Bundesamt
für Sicherheit in der
Informationstechnik

Mindeststandard des BSI zur Anwendung des HV-Benchmark kompakt 4.0

nach § 8 Absatz 1 Satz 1 BSIG – Version 1.1 vom 19.06.2018

Inhaltsverzeichnis

Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die nationale Cyber-Sicherheitsbehörde erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes auf der Grundlage des § 8 Abs. 1 BSIG. Als gesetzliche Vorgabe definieren Mindeststandards ein konkretes Mindestniveau für die Informationssicherheit. Die Definition erfolgt auf Basis der fachlichen Expertise des BSI in der Überzeugung, dass dieses Mindestniveau in der Bundesverwaltung nicht unterschritten werden darf. Der Mindeststandard richtet sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe)[1] und IT-Betriebspersonal.

IT-Systeme sind in der Regel komplex und in ihren individuellen Anwendungsbereichen durch die unterschiedlichsten (zusätzlichen) Rahmenbedingungen und Anforderungen gekennzeichnet. Daher können sich in der Praxis regelmäßig höhere Anforderungen an die Informationssicherheit ergeben, als sie in den Mindeststandards beschrieben werden. Aufbauend auf den Mindeststandards sind diese individuellen Anforderungen in der Planung, der Etablierung und im Betrieb der IT-Systeme zusätzlich zu berücksichtigen, um dem jeweiligen Bedarf an Informationssicherheit zu genügen. Die Vorgehensweise dazu beschreiben die IT-Grundschutz-Standards des BSI.

Zur Sicherstellung der Effektivität und Effizienz in der Erstellung und Betreuung von Mindeststandards arbeitet das BSI nach einer standardisierten Vorgehensweise. Zur Qualitätssicherung durchläuft jeder Mindeststandard mehrere Prüfzyklen einschließlich des Konsultationsverfahrens mit der Bundesverwaltung.[2] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Stelle des Bundes auch bei der Erschließung fachlicher Themenfelder für neue Mindeststandards einbringen oder im Hinblick auf Änderungsbedarf für bestehende Mindeststandards Kontakt mit dem BSI aufnehmen. Einhergehend mit der Erarbeitung von Mindeststandards berät das BSI die Stellen des Bundes[3] auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Analog „Informationssicherheitsbeauftragte (ISB)“
[2] Zur standardisierten Vorgehensweise siehe https://www.bsi.bund.de/mindeststandards
[3] Zur besseren Lesbarkeit wird im weiteren Verlauf für „Stelle des Bundes“ der Begriff „Behörde“ verwendet.

1 Beschreibung

Der vorliegende Mindeststandard hat zum Ziel, Mindestwerte für die im HV-Benchmark kompakt 4.0 betrachteten Aspekte der Informationssicherheit festzulegen, die bei der Anwendung des HV-Benchmark kompakt von den Rechenzentren der Stellen des Bundes mindestens erreicht werden müssen.

Er dient auch der Umsetzung des Beschlusses des Haushaltsausschusses (HHA) vom 28.09.2016[4]. In Teil IV.2 des Beschlusses fordert der HHA „die Bundesregierung auf, [...] IV. hinsichtlich [...] der IT-Sicherheit, [...] 2. das vom BSI entwickelte und pilotierte ‚Bewertungsschema zur Bestimmung der Verlässlichkeit von IT-Dienstleistungen unter besonderer Berücksichtigung von Aspekten der Hochverfügbarkeit' (‚HV-Benchmark') schrittweise auf alle Rechenzentren in der Bundesverwaltung anzuwenden. Das Verfahren soll weiter optimiert und mit der bereits etablierten Methode der IT-Sicherheitsrevision kombiniert werden".

Weiterhin fordert der HHA in Teil IV.3 des o. g. Beschlusses die Bundesregierung auf, „basierend auf dem HV-Benchmark einen Mindeststandard für die Sicherheit von Rechenzentren des Bundes festzulegen, der unabhängig vom konkreten Schutzbedarf in jedem Rechenzentrum der Bundesverwaltung erfüllt sein muss. Wird im Rahmen des Benchmarks eine Unterschreitung dieses Niveaus festgestellt, ist der Leiter der betroffenen Behörde für die Einleitung von Gegenmaßnahmen verantwortlich."

Der HV-Benchmark (HVB)[5] hat zum Ziel, die Verlässlichkeit einer zu betrachtenden IT-Dienstleistung oder eines Rechenzentrums (RZ) zu messen und zu bewerten. Dies erfolgt mit Hilfe von etwa 100 besonders relevanten Aspekten der Verlässlichkeit (sogenannte „Indikatoren") unter der Nutzung von Reifegradmodellen. Der Begriff „Verlässlichkeit" beschreibt die Erwartung, dass eine IT-Dienstleistung im Vorfeld nachweisbar und nachvollziehbar die angeforderten Funktionen erfüllt. Verlässlichkeit ist ein Maß für die Qualität von IT-Dienstleistungen und wird im Wesentlichen durch folgende sieben Kriterien bestimmt: Verfügbarkeit, Integrität, Vertraulichkeit, Betriebssicherheit, Wartbarkeit, Transparenz und Leistungsfähigkeit. Die drei Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) sind im Begriff „Verlässlichkeit" enthalten, d. h. Verlässlichkeit umfasst die Informationssicherheit, geht aber darüber hinaus.

Zu den Zielgruppen, die mit dem HVB angesprochen werden sollen, gehören vor allem RZ-Betreiber, die z. B. eine Selbsteinschätzung vornehmen möchten, und IT-Nutzer, die einen geeigneten RZ-Betreiber suchen. Der HV-Benchmark kompakt (HVB-kompakt) ist eine komprimierte Version des HV-Benchmark, die gegenüber der Vollversion des HV-Benchmark eine leicht modifizierte Methodik verwendet und um Revisionselemente ergänzt worden ist. Der HHA hat seinen Auftrag explizit „hinsichtlich [...] der IT-Sicherheit" erteilt. Mit Hilfe aller Indikatoren der Vollversion des HVB wird aber nicht nur die IT-Sicherheit „im engeren Sinne", sondern die darüber hinaus gehende „Verlässlichkeit" betrachtet. Um die Analyse der RZ auf die IT-Sicherheit „im engeren Sinne" zu fokussieren, wurde der Umfang des HVB durch den HVB-kompakt reduziert, indem solche Indikatoren ausgewählt worden sind, die den „Kern" der IT-Sicherheit repräsentieren.

Grundlage des vorliegenden Mindeststandards ist der HVB-kompakt 4.0. Er ist als Anlage 1 fester Bestandteil des Mindeststandards. Weitere Details, insbesondere die Methodik des HVB-kompakt, können der Anlage 1 entnommen werden. Der Mindeststandard legt für die 34 Indikatoren des HVB-kompakt 4.0 die aus Sicht des BSI erforderlichen Mindestwerte für die Reifegrade und Potenzialstufen fest, die bei der Anwendung des HVB-kompakt auf ein Rechenzentrum einer Stelle des Bundes – unabhängig von dessen tatsächlichem Schutzbedarf – erreicht werden müssen.

Die Einhaltung der im Mindeststandard vorgegebenen Mindestwerte ist für ein angemessenes IT-Sicherheitsniveau von Rechenzentren notwendig, aber in der Regel nicht hinreichend. Die Sollwerte für die 34 Indikatoren sind für jedes Rechenzentrum – unter Berücksichtigung des individuellen Schutzbedarfs –

[4] Beschluss des HHA zu TOP 14 a), b) und c) in seiner 82. Sitzung am 28.09.2016, Ausschussdrucksache Nr. 18(8)3472.

[5] HV-Benchmark: Bewertungsschema zur Bestimmung der Verlässlichkeit von IT-Dienstleistungen unter besonderer Berücksichtigung von Aspekten der Hochverfügbarkeit (HV), BSI.

im Einzelfall festzulegen. Die Sollwerte werden in der Regel höher, aber niemals niedriger sein, als die Mindestwerte. Um ein hinreichendes IT-Sicherheitsniveau zu erlangen, muss darüber hinaus auf der Basis anerkannter Standards eine dem tatsächlichen Schutzbedarf genügende Festlegung und Umsetzung der erforderlichen Sicherheitsmaßnahmen erfolgen. Dass die bloße Einhaltung dieses Mindeststandards noch kein angemessenes Sicherheitsniveau gewährleistet, hat folgenden Grund: Der HVB-kompakt umfasst nur einen Teil der relevanten Aspekte der RZ-Sicherheit, aber keinesfalls alle. Vollständigkeit ist nur durch Anwendung anerkannter Standards (z. B. IT-Grundschutz, DIN EN 50 600) zu erreichen. Daher kann der HVB-kompakt solche Standards keinesfalls ersetzen.

1.1 Zielgruppe des Mindeststandards

Dieser Mindeststandard richtet sich an IT-Verantwortliche und Informationssicherheitsbeauftragte[6] sowie IT-Fachkräfte von Behörden.

1.2 Konkretisierungen

Im Folgenden werden zur genauen Bestimmung und Anwendung dieses Mindeststandards notwendige Begriffe bestimmt.

1.2.1 Rechenzentrum

Der IT-Leiter legt in Absprache mit dem zuständigen Informationssicherheitsbeauftragten fest, welche IT-Betriebsbereiche räumlich das Rechenzentrum umfassen. Diese Festlegung ist zu dokumentieren und von der Hausleitung mitzutragen.

Zur Festlegung dienen folgende Rahmenregelungen:

1. Verfügt die Behörde nur über einen IT-Betriebsbereich[7], ist dieser gemeinsam mit den zugehörigen Supportbereichen als Rechenzentrum einzustufen.

2. IT-Betriebsbereiche, aus denen heraus IT-Dienstleistungen für Dritte erbracht werden, sind immer als Rechenzentrum einzustufen.

3. Verfügt die Behörde über mehrere, räumlich voneinander getrennte IT-Betriebsbereiche, die nicht über hauseigene LAN-Verbindungen miteinander gekoppelt sind, ist jeder dieser IT-Betriebsbereiche als separates Rechenzentrum einzustufen.

4. Werden IT-Betriebsbereiche innerhalb eines Standortes verteilt in mehreren Bereichen betrieben, ist mindestens einer dieser IT-Betriebsbereiche als Rechenzentrum einzustufen. Grundsätzlich sollte dies der Bereich mit der größten Konzentration von IT-Dienstleistungen sein.

5. IT-Betriebsbereiche, die kritische Geschäftsprozesse unterstützen, sind immer als Rechenzentrum einzustufen.

6. IT-Betriebsbereiche, von deren ordnungsgemäßem Betrieb der überwiegende Teil der Belegschaft abhängig ist, sind als Rechenzentrum einzustufen.

7. IT-Betriebsbereiche, die einen überwiegenden Teil an IT-Dienstleistungen bereitstellen, sind als Rechenzentrum einzustufen.

[6] Analog „IT-Sicherheitsbeauftragte“

[7] Räume, in denen Hardware aufgebaut ist und betrieben wird, die der Bereitstellung von Diensten und Daten dient. Das Rechenzentrum umfasst den IT-Betriebsbereich sowie alle weiteren technischen Supportbereiche (Stromversorgung, Kälteversorgung, Löschtechnik, Sicherheitstechnik etc.), die dem Betrieb und der Sicherheit des IT-Betriebsbereichs dienen.

1.2.2 Domänen und Indikatoren

Der HVB-kompakt nutzt sogenannte Indikatoren zur Bewertung der Informationssicherheit von Rechenzentren. Ein Indikator steht für einen Aspekt, der für die Informationssicherheit besonders relevant ist. Im HVB-kompakt werden insgesamt 34 Indikatoren aus den drei Domänen „Management", „IT-Steuerung" und „technische Umsetzung" betrachtet (siehe Tabelle 1).

Domäne	*Indikator (HVB-kompakt)*
Management	ISMS (B.b.1)
	Risikomanagement im Zusammenhang mit der Dienstleistungserbringung (B.b.2)
	Notfall- und Krisenmanagement (B.b.3)
	Einhaltung rechtlicher und organisatorischer Vorgaben durch das Personal (B.b.4)
	Infrastruktur, Grundlagen und Planung (B.b.5)
IT-Steuerung	Availability Management (B.b.6)
	Capacity Management (B.b.7)
	IT-Service Continuity Management: IT-Notfallplanung (B.b.8)
	IT-Service Continuity Management: Datensicherungen (B.b.9)
	IT-Sicherheitskonzepte: Mandantentrennung (B.b.10)
	IT-Sicherheitskonzepte: ID- und Rechtemanagement (B.b.11)
	IT-Sicherheitskonzepte: Kryptografie (B.b.12)
	IT-Sicherheitskonzepte: Sichere Datenlöschung und Aussonderung (B.b.13)
	IT-Sicherheitskonzepte: Schutz gegen Schadprogramme und netzbasierte Angriffe (B.b.14)
	Incident Management: Sicherheitsvorfallbehandlung (B.b.15)
	Patch- und Releasemanagement (Software) (B.b.16)
	Trennung von Entwicklungs-, Test- und Produktionsumgebungen (B.b.17)
Technische Umsetzung	Ausfallsicherheit / Redundanzkonzept (B.b.18)
	Netzwerk-Segmentierung (B.b.19)
	Sicherheit der aktiven Netzwerkkomponenten (B.b.20)
	Ausgestaltung der WAN-Anbindung zwischen den IT-Standorten (B.b.21)
	Sicherheit der Internet-Anbindung (B.b.22)
	Server-Sicherheit (B.b.23)
	Datensicherheit der Speicher (B.b.24)
	Datenreplikation und -sicherung (B.b.25)
	Energieversorgung: Unterbrechungsfreie Stromversorgung (B.b.26)
	Energieversorgung: Einsatz einer Netzersatzanlage (NEA) (B.b.27)
	Technischer Brandschutz des Rechenzentrums (B.b.28)
	Gebäudesicherheit. Schutz gegen Einbruch und Sabotage (B.b.29)
	Gebäudesicherheit: Technische / bauliche Maßnahmen zum Zutrittsschutz (B.b.30)
	Sicherheit der Verzeichnisdienste (B.b.31)
	Monitoring der technischen Infrastruktur (B.b.32)
	Monitoring auf IT-Sicherheitsvorfälle, Logging (B.b.33)
	Monitoring der IT-Komponenten und –Dienste auf Verfügbarkeit (B.b.34)

Tabelle 1: Domänen und Indikatoren des HVB kompakt

Die Indikatoren und die zugehören Reifegrade oder Potenzialstufen werden ausführlich im HVB-kompakt 4.0 (siehe Anlage 1) beschrieben.

Indikatoren der Domäne „Technische Umsetzung“	*Mindest-Potenzialstufe*
Ausfallsicherheit / Redundanzkonzept (B.b.18)	1
Netzwerk-Segmentierung (B.b.19)	2
Sicherheit der aktiven Netzwerkkomponenten (B.b.20)	1
Ausgestaltung der WAN-Anbindung zwischen den IT-Standorten (B.b.21)	1[9]
Sicherheit der Internet-Anbindung (B.b.22)	1
Server-Sicherheit (B.b.23)	1
Datensicherheit der Speicher (B.b.24)	1
Datenreplikation und -sicherung (B.b.25)	1
Energieversorgung: Unterbrechungsfreie Stromversorgung (B.b.26)	2[10]
Energieversorgung: Einsatz einer Netzersatzanlage (NEA) (B.b.27)	1[11]
Technischer Brandschutz des Rechenzentrums (B.b.28)	1
Gebäudesicherheit: Schutz gegen Einbruch und Sabotage (B.b.29)	1
Gebäudesicherheit: Technische / bauliche Maßnahmen zum Zutrittsschutz (B.b.30)	1
Sicherheit der Verzeichnisdienste (B.b.31)	2
Monitoring der technischen Infrastruktur (B.b.32)	1
Monitoring auf IT-Sicherheitsvorfälle, Logging (B.b.33)	1
Monitoring der IT-Komponenten und –Dienste auf Verfügbarkeit (B.b.34)	1

Tabelle 4: Mindest-Potenzialstufen für Indikatoren der Domäne „Technische Umsetzung“

[9]Der Mindestwert 1 für den Indikator „Ausgestaltung der WAN-Anbindung zwischen den IT-Standorten (B.b.21)“ muss nur erreicht werden, falls WAN-Verbindungen zur Kopplung von Rechenzentren erforderlich sind.

[10]Im Sinne der Stufe 1 des Indikators „Energieversorgung: Unterbrechungsfreie Stromversorgung (B.b.26)“ sind kritische Komponenten solche, die bei einem ungepufferten Stromausfall einen Schaden (inkl. Datenverlust) erleiden können.

[11]Für Rechenzentren, die nachweislich geringe Anforderungen an die Verfügbarkeit haben, muss der Mindestwert 1 des Indikators „Energieversorgung: Einsatz einer Netzersatzanlage (NEA) (B.b.27)“ nicht erreicht werden.

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
HHA	Haushaltsausschuss des Deutschen Bundestages
HV	Hochverfügbarkeit
HVB	HV-Benchmark
ISMS	Informations-Sicherheits-Management-System
NEA	Netzersatzanlage
RZ	Rechenzentrum
TOP	Tagesordnungspunkt
WAN	Wide Area Network (Weitverkehrsnetz)

Anlagen

1. Bundesamt für Sicherheit in der Informationstechnik, Sicherheitsanalyse aller Rechenzentren der Bundesverwaltung mittels HV-Benchmark kompakt, Umsetzung von Teil IV.2 des HHA-Beschlusses vom 28.09.2016, Version 4.0, Stand Februar 2018

Bundesamt
für Sicherheit in der
Informationstechnik

Sicherheitsanalyse aller Rechenzentren der Bundesverwaltung mittels HV-Benchmark kompakt

Umsetzung von Teil IV.2 des HHA-Beschlusses vom 28.09.2016

Stand: Februar 2018 - Version 4.0

Inhaltsverzeichnis

A. Einführung

Der „HV-Benchmark kompakt“ (HVB-kompakt) dient der Sicherheitsanalyse aller Rechenzentren der Bundesverwaltung zur Umsetzung des folgenden Auftrags des Haushaltsausschusses (HHA).

