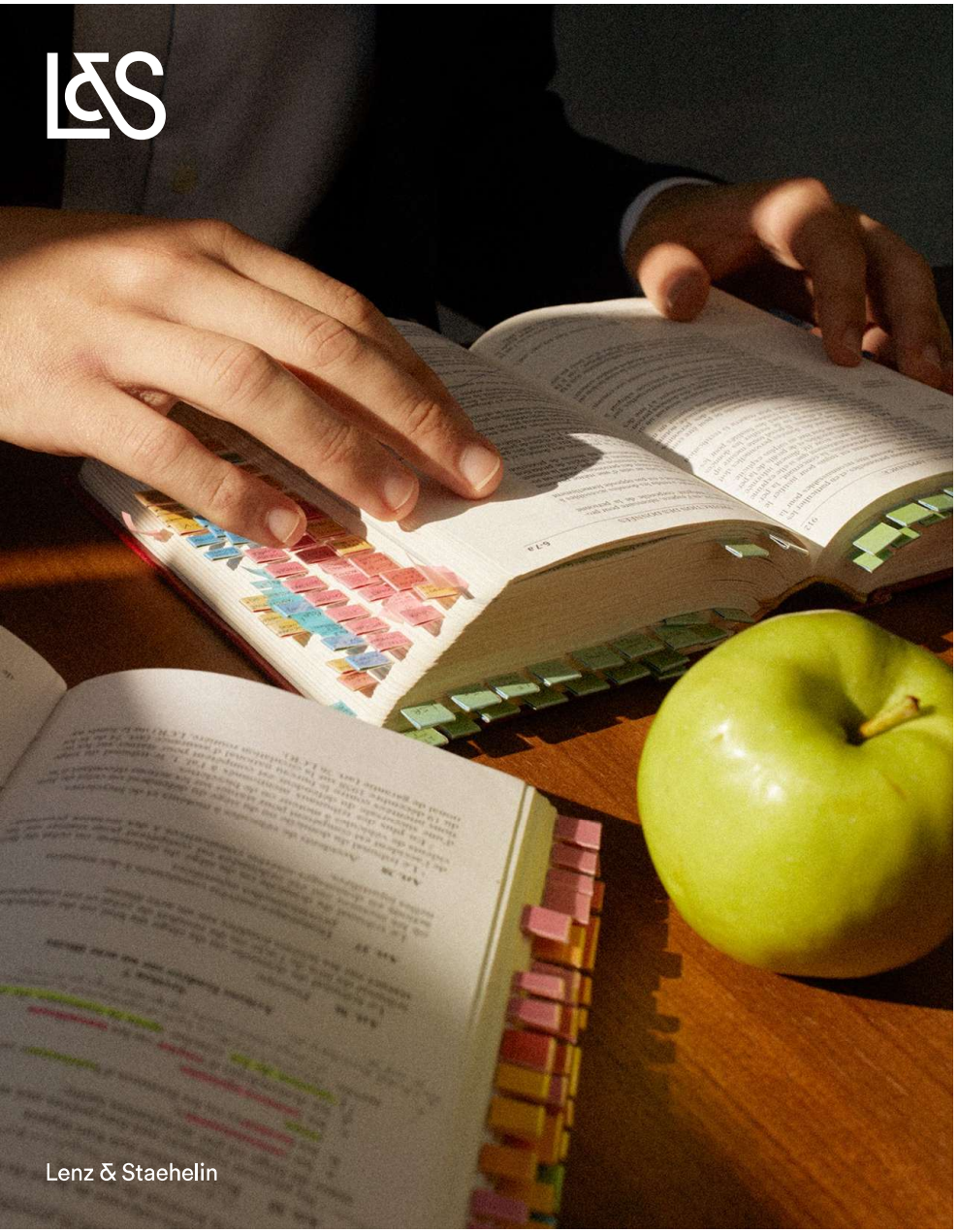
Juristische Abklärungen IT-Verträge – Outsourcing

VSKB-Legal und Compliance-Tagung 2026

Philipp Fischer

11 Juni 2026



Agenda

I. Auslagerungen
   1. Einführung
   2. Fallbeispiel
   3. Auslagerung – Definition von Outsourcing
   4. Governance und Risikomanagement: *Cloud* & KI
   5. Im Fokus: *Cloud services*
   6. Im Fokus: Künstliche Intelligenz
   7. Achtungspunkte

