EIN PROJEKT
DES IT-PLANUNGSRATS

DEUTSCHE VERWALTUNGSCLOUD

Eigenerklärung zum DVC Reifegradmodell

NAME des ANBIETERS	
NAME des Cloud-Services	
Version des Cloud-Services	
Alle Daten sind korrekt aufgenommen und erfasst worden. Einer Veröffentlichung der Daten stimmen wir zu.	

In der Kompaktansicht finden Sie alle wichtigen Informationen auf einen Blick.
Eine detaillierte Ansicht finden Sie auf den nachfolgenden Seiten.

Das **DVC-Stufenmodell** repräsentiert verschiedene Aspekte der Cloud-Services und hilft Kunden dabei, den richtigen Service für die eigenen Anforderungen zu identifizieren. Ob eine höhere Stufe und die damit verbundenen Kosten benötigt werden, obliegt

Die **Erweiterte Dimensionen für das DVC-Stufenmodell** beinhaltet einen Ausschnitt des HV-Benchmark kompakt und erlaubt Kunden die Beurteilung der Anbieter-Organisation, auch wenn diese den HV-Benchmark kompakt noch nicht vollumfänglich

Der **HV-Benchmark kompakt** wird genutzt, um die Reife der Organisation des Anbieters zu beurteilen. Der HV-Benchmark kompakt wurde vom BSI entwickelt und betrachtet diverse Aspekte der Informationssicherheit und Verfügbarkeit einer Organisation. Zudem schafft diese Beurteilung eine Transparenz für Kunden, da so eine Vergleichbarkeit der verschiedenen Anbieter hergestellt werden kann.

1) Selbsteinschätzung des Anbieters zum Cloud-Service

DVC Stufenmodell

Name	Stufe
Skalierbarkeit	0
AutoScaling	0
Barrierefreiheit	0
Neuer Programmstand	0
Bereitstellung IaaS	0
Mandantentrennung	0
Verbrauchsmonitoring	0
Verbrauchs-Reporting	0
Bestellprozess	0
Servicezeiten	0
Störung	0
Benutzerdokumentation	0
Technische Dokumentation	0
Verfügbarkeit	0
Inhalts-Verschlüsselung	0
Transport-Verschlüsselung	0
Backups	0
Authentisierung	0
Autorisierung	0
SBOM	0
Datenschutz	0
Leistungsort	0
Export von Kundendaten	0
Export von Konfiguration	0
Open Source	0

Erweiterte Dimensionen für das DVC Stufenmodell (falls HV-Benchmark kompakt nicht vorliegt)

Name	Stufe
Indikator I.1 Informationssicherheitsmanagementsystem ISMS)	0
Indikator I.3 Notfall- und Krisenmanagement	0
Indikator I.5 Infrastruktur, Grundlagen und Planung	0
Indikator I.18 Ausfallsicherheit/Redundanzkonzept	0
Indikator I.23 Server-Sicherheit	0
Indikator I.24 Datensicherheit der Speicher	0
Indikator I.25 Datenreplikation und -sicherung	0
Indikator I.26 Energieversorgung: Unterbrechungsfreie Stromversorgung	0
Indikator I.32 Monitoring der technischen Infrastruktur	0
Indikator I.33 Monitoring auf IT-Sicherheitsvorfälle / Logging	0
Indikator I.34 Monitoring der IT-Komponenten und -Dienste auf Verfügbarkeit	0

