**Prüfpunkte zum Management der Risiken kritischer Daten**

**Übersicht**

|  |  |
| --- | --- |
| **Prüfgebiet:** | **Management der Risiken kritischer Daten** |
| **Prüftiefe:** | [Prüfung / Kritische Beurteilung][[1]](#footnote-2) |
| **Grundlagen:**  (Liste ist nicht abschliessend) | Art. 3 Abs. 2 Bst. a Bankengesetz (BankG)  Art. 9 Finanzinstitutsgesetz (FINIG)  Art. 12 Bankenverordnung (BankV)  Art. 12, 67, 68 und 73 Finanzinstitutsverordnung (FINIV)  Art. 11 Abs. 4 und 15 Finanzmarktinfrastrukturverordnung (FinfraV)  Rz 13, 50, 52, 53, 58, 59 FINMA-Rundschreiben 2017/1 „Corporate Governance – Banken“ (FINMA-RS 17/1)  Rz 71–82 FINMA-Rundschreiben 2023/1 „Operationelle Risiken und Resilienz – Banken“ (FINMA-RS 23/1) |
| **Sign-offs:** | |  |  |  |  | | --- | --- | --- | --- | | **Sign-offs:** | **Name:** | **Funktion:** | **Datum:** | | Prüfer: | [Name] | [Assistant / Senior / Manager / Senior Manager / Director / Partner] | [TT. MM.JJJJ] | | Reviewer: | [Name] | [Manager / Senior Manager /  Director / Partner] | [TT. MM.JJJJ] | |

**Dies ist ein Standard-Prüfprogramm, welches bei jeder Intervention gemäss Prüfstrategie (Rz 28ff FINMA-RS 13/3 „Prüfwesen“) grundsätzlich anzuwenden ist. Es liegt in der Verantwortung des Prüfteams, das Standard-Prüfprogramm an die spezifische Situation (Grösse, Geschäftsmodell, Organisation, Prozesse, Risikoexposition usw.) des geprüften Instituts anzupassen. Werden die angegebenen Prüfungshandlungen nicht vollständig durchgeführt, ist in den Arbeitspapieren eine aussagekräftige Erläuterung dazu anzubringen. Die mit einem Stern (\*) markierten Prüfhandlungen sind bei allen Banken der Aufsichtskategorien 4 und 5 nicht anwendbar. Die mit zwei Sternen (\*\*) markierten Prüfhandlungen entfallen bei Instituten nach Art. 47*a*–47*e* ERV, Personen gemäss Art. 1*b* BankG sowie nicht-kontoführenden Wertpapierhäusern.**

**Abschliessende Zusammenfassung**

| **Thema:** | **Information / Beschreibung:** |
| --- | --- |
| Zusammenfassende Gesamtbeurteilung | |  |  | | --- | --- | | **Bestätigung im Prüfbericht:** | **Zusammenfassung:** | | Bestätigung, dass die aufsichtsrechtlichen Vorgaben zum Bereich „Management der Risiken kritischer Daten“ eingehalten wurden.  Bestätigung, dass der Beaufsichtigte die durch die FINMA angeordneten Verschärfungen eingehalten hat. | ***Ja*** *(Prüfung / kritische Beurteilung) /* ***Nein***  ***Ja*** *(Prüfung / kritische Beurteilung) /* ***Nein*** | |
| Zusammenfassung der Prüfresultate / Beanstandungen und Empfehlungen (ausführliche Informationen nachstehend) | [Zusammenfassung der Prüfresultate / Beanstandungen und Empfehlungen] |
| Prüffelder, Prüfresultate und durchgeführte Prüfungshandlungen der Internen Revision, auf die sich die Prüfgesellschaft gestützt hat (einschliesslich der Würdigung durch die Prüfgesellschaft) | [Beschreibung] |

**Prüfprogramm – Management der Risiken kritischer Daten**

| **Nr.** | **Prüfungshandlungen für Prüftiefe „kritische Beurteilung“:** | **Zusätzliche Prüfungshandlungen für Prüftiefe „Prüfung“:** | **Durchgeführte Prüfungshandlungen / Feststellungen:** | **Arbeitspapiere Ref.:** |
| --- | --- | --- | --- | --- |
| *Management der Risiken kritischer Daten unter Berücksichtigung des Proportionalitätsprinzips, d. h. unter Berücksichtigung der Grösse, Komplexität (insbesondere hinsichtlich IKT und Outsourcing) sowie Struktur, und Risikoprofil:* | | | | |
| 1 | Aneignung grundlegender Kenntnisse über den übergreifenden Umgang des Instituts mit kritischen Daten unter Berücksichtigung des Proportionalitätsprinzips und den folgenden Prüfungshandlungen. |  |  |  |
