Auswirkungen des neuen Rundschreibens operationelle Risiken auf Outsourcing-Vertragsverhältnisse

Referat IFZ Forum Bank-IT
7. Juni 2023
Campus Zug-Rotkreuz

Was hat das FINMA-Rundschreiben 2023/1 mit Outsourcing-Verträgen zu tun?

→ **Das Rundschreiben 2018/03 «Outsourcing» hat sich nicht geändert. Trotzdem sind neue Punkte im Outsourcing-Verhältnis zu beachten.**

- Das neue Rundschreiben 2023/01 gibt neue Vorgaben insbesondere rund um die Steuerung der IT vor, welche ab 1. Januar 2024 umgesetzt werden müssen.
- Dürst Consulting hat im Rahmen seiner Praxis festgestellt, dass Outsourcing-Verträge oft direkt auf das alte Rundschreiben 2008/21, insbesondere auf den Anhang 3 referenzieren.
- Das neue Rundschreiben gibt insbesondere in den Themen Business Continuity Management und Cyber-Security neue Vorgaben, welche es auch im Verhältnis mit Outsourcing-Partnern zu erfüllen und potenziell neu zu regeln gilt.

Anpassungsbedarf bei Verträgen mit Anbietern von Dienstleistungen bei Kernbankenplattformen

→ **Klassisch besteht ein Vertragskonstrukt mit einem Anbieter aus einem Rahmenvertrag, Anhängen zum Rahmenvertrag, Einzelverträgen und Beilagen/Anhänge zu den Einzelverträgen. Wo braucht es Anpassungen?**

- Die schlechte Nachricht lautet: auf allen Vertragsebenen
- Die gute Nachricht lautet: dafür sind es oft nur geringe formelle Anpassungen
- Da es leider fast jeden Teil eines Vertragskonstrukts treffen kann, ist der Analyse-aufwand der grösste Zeitfresser. Die Umsetzung selber ist – zumindest für die rein formellen Anpassungen – weniger zeitintensiv.
- Nicht zu unterschätzen sind aber die inhaltlich neuen oder anzupassenden Vertragspunkte.

Wichtigsten Anpassungs-Themen

- Ersatz des explizit genannten alten Rundschreibens 2008/21 in den Verträgen
- Neue Definition **kritische Daten** (bisheriger Fokus auf CID-Daten)
- Neue Begriffsdefinitionen (u.a. RTO für Recovery Time Objective und RPO für Recovery Point Objective)
- Neu Notwendigkeit von **RPO- und RTO-Zeiten** gemäss FINMA-Definition
- Allenfalls Anpassungen bei Governance-Themen aufgrund der neuen Minimalvorgaben im Rundschreiben
- Allenfalls Ergänzung bei den Verträgen aufgrund von Minimalvorgaben im Testing und im Reporting
- Generell: strengere Vorgaben rund um Themen wie IKS und Cyber-Risiken

Typische Rundschreiben-Artikel mit Auswirkungen auf Outsourcing-Verträge (1)

Die *Recovery Time Objective (RTO)* ist die Zeit bis zur Wiederherstellung einer Anwendung, eines Systems und/oder eines Prozesses. Die *Recovery Point Objective (RPO)* ist die maximal tolerierbare Zeitspanne eines Datenverlusts. 10

Für die kritischen Prozesse definiert das Institut die RTO und RPO nach Rz 10. Diese sind mit den dafür erforderlichen Leistungserbringern[24] abgestimmt und die Einhaltung der RTO und RPO wird durch *Service Level Agreements* oder Verträge geregelt oder durch andere geeignete Verfahren, Prozesse und Kontrollen sichergestellt. 85

Oft sind in den bestehenden Outsourcing-Verträgen RTO-Zeiten definiert, aber keine RPO-Zeiten. Das Rundschreiben fordert nebst der reinen vertraglichen Regelung indirekt auch einen Einbau ins SLA-Reporting. Das bedeutet, dass allenfalls nebst der rein vertraglichen Regelung auch die SLA-Reports ergänzt werden müssen.

Typische Rundschreiben-Artikel mit Auswirkungen auf Outsourcing-Verträge (2)

Die operationellen Risiken sind institutsweit einheitlich zu kategorisieren und in einem Inventar aufzuführen. Diese Kategorisierung kann in Anlehnung an die für die Berechnung der Mindesteigenmittel für operationelle Risiken verwendete Kategorisierung der Ereignistypen oder mittels einer internen Taxonomie erfolgen. Die Kategorisierung ist in allen Bereichen des Instituts und in allen Komponenten des Managements der operationellen Risiken konsistent anzuwenden. 28

Die Vorgabe der einheitlichen Taxonomie erfordert eine Abstimmung der Bank mit dem Outsourcing-Partner. Allenfalls ist die Taxonomie in den Verträgen oder bankintern anzupassen, um dieser Vorgabe gerecht werden zu können.

