Bundesamt
für Sicherheit in der
Informationstechnik

Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen

Hinweise zur Umsetzung der Kriterien des § 8a Absatz 1 BSIG für die Beurteilung der Informationssicherheit bei Betreibern Kritischer Infrastrukturen

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
0.9	20.12.2019	BSI	Konsolidierung im BSI
1.0	28.02.2020	BSI	Finale Abstimmung im BSI, Herstellung der Barrierefreiheit des Dokuments

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582- 0
E-Mail: kritische.infrastrukturen@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Einleitung

1.1 Zielsetzung und Adressatenkreis

Das vorliegende Dokument bietet Betreibern Kritischer Infrastrukturen (KRITIS-Betreibern) und prüfenden Stellen eine Konkretisierung der Anforderungen des § 8a Absatz 1 BSIG. Zudem stellt der Anforderungskatalog den prüfenden Stellen geeignete Kriterien für eine sachgerechte Prüfung der eingesetzten Sicherheitsvorkehrungen vor, um die geforderten Nachweise gemäß § 8a Absatz 3 BSIG erbringen zu können.

Die nachfolgend dargestellten Anforderungen dienen KRITIS-Betreibern als Orientierungsmaßstab und Hilfestellung bei der Auswahl, Umsetzung und Prüfung der von ihnen gemäß § 8a Absatz 1 BSIG umzusetzenden Sicherheitsvorkehrungen, zu der gleichwertige Alternativen bestehen können. Dieser Anforderungskatalog stellt damit kein verbindliches Kriterium im Sinne des § 8a Absatz 5 BSIG dar.

1.2 Einheitliche Anforderungen

Mit diesem Anforderungskatalog soll den KRITIS-Betreibern und prüfenden Stellen ein besseres Verständnis über die Sichtweise des BSI ermöglicht werden. Die Anforderungen basieren auf dem bekannten „Anforderungskatalog Cloud-Computing (C5)“ [C5]. Die dort formulierten Anforderungen wurden an die spezifischen KRITIS-Aspekte angepasst und, soweit es nötig war, um weitere Anforderungen ergänzt bzw. gekürzt. Die Herkunft der C5-Anforderungen wurde transparent im Anforderungskatalog referenziert, so dass für KRITIS-Betreiber ein Vergleich mit den eigenen Grundlagen zur Absicherung der Kritischen Infrastruktur möglich ist und Mehrfachprüfungen vermieden werden können.

Das vorliegende Dokument stellt einen sachgerechten Ausgangspunkt dar, um die Anforderungen gemäß § 8a Absatz 1 BSIG zu konkretisieren. Dennoch obliegt es dem Betreiber sowie der prüfenden Stelle, für den konkreten Anwendungsfall zu entscheiden, ob diese Anforderungen im Rahmen der Organisation passend sind oder ob zusätzliche, weiterführende Anforderungen notwendig wären.

1.3 Dankesworte

Dieser Anforderungskatalog wurde in Zusammenarbeit mit dem Fachausschuss für Informationstechnologie (FAIT) des Instituts der Wirtschaftsprüfer in Deutschland e. V. (IDW) auf Basis des C5 2016 entwickelt. Das BSI bedankt sich für die angenehme und gelungene Zusammenarbeit mit den Mitgliedern der Arbeitsgruppe „IT-Sicherheitsgesetz“ des FAIT.

1.4 Weiterführende Informationen

Weiterführende Informationen und beispielhafte Prüfungshandlungen für eine sachgerechte Prüfung auf Grundlage dieses Anforderungskatalogs enthält der IDW Prüfungshinweis: Die Prüfung der von Betreibern Kritischer Infrastrukturen gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen (IDW PH 9.860.2).

Weitere Informationen für eine geeignete Umsetzung der Anforderungen des § 8a Absatz 1 BSIG können entnommen werden:

- der Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG [OH1],
- der Orientierungshilfe zu branchenspezifischen Sicherheitsstandards (B3S) gemäß § 8a Absatz 2 BSIG [OH2],
- Branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a Absatz 2 BSIG, deren Eignung vom BSI festgestellt wurde,
- den einschlägigen Standards (z. B. Zertifizierungsschemata für ISO/IEC 27001 (nativ oder auf Basis von IT-Grundschutz), ISO/IEC 17021-1, ISO/IEC 27006) [GS, ISO1, ISO2, ISO3].

1.5 Referenzen

[C5] Anforderungskatalog Cloud Computing (C5), C5:2016, BSI
https://www.bsi.bund.de/dok/452180

[IDW] IDW PH 9.860.2, IDW

[ISO1] ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements, International Organization for Standardization, 2013

[ISO2] ISO/IEC 17021-1, International Organization for Standardization

[ISO3] ISO/IEC 27006, International Organization for Standardization

[GS] IT-Grundschutz, BSI
https://www.bsi.bund.de/dok/128656

[OH2] Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a Absatz 2 BSIG, BSI
https://www.bsi.bund.de/dok/126544

[OH1] Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG, BSI
https://www.bsi.bund.de/OHNachweise

2 Anforderungskatalog zur Konkretisierung der Kriterien des § 8a Absatz 1 BSIG

2.1 Informationssicherheitsmanagementsystem (ISMS)

Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Grundlage
1.	**Managementsystem für Informationssicherheit** Die Unternehmensleitung initiiert, steuert und überwacht ein Managementsystem zur Informationssicherheit (ISMS), das sich an etablierten Standards orientiert. Bei Anwendung der ISO 2700x-Reihe muss die Erklärung zur Anwendbarkeit (Statement of Applicability) die IT-Prozesse zu Entwicklung und Betrieb der kritischen Dienstleistung umfassen. Die hierzu eingesetzten Grundsätze, Verfahren und Maßnahmen ermöglichen eine nachvollziehbare Lenkung der folgenden Aufgaben und Aktivitäten zur dauerhaften Aufrechterhaltung der organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse zu Entwicklung und Betrieb der kritischen Dienstleistung und umfasst: • die Planung und Durchführung des Vorhabens, • Erfolgskontrolle bzw. Überwachung der Zielerreichung und • Beseitigung von erkannten Mängeln und Schwächen sowie kontinuierliche Verbesserung.	OIS-01
2.	**Strategische Vorgaben zur Informationssicherheit und Verantwortung der Unternehmensleitung** Eine Informationssicherheitsleitlinie mit Sicherheitszielen und strategischen Vorgaben, wie diese Ziele erreicht werden sollen, ist dokumentiert. Die Sicherheitsziele leiten sich von den Unternehmenszielen und Geschäftsprozessen, relevanten Gesetzen und Verordnungen sowie der aktuellen und zukünftig erwarteten Bedrohungsumgebung in Bezug auf Informationssicherheit ab. Die strategischen Vorgaben stellen grundlegende Rahmenbedingungen dar, die in weiteren Richtlinien und Anweisungen näher spezifiziert werden. Die Informationssicherheitsleitlinie wird von der Unternehmensleitung verabschiedet und an alle betroffenen internen und externen Parteien der kritischen Dienstleistung kommuniziert.	OIS-02

2.1 Informationssicherheitsmanagementsystem (ISMS)

3.	**Zuständigkeiten und Verantwortungen im Rahmen der Informationssicherheit** Die Verantwortlichkeiten, Pflichten sowie die Schnittstellen zum Melden von Sicherheitsvorfällen und Störungen sind definiert, dokumentiert, zugewiesen und an alle betroffenen internen und externen Parteien (z. B. Unterauftragnehmer des KRITIS-Betreibers der kritischen Dienstleistung) kommuniziert. Seitens des KRITIS-Betreibers sind mindestens die folgenden Rollen (oder vergleichbare Äquivalente) in der Informationssicherheitsleitlinie oder zugehörigen Richtlinien beschrieben und entsprechende Verantwortlichkeiten zugewiesen: • IT-Leiter (CIO) • IT-Sicherheitsbeauftragter (CISO) • Beauftragter für die Behandlung von IT-Sicherheitsvorfällen (z. B. CERT-Leiter). Veränderungen an Verantwortlichkeiten und Schnittstellen werden intern und extern so zeitnah kommuniziert, dass alle mit organisatorischen und technischen Maßnahmen betroffenen internen und externen Parteien angemessen darauf reagieren können, bevor die Änderungen wirksam werden. Der KRITIS-Betreiber identifiziert sämtliche Risiken im Zusammenhang mit überlappenden oder inkompatiblen Zuständigkeiten und Verantwortungen.	OIS-03
4.	**Funktionstrennung** Es existieren angemessene Vorgaben und Anweisungen zu organisatorischen und technischen Kontrollen, um die Trennung von Rollen und Verantwortlichkeiten („Separation of Duties“/Funktionstrennung), die hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen im Zusammenhang mit der kritischen Dienstleistung nicht miteinander vereinbar sind, zu gewährleisten (z. B. in Stellenbeschreibungen, Prozessbeschreibungen, SOD-Matrizen, etc.). Die Vorgaben adressieren insb. die folgenden Bereiche (Beispiele): • Administration von Rollen, Genehmigung und Zuweisung von Zugriffsberechtigungen für Benutzer unter Verantwortung des KRITIS-Betreibers • die Entwicklung und Implementierung von Änderungen an der kritischen Dienstleistung sowie die Wartung der für die kritische Dienstleistung relevanten physischen und logischen IT-Infrastruktur (Netzwerke, Betriebssysteme, Datenbanken) und der IT-Anwendungen • den Betrieb und die Überwachung des Betriebs der kritischen Dienstleistungen. Operative und kontrollierende Funktionen sollten nicht von einer Person gleichzeitig wahrgenommen werden dürfen. Kann aus organisatorischen oder technischen Gründen keine Funktionstrennung erreicht werden, sind angemessene kompensierende Kontrollen eingerichtet, um missbräuchliche Aktivitäten zu verhindern oder aufzudecken. Vorhandene Funktionstrennungskonflikte und die dazu eingerichteten kompensierenden Kontrollen nachvollziehbar dokumentiert (z. B. in einem Rollen- und Rechtekonzept), um eine Beurteilung über die Angemessenheit und Wirksamkeit dieser Kontrollen zu ermöglichen.	OIS-04

