Digitale Risiken im Bankensektor

Die deutschen Banken sind durch die zunehmende Digitalisierung der Arbeits- und Lebenswelt herausgefordert. Der dadurch intensivierte Wettbewerb bei Finanzdienstleistungen sowie die Erwartungen der Kunden üben seit einigen Jahren starken Anpassungs- und Veränderungsdruck aus. Neue Verfahren wie Künstliche Intelligenz sowie die breite Nutzung von skalierbaren Services in der Cloud beschleunigen die Digitalisierung. Die schon bestehende Unterstützung bankfachlicher Verfahren durch Informationstechnologie wird sich dadurch weiter intensivieren.

Bei der digitalen Transformation darf die Sicherheit nicht aus den Augen verloren werden, zumal Banken immer mehr in den Fokus von professionellen Angreifern rücken. Banken müssen sicherstellen, dass die Daten ihrer Kunden jederzeit verfügbar, vor ungewollten Veränderungen gesichert und vor unbefugter Einsichtnahme geschützt sind. Um gegen diese digitalen Risiken gewappnet zu sein, reicht Technik aber nicht aus. Die menschliche Komponente und technisch-organisatorische Maßnahmen sowie gut strukturierte, wirksame und ineinandergreifende Prozesse sind die entscheidenden Erfolgsfaktoren.

Damit die nötigen Freiräume bei der Implementierung von Maßnahmen gewahrt bleiben, setzt die Bankenaufsicht auf den bewährten prinzipien- und prozessorientierten Regulierungs- und Überwachungsansatz. Die Erwartungshaltung wird über die Rundschreiben MaRisk und BAIT technologieneutral weiter konkretisiert. Somit können auch die auf aktuellen und künftigen technologischen Entwicklungen wie Cloud-Computing und Künstlicher Intelligenz aufbauenden bankinternen Prozesse effektiv beaufsichtigt werden.

Über den bankaufsichtlichen Überprüfungs- und Beurteilungsprozesses (Supervisory Review and Evaluation Process: SREP), insbesondere durch Prüfungen in den Banken, werden neben finanziellen Risiken auch nichtfinanzielle Risiken, wie beispielsweise digitale Risiken, von der Bundesbank beurteilt. Obwohl stetige Verbesserungen bei den Risikomanagementprozessen beobachtbar sind, werden aber auch immer wieder grundsätzliche Schwachstellen und Verbesserungsbedarf im Umgang mit digitalen Risiken, besonders beim Management der Informationsrisiken, in der Informationssicherheit und beim Auslagerungsmanagement festgestellt und in den bankaufsichtlichen Fokus genommen.

Die Digitalisierung wird die gesellschaftliche und wirtschaftliche Entwicklung weiter prägen und die Geschwindigkeit des technologischen Wandels insbesondere im Bankensektor wird hoch bleiben. Die Bundesbank steht dem technologischen Fortschritt in den Banken seit jeher positiv gegenüber, denn digitale Innovation stärkt die deutschen Banken, indem diese wettbewerbsfähiger, rentabler und damit auch stabiler und widerstandsfähiger werden. Der langfristige Erfolg der Institute hängt allerdings stark von der stetigen und geordneten Nutzung innovativer Technologien ab. Die Bundesbank wird sich global und auf europäischer Ebene weiterhin für eine prinzipienorientierte und technologieneutrale Regulierung digitaler Risiken einsetzen. Technischer Fortschritt soll ebenso unterstützt werden wie eine proportionale und eigenverantwortliche Umsetzung in den Instituten. Nur der eigenständige, souveräne und ausgewogene Umgang der Institute mit den Chancen und Risiken der Digitalisierung kann die Funktionsfähigkeit des Finanzsystems auf Dauer sicherstellen.

Digitalisierung verändert das Bankgeschäft

Informationstechnologie bestimmt das Bankgeschäft

Die Arbeitsweise von Banken wurde schon immer stark durch die zur Verfügung stehenden Technologien geprägt. Eine funktionierende und moderne Informationstechnologie (IT) ist heutzutage Voraussetzung für einen immer größeren Anteil von Finanzdienstleistungen und -produkten.

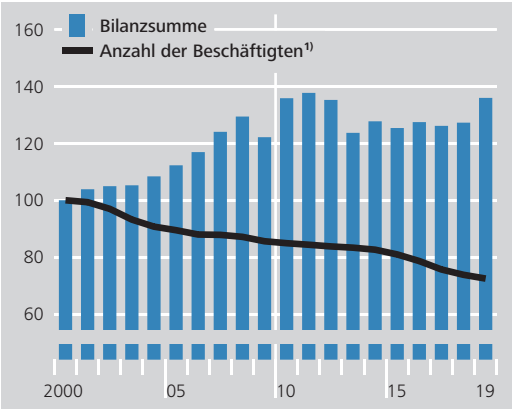
So sank die Anzahl der Beschäftigten in der deutschen Kreditwirtschaft in den letzten beiden Jahrzehnten kontinuierlich, während die Bilanzsumme in der gleichen Zeit um circa 50 % zugenommen hat. Diesen Produktivitätsschub hat nicht zuletzt auch die verstärkte Nutzung von IT ermöglicht. Ein Bankbetrieb ohne IT ist heute nicht mehr vorstellbar.

Digitalisierung schafft neue Möglichkeiten …

Die in den letzten Jahrzehnten stark angestiegene Leistungsfähigkeit und Vernetzung der IT ermöglicht die zeitnahe Übertragung und Verarbeitung enormer Datenmengen. Verfahren wie Künstliche Intelligenz und Maschinelles Lernen nutzen diese, um hochautomatisiert immer anspruchsvollere Prozesse, Aufgaben und Analysen eigenständig durchzuführen. Zudem werden mittels agiler Methoden, unter Nutzung ihres iterativen und inkrementellen Ansatzes, stetig neue Anwendungen entwickelt. Diese organisatorischen und technischen Innovationen verändern nicht nur die Erwartungshaltung der Bankkunden, sondern auch die Art und Weise, wie Finanzdienstleistungen erbracht und angeboten werden, nachhaltig.

Bilanzsummen und Beschäftigte im deutschen Kreditgewerbe

2000 = 100



1 Quelle: Statista.
Deutsche Bundesbank

Mit der Digitalisierung geht zudem eine vorher nicht mögliche Arbeitsteilung einher. Institute können heute mehr denn je entscheiden, ob sie Dienstleistungen noch selbst erbringen oder von Dritten zukaufen. Beispielsweise müssen bankfachliche Anwendungen bis hin zu Kernbankensystemen nicht mehr von den Instituten selbst entwickelt werden, sondern können von Dritten bezogen und sogar auf deren IT-Infrastruktur betrieben werden. So offerieren global tätige Anbieter einen flexiblen, schnellen und unkomplizierten Zugang zu beinahe unbegrenzt anpassbaren Computerressourcen (siehe Erläuterungen auf S. 55 ff.).

… und geht mit stärkerer Arbeitsteilung einher

Gleichzeitig übt das intensive Wettbewerbsumfeld seit einigen Jahren starken Veränderungsdruck auf die Institute und somit auf deren Geschäftsmodelle aus. Durch die weitere Transformation der Betriebsprozesse sowie deren Auslagerung erhoffen sich Institute vor allem kürzere Bereitstellungszeiten, bessere Servicequalität sowie geringere Betriebskosten.

Anpassungsdruck auf Institute steigt …

Die Corona-Pandemie hat den Trend zur Digitalisierung nochmals deutlich beschleunigt. So mussten Kunden seit mehr als einem Jahr verstärkt über digitale Kanäle mit Dienstleistungen versorgt werden. Gleichzeitig arbeitete eine bislang nicht gekannte Anzahl von Mitarbeitenden von Zuhause aus. Um dies zu ermöglichen, waren die Institute gezwungen, verstärkt in neue Soft- und Hardware zu investieren und vormals analoge Prozesse zu digitalisieren.

