
Anlage Informationssicherheit

Version 2.1 – Typ 2

Inhaltsverzeichnis

0	Gegenstand der Anlage Informationssicherheit	3
1	Informationssicherheitsmanagement	3
2	Informationsverbund.....	3
3	Sollmaßnahmen	4
4	Management von IKT-Risiken	4
5	Schulung und Sensibilisierung.....	4
6	Mandantenfähigkeit.....	4
7	Entwicklung und Test	5
8	IKT-Betrieb	5
9	Identitäts- und Rechtemanagement	6
10	Schutzmaßnahmen.....	7
11	Überwachung und Protokollierung	8
12	Datensicherung und Wiederherstellung	9
13	Business Continuity Management / Notfallmanagement	9
14	Management von Schwachstellen	10
15	Überprüfung der Sicherheit.....	11
16	Management von IKT-bezogenen Vorfällen	12
17	Eingeschränkte oder Nicht-Umsetzbarkeit der Anforderungen	13
18	Regelmäßige Berichte	13
19	Prüf- und Kontrollrechte	14

0 Gegenstand der Anlage Informationssicherheit

Gegenstand der nachfolgenden Ausführungen sind die Definition sowie die Spezifizierung der Verantwortlichkeiten, Pflichten und Leistungen des Auftragnehmers zur Aufrechterhaltung der Informationssicherheit gemäß den Anforderungen des Auftraggebers für den vereinbarten Leistungsgegenstand. Die definierten Anforderungen beziehen sich auf die IKT-Systeme, IKT-Assets und Prozesse des Auftragnehmers, die im Rahmen der Leistungserbringung vom Auftragnehmer eingesetzt bzw. betrieben werden bzw. welche die Leistungserbringung beeinflussen können.

Die gestellten Anforderungen berücksichtigen insbesondere die gesetzlichen Anforderungen gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor (DORA).

1 Informationssicherheitsmanagement

Der Auftragnehmer betreibt ein zertifiziertes Informationssicherheitsmanagementsystem ("ISMS") auf Grundlage eines gängigen Standards wie z.B. ISO/IEC 27001 oder BSI IT-Grundschutz und muss dies mittels Nachweisen belegen (z.B. Zertifikate, Audit-Bericht durch externe Stellen oder einer akkreditierten Stelle). Die Nachweise sind mindestens alle zwei Jahre zu erneuern bzw. zu bestätigen. Kopien der Zertifikate oder internen Berichte werden dem Auftraggeber unentgeltlich zur Verfügung gestellt.

Diese Anforderungen gelten ebenfalls für Subdienstleister des Auftragnehmers, die wesentlich zur vertraglich festgelegten Leistung beitragen.

Cloud-Dienstleistungen werden vom Auftraggeber auf Grundlage eines geeigneten Standards erbracht, wie z.B. des BSI Kriterienkatalogs C5 (Cloud-Computing Compliance Criteria Catalogue), der Cloud Controls Matrix (CCM) der Cloud Security Alliance (CSA) oder vergleichbaren Standards. Dies muss mit geeigneten Nachweisen (Zertifikate, Testate) belegt werden können.

Die Parteien verpflichten sich, geeignete und zentrale Ansprechpartner für die Informationssicherheit zu benennen und bekanntzugeben. Der Auftragnehmer hat die Funktion eines Informationssicherheitsbeauftragten oder Chief Information Security Officers eingerichtet.

Der Auftragnehmer lässt einmal jährlich eine Auditierung gemäß der Standards ISAE 3402 Typ 2 oder IDW PS 951 Typ B durchführen (Kontrollen / IKS) und stellt den Bericht dem Auftraggeber unentgeltlich zur Verfügung.

Der Auftragnehmer ist verpflichtet den Auftraggeber unverzüglich über Beeinträchtigungen des Informationssicherheitsmanagementsystems („ISMS“) zu informieren.

2 Informationsverbund

Der Auftragnehmer verfügt über einen aktuellen und dokumentierten Überblick über die Bestandteile seines Informationsverbundes bzw. seiner IKT-Landschaft, d.h. aller zur Erbringung der Dienstleistung eingesetzten IKT-Assets, Schnittstellen und deren Beziehung zueinander und stellt die Übersicht dem Auftraggeber bei Bedarf unentgeltlich zur Verfügung.

Auf Basis dieses Überblicks werden vom Auftragnehmer die jeweiligen Schutzbedarfe regelmäßig und anlassbezogen erhoben, wobei insbesondere die Schutzziele „Integrität“, „Verfügbarkeit“, „Vertraulichkeit“ und „Authentizität“ berücksichtigt werden. Das Schutzziel der „Authentizität“ kann in einem anderen Schutzziel inkludiert werden. Die

Schutzbedarfe des Auftragnehmers berücksichtigen die durch den Auftraggeber festgelegten und übermittelten Schutzbedarfe.

3 Sollmaßnahmen

Auf Grundlage der festgelegten Schutzbedarfe hat der Auftragnehmer in Absprache mit dem Auftraggeber Sollmaßnahmen definiert, die zur Erreichung des jeweiligen Schutzbedarfs angemessen sind. Diese berücksichtigen die in diesem Dokument definierten Informationssicherheitsanforderungen.

