Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Mindeststandard des BSI zum HV-Benchmark kompakt 5.0

nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 29.11.2023

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	26.05.2017	Erstveröffentlichung
1.1	19.06.2018	Minor Release – Anpassungen und Konkretisierungen
2.0	29.11.2023	Major Release – Anhebung der Mindestwerte auf Niveau der Standard-Absicherung nach IT-Grundschutz

Tabelle 1: Versionsgeschichte des Mindeststandards für HV-Benchmark. Eine ausführliche Änderungsübersicht zum vorliegenden Mindeststandard erhalten Sie unter: https://bsi.bund.de/dok/MST-HV-Benchmark-Log

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6262
E-Mail: mindeststandards@bsi.bund.de
Internet: https://www.bsi.bund.de

Vorwort

Risiken für die Cyber- und Informationssicherheit sind nicht zuletzt aufgrund der zunehmenden Komplexität und Vernetzung von IT-Systemen allgegenwärtig. Dadurch betreffen potenzielle Schwachstellen und Cyber-Angriffe in der Regel nicht nur einzelne Stellen.

Umso wichtiger ist die Vorgabe verbindlicher Sicherheitsanforderungen an die Informationstechnik des Bundes. So kann ein einheitliches Mindestsicherheitsniveau mit effektiven Maßnahmen zur Abwehr von Cyber-Angriffen innerhalb der heterogenen Behördenlandschaft etabliert werden.

Dazu legt das Bundesamt für Sicherheit in der Informationstechnik (BSI) Mindeststandards (MST) für die Sicherheit der Informationstechnik des Bundes[1] fest. Dies erfolgt auf der Grundlage des § 8 Absatz 1 BSIG im Benehmen mit den Ressorts. Als gesetzliche Vorgabe definieren Mindeststandards somit ein verbindliches Mindestniveau für die Informationssicherheit.

Bereits 2017 hat das Bundeskabinett mit dem Umsetzungsplan Bund 2017 (UP Bund 2017)[2] eine Leitlinie für Informationssicherheit in der Bundesverwaltung in Kraft gesetzt. Damit wurde die Beachtung der Mindeststandards für den Bereich der Einrichtungen verbindlich. Durch das IT-Sicherheitsgesetz 2.0 wurde die Einhaltung der Mindeststandards des BSI auch gesetzlich geregelt. Die Umsetzungspflicht der Mindeststandards ergibt sich aus dem dadurch neu gefassten § 8 BSIG.

Die Mindeststandards richten sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe), Informationssicherheitsbeauftragte (ISB), IT-Betriebspersonal und Beschaffungsstellen. Die Gesamtverantwortung für die Informationssicherheit und damit auch für die Einhaltung der Mindeststandards trägt gemäß UP Bund 2017 die Leitung der jeweiligen Einrichtung[1].

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 dem Mindestsicherheitsniveau 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.[3] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Einrichtung 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 Einrichtungen auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Die von den Mindeststandards adressierten Stellen werden in § 8 Absatz 1 BSIG definiert.
Vgl. BSIG, s. Literaturverzeichnis: (5)
Zur besseren Lesbarkeit wird im weiteren Verlauf für alle dort genannten Stellen der Begriff „Einrichtung“ verwendet.

[2] Vgl. UP Bund (BMI 2017), s. Literaturverzeichnis: (4)

[3] Siehe FAQ zu den MST, s. Literaturverzeichnis: (3)

Inhalt

1 Beschreibung

Der vorliegende Mindeststandard hat zum Ziel, Mindestwerte für die in dem Bewertungsschema „HV-Benchmark kompakt“ betrachteten Aspekte der Informationssicherheit festzulegen. Diese Mindestwerte müssen von den Einrichtungen bei der Anwendung des HV-Benchmark kompakt (HVB-kompakt) an ihren Rechenzentren (RZ) mindestens erreicht werden.

Grundlage und als Anlage 1 fester Bestandteil dieses Mindeststandards ist der HVB-kompakt in der Version 5.0. Der HVB-kompakt ist ein Auszug aus dem HV-Benchmark (HVB)[4].

HVB

Der HVB ist ein modular aufgebautes Bewertungsschema, mit dem die Verlässlichkeit einer zu betrachtenden IT-Dienstleistung oder eines RZ relativ einfach gemessen und bewertet werden kann. 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 (Quality of Services) 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 auch IT-Nutzer, die einen geeigneten RZ-Betreiber suchen.

HVB-kompakt

Der HVB-kompakt ist eine komprimierte Version des HVB, die entwickelt wurde, um einen Auftrag des Haushaltsausschusses des Deutschen Bundestags (HHA) umzusetzen (siehe Abschnitt „Historie des Mindeststandards“). Der HHA hatte den Auftrag erteilt, *„hinsichtlich […] der IT-Sicherheit“* den HVB *„schrittweise auf alle Rechenzentren in der Bundesverwaltung“* anzuwenden.[5] Mit Hilfe aller Indikatoren 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. Außerdem verwendet der HVB-kompakt gegenüber dem HVB eine leicht modifizierte Methodik und ist um Revisionselemente ergänzt worden. Weitere Details, insbesondere die Methodik des HVB-kompakt, können der Anlage 1 entnommen werden.

Mindeststandard zum HVB-kompakt

Der Mindeststandard legt für jeden der 34 Indikatoren des HVB-kompakt 5.0 einen Mindestwert (bzgl. der Reifegrade des Indikators) fest, der aus Sicht des BSI bei der Anwendung des HVB-kompakt auf ein Rechenzentrum einer Einrichtung – unabhängig von dessen tatsächlichem Schutzbedarf – erreicht werden muss. Eine Beschreibung hierzu ist dem Kapitel 2 Sicherheitsanforderungen (Mindestwerte) zu entnehmen.

Die Einhaltung der im Mindeststandard vorgegebenen Mindestwerte ist für ein angemessenes IT-Sicherheitsniveau von Rechenzentren notwendig, aber allein nicht ausreichend. Das hat im Wesentlichen folgende Gründe:

[4] HVB: Bewertungsschema des BSI zur Bestimmung der Verlässlichkeit von IT-Dienstleistungen unter besonderer Berücksichtigung von Aspekten der Hochverfügbarkeit (HV). https://www.bsi.bund.de/dok/HV-Benchmark

[5] Beschluss des HHA zu TOP 14 a), b) und c) in seiner 82. Sitzung am 28.09.2016, Ausschussdrucksache Nr. 18(8)3472, Teil IV.2

- Für jedes Rechenzentrum sind Sollwerte für die 34 Indikatoren – unter Berücksichtigung des individuellen Schutzbedarfs – im Einzelfall festzulegen. Die Sollwerte werden in der Regel höher, aber niemals niedriger sein als die Mindestwerte. In Anlage 2 ist eine Hilfestellung zur Ermittlung individueller Sollwerte zu finden.
- 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 der Mindestwerte aus dem vorliegenden Mindeststandard sowie die Einhaltung der im vorangegangenen Aufzählungspunkt genannten Sollwerte immer noch kein angemessenes Sicherheitsniveau gewährleistet, hat folgenden Grund: Der HVB-kompakt umfasst sehr wichtige Aspekte der RZ-Sicherheit, aber nicht alle. Die Vollständigkeit ist nur durch Anwendung anerkannter Standards (z. B. IT-Grundschutz, DIN EN 50600) zu erreichen. Daher kann der HVB-kompakt solche Standards keinesfalls ersetzen. Die Unvollständigkeit (oder – je nach Sichtweise – Fokussierung) des HVB-kompakt (wie auch des HVB) ist dem Umstand geschuldet, dass es sich dem Wesen nach um ein Messinstrument handelt. Erst der Mindeststandard zum HVB-kompakt (MST-HVB-kompakt) ist ein Anforderungsdokument, das aber die Unvollständigkeit des HVB-kompakt inhärent übernimmt.

Zusammenhang zwischen IT-Grundschutz und MST-HVB-kompakt

Aus zuvor genannten Gründen kann der MST-HVB-kompakt den IT-Grundschutz in keiner Weise ersetzen. Der IT-Grundschutz ist ein Standardwerk der Informationssicherheit mit dem Anspruch auf Vollständigkeit bezüglich aller für die Informationssicherheit relevanten Aspekte.

Der Zusammenhang zwischen dem IT-Grundschutz (auf dem Niveau Standard-Absicherung) und dem MST-HVB-kompakt stellt sich wie folgt dar:

- Ist der IT-Grundschutz auf dem Niveau Standard-Absicherung vollständig umgesetzt, so ist „automatisch“ der MST-HVB-kompakt überwiegend erfüllt. Nur bei wenigen Mindestwerten geht der MST-HVB-kompakt über den IT-Grundschutz hinaus. Für die Bundesverwaltung hielt das BSI einige Präzisierungen gegenüber dem IT-Grundschutz für erforderlich, da der IT-Grundschutz auch anderen Zielgruppen dient als nur der Bundesverwaltung.
- Ist der MST-HVB-kompakt vollständig umgesetzt, so ist der IT-Grundschutz auf Niveau Standard-Absicherung nur in Teilen umgesetzt, da der IT-Grundschutz wesentlich umfangreicher ist als der HVB-kompakt.

Der Nutzen des HVB-kompakt wie auch des MST-HVB-kompakt liegt in der Fokussierung auf außergewöhnlich wichtige und aussagekräftige Aspekte der IT-Sicherheit, sodass sich deren Umsetzung und Einhaltung in sehr kurzer Zeit überprüfen lässt. Darüber hinaus dienen beide Werke der Umsetzung von Aufträgen des HHA zur Analyse aller Rechenzentren in der Bundesverwaltung hinsichtlich ihres Stands der IT-Sicherheit. Dabei ist der MST-HVB-kompakt ein einfaches Instrument, um entscheiden zu können, ob ein Mindestsicherheitsniveau erfüllt ist oder nicht. Die Einzelheiten werden nachfolgend erläutert.

Historie des Mindeststandards

Im Jahr 2016 hatte der HHA die Bundesregierung mittels Beschluss aufgefordert,

- zum einen *„[…] hinsichtlich […] der IT-Sicherheit […] 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“. Zudem soll „das Verfahren […] weiter optimiert und mit der bereits etablierten Methode der IT-Sicherheitsrevision kombiniert werden“*[6] und

[6] Beschluss des HHA zu TOP 14 a), b) und c) in seiner 82. Sitzung am 28.09.2016, Ausschussdrucksache Nr. 18(8)3472, Teil IV.2

- zum anderen *„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“*. Weiterhin heißt es darin: *„Wird im Rahmen des Benchmarks eine Unterschreitung dieses Niveaus festgestellt, ist der Leiter der betroffenen Behörde für die Einleitung von Gegenmaßnahmen verantwortlich“*.[7]

Diese Maßgaben des HHA waren bereits mit der bisherigen Version des Mindeststandards zum HVB-kompakt (Version 1.1) umgesetzt.

Die bisherige Version des MST-HVB-kompakt, die 2017 zum ersten Mal speziell für die Sicherheitsanalyse aller RZ der Bundesverwaltung definiert worden ist, legte seinerzeit die Mindestwerte auf einem relativ niedrigen Niveau fest, das sich an der Basis-Absicherung des IT-Grundschutzes orientierte. Da es sich um die erste Festlegung des Mindeststandards handelte und die Bundesverwaltung nicht überfordert werden sollte, ist seinerzeit dieses relativ niedrige Niveau gewählt worden.