Auftrag des Haushaltsausschusses

In Teil III.2 des Haushaltsausschuss-Beschlusses vom 17.06.2015[1] fordert der HHA des Deutschen Bundestages „die Bundesregierung auf, [...] III. hinsichtlich [...] der IT-Sicherheit, [...] 2. das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte Schema (Benchmark), mit dessen Hilfe die Verlässlichkeit von IT-Dienstleistungen und Rechenzentren bewertet werden kann, an den Rechenzentren der vier Dienstleistungszentren ZIVIT, BIT, DLZ-IT (BMVI) und BWI/BMVg zu pilotieren und dem Haushaltsausschuss bis zum 31. Mai 2016 über die Ergebnisse zu berichten. Gemeinsam mit der Bundesagentur für Arbeit (BA) und der Deutschen Rentenversicherung Bund (DRV Bund) ist zu prüfen, ob deren Rechenzentren in das Benchmarking einbezogen werden können“.

Darüber hinaus fordert der HHA in Teil III.3 des o. g. Beschlusses „die Bundesregierung auf, [...] III. hinsichtlich [...] der IT-Sicherheit, [...] 3. im Fall einer erfolgreichen Pilotierung, das in Punkt III.2. genannte Schema schrittweise auf alle Rechenzentren in der Bundesverwaltung anzuwenden und ab 2017, im Rahmen des jährlichen Fortschrittberichts zur IT-Konsolidierung, dem Haushaltsausschuss über den Stand der IT-Sicherheit in den Rechenzentren und Netzen des Bundes zu berichten“.

Auf der Basis dieser Aufträge hat das BSI im Rahmen von drei Teilprüfungen bislang 68 Rechenzentren bei 36 Institutionen der Bundesverwaltung untersucht.

Weiterhin fordert der HHA in Teil IV.2 seines Beschlusses vom 28.09.2016[2] *„die Bundesregierung auf, [...] IV. hinsichtlich [...] der IT-Sicherheit, [...] 2. das vom BSI entwickelte und pilotierte ‚Bewertungsschema zur Bestimmung der Verlässlichkeit von IT-Dienstleistungen unter besonderer Berücksichtigung von Aspekten der Hochverfügbarkeit‘ (‚HV-Benchmark‘) schrittweise auf alle Rechenzentren in der Bundesverwaltung anzuwenden. Das Verfahren soll weiter optimiert und mit der bereits etablierten Methode der IT-Sicherheitsrevision kombiniert werden*“.

HV-Benchmark

Der HV-Benchmark[3] (HVB) hat zum Ziel, die Verlässlichkeit einer zu betrachtenden IT-Dienstleistung oder eines Rechenzentrums (RZ) zu messen und zu bewerten. Dies erfolgt mit Hilfe von etwa 100 besonders relevanten Aspekten der Verlässlichkeit (sogenannte „Indikatoren“) unter der Nutzung von Reifegradmodellen.

Der Begriff „Verlässlichkeit“ beschreibt die Erwartung, dass eine IT-Dienstleistung, im Vorfeld nachweisbar und nachvollziehbar, die angeforderten Funktionen erfüllt. Verlässlichkeit ist ein Maß für die Qualität von IT-Dienstleistungen und wird im Wesentlichen durch folgende sieben Kriterien bestimmt: Verfügbarkeit, Integrität, Vertraulichkeit, Betriebssicherheit, Wartbarkeit, Transparenz und Leistungsfähigkeit. Die drei Grundwerte der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) sind im Begriff „Verlässlichkeit“ enthalten, d. h. Verlässlichkeit umfasst die Informationssicherheit, geht aber darüber hinaus.

Zu den Zielgruppen, die mit dem HVB angesprochen werden sollen, gehören vor allem RZ-Betreiber, die z. B. eine Selbsteinschätzung vornehmen möchten, und IT-Nutzer, die einen geeigneten RZ-Betreiber suchen.

HV-Benchmark kompakt

Der HV-Benchmark kompakt (HVB-kompakt) ist eine komprimierte Version des HV-Benchmark, die gegenüber der Vollversion des HV-Benchmark eine leicht modifizierte Methodik verwendet und um

[1] Beschluss des HHA zu TOP 23 a) und b) in seiner 50. Sitzung am 17.06.2015, Ausschussdrucksache Nr. 18(8)2134.
[2] Beschluss des HHA zu TOP 14 a), b) und c) in seiner 82. Sitzung am 28.09.2016, Ausschussdrucksache Nr. 18(8)3472.
[3] HV-Benchmark: Bewertungsschema zur Bestimmung der Verlässlichkeit von IT-Dienstleistungen unter besonderer Berücksichtigung von Aspekten der Hochverfügbarkeit (HV), BSI.

Revisionselemente ergänzt worden ist. Der HHA hat seinen Auftrag explizit „*hinsichtlich [...] der IT-Sicherheit*“ erteilt. Mit Hilfe aller Indikatoren der Vollversion des HVB wird aber nicht nur die IT-Sicherheit „im engeren Sinne“, sondern die darüber hinaus gehende „Verlässlichkeit“ betrachtet. Um die Analyse der RZ auf die IT-Sicherheit „im engeren Sinne“ zu fokussieren, wurde der Umfang des HVB durch den HVB-kompakt reduziert, indem solche Indikatoren ausgewählt worden sind, die den „Kern“ der IT-Sicherheit repräsentieren.

Der HVB-kompakt in der vorliegenden Version 4.0 ist die Weiterentwickelung der Version 3.0 auf Basis der Erfahrungen aus den bereits durchgeführten RZ-Sicherheitsanalysen

Der für den HHA zu erstellende Bericht adressiert Abgeordnete und benötigt daher ein im politischen Raum verständliches Abstraktionsniveau im Sinne einer Management-Zusammenfassung. Der Ansatz des HVB, für unterschiedliche Indikatoren Reifegrade zu messen, ist für diesen Zweck zu technisch. Daher werden für den Bericht vier breiter verständliche Kategorien zur Darstellung der Sicherheit von RZ ausgewählt:

- Informationssicherheits-Management,
- Cyber-Sicherheit,
- Krypto-Sicherheit,
- Physische Sicherheit.

Diese Berichtskategorien wurden ihrerseits noch einmal in Unterkategorien unterteilt. Schließlich wurden solche Indikatoren aus dem HVB ausgewählt, mit deren Hilfe alle (Unter-)Kategorien abgedeckt werden können. Ausgewählt wurde etwa ein Drittel der Indikatoren des HVB. Sie bilden den HVB-kompakt. Die detaillierte Herleitung des HVB-kompakt (V 4.0) aus dem HVB ist in Anhang C.a beschrieben.

Abbildung 1 (siehe Seite 7) gibt einen Überblick über alle Indikatoren des HVB. Gelb markiert sind die Indikatoren, die für den HVB-kompakt (V 4.0) berücksichtigt worden sind.

Methodik der RZ-Sicherheitsanalyse

a) Anwendung des HVB-kompakt

Die Methodik des HVB (und auch des HVB-kompakt) beruht im Wesentlichen auf der Anwendung der einzelnen Indikatoren auf das zu analysierende Rechenzentrum. Die Indikatoren nehmen ganzzahlige Werte von 0 bis 5 an. Bei Indikatoren, die sich auf einen organisatorischen Prozess (Management / IT-Steuerung) im RZ beziehen, spricht man von fünf „Reifegraden“. Eine allgemeine Beschreibung der Reifegrade befindet sich im Anhang C.b. Bei Indikatoren, die sich auf Technik beziehen, spricht man von fünf „Potenzialstufen“. Die allgemeine Beschreibung von Potenzialstufen befindet sich in Anhang C.c.

Jeder Reifegrad sowie jede Potenzialstufe (beide im Weiteren nur „Stufe“ genannt) ist mit einer oder mehreren geschlossenen Fragen hinterlegt, also solchen, die mit „Ja“ oder „Nein“ zu beantworten sind.

Eine Stufe ist erreicht, wenn alle Fragen der betreffenden Stufe und die Fragen aller vorangehenden Stufen mit „Ja“ beantwortet werden können. Die erreichte Stufe entspricht dem Wert des Indikators. Konnte die Stufe 1 nicht erreicht werden, nimmt der Indikator den Wert Null an.

Fragen sind ihrem Sinn entsprechend zu beantworten. Kann eine Frage ihrem Wortlaut nach nicht mit „Ja“ beantwortet werden, sind aber sinngemäß gleich- oder höherwertige Maßnahmen umgesetzt, so kann die Frage dennoch als mit „Ja“ beantwortet gewertet werden.

Das Resultat der Anwendung des HVB-kompakt ist eine Übersicht über die Reife des analysierten RZ hinsichtlich der betrachteten Sicherheitsaspekte. Für den Bericht an den HHA werden diese Ergebnisse generalisiert und in die oben genannten Berichtskategorien verdichtet.

Im Rahmen der RZ-Sicherheitsanalyse erfolgt die Anwendung des HVB-kompakt zunächst in Form einer Selbsteinschätzung durch den RZ-Betreiber.

b) Plausibilisierung der Selbsteinschätzung

Die Plausibilisierung der Selbsteinschätzung erfolgt in zwei Schritten:

- Durchführung von **Interviews**, in denen die Angaben des RZ-Betreibers hinterfragt werden.

- Anwendung von sogenannten **Revisionselementen**, um die Angaben des RZ-Betreibers aus der Selbsteinschätzung und aus dem Interview zu einzelnen Indikatoren stichprobenartig zu verifizieren. Die eingesetzten Revisionselemente sind in der folgenden Tabelle dargestellt:

Revisionselement	**Beschreibung**
Dokumentenreview: Überprüfung von Dokumenten	Die Überprüfung der Dokumentation erfolgt auf der Grundlage der in der Institution eingesetzten Standards (z. B. IT-Grundschutz).
Datenanalysen: Einsichtnahme in Stichproben	Zur Überprüfung von Prozessen können Stichproben von z. B. Protokollen, Tickets, Konfigurationen etc. genutzt werden.
RZ-Begehung: Sichtprüfung eines RZ und von Komponenten	Die Begehung mindestens eines RZ pro Institution ist ein fester Bestandteil der Untersuchung.

Tabelle 1: Revisionselemente

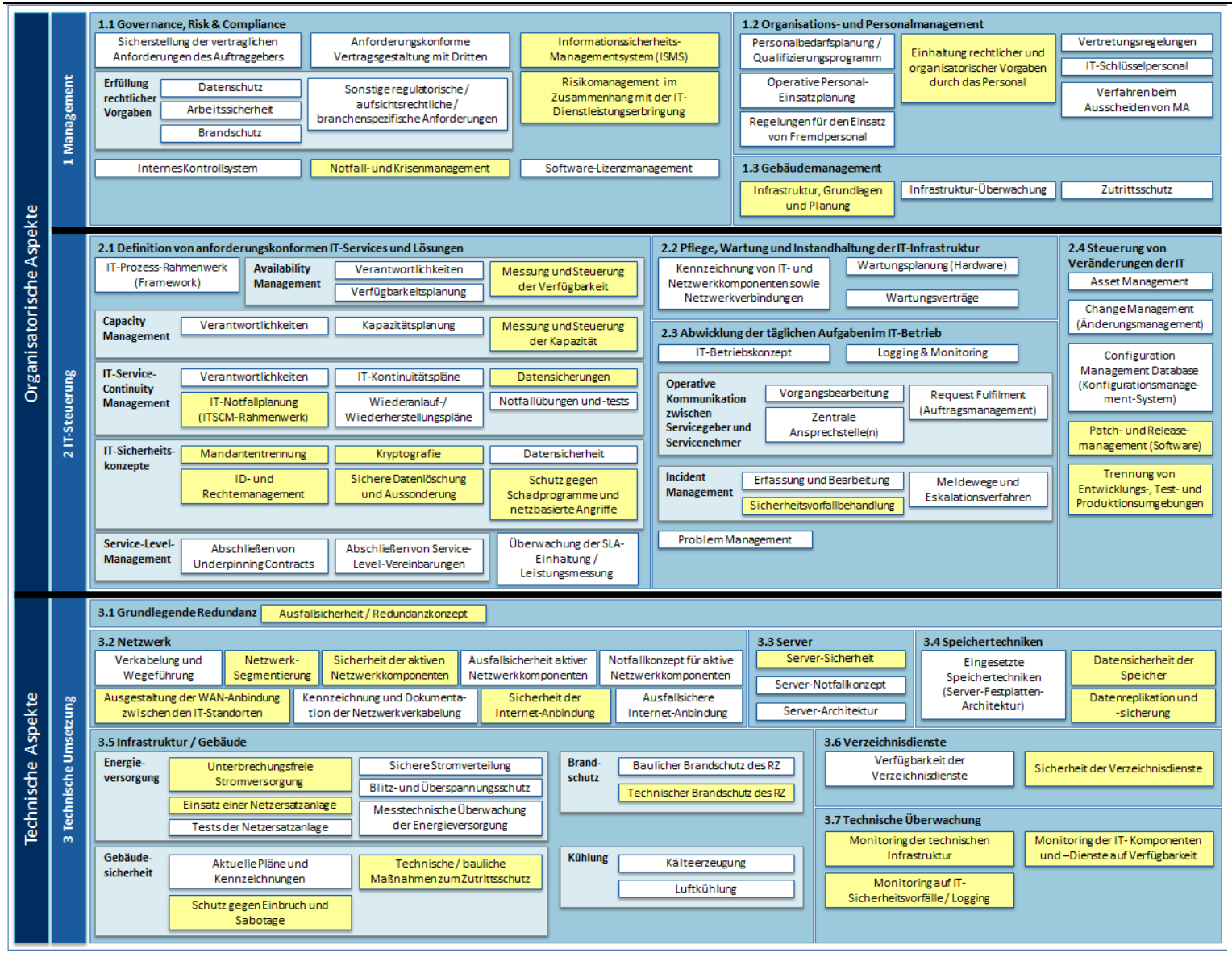

Abbildung 1: Übersicht aller Indikatoren des HVB. Gelb markiert sind die Indikatoren des HVB-kompakt.

B. Anwendung des HV-Benchmark kompakt

B.a. Gegenstand der Betrachtung

Der Auftrag des HHA sieht die Betrachtung der Rechenzentren der Bundesverwaltung vor. Der HVB-kompakt ist einzeln auf jedes RZ einer Behörde anzuwenden.

Bitte beschreiben Sie zunächst die Behörde anhand der folgenden Merkmale:

- Bezeichnung
- Sitz
- Gesamtzahl der Mitarbeiter
- Anzahl der Mitarbeiter, die sich mit der IT befassen
- Anzahl der RZ-Standorte

Beschreiben Sie weiterhin jedes RZ anhand der folgenden Merkmale:

- Ort des RZ
- Anzahl der Mitarbeiter des RZ
- Kapazität:
  - RZ-Fläche in qm
    - Wieviel davon wird tatsächlich genutzt?
  - Elektrische Leistungsaufnahme des RZ (Durchschnittswert in kVA)
- Anzahl der genutzten (physischen) Serversysteme
- Anzahl der gehosteten IT-Verfahren
  - Einige Beispiele für wichtige IT-Verfahren
  - Einige wesentliche Nutzer
- Maximal zugesicherte Verfügbarkeit
  - nach folgendem Schema der Verfügbarkeitsklassen (VK):
    - VK 0: ohne Anforderungen an die Verfügbarkeit (~ 95 %); bis zu 438 h/Jahr Ausfallzeit
    - VK 1: normale Verfügbarkeit (99 %); bis zu 88 h/Jahr Ausfallzeit
    - VK 2: hohe Verfügbarkeit (99,9 %); bis zu 9 h/Jahr Ausfallzeit
    - VK 3: sehr hohe Verfügbarkeit (99,99 %); bis zu 53 min/Jahr Ausfallzeit
    - VK 4: höchste Verfügbarkeit (99,999 %); bis zu 6 min/Jahr Ausfallzeit
    - VK 5: Desaster-tolerant
- Angabe des Schutzbedarfs hinsichtlich „Vertraulichkeit“, Integrität“ und „Verfügbarkeit
- Weitere Charakteristika des Betrachtungsgegenstands, sofern die oben genannten aus Ihrer Sicht nicht ausreichen.
- Zentraler Ansprechpartner für Rückfragen (Funktion und Kontaktdaten)

B.b. Indikatoren

Die nachfolgenden Indikatoren werden gemäß der in der Einführung beschriebenen Methodik auf jedes RZ einer Behörde angewendet.

B.b.1. Informationssicherheits-Managementsystem (ISMS) [1.1.3[4]]

Domäne:	Management
Unterdomäne:	Governance, Risk & Compliance
Indikator:	Informationssicherheits-Managementsystem (ISMS)
Kriterien:	Verfügbarkeit; Vertraulichkeit; Integrität; Transparenz; Leistungsfähigkeit
Kurz-beschreibung	Das ISMS (z. B. nach BSI IT-Grundschutz) umfasst alle Regelungen, die für die Steuerung und Lenkung der Informationssicherheit sorgen. Das ISMS legt fest, mit welchen Instrumenten und Methoden das Management einer Institution die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt (plant, durchführt, überwacht und verbessert). Zu einem ISMS gehören folgende grundlegende Komponenten: - Management-Prinzipien - Ressourcen - Mitarbeiter - Sicherheitsprozess mit a. Leitlinie zur Informationssicherheit b. Sicherheitskonzept c. Informationssicherheitsorganisation
Fragen zu 1	Ist mindestens eine Person innerhalb der Organisation für die Leitung des Informationssicherheitsmanagements benannt, etabliert und in ihrer Rolle zuständig für die Sicherstellung der Informationssicherheit (bspw. IT-Sicherheitsbeauftragter oder Chief Information Security Officer)?
Fragen zu 2	Sind Dokumentationen oder Vorgaben vorhanden, in denen beschrieben wird, wie ein anforderungsgerechter Schutz aller Informationen und IT-Ressourcen vor Bedrohungen wie Zerstörung, Enthüllung, Modifizierung oder nicht autorisierter Benutzung jederzeit sichergestellt ist und sind die dafür notwendigen Ressourcen und Mitarbeiter vorhanden?
Fragen zu 3	Sind die erforderlichen Dokumentationen (z. B. Sicherheitskonzepte) vollständig, richten sich am BSI IT-Grundschutz oder ISO 27001 aus und umfassen mindestens Folgendes: Sicherheitsleitlinie, Klassifizierung von Informationen und Systemen und deren Schutzbedarf, Risikobewertung, ID- und Rechtemanagement, Physische Sicherheit, Datensicherheit (inkl. Kommunikationssicherheit und Datensicherung), Schutz vor Malware, IT-Sicherheit am Arbeitsplatz, Sicherheitsvorfallbehandlung?
Fragen zu 4	Wird im Rahmen von regelmäßigen Sicherheitsaudits die Einhaltung der sicherheitsrelevanten Maßnahmen und Prozesse entsprechend ihrer Vorgaben überprüft? Werden erkannte Defizite abgestellt?
Fragen zu 5	Werden auch die übergeordneten Prozesse, Vorgaben und Konzepte regelmäßig auf ihre Effektivität überprüft (unter Einbeziehung der Ergebnisse gemäß 4) und schnellstmöglich verbessert?