2) Selbsteinschätzung des Anbieters zur Anbieterorganisation

HV Benchmark Kompakt

Name	Stufe
Indikator I.1 Informationssicherheitsmanagementsystem ISMS)	0
Indikator I.2 Risikomanagement im Zusammenhang mit der IT-Dienstleistungserbringung	0
Indikator I.3 Notfall- und Krisenmanagement	0
Indikator I.4 Verfahren zur Einhaltung rechtlicher und organisatorischer Vorgaben durch das Personal	0
Indikator I.5 Infrastruktur, Grundlagen und Planung	0
Indikator I.6 Availability Management (Verfügbarkeitsmanagement): Messung und Steuerung der Verfügbarkeit	0
Indikator I.7 Capacity Management (Kapazitätsmanagement): Messung und Steuerung der Kapazität	0
Indikator I.8 IT-Service Continuity Management: IT-Notfallplanung (ITSCM-Rahmenwerk)	0
Indikator I.9 IT-Service Continuity Management: Datensicherungen	0
Indikator I.10 IT-Sicherheitskonzepte: Mandantentrennung	0
Indikator I.11 IT-Sicherheitskonzepte: ID- und Rechtemanagement	0
Indikator I.12 IT-Sicherheitskonzepte: Kryptografie	0
Indikator I.13 IT-Sicherheitskonzepte: Sichere Datenlöschung und Aussonderung	0
Indikator I.14 IT-Sicherheitskonzepte: Schutz gegen Schadprogramme und netzbasierte Angriffe	0
Indikator I.15 Incident Management: Sicherheitsvorfallbehandlung	0
Indikator I.16 Patch- und Releasemanagement (Software)	0
Indikator I.17 Trennung von Entwicklungs-, Test- und Produktionsumgebungen	0
Indikator I.18 Ausfallsicherheit/Redundanzkonzept	0
Indikator I.19 Netzwerk-Segmentierung	0
Indikator I.20 Sicherheit der aktiven Netzwerkkomponenten	0
Indikator I.21 Ausgestaltung der WAN-Anbindung zwischen den IT-Standorten	0
Indikator I.22 Sicherheit der Internet-Anbindung	0
Indikator I.23 Server-Sicherheit	0
Indikator I.24 Datensicherheit der Speicher	0
Indikator I.25 Datenreplikation und -sicherung	0
Indikator I.26 Energieversorgung: Unterbrechungsfreie Stromversorgung	0
Indikator I.27 Energieversorgung: Einsatz einer Netzersatzanlage	0
Indikator I.28 Technischer Brandschutz des Rechenzentrums	0
Indikator I.29 Gebäudesicherheit: Schutz gegen Einbruch und Sabotage	0
Indikator I.30 Gebäudesicherheit: Technische/bauliche Maßnahmen zum Zutrittsschutz	0
Indikator I.31 Sicherheit der Verzeichnisdienste	0
Indikator I.32 Monitoring der technischen Infrastruktur	0
Indikator I.33 Monitoring auf IT-Sicherheitsvorfälle / Logging	0
Indikator I.34 Monitoring der IT-Komponenten und -Dienste auf Verfügbarkeit	0

Funktionelles:

Im Bereich Funktionelles werden Anforderungen zur Skalierung, Barriefreiheit und zum Umgang mit Updates definiert