II. Rechtlicher und regulatorischer Rahmen des TPRM

III. Fazit

1. Auslagerungen

Einführung (1/3)

Outsourcing (→)

- FINMA-Risikomonitor 2025 (17. November 2025)

  "*Die **zunehmende Auslagerung** bedeutender und kritischer Funktionen an Drittparteien stellt für Finanzinstitute eine **zentrale Herausforderung im Bereich des operationellen Risikomanagements** dar. Die **Abhängigkeit von externen Dienstleistern** hat in den letzten Jahren, getrieben durch Digitalisierung, Effizienzsteigerung und Fokussierung auf Kernkompetenzen, **weiter zugenommen**.*" […] "*Mit dem **Trend der Cloud-Nutzung** steigt dieser Anteil bei allen Beaufsichtigten weiter an.*"

  "*Die FINMA stellt fest, dass insbesondere **bei der Identifikation und Bewertung von Risiken entlang der Lieferkette** weiterhin Verbesserungspotenzial besteht. Die Erfüllung von an Dritte übertragenen Anforderungen, insbesondere im Bereich der System- und Informationssicherheit, muss durch die Beaufsichtigten sichergestellt werden.*"

  "*Vor dem Hintergrund dieser Entwicklungen **ist es essenziell, dass Finanzinstitute ihre Governance-Strukturen und Kontrollmechanismen im Bereich Outsourcing kontinuierlich weiterentwickeln**. Nur so kann die operationelle Resilienz gestärkt und die Funktionsfähigkeit des Finanzplatzes langfristig gesichert werden.*"

1. Auslagerungen: Cyberrisiken/IKT-Risiken

Einführung (2/3)

Cyberrisiken (↑)

- FINMA-Risikomonitor 2025 (17. November 2025)

  "*Meldungen der Beaufsichtigten an die FINMA zu Cyberattacken belegen einen **zunehmenden Trend von Cyberangriffen auf Drittparteien**. Diese Meldungen machen rund **47** Prozent aller bei der FINMA gemeldeten Cybervorfälle aus*"

  "*Wichtig sind ferner effektive Prozesse zur Erkennung und zeitnahen Behebung von Software-Schwachstellen innerhalb der Technologieinfrastruktur sowie ein lückenloses Konfigurationsmanagement. Schliesslich besteht teilweise ebenfalls Handlungsbedarf im Meldewesen, wobei b**eispielsweise Prozesse und Schwellenwerte für die Meldung von Ausfällen zu wenig definiert sind***."

  "***Die Zunahme der Komplexität von IKT-Systemen sowie der Abhängigkeit von diesen hat bestehende IKT-Risiken weiter erhöht**. Dazu gehören Risiken aufgrund fehlerhafter Softwarekomponenten, die abweichendes Systemverhalten oder sogar einen Totalausfall eines IKT-Systems verursachen können. Weiter besteht das Risiko von nicht sachgerechter Wartung bzw. menschlichen Fehlern aufgrund fehlender Fachexpertise für bestimmte Systeme.*"

IKT-Risiken (↑)

1. Auslagerungen: regulatorischer Rahmen

Einführung (3/3)

Rundschreiben und Aufsichtsmitteilungen der FINMA	
Rundschreiben 2018/3 Outsourcing	Auslagerungen Banken, Versicherungsunternehmen und ausgewählten Finanzinstituten nach FINIG
FINMA-Aufsichtsmitteilung 05/2020	Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG (7. Mai 2020)
Rundschreiben 2023/1 Operationelle Risiken und Resilienz – Banken	Management der operationellen Risiken und Sicherstellung der operationellen Resilienz
FINMA-Aufsichtsmitteilung 03/2024	Erkenntnisse aus der Cyber-Risiko-Aufsichtstätigkeit, Präzisierung zur FINMA-Aufsichtsmitteilung 05/2020 und zu szenariobezogenen Cyber-Übungen (7. Juni 2024)
FINMA-Aufsichtsmitteilung 04/2024	Management der operationellen Risiken von Fondsleitungen und Verwaltern von Kollektivvermögen (12. Juni 2024)
FINMA-Aufsichtsmitteilung 08/2024	Governance und Risikomanagement beim Einsatz Künstlicher Intelligenz (18. Dezember 2024)
FINMA-Aufsichtsmitteilung 05/2025	Operationelle Resilienz bei Banken, Personen nach Art.1b BankG, Wertpapierhäusern und Finanzmarktinfrastrukturen (10. November 2025)

1. Auslagerungen

Fallbeispiel – Konform… dem Anschein nach?