[4] Jedem Indikator ist in eckigen Klammern die Nr. des Indikators in der Vollversion des HVB beigefügt.

B.b.2. Risikomanagement im Zusammenhang mit der IT-Dienstleistungserbringung [1.1.8]

Domäne:	Management
Unterdomäne:	Governance, Risk & Compliance
Indikator:	Risikomanagement im Zusammenhang mit der IT-Dienstleistungserbringung
Kriterien:	Verfügbarkeit; Transparenz
Kurz-beschreibung	Risikomanagement ist die Gesamtheit der Aktivitäten, die eine Organisation durchführt, um sich ihrer aktuellen Risiken bewusst zu werden und diese auf ein akzeptables Maß zu reduzieren. Ein Risiko kann als die Beschreibung eines Ereignisses mit der Möglichkeit negativer Auswirkungen auf eine Organisation und ihre Ziele definiert werden. Im Gegensatz zu einem Schaden, einem realen Sachverhalt in der Vergangenheit, ist ein Risiko ein Sachverhalt, dessen Eintritt ungewiss ist, der im Falle des Eintritts aber einen konkreten Schaden verursachen kann. Dieser Indikator umfasst vor allem das Management von Risiken im Zusammenhang mit der IT-Dienstleistungserbringung, einschließlich der IT-Sicherheitsrisiken, Ausfallrisiken und Haftungsrisiken. Der Risikomanagement-Prozess besteht aus dem Identifizieren, Analysieren, Bewerten, Behandeln und Überwachen von Risiken, einschließlich der Risikokontrolle (z. B. nach ISO 31000 oder BSI-Standard 200-3).
Fragen zu 1	Ist jemand innerhalb der Organisation für die Leitung des Risikomanagements benannt, verantwortlich und in seiner Rolle zuständig für die Sicherstellung der adäquaten Identifikation, Analyse, Bewertung, Behandlung und Überwachung von Risiken sowie für die regelmäßige Anpassung der Risikostrategie der Organisation?
Fragen zu 2	Sind entsprechende Dokumentationen / Vorgaben vorhanden, in denen beschrieben wird, wie sich die Organisationskultur und -strategie bezüglich des Risikomanagements darstellt, welche Bereitschaft zur Risikoübernahme besteht, welche Prozesse zur Risikobeurteilung (Identifikation, Analyse, Bewertung), Risikobehandlung sowie zur Überwachung und Kontrolle (Messung, Meldung und Eskalation) zu etablieren / anzuwenden sind, um die aktuelle Risikolage regelmäßig auszuwerten und Vorschläge zur Anpassung der Risikostrategie abzuleiten?
Fragen zu 3	Sind die Prozesse und Ergebnisse aus den Vorgaben unter 2 in der Organisation vollständig etabliert und umgesetzt? Existieren vollständige Dokumentationen und Vorgaben?
Fragen zu 4	Wird die Einhaltung der festgelegten Risikomanagement-Prozesse regelmäßig geprüft, werden die etablierten Methoden und Maßnahmen regelmäßig auf Plausibilität geprüft und werden entsprechende Vorfälle in einer revisionssicheren Art erfasst? Werden regelmäßig die Meldewege auf Praxistauglichkeit und Aktualität überprüft? Werden erkannte Defizite abgestellt?
Fragen zu 5	Werden regelmäßig und anlassabhängig (insbesondere unter Nutzung der Prüfergebnisse gemäß 4) übergeordnete Prüfungen durchgeführt, die zur Anpassung des gesamten Risikomanagements führen (d. h. zur Anpassung von Risikostrategie und Risikoappetit) oder sogar zur Anpassung der Organisationsstrategie?

B.b.3. Notfall- und Krisenmanagement [1.1.10]

Domäne:	Management
Unterdomäne:	Governance, Risk & Compliance
Indikator:	Notfall- und Krisenmanagement
Kriterien:	Verfügbarkeit; Vertraulichkeit; Integrität; Betriebssicherheit; Wartbarkeit; Leistungsfähigkeit
Kurz-beschreibung	Kritische Ereignisse (Notfälle, Krisen, Katastrophen) sind ungeplante Ereignisse, die den normalen Betrieb stören oder unterbrechen und dabei hohe Schäden verursachen können. Da sich das Eintreten kritischer Ereignisse kaum vermeiden lässt, besteht die Notwendigkeit, auf kritische Ereignisse angemessen reagieren zu können, um den Schaden zu minimieren. Vorfälle und Störungen können sich zu kritischen Ereignissen ausweiten und müssen daher im Rahmen der normalen Geschäftstätigkeit (Störungsmanagement) beobachtet und zeitnah behoben werden. Falls sie sich zum kritischen Ereignis entwickeln, muss entsprechend eskaliert werden. Beispiele für kritische Ereignisse sind schwere Cyberangriffe, Brand, Wassereinbruch, Bombendrohung, Munitionsfund, Zerstörung von Versorgungsleitungen, aber auch Imageverlust durch Meldungen in Presse und Internet, Entführung von Mitarbeitern, Streik oder Insolvenz eines kritischen Lieferanten. Die Reaktion auf kritische Ereignisse umfasst mehrere Phasen: Vorbereitung, Entdeckung, Analyse, Eskalation, Eindämmung, Kontrolle und Nachbereitung. Im Rahmen der Vorbereitung sollten Rollen, Maßnahmen (Krisen-, Notfall-, Alarmierungspläne etc.) und Prozesse / Workflows zur Notfall- und Krisenbehandlung beschrieben, etabliert und überprüft werden. Die Phasen Entdeckung, Analyse und ggf. Eskalation umfassen Maßnahmen zur Erkennung und Klassifizierung von Vorfällen in kritische (Notfälle und Krisen) und nicht-kritische Ereignisse sowie die Einleitung von Verfahren zur Meldung, Alarmierung und Eskalation. Die Phasen Eindämmung, Kontrolle und Nachbereitung beinhalten die Abarbeitung der Maßnahmen zum angemessenen Umgang, zur Schadensbegrenzung und -bereinigung als weitere Reaktion auf das kritische Ereignis bis hin zur Wiederherstellung des Normalbetriebs. Einschlägig sind insbesondere die Standards ISO 22301 oder BSI 100-4.
Fragen zu 1	Ist jemand innerhalb der Organisation dafür zuständig sicherzustellen, dass kritische Ereignisse als solche identifiziert werden und im Falle eines kritischen Ereignisses eine Notfall- oder Krisenorganisation vorhanden ist, die in ausreichender Personalstärke auf schnellstem Wege alarmiert wird und ihre Funktion aufnimmt?
Fragen zu 2	Existieren Dokumente und Vorgaben, welche die proaktiven und reaktiven Prozesse, Pläne und Maßnahmen zur Etablierung und Umsetzung eines Notfall- und Krisenmanagements (zumindest bis zu einem gewissen Grad) definieren und beschreiben?
Fragen zu 3	Sind Anweisungen, Richtlinien, Konzepte und Pläne für ein Notfall- und Krisenmanagement etabliert, vollständig dokumentiert und vollständig umgesetzt, die sich an Standards wie BSI 100-4 oder ISO 22301 orientieren? Werden sowohl die einzelnen Meldestellen (Empfänger von Meldungen) als auch die an der Notfall- und Krisenorganisation beteiligten Mitarbeiter regelmäßig geschult und trainiert (bspw. anhand von speziellen Seminaren oder Notfallübungen), so dass sie in der Lage sind, die definierten Verfahren zur Meldung, Alarmierung und Eskalation sowie die für die Abarbeitung vorgesehenen Notfallmaßnahmen und -pläne vollumfänglich anzuwenden?
Fragen zu 4	Werden die Einhaltung der definierten Verfahren zur Meldung, Alarmierung und Eskalation, die Qualifikation der an der Notfall- und Krisenorganisation beteiligten Personen, die vorgesehenen Räumlichkeiten (z. B. Krisenstabsraum), die Einhaltung der

	Maßnahmen zur Notfall- und Krisenbewältigung sowie die Notfallkommunikation regelmäßig überprüft – insbesondere durch Übungen im Rahmen eines Übungswesens? Führen die Überprüfungen dazu, dass erkannte Lücken zwischen Soll und Ist geschlossen werden?
Fragen zu 5	Erfolgen regelmäßig Reviews und unabhängige Audits des Notfall- und Krisenmanagements insgesamt, insbesondere hinsichtlich seiner Funktionsfähigkeit und Effektivität, unter Einbeziehung der Ergebnisse aus 4? Führen die Überprüfungen zu einer Optimierung der Konzepte, Verfahren, Prozesse, Rollen, Maßnahmen, Räumlichkeiten etc. des Notfall- und Krisenmanagements?

B.b.4. Einhaltung rechtlicher und organisatorischer Vorgaben durch das Personal [1.2.4]

Domäne:	Management
Unterdomäne:	Organisations- und Personalmanagement
Indikator:	Einhaltung rechtlicher und organisatorischer Vorgaben durch das Personal
Kriterien:	Vertraulichkeit; Integrität
Kurz-beschreibung	Es muss gewährleistet werden, dass die Mitarbeiter rechtliche und organisatorische Vorgaben einhalten. Zu den dafür erforderlichen Verfahren zählen insbesondere die Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen sowie die geregelte Einarbeitung/Einweisung neuer Mitarbeiter. Eine Verpflichtung sollte nicht nur bei Einstellung erfolgen, sondern auch anlassabhängig, z. B. wenn sich Vorgaben und Regelungen ändern. Sie kann auch regelmäßig wiederholt werden. In jedem Fall sollten die Mitarbeiter über den Inhalt der Verpflichtung regelmäßig belehrt oder dafür sensibilisiert werden.
Fragen zu 1	Haben alle Mitarbeiter eine Vertraulichkeitsvereinbarung unterzeichnet (inkl. Fremdpersonal, Praktikanten, Werkstudenten, Teilzeitkräfte etc.), welche die relevanten Gesetze, Vorschriften und Regelungen berücksichtigt?
Fragen zu 2	Liegen für Mitarbeiter, die in sicherheitsrelevanten Bereichen eingesetzt werden, Führungszeugnisse vor und sind in diesen Bereichen definierte Benutzer-/Zugangsbeschränkungen umgesetzt? Erfolgt anlassabhängig (z. B. bei Änderung von Gesetzen, Vorschriften und Regelungen) eine Neuverpflichtung der betroffenen Mitarbeiter? Sind auch hierfür die entsprechenden Prozesse dokumentiert, kommuniziert und umgesetzt? Nur für behördliche Rechenzentren: Werden Sicherheitsüberprüfungen durchgeführt, die in angemessener Relation zum Schutzbedarf der Daten stehen, mit denen die Mitarbeiter in Kontakt kommen können?
Fragen zu 3	Ist ein standardisierter Mitarbeitereinführungsprozess vorhanden, in dem neben dem Aufgabengebiet (und dessen relevanten Vorschriften und Regelungen) auch Themen wie Informationssicherheit, Notfallplanung und datenschutzrelevante Aspekte vermittelt werden und wird dies vollständig dokumentiert? Erfolgt in regelmäßigen Abständen eine Mitarbeiter-Belehrung und -Sensibilisierung mit Mitarbeiter-Feedback, welche sich u. a. mit den relevanten Gesetzen, Vorschriften und Regelungen befasst (inklusive der notwendigen Dokumentation der Belehrung)?
Fragen zu 4	Wird die Einhaltung der Verfahren zur Personalverpflichtung regelmäßig geprüft? Wird in regelmäßigen Abständen geprüft, ob alle Mitarbeiter angemessen verpflichtet sind? Werden Diskrepanzen beseitigt?
Fragen zu 5	Wird der Prozess der Personalverpflichtung regelmäßig und anlassabhängig überprüft und verbessert? Werden Verbesserungsmaßnahmen (bspw. aus dem Feedbackgespräch oder aus Änderungen des Informationssicherheitsmanagements) für den Prozess der Personalverpflichtung umgesetzt und nachgehalten?

B.b.5. Infrastruktur, Grundlagen und Planung [1.3.1]

Domäne:	Management
Unterdomäne:	Gebäudemanagement
Indikator:	Infrastruktur, Grundlagen und Planung
Kriterien:	Verfügbarkeit; Vertraulichkeit; Betriebssicherheit; Leistungsfähigkeit
Kurz-beschreibung	Das Gebäudemanagement verantwortet die störungsfreie Nutzbarkeit der Gebäude, in denen das RZ betrieben wird, inkl. aller für den Betrieb erforderlichen technischen Einrichtungen. Bei der Festlegung der Grundlagen und der weiteren Planung (Standortauswahl, bauliche Struktur und Hülle, etc.) sind alle Aspekte zu berücksichtigen, die ein Gebäude betreffen. Diese sind der Schutz des Gebäudes gegen Einwirkungen von außen und innen (Feuer, Wasser, Sturm, Blitz/EMP, Ausfall des Energieversorgers, Einbruch, Anschlag, Erdbeben etc.) sowie ein ausfall- und betriebssicherer Aufbau aller technischen Gebäudeeinrichtungen (Netzersatzanlage, USV, Blitz- und Überspannungsschutz; Brandüberwachung, Löschtechnik; Kälteversorgung; Zutrittskontrolle; Gefahrenmeldetechnik etc.).
Fragen zu 1	Sind in der Organisation Verantwortliche benannt, die sich um die Berücksichtigung aller in der Kurzbeschreibung genannten Aspekte bei Planung und Betrieb des Gebäudes kümmern? Wird eine enge Zusammenarbeit der Verantwortlichen gelebt?
Fragen zu 2	Existiert (auf der Basis einer mindestens partiellen Risikoanalyse) ein Gebäudeschutz- und Gebäudemanagementkonzept, das unter Berücksichtigung gängiger Normen und Standards die Umsetzung von Maßnahmen entsprechend der Verlässlichkeitsanforderungen für die Gebäude und Gebäudeteile, in denen die Einrichtungen des RZ (sowohl IT als auch Support-Technik) betrieben werden, vorschreibt, und ist es so weit auch umgesetzt?
Fragen zu 3	Ist für alle Gebäude oder Gebäudeteile, in denen die Einrichtungen des RZ (sowohl IT als auch Support-Technik) betrieben werden, eine umfassende Risikoanalyse durchgeführt worden, ist diese vollständig dokumentiert und sind anhand der Ergebnisse entsprechende Schutzmaßnahmen vollständig umgesetzt?
Fragen zu 4	Erfolgt eine regelmäßige Überprüfung der Gebäude, ob die Anforderungen weiterhin eingehalten werden? Wird bei jeder Verlagerung oder Neueinrichtung von IT-Umgebungen geprüft, ob die Anforderungen durch das Gebäude noch erfüllt werden? Werden bei Abweichungen von den Vorgaben zur Gebäude- und Infrastrukturverlässlichkeit entsprechende Verbesserungsmaßnahmen eingeleitet und deren Umsetzung nachgehalten?
Fragen zu 5	Werden die Vorgaben des Gebäudeschutzkonzepts und des Gebäudemanagementkonzepts regelmäßig überprüft und angepasst – hinsichtlich ihrer Wirksamkeit angesichts der Gefährdungslage und des Stands der Technik?

B.b.6. Availability Management (Verfügbarkeitsmanagement): Messung und Steuerung der Verfügbarkeit [2.1.4]

Domäne:	IT-Steuerung
Unterdomäne:	Definition von anforderungskonformen IT-Services und Lösungen
Indikator:	Availability Management (Verfügbarkeitsmanagement): Messung und Steuerung der Verfügbarkeit
Kriterien:	Verfügbarkeit; Transparenz; Leistungsfähigkeit
Kurz-beschreibung	Die Messung und Steuerung der Verfügbarkeit umfasst das systematische Erfassen von Verfügbarkeitsdaten (Ist-Zustand), die Analyse dieser Daten in Bezug auf die Erfüllung der Verfügbarkeitsanforderungen (Vergleich zum Soll-Zustand) und die Reaktion auf Abweichungen zwischen Soll und Ist. Das Ziel ist, eine anforderungskonforme Verfügbarkeit zu gewährleisten.
Fragen zu 1	Wird die Verfügbarkeit für die kritischen IT-Komponenten gemessen, mit definierten Soll-Verfügbarkeitsanforderungen verglichen und auf Abweichungen reagiert?
Fragen zu 2	Werden regelmäßig Auswertungen und Analysen (Soll-Ist-Vergleiche) der gesammelten Verfügbarkeitsdaten nach einem vorgegebenen Verfahren durchgeführt und dokumentiert und wird auf Abweichungen reagiert?
Fragen zu 3	Sind die Soll-Verfügbarkeitsanforderungen einheitlich und vollständig dokumentiert, werden diese kommuniziert und erfolgt ein systematisches und einheitliches Monitoring der Verfügbarkeiten aller für die Erbringung der IT-Dienstleistung relevanten Komponenten durch Monitoringsysteme? („Einheitlich“ bedeutet hier, dass die Ergebnisse ggf. unterschiedlicher Monitoring-Systeme sinnvoll vergleichbar sind.) Sind die Vorgaben zum Monitoring vollständig dokumentiert und kommuniziert?
Fragen zu 4	Werden die Soll-Verfügbarkeitsanforderungen aktuell gehalten, werden die Ist-Zustände sowie Abweichungen kontinuierlich überprüft und werden automatisiert geeignete Meldungen über Abweichungen verschickt? Wird auf erkannte Abweichungen reagiert, so dass Lücken geschlossen werden können?
Fragen zu 5	Wird regelmäßig und anlassbezogen (auch unter Einbeziehung der Ergebnisse gemäß 4) analysiert, ob das Availability Management die Verfügbarkeit anforderungskonform steuert und werden die Prozesse der Messung und Steuerung der Verfügbarkeit entsprechend dieser Analysen verbessert?