Der Auftragnehmer verpflichtet sich, gemäß der durch den Auftraggeber festgelegten Schutzbedarfe, angemessene Schutzmaßnahmen auf Grundlage der definierten Sollmaßnahmen umzusetzen.

Der Auftragnehmer prüft regelmäßig, ob die tatsächlich umgesetzten Maßnahmen den definierten Sollmaßnahmen entsprechen (Soll-Ist Abgleich). Die Ergebnisse des Soll-Ist Abgleiches werden im jährlichen Bericht zur Informationssicherheit dokumentiert.

4 Management von IKT-Risiken

Der Auftragnehmer verfügt über festgelegte und dokumentierte Verfahren zum Management von IKT-Risiken inklusive Überwachungsprozesse, welche alle damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege definieren und aufeinander abstimmen, sowie hierfür angemessene Risikosteuerungs- und Controlling-Prozesse vorsehen.

Ein aktuelles IKT-Risikoinventar, aus dem auch Risiken aus der operativen IT-Sicherheit, z.B. aus dem Schwachstellenmanagement, hervorgehen, wird vom Auftragnehmer gepflegt.

Auf der Basis des IKT-Risikomanagements weist der Auftragnehmer den Auftraggeber unverzüglich und initiativ auf konkrete Veränderungen der Risikosituation, insbesondere bei akuter Veränderung der Bedrohungslage oder der Verwundbarkeit der durch den Auftraggeber betreuten Systeme und vereinbarten Services, hin. Er schlägt risikoreduzierende Maßnahmen vor und initiiert deren Umsetzung im Rahmen der vereinbarten Prozesse zeit- und anforderungsgerecht.

Der Auftragnehmer stellt dem Auftraggeber jährlich einen Bericht zu den identifizierten IKT-Risiken unentgeltlich zur Verfügung.

5 Schulung und Sensibilisierung

Der Auftragnehmer stellt sicher, dass seine Mitarbeiter regelmäßig zum Thema Informationssicherheit geschult werden und die festgelegten Vorgaben und Prozesse zur Informationssicherheit kennen.

Im Rahmen organisatorischer Maßnahmen stellt der Auftragnehmer sicher, dass die eingesetzten Mitarbeiter über angemessenes und aktuelles Wissen hinsichtlich des korrekten Umgangs mit sicherheitsrelevanten und vertraulichen Informationen (z.B. Daten, Informationen über Betriebsverfahren, Netzstrukturen oder sonstige technische Details) und IKT-Assets des Auftraggebers verfügen.

6 Mandantenfähigkeit

Für ausgelagerte IKT-Systeme oder Systemteile der IFB Hamburg die nicht ausschließlich durch das Institut genutzt werden, muss der Auftragnehmer deren uneingeschränkte Mandantenfähigkeit nachweisen, d.h. insbesondere:

- Es ist sicherzustellen, dass Störungen bei anderen Mandanten nicht die Abläufe und Systeme des Auftraggebers beeinträchtigen.
- Es ist sicherzustellen, dass Weisungen verschiedener Mandanten unabhängig voneinander Rechnung getragen werden kann.
- Es ist sicherzustellen, dass Daten des Auftraggebers unter allen Umständen nicht anderen Mandanten des Auftragnehmers oder weiteren Unbeteiligten zugänglich werden.
- Falls zuvor Genanntes nach Ansicht des Auftraggebers nicht zuverlässig durch eine logische Trennung umgesetzt werden kann, muss die Mandantentrennung durch physische Trennung (d.h. dezidierte Hardware) umgesetzt werden.
- Die gemeinsame Nutzung von Hardware mit anderen Mandanten ist zulässig, sofern Daten und Softwarekomponenten des Auftraggebers vollständig gekapselt sind (bspw. durch Verschlüsselung) von Daten und Softwarekomponenten anderer Mandanten.

Die Mandantenfähigkeit ist dem Auftraggeber durch den Auftragnehmer in einem Mandantenkonzept nachzuweisen.

7 Entwicklung und Test

Der Auftragnehmer verfügt, sofern die Leistungserbringung auch Softwareentwicklung bzw. Programmierung beinhaltet, über festgelegte und dokumentierte Vorgaben und Prozesse zur sicheren Entwicklung. Diese beinhalten u.a.:

- Vorgaben zur sicheren Entwicklung,
- Schutz der Entwicklungsumgebungen und Quellcode-Repositories,
- Quell-Code Reviews,
- Versionskontrolle,
- Verfahren zum Test, zur Abnahme und Freigabe,
- Änderungskontrollverfahren.

Der Auftragnehmer berücksichtigt beim Entwicklungsprozess den festgelegten Schutzbedarf sowie potentielle Bedrohungsszenarien und stellt durch geeignete Maßnahmen die Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität nachvollziehbar sicher.

Sofern Open-Source-Bibliotheken oder Bibliotheken von Dritten für IKT-Systeme im Rahmen der Leistungserbringung verwendet werden, muss der Auftragnehmer diese Bibliotheken soweit wie möglich zurückverfolgen.

Der Auftragnehmer führt vor jeder technischen Änderung und nach jeder Wartung eines IKT-Systems, angemessene Tests im Rahmen der abgestimmten Prozesse durch.