| 2 | Beurteilung der Angemessenheit interner Vorgaben (bspw. Reglemente, Richtlinien, Weisungen) in Bezug auf das Management der Risiken kritischer Daten. | Prüfung der inhaltlichen Abstimmung der Strategie im Umgang mit Risiken kritischer Daten mit anderen internen Vorgaben (bspw. Risikopolitik, Grundzüge des institutsweiten Risikomanagements, operationelles Risikomanagement, Geschäfts-, IKT- bzw. Daten-Strategie, usw.). |  |  |
| *Integration in das übergreifende operationelle Risikomanagement bzw. Strategie, Governance und Bewusstsein (Rz 23–26, 30-31, 40, 71 FINMA-RS 23/1):* | | | | |
| 3 | Beurteilung, ob die Risiken kritischer Daten (bspw. mangelnde Data Governance, mangelnde Datenqualität, mangelnde Verfügbarkeit, unerlaubte Datenmanipulation, Datenverlust, Datendiebstahl, Datenbeschädigung) als eigenständige Taxonomie in das übergreifende operationelle Risikomanagement integriert sind und dadurch umfassend, d. h. im Rahmen der Identifikation, Beurteilung, Begrenzung und Überwachung von operationellen Risiken angemessen berücksichtigt werden. |  |  |  |
| 4 | Beurteilung, ob bei der Risikobeurteilung Prüfergebnisse sowie Risiko- und Kontrollbeurteilungen gemäss Rz 30 berücksichtigt werden. |  |  |  |
| 5 | Beurteilung, ob das Oberleitungsorgan für den Umgang mit Risiken kritischer Daten regelmässig eine Strategie genehmigt und die Einhaltung derer überwacht. | Prüfung, ob folgende Aspekte in der Strategie über den Umgang mit kritischen Daten und den Schutzmassnahmen angemessen berücksichtigt werden:   * Institutsspezifische Definition von kritischen Daten, * Systematische Datenidentifikation und Kategorisierung, * Umfassendes Risikomanagement über kritische Daten, * Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) im Umgang mit kritischen Daten, * Dispositiv über Vertraulichkeits-, Integritäts- und Verfügbarkeitsschutzziele von kritischen Daten. |  |  |
| 6 | Beurteilung, ob das Oberleitungsorgan mindestens jährlich die Risikotoleranz für Risiken kritischer Daten nach Massgabe der Risikopolitik in Anbetracht der strategischen und finanziellen Ziele des Instituts beurteilt und genehmigt. |  |  |  |
| 7 | Beurteilung, ob die Identifikation von wesentlichen, inhärenten Risiken in Bezug auf Risiken kritischer Daten angemessen ist, d. h., falls Risiken kritischer Daten nicht als wesentliche, inhärente Risiken identifiziert sind, ist die Nachvollziehbarkeit der Begründung hierfür zu beurteilen. | Prüfung auf Basis einer angemessenen Stichprobe von Elementen zur Identifikation von wesentlichen Risiken und Beurteilung, ob potenzielle Risiken im Zusammenhang mit kritischen Daten erkannt und berücksichtigt werden, und ob die Beurteilung der Wesentlichkeit der inhärenten Risiken der Risikotoleranz entspricht. |  |  |
| 8 | Beurteilung der organisatorischen Massnahmen zur Stärkung des Bewusstseins der Mitarbeitenden und des wesentlichen externen Personals (inkl. Contractors) im Hinblick auf ihre Aufgaben, Kompetenz und Verantwortlichkeiten zur allgemeinen Reduktion von Risiken im Umgang mit kritischen Daten. | Prüfung auf Basis einer angemessenen Stichprobe von Schlüsselmitarbeitenden und des wesentlichen externen Personals (inkl. Contractors), ob ausreichende Massnahmen zur Stärkung des Bewusstseins im Umgang mit kritischen Daten angewendet werden. Eine Auswahl von folgenden Massnahmen ist zu erwarten:   * Bestätigung über die Kenntnisnahme und Einhaltung des Verhaltenskodexes (sog. Code of Conduct), * Schulungen zur Sensibilisierung im Umgang mit kritischen Daten, * Interne Mitteilungen und regelmässige Kommunikation über den Umgang mit kritischen Daten, Datensicherheit und Datenschutz, * Zielgruppenspezifische Schulungen für interne und externe Personen mit (erhöhten) Zugriffsrechten auf kritische Daten. |  |  |