B.b.7. Capacity Management (Kapazitätsmanagement): Messung und Steuerung der Kapazität [2.1.7]

Domäne:	IT-Steuerung
Unterdomäne:	Definition von anforderungskonformen IT-Services und Lösungen
Indikator:	Capacity Management (Kapazitätsmanagement): Messung und Steuerung der Kapazität
Kriterien:	Verfügbarkeit; Transparenz; Wartbarkeit; Leistungsfähigkeit
Kurz-beschreibung	Die Messung und Steuerung der Kapazität umfasst das systematische Erfassen von Kapazitätsdaten (Ist-Zustand), die Analyse dieser Daten in Bezug auf die Erfüllung der Kapazitätsanforderungen (Vergleich zum Soll-Zustand) und die Reaktion auf Abweichungen zwischen Soll und Ist. Ziel ist es, angemessene Kapazitäten bereitzustellen, so dass die Dienstleistungen anforderungskonform erbracht werden können. Von Bedeutung sind dabei insbesondere die für die Erbringung der IT-Dienstleistung relevanten Komponenten. Diesbezüglich werden Parameter wie z. B. die Netzwerkauslastung, der Speicherplatz im SAN, Anzahl der Speicherzugriffe, die CPU-Auslastung von Servern und Virtualisierungssystemen, der genutzte Arbeitsspeicher (RAM) von Servern oder die Kapazitätsdaten von Clients erfasst.
Fragen zu 1	Wird die Kapazität für die kritischen IT-Komponenten gemessen, mit definierten Soll-Kapazitätsanforderungen verglichen und wird auf Abweichungen reagiert?
Fragen zu 2	Werden regelmäßig Auswertungen und Analysen (Soll-Ist-Vergleiche) der gesammelten Kapazitätsdaten nach einem vorgegebenen Verfahren durchgeführt und wird auf Abweichungen reagiert?
Fragen zu 3	Sind die Soll-Kapazitätsanforderungen einheitlich und vollständig dokumentiert und erfolgt ein systematisches und einheitliches Monitoring der Kapazität aller für die Erbringung der IT-Dienstleistung relevanten Komponenten durch Monitoringsysteme? („Einheitlich“ bedeutet hier, dass die Ergebnisse ggf. unterschiedlicher Monitoring-Systeme sinnvoll vergleichbar sind.) Sind die Vorgaben zum Monitoring vollständig dokumentiert und kommuniziert? Werden die Prozesse zur Messung und Steuerung der Kapazität in der Institution kommuniziert?
Fragen zu 4	Werden die Soll-Kapazitätsanforderungen aktuell gehalten, werden die Ist-Zustände sowie Abweichungen kontinuierlich überprüft und werden automatisiert geeignete Meldungen über Abweichungen verschickt? Wird auf erkannte Abweichungen reagiert, so dass Lücken geschlossen werden können?
Fragen zu 5	Wird regelmäßig und anlassbezogen (auch unter Einbeziehung der Ergebnisse gemäß 4) analysiert, ob das Capacity Management die Kapazität anforderungskonform steuert und werden die Messung und Steuerung der Kapazität entsprechend dieser Analysen verbessert?

B.b.8. IT-Service Continuity Management: IT-Notfallplanung (ITSCM-Rahmenwerk) [2.1.9]

Domäne:	IT-Steuerung
Unterdomäne:	Definition von anforderungskonformen IT-Services und Lösungen
Indikator:	IT-Service Continuity Management: IT-Notfallplanung (ITSCM-Rahmenwerk)
Kriterien:	Verfügbarkeit; Leistungsfähigkeit
Kurz-beschreibung	Die IT-Notfallplanung verantwortet im Wesentlichen das Rahmenwerk (IT-Notfallkonzept), mit dessen Hilfe beim Eintreffen eines Notfalls der IT-Betrieb so schnell wie möglich wiederhergestellt werden kann. Vorgehen und Inhalt der Dokumentation orientieren sich beispielsweise am BSI-Standard 100-4. Die IT-Notfallplanung leistet Unterstützung bei der Bestimmung, Herstellung, Dokumentation und Verbesserung der notwendigen Ausfallsicherheit von IT-Ressourcen.
Fragen zu 1	Gibt es Verfahren für die Aufrechterhaltung oder Wiederherstellung des IT-Betriebs, welche die Verfügbarkeit der IT-Services im erforderlichen Maß und im erforderlichen Zeitraum nach Unterbrechungen oder Ausfällen sicherstellen?
Fragen zu 2	Sind sowohl Rollen, Verantwortlichkeiten und Prozesse des IT-Service Continuity Managements definiert? Sind zudem die Strukturen und Vorlagen für Entwicklung, Test und Ausführung von Wiederanlauf-, Wiederherstellungs- und IT-Kontinuitätsplänen vorgegeben?
Fragen zu 3	Gibt es ein zentrales Dokument, welches als Rahmenwerk sowohl die Bestandteile, Verfahren und Vorgaben des IT-Service Continuity Managements einheitlich und vollständig definiert, als auch an akzeptierten Standards (wie z. B. BSI 100-4, ISO 27031 oder IT-Grundschutz) ausgerichtet ist? Ist dieses Rahmenwerk vollständig umgesetzt und in der Organisation kommuniziert?
Fragen zu 4	Werden das ITSCM-Rahmenwerk, die Anforderungen an die Ausfallsicherheit und den Wiederanlauf der Ressourcen und die weiteren Dokumente zur IT-Notfallplanung (z. B. Wiederanlauf-Koordinationsplan, Kontaktlisten) regelmäßig durch das IT-Management geprüft und aktualisiert? Werden dabei die Erkenntnisse aus Notfallübungen berücksichtigt?
Fragen zu 5	Werden regelmäßig und anlassabhängig Prüfungen durchgeführt, um die übergeordneten Prozesse der IT-Notfallplanung zu pflegen und weiterzuentwickeln – auch unter Nutzung der Prüfergebnisse gemäß 4?

B.b.9. IT-Service Continuity Management: Datensicherungen [2.1.12]

Domäne:	IT-Steuerung
Unterdomäne:	Definition von anforderungskonformen IT-Services und Lösungen
Indikator:	IT-Service Continuity Management: Datensicherungen
Kriterien:	Verfügbarkeit; Vertraulichkeit; Integrität
Kurz-beschreibung	Eine Datensicherung soll gewährleisten, dass der IT-Betrieb mittels eines redundanten Datenbestands kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen oder eigenen Datenbestandes verloren gehen. Für die Datensicherungen muss ein Konzept mit verbindlichen Vorgaben vorliegen und es müssen regelmäßige Wiederherstellungstests stattfinden.
Fragen zu 1	Sind für die kritischen IT-Systeme Datensicherungsmaßnahmen vorhanden und werden Wiederherstellungstests durchgeführt?
Fragen zu 2	Gibt es Vorgaben in Bezug auf die Häufigkeit, die Art der Auslagerung und die Absicherung der Daten (z. B. Verschlüsselung) für die Durchführung von Datensicherungen und entsprechend für Wiederherstellungstests, basierend auf einem einheitlichen Schema (z. B. auf Basis einer definierten Klassifikation der Daten bzw. abgeleitet aus dem Schutzbedarf)?
Fragen zu 3	Existieren verbindliche und vollständig dokumentierte Vorgaben und Regeln zur Durchführung und externen Auslagerung von Datensicherungen (Datensicherungskonzept)? Ist das Datensicherungskonzept vollständig umgesetzt und innerhalb der Organisation kommuniziert?
Fragen zu 4	Wird die Einhaltung des Datensicherungskonzepts, insbesondere die Wirksamkeit der Datensicherungen, mittels regelmäßiger Reviews unter Berücksichtigung der aktuellen Anforderungen überprüft und werden erkannte Lücken geschlossen?
Fragen zu 5	Werden regelmäßig und anlassabhängig (auch unter Berücksichtigung der Ergebnisse der Reviews gemäß 4) das Datensicherungskonzept sowie die organisatorischen und technischen Maßnahmen zur Datensicherung überprüft und kontinuierlich verbessert?

B.b.10. IT-Sicherheitskonzepte: Mandantentrennung [2.1.14]

Domäne:	IT-Steuerung
Unterdomäne:	Definition von anforderungskonformen IT-Services und Lösungen
Indikator:	IT-Sicherheitskonzepte: Mandantentrennung
Kriterien:	Vertraulichkeit; Integrität
Kurz-beschreibung	Die Mandantentrennung umfasst die Planung, Steuerung, Verwaltung und Kontrolle der gemeinsamen Nutzung von IT-Systemen durch unterschiedliche datenverarbeitende Stellen („Mandanten“), wobei eine dem Schutzbedarf entsprechende Trennung der Datenbereiche der verschiedenen Mandanten zu gewährleisten ist. Ziel der Mandantentrennung ist es, den Datenzugriff der Nutzer durch ein dem Schutzbedarf entsprechendes mandanten- und rollenbasiertes Berechtigungsmodell so zu beschränken, dass ein unberechtigter Zugriff (auch und insbesondere durch externe Angreifer) aus dem Datenbereich eines Mandanten in den Datenbereich eines anderen Mandanten wirksam unterbunden wird. Das ist vergleichsweise einfach durch physische Trennung realisierbar. Bei Verwendung einer gemeinsamen („shared“) Infrastruktur ist eine eindeutige Zuordnung von Daten zu den jeweiligen Mandanten sowie eine Trennung der Mandanten untereinander umzusetzen. Dafür kommen u. a. folgende Maßnahmen in Frage: eigene virtuelle Server, eigene Plattenpartitionen, virtuelle LANs, Verschlüsselung der Daten.
Fragen zu 1	Ist der Datenzugriff der Nutzer durch ein Berechtigungsmodell beschränkt? Kommen mandantenspezifische Benutzerkennungen zum Einsatz, die ausschließlich zum Zugriff auf Daten der Mandanten verwendet werden?
Fragen zu 2	Werden alle oder mindestens ausgewählte Zugriffe protokolliert und werden datenschutzrechtlich relevante Mängel an den Datenschutzbeauftragten gemeldet? Sind mindestens drei der folgenden Mechanismen der Mandantentrennung (•Rechte- und Rollenmodelle, •eigene virtuelle Server, •eigene Plattenpartitionen, •dedizierte virtuelle LANs für unterschiedliche Mandanten, •unterschiedliche Verschlüsselung in den Datenbereichen unterschiedlicher Mandanten, •physische Trennung der Mandanten etc.) sowohl konzeptionell als auch technisch mit dem Ziel der Trennung existierender Mandanten umgesetzt?
Fragen zu 3	Sind die Daten einer gemeinsamen ("shared") Infrastruktur eindeutig den jeweiligen Mandanten zugeordnet? Erfolgen die Definition der Rollen und die Zuordnung von Institutionen und Personen nach einem definierten sowie nachweisbar gesteuerten Prozess, der vollständig dokumentiert, umgesetzt und kommuniziert wurde? Sind alle sechs der in Frage 2 genannten Mechanismen der Mandantentrennung sowohl konzeptionell als auch technisch mit dem Ziel der Trennung existierender Mandanten umgesetzt?
Fragen zu 4	Erfolgt eine Prüfung der rechtlichen Anforderungen an die Datenverarbeitung sowie eine regelmäßige Kontrolle der Einhaltung der Maßnahmen (technisch und prozessual) zur Mandantentrennung durch Reviews und werden ermittelte Diskrepanzen umgehend beseitigt?
Fragen zu 5	Wird das Konzept zur Mandantentrennung regelmäßig überprüft und aktualisiert? Unterliegen die übergeordneten Prozesse zur Sicherstellung der Mandantentrennung einem kontinuierlichen Verbesserungsprozess, wobei insbesondere auch die Ergebnisse der Prüfungen gemäß 4 berücksichtigt werden?

B.b.11. IT-Sicherheitskonzepte: ID- und Rechtemanagement [2.1.15]

Domäne:	IT-Steuerung
Unterdomäne:	Definition von anforderungskonformen IT-Services und Lösungen
Indikator:	IT-Sicherheitskonzepte: ID- und Rechtemanagement
Kriterien:	Verfügbarkeit; Vertraulichkeit; Integrität; Transparenz
Kurz-beschreibung	Um IT-Systeme oder System-Komponenten und Netze zu nutzen und die dort gespeicherten Informationen abrufen zu können, müssen Zugriffsrechte für die Benutzer definiert werden. Die Definition der Benutzerrechte ist von der jeweiligen Rolle abhängig und sollte dem Need-to-Know-Prinzip (nur die Zugriffsrechte, die für die Aufgabenwahrnehmung notwendig sind) sowie der Sensitivität (dem Schutzbedarf) der Daten genügen.
Fragen zu 1	Haben alle Nutzer nur die Berechtigungen, die sie auch benötigen (Prinzip der geringsten Berechtigungen)? Gibt es Verantwortliche, die für das Berechtigungsmanagement zuständig sind?
Fragen zu 2	Sind der Zugang zu und Zugriff auf Informationen und IT-Ressourcen gemäß den Anforderungen des Auftraggebers (z. B. Schutzbedarf der Daten) abgesichert? Ist dies an entsprechender Stelle dokumentiert?
Fragen zu 3	Liegt ein vollständig dokumentiertes, rollenbasiertes und auf die Compliance-Anforderungen abgestimmtes Berechtigungskonzept vor, welches die besonderen Anforderungen an den Umgang mit Administrator-Rechten (mindestens: starke Authentisierung, Verfahren zur Vergabe und Sperrung von Administrator-Konten und Vier-Augen-Prinzip für sensible Administrationstätigkeiten) sowie die Sicherheit von Anwendungs- und Netzwerkzugängen berücksichtigt? Ist das Berechtigungskonzept vollständig umgesetzt und innerhalb der Organisation kommuniziert?
Fragen zu 4	Wird die Einhaltung des Berechtigungskonzepts und der daraus abgeleiteten Sicherheitsrichtlinien und Sicherheitsmaßnahmen kontinuierlich überwacht und Diskrepanzen umgehend beseitigt?
Fragen zu 5	Werden die Ergebnisse der o. g. Prüfungen in der Weiterentwicklung des Berechtigungskonzepts berücksichtigt? Wird das Berechtigungskonzept regelmäßig überprüft und aktualisiert?

B.b.12. IT-Sicherheitskonzepte: Kryptografie [2.1.16]

Domäne:	IT-Steuerung
Unterdomäne:	Definition von anforderungskonformen IT-Services und Lösungen
Indikator:	IT-Sicherheitskonzepte: Kryptografie
Kriterien:	Vertraulichkeit; Integrität
Kurz-beschreibung	Für die Absicherung von Informationen hinsichtlich Vertraulichkeit, Integrität und Authentizität können kryptografische Verfahren eingesetzt werden. Für unterschiedliche Anwendungen existieren hierfür oftmals frei verfügbare Lösungen, wie S/MIME zur Absicherung der E-Mail-Kommunikation oder das Protokoll TLS zur Absicherung von Übertragungen. PCs und Laptops können mit einer Festplattenverschlüsselung ausgestattet werden, um im Falle eines Verlusts die darauf befindlichen Daten vor unbefugtem Zugriff zu schützen. Die in den Verfahren eingesetzten Algorithmen sollen anerkannten Standards entsprechen, sich auf dem neuesten Stand der technischen Entwicklung befinden und im Idealfall freigegeben (z. B. durch BSI) sein. Bei der Auswahl der Produkte soll auf die Vertrauenswürdigkeit der Hersteller Wert gelegt werden. Die verwendeten kryptografischen Schlüssel sollen hinreichende Längen aufweisen. Hilfestellung geben die Technischen Richtlinien des BSI, etwa TR-02102-1 für die Bewertung der Sicherheit ausgewählter kryptografischer Verfahren und deren Schlüssellängen oder TR-02102-2 zu Empfehlungen für den Einsatz von TLS. Die kryptografischen Schlüssel selbst müssen angemessen sicher gespeichert werden und auch nach einem eventuellen Datenverlust zur Wiederherstellung der Daten zur Verfügung stehen. Es werden in diesem Indikator kryptografische Verfahren und Produkte betrachtet, die in der Zuständigkeit der jeweiligen Institution liegen.
Fragen zu 1	Existiert eine Übersicht (zentral oder verteilt), anhand der erkennbar ist, für welche Aufgaben welche kryptografischen Verfahren, Algorithmen und Schlüssellängen eingesetzt und welche Daten damit geschützt werden sollen? Gibt es mindestens einen Verantwortlichen, der für die Pflege der Übersicht zuständig ist?
Fragen zu 2	Werden nur dem Stand der Technik entsprechende kryptografische Verfahren implementiert, die mit allen anderen IT-Sicherheitskonzepten konform sind? Werden diese Verfahren fachgerecht installiert und eingesetzt? Erfolgt eine unverzügliche Eskalation bei der Feststellung von Sicherheitslücken (bspw. wenn entdeckt wird, dass ein unsicheres Verfahren eingesetzt wird) sowie eine geeignete Reaktion (z. B. Rückruf bestehender Schlüssel und Austausch gegen neue Schlüssel)? Werden die Schlüssel ausreichend sicher aufbewahrt und existieren Datensicherungen der Schlüssel zur Wiederherstellung bei Datenverlust?
Fragen zu 3	Wurde eine Bedrohungsanalyse (Welche Daten sind zu schützen? Gegen was müssen die Daten abgesichert sein: Verlust der Vertraulichkeit / Integrität / Authentizität? An welcher Stelle sind die Daten angreifbar? Welche technischen Möglichkeiten werden einem Angreifer zugetraut?) durchgeführt und dokumentiert? Wurden alle kryptografischen Verfahren, die auf Basis der Anforderungen (IT-System, Datenvolumen, das angestrebte Sicherheitsniveau, Verfügbarkeitsanforderungen etc.) ausgewählt worden sind, mit ihren Algorithmen und Schlüssellängen vollständig und basierend auf gängigen Sicherheitsstandards dokumentiert und implementiert? Wurden die Benutzer für den Umgang mit kryptografischen Verfahren sensibilisiert und geschult? Gibt es ein geregeltes Verfahren für das Schlüsselmanagement sowie einen Notfallplan, falls kryptografische Schlüssel kompromittiert werden oder falls der Verdacht dafür besteht?