Der Auftragnehmer verpflichtet sich, Entwicklungs-, Test- und Produktions-Umgebungen zu trennen.

In Entwicklungsumgebungen werden ausschließlich anonymisierte oder pseudonymisierte Produktionsdaten verarbeitet.

Erfolgt die Entwicklung auf IKT-Systemen, die durch den Auftraggeber bereitgestellt werden, sind die Vorgaben zur Anwendungsentwicklung des Auftraggebers einzuhalten.

8 IKT-Betrieb

Abläufe für die Bedienung der IKT-Systeme sind dokumentiert und den entsprechenden Benutzern zugänglich gemacht.

Der Auftragnehmer verpflichtet sich, Änderungen an Anwendungen, IKT-Systemen sowie Konfiguration von IKT-Assets durch formale und festgelegte Verfahren zu steuern (Änderungskontrolle). Dies beinhaltet auch einen Prozess für Sicherheitsaktualisierungen und Notfalländerungen. IKT-Systeme sind so konfiguriert, dass Schutzmechanismen von Benutzern nicht deaktiviert werden können.

Wesentliche Änderungen, wie z.B. neue Produktversionen, veränderte IKT-Systemarchitekturen, veränderte IKT-Infrastrukturdienste, die sich auf die im Rahmen der Leistungserbringung eingesetzten IKT-Systeme auswirken können, sind hinsichtlich Ihrer Risiken durch den Auftragnehmer vor der Umsetzung zu bewerten.

Der Auftragnehmer hat einen festgelegten und dokumentierten Prozess zur Behandlung von ungeplanten Abweichungen vom Regelbetrieb (Störungen) implementiert.

Der Auftragnehmer verfügt über ein angemessenes Überwachungs-, Kapazitäts- und Performancemanagement für die im Rahmen der Leistungserbringung einzusetzenden IKT-Systeme, um die Verfügbarkeit und Effizienz der Systeme zu gewährleisten.

9 Identitäts- und Rechtemanagement

Der Zugang und Zugriff auf IKT-Systeme sowie Informationen wird durch Richtlinien geregelt, die geschäftliche und sicherheitsrelevante Anforderungen sowie die Prinzipien der minimalen Berechtigungsvergabe („Principle of least privilege“), Kenntnis nur, wenn nötig (Need-to-Know) sowie den Grundsatz der Nutzungsnotwendigkeit (Need-to-Use) berücksichtigen. Eine Funktionstrennung zur Vermeidung der Umgehung von Kontroll- und Schutzmechanismen ist umzusetzen.

Der Auftraggeber verfügt über festgelegte und dokumentierte Vorgaben und Prozesse zum Identitäts- und Berechtigungsmanagement (Neuvergabe, Änderung, Löschung von Benutzerkonten und Berechtigungen).

Die Zugangs- und Zugriffsrechte werden durch verantwortliche Personen genehmigt und regelmäßig überprüft. Zugriffsrechte werden bei Beendigung von Beschäftigungsverhältnissen oder Verträgen unmittelbar entzogen oder angepasst.

Die Benutzeridentitäten, Konten und Berechtigungen werden zentral dokumentiert und verwaltet. Jegliche Veränderungen an den Zugangs- und Zugriffsrechten sind vom Auftragnehmer nachvollziehbar zu dokumentieren.

Privilegierte bzw. administrative Benutzerkonten anderer Kunden erhalten niemals Zugriff auf Daten oder IKT-Systeme des Auftraggebers.

Zugriffe auf die für den Auftraggeber bereitgestellten IKT-Systeme, Netze und der Zugang zu Daten erfolgen ausschließlich nach vorheriger Authentifizierung des Nutzers. Zugriffe mit privilegierten Berechtigungen, z.B. bei administrativen Nutzern, erfolgen mit starker Authentifizierung, wie z.B. einer Multi-Faktor-Authentifizierung.

Der Auftragnehmer stellt sicher, dass für jedes durch den Auftragnehmer verwendete Benutzerkonto mit direktem oder indirektem Zugriff auf Systeme der IFB Hamburg eine natürliche Person identifiziert werden kann. Für nicht personalisierte Benutzerkennungen existieren Regelungen zu Zuständigkeit und Nachvollziehbarkeit des Einsatzes.

Der Auftragnehmer stellt sicher, dass seine Mitarbeiter nur die für die Durchführung ihrer Tätigkeit minimal notwendigen Zugriffsrechte erhalten bzw. dass der Kreis der mit der Leistungserbringung beauftragten Personen auf das Notwendigste reduziert ist.

Der Auftragnehmer hat für alle IKT-Systeme Berechtigungskonzepte definiert, die jährlich und anlassbezogen nachweislich überprüft und aktualisiert werden.

Der Auftragnehmer führt für die durch ihn eingeräumten Berechtigungen eine Überprüfung der Berechtigungen (Rezertifizierung) alle 6 Monate durch.