Typische Rundschreiben-Artikel mit Auswirkungen auf Outsourcing-Verträge (3)

b. Schutz der inventarisierten Bestandteile der IKT und der elektronischen kritischen Daten vor Cyber-Attacken durch die Implementierung angemessener Schutzmassnahmen, insbesondere im Hinblick auf die Vertraulichkeit, Integrität und Verfügbarkeit; 64

Diese Vorgabe bedingt aufgrund der Bezugnahme auf die inventarisierten Bestandteile der IKT sowie der kritischen Daten eine klare Kommunikation zwischen Outsourcing-Partnern und der Bank, insbesondere was die Klassifizierung als kritische Daten betrifft. Kritische Daten ist nicht deckungsgleich mit den CID-Daten gemäss altem Rundschreiben. CID-Daten dürften wohl eine Teilmenge der kritischen Daten darstellen. Die Definition ist Sache der Banken.

Typische Rundschreiben-Artikel mit Auswirkungen auf Outsourcing-Verträge (4)

c. Zeitnahe Aufzeichnung und Erkennung von Cyber-Attacken auf Basis eines Prozesses zur systematischen und durchgängigen Überwachung der inventarisierten Bestandteile der IKT und der elektronischen kritischen Daten; 65

d. Reaktion auf identifizierte Schwachstellen und Cyber-Attacken durch die Entwicklung und Implementierung angemessener Prozesse, um zeitnah Massnahmen für die Eindämmung und Beseitigung einzuleiten; und 66

e. Sicherstellung einer zeitnahen Wiederherstellung des ordentlichen Geschäftsbetriebs nach Cyber-Attacken durch geeignete Massnahmen. 67

Nur Identifikation und Schutz von Cyberrisiken reicht nicht mehr. Die Banken müssen das volle NIST-Programm (Identifikation, Schutz, Erkennung, Reaktion und Wiederherstellung) abdecken. Ist das so in den bestehenden Verträgen explizit geregelt? Meine Erfahrung zeigt, dass hier Handlungsbedarf besteht.

Typische Rundschreiben-Artikel mit Auswirkungen auf Outsourcing-Verträge (5)

Das Institut identifiziert seine kritischen Daten systematisch und vollständig, kategorisiert diese nach ihrer Kritikalität und definiert eindeutige Datenverantwortlichkeiten.	73
Die vom Institut definierten kritischen Daten werden entlang ihres gesamten Lebenszyklus verwaltet.	74
Dabei wird insbesondere die Einhaltung der Vertraulichkeit, Integrität und Verfügbarkeit bei der Verwaltung von kritischen Daten durch geeignete Prozesse, Verfahren und Kontrollen gewährleistet.	75
Kritische Daten sind im Betrieb und während der Entwicklung, Veränderung und Migration von IKT vor dem Zugriff und der Nutzung durch Unberechtigte angemessen zu schützen. Dies gilt auch für kritische Daten in Testumgebungen.	76

Diese vier Artikel beinhalten sehr viele Vorgaben, welche Ergänzungen in den Outsourcing-Verträgen erforderlich machen dürften.

Erleichterung für Kat. 4/5-Banken

Typische Rundschreiben-Artikel mit Auswirkungen auf Outsourcing-Verträge (6)

Das Institut definiert als Teil des BCP mindestens einen DRP. Wenn kritische Prozesse oder Teile davon ausgelagert sind, berücksichtigt der DRP die externen Abhängigkeiten und vertraglichen Regelungen sowie alternative Lösungen. Der DRP wird ad hoc im Falle wesentlicher Änderungen und mindestens jährlich überprüft und aktualisiert. 88

Die BCM- oder Katastrophen-Prozeduren sind mit den Outsourcing-Partnern abzustimmen und mindestens einmal jährlich auf Aktualität zu überprüfen.

Klarer Link zum Outsourcing-Rundschreiben

Bei der Auswahl von Dienstleistern, die kritische Daten bearbeiten[22] oder einsehen können, ist der Sorgfaltsprüfung (*Due Diligence*) eine hohe Bedeutung beizumessen. Es sind klare Kriterien für die Beurteilung des Umgangs der Dienstleister mit kritischen Daten zu definieren und vor Vertragsvereinbarung zu prüfen. Die Dienstleister sind im Rahmen des internen Kontrollsystems des Instituts risikoorientiert periodisch zu überwachen und zu kontrollieren. 82

Dieser Artikel fasst mehr oder weniger die Art. 16-20 des Outsourcing-Rundscheibens zusammen.

Fazit: Outsourcing-Verträge sind zu überprüfen

Es ist leider eine Tatsache: die bestehenden Outsourcing-Verträge sind einer kritischen Überprüfung zu unterziehen. Nebst dem rein inhaltlichen Interesse der Banken aus kommerziellen und Compliance-Gründen dürfte die Outsourcing-Vertragsthematik dieses Jahr wohl auch auf der «To-do»-Liste der aufsichtsrechtlichen Revisionsstellen stehen. Dies nicht wegen des neuen Rundschreibens 2023/01, sondern weil die Übergangsfrist gemäss Randziffer 37 aus dem Rundschreiben 2018/03 am 1. April 2023 abgelaufen ist.