2.2 Asset Management

Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Grundlage (C5 #)
5.	**Asset Inventar** Die zur Erbringung der kritischen Dienstleistung eingesetzten IT-Systeme und Komponenten (Assets) wie z. B. PCs, Peripheriegeräte, Telefone, Netzwerkkomponenten, Server, Installationsdokumentationen, Verfahrensanweisungen, IT-Anwendungen u. Werkzeuge sind identifiziert und inventarisiert. Durch angemessene Vorkehrungen und Maßnahmen wird sichergestellt, dass dieses Inventar vollständig, richtig, aktuell und konsistent bleibt. Änderungen an den Einträgen im Inventar werden nachvollziehbar historisiert. Soweit hierzu keine wirksamen Automatismen eingerichtet sind, wird dies durch regelmäßig stattfindende manuelle Überprüfung der Inventardaten des Assets sichergestellt.	AM-01
6.	**Zuweisung von Asset Verantwortlichen** Sämtliche inventarisierten Assets mit Relevanz für die Erbringung der kritischen Dienstleistung sind einem Verantwortlichen auf Seiten des Betreibers der kritischen Dienstleistung zugewiesen. Die Verantwortlichen des Betreibers sind über den kompletten Lebenszyklus der Assets dafür zuständig, dass diese vollständig inventarisiert und richtig klassifiziert sind.	AM-02
7.	**Nutzungsanweisungen für Assets** Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für den ordnungsgemäßen Umgang mit Assets, die für die Erbringung der kritischen Dienstleistung relevant sind und gemäß der Informationssicherheitsrichtlinie dokumentiert, kommuniziert und in der jeweils aktuellsten Version bereitgestellt werden.	AM-03
8.	**Ab- und Rückgabe von Assets** Alle internen und externen Mitarbeiter des Betreibers der kritischen Dienstleistung sind verpflichtet, sämtliche Assets, die Ihnen in Bezug auf die kritische Dienstleistung ausgehändigt wurden bzw. für die sie verantwortlich sind, zurückzugeben oder unwiderruflich zu löschen sobald das Beschäftigungsverhältnis beendet ist.	AM-04
9.	**Klassifikation von Informationen** Der Betreiber der kritischen Dienstleistung verwendet eine einheitliche Klassifizierung von Informationen und Assets, die für die Entwicklung und Erbringung der kritischen Dienstleistung relevant sind. Das Klassifizierungsschema basiert auf einer Risikoanalyse und Folgeabschätzung (4.4.3).	AM-05
10.	**Kennzeichnung von Informationen und Handhabung von Assets** Zu dem umgesetzten Klassifizierungsschema von Informationen und Assets existieren Arbeitsanweisungen und Prozesse, um die Kennzeichnung von Informationen, sowie die entsprechende Behandlung von Assets zu gewährleisten.	AM-06

2.2 Asset Management

11.	**Verwaltung von Datenträgern** Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für den sicheren Umgang mit Assets sind gemäß der IT-Sicherheitsrichtlinie dokumentiert, kommuniziert und bereitgestellt. Die Vorgaben stellen einen Bezug zur Klassifikation von Informationen her. Sie umfassen die sichere Verwendung, den sicheren Transport sowie die unwiederbringliche Löschung und Vernichtung von Datenträgern.	AM-07
12.	**Überführung und Entfernung von Assets** Geräte, Hardware, Software oder Daten dürfen nur nach erfolgter Genehmigung durch autorisierte Gremien oder Stellen des Betreibers der Kritischen Infrastruktur in externe Räumlichkeiten überführt werden. Die Überführung findet auf sicherem Wege statt, entsprechend der Art des zu überführenden Assets.	AM-08

2.3 Risikoanalysemethode

Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Grundlage (C5 #)
13.	**Richtlinie für die Organisation des Risikomanagements** Richtlinien und Anweisungen über das grundsätzliche Verfahren zur Identifikation, Analyse, Beurteilung und Behandlung von Risiken und insb. IT-Risiken, die zu Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der für die Erbringung der kritischen Dienstleistung notwendigen informationstechnischen Systeme führen, sind dokumentiert, kommuniziert und bereitgestellt.	OIS-06
14.	**Identifikation, Analyse, Beurteilung und Folgeabschätzung von IT-Risiken** Die Verfahren zur Identifikation, Analyse, Beurteilung und Behandlung von Risiken, einschließlich der für die Erbringung der kritischen Dienstleistung relevanten IT-Risiken, werden mindestens jährlich durchlaufen, um interne und externe Veränderungen und Einflussfaktoren zu berücksichtigen. Die identifizierten Risiken werden gemäß den Maßnahmen des Risikomanagements nachvollziehbar dokumentiert, bewertet und mit mitigierenden Maßnahmen versehen. Vorgaben der Unternehmensleitung für den Risikoappetit und die Risikotoleranzen sind in der Richtlinie für das Risikomanagement oder einem vergleichbar verbindlichen Dokument enthalten. Dies schließt Folgeabschätzungen der Risiken für die Nutzer der kritischen Dienstleistung ein. Die Unternehmensleitung wird mindestens quartalsweise und in angemessener Form über den Status der identifizierten Risiken und mitigierender Vorkehrungen und Maßnahmen informiert.	OIS-07

2.3 Risikoanalysemethode

15.	**Richtlinien zur Folgeabschätzung** Richtlinien und Anweisungen zum Ermitteln von Auswirkungen etwaiger Störungen der kritischen Dienstleistung sind dokumentiert, kommuniziert und bereitgestellt. Mindestens die folgenden Aspekte werden dabei berücksichtigt: • Analysen in Bezug auf Komponenten, deren Ausfall den Ausfall der gesamten Anlage auslösen kann („Single Point of Failure“) • Berücksichtigung einer Änderung der allgemeinen und branchenspezifischen Gefährdungslage • Mögliche Szenarien basierend auf einer Risikoanalyse (z. B. Ausfall von Personal, Gebäude, Infrastruktur und Dienstleister) • Identifizierung von Richtlinien und Anweisungen zu notwendigen Produkten und Dienstleistungen • Identifizierung von Abhängigkeiten, einschließlich der Prozesse (inkl. dafür benötigter Ressourcen), Anwendungen, Geschäftspartner und Dritter • Erfassung von Bedrohungen gegenüber der kritischen Dienstleistung • Ermittlung von Auswirkungen resultierend aus geplanten und ungeplanten Störungen und den Veränderungen im Laufe der Zeit auf die kritische Dienstleistung • Feststellung der maximal vertretbaren Dauer von Störungen bevor die Mindestqualität der kritischen Dienstleistung erreicht ist • Feststellung der Prioritäten zur Wiederherstellung • Feststellung zeitlicher Zielvorgaben zur Wiederaufnahme der kritischen Dienstleistung innerhalb des maximal vertretbaren Zeitraums (RTO) • Feststellung zeitlicher Vorgaben zum maximal vertretbaren Zeitraum, in dem Daten verloren und nicht wiederhergestellt werden können (RPO) • Abschätzung der zur Wiederaufnahme benötigten Ressourcen.	BCM-02

2.3 Risikoanalysemethode

16.	**Maßnahmenableitung** Es sind Richtlinien definiert, die die Ableitung von Maßnahmen und deren Überwachung regeln. Dies beinhaltet, dass die identifizierten IT-Risiken im Zusammenhang mit der kritischen Dienstleistung gemäß den Vorgaben des Risikomanagements nachvollziehbar mit Maßnahmen versehen werden, um die IT-Risiken zu reduzieren. Dabei ist zu berücksichtigen, dass gegenüber allgemeinen Risikomanagementansätzen ein unbehandeltes Risiko durch eigenständige dauerhafte Risikoakzeptanz durch den Betreiber oder Versicherung gegen Risiken in der Regel keine zulässige Option im Sinne des BSIG ist. Der Status der Maßnahmenumsetzung und der damit einhergehenden Veränderung der Risikobewertung wird überwacht und regelmäßig an die relevanten Stakeholder berichtet. Auch bei Outsourcing o. Ä. verbleibt die volle Verantwortung für eine geeignete Risikobehandlung beim Betreiber.	B3S

2.4 Continuity Management

Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Grundlage (C5 #)
17.	**Verantwortung der gesetzlichen Vertreter des Betreibers der Kritischen Infrastruktur** Die gesetzlichen Vertreter des Betreibers der Kritischen Infrastruktur haben einen Prozessverantwortlichen (bspw. ein Mitglied der Unternehmensleitung) für Kontinuitäts- und Notfallmanagement benannt, der für die Etablierung der Prozesse und die Einhaltung der Leitlinien verantwortlich ist. Von dieser Verantwortung ist umfasst, dass ausreichende Ressourcen für einen geordneten Betrieb bereitgestellt werden. Personen in der Unternehmensleitung und anderen relevanten Führungspositionen demonstrieren Führung und Engagement in Bezug auf dieses Thema, indem sie beispielsweise die Mitarbeiter dazu auffordern beziehungsweise ermutigen, zu der Effektivität des Kontinuitäts- und Notfallmanagements aktiv beizutragen.	BCM-01
18.	**Planung der Betriebskontinuität** Basierend auf der Folgeabschätzung wird ein verbindliches Rahmenwerk zur Planung der Kontinuität der für die kritische Dienstleistung notwendigen IT-Systeme (einschließlich von Notfallplänen) eingeführt, dokumentiert und angewendet, das eine konsistente Vorgehensweise (z. B. an verschiedenen Standorten der Anlagen) sicherstellt. Diese Planung berücksichtigt etablierte Standards, die in einem „Statement of Applicability“ nachvollziehbar festgelegt sind. Pläne zur Kontinuität der kritischen Dienstleistung berücksichtigen dabei folgende Aspekte: • Definierter Zweck und Umfang unter Beachtung der relevanten Abhängigkeiten • Zugänglichkeit und Verständlichkeit der Pläne für Personen, die danach handeln sollen • Eigentümerschaft durch mindestens eine benannte Person, die für die Überprüfung, Aktualisierung und Genehmigung zuständig ist • Festgelegte Kommunikationswege, Rollen und Verantwortlichkeiten • Wiederherstellungsverfahren, manuelle Übergangslösungen und Referenzinformationen (unter Berücksichtigung der Priorisierung bei der Wiederherstellung der kritischen Dienstleistung • Methoden zur Inkraftsetzung der Pläne • Kontinuierlicher Verbesserungsprozess der Pläne • Schnittstellen zum Security Incident Management.	BCM-03

