MYRA

RATGEBER FINANCIAL SERVICES

IT-Sicherheit Compliance-gerecht outsourcen

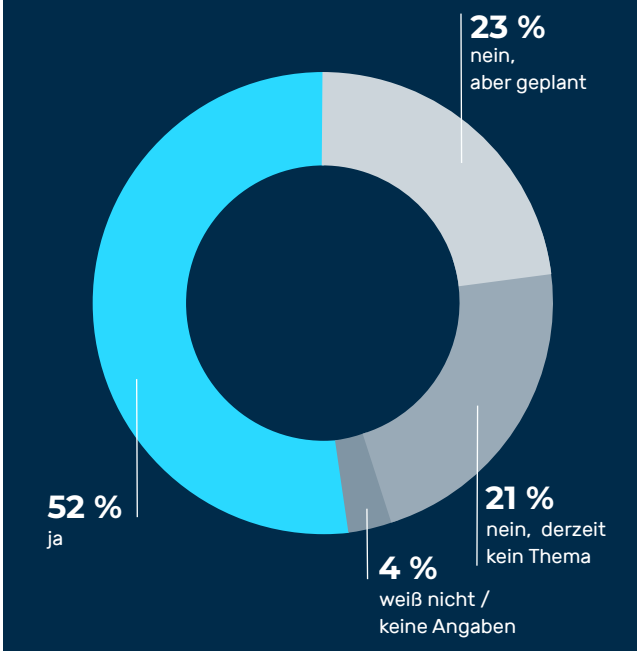
Digitale Herausforderungen in der Finanzindustrie:

- **Verschärfte Bedrohungslage** aufgrund höherer Aktivität der Angreifer bei gleichzeitig immenser Vergrößerung der Angriffsfläche durch die Digitalisierung. Insbesondere Zahl und Intensität von DDoS-Angriffen (Distributed Denial of Service) steigen.
- **Straffere Regulatorik** erfordert höheres Engagement bei IT-Sicherheit, Datenschutz und Compliance
- **Steigender Aufwand,** um Anforderungen an IT-Sicherheit und Compliance bedarfsgerecht zu decken. Umkämpfter Arbeitsmarkt für Security-Spezialisten verschärft diesen Trend.
- **Rechtliche Unsicherheit** beim IT-Outsourcing durch den Wegfall von Privacy Shield

Corona hat die Karten neu gemischt

Die anhaltende Digitalisierung sowie globale wirtschaftliche Umbrüche infolge der Corona-Pandemie sorgen auch in der Finanzindustrie für neue Herausforderungen. Behördlich verordnete Hygienemaßnahmen und Social Distancing erheben Remote Work zum gängigen Standardmodell und auch die Kundschaft verlangt nun vermehrt nach digitalen Produkten und Services.

Cloudnutzung von Finanzdienstleistern
Nutzt ihr Unternehmen gegenwärtig Cloud-Computing? Die Antworten:



Quelle: Sopra Steria Potenzialanalyse Cloud in Europa

Über die Hälfte aller Finanzdienstleister setzt 2020 auf Cloud-Computing, knapp ein Viertel plant die Implementierung.

Parallel zu dieser Entwicklung verschärft sich die virtuelle Bedrohungslage. Cyberkriminelle nutzen die vergrößerte Angriffsfläche zu ihren Gunsten und suchen gezielt nach Schwachstellen in der Cyberabwehr von Banken und Finanzdienstleistern. Das äußert sich unter anderen an einem drastischen Anstieg von DDoS-Angriffen auf Webseiten und Rechenzentren. Myra Security verzeichnete im Jahr 2020 im Vergleich zu 2019 einen Anstieg von DDoS-Angriffen auf Webseiten von über 300 Prozent. Im selben Betrachtungszeitraum verdoppelte sich die Zahl der DDoS-Attacken auf Rechenzentren. Im Visier standen zunehmend größere und zahlungskräftige Unternehmen und Organisationen aus den Bereichen Finanzen und Versicherungen, KRITIS, Behörden und dem Gesundheitswesen. Von diesen Entwicklungen berichten ebenso Aufsichts- und Ermittlungsbehörden wie Interpol[1], BKA[2], BSI[3], BaFin[4] sowie globale Hyperscaler wie Microsoft[5].

Die steigenden Anforderungen an IT-Sicherheit und Datenschutz äußern sich ebenfalls in den regulatorischen Vorgaben von Behörden und der Aufsicht, die zunehmend anspruchsvoller ausfallen. Dieser Trend wird sich auch in Zukunft fortsetzen – insbesondere im Zusammenhang mit kritischen Infrastrukturen. Banken und Finanzdienstleister werden sich daher intensiver mit der internen Datenarchitektur sowie mit Compliance-Themen befassen müssen.

1 Interpol - COVID-19 Cybercrime Analysis Report / August 2020
2 Bundeskriminalamt – Sonderauswertung Cybercrime in Zeiten der Corona-Pandemie / September 2020
3 Bundesamt für Sicherheit in der Informationstechnik - Third edition of the Franco-German commonsituational picture - Influences of COVID-19 on the IT-security situations in France and Germany / Dezember 2020
4 Bundesanstalt für Finanzdienstleistungsaufsicht - BaFinPerspektiven 1 | 2020
5 Microsoft - Digital Defense Report 2020 / September 2020

> *In einer globalisierten Finanzwelt, in der immer mehr Menschen digital bezahlen beziehungsweise Geld transferieren und in der viele Anleger ihre Geldanlage online bestreiten, haben IT-Governance und Informationssicherheit für die Aufsicht inzwischen den gleichen Stellenwert wie die Ausstattung der Institute mit Kapital und Liquidität.*
>
> *BaFin-Exekutivdirektor Raimund Röseler*

Vor diesem Hintergrund gewinnt der Einsatz externer Dienstleister für die Auslagerung digitaler Prozesse weiter an Attraktivität. Institute vermeiden mit dieser Strategie zusätzliche Aufwendungen für Software, Hardware und Personal. Angesichts eines umkämpften Arbeitsmarktes sind hochqualifizierte IT-Fachkräfte ohnehin nur schwer zu finden. Bereits Ende 2019 waren nach Angaben des Digitalverbands Bitkom hierzulande mehr als 100.000 Stellen in diesem Bereich unbesetzt.

Darüber hinaus erfordert das Compliance-gerechte IT-Outsourcing von zentralen Prozessen im Finanzwesen ein besonderes Maß an Expertise. Die von der BaFin definierten Vorgaben für wesentliche Auslagerungen verlangen, dass weder Qualität noch Sicherheit oder Kontinuität durch das IT-Outsourcing eingeschränkt werden. Zudem müssen Kontroll-, Weisungs- und Zugangsrechte vertraglich festgehalten werden.