Der zeitlich nach dem MST-HVB-kompakt verabschiedete UP Bund 2017 legt für seinen Geltungsbereich fest, dass *„bei Anwendung des modernisierten IT Grundschutzes die darin beschriebene Standard-Absicherung als Mindestanforderung [für die Bundesverwaltung]“*[8] anzusehen ist. Grund dafür ist, dass *„durch die Umsetzung von organisatorischen, personellen, infrastrukturellen und technischen Sicherheitsanforderungen […] mit der Vorgehensweise ‘Standard-Absicherung‘ ein Sicherheitsniveau […] erreicht [wird], das für den normalen Schutzbedarf angemessen und ausreichend ist […]“*.[9]

Vor diesem Hintergrund fordert der HHA die Bundesregierung in seinem Beschluss vom 10.11.2022 auf, *„[…] die Mindestwerte in dem vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelten Schema für die Analyse der IT-Sicherheit der Rechenzentren (HV-Benchmark kompakt) auf die Standard-Anforderungen des IT-Grundschutzes anzuheben“*.[10] Diese Maßgabe soll mit Hilfe der vorliegenden Überarbeitung des MST-HVB-kompakt erfüllt werden. Hierbei muss klargestellt werden, dass der MST-HVB-kompakt nicht alle Basis- und Standard-Anforderungen des IT-Grundschutzes umfassen kann, da lediglich 34 Aspekte (Indikatoren) betrachtet werden und der IT-Grundschutz wesentlich umfangreicher ist. Daher wird der Auftrag des HHA dahingehend interpretiert, dass für die 34 Indikatoren die Mindestwerte so festlegt werden sollen, dass sie sich am Schutzniveau der Standard-Absicherung orientieren.

1.1 Einleitung und Abgrenzung

Dieser Mindeststandard richtet sich an IT-Verantwortliche und Informationssicherheitsbeauftragte[11] sowie IT-Fachkräfte von Einrichtungen.

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

1.1.1 Rechenzentrum

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

Zur Festlegung dient die BSI-Definition für RZ (siehe Literaturverzeichnis: (7)). Sofern nichts anderes vermerkt ist, gilt insbesondere, dass der Begriff „Rechenzentrum“ nicht nur die IT-Betriebsflächen, sondern

[7] Beschluss des HHA zu TOP 14 a), b) und c) in seiner 82. Sitzung am 28.09.2016, Ausschussdrucksache Nr. 18(8)3472, Teil IV.3
[8] Vgl. UP Bund 2017, Kapitel 2, S. 4, s. Literaturverzeichnis: (4)
[9] Vgl. BSI-Standard 200-2, Abschnitt „1.2 Zielsetzung“, S. 8, s. Literaturverzeichnis: (6)
[10] Beschluss des HHA zu TOP 71 in seiner 34. Sitzung am 10.11.2022, Ausschussdrucksache Nr. 20(8)2851, lfd. Nr. 3
[11] Analog „IT-Sicherheitsbeauftragte“

auch alle Supportflächen (z. B. Stromversorgung, Kälteversorgung, Löschtechnik, Sicherheitstechnik) umfasst.

1.1.2 Domänen und Indikatoren

Der HVB-kompakt nutzt sogenannte Indikatoren zur Bewertung der Informationssicherheit von Rechenzentren oder IT-Dienstleistungen. 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 2).

Domäne	*Indikator-Nr.*	*Indikator-Bezeichnung*
Management	I.1	Informationssicherheitsmanagementsystem (ISMS)
	I.2	Risikomanagement im Zusammenhang mit der IT-Dienstleistungserbringung
	I.3	Notfall- und Krisenmanagement
	I.4	Verfahren zur Einhaltung rechtlicher und organisatorischer Vorgaben durch das Personal
	I.5	Infrastruktur, Grundlagen und Planung
IT-Steuerung	I.6	Availability Management (Verfügbarkeitsmanagement): Messung und Steuerung der Verfügbarkeit
	I.7	Capacity Management (Kapazitätsmanagement): Messung und Steuerung der Kapazität
	I.8	IT-Service Continuity Management: IT-Notfallplanung (ITSCM-Rahmenwerk)
	I.9	IT-Service Continuity Management: Datensicherungen
	I.10	IT-Sicherheitskonzepte: Mandantentrennung
	I.11	IT-Sicherheitskonzepte: ID- und Rechtemanagement
	I.12	IT-Sicherheitskonzepte: Kryptografie
	I.13	IT-Sicherheitskonzepte: Sichere Datenlöschung und Aussonderung
	I.14	IT-Sicherheitskonzepte: Schutz gegen Schadprogramme und netzbasierte Angriffe
	I.15	Incident Management: Sicherheitsvorfallbehandlung
	I.16	Patch- und Releasemanagement (Software)
	I.17	Trennung von Entwicklungs-, Test- und Produktionsumgebungen
Technische Umsetzung	I.18	Ausfallsicherheit/Redundanzkonzept
	I.19	Netzwerk-Segmentierung
	I.20	Sicherheit der aktiven Netzwerkkomponenten
	I.21	Ausgestaltung der WAN-Anbindung zwischen den IT-Standorten
	I.22	Sicherheit der Internet-Anbindung
	I.23	Server-Sicherheit
	I.24	Datensicherheit der Speicher

Domäne	*Indikator-Nr.*	*Indikator-Bezeichnung*
	I.25	Datenreplikation und -sicherung
	I.26	Energieversorgung: Unterbrechungsfreie Stromversorgung
	I.27	Energieversorgung: Einsatz einer Netzersatzanlage
	I.28	Technischer Brandschutz des Rechenzentrums
	I.29	Gebäudesicherheit: Schutz gegen Einbruch und Sabotage
	I.30	Gebäudesicherheit: Technische/bauliche Maßnahmen zum Zutritts-schutz
	I.31	Sicherheit der Verzeichnisdienste
	I.32	Monitoring der technischen Infrastruktur
	I.33	Monitoring auf IT-Sicherheitsvorfälle / Logging
	I.34	Monitoring der IT-Komponenten und -Dienste auf Verfügbarkeit

Tabelle 2: Domänen und Indikatoren des HVB-kompakt

Die Indikatoren und die zugehören Reifegrade oder Potenzialstufen werden ausführlich im HVB-kompakt 5.0 (siehe Anlage 1) beschrieben.

1.1.3 Reifegrad und Potenzialstufe

Bei Indikatoren, die sich auf einen Prozess beziehen, werden die Stufen unterschiedlicher Reife nachfolgend „Reifegrade“ genannt; bei solchen Indikatoren, die sich auf die technische Umsetzung beziehen, heißen sie nachfolgend „Potenzialstufen“.

1.2 Modalverben

In Anlehnung an den IT-Grundschutz[12] werden die Sicherheitsanforderungen mit den Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert. Darüber hinaus wird das Modalverb KANN für ausgewählte Prüfaspekte verwendet. Die hier genutzte Definition basiert auf RFC 2119[13] und DIN 820-2:2018[14].

MUSS / DARF NUR

bedeutet, dass diese Anforderung zwingend zu erfüllen ist. Das von der Nichtumsetzung ausgehende Risiko kann im Rahmen einer Risikoanalyse nicht akzeptiert werden.

DARF NICHT / DARF KEIN

bedeutet, dass etwas zwingend zu unterlassen ist. Das durch die Umsetzung entstehende Risiko kann im Rahmen einer Risikoanalyse nicht akzeptiert werden.

SOLLTE

bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Die Begründung muss dokumentiert und bei einem Audit auf ihre Stichhaltigkeit geprüft werden können.

SOLLTE NICHT / SOLLTE KEIN

[12] Vgl. BSI-Standard 200-2, S. 18, s. Literaturverzeichnis: (6)
[13] Vgl. Key words for use in RFCs, s. Literaturverzeichnis: (1)
[14] Vgl. DIN 820-2: Gestaltung von Dokumenten, s. Literaturverzeichnis: (2)

bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Die Begründung muss dokumentiert und bei einem Audit auf ihre Stichhaltigkeit geprüft werden können.

KANN

bedeutet, dass die Umsetzung oder Nicht-Umsetzung optional ist und ohne Angabe von Gründen unterbleiben kann.

2 Sicherheitsanforderungen (Mindestwerte)

In diesem Abschnitt werden den Indikatoren des HVB-kompakt Mindestwerte für die Reifegrade und Potenzialstufen zugeordnet, welche als Untergrenze für die Einhaltung des Mindeststandards erreicht werden MÜSSEN. Diese Mindestwerte werden je nach Art des Indikators „Mindestreifegrad“ oder „Mindestpotenzialstufe“ genannt – oder synonym für beide Begriffe „Mindeststufe“. Zur Erreichung des Mindestwertes für einen Indikator MÜSSEN – entsprechend der Methodik des HVB-kompakt – die Fragen zu allen Stufen von Stufe 1 bis einschließlich der Mindeststufe mit „Ja“ beantwortet werden können. Die Mindestwerte sind in Anlehnung an die Zyklen einer Zertifizierung nach IT-Grundschutz alle drei Jahre als erreicht nachzuweisen. Die Festlegung der Mindestwerte orientiert sich am Niveau der Standard-Absicherung des IT-Grundschutzes.

MST.2.0.01 – Mindestreifegrade

Für die 17 Indikatoren der Domänen „Management“ und „IT-Steuerung“ werden die in Tabelle 3 und Tabelle 4 genannten Werte als Mindestreifegrade festgelegt.

Indikator-Nr.	*Indikatoren der Domäne „Management“*	*Mindestreifegrad*
I.1	Informationssicherheitsmanagementsystem (ISMS)	4
I.2	Risikomanagement im Zusammenhang mit der IT-Dienstleistungserbringung	1
I.3	Notfall- und Krisenmanagement	2
I.4	Verfahren zur Einhaltung rechtlicher und organisatorischer Vorgaben durch das Personal	4
I.5	Infrastruktur, Grundlagen und Planung	2

Tabelle 3: Mindestreifegrade für die Indikatoren der Domäne „Management“

Indikator-Nr.	*Indikatoren der Domäne „IT-Steuerung“*	*Mindestreifegrad*
I.6	Availability Management (Verfügbarkeitsmanagement): Messung und Steuerung der Verfügbarkeit	2
I.7	Capacity Management (Kapazitätsmanagement): Messung und Steuerung der Kapazität	2
I.8	IT-Service Continuity Management: IT-Notfallplanung (ITSCM-Rahmenwerk)	2
I.9	IT-Service Continuity Management: Datensicherungen	4
I.10	IT-Sicherheitskonzepte: Mandantentrennung	2[15]
I.11	IT-Sicherheitskonzepte: ID- und Rechtemanagement	3
I.12	IT-Sicherheitskonzepte: Kryptografie	3
I.13	IT-Sicherheitskonzepte: Sichere Datenlöschung und Aussonderung	4

[15] Der Mindestwert 2 für den Indikator „IT-Sicherheitskonzepte: Mandantentrennung [I.10]“ muss nur für Rechenzentren erreicht werden, die zwischen verschiedenen Mandanten oder Benutzendengruppen unterscheiden müssen. Die Personalabteilung ist i. d. R. ein dedizierter Mandant oder eine dedizierte Benutzendengruppe.

Indikator-Nr.	*Indikatoren der Domäne „IT-Steuerung“*	*Mindestreifegrad*
I.14	IT-Sicherheitskonzepte: Schutz gegen Schadprogramme und netzbasierte Angriffe	4
I.15	Incident Management: Sicherheitsvorfallbehandlung	4
I.16	Patch- und Releasemanagement (Software)	3
I.17	Trennung von Entwicklungs-, Test- und Produktionsumgebungen	2

Tabelle 4: Mindestreifegrade für die Indikatoren der Domäne „IT-Steuerung“

MST.2.0.02 – Mindestpotenzialstufen

Für die 17 Indikatoren der Domäne „Technische Umsetzung“ werden die in Tabelle 5 genannten Werte als Mindestpotenzialstufen festgelegt.