Die Verwaltung von Kennwörtern ist nach dem Stand der Technik zu regeln. Dabei sind folgende Aspekte durch den Auftragnehmer zu detaillieren bzw. zu berücksichtigen:

- Kennwörter sollten mindestens 15 Zeichen lang sein. Kennwörter, die über weniger als 15 Zeichen verfügen, müssen mindestens 8 Zeichen lang sein und mindestens 1 Zeichen aus jeder der folgenden Kategorien enthalten: Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen.
- Initialkennwörter müssen nach der ersten Anmeldung durch den Nutzer geändert werden.
- Kennwörter dürfen nicht den Benutzernamen des Anwenders beinhalten.
- Es dürfen nicht die letzten 10 Kennwörter wiederverwendet werden.
- Der Prozess zur Kennwortrücksetzung muss beschrieben sein.

Kennwörter (einschließlich technischer Benutzerkonten) dürfen nicht (sofern technisch möglich) im Klartext in IKT-Systemen (z. B. Konfigurationsdateien) gespeichert werden. Zudem müssen sie angemessen geschützt werden. Jede Kennwortänderung bzw. Rücksetzung ist zu protokollieren.

Bei Verdacht auf Offenlegung von Kennwörtern wird das betroffene Kennwort sofort geändert und der Vorfall wird an eine zuständige Stelle gemeldet.

Der Benutzerzugang mit Zugriff auf schutzbedürftigen Daten bzw. ab der Schutzbedarfsklasse „hoch“ über einen aus dem öffentlichen Internet allgemein erreichbaren Zugang muss über eine Multifaktor-Authentifizierung oder eine Absicherung mit ähnlichem Vertrauenslevel abgesichert werden.

Der Zugang unter Verwendung eines Benutzerkontos mit kritischen oder privilegierten Berechtigungen über einen aus dem öffentlichen Internet allgemein erreichbaren Zugang muss über eine Multifaktor-Authentifizierung oder eine Absicherung mit ähnlichem Vertrauenslevel abgesichert werden.

Der Auftragnehmer ermöglicht und unterstützt den Auftraggeber bei der Anbindung an zentrale Authentifizierungsdienste des Instituts.

10 Schutzmaßnahmen

Der Auftragnehmer verfügt auf Grundlage eines festgelegten und dokumentierten Sicherheitskonzepts über angemessene physische Sicherheitskontrollen zum Schutz seiner Räumlichkeiten, Rechenzentren und sensiblen Bereiche (z. B. Technikräume mit Verkabelung, Sicherungsmedien, unterbrechungsfreie Stromversorgung). Zutrittssteuerungen und bauliche Maßnahmen schützen sensible Sicherheitsbereiche, um nur autorisiertem Personal Zugang zu gewähren. Der Auftragnehmer implementiert Überwachungsmaßnahmen, um unbefugten Zutritt zu verhindern.

Der Auftragnehmer hat auf Grundlage eines festgelegten und dokumentierten Sicherheitskonzeptes Vorkehrungen zum Schutz der IKT-Systeme vor Cyberangriffen aus dem Internet getroffen. Hierzu gehören Sicherheitstechnologien wie Firewall, Web-Filter, Virens Scanner, IDS/IPS-Systeme. Der Auftragnehmer betreibt auf allen im Rahmen der Leistungserbringung relevanten IKT-Systemen angemessene Anti-Virus-Software. Sicherheitsaktualisierungen werden regelmäßig vom Auftragnehmer eingespielt.

Der Auftragnehmer verfügt über eine angemessene Netzwerksegmentierung für seine IKT-Systeme und stellt sicher, dass die Regelwerke seiner Firewall-Systeme regelmäßig hinsichtlich der Angemessenheit und Notwendigkeit überprüft werden. Der Auftragnehmer implementiert Kontrollen und Maßnahmen, um Verbindungen von nicht autorisierten Geräten oder Systemen zu erkennen und zu verhindern (NAC, Network Access

Control).

Der Auftragnehmer stellt sicher, dass die zur Erbringung der Dienstleistung notwendigen Daten entsprechend ihrem Schutzbedarf sowohl bei der Übertragung („data in transit“) als auch bei der Speicherung („data in rest“) verschlüsselt sind. Der Auftragnehmer verpflichtet sich, ausschließlich Verschlüsselungstechnologien einzusetzen, die nach aktuellem Stand der Technik als sicher gelten und die den Anforderungen der technischen Richtlinie des BSI „Kryptographische Verfahren“ TR-02102-1 erfüllen. Der Auftragnehmer hat Maßnahmen gegen Datendiebstahl und Datenverlust implementiert.

Sofern sich Daten in Verwendung des IKT-Systems („data in use“) befinden, und eine kryptografische Verschlüsselung nicht möglich ist, muss der Auftragnehmer die Daten in einer abgetrennten und geschützten Umgebung verarbeiten oder anderweitige Maßnahmen ergreifen, um die Schutzziele des Auftraggebers zu gewährleisten.

Der Auftragnehmer betreibt ein Lebenszyklusmanagement für seine kryptografischen Schlüssel und führt Kontrollen zum Schutz vor Verlust, unbefugtem Zugriff, Offenlegung und Veränderung durch. Im Falle eines Verlustes, Kompromittierung oder Beschädigung, kann der Auftragnehmer die kryptografischen Schlüssel durch angemessene Maßnahmen ersetzen.