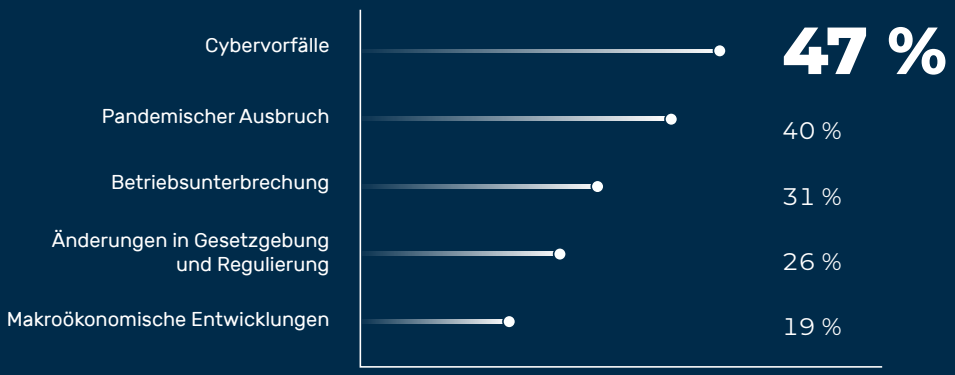
Der vorliegende Ratgeber erläutert die regulatorischen Rahmenbedingungen und zeigt Wege auf, IT-Outsourcing Compliance-gerecht zu gestalten, mit ausgelagerter IT-Security den Sicherheitsstandard zu erhöhen und gleichzeitig den Inhouse-Aufwand zu reduzieren.

Inhalt

Cyberkriminalität: Die Finanzindustrie auf der Abschussliste

Unternehmen aus der Finanzindustrie werden laut einer Untersuchung der Boston Consulting Group[6] 300-mal häufiger attackiert als andere Firmen. Accenture[7] rechnet für die globale Finanzbranche allein zwischen 2019 und 2023 mit Cybercrime-bedingten Verlusten in Höhe von etwa 347 Milliarden US-Dollar. Indessen listet die Allianz in ihrem Risk Barometer für 2021 Cybervorfälle als den größten Risikofaktor für die Finanzindustrie auf[8] – noch vor Betriebsausfällen und pandemischen Ausbrüchen.

Top 5 Geschäftsrisiken für die Finanzindustrie



Methodik: Die Zahlen geben an, wie oft ein Risiko als Prozentsatz aller Antworten ausgewählt wurde. Mehrfachnennungen von bis zu drei Risiken waren möglich. Befragt wurden über 900 Unternehmen aus der Finanzindustrie.
Quelle: Allianz Risk Barometer 2021 Appendix

Diese verschärfte Bedrohungslandschaft resultiert unter anderem aus der sukzessiven Digitalisierung des Finanzwesens. In den vergangenen Jahren wurden die Assets immer digitaler. Das klassische Bankengeschäft wurde um digitale Lösungen für Banking, Zahlungstransfer, Vermögensanlage und vieles mehr erweitert. Damit stieg auch die Zahl an wertvollen Datensätzen und Geschäftsprozessen, die das Interesse von Cyberkriminellen wecken. Auf illegalen Marktplätzen im Darknet werden Daten von Finanzdiensten und Payment-Anbietern zu Höchstpreisen gehandelt.

> *Seit Jahresbeginn hat es eine erstaunliche Häufung von DDoS-Attacken auf Finanzinstitute gegeben.*
>
> *Felix Hufeld, ehemaliger BaFin-Präsident - BaFin Perspektiven 1|2020*

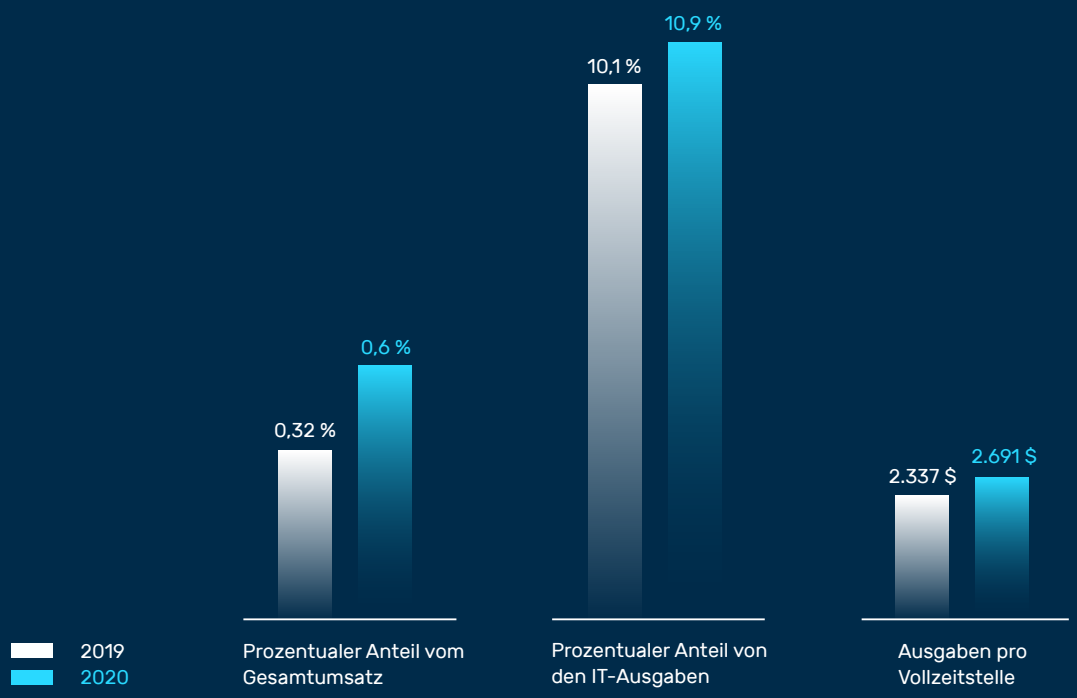
Diese konkreten Bedrohungen gefährden die Sicherheit und Verlässlichkeit digitaler Prozesse in der gesamten Finanzbranche massiv – vom Fintech-Start-up bis hin zur Großbank.

Den Aufsichtsbehörden ist die angespannte Sicherheitslage im digitalen Raum ebenfalls bewusst. Wie der ehemalige BaFin-Chef Felix Hufeld in einem Interview Mitte 2020 erläuterte, habe vor allem die Zahl der DDoS-Attacken auf Finanzinstitute signifikant zugenommen. Der Einsatz umfassender Schutzsysteme ist erforderlich, um auf die angespannte Bedrohungslage zu reagieren.