… nicht zuletzt durch Corona-Pandemie

Die Bundesbank steht technologischem Fortschritt in den Banken seit jeher positiv gegenüber. Das gilt auch für die Digitalisierung. Denn digitale Innovation stärkt die deutschen Banken, macht sie wettbewerbsfähiger, rentabler und damit auch stabiler und widerstandsfähiger. In der Bundesbank selbst werden zahl-

Die Bundesbank fördert digitale Innovation mit vielfältigen Initiativen, …

Cloud-Computing

Seit einigen Jahren kann ein zunehmender Trend zu Auslagerungen von Informationstechnologie (IT)-Prozessen beobachtet werden. Dieser Trend wirkt sich positiv auf die Digitalisierung in der Finanzbranche aus und ist mit dem Markteintritt neuer, spezialisierter Dienstleister und Technologien verbunden. An Cloud-Computing lässt sich exemplarisch illustrieren, vor welche neuen Aufgaben die Digitalisierung Banken, Aufsicht und Dienstleister stellt und wie diese gelöst werden können.

Bei einer Inanspruchnahme von IT-Dienstleistungen Dritter handelt es sich in der Regel um eine Auslagerung, wenn diese im Zusammenhang mit der Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutsspezifischen Dienstleistungen beauftragt werden.

Die gesetzlichen Anforderungen an die Risikosteuerung von Auslagerungen und sonstigem Fremdbezug von IT-Dienstleistungen durch die Institute sind in § 25a und § 25b KWG festgeschrieben und wurden durch die BaFin-Rundschreiben Mindestanforderungen an das Risikomanagement (MaRisk) und Bankaufsichtliche Anforderungen an die IT (BAIT) konkretisiert.

Cloud-Auslagerungen

Kürzere Technologiezyklen, wachsender Kostendruck und Spezialisierung sind Gründe für Institute, IT-Aktivitäten und IT-Prozesse insbesondere an Anbieter von Cloud-Lösungen auszulagern. Zudem bieten Cloud-Lösungen auch kleineren Instituten einen effizienten Zugang zu modernen Technologien wie Künstlicher Intelligenz und Maschinellem Lernen.

Die US-amerikanische Standardisierungsstelle NIST (National Institute of Standards and Technology) definiert Cloud-Computing als „ein Modell, das es erlaubt, bei Bedarf jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können.“[1)]

Cloud-Computing bietet standardisierte IT-Dienstleistungen und ermöglicht so eine größtmögliche Automation bei deren Bereitstellung. Kunden können IT-Ressourcen flexibel nach Bedarf nutzen und skalieren, wodurch sich die Institute auch effizientere Kostenstrukturen erhoffen. Institute streben neben einer größeren Flexibilität zudem einen flexibleren Bezug sowie eine Verbesserung der Verfügbarkeit und der Leistungsfähigkeit gegenüber den eigenen, meist lange gewachsenen IT-Infrastrukturen an.

Verglichen mit dem Jahr 2018, in dem sich noch 91 % der Institute für einen Eigenbetrieb ihrer IT-Infrastruktur entschieden, greifen laut einer Studie der Wirtschaftsprüfungsgesellschaft PwC mittlerweile immer mehr Institute auf IT-Dienstleistungen von Drittanbietern zurück.[2)] Dabei dominieren wenige große Unternehmen den Markt; sie teilen fast 60 %[3)] des weltweiten Angebots von Cloud-Computing-Dienstleistungen unter sich auf.

---

1 Siehe: Bundesamt für Sicherheit in der Informationstechnik (2021).
2 Siehe: PwC (2021).
3 Vgl.: statista (2021).

Auslagerungen an Cloud-Anbieter unterliegen generell den gleichen Anforderungen an Auslagerungsmanagement und Dienstleistersteuerung wie Auslagerungen an andere (IT-)Dienstleister. Mit der Orientierungshilfe zu Auslagerungen an Cloud-Anbieter[4] haben die Bundesanstalt für Finanzdienstleistungsaufsicht und die Bundesbank ihre gemeinsame Einschätzung zur Auslagerung an Cloud-Anbieter dargelegt.

Risiken, Herausforderungen und aktuelle Entwicklungen

Auch bei Auslagerungen an Cloud-Computing-Anbieter müssen Institute Prozesse zur Steuerung von Risiken etablieren, die durch die Unangemessenheit oder das Versagen von internen Verfahren, Menschen und Systemen oder durch externe Ereignisse verursacht werden, einschließlich der Rechtsrisiken (operationelles Risiko).

Sofern ein Institut Cloud-Lösungen nutzen möchte, muss es die Auswirkungen von Cloud-Computing bereits in seinem Strategieprozess berücksichtigen. So bedingt ein Wechsel auf Cloud-Lösungen meist auch eine vorherige Standardisierung der IT-Landschaft und die Anpassung interner Prozesse.

Aus Sicht der Bundesbank, aber auch aus Sicht der Risikomanagement- und Kontrolleinheiten der Institute ergeben sich bei Auslagerungen an Cloud-Anbieter besondere Herausforderungen hinsichtlich der Überwachung und Steuerung der Auslagerungen und des Dienstleisters. Dies resultiert insbesondere aus der Größe und Komplexität der Organisation und der eingesetzten Technologie der großen Cloud-Anbieter.

Bei der Nutzung von Cloud-Computing besteht das Risiko, dass sich ein Institut aufgrund rechtlicher, organisatorischer oder technischer Aspekte sehr stark an einen Anbieter bindet und nur unter großen Anstrengungen zu einem anderen Anbieter wechseln kann (sog. Vendor Lock-In). Hier erwartet die Aufsicht, dass sich die Institute schon vor Vertragsabschluss mit den Risiken auseinandersetzen und mögliche Alternativen analysieren.

Zudem stellt die eingeschränkte Verhandlungsmacht gegenüber den international und intersektoral tätigen Cloud-Anbietern eine weitere Herausforderung für die Institute dar. Gleichermaßen sehen sich Cloud-Anbieter mit einer Vielzahl im Grunde ähnlicher Anforderungen aus dem Finanz- und Bankensektor konfrontiert.

Die Interne Revision eines Instituts hat risikoorientiert und prozessunabhängig die Wirksamkeit und Angemessenheit des Risikomanagements und des internen Kontrollsystems sowie die Ordnungsmäßigkeit grundsätzlich aller Aktivitäten und Prozesse zu prüfen und zu beurteilen, auch wenn diese ausgelagert sind. Dies ist wegen der Größe und Komplexität der Cloud-Anbieter für einzelne Institute allein eine kaum zu lösende Aufgabe. Dadurch kann es zu Hindernissen bei der Durchführung von Revisionsaktivitäten kommen.

Institute nutzen daher zunehmend den von der Aufsicht bereits in den Mindestanforderungen an das Risikomanagement (MaRisk) vorgesehenen Ansatz der Sammelprüfung (Pooled Audits). Um Know-how zu bündeln und gemeinsame Sachverhalte ressourceneffizient zu erheben, führen dabei die Revisionen mehrerer Institute gemeinsam die Vor-Ort-Prüfungen bei Cloud-Anbietern durch.

4 Vgl.: Bundesanstalt für Finanzdienstleistungsaufsicht (2018).

Auch weiterhin müssen die Kompetenzen des Instituts in der laufenden Vertragsüberwachung, beim Risikomanagement sowie in der Internen Revision mit der IT- und Auslagerungsdynamik Schritt halten. Grundlegend hierfür sind auch Strukturen, Prozesse und Werkzeuge des Cloud-Anbieters, die für Transparenz beispielsweise bei Sicherheitsvorfällen, dem Umsetzungsstand risikoreduzierender Maßnahmen sowie über Test- und Revisionsergebnisse sorgen.