Indikator-Nr.	*Indikatoren der Domäne „Technische Umsetzung“*	*Mindestpotenzialstufe*
I.18	Ausfallsicherheit/Redundanzkonzept	1
I.19	Netzwerk-Segmentierung	2
I.20	Sicherheit der aktiven Netzwerkkomponenten	2
I.21	Ausgestaltung der WAN-Anbindung zwischen den IT-Standorten	1[16]
I.22	Sicherheit der Internet-Anbindung	2
I.23	Server-Sicherheit	3
I.24	Datensicherheit der Speicher	3
I.25	Datenreplikation und -sicherung	2
I.26	Energieversorgung: Unterbrechungsfreie Stromversorgung	2
I.27	Energieversorgung: Einsatz einer Netzersatzanlage	2
I.28	Technischer Brandschutz des Rechenzentrums	3
I.29	Gebäudesicherheit: Schutz gegen Einbruch und Sabotage	3
I.30	Gebäudesicherheit: Technische/bauliche Maßnahmen zum Zutrittsschutz	2
I.31	Sicherheit der Verzeichnisdienste	2
I.32	Monitoring der technischen Infrastruktur	1
I.33	Monitoring auf IT-Sicherheitsvorfälle / Logging	2
I.34	Monitoring der IT-Komponenten und -Dienste auf Verfügbarkeit	2

Tabelle 5: Mindestpotenzialstufen für die Indikatoren der Domäne „Technische Umsetzung“

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

Literaturverzeichnis

1. **Internet Engineering Task Force (IETF).** RFC 2119: Key words for use in RFCs to Indicate Requirement Levels. [Online] 1997. [Zitat vom: 23. 07 2020.] https://tools.ietf.org/html/rfc2119.

2. **Deutsches Institut für Normung e.V. (DIN).** *DIN 820-2:2018-09: Normungsarbeit – Teil 2: Gestaltung von Dokumenten.* Berlin : Beuth Verlag GmbH, 2018.

3. **Bundesamt für Sicherheit in der Informationstechnik (BSI).** BSI - Antworten auf häufig gestellte Fragen zu den Mindeststandards. *Mindeststandards des BSI.* [Online] [Zitat vom: 31. März 2023.] https://www.bsi.bund.de/dok/MST-FAQ.

4. **Bundesministerium des Innern und für Heimat (BMI).** Umsetzungsplan Bund 2017. *Bundesministerium des Innern und für Heimat.* [Online] Juli 2017. [Zitat vom: 31. März 2023.] https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.pdf.

5. **Bundesministerum der Justiz (BMJ).** BSI-Gesetz (BSIG). *§ 8 BSIG - Einzelnorm.* [Online] 2009. [Zitat vom: 31. März 2023.] https://www.gesetze-im-internet.de/bsig_2009/__8.html.

6. **Bundesamt für Sicherheit in der Informationstechik (BSI).** BSI-Standard 200-2. *IT-Grunschutz-Methodik.* [Online] 2017. [Zitat vom: 26. Juni 2023.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf.

7. **Bundesamt für Sicherheit in der Informationstechnik (BSI).** Definition eines Rechenzentrums. *Sicherheit von Rechenzentren/Hochverfügbarkeit.* [Online] 2017. [Zitat vom: 8. Mai 2023.] https://www.bsi.bund.de/dok/RZ-Definition.

Abkürzungsverzeichnis

BMI	Bundesministerium des Innern und für Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
DIN	Deutsches Institut für Normung e.V.
FAQ	Frequently Asked Questions
HHA	Haushaltsausschuss des Deutschen Bundestages
HV	Hochverfügbarkeit
HVB	HV-Benchmark
HVB-kompakt	HV-Benchmark kompakt
ID	Identity
IETF	Internet Engineering Task Force
ISB	Informationssicherheitsbeauftragte(r)
ISMS	Informationssicherheitsmanagementsystem
ITSCM	IT-Service Continuity Management
IT-SiBe	IT-Sicherheitsbeauftragte(r)
LAN	Local Area Network (lokales Netzwerk)
MST	Mindeststandard
MST-HVB-kompakt	Mindeststandard zum HV-Benchmark kompakt
RFC	Request for Comments
RZ	Rechenzentrum
TOP	Tagesordnungspunkt
UP	Umsetzungsplan
WAN	Wide Area Network (Weitverkehrsnetz)

Anlagen

1. HV-Benchmark kompakt, Version 5.0, Stand November 2023
2. Sollwertermittlung

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

HV-Benchmark kompakt

Stand: November 2023 – Version 5.0

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: hochverfuegbarkeit@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Einführung

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

1.1 Auftrag des Haushaltsausschusses

In Teil III.2 seines Beschlusses vom 17.06.2015[1] fordert der HHA *„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[2]) [3] 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“*.

Weiterhin fordert der HHA in Teil IV.2 seines Beschlusses vom 28.09.2016[4] *„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.“*.

Zudem fordert der HHA in Teil III.2 seines Beschlusses vom 21.06.2017[5] *„die Bundesregierung dazu auf, […] die Analyse der IT-Sicherheit der Rechenzentren der Bundesverwaltung durch das […] BSI weiter voranzutreiben“* sowie in Punkt III.3 *„in Einzelterminen die Leitungsebene der Behörden bzw. Ressorts, […] über die Ergebnisse zu unterrichten“*.

Die Gültigkeit der o. g. Beschlüsse hat der HHA in seinem Beschluss vom 10.11.2022[6] bestätigt.

Auf der Basis dieser Aufträge hat das BSI im Rahmen von sieben Teilprüfungen bislang 159 Rechenzentren bei 78 Institutionen der Bundesverwaltung untersucht.

1.2 HV-Benchmark

Der HV-Benchmark[7] (HVB) ist ein modular aufgebautes Bewertungsschema, mit dem die Verlässlichkeit einer IT-Dienstleistung oder eines Rechenzentrums relativ einfach gemessen und bewertet werden kann. Die Bewertung und Messung erfolgt mit Hilfe von etwa 100 besonders relevanten Aspekten der Verlässlichkeit, sogenannten Indikatoren, unter der Nutzung von Reifegradmodellen. In der Praxis wird mittels eines

[1] Beschluss des HHA zu TOP 23 a) und b) in seiner 50. Sitzung am 17.06.2015, Ausschussdrucksache Nr. 18(8)2134.

[2] Im Jahr 2022 ist das BMVI in BMDV (Bundesministerium für Digitales und Verkehr) umbenannt worden.

[3] Die drei Dienstleistungszentren ZIVIT, BIT und DLZ-IT (BMVI) sind im Jahr 2016 in das ITZBund überführt worden.

[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] Beschluss des HHA zu TOP 51 a), b), c), d), e), f) und g) in seiner 108. Sitzung am 21.06.2017, Ausschussdrucksache Nr. 18(8)4413.

[6] Beschluss des HHA zu TOP 71 in seiner 34. Sitzung am 10.11.2022, Ausschussdrucksache Nr. 20(8)2851.

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

umfangreichen Fragenkatalogs geprüft, welchen Reifegrad eine IT-Dienstleistung oder ein Rechenzentrum hinsichtlich eines Indikators erreicht.

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 (Quality of Service) 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.

Auf der Basis bewährter Standards wie COBIT und ITIL nutzt der HVB das Instrumentarium aus dem IT-Grundschutz und dem Hochverfügbarkeitskompendium (HV-Kompendium).

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

1.3 HV-Benchmark kompakt

Der HVB-kompakt ist eine komprimierte Version des HVB, die gegenüber der Vollversion 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.

Der HVB-kompakt in der vorliegenden Version 5.0 ist die Weiterentwickelung der Version 4.0 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:

- Informationssicherheitsmanagement,
- Cybersicherheit,
- Kryptosicherheit,
- 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, die den HVB-kompakt bilden. Die Herleitung des HVB-kompakt (V 5.0) aus dem HVB ist im Anhang A.1 beschrieben. Die Abbildung 1 (siehe Seite 8) gibt einen Überblick über alle Indikatoren des HVB; gelb markiert sind die Indikatoren, die für den HVB-kompakt (V 5.0) ausgewählt worden sind.

1.4 Methodik der RZ-Sicherheitsanalyse

1.4.1 Anwendung eines Indikators auf ein RZ

Die Methodik des HVB (und auch des HVB-kompakt) beruht im Wesentlichen auf der Anwendung der einzelnen Indikatoren auf das zu analysierende Rechenzentrum[8]. Die Indikatoren nehmen dabei ganzzahlige Werte von 0 bis 5 an. Bei Indikatoren, die sich auf einen organisatorischen Prozess (Management/IT-Steuerung) im RZ beziehen, spricht man von Reifegraden. Eine allgemeine Beschreibung der Reifegrade befindet sich im Anhang A.2. Bei Indikatoren, die sich auf Technik beziehen, spricht man von Potenzialstufen, deren allgemeine Beschreibung sich im Anhang A.3 befindet. Bei allen Indikatoren gibt es jeweils 5 Stufen – unabhängig, ob es sich um Reifegrade oder Potenzialstufen handelt – zuzüglich der trivialen Stufe Null.

Jeder Reifegrad sowie jede Potenzialstufe (beide im Weiteren nur „Stufe“ genannt) ist mit einer oder mehreren Entscheidungsfragen 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.

1.4.2 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

[8] Es gilt die BSI-Definition für Rechenzentren (siehe https://www.bsi.bund.de/dok/RZ-Definition). Sofern nichts anderes vermerkt ist, gilt insbesondere, dass der Begriff „Rechenzentrum“ nicht nur die IT-Betriebsflächen, sondern auch alle Supportflächen (z. B. Stromversorgung, Kälteversorgung, Löschtechnik, Sicherheitstechnik) umfasst.

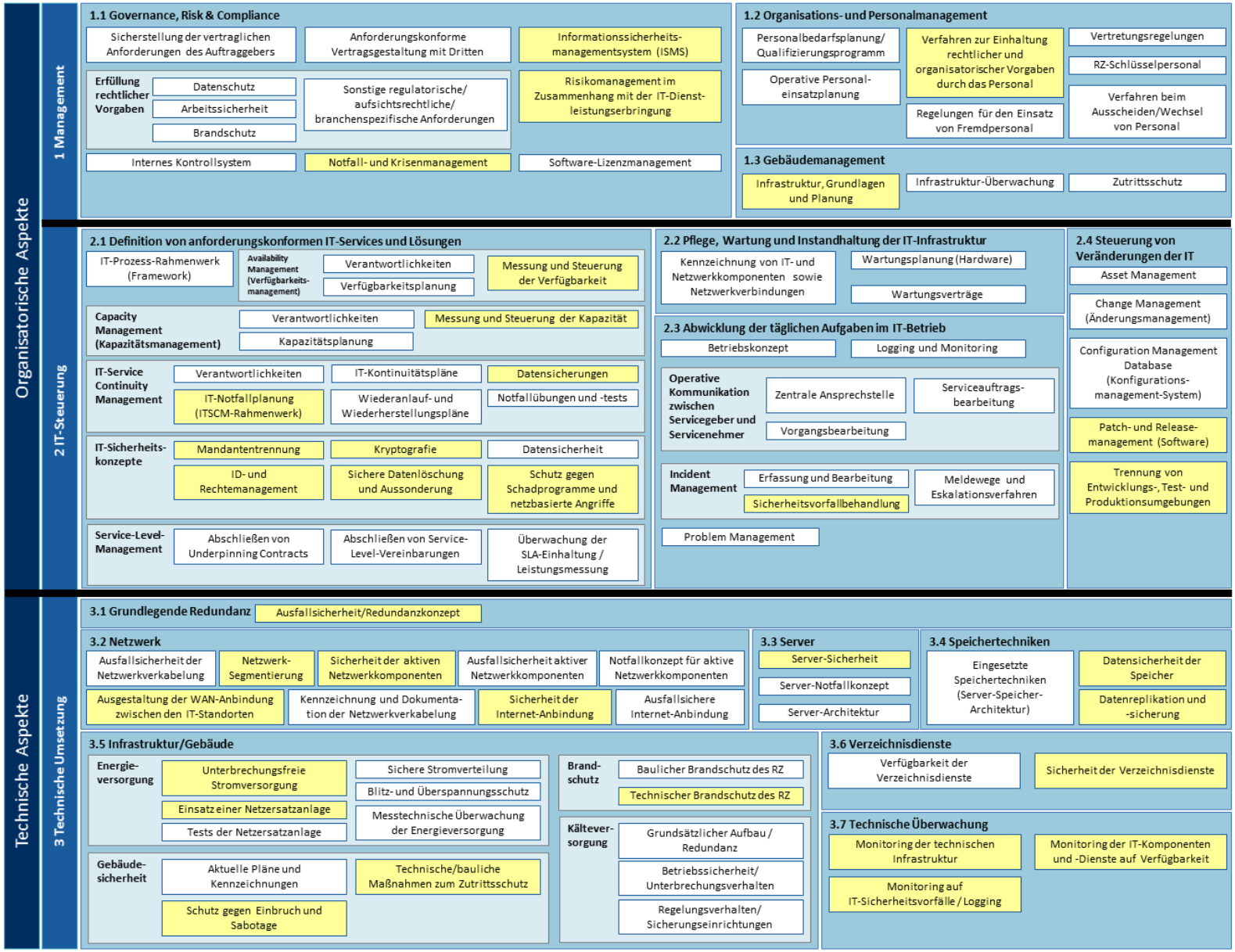

Abbildung 1: Übersicht aller Indikatoren des HVB; gelb hinterlegt sind die Indikatoren des HVB-kompakt.