6 Boston Consulting Group - Global Wealth 2019 - Reigniting Radical Growth / Juni 2019
7 Accenture - 2019 Financial Services Cost of Cyber Crime Study / März 2019
8 Allianz Global Corporate & Specialty - Allianz Risk Barometer 2021 / Januar 2021

Banken müssen daher ihre Cyberresilienz stärken, indem sie besondere Maßnahmen zur Schaffung und Erhaltung ihrer Widerstandsfähigkeit gegen Angriffe auf die Sicherheit ihrer Informations- und Kommunikationstechnik ergreifen. So gibt der Finanzsektor laut einer aktuellen Deloitte-Studie bereits etwa 10 Prozent des IT-Budgets für Cybersecurity aus[9]. Dies entspricht rund 2.700 US-Dollar je Mitarbeiter und Jahr.

Ausgaben für Cybersicherheit in der Finanzindustrie



Quelle: FS-ISAC / Deloitte Cyber & Strategic Risk Services CISO survey reports, 2019 and 2020; Deloitte Center for Financial Services analysis.

IT-Outsourcing liegt bei Banken im Trend – trotz zunehmender Regulierung

Nur wenige Konzerne sind heutzutage in der Lage, alle Digitalisierungsbemühungen komplett inhouse zu bedienen. Selbst große Banken und Finanzdienstleister, bei denen die Voraussetzungen dafür gegeben sind, tendieren zum Outsourcing von Prozessen an Spezialdienstleister in der Cloud. Die Vorteile liegen auf der Hand: direkte Aufwendungen für Betrieb, Personal, Hardware und Software fallen weg, wodurch weitere Ressourcen für das Kerngeschäft frei werden. Außerdem punkten Cloud Services mit strategischer Flexibilität und hoher Skalierbarkeit.

Angesichts eines leergefegten Arbeitsmarktes für hochqualifizierte IT-Fachkräfte gewinnt der Einsatz externer IT-Dienstleister weiter an Attraktivität. Dies gilt ganz besonders für den Bereich IT-Security. Es wird erwartet, dass bis 2022 im Bereich Cybersicherheit weltweit 1,8 Millionen Fachkräfte fehlen werden[10].

Aufgrund der steigenden Anforderungen an IT-Sicherheit und Datenschutz werden auch die regulatorischen Vorgaben von Aufsichtsbehörden zunehmend anspruchsvoller. Banken und Finanzdienstleister müssen sich daher intensiver denn je mit der eigenen IT-Architektur sowie mit Compliance-Themen befassen.

9 Deloitte - Reshaping the cybersecurity landscape / Juli 2020
https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html
10 ISC - Global Information Security Workforce Study (GISWS) / Februar 2017

IT-Outsourcing ja, aber wie?

Unternehmen in der Finanzindustrie, die eine Auslagerung von IT-Services planen, müssen viele Punkte beachten. Die BaFin hat mit ihren Bankaufsichtlichen Anforderungen an die IT (BAIT) klargestellt, wie beaufsichtigte Finanzunternehmen ihre Geschäftsorganisation im Hinblick auf Informationssicherheit zu gestalten haben. Beim Wechsel in ein Outsourcing-Modell spielen neben technischen daher auch regulatorische Faktoren eine zentrale Rolle.

Hohe Compliance-Anforderungen zum Schutz von Daten und IT-Infrastrukturen

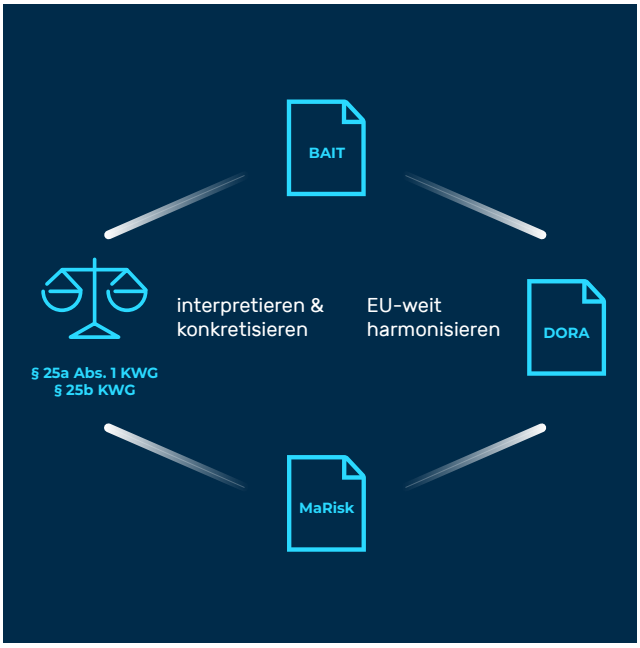
Speziell in der Finanzindustrie sind die aufsichtsrechtlichen Anforderungen an digitale Systeme und Prozesse immens. Um die Banken-IT Compliance-konform nach den Anforderungen von KWG, MaRisk, BAIT und bald auch DORA abzusichern, bedarf es höchsten Know-hows und verlässlicher Technologie. Außerdem sind die Datenschutz-Grundverordnung (DSGVO) und das IT-Sicherheitsgesetz (IT-SiG) zu beachten.

Institute, die bestimmte Schwellenwerte an Transaktionen überschreiten, zählen zu den Kritischen Infrastrukturen (KRITIS), für die nochmals höhere Vorgaben an die IT-Sicherheit gelten. Sie müssen regelmäßig nachweisen, alle verfügbaren Optionen der Cybersicherheit zum Schutz ihrer Systeme einzusetzen, um Integrität, Verfügbarkeit, Authentizität sowie Vertraulichkeit der Daten angemessen sicherzustellen.

Verletzen Finanzunternehmen die regulatorischen Vorgaben für Datensicherheit und Datenschutz, drohen drastische Geldstrafen von bis zu 20 Millionen Euro oder bis zu 4 Prozent des weltweit erzielten Jahresumsatzes. Geraten sensible Kundendaten aufgrund von Fahrlässigkeit in die falschen Hände, können verantwortliche Führungskräfte mit Geld- und sogar Freiheitsstrafen belegt werden.

BAIT und MaRisk definieren Compliance-Rahmen für das IT-Outsourcing

Die BaFin gibt in den MaRisk und den davon abgeleiteten BAIT ein striktes Regelwerk vor, das Banken und Finanzdienstleister beim Outsourcing von Prozessen zu befolgen haben. Zukünftig soll zudem DORA (Digital Operational Resilience Act) als aufsichtsrechtliche Adaption auf europäischer Ebene zur Geltung kommen.