Fragen zu 4	Wird die Einhaltung der in 3. genannten Vorgaben und Verfahren regelmäßig und anlassabhängig überprüft? Erfolgt eine regelmäßige Kontrolle, dass die Kryptierung tatsächlich eingesetzt und korrekt angewendet wird? Werden ermittelte Diskrepanzen umgehend beseitigt?
Fragen zu 5	Werden die Informationen aus den Überprüfungen und Auswertungen für eine kontinuierliche Optimierung des Einsatzes von kryptografischen Verfahren genutzt? Werden die o. g. Vorgaben und Verfahren zur Kryptografie regelmäßig überprüft, insbesondere die Aktualität und Angemessenheit der ausgewählten Kryptoverfahren (Abgleich mit den neuesten Technischen Richtlinien und mit entsprechenden Meldungen in der Fachpresse)?

B.b.13. IT-Sicherheitskonzepte: Sichere Datenlöschung und Aussonderung [2.1.17]

Domäne:	IT-Steuerung
Unterdomäne:	Definition von anforderungskonformen IT-Services und Lösungen
Indikator:	IT-Sicherheitskonzepte: Sichere Datenlöschung und Aussonderung
Kriterien:	Vertraulichkeit; Integrität
Kurz-beschreibung	Um die Vertraulichkeit schutzbedürftiger Daten/Informationen sicherzustellen, die zur Löschung vorgesehen sind, müssen diese so vernichtet oder gelöscht werden, dass eine Rekonstruktion mit hoher Wahrscheinlichkeit ausgeschlossen werden kann. Die Außerbetriebnahme oder Wiederverwendung von IT-Systemen oder Datenträgern sowie der Umgang mit den darauf gespeicherten Daten muss im Vorfeld geklärt werden. Dabei ist insbesondere dem Verlust wichtiger (noch benötigter) Daten/Informationen sowie dem Verbleib von unerwünschten Datenrückständen vorzubeugen.
Fragen zu 1	Gibt es mindestens einen Verantwortlichen, der bei der Aussonderung oder Wiederverwendung von IT-Systemen und Speichermedien sicherstellt, dass keine wichtigen Daten verloren gehen und sensitive Daten nicht rekonstruierbar sind?
Fragen zu 2	Existiert eine einheitliche, dokumentierte Vorgehensweise (je nach Art des Speichermediums und je nach Schutzbedarf) zum sicheren Löschen von IT-Systemen und Datenträgern (inklusive Datensicherungen / Archiven) sowie zur Aussonderung von Geräten (Hardware, Peripherie, Datenträger), die zudem sicherstellt, dass keine wichtigen Daten verloren gehen? Werden bei der Löschung und Vernichtung die aktuell geltenden Standards eingehalten? Wird diese Vorgehensweise von den entsprechenden Verantwortlichen eingehalten / befolgt?
Fragen zu 3	Sind die Vorgaben zur Löschung, Außerbetriebnahme und Aussonderung (inklusive Entsorgung oder Rückgabe) von IT-Systemen und Speichermedien sowie für die dabei zu erstellenden und einzuholenden Dokumente vollständig in einem entsprechenden Konzept dokumentiert, umgesetzt und kommuniziert? Sind Vereinbarungen mit Dritten abgeschlossen worden, die den internen Regelungen entsprechen, sofern Betrieb und/oder Wartung an diese ausgelagert wurden?
Fragen zu 4	Wird die Einhaltung des Konzepts zur sicheren Datenlöschung und Aussonderung regelmäßig geprüft (z. B. anhand von regelmäßigen Kontrollen der Ergebnisse von Löschungsvorgängen)? Werden identifizierte Lücken geschlossen?
Fragen zu 5	Werden die Vorgaben (Konzepte) und Prozesse zur sicheren Datenlöschung und Aussonderung regelmäßig hinsichtlich ihrer Eignung bewertet und optimiert? Wird dabei insbesondere die aktuelle technische Entwicklung von Datenträgern beachtet?

B.b.14. IT-Sicherheitskonzepte: Schutz gegen Schadprogramme und netzbasierte Angriffe [2.1.19]

Domäne:	IT-Steuerung
Unterdomäne:	Definition von anforderungskonformen IT-Services und Lösungen
Indikator:	IT-Sicherheitskonzepte: Schutz gegen Schadprogramme und netzbasierte Angriffe
Kriterien:	Verfügbarkeit; Vertraulichkeit; Integrität
Kurz-beschreibung	Der Schutz gegen Schadprogramme (Malware) und netzbasierte Angriffe (z. B. Verteilte Denial-of-Service-Attacken (DDoS)) umfasst z. B. ein Virenschutzkonzept, Intrusion Detection Systeme, ein DDoS-Mitigation-Konzept, die Einschränkung von Benutzerberechtigungen, die Prüfung auf neue sowie noch offene Schwachstellen, die Sensibilisierung der Mitarbeiter hinsichtlich Schadprogramme.
Fragen zu 1	Werden Maßnahmen gegen Schadprogramme auf den Systemen getroffen (z. B. Installation einer Antivirensoftware) und gibt es hierfür einen Verantwortlichen?
Fragen zu 2	Sind die Maßnahmen, Verpflichtungen und Meldewege (sowohl beim Auftraggeber / Kunden, als auch beim IT-Dienstleister) für den Fall, dass ein Schadprogramm-Befall oder ein netzbasierter Angriff auf die IT-Systeme erfolgt, definiert, beschrieben und umgesetzt?
Fragen zu 3	Sind die Sicherheitskonzepte zum Schutz gegen Schadprogramme vollständig dokumentiert? Erfüllen diese die Anforderungen bewährter Standards und werden die Vorgaben innerhalb der Organisation kommuniziert? Sind Verfahren, die eine Wiederherstellung der IT-Systeme nach einem Befall durch ein Schadprogramm oder einem erfolgreichen Angriff auf die IT-Systeme ermöglichen, vollständig implementiert und kommuniziert?
Fragen zu 4	Werden die Sicherheitskonzepte zum Schutz gegen Schadprogramme und netzbasierte Angriffe regelmäßig und anlassbezogen auf ihre Einhaltung geprüft (z. B. anhand von relevanten Daten aus dem Bereich Logging und Monitoring oder auf Basis von aufgetretenen Sicherheitsvorfällen)? Werden identifizierte Lücken geschlossen, z. B. indem Maßnahmen umgesetzt werden?
Fragen zu 5	Erfolgt eine Weiterentwicklung und Optimierung der übergeordneten Prozesse und Vorgaben zum Schutz vor Schadprogrammen und netzbasierten Angriffen aufgrund vorangegangener Prüfungsergebnisse? Wird insbesondere das Sicherheitskonzept zum Schutz gegen Schadprogramme und netzbasierte Angriffe regelmäßig angepasst und verbessert?

B.b.15. Incident Management (Störungsmanagement): Sicherheitsvorfallbehandlung [2.3.7]

Domäne:	IT-Steuerung
Unterdomäne:	Abwicklung der täglichen Aufgaben im IT-Betrieb
Indikator:	Incident Management (Störungsmanagement): Sicherheitsvorfallbehandlung
Kriterien:	Verfügbarkeit; Vertraulichkeit; Integrität
Kurz-beschreibung	Die Sicherheitsvorfallbehandlung beschreibt die Vorgehensweise / den Prozess zur Behandlung von Sicherheitsvorfällen (angefangen von der Vorbereitung über die Durchführung bis hin zur Nachbereitung). Sicherheitsvorfälle sind Vorfälle, welche die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen, Geschäftsprozessen, IT-Diensten, IT-Systemen oder IT-Anwendungen derart beeinträchtigen, dass ein relevanter Schaden entstehen kann. Ziel der Sicherheitsvorfallbehandlung ist es, Sicherheitsvorfälle frühzeitig zu erkennen und diese möglichst schnell (oder bereits im Vorfeld) zu analysieren und entsprechende Ursachen, die zu diesen Vorfällen führten, zu beheben bzw. zu vermeiden, um Schäden zu minimieren. Die Sicherheitsvorfallbehandlung unterstützt das übergeordnete Notfallmanagement/BCM und ergänzt das IT-Service Continuity Management.
Fragen zu 1	Werden Sicherheitsvorfälle, z. B. in den Bereichen IT oder der physischen Infrastruktur, erfasst und dokumentiert? Ist ein Sicherheitsvorfall eindeutig definiert und gegenüber anderen Ereignissen sorgfältig abgegrenzt? Wird den erfassten und dokumentierten Sicherheitsvorfällen in geeigneter Weise nachgegangen?
Fragen zu 2	Wird eine adäquate Handlungsfähigkeit sichergestellt, damit bei einem Sicherheitsvorfall die notwendigen Maßnahmen kurzfristig ergriffen werden können und ist die Erfassung, die Behandlung sowie die Nachbereitung von Sicherheitsvorfällen innerhalb eines dokumentierten Prozesses definiert? Erfolgen Schulungen zur Behandlung von Sicherheitsvorfällen?
Fragen zu 3	Schließt der Prozess die Identifizierung, zeitnahe Eskalation und Reaktion sowie die vollständige Dokumentation von Sicherheitsvorfällen aller Bereiche mit ein? Ist er allen an der Sicherheitsvorfallbehandlung beteiligten Personen bekannt, vollständig dokumentiert und vollständig umgesetzt? Erfolgt eine zentrale Auswertung der Sicherheitsvorfälle?
Fragen zu 4	Umfasst der Prozess der Sicherheitsvorfallbehandlung Abläufe (z. B. Kommunikations-, Alarmierungs- und Eskalationswege) und Regeln für die verschiedenen Arten von Sicherheitsvorfällen und werden diese regelmäßig inkl. der Beteiligung der verschiedenen Bereiche sowie der Organisationsleitung überprüft – auch durch Übungen? Wird die Einhaltung der Vorgaben für den Prozess regelmäßig geprüft und werden Diskrepanzen beseitigt?
Fragen zu 5	Werden aufgedeckte Sicherheitslücken zur (bereichsübergreifenden) Optimierung der Sicherheit genutzt? Werden regelmäßige und anlassabhängige Überprüfungen (unter Berücksichtigung der Ergebnisse gemäß 4) durchgeführt, um die Prozesse zur Sicherheitsvorfallbehandlung zu verbessern?

B.b.16. Patch- und Releasemanagement (Software) [2.4.4]

Domäne:	IT-Steuerung
Unterdomäne:	Steuerung von Veränderungen der IT
Indikator:	Patch- und Release-Management (Software)
Kriterien:	Verfügbarkeit; Vertraulichkeit; Integrität; Transparenz; Wartbarkeit
Kurz-beschreibung	Zu den Aufgaben des Patch- und Release-Managements zählen der Abnahme- und Freigabeprozess bei Patches, Updates und Releases mit dem Ziel, deren Verträglichkeit sicherzustellen, sowie das Einspielen der Patches, Updates und Releases. Zu beachten ist, dass Sicherheitspatches so schnell wie möglich einzuspielen sind. Anhand der Informationen aus dem Patch- und Release-Management wird ersichtlich, welche Patches noch fehlen und welchen Risiken der IT-Betrieb dadurch ausgesetzt ist. Ziel des Patch- und Release-Managements ist es, die o. g. Änderungen der Software steuer- und kontrollierbar zu gestalten, damit Störungen im Betrieb vermieden und insbesondere Sicherheitslücken minimiert und zeitnah beseitigt werden können. Ein fehlendes oder vernachlässigtes Patch- oder Release-Management führt schnell zu Lücken in der Sicherheit der einzelnen Software-Komponenten und damit zu möglichen Angriffspunkten.
Fragen zu 1	Werden alle Patches, Updates und Releases von mindestens einem Verantwortlichen entsprechend der Sicherheitsvorgaben identifiziert, gesteuert und kontrolliert?
Fragen zu 2	Werden Patches oder Updates mit hoher Priorität (Notfall-Changes, z. B. sicherheitsrelevante Patches, die eine kritische Sicherheitslücke schließen) vorrangig bearbeitet? Ist dies im Prozess eindeutig definiert und wird dies dokumentiert?
Fragen zu 3	Wird die Funktionalität der Systeme nach dem Einspielen eines Patches, Updates oder Releases durch Tests mit typischen (fachlichen) Anwendungsszenarien ermittelt und werden eventuelle Fehlfunktionen beseitigt (oder in einem wohldefinierten Prozess über das weitere Vorgehen entschieden [Risikomanagement, Entscheidung über Notfall-Patch]), bevor das Ausrollen im Produktivsystem erfolgt? Sind die Vorgaben für solche Tests vollständig dokumentiert und kommuniziert? Werden die Ergebnisse der Tests vollständig dokumentiert?
Fragen zu 4	Wird regelmäßig überwacht, dass das Einspielen von Patches, Updates und Releases nur nach vorherigen Tests erfolgt? Werden die in Stufe 3 genannten Verfahren eingehalten?
Fragen zu 5	Erfolgt anhand der Ergebnisse von Reviews und Auswertungen eine Weiterentwicklung und Optimierung des Patch- und Release-Managements?

B.b.17. Trennung von Entwicklungs-, Test- und Produktionsumgebungen [2.4.5]

Domäne:	IT-Steuerung
Unterdomäne:	Steuerung von Veränderungen der IT
Indikator:	Trennung von Entwicklungs-, Test- und Produktionsumgebungen
Kriterien:	Verfügbarkeit; Vertraulichkeit; Integrität; Transparenz; Wartbarkeit
Kurz-beschreibung	Um eine angemessene Betriebsstabilität sicherzustellen, werden separate Server-Umgebungen für die verschiedenen Einsatzzwecke Entwicklung, Test und Produktion eingesetzt. Ziel der Trennung der Entwicklungs-, Test- und Produktionsumgebungen ist es sicherzustellen, dass während der Entwicklungs- und Testphase keine Schäden oder Sicherheitsrisiken für den produktiven Betrieb entstehen, indem Softwareentwickler und Tester keinen Zugriff auf die Produktionsumgebung haben. Die Trennung gilt insbesondere für die Verarbeitung von Testdaten und Echtdaten sowie für die Berechtigungsvergabe, so dass ein unautorisiertes und unkontrolliertes Modifizieren von bspw. Konfigurationen oder Daten in der Produktionsumgebung ausgeschlossen ist. Die Entwicklungsumgebung, die vor allem von Softwareentwicklern genutzt und gepflegt wird, ist strikt von der Produktionsumgebung zu trennen. Die ebenfalls getrennte Testumgebung ist bezüglich der Hard- und Software "funktional äquivalent" zur Produktionsumgebung und dient dazu, dass Installationen, Konfigurationsänderungen, Updates und Patches vor dem Einspielen auf dem Produktionssystem einem Vorab-Test unterzogen werden. Für die Testumgebung werden hauptsächlich selbst erstellte Testprozeduren und anonymisierte Daten aus der Produktionsumgebung genutzt.
Fragen zu 1	Werden separate (vom Produktionsbetrieb – mindestens virtuell – getrennte) Systeme für Tests von Patches, Updates, Releases, Konfigurationsänderungen etc. einerseits und die Entwicklung andererseits eingesetzt?
Fragen zu 2	Sind die Testumgebungen funktional äquivalent zu den Produktivumgebungen aufgebaut? Sind die Test- und Entwicklungsumgebungen bezüglich der Datenverarbeitung und Berechtigungsvergabe strikt von den Produktivumgebungen getrennt? Existieren dokumentierte Vorgaben, wie derartige Trennungen zwischen allen Umgebungen zu gewährleisten sind?
Fragen zu 3	Sind die Vorgaben gemäß 2 vollständig dokumentiert? Gibt es vollständig dokumentierte Regelungen für den Transfer von Software oder Konfigurationen zwischen den Umgebungen für Entwicklung, Test und Produktion sowie Vorgaben hinsichtlich der Anonymisierung von Testdaten? Sind alle diese Vorgaben und Regelungen in der Institution kommuniziert und umgesetzt?
Fragen zu 4	Wird regelmäßig geprüft, ob die Trennung von Entwicklungs-, Test- und Produktionsumgebungen und die damit verbundenen Regelungen (z. B. Berechtigungen) den Vorgaben entsprechen, und werden erkannte Diskrepanzen beseitigt?
Fragen zu 5	Werden die Entwicklungs-, Test- und Produktionsumgebungen sowie die Regelungen und Verfahren zur Trennung der verschiedenen IT-Umgebungen kontinuierlich verbessert, insbesondere unter Nutzung der Prüfergebnisse gemäß 4?