2 Anwendung des HV-Benchmark kompakt

2.1 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. Die teilnehmende Institution wird gebeten, die nachfolgenden Informationen bereitzustellen.

Institutionsmerkmale:

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

RZ-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
  - gemäß 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 Sicht der untersuchten Institution nicht ausreichen.
- Zentraler Ansprechpartner für Rückfragen (Funktion und Kontaktdaten)

2.2 Indikatoren

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

I.1 Informationssicherheitsmanagementsystem (ISMS) [1.1.3][9]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Management
Unterdomäne	Governance, Risk und Compliance
Bezeichnung	Informationssicherheitsmanagementsystem (ISMS)
Kriterien	Verfügbarkeit; Vertraulichkeit; Integrität; Transparenz; Leistungsfähigkeit

Kurzbeschreibung	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
	  • Leitlinie zur Informationssicherheit
	  • Sicherheitskonzept
	  • Informationssicherheitsorganisation

Fragen zu 1	Ist mindestens eine Person innerhalb der Organisation für die Leitung des ISMS benannt, etabliert und für die Sicherstellung der Informationssicherheit zuständig (z. B. Informationssicherheitsbeauftragter 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? Sind die dafür notwendigen technischen und personellen Ressourcen 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 und anlassabhängig auf ihre Effektivität überprüft (unter Einbeziehung der Ergebnisse gemäß 4) und schnellstmöglich verbessert?

Tabelle 2: Indikator „Informationssicherheitsmanagementsystem (ISMS)“

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

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

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Management
Unterdomäne	Governance, Risk und Compliance
Bezeichnung	Risikomanagement im Zusammenhang mit der IT-Dienstleistungserbringung
Kriterien	Verfügbarkeit; Transparenz
Kurzbeschreibung	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 besteht, wenn eine Gefahr existiert und diese über eine Schwachstelle nachteilig auf ein Zielobjekt wirken und dadurch einen Schaden verursachen kann. Dieser Indikator umfasst vor allem das Management von Risiken im Zusammenhang mit der Erbringung von IT-Dienstleistungen, 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 als zentrale Stelle für das Risikomanagement 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 Vorgaben/Dokumentationen vorhanden, in denen z. B. beschrieben wird, • wie sich die Organisationskultur und -strategie bezüglich des Risikomanagements darstellt, • welche Bereitschaft zur Risikoübernahme existiert, • 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 kontrolliert? Werden die etablierten Methoden und Maßnahmen regelmäßig auf Plausibilität geprüft? Werden risikorelevante 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 anlassbezogene (insbesondere unter Nutzung der Prüfergebnisse gemäß 4) übergeordnete Prüfungen durchgeführt, die zur Anpassung des gesamten Risikomanagements führen (d. h. zur Anpassung von Risikostrategie und Risikobereitschaft) oder sogar zur Anpassung der Organisationsstrategie?

Tabelle 3: Indikator „Risikomanagement im Zusammenhang mit der IT-Dienstleistungserbringung“

I.3 Notfall- und Krisenmanagement [1.1.10]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Management
Unterdomäne	Governance, Risk und Compliance
Bezeichnung	Notfall- und Krisenmanagement
Kriterien	Verfügbarkeit; Vertraulichkeit; Integrität; Betriebssicherheit; Wartbarkeit; Leistungsfähigkeit
Kurzbeschreibung	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 diese 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, Pandemie, Streik, Unruhen 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-Standard 200-4.
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 grundlegende 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?

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
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-Standard 200-4 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 (z. B. 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?

Tabelle 4: Indikator „Notfall- und Krisenmanagement“

I.4 Verfahren zur Einhaltung rechtlicher und organisatorischer Vorgaben durch das Personal [1.2.3]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Management
Unterdomäne	Organisations- und Personalmanagement
Bezeichnung	Verfahren zur Einhaltung rechtlicher und organisatorischer Vorgaben durch das Personal
Kriterien	Vertraulichkeit; Integrität
Kurzbeschreibung	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. Die Mitarbeiter sollten über den Inhalt der Verpflichtung regelmäßig belehrt und dafür sensibilisiert werden.
Fragen zu 1	Haben alle Mitarbeiter inklusive Fremdpersonal eine Vertraulichkeitsvereinbarung unterzeichnet, welche die relevanten Gesetze, Vorschriften und Regelungen berücksichtigt?
Fragen zu 2	Liegen für Mitarbeiter, die in sicherheitsrelevanten Bereichen eingesetzt werden, unbedenkliche (erweiterte) 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 Mitarbeiterbelehrung 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 (auch unter Berücksichtigung der Ergebnisse gemäß 4) für den Prozess umgesetzt und nachgehalten (z. B. aus dem Feedbackgespräch oder aus Änderungen des Informationssicherheitsmanagements)?

Tabelle 5: Indikator „Verfahren zur Einhaltung rechtlicher und organisatorischer Vorgaben durch das Personal“

I.5 Infrastruktur, Grundlagen und Planung [1.3.1]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne **Unterdomäne** **Bezeichnung**	Management Gebäudemanagement Infrastruktur, Grundlagen und Planung
Kriterien	Verfügbarkeit; Vertraulichkeit; Betriebssicherheit; Leistungsfähigkeit
Kurzbeschreibung	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 nachteilige Einwirkungen von außen und innen (Feuer, Wasser, Sturm, Blitz/EMP, Ausfall des Energieversorgers, Einbruch, Anschlag, Erdbeben etc.) sowie ein betriebssicherer Aufbau aller Anlagen der technischen Gebäudeausrüstung (Energieversorgung inklusive Blitz- und Überspannungsschutz, Klimatisierung, Brandschutz und Sicherheitstechnik 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	Werden • auf der Basis einer mindestens partiellen Risikoanalyse und • unter Berücksichtigung gängiger Normen und Standards und • ensprechend der Verlässlichkeitsanforderungen Maßnahmen für den Gebäudeschutz und das Gebäudemanagement definiert und werden diese dokumentiert und umgesetzt?
Fragen zu 3	Wurde für alle Gebäude und Gebäudeteile, in denen Einrichtungen des RZ, sowohl IT als auch Support-Technik, betrieben werden, auf Basis einer umfassenden Risikoanalyse ein Gebäudeschutz- und Gebäudemanagementkonzept erstellt? Ist dieses Konzept vollständig dokumentiert und umgesetzt?
Fragen zu 4	Erfolgt eine regelmäßige Überprüfung, ob die Anforderungen eingehalten werden? Wird bei jeder baulichen oder technischen Veränderung am Gebäude sowie bei jeder Änderung der Nutzung des Gebäudes geprüft, ob das Gebäude die Anforderungen noch erfüllt? Werden bei Abweichungen von den Vorgaben entsprechende Verbesserungsmaßnahmen eingeleitet und deren Umsetzung nachgehalten?
Fragen zu 5	Werden sowohl die übergeordneten Prozesse zur Erstellung der Infrastrukturkonzeption als auch die Infrastrukturkonzeption selbst regelmäßig hinsichtlich ihrer Wirksamkeit, angesichts der Gefährdungslage und des Stands der Technik (unter Berücksichtigung der Ergebnisse gemäß 4) überprüft und angepasst?

Tabelle 6: Indikator „Infrastruktur, Grundlagen und Planung“

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

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	IT-Steuerung
Unterdomäne	Definition von anforderungskonformen IT-Services und Lösungen
Bezeichnung	Availability Management (Verfügbarkeitsmanagement): Messung und Steuerung der Verfügbarkeit
Kriterien	Verfügbarkeit; Transparenz; Leistungsfähigkeit
Kurzbeschreibung	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 zur Erbringung der Dienstleistung relevanten 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? [Hinweis: „Einheitlich“ bedeutet hier, dass die Ergebnisse ggf. unterschiedlicher Monitoring-Systeme sinnvoll zusammenführbar, vergleichbar und ausführbar 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 von den Sollwerten kontinuierlich erfasst und werden automatisiert geeignete Meldungen über Abweichungen verschickt? Wird vorausschauend auf erkannte Abweichungen so reagiert, dass zu erwartende nachteilige Abweichungen zwischen Soll und Ist verhindert oder zumindest verzögert werden?
Fragen zu 5	Wird regelmäßig und anlassbezogen analysiert, ob das Availability Management die Verfügbarkeit anforderungskonform steuert und werden die Prozesse der Messung und Steuerung der Verfügbarkeit entsprechend dieser Analysen verbessert?

Tabelle 7: Indikator „Availability Management (Verfügbarkeitsmanagement): Messung und Steuerung der Verfügbarkeit“

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

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	IT-Steuerung
Unterdomäne	Definition von anforderungskonformen IT-Services und Lösungen
Bezeichnung	Capacity Management (Kapazitätsmanagement): Messung und Steuerung der Kapazität
Kriterien	Verfügbarkeit; Transparenz; Wartbarkeit; Leistungsfähigkeit
Kurzbeschreibung	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 eine anforderungskonforme Dienstleistung gewährleistet werden kann. 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 zur Erbringung der Dienstleistung relevanten IT-Komponenten gemessen, mit definierten Soll-Kapazitätsanforderungen verglichen und auf Abweichungen reagiert?
Fragen zu 2	Werden regelmäßig Auswertungen und Analysen (Soll-Ist-Vergleiche) der gesammelten Kapazitätsdaten nach einem vorgegebenen und zumindest in Grundzügen dokumentierten Verfahren durchgeführt und wird auf Abweichungen reagiert?
Fragen zu 3	Sind die Soll-Kapazitätsanforderungen einheitlich und vollständig dokumentiert? Erfolgt ein systematisches und einheitliches Monitoring der Kapazität aller für die Erbringung der IT-Dienstleistung relevanten Komponenten durch Monitoringsysteme? [Hinweis: „Einheitliches Monitoring“ bedeutet, 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 von den Sollwerten kontinuierlich erfasst und werden automatisiert geeignete Meldungen über Abweichungen verschickt? Wird vorausschauend auf Veränderungen der Ist-Werte so reagiert, dass zu erwartende nachteilige Abweichungen zwischen Soll und Ist verhindert oder zumindest verzögert werden?
Fragen zu 5	Wird regelmäßig und anlassbezogen analysiert, ob das Capacity Management die Kapazität anforderungskonform steuert und werden die Prozesse der Messung und Steuerung der Kapazität entsprechend dieser Analysen verbessert?