Für die Aufsicht wird es zudem zunehmend wichtiger, die Abhängigkeiten der Institute von IT-Dienstleistungen zu analysieren. Konzentrationsrisiken könnten zu einem systemischen Risiko führen. Die Leitlinien zu Auslagerungen der Europäischen Bankenaufsichtsbehörde, welche aktuell im Gesetz über das Kreditwesen und in entsprechenden Rechtsverordnungen sowie den MaRisk umgesetzt werden, adressieren das unter anderem durch neue Anforderungen an ein Auslagerungsregister in den Instituten und neue Meldeanforderungen von Auslagerungsinformationen an die Aufsicht.

reiche Initiativen ergriffen, um mittels digitaler Technologien den Stabilitätsauftrag noch besser erfüllen zu können, auch in der Bankenaufsicht.

… vernetzt sich intern und in der Zentralbankgemeinschaft …

Bei der digitalen Innovation geht es nicht in erster Linie um die Technologie an sich, sondern vor allem darum, sie sinnvoll einzusetzen. Daher hat die Bundesbank eine gemeinsame Eurosystem-interne Plattform zur fachbereichsübergreifenden Zusammenarbeit für Projekte und Themen rund um die digitale Transformation der Bundesbank geschaffen. Zusammen mit der Banque de France wird die Bundesbank den BIS Innovation Hub des Eurosystems in Frankfurt betreiben, in dem moderne Technologien zur Unterstützung der Finanzaufsicht (SupTech und RegTech), Cybersicherheit und Nachhaltigkeitsthemen (Green Finance) im Fokus stehen werden.

… sowie darüber hinaus

Die Bundesbank vernetzt sich aber auch außerhalb der Zentralbankgemeinschaft, etwa mit der Start-up-Szene als institutioneller Partner der Frankfurter Innovationsplattform TechQuartier, die Unternehmen, Innovatoren, die Finanzbranche, akademische Institutionen und den öffentlich-rechtlichen Sektor zusammenbringt. Dadurch können die Ideen der Bundesbank zu den eigenen innovativen Digitalisierungsvorhaben zusätzliche Impulse erhalten, und die Bundesbank ist in der Lage, ihre eigenen Erfahrungen weiterzugeben.

Einsatz von Technologie darf Sicherheit nicht gefährden

Neue Technologien und Bezugsformen dürfen jedoch die Sicherheit der Institute nicht gefährden. Die Abhängigkeit von einer funktionsfähigen und sicheren IT ist gestiegen, denn Ausfälle wesentlicher IT-Systeme, wie beispielsweise Kernbanken-, Handels- oder Zahlungsverkehrssysteme, können schwerwiegende Auswirkungen auf die Leistungserbringung haben. Kunden spüren dies insbesondere, wenn das Onlinebanking und der Geldautomat nicht wie gewohnt funktionieren oder Zahlungen und Wertpapierorders nicht oder falsch ausgeführt werden. Die Gefährdung durch Hackerangriffe

stellt auch eine zunehmende Herausforderung für die Institute und das übrige Finanzsystem dar. Dabei profitieren die Angreifer von der wachsenden technischen Komplexität und agieren selbst immer professioneller. Von besonderem Interesse für die Angreifer sind dabei die Zahlungsverkehrssysteme, um etwa betrügerisch Gelder anweisen zu können, oder auch Kernbankensysteme, deren Beeinträchtigung wegen des damit verbundenen Schadens ein großes Erpressungspotenzial hat. Wenn der Zugriff auf betriebsnotwendige Daten gelingt, werden diese beispielsweise verschlüsselt (Ransomware), um für die Entschlüsselung anschließend ein Lösegeld zu fordern. Zudem können Angriffe wichtige IT-Systeme des Instituts zur Kommunikation mit Kunden, wie etwa E-Mail oder Internetauftritt, ausfallen lassen oder anderweitig beeinträchtigen.

Schutz vor digitalen Risiken notwendig

Der breite Einsatz und die intensive Nutzung von IT erfordern deshalb, ein verstärktes Augenmerk auf die Einhaltung der notwendigen Sicherheitsanforderungen zu richten. Institute müssen die mit der digitalen Transformation einhergehenden digitalen Risiken verlässlich steuern. Das heißt, dass die Daten der Institute und die ihrer Kunden jederzeit verfügbar, vor ungewollten Veränderungen gesichert und vor unbefugter Einsichtnahme geschützt sind.

Perspektive der Banken- und Finanzaufsicht auf digitale Risiken

Aufsichtsansatz zu digitalen Risiken

Das Finanzsystem soll die effiziente und kostengünstige Bereitstellung finanzieller Mittel und Dienstleistungen für Wirtschaftsakteure und Privatpersonen sicherstellen. Der Bankenaufsicht kommt dabei die Rolle zu, die Geschäftstätigkeit von Kreditinstituten zu überwachen, indem sie die Effizienz und Stabilität des Bankensystems sicherstellt.

Aufsicht verfolgt ganzheitlichen Ansatz und verlangt angemessene Risikomanagementprozesse

Der sichere Einsatz von IT bedingt das erfolgreiche Zusammenspiel der menschlichen Komponente mit organisatorischen und technischen Maßnahmen. Eine reine Fokussierung auf die Technik reicht folglich nicht aus. Daneben sind gut strukturierte und wirksam implementierte Prozesse ein entscheidender Erfolgsfaktor für das Management digitaler Risiken. Die Aufsicht verfolgt deshalb einen systemanalytischen, nicht nur auf die Funktionsweise einzelner Elemente des Risikomanagements, sondern auf ihr Zusammenspiel im Risikomanagementsystem und dessen Einbettung in die Gesamtbanksteuerung ausgerichteten Ansatz.

Institute müssen digitale Risiken begrenzen

Wie bei anderen wesentlichen Risiken auch hat sich hierbei ein prinzipien- und prozessorientierter Regulierungs- und Überwachungsansatz bewährt. So sollen die organisatorischen Anforderungen nach § 25a und § 25b Kreditwesengesetz (KWG) sicherstellen, dass Institute ein angemessenes Risikomanagement betreiben, was sich auch auf ausgelagerte Prozesse erstreckt.

BAIT konkretisieren Erwartungshaltung zum Umgang mit digitalen Risiken, …

Die Rundschreiben der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zu Mindestanforderungen an das Risikomanagement (MaRisk) und Bankaufsichtliche Anforderungen an die IT (BAIT) konkretisieren die Erwartungshaltung des KWG technologieneutral. In ihnen spiegeln sich die europäischen Vorgaben sowie die Erfahrungen aus IT-Prüfungen der Aufsicht wider.

… spiegeln internationale Vorgaben und langjährige Prüfungserfahrungen wider …

Bei der Entwicklung der Rundschreiben arbeiten Bundesbank und BaFin eng zusammen. Die Bundesbank stützt sich hierbei unter anderem auf ihre praktischen Erfahrungen aus bankgeschäftlichen Prüfungen. Zusammen mit Erörterungen in Fachgremien sowie öffentlichen Konsultationen wird so eine praxisnahe Ausgestaltung des Regelwerks möglich. Die Konkretisierungen in den Rundschreiben sind nicht abschließend, denn die Institute müssen sich auch an gängigen Standards und bewährten Praktiken zum Umgang mit digitalen Risiken orientieren.