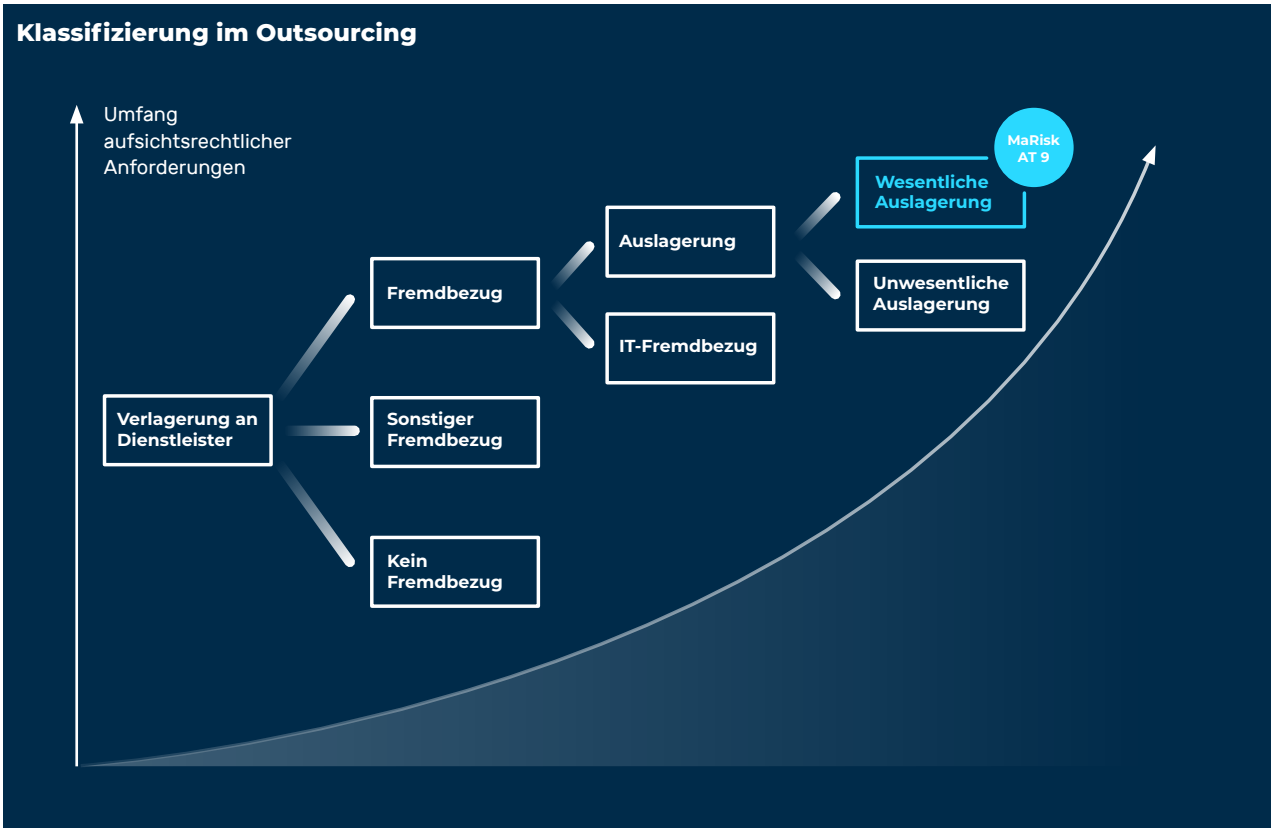


MaRisk und BAIT interpretieren und konkretisieren gleichermaßen die gesetzlichen Anforderungen aus dem KWG (§ 25a Abs. 1/ § 25b). Zielsetzung von DORA ist wiederum, übergeordnet einheitliche Vorgaben für die Finanzindustrie zu definieren. Die existierende Regulierung soll dabei unter Wahrung der Verhältnismäßigkeit auf europäischer Ebene harmonisiert werden.

Die Regularien schreiben unter anderem vor, dass ausgelagerte Aktivitäten in das Risikomanagement des auslagernden Institutes einbezogen werden müssen. Vor allem für die sogenannten wesentlichen Auslagerungen gelten besondere Vorgaben.

In den MaRisk sind Auslagerungen als „Aktivitäten und Prozesse im Zusammenhang mit der Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen“ definiert, die sonst vom jeweiligen Institut selbst bereitgestellt werden. Eine Auslagerung liegt nur vor, wenn die ausgelagerten Aktivitäten und Prozesse im Zusammenhang mit der Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen stehen und wesentlich im Sinne von § 25b Abs. 1 KWG sind. Gemäß § 25b KWG sollen Institute unabhängig von der jeweiligen Art einer Auslagerung angemessene Vorkehrungen zur Risikovermeidung in diesen Bereichen treffen.

Eine wesentliche Auslagerung von IT darf erfolgen, wenn sie die Anforderungen nach § 25 KWG und MaRisk AT 9 erfüllt. Der Entscheidungsbaum in der folgenden Abbildung veranschaulicht die Klassifizierung externer Leistungen nach MaRisk.



Die Compliance-konforme Klassifizierung von externen Dienstleistungen ist durch die BaFin geregelt. Je bedeutender der zu verlagernde Prozess für das Institut ausfällt, desto umfangreicher sind in der Regel die regulatorischen Anforderungen.

Risikoanalyse bildet Grundlage für das IT-Outsourcing

Auf Grundlage einer Risikoanalyse muss das Finanzinstitut ermitteln, ob es sich beim jeweiligen Outsourcing um eine wesentliche Auslagerung handelt, also um Dienste, die eigenverantwortlich vom Institut unter Risikogesichtspunkten als wesentlich definiert sind. Diese Analyse muss im Vorfeld der Auslagerung durchgeführt werden und sollte laut der BaFin[11] folgende Themen behandeln:

- **Ausgestaltung des genutzten Dienstes**
- **Kritikalität des auszulagernden Prozesses**
- **Risikobewertung in Bezug auf Dienstleistungs- und Bereitstellungsmodell**
- **Standort des Dienstleisters** (vor allem hinsichtlich möglicher Aufsichtsbeschränkungen, Risiken aufgrund der geopolitischen Lage sowie geltende Gesetzgebung zu Sicherheit und Datenschutz)
- **Eignung des jeweiligen Anbieters** (nachweisbar über relevante Sicherheitsstandards wie ISO 27001 oder BSI-C5)
- **Risiken für Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität von Prozessen und Daten**
- **Risiken durch Weiterverlagerungen**

11 BaFin-Merkblatt - Orientierungshilfe zu Auslagerungen an Cloud-Anbieter / November 2018

MaRisk wie auch BAIT folgen den Grundsätzen der Proportionalität und der Methodenfreiheit. Banken und Finanzdienstleister können damit die regulatorischen Vorgaben bedarfsgerecht umsetzen. Durch die einzelnen Novellierungen von MaRisk sowie BAIT erweitert und optimiert die BaFin die einschlägigen Regelwerke sukzessive, etwa um die Vorgaben der EBA einfließen zu lassen. Für Finanzunternehmen und angeschlossene Dienstleister sind solche Überarbeitungen oftmals mit strikteren Compliance-Vorgaben verknüpft. So wurden etwa in der kommenden MaRisk Novelle 2021 weitere Anforderungen zur Risikoanalyse und zur Bestimmung der Wesentlichkeit sowie zur Ausgestaltung des Auslagerungsvertrages und zur Steuerung und Überwachung der Risiken von Auslagerungsvereinbarungen aufgenommen beziehungsweise präzisiert.

