**Prüfprogramm – Minimale Prüfungshandlungen**

**Übersicht**

|  |  |
| --- | --- |
| **Prüfgebiet:** | **Informatik (IT)** |
| **Prüftiefe:** | [Prüfung / Kritische Beurteilung] |
| **Vorschriften:**  (Liste ist nicht abschliessend) | Art. 14 Finanzmarktinfrastrukturgesetz (FinfraG)  Art. 15 & 45 Finanzmarktinfrastrukturverordnung (FinfraV)  Art. 32a & 32c Nationalbankverordnung (NBV)  FINMA-Rundschreiben 2008/21 „Operationelle Risiken – Banken“ (sinngemäss) („FINMA-RS 08/21“; Randziffer 135 – 135.12) |
| **Sign-offs:** | |  |  |  |  | | --- | --- | --- | --- | | **Sign-offs:** | **Name:** | **Funktion:** | **Datum:** | | Prüfer: | [Name] | [Assistent / Senior / Manager / Senior Manager / Partner] | [TT MMMM JJJJ] | | Reviewer: | [Name] | [Senior / Manager / Senior Manager  / Partner] | [TT MMMM JJJJ] | |

**Dieses Standard-Prüfprogramm enthält minimale Prüfungshandlungen. Es liegt in der Verantwortung des Prüfteams, das Standard-Arbeitsprogramm an die spezifische Situation (Grösse, Geschäftsmodell, Organisation, Prozesse, Risikoexposure usw.) des geprüften Instituts anzupassen. Werden minimale Prüfungshandlungen nicht vollständig durchgeführt, ist in den Arbeitspapieren eine aussagekräftige Erläuterung dazu anzubringen.**

**Abschliessende Zusammenfassung**

| **Thema:** | **Information / Beschreibung:** |
| --- | --- |
| Über einen Zeitraum von 6 Jahren stufenweise abzudeckende Elemente (einschliesslich Prüftiefe) | |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **Elemente:** | **20XX-2** | **20XX-1** | **20XX** | **20XX+1** | **20XX+2** | **20XX+3** | | IT-Strategie, Organisation und Governance | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | | IT-Risiken und -Kontrollen / Cyber-Risiken | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | | Logische und physische Sicherheit / Informationsschutz | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | | IT-Infrastruktur und IT-Leistungserbringung | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | | IT-Outsourcing und Lieferantenmanagement | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | | Individuelle Datenverarbeitung (End user computing) und Datenqualität | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | [A / CA / –] | |
| Zusammenfassende Gesamtbeurteilung | |  |  | | --- | --- | | **Bestätigung im Prüfbericht:** | **Zusammenfassung:** | | Bestätigung, dass der Bereich „Informatik“ angemessen ausgestaltet war (basierend auf den Erkenntnissen der abgedeckten Elemente).  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 – Element: IT-Strategie, Organisation und Governance**