| 9 | Beurteilung der Angemessenheit der durchgeführten Schulungen zum Thema Umgang mit kritischen Daten im Hinblick auf aktuelle Risiken und angemessene zielgruppenspezifische Ausrichtung der Schulung (z.B. für Mitarbeitende mit Zugriff auf kritische Daten, Mitarbeitende mit privilegierten bzw. erhöhten Berechtigungen, Führungskräfte, externes Personal [inkl. Contractors]). |  |  |
| 10 | Beurteilung der Angemessenheit der Berichterstattung an die Geschäftsleitung (Inhalt, Regelmässigkeit usw.) über die Entwicklung der relevanten IKT-Risiken (inkl. Risiken kritischer Daten), die Wirksamkeit von Schlüsselkontrollen und die wesentlichen internen sowie externen Ereignissen. |  |  |  |
| 11 | Beurteilung der Erkenntnisse aus den Prüfungen bzw. Kontrollen der Internen Revision und/oder anderer Kontrollfunktionen (bspw. unabhängige Risikokontrolle) im Zusammenhang mit der Ausgestaltung des Managements der Risiken kritischer Daten und Durchsicht der Sitzungsprotokolle von relevanten Ausschüssen bzw. Funktionen. |  |  |  |
| *Aufgaben, Kompetenzen und Verantwortlichkeiten (Rz 72, 75 FINMA-RS 23/1):* | | | | |
| 12 | **\*\*** Beurteilung der Angemessenheit, Qualifikation und Unabhängigkeit der Einheit, welche die (unabhängige) Kontrollfunktion zur Einhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von kritischen Daten durch geeignete Prozesse, Verfahren und Kontrollen gewährleistet. |  |  |  |
| 13 | **\*\*** Beurteilung der Angemessenheit der Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) im Umgang mit den vom Institut identifizierten kritischen Daten entlang des Lebenszyklus dieser Daten, um die Vertraulichkeit, Integrität und Verfügbarkeit sicherzustellen. | **\*\*** Prüfung auf Basis einer angemessenen Stichprobe von geeigneten Dokumenten für Schlüsselmitarbeitende, ob die AKV im Umgang mit kritischen Daten angemessen definiert und zugeordnet sind. Folgende Aspekte sind zu berücksichtigen:   * Klare Beschreibung der Rollen (Bsp. Data Producer, Data Consumer, Data Administrator, Data Quality Analyst, Data Owner / Steward / Custodian usw.), * Klare Beschreibung der AKV der Rollen, * Klare Beschreibung der Organisation, Funktionsabgrenzung, Berichtslinien und Kommunikationswege. |  |  |
| 14 | **\*\*** Beurteilung der Angemessenheit der Zuweisung von Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) im Umgang mit den vom Institut identifizierten kritischen Daten entlang des Lebenszyklus dieser Daten, um die Vertraulichkeit, Integrität und Verfügbarkeit sicherzustellen. | **\*\*** Prüfung auf Basis einer angemessenen Stichprobe von geeigneten Dokumenten für Schlüsselmitarbeitende, ob die folgenden Aspekte angemessen berücksichtigt werden:   * Qualifikation und Erfahrung, * Funktion, * Verhältnismässigkeit der Zuweisung von Datenelementen pro Datenverantwortlichen. |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Verfahren, Prozesse und Kontrollen (Rz 74, 75, 76–78 FINMA-RS 23/1): | | | | |