Der Auftragnehmer hat festgelegte und dokumentierte Vorgaben zur sicheren Konfiguration und Härtung von IKT-Assets und setzt diese nachweislich um. Nur gehärtete IKT-Systeme dürfen mit dem Netzwerk der IFB Hamburg verbunden werden.

Der Auftragnehmer unterstützt bei Cloud-Dienstleistungen den Auftraggeber bei der Erstellung eines Cloud-Sicherheitskonzeptes für die jeweilige cloudbasierte Dienstleistung.

Relevante IKT-Systeme und IKT-Assets des Auftragnehmers sind auf eine vertrauenswürdige, zentrale Zeitquelle synchronisiert.

11 Überwachung und Protokollierung

Der Auftragnehmer hat Prozesse und Tools zur Protokollierung und Überwachung sicherheitsrelevanter Ereignisse, insbesondere Ereignisse im Zusammenhang mit Berechtigungs-, Kapazitäts- und Changemanagement, Netzwerk- und IKT-Systemaktivitäten, Benutzertätigkeiten, Störungen und IKT-bezogene Vorfällen festgelegt, dokumentiert und implementiert. Es ist klar definiert, welche Ereignisse protokolliert werden, wie lange die Protokolldaten aufbewahrt werden und wann sie gelöscht werden. Im Rahmen dieses Prozesses werden sicherheitsrelevante Ereignisse oder IKT-bezogene Vorfälle durch den Auftragnehmer frühzeitig identifiziert, bewertet und behandelt.

Das Protokollierungssystem des Auftragnehmers und die sich darin befindlichen Informationen sind vor Manipulation, Löschung und unbefugtem Zugriff geschützt.

Zur technischen Umsetzung betreibt der Auftraggeber ein angemessenes Security Incident und Event Management (SIEM) – System zur Protokollierung der sicherheitsrelevanten Ereignisse in seinem Verantwortungsbereich.

Die Überwachung der Sicherheitsindikatoren sowie der sicherheitsrelevanten Ereignisse erfolgt 24x7 durch ein Security Operation Center des Auftragnehmers.

Der Auftragnehmer erklärt sich bereit, bei der Anbindung von IKT-Assets, die durch den Auftraggeber bereitgestellt, aber durch den Auftraggeber verwaltet werden, auf Wunsch an ein SIEM –System des Auftraggebers mitzuwirken.

Im Zuge der Überwachung und der Protokollierung sicherheitsrelevanter Ereignisse

sind mindestens folgende Komponenten, die im Zusammenhang mit der Dienstleistungserbringung stehen bzw. Einfluss darauf haben können, zu überwachen:

- Komponenten, die das Netzwerk steuern und verwalten (inkl. Cloud, Netzwerkdienste),
- alle das Netzwerk (zentral) unterstützenden IKT-Infrastrukturen und
- alle Infrastrukturkomponenten, Server, Anwendungen, Dienste, Datenbanken und Clients.

12 Datensicherung und Wiederherstellung

Der Auftragnehmer hat ein Datensicherungskonzept festgelegt und dokumentiert, die entsprechenden Verfahren zur Datensicherung gemäß den vertraglich definierten Verfügbarkeitsanforderungen nachweislich implementiert und prüft die Verfahren zur Wiederherstellbarkeit mindestens jährlich sowie anlassbezogen.

Datensicherungen, die Informationen mit einer sehr hohen Vertraulichkeit beinhalten, sind mittels kryptografischer Maßnahmen zu verschlüsseln oder durch geeignete technische und/oder organisatorische Maßnahmen abzusichern.

Die Datensicherungen des Auftragnehmers sind angemessen gegen Manipulationen oder unbefugtem Zugriff zu schützen.

13 Business Continuity Management / Notfallmanagement

Der Auftragnehmer verfügt unter Berücksichtigung der definierten Verfügbarkeitsanforderungen über angemessene IKT-Geschäftsfortführungspläne sowie IKT-Reaktions- und Wiederherstellungspläne nach Maßgabe der zu erbringenden Leistungen, die regelmäßig überprüft und aktualisiert werden.

Der Auftragnehmer verfügt über ein Business Continuity Management, angelehnt an den BSI-Standard 200-4 oder ISO/IEC 22301:2019, dass insbesondere die beauftragten IKT-Dienstleistungen vollständig und wirksam umfasst. Die auf Grundlage schriftlich fixierter Richtlinien getroffenen Vorsorgemaßnahmen werden in einem Notfallvorsorgekonzept dargestellt und umfassen u. a. definierte Notfallszenarien, IKT-Geschäftsfortführungs-, Kommunikations- sowie IKT-Reaktions- und Wiederherstellungspläne für die kritischen Prozesse und IKT-Assets, die zur Leistungserbringung eingesetzt werden.