2.4 Continuity Management

19.	**Verifizierung, Aktualisierung und Test der Betriebskontinuität** Die Folgeabschätzung sowie die Pläne zur Kontinuität der kritischen Dienstleistung und Notfallpläne werden regelmäßig (mindestens jährlich) oder nach wesentlichen organisatorischen oder umgebungsbedingten Veränderungen überprüft, aktualisiert und getestet. Tests beziehen betroffene relevante Dritte (z. B. kritische Lieferanten) mit ein z. B. in Form von: • Internen Übungen und Systemtests • Übungen mit externen Partnern, insb. aus dem Kontext der kritischen Dienstleistung • Übungen im Rahmen des Notfallmanagements • Kommunikationsübungen • Planübungen, Krisenübungen, Training seltener Ereignisse. Die Tests werden dokumentiert und Ergebnisse werden für zukünftige Maßnahmen der Kontinuität der kritischen Dienstleistung berücksichtigt.	BCM-04

2.5 Technische Informationssicherheit

Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Grundlage (C5 #)
20.	**Notwendige/ausreichende Personal- und IT-Ressourcen (Betrieb und IT-Sicherheit)** Die Planung von Kapazitäten und Ressourcen (Personal und IT-Ressourcen) folgt einem etablierten Verfahren, um mögliche Kapazitätsengpässe zu vermeiden. Die Verfahren umfassen Prognosen von zukünftigen Kapazitätsanforderungen, um Nutzungstrends zu identifizieren und Risiken der Systemüberlastung zu beherrschen. Technische und organisatorische Maßnahmen zur Überwachung und Provisionierung bzw. De-Provisionierung bei KRITIS-Betreiber sind definiert. Dadurch stellt der Betreiber sicher, dass Ressourcen bereitgestellt bzw. Leistungen gemäß der vertraglichen Vereinbarung erbracht werden und die Einhaltung der Dienstgütevereinbarungen sichergestellt ist.	RB-01 RB-02
21.	**Schutz vor Schadprogrammen** Die logischen und physischen IT-Systeme, die der Betreiber zur Erbringung der kritischen Dienstleistung verwendet sowie die Perimeter des Netzwerks, die dem Verantwortungsbereich des KRITIS-Betreibers unterliegen, sind mit Virenschutz- und Reparaturprogrammen versehen, die eine signatur- und verhaltensbasierte Erkennung und Entfernung von Schadprogrammen ermöglichen. Die Programme werden gemäß den vertraglichen Vereinbarungen mit dem/n Hersteller/n, mindestens aber täglich aktualisiert.	RB-05
22.	**Datensicherung und Wiederherstellung** Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen zum Vermeiden von Datenverlusten sind gemäß IT-Sicherheitsrichtlinie dokumentiert, kommuniziert und bereitgestellt. Diese sehen zuverlässige Verfahren für die regelmäßige Sicherung (Backup sowie ggf. Snapshots) und Wiederherstellung von Daten (Restore) vor. Umfang, Häufigkeit und Dauer der Aufbewahrung entsprechen den Anforderungen der kritischen Dienstleistung. Der Zugriff auf die gesicherten Daten ist auf autorisiertes Personal beschränkt. Wiederherstellungsprozeduren beinhalten Kontrollmechanismen, die sicherstellen, dass Wiederherstellungen ausschließlich nach Genehmigung durch hierfür autorisierte Personen gemäß den internen Richtlinien erfolgen.	RB-06 RB-09
23.	**Datensicherung und Wiederherstellung – Überwachung** Die Ausführung der Datensicherung wird durch technische und organisatorische Maßnahmen überwacht. Störungen werden durch qualifizierte Mitarbeiter untersucht und zeitnah behoben, um die Einhaltung der Anforderungen in Bezug auf Umfang, Häufigkeit und Dauer der Aufbewahrung zu gewährleisten.	RB-07

2.5 Technische Informationssicherheit

24.	**Datensicherung und Wiederherstellung – Regelmäßige Tests** Sicherungsdatenträger und Wiederherstellungsverfahren sind von qualifizierten Mitarbeitern regelmäßig mit dedizierten Testmedien zu prüfen. Die Tests sind so gestaltet, dass die Verlässlichkeit der Sicherungsdatenträger und die Wiederherstellungszeit mit hinreichender Sicherheit überprüft werden kann. Die Tests werden durch qualifizierte Mitarbeiter durchgeführt und die Ergebnisse nachvollziehbar dokumentiert. Auftretende Fehler werden zeitnah behoben.	RB-08
25.	**Umgang mit Schwachstellen, Störungen und Fehlern – System-Härtung** Systemkomponenten, welche für die Erbringung der kritischen Dienstleistung verwendet werden, sind gemäß allgemein etablierter und akzeptierter Industriestandards gehärtet. Die herangezogenen Härtungsanleitungen werden ebenso wie der Umsetzungsstatus dokumentiert.	RB-22
26.	**Geheimhaltung von Authentifizierungsinformationen** Die Zuteilung geheimer Authentifizierungsinformationen (z. B. Passwörter, Zertifikate, Sicherheitstoken) an interne und externe Benutzer des KRITIS-Betreibers erfolgt, soweit dies organisatorischen oder technischen Verfahren des KRITIS-Betreibers unterliegt, in einem geordneten Verfahren, das die Vertraulichkeit der Informationen sicherstellt. Soweit diese initial vergeben werden, sind diese nur temporär, höchstens aber 14 Tage gültig. Benutzer werden ferner gezwungen, diese bei der ersten Verwendung zu ändern.	IDM-07
27.	**Sichere Anmeldeverfahren** Die Vertraulichkeit der Anmeldeinformationen von internen und externen Benutzern unter Verantwortung des KRITIS-Betreibers sind durch die folgenden Maßnahmen geschützt: • Identitätsprüfung durch vertrauenswürdige Verfahren • Verwendung anerkannter Industriestandards zur Authentifizierung und Autorisierung (z. B. Multi-Faktor-Authentifizierung, keine Verwendung von gemeinsam genutzten Authentifizierungsinformationen, automatischer Ablauf) • Multi-Faktor-Authentifizierung für Administratoren des KRITIS-Betreibers (z. B. durch Smart Card oder biometrische Merkmale) ist zwingend erforderlich, sofern ein Zugriff über öffentliche Netze erfolgt.	IDM-08
28.	**Systemseitige Zugriffskontrolle** Der Zugriff auf Informationen und Anwendungsfunktionen wird durch technische Maßnahmen eingeschränkt, mit denen das Rollen- und Rechtekonzept umgesetzt wird.	IDM-10

2.5 Technische Informationssicherheit

29.	**Passwortanforderungen und Validierungsparameter** Sicherheits-Parameter auf Netzwerk,- Betriebssystem- (Host und Gast), Datenbank-, und Anwendungsebene (soweit für die kritische Dienstleistung relevant) sind angemessen konfiguriert, um unautorisierte Zugriffe zu verhindern. Soweit keine Zwei-Faktor-Authentifizierung oder die Verwendung von Einmalpasswörtern möglich ist, wird die Verwendung sicherer Passwörter auf allen Ebenen und Geräten (einschließlich mobilen Endgeräten) unter Verantwortung des KRITIS-Betreibers technisch erzwungen oder in einer Passwort-Richtlinie organisatorisch gefordert. Die Vorgaben müssen mindestens die folgenden Anforderungen erfüllen: • Minimale Passwortlänge von 8 Zeichen • Mindestens zwei der folgenden Zeichentypen müssen enthalten sein: Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen • Maximale Gültigkeit von 90 Tagen, minimale Gültigkeit von 1 Tag • Passworthistorie von 6 • Übertragung und Speicherung der Passwörter in einem verschlüsselten Verfahren, das dem aktuellen Stand der Technik entspricht.	IDM-11
30.	**Einschränkung und Kontrolle administrativer Software** Die Verwendung von Dienstprogrammen und Managementkonsolen, die weitreichenden Zugriff auf die Daten der für die kritische Dienstleistung relevanten Daten ermöglichen, ist auf autorisierte Personen beschränkt. Vergabe und Änderung entsprechender Zugriffsberechtigungen erfolgen gemäß der Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen. Der Zugriff wird durch starke Authentifizierungstechniken, einschließlich Multi-Faktor-Authentifizierung gesteuert.	IDM-12
31.	**Zugriffskontrolle zu Quellcode** Der Zugriff auf den Quellcode und ergänzende für die Entwicklung der kritischen Dienstleistung relevanten Informationen (z. B. Architektur-Dokumentation, Testpläne) sind restriktiv vergeben und werden überwacht, um die Einführung von nicht autorisierten Funktionen oder das Durchführen unbeabsichtigter Änderungen zu vermeiden.	IDM-13

2.5 Technische Informationssicherheit

32.	**Richtlinie zur Nutzung von Verschlüsselungsverfahren und Schlüsselverwaltung** Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für Verschlüsselungsverfahren und Schlüsselverwaltung sind gemäß IT-Sicherheitsrichtlinie dokumentiert, kommuniziert und bereitgestellt, in denen die folgenden Aspekte beschrieben sind: • Das Nutzen von starken Verschlüsselungsverfahren (z. B. AES) und die Verwendung von sicheren Netzwerkprotokollen, die dem Stand der Technik entsprechen (z. B. TLS, IPsec, SSH) • risikobasierte Vorschriften für den Einsatz von Verschlüsselung, die mit Schemata zur Informationsklassifikation abgeglichen sind und den Kommunikationskanal, Art, Stärke und Qualität der Verschlüsselung berücksichtigen • Anforderungen für das sichere Erzeugen, Speichern, Archivieren, Abrufen, Verteilen, Entziehen und Löschen der Schlüssel • Berücksichtigung der relevanten rechtlichen und regulatorischen Verpflichtungen und Anforderungen.	KRY-01
33.	**Verschlüsselung von Daten bei der Übertragung (Transportverschlüsselung)** Verfahren und technische Maßnahmen zur starken Verschlüsselung und Authentifizierung bei der Übertragung von Daten der kritischen Dienstleistung (z. B. über öffentliche Netze transportierte elektronische Nachrichten) sind etabliert.	KRY-02
34.	**Verschlüsselung von sensiblen Daten bei der Speicherung** Verfahren und technische Maßnahmen zur Verschlüsselung sensibler Daten der kritischen Dienstleistung bei der Speicherung sind etabliert. Ausnahmen gelten für Daten, die für die Erbringung der kritischen Dienstleistung funktionsbedingt nicht verschlüsselt sein können. Die für die Verschlüsselung verwendeten privaten Schlüssel sind ausschließlich dem dafür vorgesehenen Empfänger nach geltenden rechtlichen und regulatorischen Verpflichtungen und Anforderungen bekannt. Ausnahmen (z. B. Verwendung eines Generalschlüssels durch den KRITIS-Betreiber) folgen einem geregelten Verfahren.	KRY-03