Was sind die aufsichtlichen Anforderungen bezüglich IT in den Banken?
Ausgewählte Themen der BAIT-Novelle 2021

MaRisk[1]	BAIT[2]
Strategien	**IT-Strategie** – Geschäftsleitung verantwortet die Strategie der IT und der Informationssicherheit – IT und Informationssicherheit an gängigen Standards orientieren
Internes Kontrollsystem	**IT-Governance** – Wirksame IT-Aufbau und IT-Ablauforganisation – Risikokontrollprozesse und angemessene Ressourcenausstattung
Organisations-richtlinien	**Informationsrisikomanagement** – Aktueller Überblick über IT-Systeme und deren Abhängigkeiten – Regelmäßige Überprüfung der Umsetzung von Schutzmaßnahmen
Dokumentation	**Informationssicherheitsmanagement** – ISB[3] verantwortet Definition und Überwachung von Schutzmaßnahmen – Regelmäßige Überprüfung, Sensibilisierung und Schulung zur Informationssicherheit
Personal	**Operative Informationssicherheit** – Schutzmaßnahmen und Prozesse nach dem Stand der Technik – Permanente Überwachung und unabhängige Überprüfung der Sicherheit der IT-Systeme
Berichte	**Identitäts- und Rechtemanagement** – Zugriffe auf IT-Systeme und Zutritte zu Räumlichkeiten werden begrenzt und überwacht – Regelmäßige Überprüfung eingeräumter Rechte
Technisch-organisatorische Ausstattung	**IT-Projekte und Anwendungsentwicklung** – Steuerung und Überwachung der IT-Projekte / des Projektportfolios – Sichere Entwicklung von Anwendungen inkl. umfassender Tests und Dokumentation
Funktionstrennung	**IT-Betrieb** – Überwachung der IT-Systeme, Änderungen geregelt durchführen und Störungsbearbeitung – Zuverlässige Datensicherungen und Steuerung des Kapazitätsbedarfs
Anpassungs-prozesse	**Auslagerung und sonstiger Fremdbezug von IT-Dienstleistungen** – Steuerung von Risiken aus dem sonstigen Fremdbezug von IT-Dienstleistungen – Regelmäßige Überprüfung der Risikobewertungen und Verträge mit Dienstleistern
Auslagerung	**IT-Notfallmanagement** – Identifizierung von zeitkritischen IT-Prozessen und Vorsorge für deren Ausfall – Jährliche Überprüfung der Wirksamkeit der Vorsorgemaßnahmen
Notfall-Management	
ZAIT[4]	**Management der Beziehungen mit Zahlungsdienstnutzern** – Informationspflicht gegenüber Zahlungsdienstnutzern über sicherheitsrelevante Aspekte – Zahlungsdienstnutzer müssen technische und organisatorische Unterstützung erhalten

1 Mindestanforderungen an das Risikomanagement. **2** Bankaufsichtliche Anforderungen an die IT. **3** Informationssicherheitsbeauftragter **4** Zahlungsdiensteaufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld-Instituten.

Deutsche Bundesbank

… und lassen neue Technologien und Methoden zu

Die aufsichtlichen Anforderungen sind prinzipienhaft ausgestaltet und überlassen es den Instituten zu entscheiden, welche Technologien oder Methoden bei ihnen zur Anwendung kommen. Somit sind auch aktuelle Entwicklungen wie Cloud-Computing grundsätzlich geregelt. Auch bei Künstlicher Intelligenz und Maschinellem Lernen erlauben die prinzipienhaften Anforderungen eine effektive Beaufsichtigung. Es gilt dabei, neue Methoden und Risiken frühzeitig zu erkennen und den aufsichtlichen Fokus darauf zu legen (vgl. Erläuterungen auf S. 61 ff.).

Die Rolle der Bundesbank im Umgang mit digitalen Risiken im Bankensektor

Operative Bankenaufsicht in Deutschland erfolgt durch Bundesbank

Die Bundesbank überwacht gemeinsam mit der BaFin rund 1 650 Kreditinstitute in Deutschland. Die Zusammenarbeit bei der laufenden Überwachung der Institute ist in § 7 Absatz 1 KWG und in der Aufsichtsrichtlinie geregelt. Die Arbeiten der Bundesbank erfolgen zum allergrößten Teil in den neun Hauptverwaltungen der Bundesbank in regionaler Nähe zu den Instituten. Seit 2014 ist die Bundesbank zudem Teil des einheitlichen Aufsichtsmechanismus (Single Supervisory Mechanism: SSM) zur Aufsicht über bedeutende Institute in Europa, in dem ihr durch die Mitwirkung in den gemeinsamen Aufsichtsteams ebenfalls eine bedeutende operative Rolle zukommt.

Laufende Aufsicht wertet Informationen zu digitalen Risiken aus

Kern der aufsichtlichen Tätigkeit ist die Durchführung des Überprüfungs- und Beurteilungsprozesses (Supervisory Review and Evaluation Process: SREP). In diesem Rahmen werden neben finanziellen Risiken auch nichtfinanzielle Risiken, wie beispielsweise digitale Risiken, beurteilt. Die hierzu notwendigen Informationen werden, wie bei bedeutenden Instituten,[1)] seit diesem Jahr auch direkt von den weniger bedeutenden Instituten über einen strukturierten Fragebogen erhoben. Auf dieser Grundlage wird das digitale Gefährdungspotenzial eines Instituts sowie dessen Behandlung im instituts-eigenen Risikomanagement aufsichtlich bewertet.

In bankgeschäftlichen Prüfungen erhält die Bundesbank tiefgehende Einblicke in den Geschäftsbetrieb und insbesondere in die Risikosteuerung der Institute. Die Prüfungen der Bundesbank werden bei weniger bedeutenden Instituten von der BaFin und bei bedeutenden Instituten von der Europäischen Zentralbank beauftragt. Die Prüfungsinhalte bei IT-Prüfungen beziehen sich auf die organisatorisch-technischen Pflichten nach § 25a und § 25b KWG sowie auf deren Konkretisierung über die Rundschreiben MaRisk und BAIT. Ziel dieser sogenannten Systemprüfungen ist es, die Angemessenheit des Risikomanagements vor dem Hintergrund der spezifischen Situation des Instituts zu beurteilen. Der hierdurch mögliche ganzheitliche Blick auf die digitalen Risiken eines Instituts sowie die prozessorientierte Herangehensweise bei IT-Prüfungen hat sich für die Bundesbank als sehr effektives Vorgehen erwiesen.

Bankgeschäftliche Prüfungen ermöglichen umfassenden Überblick über digitale Risiken und zeigen Optimierungspotenzial auf

Die Prüfungen der Bundesbank bei Instituten und ihren IT-Dienstleistern haben in der vergangenen Dekade immer häufiger IT-Aspekte betrachtet und stetige Verbesserungen bei den Risikomanagementprozessen feststellen können oder bewirkt. Sie zeigen aber auch immer wieder grundsätzliche Schwachstellen, Brennpunkte und Verbesserungsbedarf im Umgang mit digitalen Risiken auf. Seit 2010 hat die Bundesbank mehr als 2 000 bankgeschäftliche Prüfungen durchgeführt und bei fast jeder zweiten Prüfung wesentliche Mängel im Risikomanagement vorgefunden. Rund 15 % dieser Feststellungen betrafen IT-Themen, vordringlich im Management der Informationsrisiken, im Auslagerungsmanagement und in der Informationssicherheit.

Neben der Sensibilisierung durch die Prüfungen wirkt die Bundesbank in der Mängelnachverfol-

1 Vgl.: https://www.bankingsupervision.europa.eu/ecb/pub/html/ssm.aroutcomesrepitriskquestionnaire202007~9ed9aaa17d.en.html.

Künstliche Intelligenz und Maschinelles Lernen

Die gestiegene Leistungsfähigkeit der IT-Infrastruktur und der Fortschritt in der Anwendung maschineller Lernverfahren eröffnen auch der Kreditwirtschaft die Anwendung solcher neuer Verfahren in Markt und Marktfolgebereichen, etwa beim Ratingprozess. Von besonderem bankaufsichtlichen Interesse ist ihre Nutzung in den Risikomess- und -managementsystemen. Anstelle manueller Prozesse oder herkömmlicher Risikomodelle treten Verfahren der Künstlichen Intelligenz (KI) beziehungsweise des Maschinellen Lernens (ML), kurz: ML-Methoden. Dabei bezieht sich der Begriff KI auf das Ziel, komplexe Aufgaben, die bisher durch die Nutzung menschlicher Intelligenz gelöst werden, maschinell zu erledigen.[1)] Bei ML steht weniger die Nachbildung menschlicher Intelligenz im Vordergrund, sondern der Einsatz von Lernverfahren wie etwa neuronalen Netzen, welche in der Lage sind, komplexe, nicht lineare Zusammenhänge abzubilden und für Entscheidungsprozesse effizient nutzbar zu machen. Mit ML-Methoden entstehen allerdings auch neue Risiken, die es bankaufsichtlich zu beurteilen und letztlich auch zu begrenzen gilt.