| **Nr.** | **Thema:** | **Minimale Prüfungshandlungen für Prüftiefe „kritische Beurteilung“:** | **Zusätzliche minimale Prüfungshandlungen für Prüftiefe „Prüfung“:** | **Durchgeführte Prüfungshandlungen / Feststellungen** | **Arbeitspapiere Ref.:** |
| --- | --- | --- | --- | --- | --- |
| *„Confirmation that the area of „IT“ was designed adequately (based on the results of the audit procedures performed in connection with the covered elements)“.*  *„Bestätigung, dass der Bereich „Informatik“ angemessen ausgestaltet war (basierend auf den Erkenntnissen der abgedeckten Elemente)“.*  *„Confirmation que le secteur « informatique » était structuré de manière appropriée (sur la base des constatations relatives aux éléments effectivement couverts)“.* | | | | | |
|  | **IT-Strategie** | *Beurteilung, ob die IT-Strategie des Instituts nach Massgabe der spezifischen Situation des Instituts (Grösse, Geschäftstätigkeit, IT-Komplexität/-Risiken, Auslagerungen usw.) angemessen ist, namentlich* |  |  |  |
|  |  | Aneignung grundlegender Kenntnisse über die IT-Strategie des Instituts |  |  |  |
|  |  | Beurteilung der allgemeinen Angemessenheit interner Regelungen (Richtlinien, Weisungen usw.) in Bezug auf die IT-Strategie / das strategische IT-Projektmanagement |  |  |  |
|  |  | Beurteilung der allgemeinen Angemessenheit des strategischen IT-Projektmanagements |  |  |  |
|  |  | Beurteilung der allgemeinen Übereinstimmung der IT-Strategie mit anderen Dokumenten (Geschäftsstrategie, IT-Risikomanagement-Konzept, IT-Portfolio usw.) |  |  |  |
|  |  | Beurteilung der Angemessenheit interner Prozesse/Kontrollen zur Festlegung, Aktualisierung, Validierung/Abstimmung, Genehmigung und Kommunikation der IT-Strategie (Wirksamkeit der Ausgestaltung) | Beurteilung/Prüfung der operativen Wirksamkeit der Prozesse/Kontrollen zur Festlegung, Aktualisierung, Validierung/Abstimmung, Genehmigung und Kommunikation der IT-Strategie auf Stichprobenbasis |  |  |
|  |  | Beurteilung der Erkenntnisse aus den Prüfungen/Kontrollen der Internen Revision und/oder anderer Kontrollfunktionen (IT-Sicherheit, Risikokontrolle usw.) und/oder Dritter im Zusammenhang mit der IT-Strategie und Untersuchung der Sitzungsprotokolle von relevanten Ausschüssen/Funktionen |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **IT-Organisation und Governance** | *Beurteilung, ob die IT-Organisation und Governance des Instituts nach Massgabe der spezifischen Situation des Instituts (Grösse, Geschäftstätigkeit, IT-Komplexität/-Risiken, Auslagerungen usw.) angemessen ist, namentlich:* |  |  |  |
|  |  | Aneignung grundlegender Kenntnisse über die IT-Organisation und -Governance des Instituts |  |  |  |
|  |  | Beurteilung der allgemeinen Angemessenheit interner Regelungen (Richtlinien, Weisungen usw.) in Bezug auf die IT-Organisation und  -Governance |  |  |  |
|  |  | Beurteilung der Angemessenheit der Rollen und Verantwortlichkeiten innerhalb der IT-Organisation |  |  |  |
|  |  | Beurteilung der allgemeinen Angemessenheit der Unterstellung und Trennung der IT-bezogenen Abteilungen/Funktionen (IT-Entwicklung, IT-Betrieb, IT-Sicherheit usw.), einschliesslich verbundener Kontrollen (Wirksamkeit der Ausgestaltung) | Beurteilung/Prüfung der operativen Wirksamkeit der Prozesse/Kontrollen zur Gewährleistung der Funktionentrennung auf Stichprobenbasis |  |  |
|  |  | Beurteilung der allgemeinen Angemessenheit der internen Prozesse in Bezug auf die Führung von Mitarbeitenden in IT-bezogenen Abteilungen |  |  |  |
|  |  | Beurteilung der Angemessenheit der Überwachung der IT-Performance |  |  |  |
|  |  | Beurteilung der Erkenntnisse aus den Prüfungen/Kontrollen der Internen Revision und/oder anderer Kontrollfunktionen (IT-Sicherheit, Risikokontrolle usw.) und/oder Dritter im Zusammenhang mit der IT-Organisation und  -Governance (inkl. IT-Risikomanagement-Konzept) und Einsichtnahme in die Sitzungsprotokolle von relevanten Ausschüssen/Funktionen |  |  |  |