Um die dauerhafte Einhaltung der regulatorischen Vorgaben sicherzustellen, sollten Risikoanalysen regelmäßig erneuert werden. Nur so können Änderungen, etwa durch eine neue Gesetzgebung, in laufenden Auslagerungen berücksichtigt werden. Die BaFin empfiehlt daher, die Risikoanalyse im Fall von wesentlichen Auslagerungen jährlich zu erneuern, während bei unwesentlichen Auslagerungen eine erneute Analyse alle drei Jahre ausreicht.

Höchste Anforderungen an Dienstleister

Um die regulatorischen Vorgaben für wesentliche Auslagerungen zu erfüllen, müssen Finanzinstitute ihre Dienstleister mit größter Sorgfalt auswählen. Die strikten Anforderungen an die zu erbringenden Leistungen gilt es gemäß MaRisk von den beauftragten Unternehmen zudem laufend zu überprüfen.

Nachweise, Zertifikate und Prüfberichte: Gängige Standards belegen Qualität

Dienstleister belegen ihre Tauglichkeit etwa durch Nachweise, Zertifikate und Prüfberichte. Wer wichtige Sicherheitsstandards wie ISO 27001 auf auf Basis von IT-Grundschutz oder BSI-C5 erfüllt und die notwendige Branchenexpertise mitbringt, eignet sich in aller Regel auch als Partner für das Outsourcing digitaler Geschäftsprozesse – insbesondere, wenn diese als wesentliche Auslagerung gelten.

Rechtsunsicherheit bei außereuropäischen Partnern

Mit dem Wegfall des Privacy-Shield-Abkommens für den transatlantischen Datentransfer zwischen Europa und den USA stehen Kooperationen mit US-Anbietern auf wackeligen Beinen. Rechtssichere Datentransfers sind aufgrund der konträren Positionierung von europäischer DSGVO und US-Recht nur schwer umzusetzen. Durch die Wahl lokaler Anbieter, die derselben Rechtsprechung unterliegen, lassen sich solche Hürden umgehen.

Grundprinzip: Verantwortlichkeit lässt sich nicht outsourcen

Die BaFin stellt klar: Trotz der Auslagerung zentraler Prozesse an externe Dienstleister bleibt die Verantwortung stets bei der Geschäftsleitung des Auftraggebers erhalten. „Die Auslagerung darf nicht zu einer Delegation der Verantwortung der Geschäftsleitung an das Auslagerungsunternehmen führen“, heißt es dazu in den MaRisk AT9. Ergänzend mahnt die kommende Novellierung, dass Institute durch übermäßiges Outsourcing nicht zu einer leeren Hülle verkommen dürfen.

Compliance-konforme Vertragsgestaltung für das IT-Outsourcing

Der Auslagerungsvertrag bildet die Basis für ein zukunftsfähiges und Compliance-konformes Outsourcing digitaler Prozesse. Hier werden für alle beteiligten Parteien - vom auslagernden Institut selbst, über den angeschlossenen Dienstleister bis hin zu etwaigen Subunternehmern - sämtliche relevanten Rechte und Pflichten verbindlich fixiert.

Um die Qualität und Beständigkeit der ausgelagerten Prozesse formell abzusichern, sind unter anderem die zu erbringenden Leistungen, Prüf- und Weisungsrechte, Zutrittsrechte, Kündigungsfristen, das Exitmanagement sowie die genehmigten Subauftragnehmer festzulegen.

Aufgrund der immensen Bedeutung, die der Auslagerungsvertrag für ein erfolgreiches Outsourcing hat, soll auf den folgenden Seiten im Detail auf die relevantesten Punkte bei der Vertragsgestaltung eingegangen werden, wie sie die BaFin vorsieht.[12]

Ermittlung des Leistungsgegenstands

Service Level Agreements sichern messbare Qualitätskriterien beim IT-Outsourcing und regeln damit Art und Umfang der zu erbringenden Leistung. Inhaltlich gilt es dabei, grundsätzlich folgende Punkte zu adressieren:

- Welche Prozesse sollen wie ausgelagert werden? (Art der Dienstleistung, Bereitstellung, Umfang wie beispielsweise Performance, Verfügbarkeit, Storage, Reaktionszeiten oder Support)
- Konkrete Zuständigkeiten für Mitwirkungs- und Bereitstellungspflichten (Aktualisierungen)
- Woher soll der Service bezogen werden? (Standort der Rechenzentren)
- Vertragsbeginn und Ende
- Benchmarks und KPIs zur Prüfung des Dienstleistungsniveaus
- Grenzwerte zur Feststellung eines unannehmbaren Dienstleistungsniveaus

Exitmanagement

Das Exitmanagement muss bereits bei der Planung des Outsourcing-Projekts mit berücksichtigt werden. Speziell im Hinblick auf Cloud-Services sind klar definierte Rechte, Pflichten und Verantwortlichkeiten beider Parteien festzulegen, um Lock-in-Effekte zu vermeiden und einen reibungslosen Providerwechsel am Ende der Vertragslaufzeit zu ermöglichen. Auch eine Rückführung des ausgelagerten Prozesses zurück zum Institut muss grundsätzlich möglich bleiben. Daneben gilt es auch Szenarien wie eine Insolvenz des Dienstleisters oder dessen Übernahme durch ein anderes Unternehmen zu beachten. Vertragliche Details sind dafür in einem separaten Exit-Plan festzulegen. Ein solcher Plan regelt:

- Exit-Leistungen, die ein Providerwechsel oder eine Rückführung erforderlich machen (Kooperationsvereinbarungen mit neuen Anbietern, Weitergabe von Informationen und Dokumenten, Mitarbeiterschulungen, Übertragung von Subunternehmer-Verträgen oder weiterführende Nutzungsrechte über das Vertragsende hinaus)
- Ausreichende Reserve an vorgesehenen Projekttagen, um unvorhersehbare Probleme zu lösen
- Welche Exit-Leistungen gesondert zu vergüten und welche inbegriffen sind
- Welche Assets im Detail zu übertragen sind (etwa Verträge mit Subunternehmern)

Informations- und Prüfungsrechte des auslagernden Instituts

Auch beim IT-Outsourcing dürfen Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten von Banken vertraglich nicht eingeschränkt werden. Daher muss gewährleistet sein, dass das auslagernde Institut die erforderlichen Daten erhält, die zur Steuerung und Überwachung der verbundenen Risiken erforderlich sind.

