungsmanagement
Neben dem umfassenden Sicherheitsmanagement haben Kreditinstitute auch ein Benutzerberechtigungsmanagement einzurichten, welches alle Prozesse die der Autorisierung eines Anwenders hinsichtlich Berechtigungen auf IT-Ressourcen (Einrichtung, Zugriff und Nutzung, Bearbeitung, Deaktivierung, Löschung) dienen, umfasst. Das Institut hat über ein dokumentiertes Berechtigungskonzept bzw über Benutzerberechtigungsprozesse zu verfügen.
Berechtigungen zum Zugriff auf genau definierte Teile von IT-Systemen sind notwendig, damit bestimmte Aufgaben erfüllt werden können. Sie sind aber auch ein zentraler Baustein bei der Schaffung von IT-Sicherheit. Die Vergabekriterien von Berechtigungen berücksichtigen dabei den Grundsatz der minimalen Rechtevergabe bzw das Need-to-know-Prinzip und sind nachvollziehbar sowie konsistent.

12. Schwachstellenmanagement
Um Schwachstellen rechtzeitigen identifizieren und beseitigen zu können haben Kreditinstitute als integraler Bestandteil der Computer- und Netzsicherheit auch ein Schwachstellenmanagement einzurichten.[24]
Da ein Virenschutzprogramm zum Schutz vor Schadenssoftware heutzutage nicht mehr genügen, müssten Kreditinsitute zusätzliche Schutzmaßnahmen treffen. Dazu gehören bspw:

- Regelmäßige Sicherheitsupdates;
- Funktionierende Firewalls;
- Datensicherung (Backup und Restore).

13. Notfallmanagement

Banken haben auch ein adäquates Notfallmanagement vorzuweisen. Ein adäquates Notfallmanagement umfasst nach Vorgaben der FMA Strategien, Pläne und Handlungen zur Notfallvorsorge, Notfallbewältigung und Notfallnachsorge um kritische Prozesse und Ressourcen bei unvorhergesehenen Unterbrechungen präventiv zu schützen und rasch wiederherzustellen.[25]
Das Notfallmanagement hat dabei auf der Analyse der Bedrohungsanfälligkeiten von Geschäftsprozessen und Ressourcen zu basieren.
Da das Notfallmanagement auch die präventive Notfallvorsorge und die Notfallbewältigung zu umfassen hat, sind auch präventive Maßnahmen, Sicherungs- und Wiederherstellungsverfahren, Störfallmanagement- und Eskalationsprozesse, Kapazitätsplanungslösungen in Richtlinien festzulegen.
Um ein gut funktionierendes Notfallmanagement gewährleisten zu können, müssen in regelmäßigen Abständen jeweils dokumentierende Notfallübungen – gegebenenfalls gemeinsam mit bedeutenden IT-Dienstleistern – durchgeführt werden. Festgestellte Schwächen und Mängel müssen anschließend beseitigt werden.

14. Auslagerung

Mit 03.01.2018 ist § 25 BWG in Kraft getreten wodurch eine nationale Rechtsgrundlage für Auslagerungen von Kreditinstituten und betrieblichen Vorsorgekassen eingeführt wurde.[26] Zu verstehen ist die Auslagerung als die Verwendung eines Dritten (des „Outsourcing-Dienstleisters") durch einen konzessionierten Rechtsträger zur Durchführung von Tätigkeiten, die normalerweise vom konzessionierten Rechtsträger jetzt oder hinkünftig unternommen würden.[27]

Bei Auslagerungen nach dem BWG ist darauf Bedacht zu nehmen, dass nur wesentliche bankbetriebliche Prozesse, Dienstleistungen oder Tätigkeiten vom Begriff der Auslagerung iSv § 25 BWG erfasst sind. Ein bankbetrieblicher Prozess gilt als wesentlich, wenn deren unzureichende oder unterlassene Wahrnehmung die kontinuierliche Einhaltung der gesetzlichen Verpflichtungen des Kreditinstituts, seine Solvabilität, Liquidität, die Solidität oder Kontinuität der betriebenen Bankgeschäfte beeinträchtigen würde. Darunter werden in der Regel beispielsweise die Auslagerung der Internen Revision, des Meldewesens oder des Rechnungswesens fallen.

Liegt eine iSd § 25 BWG relevante IT-Auslagerung vor, hat das jeweilige Bankinstitut das Auslagerungsvorhaben gemäß § 25 Abs 5 BWG der FMA anzuzeigen. Die Anzeige ist noch vor dem geplanten Vertragsabschluss zu erstatten. Die Anzeige wird anschließend von der FMA geprüft.
Unbeschadet der Wesentlichkeit einer Auslagerung haben Kreditinstitute hinsichtlich Auslagerungen an Cloud-Anbieter die Empfehlungen der EBA zur Auslagerung an Cloud-Anbieter zu beachten.[28]
Nicht unter den Begriff der Auslagerung fällt der Kauf von standardisierten Softwareprodukten inklusive Wartungsverträgen (sofern es sich nicht um eine Cloud-Lösung handelt).

Resümee

Neben den ursprünglichen Risiken strategischer Natur bringt die Digitalisierung auch enorme Cyber- und IT-Risiken für Kreditinstitute mit sich, die bis dato noch nicht im Fokus der Geschäftsleitung standen.