Relevante ML-Methoden

Es existieren viele unterschiedliche Ansätze, ML zu definieren.[2)] Zur Definition der bankaufsichtlichen Aufgreifpunkte bedarf es deshalb einer pragmatischen Abgrenzung neuartiger Modelle und damit verbundener Risiken. Die Überlegungen der Bundesbank hierzu basieren auf einem dreidimensionalen ML-Szenario:[3)]

- Datengrundlage und Methodik beschreiben als erste Dimension die Komplexität der ML-Methode. Wenn Banken zum Beispiel tiefe neuronale Netze zum Einsatz bringen, führt dies zu einem hohen Grad an Komplexität. Auf der anderen Seite des Spektrums stehen klassische statistische Verfahren, wie sie seit Jahrzehnten in der Finanzbranche eingesetzt werden (z. B. logistische Regressionen oder Expertensysteme).

- Die zweite Dimension baut auf der ML-Methode selbst auf und beschreibt die Nutzung des Outputs. Sie kennzeichnet somit, welchen Stellenwert das Verfahren innerhalb der Risikosteuerung einnimmt. Hier gilt es zu berücksichtigen, welchen Anteil die ML-Methode am Gesamtmodell hat und wie und mit welchen Auswirkungen die Ergebnisse in aufsichtlich relevanten Bereichen Anwendung finden. Je nachdem, wie stark die beiden erstgenannten Dimensionen ausgeprägt sind, müssen Prüfungstechnik und -intensität der Aufsichtsprozesse angepasst werden.

- Die dritte Dimension betrifft die Themen Auslagerung und IT-Infrastruktur. Es wird ein technologieneutraler Ansatz in der Aufsicht vorgeschlagen, der insbesondere nicht zwischen Eigenentwicklung und Auslagerung oder der zugrunde liegenden IT-Infrastruktur unterscheidet. Es ist zu erwarten, dass zentrale Dienstleister und FinTechs bei der Entwicklung von ML-Methoden eine treibende Kraft darstellen werden. Daher ist vorgesehen, dass im Rahmen des bestehenden Auslagerungsregelwerks auch bankgeschäftliche Prü-

1 Siehe: Financial Stability Board (2017).
2 Definition des Financial Stability Board (2017): „Machine learning may be defined as a method of designing a sequence of actions to solve a problem, known as algorithms, which optimise automatically through experience and with limited or no human intervention." Mitchell (1997): „A computer program is said to learn from experience E with respect to some task T and some performance measure P, if its performance on T, as measured by P, improves with experience E."
3 Siehe: Deutsche Bundesbank (2020a).

fungen bei Auslagerungsunternehmen stattfinden werden.

Rolle des bestehenden Aufsichtsrechts

ML-Methoden bilden weder einen eigenen Aufsichtsbereich, noch sind sie allein wegen der neuen Technik relevant für die Aufsicht. Vielmehr lassen sich die neuen Methoden weitgehend über bestehende prozessorientierte Prüfungskonzepte risikoorientiert prüfen und bewerten. Dies betrifft beispielsweise Ratingverfahren, die ohnehin unter Genehmigungsvorbehalt stehen, oder Frühwarnsysteme, die in der Vergangenheit ohne ML betrieben wurden. Der Aufsichtsansatz kann technologieneutral angewendet werden, selbst wenn sich mit ML-Methoden spezifische Fragestellungen ergeben. Die Frage lautet also primär, welche Unterschiede sich zu klassischen Modellen und Prozessen ergeben und wie die Aufsicht damit umgehen kann. Unterschiede bestehen vor allem bei der Erklärbarkeit, der Modellentwicklung und -validierung sowie beim Trainingszyklus. Damit Banken Planungssicherheit bei Investitionen in ML-Methoden haben, sollen die aufsichtliche Sicht geschärft und etwaige neue Anforderungen transparent kommuniziert werden.[4)]

Erklärbarkeit

Banken müssen ihre Entscheidungsprozesse verstehen und Maßnahmen begründen können. Entscheidungen sollen auf Kausalitäten und Wirkungszusammenhängen basieren. ML-Methoden hingegen sind vor allem deshalb erfolgreich, weil sie Muster selbstständig und ohne die Vorgabe von festen Kausalitäten in Daten erkennen können und damit die Ableitung von Maßnahmen ermöglichen. Eine inhärente Eigenschaft vieler ML-Methoden ist, dass mit dem Verzicht auf Vorwissen über Kausalitäten ein Mangel an Erklärbarkeit einhergeht. Dieser Mangel kann ein Hindernis für deren Anwendung sein – nämlich dann, wenn es bei der Nutzung des Outputs kausaler Erklärungen bedarf. Banken müssen daher die Vorteile, die ML-Methoden bieten, gegen die Nachteile dieser Blackbox-Eigenschaft abwägen. Eine gesteigerte Modell- beziehungsweise Prognosegüte oder der Mangel an anderen geeigneten Methoden können insofern den Einsatz von ML begründen. Es gilt aber sicherzustellen, dass Entscheidungen, die maßgeblich von einer Blackbox vorbereitet oder gar getroffen werden, klar verantwortet und in eine Prozesslandschaft eingebettet werden. Es wurde eine Vielzahl von Ansätzen entwickelt, um ML nachträglich erklärbar zu machen (sog. Explainable AI: XAI). Diese Ansätze sind vielversprechend, denn sie geben einen punktuellen und oft anschaulichen Einblick in die Funktionsweise von ML-Methoden. Es ist aber auch Vorsicht geboten, denn kein XAI-Ansatz schafft völlige Erklärbarkeit. Wie viel Blackbox angemessen ist, hängt daher vom ML-Szenario des Einzelfalls ab.

Modellentwicklung und Validierung

ML-Methoden weisen im Vergleich zu klassischen statistischen Verfahren Besonderheiten bei ihrer Entwicklung und Pflege auf. Mit steigender Menge, Frequenz und Bedeutung auch unstrukturierter Daten gewinnen die Datenqualität und die Datenaufbereitung an Bedeutung. Die Gefahr besteht, dass unzureichende Daten eingesetzt werden, um dem hohen Datenbedarf von ML-Methoden zu genügen, während die Konsequenzen daraus aufgrund der Blackbox-Eigenschaft verborgen bleiben. Mangelnde Datenqualität beeinflusst aber nicht nur die Modellentwicklung, sondern erschwert auch

4 BaFin und Bundesbank haben ihre Sichtweise auf ML-Methoden gemeinsam zur Konsultation gestellt (https://www.bundesbank.de/de/aufgaben/bankenaufsicht/einzelaspekte/risikomanagement/maschinelle-lernverfahren).

eine Validierung, die insbesondere bei einer Blackbox an Bedeutung gewinnt.

Wie alle Modelle müssen deshalb auch ML-Methoden in ein geeignetes Kontrollumfeld eingebettet sein. Dieses muss sicherstellen, dass Modellentwickler, Validierer und Anwender gleichermaßen von den guten Ergebnissen des Modells überzeugt sind, die Verantwortung für Fehler klar geregelt ist und sowohl interne als auch externe Kontrolleinheiten einen ausreichenden Einblick in die ML-Methode gewinnen können.