- Eine Bank mit Sitz in Genf nutzt:
  - M365 und wird in der MS Azure-*Cloud* gehostet. Die vertragschliessende MS-Einheit hat ihren Sitz in **Zürich** (MS ZH) und betreibt eine öffentliche *Cloud* unter Einbeziehung mehrerer Subunternehmer mit redundanten Servern in **Genf** und **Frankfurt**; und
  - eine von diesem Dienstleister bereitgestellte **SaaS-Anwendung**, die auf einem **künstlichen Intelligenz-Modell** basiert, um ihr bei seinen Managemententscheidungen zu unterstützen und ihr Anlagevorschläge für ihre Kunden zu geben.
- Ein ***Ransomware***-Angriff betrifft einen Subunternehmer von MS ZH, der für das Rechenzentrum in Frankfurt zuständig ist. MS ZH informiert die Bank **am Tag nach der Entdeckung des Angriffs** durch den Subunternehmer und teilt mit, dass **keine "lesbaren" Daten** der Bank betroffen seien.

F0: Stellt der Einsatz von M365 und die Nutzung der SaaS-KI-Anwendung eine Aufgabenübertragung? JA

F1: Kann das Risiko im Zusammenhang mit dem Berufsgeheimnis als beherrscht angesehen werden, da FD1 *Cloud* zwischen der Schweiz und der Europäischen Union gehostet wird? NEIN

F2: Lässt sich aufgrund der Tatsache, dass die KI-Anwendung lediglich Anlageempfehlungen ausspricht, sämtliche aufsichtsrechtliche Risiken ausschliessen? NEIN

F3: Kann aufgrund des Fehlens "lesbaren" gestohlener Daten eine Meldepflicht ausgeschlossen werden? NEIN

F4: Ist die Bank aufgrund der raschen Benachrichtigung durch den Beauftragten in der Lage, ihren Meldepflichten nachzukommen? NEIN

Slide 6

FD1 Délégation de tâches

dingf; 2026-06-05T16:18:26.556

1. Auslagerungen

Definition von Outsourcing (FINMA-RS 18/3)

Wann liegt Outsourcing im Sinne des FINMA-RS 18/3 vor?

Es liegt im Sinne dieses Rundschreibens "Outsourcing" (Auslagerung) vor, wenn ein Unternehmen einen Dienstleister damit beauftragt, eine **für die Geschäftstätigkeit des Unternehmens wesentliche Funktion** ganz oder teilweise selbstständig und dauerhaft zu erfüllen.

FINMA-RS 18/3 wird derzeit überarbeitet – Schwerpunkt auf Resilienz und operationellen Risiken

Auftragsvertrag – Mindestinhalt (Art. 17 FINIV, FINMA-RS 18/3)

- Zuständigkeiten und Verantwortlichkeiten
- Allfällige Befugnisse zur Subdelegation
- Rechenschaftspflicht des Dritten
- Kontrollrechte

Eine Funktion, von der die Einhaltung der Ziele und Vorschriften des Finanzmarktaufsichtsrechts in erheblichem Masse abhängt

1. Auslagerungen

Governance und Risikomanagement: *Cloud* & KI

- Keine spezifischen Vorschriften für *Cloud*- oder KI-Anwendungen
- Technologieneutralität
- Aufsichtsrechtliche Anforderungen auf der Grundlage der Grundsätze der Governance, des Risikomanagements und des Controllings
- **FINMA-Aufsichtsmitteilung 08/2024** zur Governance und Risikomanagement beim Einsatz Künstlicher Intelligenz
  - Auswirkungen des Einsatzes von KI auf das Risikoprofil aktiv berücksichtigen
  - Governance, Risikomanagement und Kontrollsysteme an den Einsatz von KI anpassen
  - Hierbei Folgendes berücksichtigen:
    - › Grösse, Komplexität, Struktur und Risikoprofil der Bank
    - › Bedeutung der Instrumente für die Geschäftstätigkeit der Bank
    - › Wahrscheinlichkeit, dass die mit der KI verbundenen Risiken eintreten