Tabelle 8: Indikator „Capacity Management (Kapazitätsmanagement): Messung und Steuerung der Kapazität“

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

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	IT-Steuerung
Unterdomäne	Definition von anforderungskonformen IT-Services und Lösungen
Bezeichnung	IT-Service Continuity Management: IT-Notfallplanung (ITSCM-Rahmenwerk)
Kriterien	Verfügbarkeit; Leistungsfähigkeit
Kurzbeschreibung	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 200-4, ISO/IEC 27031 oder ITIL. 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 bei Störung bzw. nach Unterbrechungen oder Ausfällen sicherstellen?
Fragen zu 2	Sind Rollen, Verantwortlichkeiten und Prozesse des IT-Service Continuity Managements definiert? Existieren Strukturen und Vorlagen für Entwicklung, Test und Ausführung von Wiederanlauf-, Wiederherstellungs- und IT-Kontinuitätsplänen?
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-Standard 200-4, ISO 27031 oder IT-Grundschutz) ausgerichtet ist? Ist dieses ITSCM-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 sowie die weiteren Dokumente zur IT-Notfallplanung (z. B. Wiederanlauf-Koordinationsplan, Kontaktlisten) regelmäßig und anlassabhängig durch das IT-Management geprüft und aktualisiert? Werden dabei die Erkenntnisse aus den 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)?

Tabelle 9: Indikator „IT-Service Continuity Management: IT-Notfallplanung (ITSCM-Rahmenwerk)“

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

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	IT-Steuerung
Unterdomäne	Definition von anforderungskonformen IT-Services und Lösungen
Bezeichnung	IT-Service Continuity Management: Datensicherungen
Kriterien	Verfügbarkeit; Vertraulichkeit; Integrität
Kurzbeschreibung	Eine Datensicherung soll gewährleisten, dass der IT-Betrieb mittels eines redundanten Datenbestands kurzfristig wiederaufgenommen werden kann, wenn Teile des Datenbestandes verloren gehen oder die Datenintegrität verletzt ist. Für die Datensicherungen muss ein Konzept mit verbindlichen Vorgaben – insbesondere zur Wiederherstellung – vorliegen und es müssen regelmäßige Wiederherstellungstests stattfinden. Die Wiederherstellung beruht auf der Wiederherstellbarkeit eines bestimmten Datenzustands zu einem Zielzeitpunkt auf einem Zielsystem oder -objekt.
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 deren Wiederherstellung sowie entsprechend für Wiederherstellungstests? Basieren die Vorgaben auf einem einheitlichen Schema, z. B. auf einer definierten Klassifikation der Daten, die etwa aus dem Schutzbedarf abgeleitet ist?
Fragen zu 3	Existieren vollständig dokumentierte verbindliche Vorgaben und Regeln zur Durchführung und Auslagerung von Datensicherungen (Datensicherungskonzept), inkl. Wiederherstellung? 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?

Tabelle 10: Indikator „IT-Service Continuity Management: Datensicherungen“

I.10 IT-Sicherheitskonzepte: Mandantentrennung [2.1.14]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	IT-Steuerung
Unterdomäne	Definition von anforderungskonformen IT-Services und Lösungen
Bezeichnung	IT-Sicherheitskonzepte: Mandantentrennung
Kriterien	Vertraulichkeit; Integrität
Kurzbeschreibung	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. 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.
Fragen zu 1	Ist der Datenzugriff der Nutzer durch ein Berechtigungsmodell geregelt? Kommen mandantenspezifische Benutzerkennungen zum Einsatz, die ausschließlich zum Zugriff auf die eigenen 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 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 Definitionen der Rollen und die Zuordnungen von Institutionen und Personen nach einem definierten sowie nachweisbar gesteuerten Prozess, der vollständig dokumentiert, kommuniziert und umgesetzt 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?

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
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?

Tabelle 11: „IT-Sicherheitskonzepte: Mandantentrennung“

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

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	IT-Steuerung
Unterdomäne	Definition von anforderungskonformen IT-Services und Lösungen
Bezeichnung	IT-Sicherheitskonzepte: ID- und Rechtemanagement
Kriterien	Verfügbarkeit; Vertraulichkeit; Integrität; Transparenz
Kurzbeschreibung	Um IT-Systeme oder Systemkomponenten 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 sowie dem Schutzbedarf der Daten genügen.
Fragen zu 1	Haben alle Nutzer nur die Berechtigungen, die sie auch benötigen (Need-to-know-Prinzip)? 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? Berücksichtigt dieses 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? 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 in geeigneter Weise kontinuierlich überwacht und werden 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?

Tabelle 12: „IT-Sicherheitskonzepte: ID- und Rechtemanagement“

I.12 IT-Sicherheitskonzepte: Kryptografie [2.1.16]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	IT-Steuerung
Unterdomäne	Definition von anforderungskonformen IT-Services und Lösungen
Bezeichnung	IT-Sicherheitskonzepte: Kryptografie
Kriterien	Vertraulichkeit; Integrität
Kurzbeschreibung	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 und PGP 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 insbesondere die Technischen Richtlinien des BSI, wie etwa TR-02102-1 für die Bewertung der Sicherheit ausgewählter kryptografischer Verfahren und deren Schlüssellängen oder TR-02102-2 zur 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 derer 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 sicher installiert und eingesetzt? Erfolgt eine unverzügliche Eskalation bei der Feststellung von Sicherheitslücken (z. B. 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?

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Fragen zu 3	Wurde eine Bedrohungsanalyse durchgeführt und dokumentiert, die mindestens folgende Fragen beantwortet?: • 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? 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 den Fragen zu 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 der Kryptografie regelmäßig überprüft, insbesondere die Aktualität und Angemessenheit der ausgewählten Kryptoverfahren (Abgleich mit den neuesten Technischen Richtlinien und mit entsprechenden Meldungen in der Fachpresse)?

Tabelle 13: Indikator „IT-Sicherheitskonzepte: Kryptografie“

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

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	IT-Steuerung
Unterdomäne	Definition von anforderungskonformen IT-Services und Lösungen
Bezeichnung	IT-Sicherheitskonzepte: Sichere Datenlöschung und Aussonderung
Kriterien	Vertraulichkeit; Integrität
Kurzbeschreibung	Um die Vertraulichkeit schutzbedürftiger Daten/¬Informationen sicherzustellen, die zur Löschung vorgesehen sind, müssen diese so gelöscht oder vernichtet werden, dass eine Rekonstruktion mit hoher Wahrscheinlichkeit ausgeschlossen werden kann. Die Außerbetriebnahme/¬Wiederverwendung von IT-Systemen oder Datenträgern sowie der Umgang mit den darauf gespeicherten Daten muss im Vorfeld festgelegt werden. Dabei ist insbesondere dem Verlust noch benötigter Daten/¬Informationen sowie dem Verbleib von unerwünschten Datenrückständen vorzubeugen.
Fragen zu 1	Gibt es mindestens eine verantwortliche Person, die bei der Aussonderung oder Wiederverwendung von IT-Systemen und Speichermedien sicherstellt, dass keine noch benötigten Daten verloren gehen und sensitive Daten mit hoher Wahrscheinlichkeit 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 noch benötigten Daten verloren gehen? Werden bei der Löschung und Vernichtung die aktuell geltenden Standards eingehalten? Wird diese Vorgehensweise von den entsprechenden Verantwortlichen befolgt?
Fragen zu 3	Sind die Vorgaben zur Löschung, Außerbetriebnahme und Aussonderung (inklusive Vernichtung, Entsorgung und/oder Rückgabe) von IT-Systemen und Speichermedien sowie für die dabei zu erstellenden und einzuholenden Dokumente vollständig in einem entsprechenden Konzept dokumentiert, kommuniziert und umgesetzt? Sind Vereinbarungen mit Dritten abgeschlossen worden, die den internen Regelungen entsprechen, sofern Betrieb 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 erkannte Lücken geschlossen?
Fragen zu 5	Werden die Vorgaben, Konzepte und Prozesse zur sicheren Datenlöschung und Aussonderung anlassabhängig und regelmäßig hinsichtlich ihrer Eignung bewertet und optimiert? Wird dabei insbesondere die aktuelle technische Entwicklung von Datenträgern beachtet?

Tabelle 14: Indikator „IT-Sicherheitskonzepte: Sichere Datenlöschung und Aussonderung“

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

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	IT-Steuerung
Unterdomäne	Definition von anforderungskonformen IT-Services und Lösungen
Bezeichnung	IT-Sicherheitskonzepte: Schutz gegen Schadprogramme und netzbasierte Angriffe
Kriterien	Verfügbarkeit; Vertraulichkeit; Integrität
Kurzbeschreibung	Der Schutz gegen Schadprogramme (Malware, insbesondere Ransomware) und netzbasierte Angriffe (z. B. verteilte Denial-of-Service-Attacken (DDoS)) umfasst u. a. ein Virenschutzkonzept, Intrusion Detection Systeme, ein DDoS-Mitigationskonzept, die Einschränkung von Benutzerberechtigungen, die Prüfung auf neue sowie noch offene Sicherheitslücken, die Sensibilisierung der Mitarbeiter hinsichtlich Schadprogramme, Netzsegmentierung, Datensicherung. [Hinweise: 1. „Viren“ stehen als Synonym für alle Arten von Schadprogrammen. Mit „Virenschutzprogramm“ ist ein Programm zum Schutz vor jeglicher Art von Schadprogrammen gemeint. 2. Einige der oben genannten Schutzmaßnahmen werden in dedizierten Indikatoren betrachtet.]
Fragen zu 1	Werden Maßnahmen gegen Schadprogramme getroffen (z. B. Installation eines Virenschutzprogramms) und gibt es hierfür eine verantwortliche Person?
Fragen zu 2	Sind 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 aktuell und 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 erkannte Lücken geschlossen?
Fragen zu 5	Erfolgt eine Weiterentwicklung und Optimierung der übergeordneten Prozesse und Vorgaben zum Schutz vor Schadprogrammen und netzbasierten Angriffen aufgrund der Prüfungsergebnisse gemäß 4? Wird insbesondere das Sicherheitskonzept zum Schutz gegen Schadprogramme und netzbasierte Angriffe regelmäßig angepasst und verbessert?

Tabelle 15: Indikator „IT-Sicherheitskonzepte: Schutz gegen Schadprogramme und netzbasierte Angriffe“

I.15 Incident Management: Sicherheitsvorfallbehandlung [2.3.7]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	IT-Steuerung
Unterdomäne	Abwicklung der täglichen Aufgaben im IT-Betrieb
Bezeichnung	Incident Management: Sicherheitsvorfallbehandlung
Kriterien	Verfügbarkeit; Vertraulichkeit; Integrität
Kurzbeschreibung	Die Sicherheitsvorfallbehandlung beschreibt, angefangen von der Vorbereitung über die Durchführung bis hin zur Nachbereitung, den Prozess zur Behandlung von Sicherheitsvorfällen. 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. Die Sicherheitsvorfallbehandlung hat u. a. folgende Ziele: • drohende Sicherheitsvorfälle (z. B. durch Detektionsmechanismen) möglichst frühzeitig zu erkennen, • erkannte Sicherheitsvorfälle so rasch wie möglich zu analysieren und zu beheben, • akut drohende Schäden durch Sofortmaßnahmen zu begrenzen, • Ursachenforschung und daraus abgeleitet die Entwicklung von Maßnahmen (Umsetzungshinweisen) zur Vermeidung zukünftiger Sicherheitsvorfälle. Die Sicherheitsvorfallbehandlung unterstützt das übergeordnete Notfallmanagement/BCM und ergänzt das IT Service Continuity Management.
Fragen zu 1	Gibt es eine für die Sicherheitsvorfallbehandlung verantwortliche Person? Ist ein Sicherheitsvorfall eindeutig definiert und hinreichend gegenüber anderen Ereignissen abgegrenzt? Werden Sicherheitsvorfälle in den Bereichen der IT und der physischen Infrastruktur zumindest in Ansätzen erfasst, analysiert und behandelt?
Fragen zu 2	Wird sichergestellt, dass bei einem Sicherheitsvorfall die notwendigen Maßnahmen kurzfristig ergriffen werden können? Werden die im Rahmen der Vorfallbehandlung durchgeführten wesentlichen Aktionen dokumentiert? Sind 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 Erkennung, zeitnahe Eskalation und Reaktion sowie die vollständige Dokumentation von Sicherheitsvorfällen aller Bereiche (IT und physische Infrastruktur) 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 alle 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?