**Prüfprogramm – Element: IT-Risiken und –Kontrollen / Cyber-Risiken**

| **Nr.** | **Thema:** | **Minimale Prüfungshandlungen für Prüftiefe „kritische Beurteilung“:** | **Zusätzliche minimale Prüfungshandlungen für Prüftiefe „Prüfung“:** | **Durchgeführte Prüfungshandlungen / Feststellungen** | **Arbeitspapiere Ref.:** |
| --- | --- | --- | --- | --- | --- |
| *„Confirmation that the area of „IT“ was designed adequately (based on the results of the audit procedures performed in connection with the covered elements)“.*  *„Bestätigung, dass der Bereich „Informatik“ angemessen ausgestaltet war (basierend auf den Erkenntnissen der abgedeckten Elemente)“.*  *„Confirmation que le secteur « informatique » était structuré de manière appropriée (sur la base des constatations relatives aux éléments effectivement couverts)“.* | | | | | |
|  | **IT-Risiken und  -Kontrollen** | *Beurteilung, ob die Organisation des Instituts hinsichtlich IT-Risiken und -Kontrollen nach Massgabe der spezifischen Situation des Instituts (Grösse, Geschäftstätigkeit, IT-Komplexität/-Risiken, Auslagerungen usw.) angemessen ist und beurteilen, ob ein angemessenes IT-Risikomanagement-Konzept implementiert ist, namentlich* |  |  |  |
|  |  | Aneignung grundlegender Kenntnisse über den Umgang des Instituts mit IT-Risiken und  -Kontrollen (inkl. Auslagerungen) |  |  |  |
|  |  | Beurteilung der Angemessenheit interner Regelungen (Richtlinien, Weisungen usw.) im Zusammenhang mit der Identifikation von IT-Risiken / der Festlegung von IT-Kontrollen |  |  |  |
|  |  | Beurteilung der Existenz eines formalisierten IT-Risikomanagement-Konzepts (Rz 135 FINMA-RS 08/21) und Beurteilung, ob dieses eine Übersicht über die wesentlichsten Bestandteile der Netzwerkinfrastruktur und ein Inventar aller kritischen Applikationen enthält (Rz 135.2 FINMA-RS 08/21) |  |  |  |
|  |  | Beurteilung der Angemessenheit der Rollen, Aufgaben und Verantwortlichkeiten innerhalb der IT Organisation, namentlich in Bezug auf die kritischen Applikationen sowie damit verbundener IT-Infrastruktur und kritischen und/oder sensitiven Daten und Prozesse (Rz 135.3 FINMA-RS 08/21) |  |  |  |
|  |  | Beurteilung der Angemessenheit des Prozesses im Hinblick auf die Identifikation und Beurteilung von IT-Risiken im Rahmen der Sorgfaltsprüfung (Due Diligence) insbesondere bei Auslagerungen (Rz 135.4 FINMA-RS 08/21) |  |  |  |
|  |  | Beurteilung der Angemessenheit der im IT-Risikomanagement-Konzept vorgesehenen Massnahmen zur Stärkung des Bewusstseins der Mitarbeiter im Hinblick auf Ihre Verantwortung zur Reduktion von IT-Risiken sowie zur Einhaltung und Stärkung der IT-Informationssicherheit (Rz 135.5 FINMA-RS 08/21) | Prüfung der Umsetzung und Beurteilung der operativen Wirksamkeit der Massnahmen zur Stärkung des Bewusstseins der Mitarbeiter im Hinblick auf Ihre Verantwortung zur Reduktion von IT-Risiken sowie Einhaltung und Stärkung der IT-Informationssicherheit. |  |  |
|  |  | Beurteilung der Angemessenheit des IT-Risikomanagementkonzepts und dessen Eingliederung in das breiter gefasste Risikomanagementkonzept der Organisation |  |  |  |
|  |  | Beurteilung der Angemessenheit der Zuweisung von Aufgaben und Verantwortlichkeiten zur Steuerung von IT-Risiken / IT-Kontrollen an die betroffenen Abteilungen und deren Integration in andere interne Risikomanagement-/Risikokontrollfunktionen |  |  |  |
|  |  | Beurteilung der Angemessenheit der Prozesse zur Identifikation, Beurteilung, Adressierung und Akzeptanz von IT-bezogenen Schlüsselrisiken | Beurteilung / Prüfung der operativen Wirksamkeit der Prozesse und Kontrollen zur Identifikation, Beurteilung, Adressierung und Akzeptanz von IT-bezogenen Schlüsselrisiken auf Stichprobenbasis |  |  |