2.5 Technische Informationssicherheit

35.	**Sichere Schlüsselverwaltung** Verfahren und technische Maßnahmen zur sicheren Schlüsselverwaltung beinhalten mindestens die folgenden Aspekte: • Schlüsselgenerierung für unterschiedliche kryptografische Systeme und Applikationen • Ausstellung und Einholung von Public-Key-Zertifikaten • Provisionierung und Aktivierung von Schlüsseln für beteiligte Dritte • Sicheres Speichern eigener Schlüssel (sonstiger Dritter) einschließlich der Beschreibung, wie autorisierte Nutzer den Zugriff erhalten • Ändern oder Aktualisieren von kryptografischen Schlüsseln einschließlich Richtlinien, die festlegen, unter welchen Bedingungen und auf welche Weise die Änderungen bzw. Aktualisierungen zu realisieren sind • Umgang mit kompromittiertem Schlüssel • Entzug und Löschen von Schlüsseln, bspw. im Falle von Kompromittierung oder Mitarbeiterveränderungen.	KRY-04
36.	**Technische Schutzmaßnahmen** Basierend auf den Ergebnissen einer durchgeführten Risiko-Analyse, hat der KRITIS-Betreiber technische Schutzmaßnahmen implementiert, die geeignet sind, um netzwerkbasierte Angriffe auf Basis anomaler Eingangs- oder Ausgangs-Traffic-Muster (z. B. durch MAC-Spoofing und ARP-Poisoning-Angriffe) und/oder Distributed-Denial-of-Service (DDoS)-Angriffe zeitnah zu erkennen und darauf zu reagieren. Zusätzlich werden, wo notwendig bzw. sinnvoll, Intrusion Detection- und Intrusion Prevention-Systeme (IDS und IPS) eingesetzt.	KOS-01
37.	**Überwachen von Verbindungen** Physische und virtualisierte Netzwerkumgebungen sind so konzipiert und konfiguriert, dass die Verbindungen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Netzen zu beschränken und überwachen sind. In festgelegten Abständen wird die geschäftliche Rechtfertigung für die Verwendung aller Dienste, Protokolle und Ports überprüft. Darüber hinaus umfasst die Überprüfung auch die Begründungen für kompensierende Kontrollen für die Verwendung von Protokollen, die als unsicher angesehen werden.	KOS-02
38.	**Netzwerkübergreifende Zugriffe** Jeder Netzwerkperimeter wird von Sicherheitsgateways kontrolliert. Die Zugangsberechtigung für netzübergreifende Zugriffe basiert auf einer Sicherheitsbewertung.	KOS-03

2.5 Technische Informationssicherheit

39.	**Netzwerke zur Administration** Es existieren gesonderte Netzwerke zur administrativen Verwaltung der Infrastruktur und für den Betrieb von Managementkonsolen, die logisch oder physisch vom Netzwerk des KRITIS-Betreibers getrennt und durch Multi-Faktor-Authentifizierung vor unberechtigten Zugriffen geschützt sind. Netzwerke, die zum Zwecke der Migration oder dem Erzeugen von virtuellen Maschinen dienen, sind ebenfalls physisch oder logisch von anderen Netzwerken zu separieren.	KOS-04
40.	**Dokumentation der Netztopologie** Die Architektur des Netzwerks ist nachvollziehbar und aktuell dokumentiert (z. B. in Form von Diagrammen), um im Wirkbetrieb Fehler in der Verwaltung zu vermeiden und um im Schadensfall eine zeitgerechte Wiederherstellung gemäß den vertraglichen Verpflichtungen zu gewährleisten. Aus der Dokumentation gehen die unterschiedlichen Umgebungen (z. B. Administrations-Netzwerk und geteilte Netzwerksegmente) und Datenflüsse hervor.	KOS-06
41.	**Richtlinien zur Datenübertragung** Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen zum Schutz der Datenübertragung vor unbefugtem Abfangen, Manipulieren, Kopieren, Modifizieren, Umleiten oder Vernichten (z. B. Einsatz von Verschlüsselung) sind gemäß IT-Sicherheitsrichtlinie dokumentiert, kommuniziert und bereitgestellt. Die Vorgaben stellen einen Bezug zur Klassifikation von Informationen her (vgl. Nr. 9).	KOS-07
42.	**Vertraulichkeitserklärung** Die mit internen Mitarbeitern, externen Dienstleistern sowie Lieferanten des KRITIS-Betreibers zu schließenden Geheimhaltungs- oder Vertraulichkeitserklärungen basieren auf den Anforderungen des KRITIS-Betreibers zum Schutz vertraulicher Daten und betrieblicher Details. Die Anforderungen sind zu identifizieren, dokumentieren und in regelmäßigen Abständen (mindestens jährlich) zu überprüfen. Soweit sich aus der Überprüfung ergibt, dass die Anforderungen anzupassen sind, werden mit den internen Mitarbeitern, den externen Dienstleistern sowie den Lieferanten des KRITIS-Betreibers neue Geheimhaltungs- oder Vertraulichkeitserklärungen abgeschlossen. Die Geheimhaltungs- oder Vertraulichkeitserklärungen sind vor Beginn des Vertragsverhältnisses bzw. vor Erteilung des Zugriffs auf Daten des KRITIS-Betreibers durch interne Mitarbeiter, externe Dienstleister oder Lieferanten des KRITIS-Betreibers zu unterzeichnen. Soweit sich aus der Überprüfung Anpassungen an die Geheimhaltungs- oder Vertraulichkeitserklärungen ergeben, sind die internen und externen Mitarbeiter des Betreibers der Kritischen Infrastrukturen darüber in Kenntnis zu setzen und neue Bestätigungen einzuholen.	KOS-08

2.5 Technische Informationssicherheit

43.	**Richtlinien zur Entwicklung/Beschaffung von Informationssystemen** Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für die ordnungsgemäße Entwicklung und/oder Beschaffung von Informationssystemen für die Entwicklung oder den Betrieb der kritischen Dienstleistung, einschließlich Anwendungen, Middleware, Datenbanken, Betriebssystemen und Netzwerkkomponenten sind gemäß IT-Sicherheitsrichtlinie dokumentiert, kommuniziert und bereitgestellt. In den Richtlinien und Anweisungen sind mindestens die folgenden Aspekte beschrieben: • Sicherheit in der Softwareentwicklungsmethodik in Übereinstimmung mit in der Industrie etablierten Sicherheitsstandards (z. B. OWASP für Webapplikationen) • Sicherheit der Entwicklungsumgebung (z. B. getrennte Entwicklungs-/Test-/Produktivumgebungen) • Programmierrichtlinien für jede verwendete Programmiersprache (z. B. bzgl. Buffer Overflows, Verbergen interner Objektreferenzen gegenüber Benutzern) • Sicherheit in der Versionskontrolle.	BEI-01
44.	**Auslagerung der Entwicklung** Bei ausgelagerter Entwicklung der kritischen Dienstleistung (oder Teilen davon) in Bezug auf Design, Entwicklung, Test und/oder Bereitstellung von Quellcode der kritischen Dienstleistung ist ein hohes Maß an Sicherheit gefordert. Deshalb sind mindestens die folgenden Aspekte vertraglich zwischen KRITIS-Betreiber und externem Dienstleister zu vereinbaren: • Anforderungen an einen sicheren Software-Entwicklungsprozess (insbesondere Design, Entwicklung und Test) • Bereitstellung von Nachweisen, dass eine ausreichende Prüfung vom externen Dienstleister durchgeführt wurde • Abnahmeprüfung der Qualität der erbrachten Leistungen gemäß den vereinbarten funktionalen und nicht-funktionalen Anforderungen • Das Recht, den Entwicklungsprozess und Kontrollen einer Prüfung, auch stichprobenartig, zu unterziehen.	BEI-02

2.5 Technische Informationssicherheit

45.	**Richtlinien zur Änderung von Informationssystemen** Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für eine ordnungsgemäße Verwaltung von Änderungen (Change Management) an Informationssystemen für die Entwicklung oder den Betrieb der kritischen Dienstleistung, einschließlich Anwendungen, Middleware, Datenbanken, Betriebssystemen und Netzwerkkomponenten sind gemäß IT-Sicherheitsrichtlinie dokumentiert, kommuniziert und bereitgestellt. **Mindestens die folgenden Aspekte sind dabei zu berücksichtigen:** • Risikobeurteilung • Kriterien zur Kategorisierung und Priorisierung von Änderungen und damit verbundene Anforderungen an Art und Umfang durchzuführender Tests und einzuholender Genehmigungen • Anforderungen zur Benachrichtigung betroffener Stakeholder gemäß den vertraglichen Vereinbarungen • Anforderungen an die Dokumentation von Tests sowie zur Beantragung und Genehmigung von Änderungen • Anforderungen an die Durchführung von Roll-Backs • Anforderungen an die Dokumentation von Änderungen in der System-, Betriebs- und Benutzerdokumentation • Anforderungen an die Durchführung von Notfalländerungen • Anforderungen an die System- und Funktionstrennung.	BEI-03
46.	**Risikobewertung der Änderungen** Der Auftraggeber einer Änderung von Informationssystemen führt zuvor eine Risikobewertung durch. Alle möglicherweise von der Änderung betroffenen Konfigurationsobjekte werden auf potenzielle Auswirkungen hin bewertet. Das Ergebnis der Risikobewertung ist angemessen und nachvollziehbar zu dokumentieren.	BEI-04
47.	**Kategorisierung der Änderungen** Alle Änderungen von Informationssystemen werden basierend auf einer Risikobewertung kategorisiert (z. B. als geringfügige, erhebliche oder weitreichende Folgen), um eine angemessene Autorisierung vor Bereitstellung der Änderung in der Produktivumgebung einzuholen.	BEI-05
48.	**Priorisierung der Änderungen** Alle Änderungen werden basierend auf einer Risikobewertung priorisiert (z. B. als niedrig, normal, hoch, Notfall), um eine angemessene Autorisierung vor Bereitstellung der Änderung in der Produktivumgebung einzuholen.	BEI-06