Tabelle 16: Indikator „Incident Management: Sicherheitsvorfallbehandlung“

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

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	IT-Steuerung
Unterdomäne	Steuerung von Veränderungen der IT
Bezeichnung	Patch- und Releasemanagement (Software)
Kriterien	Verfügbarkeit; Vertraulichkeit; Integrität; Transparenz; Wartbarkeit
Kurzbeschreibung	Zu den Aufgaben des Patch- und Releasemanagements 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 Releasemanagement wird ersichtlich, welche Patches noch fehlen und welchen Risiken der IT-Betrieb dadurch ausgesetzt ist. Ziel des Patch- und Releasemanagements 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 Releasemanagement führt schnell zu Lücken in der Sicherheit der einzelnen Softwarekomponenten und damit zu möglichen Angriffspunkten.
Fragen zu 1	Werden alle Patches, Updates und Releases von mindestens einer verantwortlichen Person 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 dieses Vorgehen eindeutig definiert und wird dieses Vorgehen in jedem Einzelfall 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 3 genannten Verfahren eingehalten?
Fragen zu 5	Erfolgt anhand der Ergebnisse von Reviews und Auswertungen eine Weiterentwicklung und Optimierung des Patch- und Releasemanagements?

Tabelle 17: Indikator „Patch- und Releasemanagement (Software)“

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

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	IT-Steuerung
Unterdomäne	Steuerung von Veränderungen der IT
Bezeichnung	Trennung von Entwicklungs-, Test- und Produktionsumgebungen
Kriterien	Verfügbarkeit; Vertraulichkeit; Integrität; Transparenz; Wartbarkeit
Kurzbeschreibung	Um eine angemessene Betriebsstabilität sicherzustellen, werden separate Serverumgebungen 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 oder unkontrolliertes Modifizieren von z. B. 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 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 Produktionsumgebungen aufgebaut? Sind die Test- und Entwicklungsumgebungen bezüglich der Datenverarbeitung und Berechtigungsvergabe strikt von den Produktionsumgebungen 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 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)?

Tabelle 18: Indikator „Trennung von Entwicklungs-, Test- und Produktionsumgebungen“

I.18 Ausfallsicherheit/Redundanzkonzept [3.1.1]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Technische Umsetzung
Unterdomäne	Grundlegende Redundanz
Bezeichnung	Ausfallsicherheit/Redundanzkonzept
Kriterien	Verfügbarkeit
Kurzbeschreibung	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 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 in räumlich von anderen Nutzungen getrennten Bereichen? Andere Nutzungen sind Büroflächen, Lager etc. 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, also solche, die für die Erbringung der Kernfunktionalität relevant sind, redundante Ausweichsysteme, die sich in einem anderen räumlich getrennten Bereich befinden? Stellen beide räumlichen Bereiche mindestens anforderungskonformen Schutz bereit?
Fragen zu 3	Sind die für die Erbringung der IT-Services erforderlichen Infrastrukturen, IT- und Netzwerkkomponenten vollständig redundant aufgebaut und – dem Zweck der Redundanz genügend – auf unterschiedliche räumlich getrennte Bereiche verteilt, welche die Qualität von brandgeschützten Bereichen mit mindestens 90 min. Feuerwiderstandszeit aufweisen? Sind diese Bereiche hinsichtlich der übrigen Schutzmerkmale anforderungskonform mindestens gleichwertig? Findet ein Failover zwischen den redundanten Systemen ohne für den Nutzer relevante Verzögerungen oder sonstige Auswirkungen statt?
Fragen zu 4	Sind sowohl die IT-Services als auch die für die Erbringung der IT-Services erforderlichen Infrastrukturen, IT- und Netzwerkkomponenten redundant auf georedundante Standorte verteilt? Findet bei Ausfall eines Standorts ein Failover zwischen den Standorten ohne für den Nutzer relevante Verzögerungen oder sonstige Auswirkungen im Rahmen des technisch Möglichen statt? [Hinweis: Anforderungen an Georedundanz sind in der BSI-Veröffentlichung „RZ-Standortkriterien“ genannt (siehe: https://www.bsi.bund.de/dok/RZ-Standortkriterien).]
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 können?

Tabelle 19: Indikator „Ausfallsicherheit/Redundanzkonzept“

I.19 Netzwerk-Segmentierung [3.2.2]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Technische Umsetzung
Unterdomäne	Netzwerk
Bezeichnung	Netzwerk-Segmentierung
Kriterien	Verfügbarkeit; Vertraulichkeit; Integrität
Kurzbeschreibung	Eine wesentliche Maßnahme zur Steigerung der Sicherheit des Netzwerks im RZ ist die Segmentierung. Eine geeignete logische oder auch physische Segmentierung sorgt zum einen für einen störungsärmeren 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 mit gleichem oder niedrigerem Schutzbedarf 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 (z. B. Office-Netz, DMZ)? Werden Daten, welche über Wege transportiert werden, die nicht im Einflussbereich des RZ-Betreibers liegen, geeignet verschlüsselt?
Fragen zu 2	Sind Netzsegmente mit Verbindungen in öffentliche Netze durch Sicherheitskomponenten (dem Schutzbedarf genügend, mindestens durch Paketfilter) von rein intern genutzten Segmenten getrennt?
Fragen zu 3	Ist zwischen den internen Netzsegmenten ein Sicherheitsgateway (z. B. eine Firewall) im Einsatz, das den Zugriff so kontrolliert, dass nur Kommunikationsbeziehungen gemäß den IT-Sicherheitskonzepten zugelassen werden? Werden die Protokollierungsdaten regelmäßig und zusätzlich anlassbezogen 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	Kann ein beliebiges Segment einzeln zu Wartungsarbeiten deaktiviert werden, ohne dass der zusätzliche spontane Ausfall eines weiteren Segments zum Ausfall des Dienstes führt (Wartungsredundanz)?

Tabelle 20: Indikator „Netzwerk-Segmentierung“

I.20 Sicherheit der aktiven Netzwerkkomponenten [3.2.3]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Technische Umsetzung
Unterdomäne	Netzwerk
Bezeichnung	Sicherheit der aktiven Netzwerkkomponenten
Kriterien	Verfügbarkeit; Vertraulichkeit; Integrität
Kurzbeschreibung	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 und Zugriff gesichert (z. B. durch verschlossene Räume oder Schutzschränke) und sind elementare Sicherheitsmaßnahmen 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? Findet eine ständige Überwachung der sicherheitsrelevanten Meldungen der Komponenten (Monitoring) mit geeigneter Reaktion statt?
Fragen zu 3	Geschieht das Management „Out of Band“, d. h. über ein eigenes, physisch getrenntes Netzwerk? Erfolgt eine regelmäßige Überprüfung der Einhaltung der Sicherheitsvorgaben sowie der Umsetzung der Sicherheitsmaßnahmen? Erfolgt eine zeitnahe Beseitigung der gefundenen Schwachstellen?
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?

Tabelle 21: Indikator „Sicherheit der aktiven Netzwerkkomponenten“

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

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Technische Umsetzung
Unterdomäne	Netzwerk
Bezeichnung	Ausgestaltung der WAN-Anbindung zwischen den IT-Standorten
Kriterien	Verfügbarkeit; Vertraulichkeit
Kurzbeschreibung	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.
Fragen zu 1	Sind vorhandene WAN-Anbindungen durch Verschlüsselung abgesichert (mindestens Software-Verschlüsselung) und entsprechen die SLA den Anforderungen?
Fragen zu 2	Werden vorhandene WAN-Anbindungen durch Monitoring auf Ausfall oder Störung überwacht und wird im Bedarfsfall angemessen reagiert?
Fragen zu 3	Wird bei Ausfall einer Verbindung eine redundante Verbindung automatisch genutzt? Gibt es zwei räumlich getrennte Hauseinführungen, die zu jeweils getrennten Verteilern des/der Dienstleister/s (Carrier) führen?
Fragen zu 4	Verfügen die redundanten Verbindungen über eine gleichwertige Kapazität (z. B. 2 x 1 GBit/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)?

Tabelle 22: Indikator „Ausgestaltung der WAN-Anbindung zwischen den IT-Standorten“

I.22 Sicherheit der Internet-Anbindung [3.2.8]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Technische Umsetzung
Unterdomäne	Netzwerk
Bezeichnung	Sicherheit der Internet-Anbindung
Kriterien	Verfügbarkeit; Vertraulichkeit; Integrität
Kurzbeschreibung	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 z. B. den Einsatz von Sicherheitsgateways (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 Sicherheitsgateway kontrolliert und protokolliert und wird sichergestellt, dass kein ungewollter Verbindungsaufbau von außen stattfindet?
Fragen zu 2	Ist die Sicherheitsgateway-Architektur mehrstufig und werden die übertragenen Inhalte auf Schadsoftware kontrolliert? Kontrolliert das Sicherheitsgateway auf Applikationsebene (soweit möglich, z. B. Mail, HTTP, FTP u. a.) die übertragenen Inhalte auch auf Protokollkonformität?
Fragen zu 3	Sind die Komponenten des Sicherheitsgateways vollständig redundant ausgelegt (z. B. Paketfilter, Application Level Gateway, Intrusion Detection System)?
Fragen zu 4	Werden an den Standorten mit eigener Internet-Anbindung gleichwertige Sicherheitsmaßnahmen (für die Internet-Anbindung) auf dem gleichen Sicherheitsniveau georedundant umgesetzt?
Fragen zu 5	Ist eine Wartung jeweils eines Teils des Sicherheitsgateway-Clusters jederzeit möglich, ohne dass ein Ausfall einer weiteren Sicherheitskomponente zu Einschränkungen der Sicherheitsmaßnahmen der Internet-Anbindung führt (Wartungsredundanz)?

Tabelle 23: Indikator „Sicherheit der Internet-Anbindung“

I.23 Server-Sicherheit [3.3.1]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Technische Umsetzung
Unterdomäne	Server
Bezeichnung	Server-Sicherheit
Kriterien	Verfügbarkeit; Vertraulichkeit; Integrität
Kurzbeschreibung	Zum sicheren Betrieb eines Servers tragen Sicherheitsmaßnahmen, insbesondere die Systemhärtung, bei. Die Härtung eines Servers erschwert einem Angreifer den Zugriff und sorgt für einen störungsfreieren Betrieb, indem z. B. überflüssige Dienste/Services deaktiviert werden. Einen Anhalt für solche Maßnahmen geben die entsprechenden Umsetzungshinweise des IT-Grundschutzes 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 „Standardniveau“) und umgesetzt? Werden aktuelle Sicherheitsupdates zeitnah installiert und ist ein stets aktueller Schutz gegen Schadprogramme aktiv?
Fragen zu 2	Sind zusätzlich auch weitergehende Maßnahmen berücksichtigt, die für die Härtung der Systeme sinnvoll/erforderlich sind (z. B. die Anforderungen bei erhöhtem Schutzbedarf gemäß 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 geeignete 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?

Tabelle 24: Indikator „Server-Sicherheit“

I.24 Datensicherheit der Speicher [3.4.2]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Technische Umsetzung
Unterdomäne	Speichertechniken
Bezeichnung	Datensicherheit der Speicher
Kriterien	Vertraulichkeit; Integrität
Kurzbeschreibung	Daten, die auf einem Speichersystem gelagert werden, können verschiedene Schutzbedarfe haben. Für die Sicherheit der Daten werden unterschiedliche Maßnahmen, wie z. B. 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 IT-Grundschutz eingerichtet (z. B. eine verschlüsselte Datenablage gemäß Schutzbedarf)?
Fragen zu 2	Sind Separierungen (z. B. 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 (geo-)redundanten 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?