B.b.18. Ausfallsicherheit / Redundanzkonzept [3.1.1]

Domäne:	Technische Umsetzung
Unterdomäne:	Grundlegende Redundanz
Indikator:	Ausfallsicherheit / Redundanzkonzept
Kriterien:	Verfügbarkeit
Kurz-beschreibung	Für die Erbringung verlässlicher IT-Services sind mindestens zuverlässige Komponenten zu verwenden und angemessene Redundanzkonzepte zu erarbeiten. Für höhere Verfügbarkeiten sollten diese Konzepte Failover-Mechanismen vorsehen, die z. B. einen kompletten Ausfall eines Standorts vollständig und transparent kompensieren. Diese Konzepte sind entsprechend umzusetzen, um die angestrebte Verfügbarkeit zu gewährleisten.
Fragen zu 1	Befinden sich die für die Erbringung der IT-Services erforderlichen Infrastrukturen, IT- und Kern-Netzwerkkomponenten, an einem Standort in mindestens einem eigenen räumlich getrennten Bereich? (Sind diese beispielsweise räumlich getrennt von normalen Büroflächen?) Werden für die Erbringung der IT-Services ausschließlich solche Hardware- und Infrastrukturkomponenten verwendet, die für den Betrieb in Rechenzentren und Serverräumen ausgelegt sind?
Fragen zu 2	Gibt es für kritische Komponenten redundante Ausweichsysteme, die sich in einem anderen räumlich getrennten Bereich befinden? Stellen beide räumlichen Bereiche mindestens anforderungskonformen Schutz bereit? Hinweis: Kritische Komponenten sind solche, die für die Erbringung der Kernfunktionalität relevant sind.
Fragen zu 3	Sind die für die Erbringung der IT-Services erforderlichen Infrastrukturen, IT- und Netzwerkkomponenten vollständig redundant aufgebaut und – der Redundanz entsprechend – auf unterschiedliche räumlich getrennte Bereiche verteilt, die die Qualität von Brandabschnitten aufweisen und die hinsichtlich der übrigen Schutzmerkmale anforderungskonform mindestens gleichwertig sind? Findet ein Failover zwischen den redundanten Systemen ohne nennenswerte Verzögerungen oder sonstige Auswirkungen für den Nutzer statt?
Fragen zu 4	Sind sowohl die IT-Services als auch die für die Erbringung der IT-Services erforderlichen Infrastrukturen, IT- und Netzwerkkomponenten redundant in räumlich getrennten Standorten verteilt (Georedundanz) und findet bei Ausfall eines Standorts ein Failover zwischen den Standorten ohne nennenswerte Verzögerungen oder sonstige Auswirkungen für den Nutzer statt?
Fragen zu 5	Besteht hinsichtlich der Standorte Wartungsredundanz, d. h. gibt es mindestens drei Standorte, so dass bei Abschaltung eines Standorts zu Wartungszwecken und gleichzeitigem Ausfall eines weiteren Standorts die IT-Services in vollem Umfang durch den dritten Standort erbracht werden?

B.b.19. Netzwerk-Segmentierung [3.2.2]

Domäne:	Technische Umsetzung
Unterdomäne:	Netzwerk
Indikator:	Netzwerk-Segmentierung
Kriterien:	Verfügbarkeit; Vertraulichkeit; Integrität
Kurz-beschreibung	Eine wesentliche Maßnahme zur Steigerung der Sicherheit des Netzwerks im RZ ist die Segmentierung. Eine geeignete logische oder auch physikalische Segmentierung sorgt zum einen für einen störungsloseren Betrieb. Sie dient aber auch dazu, die Netzwerksegmente durch jeweils geeignete Netzübergänge vor nicht autorisierten oder nicht notwendigen Zugriffen zu schützen. Der Netzwerkverkehr zwischen den Segmenten sollte so gesteuert und kontrolliert werden, dass der Zugriff nur von Zonen mit höherem Schutzbedarf auf Zonen gleichen oder niedrigeren Schutzbedarfs möglich ist. Der Verkehr zwischen Segmenten, welcher über Wege geht, die nicht im Einflussbereich des Betreibers liegen, muss angemessen verschlüsselt werden.
Fragen zu 1	Ist das Netzwerk in verschiedene Segmente unterteilt, die dem Schutzbedarf der Komponenten des Segments entsprechen (bspw. Office-Netz, DMZ) und werden Daten, die durch Netze außerhalb der eigenen Liegenschaften transportiert werden, geeignet verschlüsselt?
Fragen zu 2	Sind Netz-Segmente mit Verbindungen in öffentliche Netze durch Sicherheitskomponenten (dem Schutzbedarf entsprechend, mindestens durch Paketfilter) von rein intern genutzten Segmenten getrennt?
Fragen zu 3	Ist zwischen den internen Netzsegmenten ein Sicherheits-Gateway (z. B. Firewall) im Einsatz, das den Zugriff so kontrolliert, dass nur Kommunikationsbeziehungen gemäß den IT-Sicherheitskonzepten zugelassen werden? Werden die entsprechenden Protokollierungsdaten anlassbezogen und regelmäßig ausgewertet?
Fragen zu 4	Sind auch die Netze an den georedundanten Standorten entsprechend Frage 3 segmentiert und ist die Kommunikation zwischen diesen Standort-Segmenten geeignet verschlüsselt?
Fragen zu 5	Können jeweils einzelne Segmente zu Wartungsarbeiten deaktiviert werden, ohne dass der Ausfall einer weiteren Komponente zum Dienstausfall führt (Wartungsredundanz)?

B.b.20. Sicherheit der aktiven Netzwerkkomponenten [3.2.3]

Domäne:	Technische Umsetzung
Unterdomäne:	Netzwerk
Indikator:	Sicherheit der aktiven Netzwerkkomponenten
Kriterien:	Verfügbarkeit; Vertraulichkeit; Integrität
Kurz-beschreibung	Der unberechtigte Zugang zu und Zugriff (auch virtuell) auf aktive Netzwerkkomponenten im RZ (Router, Switche etc.) kann weitgehende Gefährdungen mit sich bringen. Daher müssen diese Komponenten mit geeigneten Sicherheitsmaßnahmen u. a. vor unerlaubten Zugriffen und Manipulationen geschützt werden. Eine Überwachung des Netzwerks auf Vorfälle unterstützt diesen Prozess
Fragen zu 1	Ist ein Härtungskonzept für Netzwerkkomponenten vorhanden und umgesetzt, sind die Netzwerkkomponenten vor unbefugtem Zugang gesichert (bspw. durch verschlossene Räume oder Schutzschränke) und sind elementare Sicherheitsmaßnahmen nach IT-Grundschutz umgesetzt (Standard-Passwort geändert, sichere Protokolle zur Administration, Backup der Konfiguration, Updates der Images, aktueller Patchlevel etc.)?
Fragen zu 2	Wird das Management der Netzwerkkomponenten in einem dedizierten Management-Netz durchgeführt und findet eine ständige Überwachung der sicherheitsrelevanten Meldungen der Geräte (Monitoring) mit entsprechender Reaktion statt?
Fragen zu 3	Erfolgt eine regelmäßige Überprüfung der Einhaltung der Sicherheitsmaßnahmen und erfolgt eine zeitnahe Beseitigung der gefundenen Schwachstellen? Geschieht das Management „Out of Band“, d. h. über ein eigenes, physikalisch getrenntes Netzwerk?
Fragen zu 4	Sind alle Sicherheitsmaßnahmen an allen Standorten umgesetzt und werden Ausfälle und Fehlermeldungen zentral zusammengeführt und ausgewertet (Soll-Ist-Abgleich)?
Fragen zu 5	Dient die Auswertung der Fehlermeldungen und Ereignisse („events“) nicht nur dazu, die unmittelbaren Fehler zu beheben, sondern auch dazu, die Sicherheitsmaßnahmen stetig zu überarbeiten?

B.b.21. Ausgestaltung der WAN-Anbindung zwischen den IT-Standorten [3.2.6]

Domäne:	Technische Umsetzung
Unterdomäne:	Netzwerk
Indikator:	Ausgestaltung der WAN-Anbindung zwischen den IT-Standorten
Kriterien:	Verfügbarkeit; Vertraulichkeit
Kurz-beschreibung	Zur Datenkommunikation zwischen IT-Standorten (RZ-RZ-Kopplungen) sind WAN-Verbindungen erforderlich. Bei gemieteten Leitungen müssen angemessene Service-Level-Vereinbarungen (SLA) festgeschrieben werden. Für eine verlässliche Datenkommunikation sollten die Verbindungen redundant gestaltet und idealerweise mit Failover-Mechanismen versehen werden, die Ausfälle von Verbindungen vollständig und vom Nutzer unbemerkt kompensieren. Für eine vertrauliche Kommunikation ist die Verbindung zu verschlüsseln. Falls keine WAN-Verbindungen erforderlich sind (z. B. weil nur ein Standort vorhanden ist), muss der Indikator nicht berücksichtigt werden.
Fragen zu 1	Sind vorhandene WAN-Anbindungen durch Verschlüsselung abgesichert (mindestens Software-Verschlüsselung) und entsprechen die Service-Level-Vereinbarungen (SLA) den Anforderungen?
Fragen zu 2	Werden vorhandene WAN-Anbindungen durch ein Monitoring auf Ausfall oder Störung überwacht und wird im Bedarfsfall entsprechend reagiert?
Fragen zu 3	Wird bei Ausfall einer Verbindung eine vorhandene redundante Verbindung automatisch genutzt? Gibt es zwei räumlich getrennte Hauseinführungen, die zu jeweils getrennten Verteilern des/der Dienstleister führen?
Fragen zu 4	Verfügen die redundanten Verbindungen über eine gleichwertige Kapazität (bspw. 2 x 1GBit/s)?
Fragen zu 5	Sind die WAN-Verbindungen redundant ausgelegt, so dass eine Wartung an einer WAN-Verbindung im laufenden Betrieb stattfinden kann, ohne dass der Ausfall einer weiteren Verbindung zum Dienstausfall führt (Wartungsredundanz)?

B.b.22. Sicherheit der Internet-Anbindung [3.2.8]

Domäne:	Technische Umsetzung
Unterdomäne:	Netzwerk
Indikator:	Sicherheit der Internet-Anbindung
Kriterien:	Verfügbarkeit; Vertraulichkeit; Integrität
Kurz-beschreibung	Eine Internet-Anbindung ist mit Risiken verbunden: Unautorisierter Zugriff und ungewünschter Abfluss von Daten muss genauso vermieden werden wie die Einschleusung von Schadsoftware (Malware) oder die Manipulation von Daten. Durch Sicherheitsmaßnahmen, wie bspw. den Einsatz von Sicherheits-Gateways (Elemente zur Netztrennung, oft auch als „Firewall“ bezeichnet), wird die Anbindung an das Internet abgesichert. Auch diese Architektur muss gegen Ausfall gesichert werden.
Fragen zu 1	Wird der Zugriff auf das Netzwerk aus fremden Netzen (Partner, Internet) durch ein Sicherheits-Gateway kontrolliert und protokolliert und wird sichergestellt, dass kein ungewollter Verbindungsaufbau von außen stattfindet?
Fragen zu 2	Ist die Sicherheits-Gateway-Architektur mehrstufig und werden die übertragenen Inhalte auf Schadsoftware kontrolliert? Kontrolliert das Sicherheits-Gateway auf Applikationsebene (soweit möglich, z. B. Mail, HTTP, FTP u. a.) die übertragenen Inhalte auch auf Protokollkonformität?
Fragen zu 3	Sind die Komponenten des Sicherheits-Gateways vollständig redundant ausgelegt (z. B. Paketfilter, Application Level Gateway, Intrusion Detection System)?
Fragen zu 4	Werden an den georedundanten Standorten mit eigener Internet-Anbindung die gleichen Sicherheitsmaßnahmen auf dem gleichen Sicherheitsniveau umgesetzt?
Fragen zu 5	Ist eine Wartung jeweils eines Teils des Sicherheits-Gateway-Clusters jederzeit möglich, ohne dass ein Ausfall einer weiteren Sicherheitskomponente zum Ausfall der Internet-Anbindung führt (Wartungsredundanz)?

B.b.23. Server-Sicherheit [3.3.1]

Domäne:	Technische Umsetzung
Unterdomäne:	Server
Indikator:	Server-Sicherheit
Kriterien:	Verfügbarkeit; Vertraulichkeit; Integrität
Kurz-beschreibung	Zum sicheren Betrieb eines Servers tragen Sicherheitsmaßnahmen, insbesondere die Systemhärtung, bei. Die Härtung eines Servers erschwert einem Angreifer den Zugriff und sorgt zudem für einen störungsfreieren Betrieb, indem bspw. überflüssige Dienste/Services deaktiviert werden. Einen Anhalt für solche Maßnahmen geben die entsprechenden IT-Grundschutzbausteine oder andere „best practices“. Die Serverhärtung muss immer wieder mit den aktuellen Bedrohungen abgeglichen werden; dies beinhaltet insbesondere das zeitnahe Einspielen von Sicherheitspatches.
Fragen zu 1	Sind für alle Server Härtungskonzepte vorhanden (z. B. Sicherheitsmaßnahmen nach IT-Grundschutz) und umgesetzt? Werden aktuelle Sicherheitsupdates zeitnah installiert und ist ein stets aktueller Malwareschutz aktiv?
Fragen zu 2	Sind zusätzlich auch weitergehende Maßnahmen umgesetzt, die für die Härtung der Systeme sinnvoll sind (z. B. die Z-Maßnahmen nach IT-Grundschutz) und werden diese durchgängig umgesetzt?
Fragen zu 3	Ist die Härtung der Systeme vollständig dokumentiert und gibt es Prozesse, die einen aktuellen Stand der Härtung sicherstellen?
Fragen zu 4	Wird durch interne und externe Reviews oder Penetrationstests regelmäßig geprüft, ob die Sicherheit der Server-Systeme dem angestrebten Ziel und den Vorgaben entspricht und werden bei Abweichungen entsprechende Maßnahmen ergriffen?
Fragen zu 5	Werden die Härtungskonzepte regelmäßig überprüft? Fließen auch die Ergebnisse der Reviews und Pentests in den weiteren Härtungsprozess mit ein, so dass die Härtungsverfahren und -konzepte systematisch verbessert werden?

B.b.24. Datensicherheit der Speicher [3.4.2]

Domäne:	Technische Umsetzung
Unterdomäne:	Speichertechniken
Indikator:	Datensicherheit der Speicher
Kriterien:	Vertraulichkeit; Integrität
Kurz-beschreibung	Daten, die auf einem Speichersystem gelagert werden, können verschiedene Schutzbedarfe haben. Für die Sicherheit der Daten werden unterschiedliche Maßnahmen, wie bspw. Verschlüsselung eingesetzt. Besonders ist dies bei mehreren Mandanten auf den Speichersystemen zu beachten. Als Basis hierfür muss ein geeignetes, abgestuftes Datensicherheitskonzept für die Speichersysteme existieren.
Fragen zu 1	Sind die Speichersysteme gemäß den IT-Grundschutzkatalogen eingerichtet (z. B. eine verschlüsselte Datenablage gemäß Schutzbedarf)?
Fragen zu 2	Sind Zonen und Masken (sofern erforderlich) gemäß den Schutzzonen der Anwendungen und Daten umgesetzt und erfolgt die Administration nur aus separaten Netzen?
Fragen zu 3	Werden die Systemmeldungen der Speichersysteme automatisiert auf Verletzungen der Datensicherheit überprüft? Sind für Zonen mit besonderem Schutzbedarf dedizierte Speichernetze eingerichtet?
Fragen zu 4	Erfolgt zwischen georedundanten Standorten eine automatische Datensynchronisation und werden dabei Sicherheitsmaßnahmen gegen mögliche Verluste der Vertraulichkeit und der Integrität getroffen? Ist das Datensicherheitskonzept an allen Standorten gleichermaßen umgesetzt?
Fragen zu 5	Wird die korrekte Umsetzung des Datensicherheitskonzepts für die Speichersysteme regelmäßig durch Reviews und technische Tests überprüft und werden erkannte Schwachstellen eliminiert?

B.b.25. Datenreplikation und -sicherung [3.4.3]

Domäne:	Technische Umsetzung
Unterdomäne:	Speichertechniken
Indikator:	Datenreplikation und -sicherung
Kriterien:	Verfügbarkeit
Kurz-beschreibung	Zur Steigerung der Verfügbarkeit werden Replikationsmechanismen eingesetzt. Replikation sorgt für eine Redundanz der Daten und somit für eine größere Ausfallsicherheit, indem die Daten zwischen den verschiedenen, redundant aufgebauten Datenträgern oder Datenbanken stets konsistent gehalten werden. Bei Ausfall des (Haupt-)Datenträgers wird auf einen Datenenträger mit einer Replik umgeschaltet. Replikationen unterliegen häufigen Änderungen. Sie schützen zwar vor technischen Fehlern wie z. B. einem Datenträgerausfall, aber nicht vor Datenverlusten aufgrund von Löschvorgängen, Manipulationen, Schadprogrammen oder anderen Ereignissen. Daher ist neben der Replikation auch eine Sicherung der Daten (Backup) erforderlich. Diese liefert Offline-Kopien, die einen definierten Zustand für längere Zeit unveränderlich aufbewahren und die es dem Informationseigner ermöglichen, auf Wunsch einen vorherigen Zustand wiederherzustellen..
Fragen zu 1	Sind die Daten identifiziert, die über Replikationsmechanismen und/oder Backup geschützt werden müssen, und sind diese Maßnahmen jeweils umgesetzt? Wurde anhand von Funktionstests nachgewiesen, ob bei einem Ausfall des (Haupt-)Datenträgers auf den redundanten Datenträger umgeschaltet werden kann? Wurde das Wiedereinspielen der Daten aus dem Backup (Restore) getestet?
Fragen zu 2	Ist (im Rahmen der mit dem Kunden getroffenen Vereinbarungen) eine Wiederherstellung von Daten auf Wunsch der Informationseigner möglich, im abgestimmten Zeitrahmen durchführbar und wurde dies getestet? Werden die (gemäß Frage 1) für die Replikation identifizierten Daten mindestens zwischen zwei Brandabschnitten repliziert?
Fragen zu 3	Werden Datensicherungen an externe Orte, die ein gleichwertiges Sicherheitsniveau haben, ausgelagert?
Fragen zu 4	Werden die Daten gemäß Frage 1-3 zwischen mindestens zwei georedundanten Standorten repliziert und werden diese Daten an beiden Standorten gesichert? Ist das gesamte Speichernetz georedundant ausgelegt?
Fragen zu 5	Ist sowohl die Replikation als auch die Sicherung so umgesetzt, dass bei Wartung eines Speichersystems auch der Ausfall des entsprechenden Ersatz-Speichersystems nicht zum Gesamtausfall der Speicherung führt (Wartungsredundanz)?