2.5 Technische Informationssicherheit

49.	**Testen der Änderungen** Alle Änderungen an der kritischen Dienstleistung werden Tests (z. B. auf Integration, Regression, Sicherheit und Benutzerakzeptanz) während der Entwicklung und vor der Bereitstellung in der Produktivumgebung unterzogen. Die Tests werden von angemessen qualifiziertem Personal des KRITIS-Betreibers durchgeführt.	BEI-07
50.	**Zurückrollen der Änderungen** Es sind Abläufe definiert, um erforderliche Änderungen in Folge von Fehlern oder Sicherheitsbedenken zurückrollen zu können und betroffene Systeme oder Dienste im vorherigen Zustand wiederherzustellen.	BEI-08
51.	**Überprüfen von ordnungsgemäßer Testdurchführung und Genehmigung** Bevor eine Änderung in der Produktivumgebung veröffentlicht wird (Release), ist diese durch eine hierzu autorisierte Stelle oder ein entsprechendes Gremium dahingehend zu überprüfen, ob die geplanten Tests erfolgreich abgeschlossen und die erforderlichen Genehmigungen erteilt sind. Für eine angemessene Zufallsstichprobe von Änderungen in der Produktivumgebung wird in einem risikoorientierten Ansatz überprüft, ob die internen Anforderungen in Bezug auf ordnungsgemäße Klassifizierung, Test und Genehmigung von Änderungen eingehalten wurden.	BEI-09
52.	**Notfalländerungen** Notfalländerungen sind als solche von dem Änderungsmanager zu klassifizieren, der die Änderungsdokumentation vor Übertragung der Änderung in die Produktivumgebung erstellt. Anschließend (z. B. innerhalb von 5 Werktagen) fügt der Änderungsmanager Begründung und Ergebnis der Übertragung der Notfalländerung zu der Änderungsdokumentation hinzu. Aus der Begründung muss hervorgehen, warum der reguläre Änderungsprozess nicht durchlaufen werden konnte und was die Folgen einer Verzögerung durch Einhaltung des regulären Prozesses gewesen wären.	BEI-10
53.	**Systemlandschaft** Produktivumgebungen sind von Nicht-Produktivumgebungen physisch oder logisch getrennt, um unbefugten Zugriff oder Änderungen an Produktivdaten zu vermeiden. Produktivdaten werden nur im Rahmen von definierten Vorgaben in Test- oder Entwicklungsumgebungen repliziert, um deren Vertraulichkeit zu wahren.	BEI-11
54.	**Funktionstrennung** Verfahren zum Change Management beinhalten rollenbasierte Autorisierungen, um eine angemessene Funktionstrennung bei Entwicklung, Freigabe und Migration von Änderungen zwischen den Umgebungen sicherzustellen**.**	BEI-12

2.5 Technische Informationssicherheit

55.	**Richtlinien und Verfahren zur Risikominimierung des Zugriffs über mobile Endgeräte des KRITIS-Betreibers** Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für die ordnungsgemäße Verwendung mobiler Endgeräte sowie andere Remote-Zugriffe (bspw. mobile Arbeitsplätze) im Verantwortungsbereich des KRITIS-Betreibers, die Zugriff auf IT-Systeme zur Entwicklung und zum Betrieb der kritischen Dienstleistung ermöglichen, sind gemäß IT-Sicherheitsrichtlinie dokumentiert, kommuniziert und bereitgestellt. Darin werden mindestens folgende Aspekte beachtet, soweit diese auf die Situation des KRITIS-Betreibers anwendbar sind: • Verschlüsselung der Geräte und der Datenübertragung • verstärkter Zugriffsschutz • erweitertes Identitäts- und Berechtigungsmanagement • Verbot von Jailbreaking/Rooting • Installation nur von freigegebenen Anwendungen aus als vertrauenswürdig eingestuften „App Stores“ • Bring-Your-Own-Device (BYOD) – Mindestanforderungen an private Endgeräte.	MDM-01

2.6 Personelle und organisatorische Sicherheit

Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Grundlage (C5 #)
56.	**Einstellung und Sicherheitsüberprüfung** Die Vergangenheit aller internen und externen Mitarbeiter des KRITIS-Betreibers mit Zugriff auf die für die Erbringung der kritischen Dienstleistung notwendigen informationstechnischen Systeme, Komponenten und Prozesse wird vor Beginn des Beschäftigungsverhältnisses gemäß der lokalen Gesetzgebung und Regulierung durch den KRITIS-Betreiber überprüft. Besondere Genehmigungsverfahren im Einstellungsprozess für Mitarbeiter und Positionen, bei denen Zugriff auf besonders sensible Informationen besteht, sind etabliert. Soweit rechtlich zulässig, umfasst die Überprüfung folgende Bereiche: • Verifikation der Person durch Personalausweis • Verifikation des Lebenslaufs • Verifikation von akademischen Titeln und Abschlüssen • Anfrage eines polizeilichen Führungszeugnisses bei sensiblen Positionen im Unternehmen. Besondere Genehmigungsverfahren im Einstellungsprozess für Mitarbeiter und Positionen, bei denen Zugriff auf besonders sensible Informationen besteht, sind etabliert.	HR-01
57.	**Einstellung und Beschäftigungsvereinbarungen** Beschäftigungsvereinbarungen beinhalten die Verpflichtungen der internen und externen Mitarbeiter des KRITIS-Betreibers auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen in Bezug zur Informationssicherheit. Die Sicherheitsleitlinie sowie die davon abgeleiteten Richtlinien und Anweisungen zur Informationssicherheit sind den Unterlagen zur Beschäftigungsvereinbarung beigefügt. Deren Einhaltung wird durch den Mitarbeiter schriftlich bestätigt, bevor Zugriff auf die kritische Dienstleistung oder die IT-Infrastruktur möglich ist.	HR-02

2.6 Personelle und organisatorische Sicherheit

58.	**Rollenzuweisung und Vieraugenprinzip oder Funktionstrennung** Ein auf den Geschäfts- und Sicherheitsanforderungen des KRITIS-Betreibers basierendes Rollen- und Rechtekonzept sowie eine Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen sind dokumentiert, kommuniziert und bereitgestellt und adressieren die folgenden Bereiche: • Die Vergabe und Änderung (Provisionierung) von Zugriffsberechtigungen auf Basis des Prinzips der geringsten Berechtigung („Least Privilege Prinzip“) und wie es für die Aufgabenwahrnehmung notwendig ist („Need to know Prinzip“) • Funktionstrennung zwischen operativen und kontrollierenden Funktionen („Separation of Duties“) • Funktionstrennung in der Administration von Rollen, Genehmigung und Zuweisung von Zugriffsberechtigungen • regelmäßige Überprüfung vergebener Berechtigungen • Berechtigungsentzug (Deprovisionierung) bei Veränderungen des Arbeitsverhältnisses Anforderungen an Genehmigung und Dokumentation der Verwaltung von Zugangs- und Zugriffsberechtigungen.	IDM-01
59.	**Identitäts- und Berechtigungsmanagement – Benutzerregistrierung** Zugangsberechtigungen für Benutzer unter Verantwortung des KRITIS-Betreibers (interne und externe Mitarbeiter) werden in einem formalen Verfahren erteilt. Organisatorische und/oder technische Maßnahmen stellen sicher, dass eindeutige Benutzerkennungen vergeben werden, die jeden Benutzer eindeutig identifizieren.	IDM-02
60.	**Identitäts- und Berechtigungsmanagement – Zugriffsberechtigung** Vergabe und Änderung von Zugriffsberechtigungen für Benutzer unter Verantwortung des KRITIS-Betreibers erfolgen gemäß der Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen. Organisatorische und/oder technische Maßnahmen stellen sicher, dass die vergebenen Zugriffe die folgenden Anforderungen erfüllen: • Zugriffsberechtigungen entsprechen dem Prinzip der geringsten Berechtigung („Least-Privilege-Prinzip“) • Zugriffsberechtigungen werden nur so vergeben, wie es für die Aufgabenwahrnehmung notwendig ist („Need-to-know-Prinzip“) • die formalen Genehmigungen erfolgen durch eine autorisierte Person, bevor die Zugriffsberechtigungen eingerichtet werden (d. h. bevor der Benutzer auf die Systeme der kritischen Dienstleistung oder Komponenten der geteilten IT-Infrastruktur zugreifen kann) • die technisch zugewiesenen Zugriffsberechtigungen dürfen die formalen Genehmigungen nicht übersteigen.	IDM-03

2.6 Personelle und organisatorische Sicherheit

61.	**Vergabe und Änderung (Provisionierung) von Zugriffsberechtigungen** Zugriffsberechtigungen von Benutzern unter Verantwortung des KRITIS-Betreibers (interne und externe Mitarbeiter) werden bei Änderungen im Beschäftigungsverhältnis (Kündigung, Versetzung, längerer Abwesenheit/Sabbatical/Elternzeit) zeitnah, spätestens aber 30 Tage nach Inkrafttreten entzogen bzw. vorübergehend ruhe stellend gesetzt. Zugänge werden vollständig deaktiviert, sobald das Beschäftigungsverhältnis erlischt.	IDM-04
62.	**Identitäts- und Berechtigungsmanagement – Überprüfungen** Zugriffsberechtigungen von Benutzern unter Verantwortung des KRITIS-Betreibers (interne und externe Mitarbeiter) werden mindestens jährlich überprüft, um diese zeitnah auf Änderungen im Beschäftigungsverhältnis (Kündigung, Versetzung, längerer Abwesenheit/Sabbatical/Elternzeit) anzupassen. Die Überprüfung erfolgt durch hierzu autorisierte Personen aus den Unternehmensbereichen des KRITIS-Betreibers, die aufgrund ihres Wissens über die Zuständigkeiten die Angemessenheit der vergebenen Berechtigungen überprüfen können. Die Überprüfung sowie die sich daraus ergebenden Berechtigungsanpassungen werden nachvollziehbar dokumentiert. Administrative Berechtigungen werden regelmäßig (mind. jährlich) überprüft.	IDM-05
63.	**Identitäts- und Berechtigungsmanagement – Administratoren** Vergabe und Änderung von Zugriffsberechtigungen für interne und externe Benutzer mit administrativen oder weitreichenden Berechtigungen unter Verantwortung des KRITIS-Betreibers erfolgen gemäß der Richtlinie zur Verwaltung von Zugangs- und Zugriffsberechtigungen. Die Zuweisung erfolgt personalisiert und wie es für die Aufgabenwahrnehmung notwendig ist („Need-to-know-Prinzip“). Organisatorische und/oder technische Maßnahmen stellen sicher, dass durch die Vergabe dieser Berechtigungen keine ungewollten, kritischen Kombinationen entstehen, die gegen das Prinzip der Funktionstrennung verstoßen (z. B. Zuweisen von Berechtigungen zur Administration der Datenbank wie auch des Betriebssystems). Soweit dies in ausgewählten Fällen nicht möglich ist, sind angemessene, kompensierende Kontrollen eingerichtet, um einen Missbrauch dieser Berechtigungen zu identifizieren (z. B. Protokollierung und Überwachung durch eine SIEM-Lösung (Security Information and Event Management)).	IDM-06
64.	**Identitäts- und Berechtigungsmanagement – Notfallbenutzer** Die Verwendung von Notfallbenutzern (für Aktivitäten, die mit personalisierten, administrativen Benutzern nicht durchgeführt werden können) ist dokumentiert, zu begründen und bedarf der Genehmigung durch eine autorisierte Person, die unter Berücksichtigung des Prinzips der Funktionstrennung zu erfolgen hat. Die Freischaltung des Notfallbenutzers erfolgt nur solange, wie es für die Aufgabenwahrnehmung notwendig ist. Mindestens jährlich wird ein manueller Abgleich zwischen den erfolgten Freischaltungen der Notfallbenutzer und den entsprechenden Genehmigungen durchgeführt. Auffälligkeiten werden untersucht, um Missbrauch dieser Benutzer festzustellen und zukünftig zu verhindern. Die Aktivitäten der Notfallbenutzer werden revisionssicher protokolliert. Die Protokollierung ist hinreichend detailliert, um es einem sachverständigen Dritten zu ermöglichen, die Aktivitäten nachzuvollziehen.	IDM-09