Trainingszyklus

ML-Methoden erlauben häufig eine laufende Anpassung an neue Daten. Dieser als Re-training bezeichnete Prozess kann entweder die Struktur der Methode und sogenannter Hyperparameter[5)] verändern oder sich auf die Optimierung in dem bestehenden Rahmen beschränken. Über diesen Weg kann ein Modell an eine sich ändernde Wirklichkeit (z. B. im Fall von Strukturänderungen und -brüchen) angenähert werden. Banken sollten sich allerdings der Nachteile von Re-trainings, nämlich sinkender Kontinuität und Vergleichbarkeit, bewusst sein. Es ist entscheidend, dass Banken die Notwendigkeit des Trainingszyklus begründen. Insbesondere muss auch die typischerweise in definierten Zyklen verlaufende Modellvalidierung ein Modell mit laufendem Retraining adäquat abdecken und umfassend beurteilen können.

5 Parameter der ML-Methode, der vor der Optimierung festgelegt wird.

gung und durch Nachschauprüfungen auf die nachhaltige Beseitigung der Defizite hin. Die Aufsicht räumt dem Thema digitale Risiken somit weiterhin einen hohen Stellenwert ein, zumal die Prüfungen regelmäßig deutlich machen, vor welchen Aufgaben die Institute standen und teilweise noch stehen.

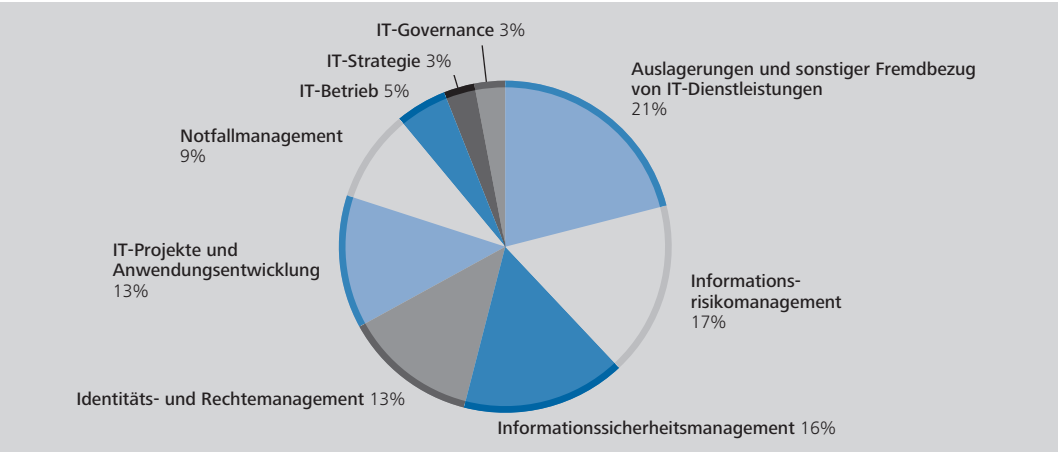
Institute müssen mehr Transparenz über ihre digitalen Risiken erlangen, …

Dem Informationsrisikomanagement kommt bei der Steuerung digitaler Risiken eine besondere Bedeutung zu. Es stellt einen Regelkreislauf dar, in dem allen IT-Komponenten Schutzmaßnahmen zugeordnet und Risiken, insbesondere aus deren unvollständiger Umsetzung, identifiziert und laufend überwacht werden. Prozessschwächen im Informationsrisikomanagement können dazu führen, dass dem Institut die Transparenz zu digitalen Risiken fehlt und diese in der Folge auch keiner angemessenen Steuerung unterliegen. Häufig wird beobachtet, dass Instituten ein vollständiger Gesamtüberblick über die maßgeblichen IT-Komponenten fehlt und somit nicht alle notwendigen Teile in die Risikoanalysen einbezogen werden können. Zudem müssen Institute vielfach noch vollständige und konsistente Vorgaben für die notwendigen Schutzmaßnahmen erstellen und erforderliche Pflegeprozesse implementieren. Sofern Vorgaben vorhanden sind, wird oft nicht ausreichend umfänglich oder nur mit einer unzureichenden Frequenz überprüft, dass diese Vorgaben dann auch tatsächlich eingehalten werden.

… Risiken aus ausgelagerten Prozessen und Aktivitäten steuern und überwachen …

Aufgabe des Auslagerungsmanagements ist es, ausgelagerte Prozesse und damit verbundene Risiken zu steuern und zu überwachen. Dies erfolgt in erster Linie dezentral in den auslagernden Fachbereichen des Instituts, welche durch zentrale Stellen wie einen Auslagerungsbeauftragten oder ein zentrales Auslagerungsmanagement unterstützt werden sollen. Als wichtigstes Prinzip im Auslagerungsmanagement gilt, dass ein Institut zwar Prozesse an sich, aber nie die Verantwortung für diese Prozesse auslagern kann. Jedes Institut muss also

Wesentliche Mängel aus IT-Prüfungen der letzten zehn Jahre bei deutschen Banken



Deutsche Bundesbank

über ausreichend Expertise verfügen, um seine Auslagerungen und Auslagerungsrisiken vollständig überwachen zu können. Mängel im Prozess der Auslagerungssteuerung können dazu führen, dass insbesondere beim Bezug von IT-Dienstleistungen digitale Risiken unerkannt bleiben oder nur rudimentär bewertet werden können. Dabei stellen Prüfungen wiederholt fest, dass Dienstleistungen nicht als Auslagerungen klassifiziert werden und die Risikoanalysen zur Feststellung der Wesentlichkeit einer Auslagerung grundlegende Mängel aufweisen. Auch kommen wiederholt Mängel bei der vertraglichen Verankerung von Informations- und Prüfungsrechten sowie von Regelungen für Weiterverlagerungen zutage. Das Überwachen von Auslagerungsketten stellt eine anspruchsvolle Aufgabe für das Auslagerungsmanagement dar.

… und durchgängig wirksame Schutzmaßnahmen nach Stand der Technik anwenden

Im Informationssicherheitsmanagement werden unter Leitung des Informationssicherheitsbeauftragten Maßnahmen zum Schutz der IT definiert und deren Einhaltung überwacht. Der Schutz vor Angreifern ist jedoch immer nur so gut wie das schwächste Glied in der Kette. Prozessschwächen im Informationssicherheitsmanagement können verhindern, dass Institute ein angemessenes und durchgängiges Schutzniveau erreichen. Deshalb sollen implementierte Maßnahmen zum Schutz der IT immer den Vorgaben gängiger Standards und dem Stand der Technik entsprechen und regelmäßig getestet werden. Wenn Informationssicherheitsbeauftragte aber zu nah an den von ihnen zu überwachenden operativen Einheiten verortet sind, besteht die Gefahr, dass sie nicht frei von Interessenkonflikten agieren können. Bei beiden Aspekten zeigt die Prüfungspraxis oftmals Nachholbedarf. Überdies werden interne Tests zur Überprüfung der Wirksamkeit implementierter Schutzmaßnahmen nicht immer in ausreichendem Maße oder mit der notwendigen Frequenz durchgeführt.

Bundesbank unterstützt freiwillige Überprüfung der Widerstandsfähigkeit des Finanzsektors gegen digitale Risiken

Insbesondere Angriffe, die unzureichende Schutzmaßnahmen ausnutzen, stellen mittlerweile ein bedeutendes digitales Risiko dar und fordern aufgrund der komplexen Verflechtungen der IT zwischen den Instituten inzwischen das gesamte Finanzsystem heraus. Mit der Durchführung von TIBER[2)]-DE-Tests leistet die Bundesbank einen essenziellen Beitrag zur nachhaltigen Verbesserung der Cyberwiderstandsfähigkeit des deutschen Finanzsektors, da mit diesen Tests die Verteidigungsfähigkeiten der Unternehmen gegen Cyberangriffe mit möglichst realen Angriffsszenarien auf ihre Wirksamkeit hin überprüft werden (siehe Erläuterungen S. 65 f.).