Die IKT-Reaktions- und Wiederherstellungspläne des Auftragnehmers müssen folgende Szenarien angemessen berücksichtigen:

- Cyberangriffe und Umstellungen von der primären IKT-Infrastruktur auf die redundanten Kapazitäten, Backups und redundanten Systeme;
- Szenarien, in denen die Qualität der Bereitstellung der IKT-Dienstleistung auf ein inakzeptables Niveau absinkt oder diese Funktion ganz ausfällt und in denen die potenziellen Auswirkungen der Insolvenz oder sonstiger Ausfälle eines relevanten IKT-Drittdienstleisters gebührend berücksichtigt werden;
- teilweiser oder vollständiger Ausfall von Räumlichkeiten, insbesondere auch von Büro- und Geschäftsräumen, sowie von Rechenzentren;
- erheblicher Ausfall von IKT-Assets oder der Kommunikationsinfrastruktur;
- Nichtverfügbarkeit einer kritischen Anzahl von Mitarbeitern oder von Mitarbeitern, die für die Gewährleistung der Betriebskontinuität zuständig sind;
- Auswirkungen von Ereignissen im Zusammenhang mit Klimawandel und Umweltzerstörung, Naturkatastrophen, Pandemien und physischen Angriffen, insbesondere auch durch Eindringen und Terroranschläge;

- Angriffe durch Insider;
- politische und soziale Instabilität, sofern relevant im Land des Auftragnehmers und am Standort der Datenspeicherung und -verarbeitung;
- weitverbreitete Stromausfälle.

Der Auftragnehmer unterhält für IKT-Dienstleistungen, die kritische oder wichtige Funktionen des Auftraggebers unterstützen, einen sekundären Verarbeitungsstandort, der die Fortführung der IKT-Dienstleistung in gleicher Weise wie am Primärstandort gewährleisten kann.

Sind die primären Wiederherstellungsmaßnahmen möglicherweise wegen Kosten, Risiken, Logistik oder unvorhergesehener Umstände kurzfristig nicht durchführbar, so werden in den IKT-Reaktions- und Wiederherstellungsplänen des Auftragnehmers auch Alternativen erwogen.

Die IKT-Geschäftsfortführungs-, IKT-Reaktions- und Wiederherstellungspläne gewährleisten, dass im Notfall, d. h. z.B. nach einem Ereignis höherer Gewalt oder einem sonstigen zu einer (schwerwiegenden) Betriebsunterbrechung führenden Ereignis, zeitnah Ersatzlösungen zur Verfügung stehen und eine Rückkehr zum Normalbetrieb innerhalb der festgelegten Zeiträume vorgenommen werden kann.

Die Wirksamkeit der festgelegten IKT-Geschäftsfortführungs-, IKT-Reaktions- und Wiederherstellungspläne ist durch den Auftragnehmer durch geplante Notfalltests und –Übungen regelmäßig zu prüfen und gegenüber dem Auftraggeber nachzuweisen. Die Einhaltung der Wiederanlaufparameter (z.B. Recovery Time Objective, Recovery Point Objective) sind durch innerhalb der Notfallkonzeption zu etablierender Notfallvorsorge- und Notfallbewältigungsprozesse sicherzustellen.

Der Auftragnehmer führt in Abstimmung mit dem Auftraggeber unter Gewährleistung der Betriebssicherheit mindestens jährlich Notfallübungen durch und dokumentiert die Ergebnisse. Die Ergebnisberichte der Notfallübungen werden dem Auftraggeber nach Fertigstellung zur Verfügung gestellt.

Der Auftragnehmer ist für die laufende Überprüfung und Anpassung (mindestens jährlich) der IKT-Geschäftsfortführungs-, Kommunikations- sowie Reaktions- und Wiederherstellungspläne in Abstimmung mit dem Auftraggeber verantwortlich.

Die durch den Auftragnehmer im Rahmen der Leistungserbringung erstellten Kommunikationspläne für den Notfall sind mit dem Auftraggeber abzustimmen.

14 Management von Schwachstellen

Der Auftragnehmer verwendet keine End-of-Life Systeme.

Der Auftragnehmer verfügt über einen festgelegten und dokumentierten Prozess zum Schwachstellenmanagement zur Erkennung, Bewertung, Behandlung und Dokumentation von Schwachstellen und Cyberbedrohungen. Hierzu verfügt der Auftragnehmer über ein angemessenes Patchmanagement, das die Identifikation und Bewertung notwendiger Sicherheitsupdates und die Planung, Testung und Implementierung der Installationen umfasst. Die Implementierung wird durch den Auftragnehmer überwacht und verifiziert.

Der Auftragnehmer führt automatisierte Schwachstellen-Scans von IKT-Assets, die im Rahmen der Leistungserbringung verwendet werden, mindestens einmal wöchentlich durch.

Der Auftragnehmer verpflichtet sich, verfügbare Patches, Updates und Maßnahmen zur Behebung von Sicherheitsschwachstellen auf den IKT-Systemen, die zur Erbrin-

gung der Dienstleistung eingesetzt werden, im Rahmen der mit dem Auftraggeber abgestimmten Regelungen zum Änderungsmanagement unter Berücksichtigung der Kritikalität auf Grundlage des Common Vulnerability Scoring Systems (CVSS, mindestens Version 3.0) regelmäßig einzuspielen bzw. durchzuführen. Dabei sind folgende Zeiten mindestens einzuhalten :

Kritikalität der Schwachstelle	Reaktionszeit zur Initiierung von Maßnahmen
Niedrig (CVSS Score 0,1 – 3,9)	innerhalb von 90 Werktagen
Mittel (CVSS Score 4,0 – 6,9)	innerhalb von 30 Werktagen
Hoch (CVSS Score 7,0 – 8,9)	innerhalb von 7 Werktagen
Sehr hoch / Kritisch (CVSS Score >9,0)	Unverzüglich

Der Auftragnehmer ist hinsichtlich ihn betreffende Schwachstellen und dem Status der Maßnahmenumsetzung gegenüber dem Auftraggeber auskunftsverpflichtet.