2.6 Personelle und organisatorische Sicherheit

65.	**Festlegung notwendiger Kompetenzen (Betrieb und IT-Sicherheit)** Von der Sicherheitsleitlinie abgeleitete Richtlinien und Anweisungen zur Informationssicherheit oder verwandter Themen sind nach einer einheitlichen Struktur dokumentiert. Sie werden sach- und bedarfsgerecht an alle relevanten Stakeholder kommuniziert und bereitgestellt. Sicherheitsleitlinien werden versioniert und von der Unternehmensleitung freigegeben. Die Richtlinien und Anweisungen beschreiben mindestens die folgenden Aspekte: • Ziele • Geltungsbereiche • Rollen und Verantwortlichkeiten einschließlich Anforderungen an die Qualifikation des Personals und das Einrichten von Vertretungsregelungen • die Koordination unterschiedlicher Unternehmensbereiche • Sicherheitsarchitektur und -maßnahmen zum Schutz von Daten, IT-Anwendungen und IT-Infrastrukturen, die durch den Betreiber der kritischen Dienstleistung oder von Dritten verwaltet werden sowie • Maßnahmen zur Einhaltung rechtlicher und regulatorischer Anforderungen (Compliance).	SA-01
66.	**Überprüfung und Freigabe von Richtlinien und Anweisungen** Die Richtlinien und Anweisungen zur Informationssicherheit werden mindestens jährlich durch mit dem Thema vertraute Fachkräfte des Betreibers der kritischen Dienstleistung hinsichtlich ihrer Angemessenheit und Wirksamkeit überprüft. Die Überprüfung berücksichtigt mindestens • organisatorische Änderungen beim Betreiber der kritischen Dienstleistung, • rechtliche und technische Änderungen im Umfeld des Betreibers der kritischen Dienstleistung. Überarbeitete Richtlinien und Anweisungen werden durch hierzu autorisierte Gremien oder Stellen des Betreibers der kritischen Dienstleistung genehmigt, bevor diese Gültigkeit erlangen. Die regelmäßige Überprüfung wird durch zentrale Stellen beim Betreiber nachgehalten.	SA-02
67.	**Abweichungen von bestehenden Richtlinien und Anweisungen** Ausnahmen von Richtlinien und Anweisungen zur Informationssicherheit werden durch hierzu autorisierte Gremien oder Stellen des Betreibers der kritischen Dienstleistung in dokumentierter Form genehmigt. Die Angemessenheit genehmigter Ausnahmen und die Beurteilung der daraus entstehenden Risiken wird mindestens jährlich durch mit den Themen vertraute Fachkräfte des Betreibers der kritischen Dienstleistung vor dem Hintergrund der aktuellen und zukünftig erwarteten Bedrohungsumgebung in Bezug auf die Informationssicherheit überprüft.	SA-03

2.6 Personelle und organisatorische Sicherheit

68.	**Schulungen und Awareness** Ein Programm zur zielgruppenorientierten Sicherheitsausbildung und Sensibilisierung zum Thema Informationssicherheit existiert und ist verpflichtend für alle internen und externen Mitarbeiter des KRITIS-Betreibers. Das Programm wird regelmäßig in Bezug auf die gültigen Richtlinien und Anweisungen, den zugewiesenen Rollen und Verantwortlichkeiten sowie den bekannten Bedrohungen aktualisiert und ist dann erneut zu durchlaufen. Das Programm umfasst mindestens die folgenden Inhalte: • Die regelmäßige und dokumentierte Unterweisung hinsichtlich der sicheren Konfiguration und des sicheren Betriebs der für die kritische Dienstleistung erforderlichen IT-Anwendungen und IT-Infrastruktur, einschließlich mobiler Endgeräte • die regelmäßige und dokumentierte Unterrichtung über bekannte Bedrohungen und • das regelmäßige und dokumentierte Training des Verhaltens beim Auftreten sicherheitsrelevanter Ereignisse. Externe Dienstleister und Lieferanten des KRITIS-Betreibers, die zum Betrieb der kritischen Dienstleistung beitragen, werden vertraglich verpflichtet, ihre Mitarbeiter und Unterauftragnehmer auf die spezifischen Sicherheitsanforderungen des KRITIS-Betreibers hinzuweisen und ihre Mitarbeiter allgemein zum Thema Informationssicherheit zu schulen. Das Programm berücksichtigt verschiedene Profile und umfasst weiterführende Informationen für Positionen und Mitarbeiter, die umfangreiche Berechtigungen oder Zugriff auf sensible Daten haben. Externe Mitarbeiter von Dienstleistern und Lieferanten des KRITIS-Betreibers, die zum Betrieb der kritischen Dienstleistung beitragen, werden in den spezifischen Sicherheitsanforderungen des Betreibers der kritischen Infrastrukturen sowie allgemein zum Thema Informationssicherheit unterwiesen.	HR-03
69.	**Disziplinarverfahren** Ein Prozess für die Durchführung von Disziplinarmaßnahmen ist implementiert und an die Mitarbeiter kommuniziert, um die Konsequenzen von Verstößen gegen die gültigen Richtlinien und Anweisungen, sowie rechtliche Vorgaben und Gesetze transparent zu machen.	HR-04
70.	**Beendigung des Beschäftigungsverhältnisses** Interne sowie externe Mitarbeiter sind darüber informiert, dass die Verpflichtungen auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen in Bezug zur Informationssicherheit auch bei einem Wechsel des Aufgabengebietes oder der Auflösung des Beschäftigungsverhältnisses bestehen bleiben.	HR-05

2.7 Bauliche/physische Sicherheit

Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Grundlage (C5 #)
71.	**Rechenzentrumsversorgung** Die Versorgung der für den Betrieb der kritischen Dienstleistung notwendigen IT-Systeme (z. B. Elektrizität, Temperatur- und Feuchtigkeitskontrolle, Telekommunikation und Internetverbindung) ist abgesichert, überwacht und wird regelmäßig gewartet und getestet, um eine durchgängige Wirksamkeit zu gewährleisten. Sie ist mit automatischen Ausfallsicherungen und anderen Redundanzen konzipiert. Die Wartung wird in Übereinstimmung mit den von den Lieferanten empfohlenen Wartungsintervallen und Vorgaben sowie ausschließlich von autorisiertem Personal durchgeführt. Wartungsprotokolle einschließlich vermuteter oder festgestellter Mängel werden für den Zeitraum der zuvor vertraglich vereinbarten Frist aufbewahrt.	BCM-05
72.	**Perimeterschutz** Es ist ein geeigneter Rahmen für die bauliche und physische Sicherheit, die zum sicheren Betrieb einer kritischen Dienstleistung notwendig ist, zu setzen. Die Begrenzungen von Räumlichkeiten oder Gebäuden, die sensible oder kritische Informationen, Informationssysteme oder sonstige Netzwerkinfrastruktur beherbergen, sind physisch solide und durch angemessene Sicherheitsmaßnahmen geschützt, die dem Stand der Technik entsprechen. Das Sicherheitskonzept beinhaltet die Einrichtung von verschiedenen Sicherheitszonen, die durch Sicherheitslinien als überwachte und gesicherte Übergänge zwischen den Zonen getrennt sind, wenn dies für den Schutz der kritischen Dienstleistung notwendig ist.	PS-01
73.	**Physischer Zutrittsschutz** Zugänge zu Räumlichkeiten oder Gebäuden, die sensible oder kritische Informationen, Informationssysteme oder sonstige Netzwerkinfrastruktur für den Betreiber einer kritischen Dienstleistung beherbergen, sind durch physische Zutrittskontrollen gesichert und überwacht, um unbefugten Zutritt zu verhindern.	PS-02