|  |  | Beurteilung der Angemessenheit der Prozesse zur Festlegung und Überwachung der IT-bezogenen Kontrollen, welche die relevanten Risiken reduziert (Wirksamkeit der Ausgestaltung) | Beurteilung / Prüfung der operativen Wirksamkeit der Prozesse und Kontrollen zur Ermittlung und Überwachung von IT-bezogenen Schlüsselrisiken / IT-bezogenen Risiken auf Stichprobenbasis |  |  |
|  |  | Beurteilung der allgemeinen Angemessenheit der internen Berichterstattung bezüglich IT-Risiken und -Kontrollen an die Leitungsorgane / internen (Kontroll-)Funktionen | Beurteilung / Prüfung der Angemessenheit der internen Berichterstattung in Zusammenhang mit IT-Risiken und -Kontrollen an die Leitungsorgane / internen (Kontroll-)Funktionen auf Stichprobenbasis |  |  |
|  |  | Beurteilung der Erkenntnisse aus den Prüfungen der Internen Revision und/oder anderer Kontrollfunktionen (IT-Sicherheit, Risikokontrolle usw.) und/oder Dritter im Zusammenhang mit der Identifikation von IT-Risiken / Festlegung von IT-Kontrollen |  |  |  |
|  | **Cyber-Risiken** | *Beurteilung, ob die Organisation des Instituts hinsichtlich Umgang mit Cyber-Risiken nach Massgabe der spezifischen Situation des Instituts (Grösse, Geschäftstätigkeit, IT-Komplexität/-Risiken, Auslagerungen usw.) angemessen ist, namentlich* |  |  |  |
|  |  | Beurteilung der Angemessenheit und der Vollständigkeit des Konzepts zur Bewirtschaftung von Cyber-Risiken (Rz 135.6 – 135.11 FINMA-RS 08/21) bezüglich:   * Identifikation der institutsspezifischen Bedrohungspotenziale durch Cyber-Attacken, insbesondere in Bezug auf kritische und/ oder sensitive Daten und IT-Systeme. Definition von Schutz- und Gegenmassnahmen für die identifizierten Bedrohungspotenziale * Schutz der Geschäftsprozesse und der Technologieinfrastruktur vor Cyber-Attacken unter Berücksichtigung der Dimensionen Mensch, Prozesse und Technologie * zeitnahe Erkennung und Aufzeichnung von Cyber-Attacken auf Basis von Prozessen und Technologie zur systematischen Überwachung der Technologieinfrastruktur * Reaktion auf Cyber-Attacken durch zeitnahe und gezielte Massnahmen sowie bei wesentlichen, die Aufrechterhaltung des normalen Geschäftsbetriebs bedrohenden Cyber-Attacken in Abstimmung mit dem BCM (Business Continuity Management) * Sicherstellung einer zeitnahen Wiederherstellung des normalen Geschäftsbetriebs nach Cyber-Attacken durch geeignete  Massnahmen (unter Berücksichtigung der Schutzziele Verfügbarkeit und Integrität der Systeme und Daten) | Prüfung, ob die Identifikation der institutsspezifischen Bedrohungspotenziale durch Cyber-Attacken insbesondere in Bezug auf die kritischen und/oder sensitiven Daten und IT-Systeme periodisch unter Teilnahme aller relevanter Stakeholder im Institut erfolgt.  Prüfung, ob die Schutz- und Gegenmassnahmen für die identifizierten Bedrohungspotenziale periodisch und angemessen auf ihre Wirksamkeit hin getestet und die Ergebnisse entsprechend rapportiert werden.  Prüfung, ob im Rahmen der Schutzmassnahmen vor Cyberrisiken die Dimensionen Mensch, Prozesse und Technologie gleichermassen und angemessen berücksichtigt werden.  Prüfung der Wirksamkeit der Aufzeichnung und Erkennung von Cyber-Attacken anhand von effektiv aufgetretenen Fällen.  Prüfung, ob entsprechende Simulationen (Cyber Security Incident Simulations) bezüglich Reaktion auf Cyber-Attacken durchgeführt wurden und mit welchem Ergebnis. Überprüfung, ob diese Aktivitäten angemessen mit dem BCM der Bank abgestimmt sind.  Überprüfung der Resultate von Wiederherstellungstests (Verfügbarkeit und Integrität der Systeme und Daten) im Zusammenhang mit Cyber-Attacken |  |  |
|  |  | Beurteilung der Angemessenheit der Prozesse zur Durchführung von Verwundbarkeitsanalysen und Penetration Testings sowie der dafür vorgesehenen Ressourcen (Rz 135.12 FINMA-RS 08/21) | Beurteilung / Prüfung der operativen Wirksamkeit der Prozesse und Kontrollen in Zusammenhang mit Verwundbarkeitsanalysen und Penetration Tests (Rz 135.12 FINMA-RS 08/21), inkl. der Schliessung von gefundenen Schwachstellen. |  |  |