2 Bedrohungsgeleitete ethische Hacking-Übungen (Threat Intelligence-based Ethical Red Teaming: TIBER).

TIBER-DE

Die zunehmende Digitalisierung im Finanzsektor und die damit einhergehende steigende Verwundbarkeit gegenüber Cyberangriffen rücken die Widerstandsfähigkeit gegen interne wie externe Angriffe immer stärker in den Fokus der Notenbanken.

Die Bundesbank und das Bundesministerium der Finanzen haben im Sommer 2019 das Rahmenwerk für bedrohungsgeleitete ethische Hacking-Übungen (Threat Intelligence-based Ethical Red Teaming: TIBER-EU) des Europäischen Systems der Zentralbanken in Deutschland als TIBER-DE umgesetzt.[1)] Das TIBER-DE-Umsetzungsdokument wurde im Juli 2020 veröffentlicht.[2)] Mit TIBER-DE soll die Cyberwiderstandsfähigkeit der Unternehmen des deutschen Finanzsektors gefördert und damit ein wesentlicher Beitrag zu einem funktionsfähigen und stabilen Finanzsystem geleistet werden.

Bei einem TIBER-DE-Test werden simulierte Angriffe von ethischen Hackern auf ein Unternehmen durchgeführt. Dies geschieht unter kontrollierten Bedingungen und gestützt durch ein stringentes Risikomanagement. Ziel ist, die Verteidigungsfähigkeiten des Unternehmens gegen Cyberangriffe mit möglichst realen Angriffsszenarien auf ihre Wirksamkeit hin zu prüfen. Dafür werden während des TIBER-DE-Tests gesammelte Informationen über die unternehmensspezifische Bedrohungslage genutzt und Techniken realer Angreifer verwendet. Hierbei stehen explizit die kritischen Funktionen des Unternehmens und die entsprechenden Produktivsysteme im Fokus. Bei Banken können dies beispielsweise die Systeme des baren und unbaren Zahlungsverkehrs, die Kreditvergabesysteme oder das Onlinebanking sein. Im Gegensatz zu klassischen Penetrationstests zielen TIBER-DE-Tests nicht alleine auf technische Schwachstellen in den Systemen ab, sondern beziehen auch organisatorische Mängel sowie den Faktor Mensch in die Angriffsszenarien ein.

TIBER-DE richtet sich an große Banken, Versicherungen, Finanzmarktinfrastrukturen und deren kritische Dienstleister. Eine Teilnahme an TIBER-DE-Tests erfolgt freiwillig und fördert die eigenständige Auseinandersetzung der Unternehmen mit der eigenen Cyberwiderstandsfähigkeit. Der Vorstand der getesteten Unternehmen wird von Anfang an in einen TIBER-DE-Test eingebunden, um gezielt das Bewusstsein für das steigende Risiko von Cyberangriffen zu schärfen. Ein TIBER-DE-Test sollte nicht als Prüfung verstanden werden, die es zu bestehen gilt. Er ist vielmehr dann erfolgreich, sofern er rahmenwerkskonform durchgeführt wurde.

Das nationale Kompetenzzentrum für TIBER-DE – das sogenannte TIBER Cyber Team – ist bei der Bundesbank angesiedelt und sowohl organisatorisch als auch prozessual von der Finanzaufsicht getrennt. Die Finanzaufsicht wird aber über die Testdurchführung informiert und zu festgelegten Zeitpunkten eingebunden. Das TIBER Cyber Team ist einem Lenkungsausschuss aus Vertretern von Bundesbank und Bundesanstalt für Finanzdienstleistungsaufsicht unterstellt. Diesem Lenkungsausschuss obliegt die strategische Steuerung von TIBER-DE.

Das TIBER Cyber Team begleitet die Unternehmen während der gesamten TIBER-DE-Testphase, unterstützt diese mit dem benö-

1 Vgl.: Deutsche Bundesbank und Bundesministerium der Finanzen (2019).
2 Vgl.: Deutsche Bundesbank (2020b).

tigten Fachwissen und kontrolliert die Einhaltung der Rahmenbedingungen von TIBER-DE. Am Ende eines Tests, der bis zu einem Jahr dauern kann, wird dem getesteten Unternehmen durch das TIBER Cyber Team attestiert, dass ein rahmenwerkskonformer Test durchgeführt wurde.

Das TIBER-EU-Rahmenwerk wurde auch in einigen anderen Mitgliedstaaten der EU implementiert, beispielsweise in den Niederlanden, in Dänemark und in Belgien. Zwischen den Mitgliedstaaten, die TIBER-EU umgesetzt haben, ist eine wechselseitige Anerkennung der Testteilnahme durch das Rahmenwerk gewährleistet. Durch eine enge Zusammenarbeit zwischen den beteiligten Behörden und den Unternehmen soll in einem kooperativen Ansatz die Cyberwiderstandsfähigkeit im gesamten Finanzsektor erhöht werden, um den mit der Digitalisierung einhergehenden Risiken angemessen zu begegnen.

Die Akzeptanz und Nachfrage nach TIBER-DE im deutschen Finanzsektor ist hoch. Bislang wurden bereits neun TIBER-DE-Tests begonnen.

TIBER-DE-Tests können einen erheblichen Beitrag zur Steigerung der Cyberwiderstandsfähigkeit leisten. Insbesondere ermöglichen es TIBER-DE-Tests den teilnehmenden Unternehmen, das Zusammenspiel zwischen verschiedenen Prozessen zur Abwehr von Cyberangriffen und den an diesen Prozessen beteiligten Mitarbeitern und den verknüpften Systemen an einem konkreten Angriffsszenario zu erproben. So zeigen TIBER-DE-Tests, dass technisch hochwertige Schutzmechanismen durch menschliche Fehler oder mangelhafte Sicherheitsvorgaben unwirksam werden können. Außerdem werden Mängel in bestehenden Prozessen und unzureichende Investitionen in Schutzmechanismen durch einen TIBER-DE-Test auch gegenüber der Unternehmensleitung transparent gemacht. Dieses gesteigerte Bewusstsein in der Unternehmensleitung über konkrete Cyberrisiken kann dabei helfen, zusätzlichen Investitionsbedarf aufzuzeigen, Budgetentscheidungen stärker am Sicherheitsbedarf auszurichten und Behebungsmaßnahmen zielgerichteter umzusetzen.

TIBER-DE-Tests zeigen auch, dass aufmerksame und sensibilisierte Beschäftigte selbst ausgefeilte Angriffe frühzeitig erkennen und abwehren können, sofern es im Unternehmen wohldefinierte interne Sicherheitsregeln und -prozesse gibt. Regelmäßige Kampagnen zur Sensibilisierung der Belegschaft stellen eine mögliche Maßnahme zur Abwehr von Cyberangriffen dar, deren Effektivität durch TIBER-DE-Tests geprüft werden.

Mit der Umsetzung einheitlicher TIBER-Tests in Deutschland stellt die Bundesbank sicher, dass die Widerstandsfähigkeit der Unternehmen nicht nur auf dem Papier existiert, sondern auch praktisch und realitätsnah überprüft wird. TIBER-DE Tests leisten somit auch angesichts der zunehmenden Risikolage einen essenziellen Beitrag zur nachhaltigen Verbesserung der Cyberwiderstandsfähigkeit des deutschen Finanzsektors.

Ausblick

Bundesbank trägt zur wirksamen Aufsicht über digitale Risiken bei und passt Praxis neuen Gegebenheiten an

Die Bundesbank behandelt digitale Risiken sowohl im aufsichtlichen Überprüfungs- und Beurteilungsprozess als auch bei bankgeschäftlichen Prüfungen. TIBER-DE-Tests unterstützen zudem die freiwillige Überprüfung der Widerstandsfähigkeit des Finanzsektors bezüglich digitaler Risiken. Die fortschreitende Arbeitsteilung der Marktteilnehmer und deren Vernetzung sowie technisch-organisatorische Innovationen bedingen jedoch auch Anpassungen in der Herangehensweise der Aufsicht.