| 15 | Beurteilung der Angemessenheit der Schlüsselkontrollen im Umgang mit kritischen Daten, welche die Vertraulichkeit, Integrität und Verfügbarkeit sicherstellen. Angemessene Schlüsselkontrollen werden regelmässig ausgeführt und schützen kritische Daten entlang des gesamten Lebenszyklus. Dieser umfasst: Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Transferieren, Archivieren, Löschen, Vernichten von Daten. | **\*** Prüfung der operativen Wirksamkeit der Schlüsselkontrollen zur Sicherstellung der:   * Vertraulichkeit, bspw. hinsichtlich Kontrollen im Bereich Informationssicherheit und Privacy, Compliance Checks, Access Management, Code of Conduct, Awareness-Training usw. * Integrität, bspw. hinsichtlich Datenqualitätskontrollen, Plausibilitätskontrollen, automatische und/oder manuelle Abgleichungskontrollen, fachliche Genehmigung, Vier-Augen-Prinzip, Funktionstrennung usw. * Verfügbarkeit, bspw. hinsichtlich Überwachung Datenübermittlung und Datenverarbeitung, Rückverfolgbarkeit der Daten, Back-Up und Wiederherstellung von Daten usw. * Vollständigkeit hinsichtlich Datenvernichtung |  |  |
| 16 | **\*** Beurteilung der Prozesse, Verfahren und Kontrollen des Instituts zur Gewährleistung eines angemessenen Grads an Vertraulichkeit bzw. entsprechenden Sicherheitsanforderungen im Umgang mit kritischen Daten während des Betriebs (Run) als auch der Entwicklung, Veränderung und Migration (Change) von kritischen Daten. | **\*** Prüfung der operativen Wirksamkeit der Schlüsselkontrollen des Instituts zur Gewährleistung eines angemessenen Grads an Vertraulichkeit bzw. entsprechenden Sicherheitsanforderungen im Umgang mit kritischen Daten während des Betriebs (Run) als auch der Entwicklung, Veränderung und Migration (Change) von kritischen Daten. |  |  |
| *Inventarisierung (Rz 53, 63, 73 FINMA-RS 23/1):* | | | | |
| 17 | Beurteilung, ob die kritischen Daten der Organisation systematisch identifiziert, erfasst und kategorisiert werden. Ein Dateninventar enthält bspw. folgende Informationsangaben (Attribute):   * Ablageort bzw. Cloudumgebung, * Software (inkl. Versionierung), * Kategorisierung (Kritikalität), * Abhängigkeiten innerhalb des Instituts, * Interne und externe Quellen, * Schnittstellen zu externen Dienstleistern, * Datenverantwortlichkeit. | Prüfung auf Basis einer angemessenen Stichprobe von Plausibilitäts- bzw. Datenqualitätskontrollen des Instituts, die dazu beitragen, die Vollständigkeit und Richtigkeit des Dateninventars zu gewährleisten. |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Zugriffsmanagement (Rz 76–78, 80 FINMA-RS 23/1):* | | | | |
| 18 | **\*** Beurteilung der Angemessenheit von Prozessen, Verfahren und Kontrollen zur Gewährung des Zugriffes auf kritische Daten und verarbeitenden Funktionen für Mitarbeitende und Dritte (Definition von Rollen, Genehmigungsprozesse usw.). | **\*** Prüfung der operativen Wirksamkeit der Kontrollen zur Gewährung des Zugriffs auf kritische Daten und verarbeitende Funktionen für Mitarbeitende und Dritte auf angemessener Stichprobenbasis. Insbesondere sind zu berücksichtigen:   * Need-to-know- / Least-Privilege-Prinzip, * Vorhandensein eines Authentifizierungs- und Autorisierungssystems, * Umfang und Integration von Systemen mit kritischen Daten im Autorisierung- und Identifikationsprozess, * Umfang und Integration von verschiedenen Benutzerkonten (bspw. technische Accounts, System Accounts, privilegierte Accounts, Gäste Accounts, Remote Service Accounts usw.). |  |  |
| 19 | **\*** Beurteilung der Angemessenheit der Prozesse und Kontrollen zur Identifikation, Steuerung und Überwachung des Zugangs (Standard sowie Privilegiert) zu kritischen Daten. | **\*** Prüfung der operativen Wirksamkeit der Schlüsselkontrollen zur Identifikation, Steuerung und Überwachung des Zugangs (sowohl standardisiert als auch privilegiert) zu kritischen Daten auf angemessener Stichprobenbasis. |  |  |