1. Auslagerungen

Im Fokus: *Cloud services* (1/3)

Feststellung der FINMA:
Zunehmende Nutzung öffentlicher *Clouds*

- ***Cloud*** vs. ***On premises***
  - Schweizer *Cloud* oder ausländische *Cloud*? Private *Cloud* oder öffentliche *Cloud*?
  - Auswirkungen: Erfassung, Bewertung und Management der mit der gewählten Struktur verbundenen Risiken (insbesondere Vertraulichkeit, Integrität und Verfügbarkeit kritischer Daten)
- Einige **spezifische bzw. verstärkte Risiken** im Zusammenhang mit der *Cloud*
  - Abhängigkeit – Dienste und Infrastruktur unter der Kontrolle des Beauftragten
  - Geschäftskontinuität (*Business Continuity*) – Risiko einer sofortigen Unterbrechung der Dienste sowie BCP/DRP des Dienstleisters
  - Datenfluss – Speicherung und Hosting der für den Dienst erforderlichen Daten auf einer vom Beauftragten (oder dessen Subunternehmern) verwalteten Infrastruktur
  - Grenzüberschreitende Geschäftstätigkeit (*Global Delivery Model*) – Beauftragter, Subunternehmer, Personal, Infrastruktur, Server, Hardware, Fachwissen im Ausland
  - Komplexität/Anfälligkeit der Lieferkette – Vielzahl von Subunternehmern, von denen die Dienste abhängen (Abhängigkeit)
  - Einhaltung gesetzlicher Vorschriften – wirksame Kontrolle des Beauftragten, Datenschutz (DSG) und kritische Funktionen, Geheimnis

1. Auslagerungen

Im Fokus: *Cloud services* (2/3)

Praxisempfehlungen:
- Einbeziehung der spezifischen Cloud-Risiken in die Verfahren zum Risikomanagement bei Drittanbietern (*Third-Party-Risk-Management*)
- Spezifische Risiken sind vor der Auswahl des Anbieters zu identifizieren (*Due Diligence*) und während der gesamten Dauer der Geschäftsbeziehung regelmässig (einmal jährlich) zu überprüfen.

- Einige **Kontrollmassnahmen für Risiken** im Zusammenhang mit der *Cloud*:
  - **Abhängigkeiten / Komplexität der Lieferkette**
    - **Klumpenrisiken** definieren und überwachen (insb. über **Bestandsaufnahmen**),
    - wesentliche Subunternehmer (***Key Third Parties***) identifizieren und ein Register führen,
    - **vertraglicher Rahmen** (insb. Kontrolle des Standorts der Dienste, Kontrolle der wesentlichen Subunternehmer (einschliesslich Hosting) sowie Audit- und Überwachungsrechte in Bezug auf Leistung, Sicherheit und Hosting sowie in Bezug auf *Key Third Parties*, Meldepflicht bei Vorfällen und *flow through*-Klauseln für *Key Third Parties*),
    - Markt- und Alternativenanalyse (**Ersetzbarkeit**),
    - Erstellung eines Plan B (***exit strategy***)
  - **Geschäftskontinuität *(business continuity)***
    - **Vertraglicher Rahmen** (insb. Gewährleistung der Dienstkontinuität, BCP/DRP sowie Begrenzung von Aussetzern/Unterbrechungen, *termination assistance*),
    - die **BCP/DRP-Verfahren des Dienstleisters** analysieren und auf Übereinstimmung mit der Risikobereitschaft der Bank prüfen (sowie darauf, ob die BCP/DRP von **ISO/SAE**-zertifizierten Stellen geprüft sind),
    - die **internen BCP/DRP-Verfahren anpassen**, um im Falle einer Störung die Wiederaufnahme des Betriebs innerhalb einer angemessenen Frist (RTO) sicherzustellen

1. Auslagerungen

Im Fokus: *Cloud services* (3/3)

Praxisempfehlungen:
- Einbeziehung der spezifischen Cloud-Risiken in die Verfahren zum Risikomanagement bei Drittanbietern (*Third-Party-Risk-Management*)
- Spezifische Risiken sind vor der Auswahl des Anbieters zu identifizieren (*Due Diligence*) und während der gesamten Dauer der Geschäftsbeziehung regelmässig (einmal jährlich) zu überprüfen.