**Prüfprogramm – Element: Logische und physische Sicherheit / Informationsschutz**

| **Nr.** | **Thema:** | **Minimale Prüfungshandlungen für Prüftiefe „kritische Beurteilung“:** | **Zusätzliche minimale Prüfungshandlungen für Prüftiefe „Prüfung“:** | **Durchgeführte Prüfungshandlungen / Feststellungen** | **Arbeitspapiere Ref.:** |
| --- | --- | --- | --- | --- | --- |
| *„Confirmation that the area of „IT“ was designed adequately (based on the results of the audit procedures performed in connection with the covered elements)“.*  *„Bestätigung, dass der Bereich „Informatik“ angemessen ausgestaltet war (basierend auf den Erkenntnissen der abgedeckten Elemente)“.*  *„Confirmation que le secteur « informatique » était structuré de manière appropriée (sur la base des constatations relatives aux éléments effectivement couverts)“.* | | | | | |
|  | **Logische und physische Sicherheit / Schutz von Informationen** | *Beurteilung, ob die Organisation des Instituts hinsichtlich logischer und physischer Sicherheit / Informationsschutz nach Massgabe der spezifischen Situation des Instituts (Grösse, Geschäftstätigkeit, IT-Komplexität/-Risiken, Auslagerungen usw.) angemessen ist, namentlich* |  |  |  |
|  |  | Aneignung grundlegender Kenntnisse über den Umgang des Instituts mit logischer/physischer Sicherheit und dem Schutz von Informationen |  |  |  |
|  |  | Beurteilung der Angemessenheit der internen Regelungen (Richtlinien, Weisungen usw.) im Zusammenhang mit Informationssicherheit |  |  |  |
|  |  | Beurteilung der organisatorischen Massnahmen des Instituts zur Gewährleistung eines angemessenen Grads an Informationssicherheit (Unterstellung / Organisation der involvierten Abteilungen, Funktionentrennung, Beschreibung von Aufgaben/Verantwortlichkeiten der involvierten Abteilungen, personelle/technische Ressourcen, Meldepflichten/Eskalationsprozesse, Datenklassifizierung und Daten-Ownership usw.) | Beurteilung/Prüfung der operativen Wirksamkeit der organisatorischen Massnahmen und Kontrollen des Instituts zur Gewährleistung eines angemessenen Grads an Informationssicherheit |  |  |
|  |  | Beurteilung der Angemessenheit von Prozessen und Kontrollen zur Gewährung des logischen/ physischen Zugangs zu IT-Systemen/Applika­tionen/Räumlichkeiten für Mitarbeitende und Dritte (Definition von Rollen, Genehmigungsprozessen usw.) (Wirksamkeit der Ausgestaltung) | Beurteilung/Prüfung der operativen Wirksamkeit der Kontrollen zur Gewährung des logischen/ physischen Zugangs zu IT-Systemen/Applika­tionen/Räumlichkeiten für Mitarbeitende und Dritte auf Stichprobenbasis |  |  |
|  |  | Beurteilung der Angemessenheit von Prozessen und Kontrollen zur (regelmässigen) Bestätigung des logischen/physischen Zugangs zu IT-Systemen/Applikationen/Räumlichkeiten für Mitarbeitende und Dritte (Wirksamkeit der Ausgestaltung) | Beurteilung/Prüfung der operativen Wirksamkeit der Kontrollen zur (regelmässigen) Bestätigung des logischen/physischen Zugangs zu IT-Systemen/Applikationen/Räumlichkeiten für Mitarbeitende und Dritte auf Stichprobenbasis |  |  |
|  |  | Beurteilung der Angemessenheit der Prozesse und Kontrollen zur Identifikation, Steuerung und Überwachung des privilegierten Zugangs zu IT-Systemen/Applikationen (Wirksamkeit der Ausgestaltung) | Beurteilung/Prüfung der operativen Wirksamkeit der Kontrollen zur Identifikation, Steuerung und Überwachung des privilegierten Zugangs zu IT-Systemen/Applikationen auf Stichprobenbasis |  |  |
|  |  | Beurteilung der Angemessenheit der Prozesse und Kontrollen zur Steuerung der Infrastruktur- und Netzwerksicherheit (z. B. Firewalls, IDS, Virenschutz usw.) (Wirksamkeit der Ausgestaltung) | Beurteilung/Prüfung der operativen Wirksamkeit der Kontrollen zur Steuerung der Infrastruktur- und Netzwerksicherheit (z. B. Firewalls, IDS, Virenschutz usw.) auf Stichprobenbasis |  |  |
|  |  | Beurteilung der allgemeinen Angemessenheit der internen Berichterstattung bezüglich Informationssicherheit an die Leitungsorgane/internen (Kontroll-)Funktionen |  |  |  |
|  |  | Beurteilung der Erkenntnisse aus den Prüfungen der Internen Revision und/oder anderer Kontrollfunktionen (IT-Sicherheit, Risikokontrolle usw.) und/oder Dritter im Zusammenhang mit Informationssicherheit |  |  |  |