Um die Einhaltung von Informations- und Prüfungsrechten sicherzustellen, sind mehrere

12 MaRisk AT 9 Ziffer 7

Punkte vertraglich zu fixieren. So muss etwa ein uneingeschränkter Zugriff auf Daten und Informationen bestehen, die bei der Leistungserbringung anfallen. Daneben sollte auch Zugang zu den Geschäftsräumen und Rechenzentren des Anbieters bestehen, von wo aus die Leistung erbracht wird. Das schließt auch die einzelnen eingesetzten Geräte, Systeme, Netzwerke und Prozesse. Insgesamt müssen über die gesamte Auslagerungskette hinweg effektive Kontroll- und Prüfungsmöglichkeiten bestehen – das umfasst auch die mögliche Durchführung von Vor-Ort-Prüfungen beim Provider und gegebenenfalls dessen Dienstleistern.

Achtung: Rechte dürfen nicht per Klauseln eingeschränkt werden

Als unerlaubte „(mittelbare) Einschränkung der Rechte" definiert die BaFin insbesondere vertragliche Vereinbarungen zwischen den Parteien, die Informations- und Prüfungsrechten nur unter bestimmten Voraussetzungen festlegen, etwa:

- Vereinbarung, die eine Priorisierung von Prüfungsberichten, Zertifikaten und anderen Qualitätsnachweisen des Providers vor den Prüfungen des Instituts vorsehen.
- Die Beschränkung von Informations- und Prüfungsrechte auf eine reine Vorlage von Prüfungsberichten, Zertifikaten und anderen Standard-Qualitätsnachweisen des Providers.
- Schulungsklauseln für den Zugang zu Informationen
- Klauseln, die Prüfungen anhand von wirtschaftlicher Zumutbarkeit abhängig machen
- Personelle oder zeitliche Beschränkungen für Prüfungen (Verweise auf Anmeldung und übliche Geschäftszeiten sind vertretbar)
- Beschränkung der Informations- und Prüfungsrechte auf Managementkonsolen und ähnlichen Tools
- Konkrete Vorgaben für Ablauf und Umfang der Prüfungen

Erleichterungen bei der Prüfung

Für eine effiziente Prüfungshandlung dürfen Unternehmen auch auf Sammelprüfungen oder gängige Qualitätsstandards wie einschlägige Zertifikate oder Prüfberichte anerkannter Dritter zurückgreifen. Das schließt ebenfalls interne Prüfberichte des Dienstleisters mit ein.

Alle Erleichterungen dieser Art müssen allerdings im Rahmen der aufsichtsrechtlichen Vorgaben erfolgen.

Nachweise, Zertifikate und Prüfberichte: auf gängige Standards achten

Auslagernde Institute sollten grundsätzlich Nachweise, Zertifikate und Prüfberichte bezüglich des IT-Outsourcings nachweisen können. Im Fokus stehen dabei gängige Sicherheitsstandards wie ISO 27001 auf Basis von IT-Grundschutz oder der C5-Anforderungskatalog des BSI. Prüfberichte anerkannter Dritter oder interne Prüfberichte des Providers sind ebenfalls wünschenswert. Immer zu berücksichtigen sind bei allen Nachweisen Umfang, Detailtiefe, Aktualität und Eignung des Zertifizierers oder Prüfers.

Durch den Auslagerungsvertrag müssen Zugang zu Geschäftsräumen, Rechenzentren und Arbeitsgeräten des Dienstleisters sowie die Möglichkeit von Vor-Ort-Prüfungen gewährleistet sein.

Informations- und Prüfungsrechte der BaFin

Die Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten auf Seiten der BaFin orientieren sich an denen des auslagernden Instituts und dürfen vertraglich ebenso wenig eingeschränkt werden. Vielmehr müssen der BaFin dieselben Möglichkeiten zur Kontrolle des Dienstleisters zur Verfügung stehen, wie sie gesetzlich auch für das beaufsichtigte Institut vorgesehen sind. Um diesen Sachverhalt vertraglich festzusetzen, sollte der Provider zur uneingeschränkten Zusammenarbeit mit der Aufsicht verpflichtet werden. Ferner müssen Datenzugriff, Zugang zu Geschäftsräumen, Rechenzentren und Arbeitsgeräten sowie die Möglichkeit von Vor-Ort-Prüfungen gewährleistet sein. Ziel ist es dabei, der Aufsicht eine effektive Kontroll- und Prüfungsmöglichkeiten der gesamten Auslagerungskette zu sichern. Im Falle einer Weiterverlagerung müssen sämtliche Punkte natürlich auch für den Subdienstleister geltend gemacht

werden. Darüber hinaus ist bei den Informations- und Prüfungsrechten der BaFin ebenfalls keine (mittelbare) Einschränkung der Rechte zulässig.

Weisungsrechte sichern Kontrolle und Datenhoheit

Durch die vertragliche Definition von Weisungsrechten bleiben Instituten auch beim Outsourcing die notwendigen Steuermöglichkeiten über den ausgelagerten Prozess erhalten. Die Weisungsrechte sollten auch Nachweise und Zertifizierungen einschließen, damit eine Einflussnahme auf Art und Umfang möglich bleibt. Auf diese Weise können beispielsweise Prüfberichte um relevante Systeme erweitert werden.

Von großer Bedeutung ist auch die vertragliche Sicherung der Datenhoheit. Das auslagernde Institut muss jederzeit befugt sein, auf die im Rahmen der Auslagerung verarbeiteten Daten zuzugreifen oder deren Löschung beziehungsweise Sperrung anzuordnen. Daneben sollte auch eine unbeschränkte und unverzügliche Rückführung der Daten vom Dienstleister zurück zum Institut möglich sein.

Außerdem sollte das beaufsichtigte Institut jederzeit zur Erteilung von Weisungen an den Provider in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten befugt sein und der Provider die Daten nur im Rahmen der erteilten Weisungen des beaufsichtigten Unternehmens erheben, verarbeiten oder nutzen dürfen. Davon umfasst sein sollte auch die Möglichkeit zur jederzeitigen Erteilung einer Weisung zur unverzüglichen und unbeschränkten Rücküberführung der vom Dienstleister verarbeiteten Daten an das beaufsichtigte Institut.

Datensicherheit und Datenschutz

Im Auslagerungsvertrag sind Regeln zu vereinbaren, die die Einhaltung rechtlicher Bestimmungen hinsichtlich Datensicherheit und Datenschutz sicherstellen. So muss dem Institut etwa der Ort der Datenspeicherung beziehungsweise des Rechenzentrums bekannt sein. Laut BaFin genügt hier grundsätzlich die Ortsangabe. Falls durch das Risikomanagement erforderlich, muss aber auch die genaue Anschrift vom Provider ausgegeben werden. Darüber hinaus sieht die Aufsicht vor, dass Daten und Systeme von ausgelagerten Prozessen redundant abgesichert sind, damit lokale Ausfälle in Rechenzentren keinen Einfluss auf die Verfügbarkeit haben.