	Antwort	Kommentarfeld	Keine Stufe	Stufe 1: Minimalkriterien		Stufe 2		Stufe 3		Stufe 4		Stufe 5: Optimiert	
Skalierbarkeit	**0**		**Noch keine Stufe erreicht**									F1d	Der Service ist gemäß NIST skalierbar und es kann beliebig viel Leistung manuell dazugebucht werden. (Im Falle von AutoScaling kann auf das manuelle Zubuchen verzichtet werden)
AutoScaling	**0**		**Noch keine Stufe erreicht**									F2a	Der Service unterstützt AutoScaling, so dass ein konstantes Systemverhalten bei unterschiedlichen Last-Aufkommen möglich ist. Für das AutoScaling können Obergrenzen definiert werden.
Barrierefreiheit	**0**		**Noch keine Stufe erreicht**					F3a	Für Funktionen, die eine Interaktion ermöglichen, werden die Erfolgskriterien der WCAG 2.1 mit der Konformitätsstufe A beachtet.	F3b	Für Funktionen, die eine Interaktion ermöglichen, werden die Erfolgskriterien der WCAG 2.1 mit der Konformitätsstufe AA beachtet.	F3c	Die Anforderungen der BITV 2.0 werden erfüllt (gemäß Anwendungsbereich §2 BITV 2.0).
Neuer Programmstand	**0**		**Noch keine Stufe erreicht**	F4a	Neue Programmstände werden eine angemessene Zeit im Voraus inkl. Zeitpunkt und Dauer des geplanten Wartungsfensters angekündigt. (In sicherheitsrelevanten Notfällen ist die angemessene Zeit deutlich reduziert. Eine Ankündigung muss dennoch erfolgen).	F4b	Neue Programmstände werden eine angemessene Zeit im Voraus inkl. Zeitpunkt und Dauer des geplanten Wartungsfensters angekündigt. Die Dauer des Wartungsfensters beträgt maximal 8 Stunden und liegt außerhalb der Servicezeiten (außer es liegt 24/7 vor, aber dennoch außerhalb der Geschäftszeiten).	F4c	Neue Programmstände werden eine angemessene Zeit im Voraus inkl. Zeitpunkt und Dauer des geplanten Wartungsfensters angekündigt. Die Dauer des Wartungsfensters beträgt maximal 4 Stunden und liegt außerhalb der Servicezeiten (außer es liegt 24/7 vor, aber dennoch außerhalb der Geschäftszeiten).	F4d	Neue Programmstände werden eine angemessene Zeit im Voraus inkl. Zeitpunkt und Dauer des geplanten Wartungsfensters angekündigt. Die Dauer des Wartungsfensters beträgt maximal 1 Stunde und liegt außerhalb der Servicezeiten (außer es liegt 24/7 vor, aber dennoch außerhalb der Geschäftszeiten).	F4e	Neue Programmstände werden eine angemessene Zeit im Voraus angekündigt und im laufenden Betrieb unterbrechungsfrei eingespielt.
Bereitstellung	**0**		**Noch keine Stufe erreicht**			F5a	Bestellte Services werden innerhalb von 4 Wochen bereitgestellt, so dass diese durch den Kunden nutzbar bzw. kundenseitig konfigurierbar sind.	F5b	Bestellte Services werden innerhalb von einer Woche bereitgestellt, so dass diese durch den Kunden nutzbar bzw. kundenseitig konfigurierbar sind.	F5c	Bestellte Services werden automatisiert innerhalb von 1 Tag bereitgestellt, so dass diese durch den Kunden nutzbar bzw. kundenseitig konfigurierbar sind.	F5d	Bestellte Services werden automatisiert in unter 15 Minuten bereitgestellt, so dass diese durch den Kunden nutzbar bzw. kundenseitig konfigurierbar sind.
Mandantentrennung	**0**		**Noch keine Stufe erreicht**	F7a	Der Service unterstützt eine nach aktuellem Stand der Technik sichere Art der Mandantentrennung.								

Abrechnung:

Im Bereich Abrechnung werden Anforderungen zu den Verbrauchsdaten und dem Bestellprozess definiert.

	Antwort	Kommentarfeld	Keine Stufe	Stufe 1: Minimalkriterien		Stufe 2		Stufe 3		Stufe 4		Stufe 5: Optimiert	
Verbrauchsmonitoring	**0**		**Noch keine Stufe erreicht**					A1a	Ein Verbrauchsmonitoring ist auf Anfrage möglich.	A1b	Das Verbrauchsmonitoring erfolgt automatisiert und fortlaufend.	A1c	Das Verbrauchsmonitoring erfolgt automatisiert und fortlaufend und ist zudem an die zugehörige DVC API angebunden.
Verbrauchs-Reporting	**0**		**Noch keine Stufe erreicht**					A2a	Ein Verbrauchsreporting ist auf Anfrage möglich.	A2b	Ein Verbrauchs-Reporting wird dem Kunden automatisch und fortlaufend zur Verfügung gestellt.	A2c	Das Verbrauchs-Reporting wird dem Kunden automatisch und fortlaufend zur Verfügung gestellt und ist zusätzlich an die DVC API angebunden (vgl. A1c).
Bestellprozess	**0**		**Noch keine Stufe erreicht**	A3a	Der Service ist im Self-Service bestellbar.	A3b	Der Service ist im Self-Service bestellbar und kündbar.	A3c	Der Service ist im Self-Service bestellbar und kündbar. Die Service-Konditionen sind dynamisch nach jeder Abrechnungsperiode anpassbar.	A3d	Der Service ist im Self-Service bestellbar und kündbar. Die Service-Konditionen sind jederzeit dynamisch anpassbar.	A3e	Wie A3d, zudem ist der Service auch im Self-Service pausierbar (eine Grundgebühr für die Bereitschaft kann weiterhin erhoben werden).