**Prüfprogramm – Element: IT-Infrastruktur und IT-Leistungserbringung**

| **Nr.** | **Thema:** | **Minimale Prüfungshandlungen für Prüftiefe „kritische Beurteilung“:** | **Zusätzliche minimale Prüfungshandlungen für Prüftiefe „Prüfung“:** | **Durchgeführte Prüfungshandlungen / Feststellungen** | **Arbeitspapiere Ref.:** |
| --- | --- | --- | --- | --- | --- |
| *„Confirmation that the area of „IT“ was designed adequately (based on the results of the audit procedures performed in connection with the covered elements)“.*  *„Bestätigung, dass der Bereich „Informatik“ angemessen ausgestaltet war (basierend auf den Erkenntnissen der abgedeckten Elemente)“.*  *„Confirmation que le secteur « informatique » était structuré de manière appropriée (sur la base des constatations relatives aux éléments effectivement couverts)“.* | | | | | |
|  | **IT-Infrastruktur und IT-Leistungs­erbringung** | *Beurteilung, ob die Organisation des Instituts hinsichtlich IT-Infrastruktur und IT-Leistungs­erbringung nach Massgabe der spezifischen Situation des Instituts (Grösse, Geschäftstätigkeit, IT-Komplexität/-Risiken, Auslagerungen usw.) angemessen ist, namentlich* |  |  |  |
|  |  | Aneignung grundlegender Kenntnisse über die IT-Infrastrukturumgebung und das IT-Leistungs­erbringungsmodell des Instituts (einschliesslich Änderungsmanagementprozessen [change management processes]) |  |  |  |
|  |  | Beurteilung der Angemessenheit interner Regelungen (Richtlinien, Weisungen usw.) im Zusammenhang mit IT-Infrastruktur / IT-Leistungserbringung / Änderungsmanagement der Programme |  |  |  |
|  |  | Beurteilung der Angemessenheit der Zuweisung von Aufgaben und Verantwortlichkeiten zur Steuerung und Überwachung der IT-Infrastruktur und der Aufgaben betreffend die IT-Leistungserbringung (Lebenszyklusmanagement der IT-Infrastruktur, Überwachung, Service Level Management, Änderungsmanagement der Programme usw.) |  |  |  |
|  |  | Beurteilung der Angemessenheit des Änderungs- / Release-Managementprozesses in Zusammenhang mit der IT-Infrastruktur und den Applikationen (Testen/Genehmigung von Änderungen, Umsetzung von Änderungen [einschl. Funktionentrennung] usw. (Wirksamkeit der Ausgestaltung) | Beurteilung/Prüfung der operativen Wirksamkeit des Änderungs- / Release-Managementprozesses in Zusammenhang mit der IT-Infrastruktur und den Applikationen auf Stichprobenbasis |  |  |
|  |  | Beurteilung der Angemessenheit des Prozesses zur Gewährleistung einer vollständigen, korrekten und zeitnahen Verarbeitung von System-Jobs (einschl. Überwachung von Batch-Jobs, Änderungsmanagement, Zugangskontrolle und zeitnahe und ordnungsgemässe Behebung von Fehlern bei der Verarbeitung) (Wirksamkeit der Ausgestaltung) | Beurteilung/Prüfung der operativen Wirksamkeit des Prozesses zur Gewährleistung einer vollständigen, korrekten und zeitnahen Verarbeitung von System-Jobs auf Stichprobenbasis |  |  |
|  |  | Beurteilung der Angemessenheit des Störungs- und Problemmanagement-Prozesses (Aufdeckung von Störungen/Problemen, Eskalation, Reporting, angemessene Behebung usw.) (Wirksamkeit der Ausgestaltung) | Beurteilung/Prüfung der operativen Wirksamkeit des Störungs- und Problemmanagement-Prozesses auf Stichprobenbasis |  |  |
|  |  | Beurteilung der Angemessenheit des Back-up- und Wiederherstellungsprozesses (Wirksamkeit der Ausgestaltung) | Beurteilung/Prüfung der operativen Wirksamkeit des Back-up- und Wiederherstellungsprozesses auf Stichprobenbasis |  |  |
|  |  | Beurteilung des Prozesses zur Gewährleistung vollständiger und korrekter Daten im IT Asset Inventory / in der Configuration Management Database (CMDB) |  |  |  |
|  |  | Beurteilung der allgemeinen Angemessenheit der internen Berichterstattung im Zusammenhang mit der IT-Infrastruktur / IT-Leistungs­erbringung an die Leitungsorgane / internen (Kontroll-)Funktionen |  |  |  |
|  |  | Überprüfung der Erkenntnisse aus den Prüfungen der Internen Revision und/oder anderer Kontrollfunktionen (IT-Sicherheit, Risikokontrolle usw.) und/oder Dritter im Zusammenhang mit der IT-Infrastruktur / IT-Leistungserbringung |  |  |  |