Wie schon im Kapitel zu Weisungsrechten erläutert, muss auch die Datenhoheit vertraglich festgeschrieben sein. Speziell bei der Rückführung von Daten gilt es sicherzustellen, dass ein solcher Prozess die Verwendbarkeit der Daten nicht einschränkt oder unmöglich macht. Daher empfiehlt sich die Nutzung von plattformunabhängigen Standardformaten, die Kompatibilität zu unterschiedlichen Systemen aufweisen.

Kündigungsmodalitäten

Die Regelung von Kündigungsrechten und angemessene Kündigungsfristen muss ebenfalls vertraglich vereinbart sein. Insbesondere gilt es Sonderkündigungsrechte zu vereinbaren, die einen Ausstieg aus dem Vertragsverhältnis aus triftigen Gründen vorsieht – etwa auf Anweisung von Aufsichtsbehörden. Bei einer Kündigung muss der nahtlose Übergang zu einem anderen Provider oder eine Rückführung des jeweiligen Prozesses in das Institut gewährleistet sein. Außerdem muss festgeschrieben sein, in welcher Art, Form und Qualität der ausgelagerte Prozess und insbesondere die dazugehörigen Daten samt Dokumentation übergeben werden. Ferner sind die Übergabe der Auslagerungsdaten nach Vertragsbeendigung und die Übergabe derselben vertraglich zu fixieren.

Weiterverlagerung

Der Einsatz von Subdienstleistern für die sogenannte Weiterverlagerung von Prozessen und Daten sollte auch vertraglich geregelt sein, um sicherzustellen, dass in einem solchen Falle ebenso die aufsichtsrechtlichen Anforderungen eingehalten werden. Dabei ist besonders darauf zu achten, dass die erforderlichen Informations- und Prüfungsrechte sowie Kontrollmöglichkeiten durch das Institut und die BaFin weiterhin gegeben sind. Zudem sollten Zustimmungsvorbehalte oder konkrete Voraussetzungen für Weiterverlagerungen vereinbart werden. Im Zuge neuer Weiterverlagerungen empfiehlt die BaFin außerdem eine Überprüfung der vorgenommenen Risikoanalyse.

Informationspflichten

Störungen und andere Ereignisse, die Einfluss auf den ausgelagerten Prozess haben könnten, müssen vom Dienstleister umgehend an das Institut gemeldet werden. Über relevante Änderungen an den zu erbringenden Diensten sollte der Dienstleister vorab informieren. Diese Informationspflichten gilt es, vertraglich festzuhalten.

Anwendbares Recht

Um die Rechtssicherheit sicherzustellen, sollte für die vertragliche Rechtswahlklausel nach Möglichkeit das deutsche Recht oder zumindest das Recht eines Staates der Europäischen Union bzw. des Europäischen Wirtschaftsraums festgelegt sein.

MaRisk Novelle 2021

Auslagerungsbeauftragter & Auslagerungsmanagement für komplexes Outsourcing

Die anstehende MaRisk Novelle 2021 sieht vor, dass jedes Institut, das Auslagerungen vornimmt, einen zentralen Auslagerungsbeauftragten ernennen muss. Dieser ist der Geschäftsführung direkt unterstellt und kümmert sich um die sukzessive Weiterentwicklung des Auslagerungsmanagements mitsamt der darin enthaltenen Kontroll- und Überwachungsfunktionen.

Speziell große Institute, die viele Auslagerungen zu verwalten haben, kamen schon bisher um ein zentrales Auslagerungsmanagement nicht herum – dieses dient als Unterstützung für den Auslagerungsbeauftragten. Hier müssen für die Aufsicht jährlich Berichte erstellt werden, die alle wesentlichen Auslagerungen festhalten. Ferner sind Institute zu entsprechenden Kontroll- und Überwachungsprozessen verpflichtet. Eine kontinuierliche Dokumentation sowie die Koordination und Überprüfung der durchgeführten Risikoanalysen sind ebenso sicherzustellen.

Das zentrale Auslagerungsmanagement bringt vor allem bei der Weiterverlagerung Vorteile, mit der in der Praxis viele Institute konfrontiert sind. Wer auch bei komplexen Outsourcing-Strukturen mit diversen Dienstleistern, Subunternehmen und Abhängigkeiten die Kontrolle behält, kann strategische Anpassungen agil vornehmen, um auf Marktveränderungen zu reagieren. So können Banken und Finanzdienstleister auch in Krisensituationen wie der aktuellen Corona-Pandemie sicherstellen, dass ihre Partner im Stande sind, die zugesicherten Leistungen zu erbringen.

Aufbau und Pflege eines aktuellen Auslagerungsregisters mit Informationen über alle Auslagerungs-vereinbarungen mitsamt als wesentlich eingestufter Weiterverlagerungen sind ebenfalls in der MaRisk Novelle 2021 vorgesehen.

Erleichterungen für Gruppen und Finanzverbünde im Rahmen der MaRisk Novelle 2021

Der aktuelle Entwurf für die kommende MaRisk Novelle 2021 sieht zudem eine Reihe von regulatorischen Erleichterungen für Gruppen und Finanzverbünde vor. So besteht für diese etwa die Möglichkeit, ein zentrales Auslagerungsmanagement auf Gruppen- oder Verbundebene aufzubauen. Ferner soll das verbundinterne Auslagern von Risikocontrolling, Compliance und der internen Revision auf Schwesterinstitute innerhalb einer Institutsgruppe bei Vorliegen bestimmter Voraussetzungen möglich sein. Risikomindernd lassen sich ebenso ein einheitliches Risikomanagement sowie übergreifende Durchgriffsrechte im Rahmen der Risikoanalyse berücksichtigen.

IT-Security und Outsourcing-Compliance: Eine Sache für Experten

Wie kaum ein anderer Sektor wird die Finanzbranche vom Bedürfnis nach Cybersicherheit bestimmt. Zu Recht haben die Aufsichtsbehörden die Compliance bei der Auslagerung entsprechender IT-Security-Leistungen an externe Anbieter streng geregelt.

Auf Cybersicherheit spezialisierte Dienstleister, die über eine hochgradige Kompetenz in Sachen Aus-lagerungs-Compliance verfügen, können Banken und Finanzdienstleister gezielt und effizient unterstützen. Denn nur sie sind in der Lage, eine vollständige Erfüllung der regulatorischen Anforderungen im Outsourcing sicherzustellen und die Bedürfnisse nach Cybersicherheit und Compliance gleichermaßen abzudecken.

Glossar IT-Outsourcing & IT-Security im Finanzwesen

BAIT: Bankaufsichtliche Anforderungen an die IT. Richtlinie der BaFin.

C5: Anforderungskatalog Cloud Computing. Dabei handelt es sich um Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten, aufgestellt vom BSI.