- Einige **Massnahmen zur Risikokontrolle** im Zusammenhang mit der *Cloud*:
  - **Datenflüsse / grenzüberschreitende Vorgänge**
    - **Data mapping** bei der Auswahl des Dienstleisters
    - Vertraglicher Rahmen (insb. ***data processing agreement*** zur Regelung der Bedingungen für die Verarbeitung und Übermittlung von Daten, **Geheimhaltungsklausel**, **Prüfungs- und Kontrollrecht** auch im Ausland sowie zugunsten der Revisoren und der FINMA)
    - Konformitätsanalyse zum **DSG** / **Berufsgeheimnis** bei der Übermittlung **personenbezogener Daten / CID ins Ausland** (siehe unten)
  - **Einhaltung regulatorischer Vorschriften**
    - Analyse zur Einhaltung regulatorischer Vorschriften
    - Insbesondere in Bezug auf: (1) Mindestinhalt des **Delegations-/Outsourcingvertrags**; (2) **Governance und Risikomanagement**; (3) **Meldung von Vorfällen**; (4) Datenschutz (insbesondere hinsichtlich **Transparenz** und **internationaler Datenübermittlung**); (5) **Berufsgeheimnis** bei Zugriff auf CID

1. Auslagerungen

Im Fokus: Künstliche Intelligenz (1/3)

- **Definition**
  - Die FINMA stützt sich auf die Definition der OECD in deren *Explanatory memorandum on the updated OECD definition of an AI system*:
    - *Ein System der künstlichen Intelligenz ist ein **maschinengestütztes System**, das für **explizite oder implizite Ziele** aus den ihm **zugeführten Eingabedaten** (Input) ableitet, wie **Ausgabedaten** (Output) wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen **zu generieren** sind, die **physische oder virtuelle Umgebungen beeinflussen können**.* Die verschiedenen Systeme der künstlichen Intelligenz unterscheiden sich hinsichtlich ihres Autonomiegrades und ihrer Anpassungsfähigkeit nach ihrer Einführung.
- **Hauptrisiken** (vgl. FINMA-Aufsichtsmitteilung 08/2024): **operationelle Risiken**, **IT-Risiken**, **Cyberrisiken**, **Abhängigkeit** von Dritten
  - Aufsichtsrechtliche Erwartungen in Bezug auf KI-Risiken
    - **Governance und Verantwortung** – Verantwortlichkeiten und Risikomanagementprozesse – keine Delegation von Entscheidungsbefugnissen an eine KI-Anwendung – alle Beteiligten müssen über ausreichende Kenntnisse verfügen
    - **Robustesse et fiabilité** – Stabilität und Zuverlässigkeit – Risiken durch schlechte Datenqualität, *Drift*-Risiken (falsche Modellentwicklung) – Kritische Prüfung des Modells und der Ergebnisse – Überprüfung, ob die Ergebnisse ausreichend präzise, belastbar und zuverlässig sind
    - **Transparenz und Erklärbarkeit** – Sicherstellung der Erklärbarkeit der Ergebnisse und der Transparenz hinsichtlich der Nutzung der KI-Anwendung
    - **Gleichbehandlung** – Vermeidung ungerechtfertigter Ungleichbehandlung

1. Auslagerungen

Im Fokus: Künstliche Intelligenz (2/3)

Praxisempfehlungen im Zusammenhang mit der Risikoklassifizierung:
- Eine interne/externe Ressource für diese Aufgaben abstellen,
- Ein Standardklassifizierungsmodell von Dritten (Anwaltskanzlei/Big4) einholen und an das Geschäftsmodell anpassen;
- Risiken und Kontrollen anhand *use cases* ermitteln (z. B. Verfassen von E-Mails, Ausarbeitung von Verträgen, Anlageempfehlungen, Verwaltung des Einstellungsprozesses usw.).