Service & Support:

Im Bereich Service & Support werden Anforderungen zur Verfügbarkeit, zum Reporting und zur Dokumentation definiert

	Antwort	Kommentarfeld	Keine Stufe	Stufe 1: Minimalkriterien		Stufe 2		Stufe 3		Stufe 4		Stufe 5: Optimiert	
Servicezeiten	**0**		**Noch keine Stufe erreicht**			S1a	Die Servicezeiten (i.S.d. EVB-IT Cloud-AGB) des Supports umfassen mindestens 40 Stunden pro Woche.	S1b	Die Servicezeiten (i.S.d. EVB-IT Cloud-AGB) des Supports umfassen mindestens 45 Stunden pro Woche in Form von 9/5.	S1c	Die Servicezeiten (i.S.d. EVB-IT Cloud-AGB) des Supports umfassen mindestens 63 Stunden pro Woche in Form von 9/7.	S1d	Die Servicezeiten (i.S.d. EVB-IT Cloud-AGB) des Supports umfassen 168 Stunden pro Woche (24/7).
Störung	**0**		**Noch keine Stufe erreicht**	S2a	Für den Service existieren dedizierte Kanäle zur strukturierten Annahme von Störungen.			S2b	Wie S2a, zudem kann der Status der einzelnen Störungsmeldungen kann (vom Kunden) transparent nachvollzogen werden.	S2c	Wie S2a, zudem ermöglicht die Dokumentation der Störungen eine übergreifende Auswertung der Störungen durch den Kunden.	S2d	Wie S2c, zudem wird die Annahme und Bearbeitung von Störungsmeldungen durch ein Ticketsystem abgebildet, das an das zentrale Ticketsystem des CSP angebunden ist.
Benutzerdokumentation	**0**		**Noch keine Stufe erreicht**	S3a	Eine Benutzer-Dokumentation für alle wesentlichen Funktionen ist vorhanden und für Kunden des CSP online verfügbar.							S3b	Wie S3a, zudem beinhaltet die Benutzer-Dokumentation interaktive oder visuelle Elemente zur besseren Veranschaulichung für die wesentlichen Funktionen.
Technische Dokumentation	**0**		**Noch keine Stufe erreicht**							S4a	Eine technische Dokumentation zur Konfiguration und Administration des Services ist vorhanden und für Kunden des CSPs einsehbar.	S4b	Wie S4a, zudem enthält die technische Dokumentation aussagekräftige Beispiele zur Lösung spezifischer Fragestellungen im Rahmen der Konfiguration und Administration des Services (z.B. Beispiel-Code zur Interaktion mit Schnittstellen).
Verfügbarkeit	**0**		**Noch keine Stufe erreicht**			S5a	Der Service erfüllt die Verfügbarkeitsklasse 1 gemäß HV Kompendium des BSI Band G, Kapitel 2 (99.0% Verfügbarkeit mit einer Ausfallzeit < 8 h pro Monat)	S5b	Der Service erfüllt die Verfügbarkeitsklasse 2 gemäß HV Kompendium des BSI Band G, Kapitel 2 (99.9% Verfügbarkeit mit einer Ausfallzeit < 44 min pro Monat)	S5c	Der Service erfüllt die Verfügbarkeitsklasse 3 gemäß HV Kompendium des BSI Band G, Kapitel 2 (99.99% Verfügbarkeit mit einer Ausfallzeit < 5 min pro Monat)	S5d	Der Service erfüllt die Verfügbarkeitsklasse 3 gemäß HV Kompendium des BSI Band G, Kapitel 2 (99.999% Verfügbarkeit mit einer Ausfallzeit < 26 s pro Monat)

Informationssicherheit & Datenschutz:

Im Bereich Informationssicherheit & Datenschutz werden Anforderungen an Zugriffsrechte und Datensicherheit definiert.