| 20 | **\*** Beurteilung, ob die physische und logische IKT, welche die kritischen Daten speichert oder verarbeitet, angemessen geschützt ist. | **\*** Prüfung auf Basis einer angemessenen Stichprobe kritischer Ressourcen[[2]](#footnote-3), ob kritische Daten bspw. durch Verschlüsselung, sicherer Übertragung und andere technische Massnahmen angemessen geschützt sind. |  |  |
| 21 | | **\*** Beurteilung der Angemessenheit der Kontrollen und Sicherheitsanforderungen für Benutzerprofile mit erhöhten Privilegien. | **\*** Prüfung der Angemessenheit der Kontrollen (Bsp. Auswertung von Log-Dateien, nur temporäre Zugriffsberechtigungserteilung, erhöhte Regelmässigkeit von Review-Kontrollen, Vier-Augen-Prinzip / Peer-Reviews) und Sicherheitsanforderungen für Personen mit erhöhten Privilegien sowie Prüfung, ob eine Liste dieser Personen geführt wird und regelmässig aktualisiert wird. |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Zugriffsmanagement Ausland (Rz 79 FINMA-RS 23/1):* | | | | |
| 22 | **\*\*** Falls kritische Daten ausserhalb der Schweiz gespeichert werden oder vom Ausland aus auf sie zugegriffen werden kann, Beurteilung, ob die damit verbundenen erhöhten Risiken angemessen begrenzt und die Daten angemessen geschützt sind. | **\*\*** Prüfung auf Basis einer angemessenen Stichprobe, ob organisatorische und technische Massnahmen vorhanden sind, um die erhöhten Risiken angemessen zu kontrollieren und kritische Daten angemessen zu schützen, wenn diese ausserhalb der Schweiz gespeichert werden oder vom Ausland aus auf sie zugegriffen werden kann. |  |  |
| *Vorfälle (Rz 81 FINMA-RS 23/1):* | | | | |
| 23 | Beurteilung der Angemessenheit der Prozesse, Verfahren und Kontrollen für das Management von Vorfällen, die die Vertraulichkeit, Integrität oder Verfügbarkeit von kritischen Daten wesentlich beeinträchtigen. | Prüfung der operativen Wirksamkeit des Meldeprozesses an die Finma auf Basis einer angemessenen Stichprobe von Vorfällen, welche die Vertraulichkeit, Integrität oder Verfügbarkeit von kritischen Daten beeinträchtigt haben. |  |  |
| Sorgfaltsprüfung (*Rz 82 FINMA-RS 23/1):* | | | | |
| 24 | Beurteilung der Angemessenheit der Sorgfaltsprüfung (*Due Diligence*) bei der Auswahl von Dienstleistern, die auf kritische Daten zugreifen können oder solche verwalten. | Prüfung auf Basis einer angemessenen Stichprobe von Dienstleistern mit Zugriff auf kritische Daten, ob bei der Auswahl des Dienstleisters eine angemessene Sorgfaltsprüfung (*Due Diligence*) durchgeführt wurde bzw. wird. |  |  |
| 25 | | Beurteilung, ob angemessene Kriterien für den Umgang mit Dienstleistern, die Zugang auf kritische Daten verfügen, definiert und in der Vertragsvereinbarung geregelt werden. | Prüfung auf Basis einer angemessenen Stichprobe von Dienstleistern mit Zugriff auf kritische Daten, ob der Umgang mit kritischen Daten vor Vertragsvereinbarung geprüft und geregelt wurde. |  |  |
| 26 | | Beurteilung, ob Dienstleister mit Zugang zu kritischen Daten im Rahmen des internen Kontrollsystems des Instituts periodisch überwacht und kontrolliert werden. | Prüfung auf Basis einer angemessenen Stichprobe von Dienstleistern mit Zugriff auf kritische Daten, ob deren Datennutzung risikoorientiert periodisch überwacht und kontrolliert werden. |  |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. Rz 33 und 34 FINMA-RS 13/3 [↑](#footnote-ref-2)
2. FINMA-RS 23/1 Anhang 1 [↑](#footnote-ref-3)