- Ausgewählte **Risikomanagementmassnahmen** (vgl. FINMA-Aufsichtsmitteilung 08/2024):
  - **Zentrales** KI-Anwendungen **Verzeichnis**
    - Auf der Grundlage systematischer Kriterien
    - Ermittlung von KI-Anwendungen mit erhöhtem Risiko (z. B. wenn sie für die Einhaltung regulatorischer Vorschriften oder für die Ausführung kritischer Funktionen entscheidend sind) → entsprechende Anpassung des Risikomanagements
  - **Klassifizierung** von Risiken und Massnahmen
  - Bestimmung der **Kompetenzen und Verantwortlichkeiten** für Auswahl, Entwicklung, Implementierung, Überwachung und Nutzung von KI
  - Verfahren und Vorschriften für **Tests und Kontrollen** von KI-Anwendungen
    - Vorabdefinition von *KPI*s zur Überprüfung der Leistung
    - Kontrollen der Datenqualität
    - Prüfungen auf Richtigkeit, Belastbarkeit, Stabilität und Verzerrungen (z. B. *backtesting*, *stress testing*, *adversarial testing*)

1. Auslagerungen

Im Fokus: Künstliche Intelligenz (3/3)

- Ausgewählte **Risikomanagementmassnahmen** (vgl. FINMA-Aufsichtsmitteilung 08/2024):
  - **Interne Schulungen**
  - Bei **Auslagerung**: Due Diligence, Tests, Kontrollen und spezifische Vertragsklauseln
  - **Dokumentation**
    - Allgemeine Richtlinien zur Auswahl, Entwicklung, Bereitstellung, Überwachung und Nutzung von KI-Anwendungen
    - Spezifische Vorschriften für bestimmte kritische KI-Anwendungen (z. B. KI-Anwendungen mit erhöhtem Risiko, die für die Einhaltung gesetzlicher Vorschriften oder die Ausführung kritischer Funktionen entscheidend sind)
      - Zweck der Anwendung, Auswahl, Datenaufbereitung (Input), Modellauswahl, Leistungsmessgrössen (*KPIs*), Annahmen, Einschränkungen, Tests und Kontrollen sowie Ausweichlösungen;
      - Bewertung der Stabilität, Zuverlässigkeit und Nachvollziehbarkeit der KI-Anwendung

1. Auslagerungen

Achtungspunkte – Auftragsvertrag / *Best practices*

Auftragsvertrag – Mindestinhalt (FINMA-RS 18/3)

- Zuständigkeiten und Verantwortlichkeiten
- Mögliche Befugnisse zur Subdelegation
- Rechenschaftspflicht des Dritten
- Kontrollrechte

- **Anweisung** und **Beaufsichtigung** des Beauftragten
- Kontrolle der **Subunternehmer** des Beauftragten (Kündigung vs. Widerspruch)
- **Vertraulichkeit**, **Datensicherheit** und **Geschäftskontinuität**
  - Technische und organisatorische Massnahmen (*Business continuity plan* & *Disaster recovery plan)*
- **Audit**: Durchführung, interne und externe Revisoren, OS und FINMA
- **Übergang** (Migration zu einem Ersatzbeauftragten / *reinsourcing*)
  - *Termination assistance*
- **Berufsgeheimnis**
- Meldung von **Sicherheitsvorfällen**
  - Cyberangriffe – **Meldefristen FINMA 24 Std. / 72 Std.** (ab Kenntnisnahme durch den Beauftragten)
  - Vorfälle, die die **Vertraulichkeit**, **Integrität** oder **Verfügbarkeit** kritischer Daten erheblich beeinträchtigen (Quelle: FINMA-RS 2023/1, anwendbar auf Banken und Versicherungen)

Art. 29 FINMAG

FINMA-Aufsichtsmitteilung 05/2020 vom 7. Mai 2020

FINMA-Aufsichtsmitteilung 03/2024 vom 7. Juni 2024

2. Rechtlicher und regulatorischer Rahmen des TPRM

Zentrale regulatorische Anforderung: Das Modell der Drei Verteidigungslinien

1. Linie – Operative Management

- Verantwortlich für die Beziehungen zu Dritten
- Risikoidentifizierung und Einhaltung der TPRM-Anforderungen
- Operative Überwachung der Dienstleister

2. Linie – Überwachungsfunktionen

- Festlegung der TPRM-Standards und –Instrumente
- Unabhängige Überprüfung der Risikobewertungen
- Konsolidiertes Reporting und Überwachung der *key risk indicators* (KRI).