**Prüfprogramm – Element: IT-Outsourcing und Lieferantenmanagement**

| **Nr.** | **Thema:** | **Minimale Prüfungshandlungen für Prüftiefe „kritische Beurteilung“:** | **Zusätzliche minimale Prüfungshandlungen für Prüftiefe „Prüfung“:** | **Durchgeführte Prüfungshandlungen / Feststellungen** | **Arbeitspapiere Ref.:** |
| --- | --- | --- | --- | --- | --- |
| *„Confirmation that the area of „IT“ was designed adequately (based on the results of the audit procedures performed in connection with the covered elements)“.*  *„Bestätigung, dass der Bereich „Informatik“ angemessen ausgestaltet war (basierend auf den Erkenntnissen der abgedeckten Elemente)“.*  *„Confirmation que le secteur « informatique » était structuré de manière appropriée (sur la base des constatations relatives aux éléments effectivement couverts)“.* | | | | | |
|  | **IT-Outsourcing und Lieferantenmanagement** | *Beurteilung, ob die Organisation des Instituts hinsichtlich IT-Outsourcing und Lieferantenmanagement nach Massgabe der spezifischen Situation des Instituts (Grösse, Geschäftstätigkeit, IT-Komplexität/-Risiken, Auslagerungen usw.) angemessen ist, namentlich* |  |  |  |
|  |  | Aneignung grundlegender Kenntnisse über den Ansatz des Instituts bezüglich IT-Outsourcing und Lieferantenmanagement |  |  |  |
|  |  | Beurteilung der Angemessenheit interner Regelungen (Richtlinien, Weisungen usw.) im Zusammenhang mit IT-Outsourcing und Lieferantenmanagement |  |  |  |
|  |  | Beurteilung der Angemessenheit der Zuweisung von Aufgaben und Verantwortlichkeiten zur Steuerung/Überwachung von IT-Outsourcing-Dienstleistern und IT-Anbietern (Auswahl. Überwachung usw.) |  |  |  |
|  |  | Beurteilung der Angemessenheit des Prozesses zur Auswahl von IT-Dienstleistern/Anbietern (Auswahlkriterien, Genehmigungsprozess usw.) | Beurteilung/Prüfung der operativen Wirksamkeit des Prozesses zur ordnungsgemässen Auswahl von IT-Dienstleistern/Anbietern auf Stichprobenbasis |  |  |
|  |  | Beurteilung der Angemessenheit des Prozesses zur ordnungsgemässen Überwachung und Bewertung von IT-Dienstleistern/Anbietern (KPIs, Service Reports, Bewertungsprogramm usw.) (Wirksamkeit der Ausgestaltung) | Beurteilung/Prüfung der operativen Wirksamkeit des Prozesses zur ordnungsgemässen Überwachung und Bewertung von IT-Dienstleistern/Anbietern auf Stichprobenbasis |  |  |
|  |  | Beurteilung der Angemessenheit des Post-Deal-Risikobewertungsprozesses für IT-Dienstleister/ Anbieter und dessen Eingliederung in das breiter gefasste Risikomanagementkonzept der Organisation (Wirksamkeit der Ausgestaltung) | Beurteilung/Prüfung der operativen Wirksamkeit des Post-Deal-Risikobewertungsprozesses für IT-Dienst­leister/Anbieter und dessen Eingliederung in das breiter gefasste Risikomanagementkonzept der Organisation auf Stichprobenbasis |  |  |
|  |  | Beurteilung der Angemessenheit des Prozesses zur Beurteilung oder zur Gewährleistung von Schlüsselkontrollen, die an Dienstleister ausgelagert wurden (z. B. unabhängige Beurteilungen, SOC-Berichte usw.) |  |  |  |
|  |  | Beurteilung der Angemessenheit des Prozesses zur Aufdeckung, Beurteilung und Behebung von Mängeln bezüglich der Qualität der Leistungserbringung von IT-Dienstleistern/Anbietern (Wirksamkeit der Ausgestaltung) | Beurteilung/Prüfung der Angemessenheit des Prozesses zur Aufdeckung, Beurteilung und Behebung von Mängeln bezüglich der Qualität der Leistungserbringung von IT-Dienstleistern/Anbietern auf Stichprobenbasis |  |  |
|  |  | Beurteilung der allgemeinen Angemessenheit der internen Berichterstattung im Zusammenhang mit IT-Outsourcing und Lieferantenmanagement an die Leitungsorgane / internen (Kontroll-)Funktionen |  |  |  |
|  |  | Überprüfung der Erkenntnisse aus den Prüfungen der Internen Revision und/oder anderer Kontrollfunktionen (IT-Sicherheit, Risikokontrolle usw.) und/oder Dritter im Zusammenhang mit IT-Outsourcing und Lieferantenmanagement |  |  |  |
|  |  | Hinweis: Sofern das Outsourcing die im FINMA-Rundschreiben 2018/3 aufgeführten Kriterien für Outsourcing erfüllt, muss die Outsourcing-Beziehung den Vorgaben des Rundschreibens entsprechen Im Rahmen dieses Prüfprogramms wird die Einhaltung dieser Vorgaben nicht überprüft, da dies Bestandteil des Prüffelds ist, das sich auf Outsourcing bezieht |  |  |  |