So hat der Baseler Ausschuss für Bankenaufsicht dem Bankensektor in aktualisierten Prinzipien zum Management operationeller Risiken[3)] sowie mit neuen Prinzipien zur operationellen Resilienz[4)] kürzlich klare Hinweise zur Ausgestaltung der essenziellen Elemente im Umgang mit digitalen Risiken und zu deren Behandlung gegeben. Diese Prinzipien werden von der Aufsicht unter anderem in nationale Regelwerke und die Aufsichtspraxis übernommen und sollen von Banken proportional implementiert werden.

Zudem wird die Europäische Kommission mit der Erarbeitung der Verordnung Digital Operational Resilience Act (DORA)[5)] harmonisierte Anforderungen zum Umgang mit digitalen Risiken der Institute schaffen, die Transparenz hinsichtlich möglicher Konzentrationen digitaler Risiken erhöhen und die Handlungsfähigkeit der Finanzaufsicht gegenüber Banken sowie kritischen IT-Drittanbietern stärken. Dieser Auslagerungsaspekt wird auch im Gesetz zur Stärkung der Finanzmarktintegrität (FISG)[6)] adressiert, das im Mai dieses Jahres vom Bundestag verabschiedet wurde.

Auch der Aufsichtsansatz für Künstliche Intelligenz und Maschinelles Lernen soll künftig international vereinheitlicht werden, um ein Level-Playing-Field zu schaffen. Neben dem Baseler Ausschuss für Bankenaufsicht beschäftigt sich auch die Europäische Kommission mit einem Verordnungsentwurf für Künstliche Intelligenz, mit dem über die Finanzbranche hinaus einheitliche Regeln vorgeschlagen werden.[7)] Am Beispiel des Maschinellen Lernens zeigt sich jedoch, dass die Risiken aus neuen Technologien und Methoden durchaus bereits mit den bestehenden regulatorischen Anforderungen angemessen behandelt werden können.

Bankgeschäft wird weiter durch die Digitalisierung geprägt, …

Die Digitalisierung wird die gesellschaftliche und wirtschaftliche Entwicklung weiter prägen, und die Geschwindigkeit des technologischen Wandels insbesondere im Bankensektor wird hoch bleiben. Der langfristige Erfolg der Institute hängt deshalb auch stark von der stetigen und geordneten Nutzung der Technologien für Innovationen ab. Institute müssen sich diesem rasanten Wandel stellen und ihn aktiv gestalten, um ihren Kunden weiterhin für sie relevante Dienstleistungen anbieten zu können und so strukturell wettbewerbsfähig zu bleiben.

… konsequenter Umgang mit digitalen Risiken ist deshalb unumgänglich

Kehrseite der Digitalisierung ist jedoch, dass durch die steigende Komplexität und zunehmende Arbeitsteilung des Bankgeschäfts auch das Gefährdungspotenzial wächst. Dies gilt umso mehr, wenn Institute weiterhin mit stark fragmentierten IT-Landschaften und historisch gewachsenen Technologien arbeiten. IT-Infrastrukturen und Anwendungen müssen weiterhin sicher betrieben und bedarfsgerecht weiterentwickelt werden, um die sensiblen Daten der Kunden zu schützen und einen stabilen Betrieb zu gewährleisten. Dazu benötigen Banken vor allem ein umfassendes Verständnis und müssen einen angemessenen Umgang mit ihren digitalen Risiken sicherstellen. Dies gilt auch für ausgelagerte Prozesse. Nur so bewahren die Institute das Vertrauen ihrer Kunden und die notwendige Widerstandsfähigkeit als wesentliche Bestimmungsgründe für nachhaltigen wirtschaftlichen Erfolg.

---

3 Vgl.: Bank für Internationalen Zahlungsausgleich (2021a).
4 Vgl.: Bank für Internationalen Zahlungsausgleich (2021b).
5 Vgl.: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020PC0595&from=EN.
6 Vgl.: Bundesministerium der Finanzen (2021) – Gesetz zur Stärkung der Finanzmarktintegrität (Finanzmarktintegritätsstärkungsgesetz – FISG)
7 Vgl.: Europäische Kommission (2021)

Bundesbank setzt sich weiterhin für prinzipienorientierte, technologieneutrale, praxisnahe und damit wirksame Aufsicht des digitalen Risikos ein

Die Bundesbank wird sich auf allen Ebenen weiterhin für eine prinzipienorientierte und technologieneutrale Regulierung digitaler Risiken einsetzen. Technischer Fortschritt soll ebenso unterstützt werden wie eine proportionale und eigenverantwortliche Umsetzung der Regulierung in den Instituten. Zudem wird die Bundesbank die Institute weiterhin ermutigen, die Chancen der Digitalisierung entschieden zu ergreifen. Gleichzeitig ist es jedoch erforderlich, dass die Banken das Management der damit einhergehenden Risiken konsequent stärken, um mit den zunehmenden digitalen Risiken Schritt zu halten. Denn nur der eigenständige, souveräne und ausgewogene Umgang der Institute mit den Chancen und Risiken der Digitalisierung kann die Funktionsfähigkeit des Finanzsystems auf Dauer sicherstellen.

Literaturverzeichnis

Bank für Internationalen Zahlungsausgleich (2021a), Revisions to the Principles for the Sound Management of Operational Risk, abrufbar unter: https://www.bis.org/bcbs/publ/d515.pdf.

Bank für Internationalen Zahlungsausgleich (2021b), Principles for operational resilience, abrufbar unter: https://www.bis.org/bcbs/publ/d516.pdf.

Bundesamt für Sicherheit in der Informationstechnik (2021), abgerufen am 25. Mai 2021 unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen_node.html.

Bundesanstalt für Finanzdienstleistungsaufsicht (2018), Orientierungshilfe der BaFin zu Auslagerungen an Cloud-Anbieter.

Bundesministerium der Finanzen (2021), Gesetz zur Stärkung der Finanzmarktintegrität (Finanzmarktintegritätsstärkungsgesetz: FISG), abrufbar unter: https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_VII/19_Legislaturperiode/2021-06-10-FISG/0-Gesetz.html.

Deutsche Bundesbank (2020a), The Use of Artificial Intelligence and Machine Learning in the Financial Sector, abrufbar unter: https://www.bundesbank.de/resource/blob/598256/d7d26167bceb18ee7c0c296902e42162/mL/2020-11-policy-dp-aiml-data.pdf.

Deutsche Bundesbank (2020b), Implementierung von TIBER-DE, 22. Juli 2020, abrufbar unter: https://www.bundesbank.de/resource/blob/842288/2549219ae1fc9f9a9741d0a2317568fc/mL/tiber-implementierung-data.pdf.

Deutsche Bundesbank und Bundesministerium der Finanzen (2019), TIBER-DE macht das deutsche Finanzsystem sicherer, 12. September 2019, abrufbar unter: https://www.bundesbank.de/de/presse/pressenotizen/tiber-de-macht-das-deutsche-finanzsystem-sicherer-806020.

Europäische Kommission (2021), Gesetz über Künstliche Intelligenz, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.

Financial Stability Board (2017), Artificial intelligence and machine learning in financial services.

Mitchell, T. (1997), Machine Learning.

PwC (2021), Cloud-Computing im Bankensektor, abgerufen am 25. Mai 2021 unter: https://www.pwc.de/de/finanzdienstleistungen/cloud-computing-im-bankensektor.html.

statista (2021), abrufbar unter: https://de.statista.com/infografik/20802/weltweiter-marktanteil-von-cloud-infrastruktur-dienstleistern/.