B.b.26. sEnergieversorgung: Unterbrechungsfreie Stromversorgung [3.5.1]

Domäne:	Technische Umsetzung
Unterdomäne:	Infrastruktur / Gebäude
Indikator:	Energieversorgung: Unterbrechungsfreie Stromversorgung
Kriterien:	Verfügbarkeit
Kurz-beschreibung	Eine unterbrechungsfreie Stromversorgung (USV) dient dem unterbrechungsfreien Betrieb der nachgeschalteten Anlagen und Systeme bei einem Netzausfall. Je nach Kategorie der USV filtert diese zudem Störungen, die aus dem Netz des Energieversorgers oder von der eigenen Netzersatzanlage (NEA) stammen. Für einen störungsfreien Betrieb von IT ist dafür eine USV der Kategorie VFI-SS-111 erforderlich, da nur diese in der Lage ist, vor den Schadeinwirkungen von Spannungseinbrüchen, Spannungsspitzen, Überspannungen, Blitzschlägen, Spannungsstößen, Frequenzschwankungen, Spannungsverzerrungen und Spannungsoberschwingungen zu schützen.
Fragen zu 1	Werden die kritischen Komponenten im Rechenzentrum mindestens durch lokale USV-Anlagen versorgt? Hinweis: Kritische Komponenten sind mindestens solche, die bei einem ungepufferten Stromausfall einen Schaden (inkl. Datenverlust) erleiden können.
Fragen zu 2	Wird das Rechenzentrum durch mindestens eine zentrale USV-Anlage versorgt, welche die Einschaltlücke der NEA in ausreichender Qualität sicher überbrückt? („Einschaltlücke“ ist die Zeitspanne zwischen dem Ausfall der Energieversorgung und der Versorgungsübernahme durch die NEA.)
Fragen zu 3	Wird das Rechenzentrum komplett durch mindestens zwei sich gegenseitig Betriebsredundanz gebende zentrale USV-Anlagen der Kategorie VFI-SS-111 nach IEC 62040-3 versorgt und stellt deren jeweilige Kapazität das „zeitgerechte sichere Herunterfahren" bei einem Stromausfall und gleichzeitigem Ausfall der NEA sicher? („Betriebsredundanz“, auch „(N+1)-Redundanz“ genannt, bedeutet, dass bei Ausfall einer modularen Komponente der USV die verbleibenden Komponenten ausreichen, um die erforderliche elektrische Leistung bereitzustellen.)
Fragen zu 4	Wird mindestens eine USV-Anlage gemäß 3 an jedem georedundanten Standort eingesetzt? Hinweis: In diesem Fall kann auf die Betriebsredundanz an den einzelnen Standorten verzichtet werden, weil die Georedundanz die Betriebsredundanz des RZ-Verbundes gewährleistet.
Fragen zu 5	Ist es möglich unter alleinigem USV-Betrieb (Ausfall der Netz- und der NEA-Versorgung) die relevanten Systeme sicher herunterzufahren ohne dass die Systeme dabei einen temperaturbedingten Schaden erleiden.

B.b.27. Energieversorgung: Einsatz einer Netzersatzanlage (NEA) [3.5.2]

Domäne:	Technische Umsetzung
Unterdomäne:	Infrastruktur / Gebäude
Indikator:	Energieversorgung: Einsatz einer Netzersatzanlage (NEA)
Kriterien:	Verfügbarkeit
Kurz-beschreibung	Energiequellen, die im Falle einer Unterbrechung der Primärversorgung eine Ersatzstromversorgung zur Verfügung stellen, werden als Netzersatzanlagen (NEA) bezeichnet. Hierbei handelt es sich um autarke Systeme, welche die Stromversorgung übernehmen. Es sind hier ausdrücklich nicht nur Systeme auf Basis von Mineralölprodukten gemeint, sondern auch andere, wie z. B. Brennstoffzellentechnik.
Fragen zu 1	Ist eine ortsfeste Netzersatzanlage (oNEA) vorhanden oder kann eine mobile Netzersatzanlage (mNEA) für den Fall eines längeren Stromausfalls bereitgestellt werden (z. B. durch Energieversorger, Service-Dienstleister) und ist ein Anschlusspunkt für diese mNEA vorbereitet oder einfach herstellbar?
Fragen zu 2	Ist eine USV vorhanden, deren Überbrückungszeit (Autonomiezeit) bis zur Betriebsbereitschaft der NEA gemäß 1 ausreicht?
Fragen zu 3	Ist eine oNEA vorhanden, deren Generator mindestens der Ausführungsklasse G3 nach ISO 8528-5:2013-03 entspricht, die den zu erwartenden Betriebsansprüchen sicher genügt und deren Betriebsmittelvorrat für mindestens 24 h ausreicht?
Fragen zu 4	Ist an jedem von mindestens zwei georedundanten Standorten mindestens eine oNEA gemäß 3 vorhanden, deren Betriebsmittelvorrat für mindestens 72 h ausreicht?
Fragen zu 5	Ist an jedem von mindestens drei georedundanten Standorten eine oNEA gemäß 3 vorhanden? Reicht der Betriebsmittelvorrat an jedem der Standorte für mindestens 120 h aus und entsprechen die Generatoren der eingesetzten NEAs der Ausführungsklasse G4 nach ISO 8528-5:2013-03?

B.b.28. Technischer Brandschutz des Rechenzentrums [3.5.8]

Domäne:	Technische Umsetzung
Unterdomäne:	Infrastruktur / Gebäude
Indikator:	Technischer Brandschutz des Rechenzentrums
Kriterien:	Verfügbarkeit; Betriebssicherheit
Kurz-beschreibung	Der technische Brandschutz ergänzt den baulichen Brandschutz. Er umfasst die Gesamtheit aller Brandschutzmaßnahmen, die durch Nutzung spezieller Anlagen und technischer Mittel sowohl vorbeugend (Überwachung, Detektion) als auch abwehrend (automatische Löschung) wirken. Die Brandschutzmaßnahmen zum Schutz der IT gehen zum Teil über die Anforderungen aus den jeweiligen Bauordnungen hinaus.
Fragen zu 1	Wird das Rechenzentrum durch eine Brandmeldeanlage (BMA) mindestens mit lokaler Meldung überwacht und gibt es Möglichkeiten zur Brandbekämpfung eines Entstehungsbrandes z. B. durch Handfeuerlöscher?
Fragen zu 2	Wird das Rechenzentrum (inkl. Supportbereich für „grobe“ Technik) und dessen Umfeld durch eine auf die örtliche Feuerwehr aufgeschaltete BMA überwacht und besteht mindestens die Möglichkeit, die Stromversorgung im Brandfall gezielt per Hand abzuschalten?
Fragen zu 3	Wird das Rechenzentrum mit einer Brandfrüherkennungsanlage überwacht und durch eine Löschanlage geschützt? (Brandfrüherkennung bedeutet hier, dass ein Brand deutlich früher und deutlich lokalisierter erkannt wird als durch eine normale Raumüberwachung, z. B. durch Deckenmelder.)
Fragen zu 4	Wird das Rechenzentrum mit einer Brandfrühesterkennungsanlage überwacht und ist eine dedizierte, ausschließlich das RZ schützende Löschanlage (oder eine mindestens gleichwertige andere technische Einrichtung) vorhanden, die so ausgelegt ist, dass alle Bereiche (inkl. Supportbereiche) mindestens mit zwei Volllöschungen beaufschlagt werden können? (Brandfrühesterkennung bedeutet hier, dass die Brandfrüherkennung zusätzlich in der Lage ist, schon vor Erreichen der eigentlichen Meldeschwelle über mindestens eine - besser mehrere - Voralarmstufen schadensmindernde Reaktionen auszulösen, und dass diese Möglichkeit auch genutzt wird.)
Fragen zu 5	Werden zusätzlich auch die unmittelbaren Nachbarbereiche (vertikal und horizontal) des RZ mit einer Brandfrühesterkennungsanlage überwacht und werden diese Nachbarbereiche durch eine reaktive Löschanlage (oder eine mindestens gleichwertige andere technische Einrichtung) geschützt und wird in den Räumen der IT-Betriebsflächen des RZ der Sauerstoff-Anteil der Luft auf <= 17 Vol.-% gehalten?

B.b.29. Gebäudesicherheit: Schutz gegen Einbruch und Sabotage [3.5.10]

Domäne:	Technische Umsetzung
Unterdomäne:	Infrastruktur / Gebäude
Indikator:	Gebäudesicherheit: Schutz gegen Einbruch und Sabotage
Kriterien:	Verfügbarkeit; Vertraulichkeit; Integrität; Betriebssicherheit
Kurz-beschreibung	In einem Rechenzentrum werden vielfach schutzbedürftige Daten verarbeitet, die vor unberechtigtem Zugriff, Löschung und Manipulation zu schützen sind. Ein Teil der hierfür notwendigen Schutzmaßnahmen sind solche zum Schutz gegen Einbruch und Sabotage. Diese umfassen insbesondere bauliche Maßnahmen sowie solche zur personellen und technischen Gebäudeüberwachung, unterstützt z. B. durch Videotechnik.
Fragen zu 1	Sind bauliche Maßnahmen für den Einbruchschutz umgesetzt, bei denen alle raumbildenden Teile (Wände, Decken, Böden, Türen, Fenster) mindestens der Widerstandsklasse RC3 nach EN 1627:2011-09 genügen?
Fragen zu 2	Werden mindestens alle für den ordnungsgemäßen Betrieb des RZ erforderlichen Bereiche, also auch die Supportbereiche, regelmäßig durch Kontrollgänge bestreift? Ist die zeitnahe Reaktion auf alle sicherheitsrelevanten Meldungen (aus der IT und der Infrastruktur, siehe B.b.32) zu jeder Zeit, also auch während der Kontrollgänge, sichergestellt?
Fragen zu 3	Genügen alle raumbildenden Teile der Widerstandsklasse RC4 nach EN 1627:2011-09 und ist eine Einbruchmeldeanlage (EMA) installiert, deren Meldungen rund um die Uhr an qualifiziertes Personal weitergebeben werden, um eine Alarmverfolgung sicherzustellen? (Die Meldung der EMA muss im Moment des Angriffsbeginns erfolgen und nicht erst nach Überwindung des mechanischen Widerstands.)
Fragen zu 4	Erfolgt eine auf die Erkennung von Einbruchsversuchen ausgerichtete Videoüberwachung der RZ-Hülle sowie der Supportbereich innerhalb und außerhalb des Gebäudes mit sofortiger automatischer Ereignismeldung an qualifiziertes Personal, das rund um die Uhr eine durchsetzungsfähige Reaktion sicherstellt? Hinweis: Durchsetzungsfähige Reaktion bedeutet hier, dass hinreichend ausgerüstetes und ausgebildetes Sicherheitspersonal eingreift.
Fragen zu 5	Sind Maßnahmen für den Sabotageschutz entsprechend der Sicherheitskonzeption umgesetzt (z. B. Barrieren oder Hindernisse zur Distanzerzeugung, insbesondere zum Schutz vor Anschlägen sowie zum Schutz von Lüftungseingängen vor der Einbringung von schädlichen Materialien)?

B.b.30. Gebäudesicherheit: Technische / bauliche Maßnahmen zum Zutrittsschutz [3.5.11]

Domäne:	Technische Umsetzung
Unterdomäne:	Infrastruktur / Gebäude
Indikator:	Gebäudesicherheit: Technische / bauliche Maßnahmen zum Zutrittsschutz
Kriterien:	Verfügbarkeit; Vertraulichkeit; Integrität
Kurz-beschreibung	Ein Rechenzentrum hat aus zahlreichen Gründen besondere Anforderungen an den Schutz gegen unbefugten Zutritt. Organisatorische Anweisungen und Maßnahmen allein reichen nicht aus. Die Einhaltung der Regelungen muss durch weitere Maßnahmen unterstützt werden.
Fragen zu 1	Wird durch eine räumlich getrennte Unterbringung der Informationstechnik einerseits sowie der Supporttechnik (Klima, Stromversorgung inkl. USV und NEA, Löschanlage etc.) andererseits sichergestellt, dass auch hinsichtlich des Zutritts eine konsequente Trennung der „feinen“ von der „groben“ Technik erzwungen wird? Hinweis: Dies setzt insbesondere die räumliche Trennung von allen anderen Nutzungen (etwa von normalen Büroflächen) voraus. Ist der Zutritt zu den jeweiligen Bereichen organisatorisch und technisch in der Weise geregelt, dass im Nachgang ausreichend sicher festgestellt werden kann, wer einen Bereich wann betreten hat?
Fragen zu 2	Erfolgt die Legitimationsprüfung und Freigabe des Zutritts für alle Bereiche (siehe Frage 1) durch eine Zutrittskontrollanlage mit Protokollierung der Bewegungen und erfolgt bei wiederholten unberechtigten Zutrittsversuchen eine automatische Meldung oder Sperrung des verwendeten Zutrittsmediums?
Fragen zu 3	Kontrolliert die Zutrittskontrollanlage den Zu- und Austritt und erfolgt der Zutritt mittels einer Zwei-Faktor-Authentifizierung oder einer vergleichbaren oder besseren Lösung? (Zwei-Faktor-Authentifizierung bedeutet „Besitz und Wissen“, wobei hier der Besitz auch durch Biometrie erbracht werden kann. „Besitz und Besitz“ oder „Wissen und Wissen“ gilt nicht als Zwei-Faktor-Authentifizierung!)
Fragen zu 4	Erfolgt der Zutritt über eine Vereinzelungsanlage – mindestens für das Gesamt-RZ, in Abgrenzung zu Bereichen, die nicht zum RZ gehören?
Fragen zu 5	Wird mittels der technischen Einrichtungen der Zutrittskontrollanlage sichergestellt, dass der Zutritt zu einem geschützten Bereich nur durch das zeitlich unmittelbar zusammenhängende berechtigte Handeln von mindestens einer weiteren Person neben dem Zutrittsberechtigten möglich ist (technisch erzwungene Umsetzung des „Vier-Augen-Prinzips“)?

B.b.31. Sicherheit der Verzeichnisdienste [3.6.2]

Domäne:	Technische Umsetzung
Unterdomäne:	Verzeichnisdienste
Indikator:	Sicherheit der Verzeichnisdienste
Kriterien:	Vertraulichkeit; Integrität
Kurz-beschreibung	Die Verzeichnisdienste halten die Benutzerkennungen und die dazu gehörenden Geheimnisse wie Passwörter, Schlüssel oder Biometrie-Daten vor. Die Sicherheit der Anmeldedaten und der zugehörigen hinterlegten Rollen wirkt sich direkt auf die Sicherheit der zu nutzenden Anwendungen aus, da sich durch Veränderung oder Kenntnisnahme ein unbefugter Zugang zu Anwendungen und Daten erschleichen lässt.
Fragen zu 1	Ist die Kommunikation mit dem Verzeichnisdienst, die außerhalb der abgesicherten Bereiche des Rechenzentrums verläuft, verschlüsselt und wird durch Anwendung der entsprechenden Grundschutzbausteine sichergestellt, dass hinterlegte Geheimnisse vor unbefugtem Zugriff geschützt sind?
Fragen zu 2	Werden den Kennungen Rollen zugewiesen, über die die Rechte auf den IT-Systemen und Anwendungen geregelt sind?
Fragen zu 3	Meldet der Verzeichnisdienst fehlgeschlagene Anmeldeversuche an ein zentrales System zur Protokollierung und werden diese Protokolle regelmäßig ausgewertet? Ist die Dauer der Anmeldungen über den Verzeichnisdienst ausreichend limitiert?
Fragen zu 4	Werden die hinterlegten Kennungen und die ihnen zugewiesenen Rollen regelmäßig mit der Personalverwaltung abgeglichen und auf unnötige Rollenzuweisungen kontrolliert? Werden erkannte Defizite abgestellt?
Fragen zu 5	Werden die Kontrollen des Verzeichnisdienstes (beispielsweise von fehlgeschlagenen Anmeldungsversuchen) durch Personen außerhalb der regulären Verwaltung des Verzeichnisdienstes durchgeführt?

B.b.32. Monitoring der technischen Infrastruktur [3.7.1]

Domäne:	Technische Umsetzung
Unterdomäne:	Technische Überwachung / Monitoring
Indikator:	Monitoring der technischen Infrastruktur
Kriterien:	Verfügbarkeit; Leistungsfähigkeit
Kurz-beschreibung	Die Infrastrukturkomponenten sind die Basis eines IT-Betriebs. Zur Minimierung von Störungen sind diese zu überwachen (Monitoring), d. h. Betriebszustände und Parameter werden erfasst, übertragen, dargestellt und ausgewertet. Zur schnellen Reaktion bei Störungen / Ausfall dieser Infrastrukturkomponenten sind mit den Herstellern, den für die Installation zuständigen Firmen oder anderen Service-Unternehmen Serviceverträge zu vereinbaren (Störungsbeseitigung / Notdienst). Dies gilt insbesondere für die Stromversorgung, Klimaanlagen, Löschanlagen und Melder (Wasser, Brand, Rauch).
Fragen zu 1	Wird die Funktion der Infrastrukturkomponenten (Stromversorgung, Klimaanlage, Wasser, etc.) überwacht und geschieht dies in einem regelmäßigen Modus, der eine Reaktion erlaubt, die den ermittelten Verfügbarkeitsanforderungen entspricht?
Fragen zu 2	Ist eine Störungsmeldung / -übertragung für die wesentlichen Infrastrukturkomponenten (z. B. Klima, Strom, Wasser) implementiert? Werden mindestens technisch sortierte Gruppenmeldungen zu einer 24/7-besetzten Interventionsstelle übertragen, die auf Basis vorgegebener Kriterien angemessen auf die Meldungen reagiert?
Fragen zu 3	Erfolgen die Meldungen für jeden Sensor individuell (also keine Gruppenmeldungen) und erfolgen die Meldungen in klar verständlichem Text mit ersten Handlungsanweisungen?
Fragen zu 4	Werden die Meldungen über einen gesicherten Weg übertragen, d. h. sind die Leitungen geschützt gegen versehentliche oder vorsätzliche Beschädigung durch einfache Mittel (z. B. einfache Werkzeuge wie Schraubendreher oder Seitenschneider)? Hinweis: Der Schutz gegen vorsätzliche Beschädigung kann innerhalb der RZ durch dessen Schutz als gegeben angenommen werden.
Fragen zu 5	Gibt es zusätzlich zum lokalen Monitoring an den georedundanten Standorten auch ein zentrales Monitoring, an dem die Meldungen aller Standorte auflaufen? Ist die Übertragung der Störungsmeldungen durch redundante, verschlüsselte Leitungen abgesichert?