2.7 Bauliche/physische Sicherheit

74.	**Schutz vor Bedrohungen von außen** Räumlichkeiten oder Gebäude, die sensible oder kritische Informationen, Informationssysteme oder sonstige Netzwerkinfrastruktur für die kritische Dienstleistung beherbergen, sind durch bauliche, technische und organisatorische Maßnahmen vor Feuer, Wasser, Erdbeben, Explosionen, zivile Unruhen und andere Formen natürlicher und von Menschen verursachter Bedrohungen geschützt. An zwei georedundanten Standorten sind mindestens die folgenden Maßnahmen getroffen: Bauliche Maßnahmen: • Einrichtung eines eigenen Brandabschnitts für das Rechenzentrum • Verwendung feuerbeständiger Materialien gemäß DIN 4102-1 oder EN 13501 (Feuerwiderstandsdauer von mindestens 90 Minuten). Technische Maßnahmen: • Sensoren zum Überwachen von Temperatur und Luftfeuchtigkeit • Aufschalten des Gebäudes an einer Brandmeldeanlage mit Meldung an die örtliche Feuerwehr • Brandfrüherkennungs- und Löschanlage. Organisatorische Maßnahmen: • Regelmäßige Brandschutzübungen und Brandschutzbegehungen, um die Einhaltung der Brandschutzmaßnahmen zu prüfen. Es findet eine Überwachung der Umgebungsparameter statt. Bei Verlassen des zulässigen Regelbereichs werden Alarmmeldungen generiert und an die dafür zuständigen Stellen weitergeleitet.	PS-03
75.	**Schutz vor Unterbrechungen durch Stromausfälle und andere derartige Risiken** Dem Ausfall von Versorgungsleistungen wie Strom, Kühlung oder Netzanbindungen für Anlagen der kritischen Dienstleistung wird durch geeignete Maßnahmen und Redundanzen, in Abstimmung mit den Maßnahmen zur Betriebssicherheit, vorgebeugt. Versorgungsleistungen für Strom und Telekommunikation, welche Daten transportieren oder Informationssysteme versorgen, sind vor Abhören und Beschädigung geschützt. Es findet eine Überwachung der Versorgungsleistungen statt. Bei Verlassen des zulässigen Regelbereichs werden Alarmmeldungen generiert und an die dafür zuständigen Stellen weitergeleitet. Der Betreiber der kritischen Dienstleistung ermittelt und kommuniziert die Autark-Zeiten, die durch die getroffenen Maßnahmen bei Ausfall der Versorgungsleistungen oder beim Eintritt von außergewöhnlichen Ereignissen (z. B. Hitzeperioden, länger anhaltender Stromausfall) erreicht werden sowie die maximal tolerierbaren Zeiten für einen Ausfall der Versorgungsleistungen. Verträge für die Aufrechterhaltung der Notfallversorgung mit entsprechenden Dienstleistern sind abgeschlossen (z. B. für den Treibstoff der Notstromversorgung).	PS-04

2.7 Bauliche/physische Sicherheit

76.	**Wartung der Infrastruktur** Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für die Erbringung der kritischen Dienstleistung sind dokumentiert, kommuniziert und bereitgestellt, welche die Wartung (insb. Fernwartung), Löschung, Aktualisierung und Wiederverwendung von Assets in der Informationsverarbeitung in ausgelagerten Räumlichkeiten oder durch externes Personal beschreiben.	PS-05

2.8 Vorfallserkennung und -bearbeitung

Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Grundlage (C5 #)
77.	**Verantwortlichkeiten und Vorgehensmodell** Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen sind gemäß der Informationssicherheitsrichtlinie dokumentiert, kommuniziert und bereitgestellt, um eine schnelle, effektive und ordnungsgemäße Reaktion auf alle bekannten Sicherheitsvorfälle, i. S. von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der betriebenen Kritischen Infrastrukturen geführt haben, zu gewährleisten. Seitens des KRITIS-Betreibers sind dabei mindestens die in der Informationssicherheitsrichtlinie aufgeführten Rollen zu besetzen, Vorgaben zur Klassifizierung, Priorisierung und Eskalation von Sicherheitsvorfällen zu definieren und Schnittstellen zum Incident Management sowie dem Business Continuity Management zu schaffen. Zusätzlich hat der KRITIS-Betreiber ein Team zur Behandlung von Informationssicherheitsvorfällen eingerichtet, das zur koordinierten Lösung von konkreten Sicherheitsvorfällen beiträgt.	SIM-01
78.	**Bearbeitung von Sicherheitsvorfällen** Ereignisse, die einen Sicherheitsvorfall darstellen könnten, werden durch qualifiziertes Personal des KRITIS-Betreibers oder in Verbindung mit externen Sicherheitsdienstleistern klassifiziert, priorisiert und einer Ursachenanalyse unterzogen.	SIM-03
79.	**Dokumentation und Berichterstattung über Sicherheitsvorfälle** Alle Sicherheitsvorfälle werden gemäß Informationssicherheitsrichtlinie dokumentiert. Eine verantwortliche Stelle für meldepflichtige Sicherheitsvorfälle ist eingerichtet. Eine Richtlinie ist umgesetzt, die regelt, welche Sicherheitsvorfälle der verantwortlichen Stelle zu melden sind und welche Sicherheitsvorfälle gemäß den Vorgaben aus § 8b Absatz 4 BSIG unverzüglich an das BSI zu melden sind: • Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben • erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können.	SIM-04
80.	**Security Incident Event Management** Protokollierte Vorfälle werden zentral aggregiert und konsolidiert (Event-Korrelation). Regeln zur Erkennung von Beziehungen zwischen Vorfällen und zur Beurteilung gemäß Kritikalität sind implementiert. Die Behandlung dieser Vorfälle erfolgt gemäß dem Security Incident Management Prozess.	SIM-05

2.8 Vorfallserkennung und -bearbeitung

81.	**Verpflichtung der Nutzer zur Meldung von Sicherheitsvorfällen an eine zentrale Stelle** Mitarbeiter und externe Geschäftspartner werden über ihre Verpflichtungen informiert. Falls erforderlich willigen sie dazu ein oder verpflichten sich vertraglich dazu, alle Sicherheitsereignisse zeitnah an eine zuvor benannte zentrale Stelle zu melden. Zusätzlich wird darüber informiert, dass „Falschmeldungen“ von Ereignissen, die sich im Nachhinein nicht als Vorfälle herausstellen, keine negativen Folgen nach sich ziehen.	SIM-06
82.	**Auswertung und Lernprozess** Mechanismen sind vorhanden, um Art und Umfang der Sicherheitsvorfälle messen und überwachen sowie an unterstützende Stellen melden zu können. Die aus der Auswertung gewonnenen Informationen werden dazu verwendet, wiederkehrende oder mit erheblichen Folgen verbundene Vorfälle zu identifizieren und Notwendigkeiten für erweiterte Schutzmaßnahmen festzustellen.	SIM-07

2.9 Überprüfung im laufenden Betrieb

Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Grundlage (C5 #)
83.	**Anlassbezogene Prüfungen – Konzept** Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen sind gemäß Informationssicherheitsrichtlinie dokumentiert, kommuniziert und bereitgestellt, um das zeitnahe Identifizieren und Adressieren von Schwachstellen aller KRITIS-relevanten IT-Systeme, die unter Verantwortung des KRITIS-Betreibers stehen, zu gewährleisten. Die Maßnahmen umfassen unter anderem: • Regelmäßiges Identifizieren und Analysieren von Schwachstellen (Vulnerabilities) • Regelmäßiges Nachhalten von Maßnahmen zum Adressieren identifizierter Maßnahmen (z. B. Einspielen von Sicherheitsaktualisierungen gemäß interner Zielvorgaben).	RB-17
84.	**Umgang mit Schwachstellen, Störungen und Fehlern – Prüfung offener Schwachstellen** Die IT-Systeme, welche der KRITIS-Betreiber für die Entwicklung und Erbringung der kritischen Dienstleistung verwendet, werden mindestens monatlich automatisiert auf bekannte Schwachstellen (Vulnerabilities) geprüft. Im Falle von Abweichungen zu den erwarteten Konfigurationen (u. a. dem erwarteten Patch-Level) werden die Gründe hierzu zeitnah analysiert und die Abweichungen behoben oder gemäß dem Ausnahmeprozess dokumentiert.	RB-21
85.	**Informieren der Unternehmensleitung** Die Unternehmensleitung wird durch regelmäßige Berichte über den Stand der Informationssicherheit auf Grundlage der Sicherheitsprüfungen informiert und ist verantwortlich für die zeitnahe Behebung von daraus hervorgegangenen Feststellungen.	SPN-01
86.	**Interne Überprüfungen der Compliance von IT-Prozessen mit internen Informationssicherheitsrichtlinien und Standards** Qualifiziertes Personal (z. B. Interne Revision) oder durch den Betreiber der kritischen Dienstleistung beauftragte sachverständige Dritte überprüfen jährlich die Compliance der internen IT-Prozesse mit den entsprechenden internen Richtlinien und Standards sowie der für den Betrieb der kritischen Dienstleistung rechtlichen, regulativen und gesetzlich vorgeschriebenen Anforderungen. Die identifizierten Abweichungen werden priorisiert und in Abhängigkeit ihrer Kritikalität werden Maßnahmen zur Behebung zeitnah definiert, nachverfolgt und umgesetzt. Die Prüfung wird regelmäßig durchgeführt. Die Prüfung umfasst auch die Einhaltung der Anforderungen dieses Anforderungskatalogs.	SPN-02

2.9 Überprüfung im laufenden Betrieb

87.	**Prüfungen in anderen, anderweitig vorgegebenen Prüfzyklen – interne IT-Prüfungen** Qualifiziertes Personal (z. B. Interne Revision) des KRITIS-Betreibers oder durch den KRITIS-Betreiber beauftragte sachverständige Dritte überprüfen mindestens jährlich die Compliance der IT-Systeme, soweit diese ganz oder teilweise im Verantwortungsbereich des KRITIS-Betreibers liegen und für die Entwicklung oder den Betrieb der kritischen Dienstleistung relevant sind, mit den entsprechenden internen Richtlinien und Standards sowie der für die kritischen Dienstleistungen relevanten rechtlichen, regulativen und gesetzlich vorgeschriebenen Anforderungen. Die identifizierten Abweichungen werden priorisiert und in Abhängigkeit ihrer Kritikalität werden Maßnahmen zur Behebung zeitnah definiert, nachverfolgt und umgesetzt. Der KRITIS-Betreiber verpflichtet seine Unterauftragnehmer zu solchen Prüfungen und lässt sich die Prüfberichte im gleichen Turnus vorlegen und verwertet sie bei seinen Überprüfungen.	SPN-03
88.	**Prüfungen in anderen, anderweitig vorgegebenen Prüfzyklen – Planung externer Audits** Unabhängige Überprüfungen und Beurteilungen von Systemen oder Komponenten, die zur Erbringung der kritischen Dienstleistung beitragen, sind vom KRITIS-Betreiber so geplant, dass die folgenden Anforderungen erfüllt werden: • Es erfolgt ausschließlich lesender Zugriff auf die kritische Dienstleistung und Daten. • Aktivitäten, die möglicherweise die Verfügbarkeit der IT oder Komponenten beeinträchtigen und so zu Beeinträchtigungen der Verfügbarkeit der kritischen Dienstleistung führen könnten, werden außerhalb der regulären Geschäftszeiten bzw. nicht zu Zeiten von Lastspitzen durchgeführt. • Die durchgeführten Aktivitäten werden protokolliert und überwacht. Der KRITIS-Betreiber hat Vorkehrungen für außerplanmäßige Audits getroffen.	COM-02
89.	**Prüfungen in anderen, anderweitig vorgegebenen Prüfzyklen – Durchführung externer Audits** Prüfungen und Beurteilungen von Prozessen, IT-Systemen und IT-Komponenten, soweit diese ganz oder teilweise im Verantwortungsbereich des KRITIS-Betreibers liegen und für den Betrieb der kritischen Dienstleistung relevant sind, werden mindestens jährlich durch unabhängige Dritte (z. B. Wirtschaftsprüfer) durchgeführt, um Nichtkonformitäten mit rechtlichen, regulativen und gesetzlich vorgeschriebenen Anforderungen zu identifizieren. Die identifizierten Abweichungen werden priorisiert und in Abhängigkeit ihrer Kritikalität werden Maßnahmen zur Behebung zeitnah definiert, nachverfolgt und umgesetzt. Falls notwendig, können außerplanmäßige Überprüfungen durch unabhängige Dritte durchgeführt werden.	COM-03