Mit dem Erlass eines präzisen Leitfadens hat die FMA eine angemessene Orientierungshilfe für das Bankwesen beim Umgang mit IKT-Risiken geschaffen. Die Aufsichtsbehörden haben hierbei allerdings sehr vorsichtig zu agieren. Sie müssen nämlich nicht nur die Risiken hervorheben, sondern auch die mit der Digitalisierung entstandenen Chancen sehen.
Die Aufsichtsbehörden haben jedoch darauf zu achten, dass eine Überregulierung die Fortentwicklung der Digitalisierung verhindern kann. Daher wäre es weiterhin notwendig, die weitere Entwicklung aufsichtslicher Anforderungen sehr praxisnah zu gestalten. Der derzeitige Leitfaden der FMA stellt hierfür eine plausible Grundlage dar.

Korrespondenz: Dr. Gerald Ganzger, ganzger@lansky.at ;

Dr. Levente Nagy, nagy@lansky.at .

---

[1] *FMA*, Leitfaden IKT-Sicherheit in Kreditinstituten https://www.fma.gv.at/download.php?d=3370 , abgerufen am 25.6.2019.

[2] *Bafin*, big Data trifft auf künstliche Intelligenz (2018) 11 ff.

[3] *Deutsche Bank Research*, Kommentar – Start-ups beflügeln Märkte mit digitalen Technologien (Fintech #7), https://www.dbresearch.de/PROD/RPS_DE-PROD/PROD0000000000447700/Start-ups_beflügeln_Märkte_mit_digitalen_Technolog.PDF , abgerufen am 23.6.2019.

[4] *IT Finanzmagazin*, 70 Prozent der Banken und Versicherer entwickeln mit agilen IT-Methoden wie Scrum oder Kanban, https://www.it-finanzmagazin.de/70-prozent-der-banken-und-versicherer-entwickeln-mit-agilen-it-methoden-wie-scrum-oder-kanban-35438/ , abgerufen am 26.6.2019.

[5] Siehe dazu auch, *Deutsche Bank Research*, Kommentar – Start-ups beflügeln Märkte mit digitalen Technologien (Fintech #7), https://www.dbresearch.de/PROD/RPS_DE-PROD/PROD0000000000447700/Start-ups_beflügeln_Märkte_mit_digitalen_Technolog.PDF , abgerufen am 23.6.2019.

[6] *Stollarz*, Digitalisierung in der Finanzbranche ist kein Selbstzweck, in Börsen-Zeitung online, 28.4.2018, Seite B5.

[7] *Bafin*, Digitalisierung und Informationssicherheit im Finanz- und Versicherungswesen im Fokus aufsichtlicher Anforderungen https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/BaFinPerspektiven/2018/bp_18-1_Beitrag_Gampe.html (abgerufen am 25.6.2019).

[8] https://www.etc.at/itil/

[9] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

[10] http://www.isaca.org/cobit/pages/default.aspx

[11] https://www.iso.org/standard/54534.html

[12] https://www.sicherheitshandbuch.gv.at/

[13] *EBA*, Leitlinien zu gemeinsamen Verfahren und Methoden für den aufsichtlichen Überprüfungs- und Bewertungsprozess, https://www.fma.gv.at/download.php?d=668 (abgerufen am 25.6.2019).

[14] *Kammel* in Laurer/M. Schütz/Kammel/Ratka, BWG⁴ § 39 (Stand 1.5.2018, rdb.at) Rz 34 ff.

[15] Siehe dazu, *FMA*, Leitfaden IKT-Sicherheit in Kreditinstituten (2018).

[16] Vgl auch, *Studer*, Aufsichtsrecht und Risikomanagement (ÖBA 2018), 310 ff.

[17] Siehe dazu, *Laurer/Kammel* in Laurer/M. Schütz/Kammel/Ratka, BWG⁴ § 2 (Stand 1.1.2017, rdb.at) Rz 1.

[18] *FMA*, Leitfaden IKT-Sicherheit in Kreditinstituten (2018) 6 ff.

[19] *FMA*, Leitfaden IKT-Sicherheit in Kreditinstituten (2018) 7.

[20] *FMA*, Leitfaden IKT-Sicherheit in Kreditinstituten (2018) 7.

[21] *FMA*, Leitfaden IKT-Sicherheit in Kreditinstituten (2018) 10.

[22] *FMA*, Leitfaden IKT-Sicherheit in Kreditinstituten (2018) 9 ff.

[23] *FMA*, Leitfaden IKT-Sicherheit in Kreditinstituten (2018) 11 ff.

[24] *FMA*, Leitfaden IKT-Sicherheit in Kreditinstituten (2018) 12 ff.

[25] *FMA*, Leitfaden IKT-Sicherheit in Kreditinstituten (2018) 18.

[26] Siehe dazu auch, *Napokoj* in Laurer/M. Schütz/Kammel/Ratka, BWG⁴ § 25 (Stand 1.1.2019, rdb.at) Rz 1 ff.

[27] *CEBS*, Guidelines on outsourcing, https://eba.europa.eu/documents/10180/104404/GL02OutsourcingGuidelines.pdf.pdf (abgerufen a, 25.6.2019).

[28] *EBA*, Empfehlungen zur Auslagerung an Cloud-Anbieter, https://eba.europa.eu/documents/10180/2170125/Recommendations_on_Cloud_Outsourcing_(EBA-Rec-2017-03)_DE.pdf/afd89dc3-45a7-4054-a642-d03b4e35fa1f (abgerufen am 25.6.2019).