B.b.33. Monitoring auf IT-Sicherheitsvorfälle, Logging [3.7.2]

Domäne:	Technische Umsetzung
Unterdomäne:	Technische Überwachung / Monitoring
Indikator:	Monitoring auf IT-Sicherheitsvorfälle / Logging
Kriterien:	Vertraulichkeit; Integrität
Kurz-beschreibung	Bei diesem Indikator geht es um die technische Überwachung von Vorfällen unter besonderer Berücksichtigung von IT-Sicherheitsvorfällen, die die Vertraulichkeit und Integrität der datenverarbeitenden Prozesse betreffen (z. B. mittels IDS (Intrusion Detection System) und/oder SIEM (Security Information and Event Management)). Die Überwachung der Verfügbarkeit wird durch den Indikator B.b.34 Monitoring der IT-Komponenten und -Dienste auf Verfügbarkeit abgedeckt.
Fragen zu 1	Speichern die IT-Systeme (inkl. Netzwerk- und Speicherkomponenten) die Meldungen/Log-Daten des Betriebssystems und der darauf laufenden Anwendungen für einen vom Sicherheitsmanagement festgelegten Zeitraum und ist dieser Zeitraum ausreichend, um Vorfälle angemessen aufzuklären?
Fragen zu 2	Melden die IT-Systeme sicherheitsrelevante Vorgänge an zentrale Systeme zur Speicherung und sind diese Systeme in die Datensicherung eingebunden? Gibt es Vorgaben zum Monitoring, in denen für alle als relevant identifizierten Verfahren Art und Umfang des Monitorings, Dauer der Log-Daten-Speicherung und die Auswertung geregelt sind?
Fragen zu 3	Werden die Meldungen der Systeme ständig und automatisch auf gängige potenzielle Sicherheitsvorfälle überwacht (d. h. es erfolgt eine automatische Auswertung der Log-Daten) und erfolgt eine automatische Meldung an das IT-Sicherheitsmanagement? Kommt ein IDS zum Einsatz? Sind die Vorgaben zum Monitoring vollständig umgesetzt?
Fragen zu 4	Werden die Systeme automatisch auf andere, d. h. außergewöhnliche Sicherheitsvorfälle überwacht (z. B. mittels SIEM)? Wird regelmäßig geprüft, ob die Log-Daten den Vorgaben entsprechend im erforderlichen Umfang erhoben und ausgewertet werden?
Fragen zu 5	Sind zusätzlich alle Standorte auch in ein zentrales Monitoring eingebunden und ist das zentrale Monitoring auch bei Wartung eines Standortes und gleichzeitigem Ausfall eines weiteren Standortes funktionsfähig? Werden die Vorgaben / Anforderungen an das Monitoring regelmäßig überprüft? Entsprechen sie dem jeweils aktuellen Stand?

B.b.34. Monitoring der IT-Komponenten und -Dienste auf Verfügbarkeit [3.7.3]

Domäne:	Technische Umsetzung
Unterdomäne:	Technische Überwachung
Indikator:	Monitoring der IT-Komponenten und -Dienste auf Verfügbarkeit
Kriterien:	Verfügbarkeit
Kurz-beschreibung	Die Überwachung der Verfügbarkeit aller IT-Komponenten spielt eine wichtige Rolle für den verlässlichen Betrieb der IT-Dienste. Die rechtzeitige Detektion von Abweichungen vom Soll-Zustand sowie eine schnelle und effektive Reaktion auf erkannte Abweichungen helfen, Ausfallzeiten zu minimieren. Dafür gibt es unterschiedliche sich ergänzende Lösungen, die teilweise auch weitere nützliche Informationen bereitstellen. Beispielsweise dient ein Netzwerkmonitoring auch der Überwachung des Netzes auf Änderungen des Gesamtsystems, wie z. B. das Einbringen neuer Komponenten in das Netzwerk.
Fragen zu 1	Existiert ein Monitoring zur Messung der Verfügbarkeit der kritischen IT-Komponenten und wird das Incident-, Security- oder Continuity Management über Abweichungen vom Soll informiert?
Fragen zu 2	Sind alle zentralen IT-Komponenten im Monitoring enthalten? Gibt es Vorgaben zum Monitoring, in denen für alle relevanten Verfahren Art und Umfang des Monitorings, Dauer der Log-Daten-Speicherung, die Auswertung der Daten und die Reaktion auf Abweichungen geregelt sind?
Fragen zu 3	Erfolgt ein Monitoring der IT-Dienste mit allen Aspekten, die für die ordnungsgemäße Funktion relevant sind, erfasst es deren Funktionalität inkl. Abhängigkeiten von anderen Diensten und erfolgt im Falle einer Störung eine automatische Information des Incident-, Security- oder Continuity Managements zur Behebung der Störung? Sind die Vorgaben zum Monitoring vollständig dokumentiert und umgesetzt?
Fragen zu 4	Sind für die georedundanten Standorte die Stufen 1 bis 3 erreicht? Werden bei signifikanten Abweichungen der gemessenen Werte vom Soll automatisch entsprechende Meldungen verschickt? Werden die Soll-Verfügbarkeitsanforderungen aktuell gehalten? Wird regelmäßig geprüft, ob das Monitoring der Systeme und Dienste den aktuellen Vorgaben entspricht und werden Defizite behoben?
Fragen zu 5	Sind alle Standorte auch in ein zentrales Monitoring eingebunden und ist das zentrale Monitoring auch bei Wartung eines Standortes und gleichzeitigem Ausfall eines weiteren Standortes funktionsfähig?

C. Anhang

C.a. Herleitung des HVB-kompakt aus dem HVB

In Tabelle 1 wird dargestellt, welche Indikatoren aus dem HV-Benchmark ausgewählt worden sind (Spalte 5), um die für den Bericht an den HHA festgelegten Kategorien (Spalte 2) und Unterkategorien (Spalte 4) abdecken zu können.

Nr.	Kategorie für den HHA-Bericht	Nr.	Unterkategorie für den HHA-Bericht	Nr. des Indikators aus dem HVB-kompakt, der die Unterkategorie abdeckt
I	Informations-sicherheits-Management	I.a	Informationssicherheits-Managementsystem (ISMS)	1
		I.b	Risikomanagement	2
		I.c	Notfallvorsorge	3, 8
		I.d	Personalmanagement	4
		I.e	Sicherheitskonzepte	10, 11, 13, 14
II	Cyber-sicherheit	II.a	Prävention	16, 17, 19, 20, 22, 23, 24, 31
		II.b	Verfügbarkeit des RZ über das Netz	18, 20, 21
		II.c	Detektion, Monitoring	6, 7, 22, 33, 34
		II.d	Reaktion	8, 15
		II.e	Datensicherung, Wiederherstellung	9, 18, 25
III	Krypto-sicherheit	III.a	Vertraulichkeit und Integrität beim Datentransport	12, 21, 31
		III.b	Vertraulichkeit und Integrität der gespeicherten Daten	12, 31
IV	Physische Sicherheit	IV.a	Redundanz	18
		IV.b	Baulich/technische Grundlagen	5
		IV.c	Stromversorgung	5, 26, 27
		IV.d	Zutritts-, Einbruch- und Sabotageschutz	5, 29, 30
		IV.e	Brandschutz	5, 28
		IV.f	Monitoring	32

Tabelle 2: Zuordnung der Indikatoren des HVB-kompakt zu den Kategorien und Unterkategorien für den Bericht an den HHA

Domäne im HVB	Nr.	Indikator im HVB-kompakt (in Klammern: Nr. des Indikators im HVB)	ISM[5]	CS	KS	PS
Manage-ment	1	Informationssicherheits-Managementsystem (ISMS) (1.1.3)	X			
	2	Risikomanagement (1.1.8)	X			
	3	Notfall- und Krisenmanagement (1.1.10)	X			
	4	Einhaltung rechtlicher und organisatorischer Vorgaben durch das Personal (1.2.4)	X			
	5	Infrastruktur, Grundlagen und Planung (1.3.1)				X
IT-Steuer-ung	6	Availability Management (Verfügbarkeitsmanagement): Messung und Steuerung der Verfügbarkeit (2.1.4)		X		
	7	Capacity Management: Messung und Steuerung der Kapazität (2.1.7)		X		
	8	IT-Service Continuity Management: IT-Notfallplanung (ITSCM-Rahmenwerk) (2.1.9)	X	X		
	9	IT-Service Continuity Management: Datensicherungen (2.1.12)		X		
	10	IT-Sicherheitskonzepte: Mandantentrennung (2.1.14)	X			
	11	IT-Sicherheitskonzepte: ID- und Rechtemanagement (2.1.15)	X			
	12	IT-Sicherheitskonzepte: Kryptografie (2.1.16)			X	
	13	IT-Sicherheitskonzepte: Sichere Datenlöschung und Aussonderung (2.1.17)	X			
	14	IT-Sicherheitskonzepte: Schutz gegen Schadprogramme und netzbasierte Angriffe (2.1.19)	X			
	15	Incident Management: Sicherheitsvorfallbehandlung (2.3.7)		X		
	16	Patch- und Releasemanagement (Software) (2.4.4)		X		
	17	Trennung von Entwicklungs-, Test- und Produktionsumgebungen (2.4.5)		X		
Technik	18	Ausfallsicherheit / Redundanzkonzept (3.1.1)		X		X
	19	Netzwerk-Segmentierung (3.2.2)		X		
	20	Sicherheit der aktiven Netzwerkkomponenten (3.2.3)		X		
	21	Ausgestaltung der WAN-Anbindung zw. den IT-Standorten (3.2.6)		X	X	
	22	Sicherheit der Internetanbindung (3.2.8)		X		
	23	Server-Sicherheit (3.3.1)		X		
	24	Datensicherheit der Speicher (3.4.2)		X		
	25	Datenreplikation und -sicherung (3.4.3)		X		
	26	Energieversorgung: Unterbrechungsfreie Stromversorgung (3.5.1)				X
	27	Energieversorgung: Einsatz einer Netzersatzanlage (3.5.2)				X
	28	Technischer Brandschutz des Rechenzentrums (3.5.8)				X
	29	Gebäudesicherheit: Schutz gegen Einbruch und Sabotage (3.5.10)				X

[5] IS-M = Informationssicherheits-Management; CS = Cyber-Sicherheit; KS = Krypto-Sicherheit; PS = Physische Sicherheit

	30	Gebäudesicherheit: Technische / bauliche Maßnahmen zum Zutrittsschutz (3.5.11)				X
	31	Sicherheit der Verzeichnisdienste (3.6.2)		X	X	
	32	Monitoring der technischen Infrastruktur (3.7.1)				X
	33	Monitoring auf IT-Sicherheitsvorfälle, Logging (3.7.2)		X		
	34	Monitoring der IT-Komponenten und -Dienste auf Verfügbarkeit (3.7.3)		X		

Tabelle 3: Übersicht der Indikatoren des HVB-kompakt und Abbildung auf die vier Darstellungskategorien für den Bericht an den HHA

C.b. Reifegrade

Allgemeine Beschreibung der fünf Reifegrade zur Bewertung von organisatorischen Prozessen:

Stufe	Reifegrad	Beschreibung des Reifegrads
1	Initial	Es gibt Verantwortliche, denen der Handlungsbedarf und ihre Aufgaben bekannt sind. Die Prozesse werden ereignisgetrieben (reaktiv) und eher „intuitiv“ gelebt, wobei sich das Know-how dazu in den Köpfen Einzelner befindet. Es werden Ergebnisse im Sinne der Zielsetzung erreicht, jedoch nicht nach definiertem Muster bzw. dokumentierter und angewiesener Vorgehensweise. Die Einbeziehung einzelner Kompetenzträger und Experten erfolgt situationsabhängig.
2	Wiederholbar	Die Ausführung der Prozesse hat durch festgelegte Ablaufmuster ein gewisses Maß an Robustheit erreicht. Durch das festgelegte Ablaufmuster werden Prozesse wiederholbar. Es existieren Dokumente und Vorgaben, welche die Prozesse und Maßnahmen – zumindest bis zu einem gewissen Grad – definieren und beschreiben und die auch umgesetzt sind. Die Qualität dieser Dokumentation ist ausreichend, so dass die Prozesse auch von fachnahen Mitarbeitern (z. B. im Vertretungsfall) im Sinne der Zielerreichung durchgeführt werden können. Die Dokumentation ist jedoch nicht ausführlich genug, um die Prozessdurchführung von sachverständigen Dritten vornehmen zu lassen. Die Prozesse und Zuständigkeiten sind innerhalb der Organisation noch nicht umfassend kommuniziert.
3	Standardisiert	Prozesse sind vollständig standardisiert und dokumentiert, werden kommuniziert und sind vollständig umgesetzt. Die Definition der Prozesse orientiert sich an einem Standard, entweder als formales Abbild bestehender Praktiken oder auf der Basis etablierter Standards (z. B. COBIT, ITIL, ISO 27001, IT-Grundschutz des BSI). Für Prozesse sind Ziele im Konsens entwickelt und operationalisiert. Die Definition erfolgt durch Festlegung von Abläufen und Verantwortlichkeiten; das notwendige Wissen dazu ist dokumentiert und wird weitergegeben.
4	Gesteuert	Für die Prozesse existieren Zielvorgaben, an denen der Prozess gemessen, überwacht und gesteuert wird. Die Prozesse werden regelmäßig und anlassbezogen auf Basis der Soll-Vorgaben überprüft und in ihrer Zielerreichung (Wirksamkeit) bewertet (Soll-/Ist-Vergleich, Prüfung der Einhaltung der Vorgaben). Die identifizierten Lücken werden geschlossen.
5	Optimiert	Die Prozesse werden zusätzlich auf übergeordneter Ebene regelmäßig überprüft und verbessert / optimiert, wodurch das IT-Management und die Service Qualität insgesamt ständig verbessert werden. Die Effektivität der Prozesse wird über „Stellgrößen“ optimiert und nachgehalten.

Tabelle 4: Allgemeine Beschreibung der fünf Reifegrade zur Bewertung von organisatorischen Prozessen

C.c. Potenzialstufen

Allgemeine Beschreibung der fünf Potenzialstufen zur Bewertung technischer Umsetzungen:

Stufe	Definition Potenzialstufe	Beschreibung der Potenzialstufe und Beispiele
1	Normale (d. h. keine außergewöhnlichen) Anforderungen an die Verlässlichkeit der IT (die bei den Potenzialstufen im Wesentlichen durch die Verfügbarkeit bestimmt wird)	– Verfügbarkeit: Die Maßnahmen für Potenzialstufe 1 aus dem HV-Kompendium müssen umgesetzt werden. – Einsatz robuster Komponenten: Hochwertige Materialien und robustes Design von Software- und Hardwarearchitekturen – Betriebssicherheit als Grundanforderung – Erfüllung relevanter Normen (DIN, GEFMA, etc.) – Stabile geografische Lage – Härtung von Komponenten
2	Hohe Anforderungen an die Verlässlichkeit der IT	– Verfügbarkeit: Die Maßnahmen für Potenzialstufe 2 aus dem HV-Kompendium müssen umgesetzt werden. – Redundanzen bei den wesentlichen Komponenten – Definiertes Notfallkonzept für gefährdete Bestandteile der IT, basierend auf dem Ergebnis von Risikoanalysen (BSI 200-3) – Verbesserte Härtung von Komponenten (minimalisiert auf die zugedachte Funktionalität) – Räumliche Trennung / getrennte Brandabschnitte – Umfassendes Logging / technische Protokollierung
3	Sehr hohe Anforderungen an die Verlässlichkeit der IT	– Verfügbarkeit: Die Maßnahmen für Potenzialstufe 3 aus dem HV-Kompendium müssen umgesetzt werden. – Vollständig ausgebaute Redundanzen mit gleicher Kapazität – Strenge Limitierung von Zutritt, Zugang und Zugriff (bspw. Anzahl und Dauer von Anmeldungen an Dienste / Administrationssoftware) – Regelmäßige Überprüfung von technischen Komponenten und Protokollen – Fehlertolerante IT (bspw. NEA-gestützt gegen Stromausfälle) – Früherkennung von Störungen – Externe Auslagerung von Datensicherungen – Automatismen / automatisch ablaufende Regelmechanismen zum Ausgleich von Störungen (bspw. Wiederanlauf nach einem Stromausfall)
4	Höchste Anforderungen an die Verlässlichkeit der IT	– Verfügbarkeit: Die Maßnahmen für Potenzialstufe 4 aus dem HV-Kompendium müssen umgesetzt werden. – Geo-Redundanz – Ständige Überwachung – Kurze Reaktionszeiten auf Störungen
5	Desaster-tolerant	– Verfügbarkeit: Die Maßnahmen für Potenzialstufe 5 aus dem

Stufe	Definition Potenzialstufe	Beschreibung der Potenzialstufe und Beispiele
	(Desaster-tolerant bedeutet, die IT muss auch in Ausnahmesituationen und unter Extrembedingungen (z. B. bei „höherer Gewalt") verlässlich funktionieren.)	HV-Kompendium müssen umgesetzt werden. – Geo- und Wartungsredundanz, so dass z. B. ein Abschalten zu Wartungszwecken jederzeit möglich ist (bspw. Austausch von Komponenten im laufenden Betrieb), ohne dass der Ausfall einer weiteren Komponente zum Ausfall des Dienstes führt – Mechanismen zur Überbrückung von längeren Ausfallereignissen (bspw. mehrtägiger, regionaler Stromausfall) – Sabotagesichere Leitungen

Tabelle 5: Allgemeine Beschreibung der fünf Potenzialstufen zur Bewertung technischer Umsetzungen