3. Linie – Interne Revision

- Unabhängige Bewertung der Wirksamkeit des TPRM-Systems
- Empfehlungen und Überwachung der Aktionspläne

3. Fazit

Die wesentliche regulatorische Anforderungen: Monitoring und Risikomanagement

- **Das Outsourcing von Tätigkeiten führt zu keiner Übertragung der Verantwortung vom Finanzdienstleister.**
  - Die Bank bleibt gegenüber den Kunden und der FINMA vollständig verantwortlich.
- **Rolle der FINMA**
  - Die FINMA legt die aufsichtsrechtlichen Anforderungen fest.
  - Ein auf Risiko und Verhältnismässigkeit basierender Ansatz.
  - Der Schwerpunkt liegt auf der Betrieblichen Resilienz und den kritischen Dienstleistern.
- **Kernerwartung**
  - Dokumentiertes, nachvollziehbares und tatsächlich umgesetztes TPRM-System.
  - Nachweisbare Fähigkeit, Risiken im Zusammenhang mit Dritten auf der Grundlage eines risikobasierten Ansatzes zu identifizieren, zu überwachen und zu kontrollieren.

Anhang 1 – Identifizierung von Outsourcing-Risiken (1/2)

Risiken im Bereich der Cybersicherheit

Allgemeine Risiken:

- Strafrechtliche Haftung bei unbefugter Weitergabe
- Unzureichende Verwaltung von Zugriffsrechten und Berechtigungen
- Unzuverlässigkeit der Verschlüsselung & der Schlüsselverwaltung

KI-Besonderheiten :

- Trainingsdaten & Verstösse gegen die Einwilligung
- Mangelnde Erklärbarkeit & Transparenz
- Datenlokalisierung in KI-Systemen
- KI-Dienste von Drittanbietern & Transparenz

Anhang 1 – Identifizierung von Outsourcing-Risiken (2/2)

Risiken im Bereich der Cybersicherheit

Cross-border-Besonderheiten:

- Zuständigkeitskonflikte & Offenlegungspflichten
- Datensouveränität & Kontrollverlust
- Datenverlust/-lecks bei grenzüberschreitenden Übermittlungen
- Datenverlust während der Übertragung und Speicherung
- Unzureichendes *logging* & Monitoring *across borders*

Cloud-Besonderheiten:

- Konfigurationsfehler in *Cloud*-Umgebungen
- *API*-Sicherheit & unbefugter Zugriff
- Sicherheitslücken bei Subunternehmern & Dienstleister
- Abhängigkeit von Anbietern und Kontrollverlust
- Ausfall des Dienstes
- Anbieterabhängigkeit (*lock-in*) & Datenübertragbarkeit

Anhang 2 – Anforderungen der FINMA beim Outsourcing

Rundschreiben 2018/3 (Auszug der wichtigsten Anforderungen)

Anforderung	Kurzbeschreibung	Ref.
Verzeichnis der ausgelagerten Funktionen	Vollständiges und aktuelles Verzeichnis der ausgelagerten Funktionen (einschliesslich Funktion, Dienstleister und Subunternehmer, Leistungsempfänger und verantwortliche Stelle).	Rz. 14
Bestimmung und Auswahl der Dienstleister	Vorherige Auswahl und Dokumentation der Anforderungen und Risiken im Zusammenhang mit der Auslagerung, Kriterien für die Auswahl des Dienstleisters und Berücksichtigung des Klumpenrisiko.	Rz. 16
Dauerhaftigkeit und Umkehrbarkeit	Nachhaltigkeit der Auslagerung, Umkehrbarkeit und vertragliche Aufteilung der Verantwortlichkeiten.	Rz. 18, 18.1 et 19
Governance und Kontrolle	Interne Kontrollen, Risikomanagement, interner Verantwortlicher für die Überwachung sowie Weisungs- und Kontrollbefugnisse gegenüber dem Dienstleister.	Rz. 20-21
Sicherheit	Sicherheitsanforderungen, kontinuierliche Überwachung und Geschäftskontinuität im Notfall.	Rz. 24-25
Auditrechte	Uneingeschränkter Zugang und Einsicht für die FINMA, die Bank und dessen Revisionsstelle; mögliche Beauftragung Dritter und Bereitstellung von Informationen.	Rz. 26-29
Datenübermittlung ins Ausland	Zugang und Einsichtnahme im betreffenden Land, Verfügbarkeit von Informationen für eine Umstrukturierung oder Abwicklung.	Rz. 30-31
Subunternehmer	Vorabinformation, Widerspruchsrecht, Kündigungsrecht, entsprechende Verpflichtungen für Subunternehmer.	Rz. 33