Sobald dem Auftragnehmer Informationen über kritische Schwachstellen, die direkt oder indirekt für die im Rahmen der Leistungserbringung eingesetzten IKT-Systeme relevant sind, vorliegen und diese Schwachstellen nicht innerhalb von 7 Werktagen durch Maßnahmen seitens des Auftragnehmers geschlossen oder mitigiert werden können, ist der Auftragnehmer verpflichtet, den Auftraggeber darüber in Kenntnis zu setzen und die zur Behebung der Schwachstelle notwendigen Maßnahmen, einschließlich Einspielen relevanter Patches oder Updates, in Abstimmung mit dem Auftraggeber unverzüglich unter Berücksichtigung der definierten Änderungskontrollprozesse durchzuführen.

15 Überprüfung der Sicherheit

Der Auftragnehmer verpflichtet sich, mindestens jährlich angemessene Sicherheitstests (z.B. technische Schwachstellen-Scans, Systemaudits, Health Checks) auf eigene Kosten durchzuführen oder Dritte mit der Durchführung zu beauftragen.

Der Auftragnehmer muss, sofern die Leistungserbringung internetbasierte Technologien oder Dienste verwendet, mindestens jährlich einen Penetrationstest auf eigene Kosten durchführen oder Dritte mit der Durchführung beauftragen, um die Sicherheit der für die Leistungserbringung eingesetzten IKT-Infrastruktur sowie der IKT-Anwendungen des Auftragnehmers nachzuweisen.

Der Auftragnehmer stellt dem Auftraggeber die bewerteten Ergebnisse der Audits unentgeltlich zur Verfügung.

Zusätzlich hat der Auftraggeber das Recht, auf eigene Kosten Schwachstellenanalysen oder Penetrationstests selbst durchzuführen oder einen Dritten mit der Durchführung zu beauftragen. Eine solche Analyse wird mit einem Vorlauf von mindestens 4 Wochen an den Auftragnehmer kommuniziert.

Sofern der begründete Verdacht auf gravierende Sicherheitsschwachstellen besteht, ist der Auftraggeber zur Durchführung von ad-hoc-Prüfungen berechtigt. Eine gravierende Sicherheitsschwachstelle liegt vor, wenn eine kritische Schwachstelle leicht und von

außen ausnutzbar ist und die verletzbaren IKT-Systeme im Rahmen der Leistungserbringung eingesetzt werden.

Die im Rahmen von Penetrationstests ermittelten Befunde werden vom Auftragnehmer innerhalb von 4 Wochen bewertet, priorisiert und ggf. mit Maßnahmen versehen. Der Status der Maßnahmenumsetzung wird dem Auftraggeber, unter Berücksichtigung der Kritikalität der Befunde, regelmäßig mitgeteilt.

Sofern der Auftraggeber seitens der BaFin verpflichtet wird, bedrohungsorientierte Penetrationstest gemäß DORA Artikel 26 (Threat-Led-Penetrationstests, TLPT) durchzuführen, beteiligt sich der Auftragnehmer angemessen.

16 Management von IKT-bezogenen Vorfällen

Ein IKT-bezogener Vorfall (Information security incident) ist ein ungewolltes oder unerwartetes informationssicherheitsrelevantes Ereignis (oder eine Reihe entsprechender Ereignisse), das die Vertraulichkeit, Verfügbarkeit, Integrität oder Authentizität der Daten oder IKT-Systeme des Auftragnehmers in der Art beeinträchtigt, so dass ein Schaden für den Auftraggeber oder dessen Kunden entstehen kann oder entstanden ist.

Der Auftraggeber ist gesetzlich verpflichtet, schwerwiegende IKT-bezogene Vorfälle an die Bundesanstalt für Finanzdienstleistungen (BaFin) zu melden. Der Auftragnehmer verpflichtet sich, die für die Meldung notwendigen Informationen unverzüglich bereitzustellen, damit der Auftraggeber die Meldung vornehmen kann.

Der Auftragnehmer verfügt über einen festgelegten und dokumentierten Prozess zur Behandlung von Informationssicherheitsvorfällen.

Der Auftragnehmer ist verpflichtet, den Auftraggeber über wesentliche IKT-bezogene Vorfälle, die potentiell Einfluss auf die Leistungserbringung oder die Sicherheit der Daten oder IKT-Systeme des Auftragnehmers haben können, innerhalb von 4 Stunden nach initialer Beurteilung und Klassifizierung zu informieren. Beispiele für wesentliche IKT-bezogene Vorfälle sind:

- Ausfälle oder Teilausfälle von wesentlichen Prozessen oder IKT-Systemen.
- Vorfälle, die zu einer Verletzung der Vertraulichkeit gemäß Art. 33 und 34 DSGVO geführt haben.
- Vorfälle, die zu signifikanten Reputationsschäden für Auftraggeber oder Auftragnehmer führen können.
- Vorfälle, die vom Auftragnehmer als Notfall gewertet werden und bei denen definierte Notfallmaßnahmen zum Einsatz kommen.
- Verdacht auf einen Cyberangriff.
- Verdacht auf Straftaten.