**Prüfprogramm – Element: Individuelle Datenverarbeitung (End user computing) und Datenqualität**

| **Nr.** | **Thema:** | **Minimale Prüfungshandlungen für Prüftiefe „kritische Beurteilung“:** | **Zusätzliche minimale Prüfungshandlungen für Prüftiefe „Prüfung“:** | **Durchgeführte Prüfungshandlungen / Feststellungen** | **Arbeitspapiere Ref.:** |
| --- | --- | --- | --- | --- | --- |
| *„Confirmation that the area of „IT“ was designed adequately (based on the results of the audit procedures performed in connection with the covered elements)“.*  *„Bestätigung, dass der Bereich „Informatik“ angemessen ausgestaltet war (basierend auf den Erkenntnissen der abgedeckten Elemente)“.*  *„Confirmation que le secteur « informatique » était structuré de manière appropriée (sur la base des constatations relatives aux éléments effectivement couverts)“.* | | | | | |
|  | **Individuelle Datenverarbeitung und Datenqualität** | *Beurteilung, ob die Organisation des Instituts hinsichtlich der individuellen Datenverarbeitung und Datenqualität nach Massgabe der spezifischen Situation des Instituts (Grösse, Geschäftstätigkeit, IT-Komplexität/-Risiken, Auslagerungen usw.) angemessen ist, namentlich* |  |  |  |
|  |  | Aneignung grundlegender Kenntnisse über die Nutzung der individuellen Datenverarbeitung (IDV) und des allgemeinen Datenqualitätsansatzes des Instituts |  |  |  |
|  |  | Beurteilung der Angemessenheit interner Regelungen (Richtlinien, Weisungen usw.) im Zusammenhang mit IDV und Datenqualität |  |  |  |
|  |  | Beurteilung der Angemessenheit der Zuweisung von Aufgaben und Verantwortlichkeiten zur Steuerung/Überwachung von IDV und Datenqualität |  |  |  |
|  |  | Beurteilung der Angemessenheit des Prozesses zur Identifikation von IDV-Anwendungen und des Prozesses zur Pflege des IDV-Inventars (Wirksamkeit der Ausgestaltung) | Beurteilung/Prüfung der operativen Wirksamkeit des Prozesses zur Identifikation von IDV-Anwendungen und des Prozesses zur Pflege des IDV-Anwendungsinventars auf Stichprobenbasis |  |  |
|  |  | Beurteilung der Angemessenheit des Prozesses zur Gewährleistung einer angemessenen Dokumentation von IDV-Anwendungen (einschliesslich Zweck, Owners, Nutzer, Kritikalität usw.) (Wirksamkeit der Ausgestaltung) | Beurteilung/Prüfung der operativen Wirksamkeit des Prozesses zur Gewährleistung einer angemessenen Dokumentation von IDV-Anwendungen auf Stichprobenbasis |  |  |
|  |  | Beurteilung der Angemessenheit der Zugangskontrollprozesse für IDV-Anwendungen (sofern als notwendig erachtet) (Wirksamkeit der Ausgestaltung) | Beurteilung/Prüfung der operativen Wirksamkeit der Zugangskontrollprozesse für IDV-Anwendungen auf Stichprobenbasis |  |  |
|  |  | Beurteilung der Angemessenheit des Änderungs­managementprozesses für IDV-Anwendungen (einschliesslich Genehmigung und Tests von Änderungen, Versionenkontrolle) (Wirksamkeit der Ausgestaltung) | Beurteilung /Prüfung der operativen Wirksamkeit des Änderungsmanagementprozesses für IDV-Anwendungen auf Stichprobenbasis |  |  |
|  |  | Beurteilung des Prozesses zur Gewährleistung, dass die IDV-Anwendungen mit adäquaten Kontrollen (Berechnungen, Verarbeitungs-/Input-/Output-Kontrollen, Zellschutz usw.) ausgestattet sind (Wirksamkeit der Ausgestaltung) | Beurteilung/Prüfung der operativen Wirksamkeit des Prozesses, der sicherstellt, dass IDV-Anwendun­gen mit adäquaten Kontrollen ausgestattet sind, auf Stichprobenbasis |  |  |
|  |  | Beurteilung der allgemeinen Angemessenheit des Data-Governance-Prozesses / der Data-Governance-Prozesse zur Gewährleistung der Datenqualität |  |  |  |
|  |  | Beurteilung des Prozesses zur Überwachung der Datenqualität (einschliesslich qualitätsbezogener KPIs) |  |  |  |
|  |  | Beurteilung der allgemeinen Angemessenheit der internen Berichterstattung im Zusammenhang mit IDV an die Leitungsorgane / internen (Kontroll-)Funktionen |  |  |  |
|  |  | Überprüfung der Erkenntnisse aus den Prüfungen der Internen Revision und/oder anderer Kontrollfunktionen (IT-Sicherheit, Risikokontrolle usw.) und/oder Dritter im Zusammenhang mit individueller Datenverarbeitung und Datenqualität |  |  |  |

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