Anhang 3 – Anforderungen der FINMA beim Outsourcing

Rundschreiben 2023/1 (1/2) (Auszug der wichtigsten Anforderungen)

Anforderung	Kurzbeschreibung	Ref.
Risikotoleranz im operativen Bereich	Festlegung, Dokumentation und Überwachung der operativen Risikotoleranz (inhärente und Restrisiken).	Rz. 38
Bestandsaufnahme der Informations- und Kommunikationstechnologien (IKT)	Vollständiges und stets aktuelles Inventar der IKT-Komponenten (Hardware, Software, Abhängigkeiten, Dienstleister usw.).	Rz. 53
Management schwerwiegender IKT-Störungen	Verfahren, Prozesse und Kontrollen für schwerwiegende IKT-Störungen, einschliesslich externer Abhängigkeiten, des gesamten Lebenszyklus und der Zuständigkeitsverteilung.	Rz. 58
Cybervorfälle / Meldung an die FINMA	Cyber-Risikomanagement, das eine Analyse jedes Cyberangriffs unter Berücksichtigung seiner Schwere sowie der betroffenen kritischen Daten und Prozesse gewährleistet, sowie die Einhaltung der Meldepflichten gemäss FINMAG (24 Stunden, 72 Stunden und Abschlussbericht).	Rz. 68
Verwaltung kritischer Daten	Ermittlung kritischer Daten (einschliesslich IKT-Komponenten), Einführung geeigneter Verwaltungsabläufe, Beschränkung des Zugriffs auf solche Daten.	Rz. 71ff.
Due-Diligence-Prüfung von Dienstleistern bei kritischen Daten	Klare Kriterien, verstärkte Sorgfaltspflicht, regelmässige Überwachung.	Rz. 82

Anhang 3 – Anforderungen der FINMA beim Outsourcing

Rundschreiben 2023/1 (2/2) (Auszug der wichtigsten Anforderungen)

Anforderung	Kurzbeschreibung	Ref.
Business impact analysis (**BIA**)	Ermittlung kritischer Prozesse und Ressourcen mittels einer BIA.	Rz. 84
Recovery Time Objective (**RTO**) / Recovery Point Objective (**RPO**)	Festlegung von RTO und RPO, vertragliche Vereinbarung und Überwachung ihrer Einhaltung	Rz. 85
Disaster recovery plan (**DRP**)	DRP im Business Continuity Plan (BCP) (bei Auslagerung: Berücksichtigung externer Abhängigkeiten und vertraglicher Bestimmungen), jährliche Aktualisierung oder bei Änderungen.	Rz. 88
Risiken für Dienstleister bei grenzüberschreitenden Dienstleistungen	Berücksichtigung der Risiken im Zusammenhang mit externen Vermögensverwaltern, Vermittlern und anderen Dienstleistern sowie deren sorgfältige Auswahl und Unterweisung.	Rz. 99
Koordination	Koordination der relevanten Komponenten eines umfassenden Risikomanagements (einschliesslich IKT-Risiken, Cyberrisiken, Business Continuity Management, Outsourcing und Notfallplanung) zur Stärkung der operativen Widerstandsfähigkeit.	Rz. 104
Resilienz-Tests	Regelmässige Prüfungen unter strengen, aber realistischen Bedingungen.	Rz. 110

Vielen Dank für Ihre Aufmerksamkeit.

Philipp Fischer

Partner
+41 58 450 72 20
philipp.fischer@lenzstaehelin.com

Lenz & Staehelin
www.lenzstaehelin.com