Wenn die Beurteilung oder Klassifizierung eines potentiellen IKT-bezogenen Vorfalls nicht innerhalb von 8 Stunden abgeschlossen werden konnte, ist der Auftraggeber ebenfalls zu informieren.

Eine Vorfallsmeldung beinhaltet:

- Datum und Uhrzeit der Entdeckung
- Beschreibung des Vorfalls inkl. betroffene IKT-Assets und Prozesse,
- Vorhandene oder zu erwartende negative Auswirkungen auf die Leistungserbringung,

- Betroffene Maßnahmen des Auftragnehmers,
- Empfohlene Maßnahmen für den Auftraggeber,
- Voraussichtlicher Wiederherstellungszeitpunkt und
- Zeitpunkt der nächsten Meldung.

Der Auftragnehmer informiert den Auftraggeber fortlaufend über neue Erkenntnisse hinsichtlich des IKT-bezogenen Vorfalls und aktualisiert die Vorfallsmeldung. Dies umfasst auch korrigierende bzw. risikominimierende Maßnahmen und deren Umsetzungsfortschritt.

Die Meldung IKT-bezogener Vorfälle hat, ergänzend zu sonstigen Vereinbarungen, an die Adresse it-vorfall@ifbhh.de zu erfolgen.

Der Auftragnehmer ist verantwortlich für die Analyse eines vermuteten IKT-bezogenen Vorfalls und die Koordination der Behandlung (Security Incident Handling) des Vorfalls, sofern dieser im Kontrollbereich des Auftragnehmers liegt.

Der Auftragnehmer dokumentiert alle IKT-bezogenen Vorfälle und stellt dem Auftraggeber die Dokumentation im Bedarfsfall unentgeltlich zur Verfügung.

Darüber hinaus sind bei IKT-bezogenen Vorfällen alle für forensische Untersuchungen angeforderten Informationen unverzüglich durch den Auftragnehmer bereitzustellen. Dabei ist eine durchgehende Beweiskette zu gewährleisten. Daher verpflichtet sich der Auftragnehmer über geeignete Prozesse zur IKT-Forensik zu verfügen und diese auch regelmäßig testen. Darüberhinausgehende Unterstützungsleistungen sind fallweise gesondert zu verhandeln. Bei Bedarf ist dem Auftraggeber oder durch ihn beauftragte Personen der Zugang zu den betreffenden Systemen zu ermöglichen.

Der Auftragnehmer verpflichtet sich, einen Abschlussbericht nach der vollständigen Behebung des Vorfalls zur Verfügung zu stellen.

17 Eingeschränkte oder Nicht-Umsetzbarkeit der Anforderungen

Sofern der Auftragnehmer die hier festgelegten Anforderungen nicht oder nur eingeschränkt umsetzen kann, ist dies dem Auftraggeber gegenüber mitzuteilen. Dies beinhaltet die Offenlegung der Gründe, weshalb die Umsetzung nicht oder nur eingeschränkt erfolgen kann. Außerdem muss der Auftragnehmer darlegen, welche kompensierenden Maßnahmen für die Risikobegrenzung getroffen werden sollen, um das Sicherheitsniveau des Auftraggebers zu erfüllen.

Der Auftraggeber prüft die daraus resultierende Risikosituation und teilt dem Auftragnehmer das Ergebnis und die daraus zu ziehenden Schlussfolgerungen mit.

18 Regelmäßige Berichte

Der Auftragnehmer ist verpflichtet, dem Auftraggeber unentgeltlich

- jährlich einen IKT-Risikobericht (siehe 4),
- jährlich einen Bericht zur Informationssicherheit,
- mindestens alle 2 Jahre einen Nachweis über ein wirksames Informationssicherheits-Managementsystem (ISMS), ausgerichtet an definierte Standards (siehe 1) und
- mindestens einmal pro Kalenderjahr eine Auditierung gemäß der Standards ISAE 3402 Typ 2 oder IDW PS 951 Typ B (siehe 1.6)

zur Verfügung zu stellen.

19 Prüf- und Kontrollrechte

Zur Gewährleistung der Informations- und Prüfungsrechte

- gewährt der Auftragnehmer dem Auftraggeber oder Dritten, die durch den Auftraggeber beauftragt wurden, auf vorherige Anfrage des Auftraggebers unentgeltlich uneingeschränkten Zugriff auf Informationen und Daten sowie Zugang zu den Geschäftsräumen des Auftragnehmers, einschließlich aller Rechenzentren, Geräte, IKT-Systeme, Netzwerke, die zur Leistungserbringung eingesetzt werden und
- verpflichtet sich der Auftragnehmer zur uneingeschränkten Zusammenarbeit bei Vor-Ort-Inspektionen und Audits, die von den zuständigen Aufsichtsbehörden, dem Auftraggeber oder einem von dem Auftraggeber beauftragten Dritten durchgeführt werden.