Tabelle 25: Indikator „Datensicherheit der Speicher“

I.25 Datenreplikation und -sicherung [3.4.3]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Technische Umsetzung
Unterdomäne	Speichertechniken
Bezeichnung	Datenreplikation und -sicherung
Kriterien	Verfügbarkeit
Kurzbeschreibung	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 Datenträger 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, die über Replikationsmechanismen und/oder Backup geschützt werden müssen, identifiziert? Sind diese Maßnahmen 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 (z. B. SLA) eine Wiederherstellung von Daten auf Wunsch der Informationseigner möglich? Ist dies im abgestimmten Zeitrahmen durchführbar und wurde dies getestet? Werden die (gemäß Frage 1) für die Replikation identifizierten Daten mindestens zwischen zwei brandgeschützten Bereichen mit mindestens 90 min. Feuerwiderstandszeit repliziert?
Fragen zu 3	Werden Datensicherungen an externe Orte, die ein gleichwertiges Sicherheitsniveau haben, ausgelagert?
Fragen zu 4	Werden die Daten gemäß Fragen 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)?

Tabelle 26: Indikator „Datenreplikation und -sicherung“

I.26 Energieversorgung: Unterbrechungsfreie Stromversorgung [3.5.1]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Technische Umsetzung
Unterdomäne	Infrastruktur/Gebäude
Bezeichnung	Energieversorgung: Unterbrechungsfreie Stromversorgung
Kriterien	Verfügbarkeit
Kurzbeschreibung	Eine unterbrechungsfreie Stromversorgung (USV) dient dem unterbrechungsfreien Betrieb der nachgeschalteten Anlagen und Systeme bei einem Ausfall des vorgelagerten Versorgungsnetzes. Je nach Kategorie der USV filtert diese zudem Störungen, die z. B. 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, denn nur diese schützt vor den Schadeinwirkungen relevanter Netzstörungen, wie z. B. Spannungseinbrüche und -spitzen, Frequenzschwankungen und Oberschwingungen. Ein ausdrücklicher Blitz- und Überspannungsschutz kann durch eine USV nicht geleistet werden.
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? Wenn keine NEA vorhanden ist, muss das sichere Herunterfahren gewährleistet werden. [Hinweis: „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? [Hinweis: 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?

Tabelle 27: Indikator „Energieversorgung: Unterbrechungsfreie Stromversorgung“

I.27 Energieversorgung: Einsatz einer Netzersatzanlage [3.5.2]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Technische Umsetzung
Unterdomäne	Infrastruktur/Gebäude
Bezeichnung	Energieversorgung: Einsatz einer Netzersatzanlage
Kriterien	Verfügbarkeit
Kurzbeschreibung	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 Betriebsgrenzwerte mindestens der Ausführungsklasse G3 nach ISO 8528-5:2022-06 entsprechen 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	Sind an mindestens zwei georedundanten Standorten jeweils betriebsredundante oNEAs gemäß 3 vorhanden oder 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? Wurden die Betriebsgrenzwerte der eingesetzten NEAs auf Basis der technischen und betrieblichen Anforderungen des RZ individuell vorgegeben, womit die NEAs der Ausführungsklasse G4 nach ISO 8528-5:2022-06 entsprechen? Gibt es einen definierten Prozess, der sicherstellt, dass die Betriebsgrenzwerte der NEAs dauerhaft den technischen und betrieblichen Anforderungen genügen?

Tabelle 28: Indikator „Energieversorgung: Einsatz einer Netzersatzanlage“

I.28 Technischer Brandschutz des Rechenzentrums [3.5.8]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Technische Umsetzung
Unterdomäne	Infrastruktur/Gebäude
Bezeichnung	Technischer Brandschutz des Rechenzentrums
Kriterien	Verfügbarkeit; Betriebssicherheit
Kurzbeschreibung	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 baurechtliche Anforderungen hinaus.
Fragen zu 1	Wird das Rechenzentrum durch eine Brandmeldeanlage (BMA) mindestens mit lokaler Meldung überwacht und gibt es Möglichkeiten zur Bekämpfung eines Entstehungsbrandes z. B. durch Handfeuerlöscher?
Fragen zu 2	Wird das gesamte Rechenzentrum (IT-Betriebsbereich und Supportbereich) sowie dessen Umfeld durch eine BMA überwacht? Wird die Meldung der BMA auf eine angemessen reaktionsfähige hilfeleistende Stelle (Feuerwehr, Haussicherheitsdienst etc.) weitergeleitet? 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? [Hinweis: 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 reaktive Löschanlage (oder eine mindestens gleichwertige andere technische Einrichtung) vorhanden? Ist diese so ausgelegt, dass alle Bereiche (inkl. Supportbereiche) mindestens mit zwei Volllöschungen beaufschlagt oder gleichwertig behandelt werden können? [Hinweis: 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?

Tabelle 29: Indikator „Technischer Brandschutz des Rechenzentrums“

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

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Technische Umsetzung
Unterdomäne	Infrastruktur/Gebäude
Bezeichnung	Gebäudesicherheit: Schutz gegen Einbruch und Sabotage
Kriterien	Verfügbarkeit; Vertraulichkeit; Integrität; Betriebssicherheit
Kurzbeschreibung	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 bzgl. des gesamten Rechenzentrums inkl. der Supportbereiche. 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 etc.) der Widerstandsklasse RC 3 nach DIN EN 1627:2021 genügen?
Fragen zu 2	Werden mindestens alle für den ordnungsgemäßen Betrieb des RZ erforderlichen Bereiche, also auch die Supportbereiche, durch Kontrollgänge bestreift? Ist die zeitnahe Reaktion auf alle sicherheitsrelevanten Meldungen (aus der IT und der Infrastruktur, (siehe auch Indikator I.32 Monitoring der technischen Infrastruktur [3.7.1]) gewährleistet, also auch während der Kontrollgänge, sichergestellt?
Fragen zu 3	Ist eine Einbruchmeldeanlage (EMA) installiert? Werden die Meldungen der EMA rund um die Uhr an qualifiziertes Personal weitergeleitet, um eine Alarmverfolgung sicherzustellen? [Hinweis: Die Meldung der EMA muss im Moment des Angriffbeginns erfolgen und nicht erst nach Überwindung des mechanischen Widerstands.]
Fragen zu 4	Genügen alle raumbildenden Teile der Widerstandsklasse RC 4 nach DIN EN 1627:2021? Erfolgt die Meldung aus der EMA (gemäß 3) oder anderer Meldeeinrichtungen (z. B. Zaunüberwachung oder Videobewegungsmelder) unmittelbar an qualifiziertes Personal, das rund um die Uhr eine durchsetzungsfähige Reaktion sicherstellt? Ist es möglich, den Meldeort einer EMA oder anderer Meldeeinrichtungen mittels zuschaltbarer Videotechnik zum Zweck der Einsatzoptimierung einzusehen? [Hinweis: Durchsetzungsfähige Reaktion bedeutet hier, dass hinreichend ausgerüstetes und ausgebildetes Sicherheitspersonal eingreift.]
Fragen zu 5	Ist eine auf die automatische Erkennung unzulässiger Ereignisse ausgelegte Videoüberwachung der RZ-Hülle sowie der Supportbereiche mit sofortiger Meldung (entsprechend Fragen zu 4) vorhanden? 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 Substanzen)?

Tabelle 30: Indikator „Gebäudesicherheit: Schutz gegen Einbruch und Sabotage“

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

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Technische Umsetzung
Unterdomäne	Infrastruktur/Gebäude
Bezeichnung	Gebäudesicherheit: Technische/bauliche Maßnahmen zum Zutrittsschutz
Kriterien	Verfügbarkeit; Vertraulichkeit; Integrität
Kurzbeschreibung	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 und der Supporttechnik (Stromversorgung inkl. USV und NEA, Klima, Löschanlage etc.) sichergestellt, dass 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.] [Hinweis: Bei einer technisch erforderlichen Überschneidung der Bereiche (grobe/feine Technik) muss durch organisatorische Maßnahmen (z. B. Begleitung) ein zur Trennung gleichwertiger Schutz sichergestellt werden.] Ist der Zutritt zu den jeweiligen Bereichen organisatorisch und technisch in der Weise geregelt, dass im Nachgang ausreichend sicher festgestellt werden kann, wer durch die Nutzung seiner Zutrittsmittel den Zutritt wann ermöglicht hat?
Fragen zu 2	Erfolgt die Legitimationsprüfung und Freigabe des Zutritts für alle Bereiche (siehe Frage 1) durch eine Zutrittskontrollanlage mit Protokollierung der Zutritte und erfolgt bei wiederholten unberechtigten Zutrittsversuchen eine automatische Meldung oder Sperrung des verwendeten Zutrittsmittels?
Fragen zu 3	Kontrolliert die Zutrittskontrollanlage den Zu- und Austritt und erfolgt der Zutritt im Rahmen einer Zwei-Faktor-Authentifizierung mittels „Besitz und Wissen“ oder einer vergleichbaren oder besseren Lösung? [Hinweis: Besitz kann auch durch Biometrie erbracht werden. „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“)?

Tabelle 31: Indikator „Gebäudesicherheit: Technische/bauliche Maßnahmen zum Zutrittsschutz“

I.31 Sicherheit der Verzeichnisdienste [3.6.2]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Technische Umsetzung
Unterdomäne	Verzeichnisdienste
Bezeichnung	Sicherheit der Verzeichnisdienste
Kriterien	Vertraulichkeit; Integrität
Kurzbeschreibung	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	Ist die Anzahl der fehlgeschlagenen Anmeldeversuche einer einzelnen Kennung begrenzt? Meldet der Verzeichnisdienst fehlgeschlagene Anmeldeversuche oder das Erreichen der maximalen Anzahl fehlgeschlagener 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 den entsprechenden Personalverwaltungen 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?

Tabelle 32: Indikator „Sicherheit der Verzeichnisdienste“

I.32 Monitoring der technischen Infrastruktur [3.7.1]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Technische Umsetzung
Unterdomäne	Technische Überwachung
Bezeichnung	Monitoring der technischen Infrastruktur
Kriterien	Verfügbarkeit; Leistungsfähigkeit
Kurzbeschreibung	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 von 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 automatisch arbeitende Störungsmeldung/-übertragung für die wesentlichen Infrastrukturkomponenten (z. B. Strom, Klima, 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 mit einfachen Mitteln (z. B. einfache Werkzeuge wie Schraubendreher, Seitenschneider oder Multitool)? [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?

Tabelle 33: Indikator „Monitoring der technischen Infrastruktur“

I.33 Monitoring auf IT-Sicherheitsvorfälle / Logging [3.7.2]

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Technische Umsetzung
Unterdomäne	Technische Überwachung
Bezeichnung	Monitoring auf IT-Sicherheitsvorfälle / Logging
Kriterien	Vertraulichkeit; Integrität
Kurzbeschreibung	Bei diesem Indikator geht es um die technische Überwachung von Vorfällen unter besonderer Berücksichtigung von IT-Sicherheitsvorfälle, welche 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 I.34 Monitoring der IT-Komponenten und -Dienste auf Verfügbarkeit [3.7.3] 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? Ist dieser Zeitraum ausreichend, um Vorfälle angemessen aufzuklären?
Fragen zu 2	Melden die IT-Systeme sicherheitsrelevante Vorgänge an zentrale Systeme zur Speicherung? 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, die Auswertung der Daten und die Reaktion auf Abweichungen 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 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?

Tabelle 34: Indikator „Monitoring auf IT-Sicherheitsvorfälle / Logging“

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

Eigenschaft	*Ausprägung der Eigenschaft des Indikators*
Domäne	Technische Umsetzung
Unterdomäne	Technische Überwachung
Bezeichnung	Monitoring der IT-Komponenten und -Dienste auf Verfügbarkeit
Kriterien	Verfügbarkeit
Kurzbeschreibung	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 Netzwerk-Monitoring 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? 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?

Tabelle 35: Indikator „Monitoring der IT-Komponenten und -Dienste auf Verfügbarkeit“

Anhang

A.1 Herleitung des HVB-kompakt aus dem HVB

In diesen Tabellen wird dargestellt, welche Indikatoren aus dem HVB ausgewählt worden sind, um die für den Bericht an den HHA festgelegten Kategorien (I. - IV.) und Unterkategorien (I. a - IV. f) abdecken zu können. Diese Indikatoren aus dem HVB bilden den HVB-kompakt.