2.9 Überprüfung im laufenden Betrieb

90.	**Systematische Log-Auswertung – Konzept** Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt, um Ereignisse auf allen Assets, die zur Entwicklung oder zum Betrieb der kritischen Dienstleistung verwendet werden, zu protokollieren und an zentraler Stelle aufzubewahren. Die Protokollierung umfasst definierte Ereignisse, welche die Sicherheit und Verfügbarkeit der kritischen Dienstleistung beeinträchtigen können, einschließlich einer Protokollierung des Aktivierens, Stoppens und Pausierens der verschiedenen Protokollierungen. Die Protokolle werden bei unerwarteten oder auffälligen Ereignissen durch autorisiertes Personal anlassbezogen überprüft, um eine zeitnahe Untersuchung von Störungen und Sicherheitsvorfällen sowie das Einleiten geeigneter Maßnahmen zu ermöglichen. Ergänzende Informationen zur Basisanforderung Sicherheitsrelevante Ereignisse sind u. a. • An- und Abmeldevorgänge • Erstellung, Änderung oder Löschung von Benutzern und Erweiterung der Berechtigungen • Verwendung, Erweiterung und Änderungen von privilegierten Zugriffsberechtigungen • Nutzung von temporären Berechtigungen. Da es sich bei den protokollierten Daten i. d. R. um personenbezogene Daten handelt, sind in dem Fall datenschutzrechtliche Anforderungen an die Aufbewahrung zu beachten und zu überprüfen. Erfahrungsgemäß sollte eine Frist von einem Jahr nicht überschritten werden.	RB-10 RB-14
91.	**Systematische Log-Auswertung – kritische Assets** Der KRITIS-Betreiber führt eine Liste aller protokollierungs- und überwachungskritischen Assets und überprüft diese Liste regelmäßig auf deren Aktualität und Korrektheit. Für diese kritischen Assets wurden Protokollierungs- und Überwachungsmaßnahmen definiert.	RB-12
92.	**Systematische Log-Auswertung – Aufbewahrung** Die erstellten Protokolle werden auf zentralen Protokollierungsservern aufbewahrt, wo sie vor unautorisierten Zugriffen und Veränderungen geschützt sind. Protokolldaten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Zwischen den Protokollierungsservern und den protokollierten Assets erfolgt eine Authentisierung, um die Integrität und Authentizität der übertragenen und gespeicherten Informationen zu schützen. Die Übertragung erfolgt nach einer dem Stand der Technik entsprechenden Verschlüsselung oder über ein eigenes Administrationsnetz (Out-of-Band-Management).	RB-13

2.9 Überprüfung im laufenden Betrieb

93.	**Systematische Log-Auswertung – Konfiguration** Der Zugriff und die Verwaltung der Protokollierungs- und Überwachungsfunktionalitäten ist beschränkt auf ausgewählte und autorisierte Mitarbeiter des KRITIS-Betreibers. Änderungen der Protokollierungen und Überwachungen werden vorab durch unabhängige und autorisierte Mitarbeiter überprüft und freigegeben. Der Zugriff und die Verwaltung der Protokollierungs- und Überwachungsfunktionalitäten erfordert eine Multi-Faktor-Authentifizierung.	RB-15
94.	**Systematische Log-Auswertung – Verfügbarkeit** Die Verfügbarkeit der Protokollierungs- und Überwachungssoftware wird unabhängig überwacht. Bei einem Ausfall der Protokollierungs- und Überwachungssoftware werden die verantwortlichen Mitarbeiter umgehend informiert. Die Protokollierungs- und Überwachungssoftware ist redundant vorhanden, um auch bei Ausfällen die Sicherheit und Verfügbarkeit der Systeme der kritischen Dienstleistung zu überwachen.	RB-16
95.	**Penetrationstest** Der KRITIS-Betreiber lässt mindestens jährlich Penetrationstests durch qualifiziertes internes Personal oder externe Dienstleister durchführen. Die Penetrationstests erfolgen nach einer dokumentierten Testmethodik und umfassen die für den sicheren Betrieb der kritischen Dienstleistung als kritisch definierte Infrastruktur-Komponenten, die im Rahmen einer Risiko-Analyse als solche identifiziert wurden. Art, Umfang Zeitpunkt/Zeitraum und Ergebnisse werden für einen sachverständigen Dritten nachvollziehbar dokumentiert. Feststellungen aus den Penetrationstests werden bewertet und mindestens bei mittlerer bis sehr hoher Kritikalität in Bezug auf die Vertraulichkeit, Integrität oder Verfügbarkeit der kritischen Dienstleistung nachverfolgt und behoben. Die Einschätzung der Kritikalität und der mitigierenden Maßnahmen zu den einzelnen Feststellungen werden dokumentiert.	RB-18
96.	**Umgang mit Schwachstellen, Störungen und Fehlern – Integration mit Änderungs- und Incident-Management** Richtlinien und Anweisungen mit technischen und organisatorischen Maßnahmen für den Umgang mit kritischen Schwachstellen sind gemäß SA-01 dokumentiert, kommuniziert und bereitgestellt. Die Maßnahmen sind mit den Aktivitäten des Änderungsverfahrens (Change Management) und der Störungs- und Fehlerbehebung (Incident Management) abgestimmt.	RB-19

2.10 Externe Informationsversorgung und Unterstützung

Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Grundlage (C5 #)
97.	**Kontakt zu relevanten Behörden und Interessenverbänden** Angemessene und für den Anbieter der kritischen Dienstleistung relevante Kontakte zu Behörden und Interessenverbänden sind etabliert, um stets über aktuelle Bedrohungslagen und Gegenmaßnahmen informiert zu sein und zeitnah und angemessen darauf zu reagieren. Es sind Verfahren definiert und dokumentiert, um die erhaltenen Informationen an die internen und externen Mitarbeiter des Anbieters der kritischen Dienstleistung zu kommunizieren und zeitnah und angemessen darauf zu reagieren.	OIS-05

2.11 Lieferanten, Dienstleister und Dritte

Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Grundlage (C5 #)
98.	**Richtlinie zum Umgang mit und Sicherheitsanforderungen an Dienstleister des KRITIS-Betreibers** Richtlinien und Anweisungen zur Sicherstellung des Schutzes von Informationen (insb. deren Verfügbarkeit) auf sonstige Dritte (z. B. Dienstleister bzw. Lieferanten des KRITIS-Betreibers), die wesentliche Teile für den Betrieb der kritischen Dienstleistung beitragen, sind gemäß IT-Informationssicherheitsrichtlinie dokumentiert, kommuniziert und bereitgestellt. Die Vorgaben dienen der Reduzierung von Risiken, die durch die Auslagerung von IT-Systemen entstehen können. Dabei werden mindestens die folgenden Aspekte berücksichtigt: • Definition und Beschreibung von Mindest-Sicherheitsanforderungen in Bezug auf die verarbeiteten Informationen, die sich an etablierten Informationssicherheitsstandards orientieren • Anforderungen an das Incident- und Vulnerability-Management (insb. Benachrichtigungen und Kollaborationen während einer Störungsbehebung) • Weitergabe und vertragliche Verpflichtung auf die Mindest-Sicherheitsanforderungen auch an Unterauftragnehmer, wenn diese nicht nur unwesentliche Teile zu Entwicklung oder Betrieb der kritischen Dienstleistung (z. B. RZ-Dienstleister) beitragen • die Definition der Anforderungen ist in das Risikomanagement des KRITIS-Betreibers eingebunden. Diese müssen regelmäßig auf ihre Angemessenheit hin überprüft werden. (vgl. Nr. 14)	DLL-01
99.	**Kontrolle der Leistungserbringung und der Sicherheitsanforderungen an Dienstleister und Lieferanten des KRITIS-Betreibers** Verfahren zur regelmäßigen Überwachung und Überprüfung der vereinbarten Leistungen und Sicherheitsanforderungen von Dritten (z. B. Dienstleister bzw. Lieferanten des KRITIS-Betreibers), die wesentliche Teile für den Betrieb der kritischen Dienstleistung beitragen, sind implementiert. Die Maßnahmen umfassen mindestens: • Regelmäßige Kontrolle von Dienstleistungsberichten (z. B. SLA-Reportings), soweit diese von Dritten erbracht werden • Überprüfung von sicherheitsrelevanten Vorfällen, Betriebsstörungen oder Ausfällen und Unterbrechungen, die mit der Dienstleistung zusammenhängen • außerplanmäßige Überprüfungen nach wesentlichen Änderungen der Anforderungen oder des Umfelds. Die Notwendigkeit für außerplanmäßige Überprüfungen ist durch den KRITIS-Betreiber zu beurteilen und nachvollziehbar zu dokumentieren. Festgestellte Abweichungen werden gemäß der Anforderung OIS-07 (vgl. Nr. 14) einer Risikoanalyse unterzogen, um diese zeitgerecht durch mitigierende Maßnahmen wirksam zu adressieren.	DLL-02

2.12 Meldewesen

Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Grundlage (C5 #)
100.	**Einrichtung einer Kontaktstelle** Der Betreiber hat die Aufgaben und Zuständigkeiten für die Entgegennahme der Vorfallsmeldungen, deren Beurteilung sowie Weiterleitung an das BSI geregelt. Hierzu hat er eine Kontaktstelle gemäß § 8b Absatz 3 BSIG eingerichtet.	keine