DORA: Der Digital Operational Resilience Act sieht die Einführung eines umfassenden Rechtsrahmens auf EU-Ebene vor, der Vorschriften zur digitalen Betriebsstabilität für alle beaufsichtigten Finanzinstitute enthält. Im Kern zielt DORA dabei auf eine EU-weite Harmonisierung der geltenden Regulatorik ab. Daher umfasst der Anforderungskatalog im Wesentlichen die Vorgaben aus bekannten Regelwerken wie die EBA-Leitlinien, MaRisk oder auch BAIT.

Exitmanagement: Die Beendigung der Auslagerung bzw. der Wechsel zu einem anderen Anbieter ist bereits bei der Vertragsgestaltung zu regeln und die Modalitäten sind in einem Exit-Plan festzuhalten.

Fremdbezug bzw. sonstiger Fremdbezug: Nicht als Auslagerung im Sinne von MaRisk AT 9 einzustufen ist der sonstige Fremdbezug von Leistungen. Hierzu zählt der einmalige oder gelegentliche Fremdbezug von Gütern und Dienstleistungen sowie der Fremdbezug von Leistungen, die typischerweise vom Institut nicht selbst erbracht werden. Die angemessene Risikobehandlung sowie die Sicherstellung der Ordnungsmäßigkeit der Geschäftsorganisation gilt auch beim sonstigen Fremdbezug von Leistungen gemäß § 25a Abs. 1 KWG.

ISO 27001: Die Norm spezifiziert die Anforderungen an Aufbau, Umsetzung, Betrieb, Überwachung, Bewertung, Wartung und Verbesserung von dokumentierten Informationssicherheitsmanagementsystemen (ISMS) in Bezug auf die allgemeinen Geschäftsrisiken. Die Norm verfolgt einen Top-Down-Ansatz, bei dem die Prozesse im Mittelpunkt stehen und die notwendigen Sicherheitsmaßnahmen auf Basis einer individuellen Risikoanalyse implementiert werden.

KRITIS: Akronym für Kritische Infrastrukturen. Dabei handelt es sich um Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen.

KWG: Kreditwesengesetz. Sein Zweck ist die Marktregulierung für Banken und Finanzdienstleister.

MaRisk (BA): Akronym für Mindestanforderungen an das Risikomanagement (BA für Bankenaufsicht). Es handelt sich um Verwaltungsanweisungen der BaFin, die verbindliche Vorgaben für das Risiko-management deutscher Kreditinstitute machen. Die MaRisk konkretisieren den § 25a KWG und sind die Umsetzung der qualitativen Anforderungen aus Basel II bzw. Basel III an das Risikocontrolling von Banken.

MaRisk AT 9: Allgemeiner Teil 9 der MaRisk-Regularien. Neben AT 9 definieren auch BAIT & §25b KWG die aufsichtsrechtlichen Vorgaben für Auslagerungen. Inhaltlich sind diese am ausführlichsten in MaRisk abgebildet.

SLA: Service Level Agreement. Bezeichnet in der Regel einen Rahmenvertrag, in dem wiederkehrende Dienstleistungen vereinbart und geregelt werden.

Weiterverlagerung: Weitergabe der Ausführung von Leistungen durch einen Subunternehmer. Nach MaRisk AT 9 ist vertraglich sicherzustellen, dass die Vereinbarungen des Auslagerungsunternehmens mit Subunternehmen im Einklang mit den vertraglichen Vereinbarungen des originären Auslagerungsvertrags stehen.

Wesentliche Auslagerung: Wesentliche Auslagerungen im Sinne von MaRisk AT 9 sind Dienste, die eigenverantwortlich vom Institut unter Risikogesichtspunkten als wesentlich definiert sind.

Das macht Myra zum richtigen Partner für die Finanzindustrie

- Revisionssicher: Myra erfüllt alle Anforderung an die wesentliche Auslagerung nach KWG § 25, MaRisk AT9 und BAIT
- Investitionssichere Technologie: vollautomatische Angriffsmitigation, hochperformante Auslieferung, maximale Skalierbarkeit
- DSGVO-konformer Spezialanbieter mit Branchenexpertise
- Myra erfüllt bereits jetzt die meisten Anforderungen des geplanten EU Digital Operational Resilience Act (DORA) an Risikomanagement, Reporting, Testing und Auslagerung
- Hochzertifizierte Qualität: ISO 27001 auf Basis von IT-Grundschutz, PCI-DSS-zertifiziert, IDW PS 951 Typ 2 (ISAE 3402) geprüft, BSI-KRITIS-qualifiziert, BSI-C5-Testat (in Arbeit), Trusted Cloud.

Erstklassige Service-Qualität dank zertifizierter Sicherheit

Als Spezialanbieter im Finanzsektor und in anderen sensiblen Bereichen ist es für Myra selbstverständlich, dieselben strengen Anforderungen zu erfüllen wie seine Kunden. Die umfassenden Zertifizierungen von Myra gehen weit über das normale Maß hinaus und sorgen dafür, dass seine Kunden bei Sicherheit und Compliance das Maximum erreichen. Myra ist hochzertifiziert und erfüllt alle 37 Kriterien des BSI für qualifizierte KRITIS-Sicherheitsdienstleister. Damit setzen wir den Maßstab in der IT-Sicherheit.

ISO 27001 BSI zertifiziert auf der Basis von IT-Grundschutz Zertifikat Nr.: BSI-IGZ-0479-2021 | PCI DSS Certified | BSIG KRITIS-qualifiziert | EU-DSGVO konform | BSI C5 TESTAT | Trusted Cloud | CERTIFIED IDW PS 951 ISAE 3402

Zertifiziert vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz | Zertifiziert nach Payment Card Industry Data Security Standard | KRITIS-qualifiziert nach §3 BSI-Gesetz | Konform mit der (EU) 2016/679 Datenschutz-Grundverordnung | BSI-C5-Testat (in Kürze) | Geprüfter Trusted Cloud Service | IDW PS 951 Typ 2 (ISAE 3402) geprüfter Dienstleister |

Myra Security ist der neue Maßstab für globale IT-Sicherheit

Die Myra-Technologie überwacht, analysiert und filtert schädlichen Internet-Traffic bevor virtuelle Angriffe einen realen Schaden anrichten. Unsere zertifizierte Security-as-a-Service-Plattform schützt Ihre digitalen Geschäftsprozesse vor vielfältigen Risiken wie DDoS-Angriffen, Bot-Netzwerken und Angriffen auf Datenbanken.

Die Bundesregierung | Bundesministerium für Gesundheit | Bundesministerium der Finanzen | msc Munich Security Conference

Finanzportal | auxmoney | swissix SWISS INTERNET EXCHANGE | flatex AKTIEN. ONLINE. HANDELN.