I. Kategorie: Informationssicherheitsmanagement

Nr.	***Unterkategorie für den HHA-Bericht***	***Nr. der Indikatoren aus dem HVB-kompakt, die die jeweilige Unterkategorie abdecken***
I. a	Informationssicherheitsmanagementsystem (ISMS)	1
I. b	Risikomanagement	2
I. c	Notfallvorsorge	3, 8
I. d	Personalmanagement	4
I. e	Sicherheitskonzepte	10, 11, 13, 14

Tabelle 36: Kategorie: Informationssicherheitsmanagement – Zuordnung der Indikatoren

II. Kategorie: Cybersicherheit

Nr.	***Unterkategorie für den HHA-Bericht***	***Nr. der Indikatoren aus dem HVB-kompakt, die die jeweilige Unterkategorie abdecken***
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

Tabelle 37: Kategorie: Cybersicherheit – Zuordnung der Indikatoren

III. Kategorie: Kryptosicherheit

Nr.	***Unterkategorie für den HHA-Bericht***	***Nr. der Indikatoren aus dem HVB-kompakt, die die jeweilige Unterkategorie abdecken***
III. a	Vertraulichkeit und Integrität beim Datentransport	12, 21, 31
III. b	Vertraulichkeit und Integrität der gespeicherten Daten	12, 31

Tabelle 38: Kategorie: Kryptosicherheit – Zuordnung der Indikatoren

IV. Kategorie: Physische Sicherheit

Nr.	***Unterkategorie für den HHA-Bericht***	***Nr. der Indikatoren aus dem HVB-kompakt, die die jeweilige Unterkategorie abdecken***
IV. a	Redundanz	18
IV. b	Baulich-technische Grundlagen	5
IV. c	Stromversorgung	5, 26, 27

Nr.	*Unterkategorie für den HHA-Bericht*	*Nr. der Indikatoren aus dem HVB-kompakt, die die jeweilige Unterkategorie abdecken*
IV. d	Zutritts-, Einbruch- und Sabotageschutz	5, 29, 30
IV. e	Brandschutz	5, 28
IV. f	Monitoring	32

Tabelle 39: Kategorie: Physische Sicherheit – Zuordnung der Indikatoren

Übersicht der Indikatoren des HVB-kompakt

Die nachfolgende Übersicht zeigt die umgekehrte Richtung, d. h. die Abbildung der 34 Indikatoren des HVB-kompakt auf die vier Darstellungskategorien für den Bericht an den HHA:

Domäne	*Nr.*	*Indikator im HVB-kompakt (in eckigen Klammern: Nr. des Indikators im HVB)*	*Kategorien[10] für HHA-Bericht*
Management	1	Informationssicherheitsmanagementsystem (ISMS) [1.1.3]	ISM
	2	Risikomanagement im Zusammenhang mit der IT-Dienstleistungserbringung [1.1.8]	ISM
	3	Notfall- und Krisenmanagement [1.1.10]	ISM
	4	Verfahren zur Einhaltung rechtlicher und organisatorischer Vorgaben durch das Personal [1.2.3]	ISM
	5	Infrastruktur, Grundlagen und Planung [1.3.1]	PS
IT-Steuerung	6	Availability Management (Verfügbarkeitsmanagement): Messung und Steuerung der Verfügbarkeit [2.1.4]	CS
	7	Capacity Management (Kapazitätsmanagement): Messung und Steuerung der Kapazität [2.1.7]	CS
	8	IT-Service Continuity Management: IT-Notfallplanung (ITSCM-Rahmenwerk) [2.1.9]	ISM, CS
	9	IT-Service Continuity Management: Datensicherungen [2.1.12]	CS
	10	IT-Sicherheitskonzepte: Mandantentrennung [2.1.14]	ISM
	11	IT-Sicherheitskonzepte: ID- und Rechtemanagement [2.1.15]	ISM
	12	IT-Sicherheitskonzepte: Kryptografie [2.1.16]	KS
	13	IT-Sicherheitskonzepte: Sichere Datenlöschung und Aussonderung [2.1.17]	ISM
	14	IT-Sicherheitskonzepte: Schutz gegen Schadprogramme und netzbasierte Angriffe [2.1.19]	ISM
	15	Incident Management: Sicherheitsvorfallbehandlung [2.3.7]	CS
	16	Patch- und Releasemanagement (Software) [2.4.4]	CS
	17	Trennung von Entwicklungs-, Test- und Produktionsumgebungen [2.4.5]	CS

[10] ISM = Informationssicherheitsmanagement; CS = Cybersicherheit; KS = Kryptosicherheit; PS = Physische Sicherheit

Domäne	*Nr.*	*Indikator im HVB-kompakt (in eckigen Klammern: Nr. des Indikators im HVB)*	*Kategorien[10] für HHA-Bericht*
Technische Umsetzung	18	Ausfallsicherheit/Redundanzkonzept [3.1.1]	CS, PS
	19	Netzwerk-Segmentierung [3.2.2]	CS
	20	Sicherheit der aktiven Netzwerkkomponenten [3.2.3]	CS
	21	Ausgestaltung der WAN-Anbindung zwischen den IT-Standorten [3.2.6]	CS, KS
	22	Sicherheit der Internet-Anbindung [3.2.8]	CS
	23	Server-Sicherheit [3.3.1]	CS
	24	Datensicherheit der Speicher [3.4.2]	CS
	25	Datenreplikation und -sicherung [3.4.3]	CS
	26	Energieversorgung: Unterbrechungsfreie Stromversorgung [3.5.1]	PS
	27	Energieversorgung: Einsatz einer Netzersatzanlage [3.5.2]	PS
	28	Technischer Brandschutz des Rechenzentrums [3.5.8]	PS
	29	Gebäudesicherheit: Schutz gegen Einbruch und Sabotage [3.5.10]	PS
	30	Gebäudesicherheit: Technische/bauliche Maßnahmen zum Zutrittsschutz [3.5.11]	PS
	31	Sicherheit der Verzeichnisdienste [3.6.2]	CS, KS
	32	Monitoring der technischen Infrastruktur [3.7.1]	PS
	33	Monitoring auf IT-Sicherheitsvorfälle / Logging [3.7.2]	CS
	34	Monitoring der IT-Komponenten und -Dienste auf Verfügbarkeit [3.7.3]	CS

Tabelle 40: Übersicht der Indikatoren des HVB-kompakt und Abbildung auf die vier Darstellungskategorien für den Bericht an den HHA

A.2 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 oder 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	Die 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 die Prozesse sind Ziele im Einvernehmen mit den beteiligten Akteuren entwickelt und operationalisiert. Die Definition der Prozesse 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 jeweilige 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 41: Allgemeine Beschreibung der fünf Reifegrade zur Bewertung von organisatorischen Prozessen

A.3 Potenzialstufen

Allgemeine Beschreibung der fünf Potenzialstufen zur Bewertung technischer Umsetzungen:

Stufe	*Potenzialstufe*	*Beschreibung der Potenzialstufe anhand von Beispielen*
1	Normale (d. h. keine außergewöhnlichen) Anforderungen an die Verlässlichkeit der IT (die bei den Potenzialstufen im Wesentlichen durch die Verfügbarkeit bestimmt wird)	• 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	• Redundanzen bei den wesentlichen Komponenten • Definiertes Notfallkonzept für gefährdete Bestandteile der IT, basierend auf dem Ergebnis von Risikoanalysen (z. B. BSI-Standard 200-3) • Verbesserte Härtung von Komponenten (minimalisiert auf die zugedachte Funktionalität) • Räumliche Trennung • Umfassendes Logging / technische Protokollierung
3	Sehr hohe Anforderungen an die Verlässlichkeit der IT	• Vollständig ausgebaute Redundanzen mit gleicher Kapazität • Strenge Limitierung von Zutritt, Zugang und Zugriff (z. B. Anzahl und Dauer von Anmeldungen an Dienste/Administrationssoftware) • Regelmäßige Überprüfung von technischen Komponenten und Protokollen • Fehlertolerante IT (z. B. NEA-gestützt gegen Stromausfälle) • Früherkennung von Störungen • Externe Auslagerung von Datensicherungen • Automatismen / automatisch ablaufende Regelmechanismen zum Ausgleich von Störungen (z. B. Wiederanlauf nach einem Stromausfall) • Getrennte brandgeschützte Bereiche
4	Höchste Anforderungen an die Verlässlichkeit der IT	• Geo-Redundanz: RZ sollen räumlich so weit voneinander entfernt aufgebaut sein, dass selbst ein weiträumiges Großschadensereignis nicht gleichzeitig oder zeitnah mehrere RZ einer Georedundanzgruppe treffen kann (Details: siehe Dokument „RZ-Standortkriterien“).[11] • Ständige Überwachung • Kurze Reaktionszeiten auf Störungen
5	Desaster-tolerant (Desaster-tolerant bedeutet, die IT muss auch in Ausnahmesituationen und unter Extrembedingungen (z. B. bei „höherer Gewalt") verlässlich funktionieren.)	• Geo- und Wartungsredundanz, so dass ein geplantes Abschalten einer Komponente (u. a. zu Wartungszwecken) jederzeit möglich ist (z. B. Austausch von Komponenten im laufenden Betrieb), ohne dass der Ausfall einer weiteren Komponente zum Ausfall des Dienstes führt • Mechanismen zur Überbrückung von längeren Ausfallereignissen (z. B. mehrtägiger, regionaler Stromausfall) • Sabotage-geschützte Leitungen

Tabelle 42: Allgemeine Beschreibung der fünf Potenzialstufen zur Bewertung technischer Umsetzungen

[11] Dokument „RZ-Standortkriterien“ ist abrufbar unter: https://www.bsi.bund.de/dok/RZ-Standortkriterien.

Anlage 2: Sollwertermittlung

Im Folgenden wird eine mögliche Methode zur Ermittlung individueller Sollwerte für ein Rechenzentrum oder für eine IT-Dienstleistung auf der Basis des HVB-kompakt vorgestellt. Diese Methode ist lediglich als Vorschlag und Hilfestellung anzusehen. Damit ist weder der Anspruch verbunden, dies sei die einzig zulässige Methode, noch, dass genau diese Methode anzuwenden wäre.

Schritt 0:

Die zu betrachtenden Sicherheitsaspekte sind durch die Indikatoren des HVB-kompakt vorgegeben.

Schritt 1:

Es sind die Sicherheitskonzepte der eigenen Institution zu identifizieren (oder festzulegen), die von den in Schritt 0 betrachteten Sicherheitsaspekten betroffen sind.

Schritt 2:

Die betroffenen Sicherheitskonzepte werden zumindest bezüglich der zu betrachtenden Sicherheitsaspekte (siehe Schritt 0) ausformuliert. Dabei sind die in den Indikatoren genannten Maßnahmen sinnvolle Anhaltspunkte. Die Herleitung dem Schutzbedarf angemessener Maßnahmen erfolgt aus den Standardwerken der Informationssicherheit insbesondere dem IT-Grundschutz und den Mindeststandards nach § 8 Abs. 1 Satz 1 BSIG.

Schritt 3:

Danach wird der HVB-kompakt fiktiv auf die im Schritt 2 ausgearbeiteten IT-Sicherheitskonzepte (inkl. Maßnahmen) angewendet. Dadurch wird ermittelt, welcher der jeweils fünf Reifegrade/Potenzialstufen für jeden Indikator mit Hilfe der IT-Sicherheitskonzepte erreicht würde.

[Hinweis: Wie auch bei der Ist-Wert-Feststellung gilt, dass die im HVB-kompakt genannten Maßnahmen der Veranschaulichung des Sicherheitsniveaus dienen. Gleich- oder höherwertige Maßnahmen aus den Standardwerken sind selbstverständlich zulässig.]

Schritt 4:

Die so ermittelten Reifegrade/Potenzialstufen stellen für jeden Indikator den zu erreichenden Sollwert für das zu untersuchende Rechenzentrum oder die zu untersuchende IT-Dienstleistung dar.