	Antwort	Kommentarfeld	Keine Stufe	Stufe 1: Minimalkriterien		Stufe 2		Stufe 3		Stufe 4		Stufe 5: Optimiert	
Inhalts-Verschlüsselung	**0**		**Noch keine Stufe erreicht**							I1a	Die Kunden-Daten können gemäß BSI TR-02102-1 verschlüsselt abgespeichert werden und die Verschlüsselung ist kundenseitig de-/aktivierbar.	I1b	Wie I1a, zudem können Backups, welche Kundendaten beinhalten, verschlüsselt abgespeichert werden.
Transport-Verschlüsselung	**0**		**Noch keine Stufe erreicht**	I2a	Alle Verbindungen zum Service sind gemäß BSI TR-02102 transportverschlüsselt.					I2b	Wie I2a, zudem ist der Service gegen Rückwärts-Kompatibilität von Protokollen abgesichert, so dass keine schwächere oder ältere Verschlüsselungsmethode eingesetzt werden kann (z.B. mittels Perfect Forward Secrecy (PFS)).	I2c	Wie I2b, zudem ist im Service eine End-to-End-Verschlüsselung implementiert, bei der Daten vom Ursprung bis zum Ziel durchgängig verschlüsselt bleiben, ohne dass Service-Anbieter Zugriff auf die Klartext-Daten haben.
Backups	**0**		**Noch keine Stufe erreicht**	I3a	Im Service erfolgt während der gesamten Nutzungsdauer ein regelmäßiges Backup der Kundendaten, um eine Wiederherstellung durch den Anbieter bei einem Ausfall zu ermöglichen (Disaster Recovery)			I3b	Wie I3a, zudem ermöglicht der Service einen Restore einzelner Datensätze und/oder Dateien.	I3c	Wie I3b, zusätzlich wird die erfolgreiche Ausführung der Backups überwacht und zugehörige Benachrichtigungen an den Kunden ausgelöst, sofern ein Backup fehlschlägt.	I3d	Wie I3c, zudem werden die Backup & Restore Funktionalitäten dem Kunden im Self-Service angeboten. Zusätzlich werden alle Backups mindestens monatlich auf Integrität geprüft.
Authentisierung	**0**		**Noch keine Stufe erreicht**	I5a	Der Service besitzt ein Authentisierungsverfahren.					I5b	Der Service besitzt ein Authentisierungsverfahren, welches die Anbindung eines externen Identity Provider über gängige Standard-Protokolle unterstützt.	I5c	Das Authentisierungsverfahren des Services ist an das IAM der DVC angebunden.
Autorisierung	**0**		**Noch keine Stufe erreicht**	I4a	Der Service besitzt ein Autorisierungverfahren			I4b	Das Autorisierungsverfahren des Services erlaubt die Zuweisung von Standard Rollen und Berechtigungen durch den Kunden.	I4c	Wie I4b, zudem erlaubt das Autorisierungsverfahren des Services eine feingranulare Erstellung und Zuweisung von Rollen und Berechtigungen durch den Kunden. (d.h. auf Objekt-, Funktionsebene und/oder in vergleichbarer Granularität)	I4d	Wie I4c, zudem ist das Autorisierungsverfahren des Service an das IAM der DVC angebunden.
SBOM	**0**		**Noch keine Stufe erreicht**			I6a	Eine SBOM liegt immer für den aktuellen Programmstand des Services in einem auswertbaren Format vor.	I6b	Die SBOM wird dem Kunden auf Anfrage zur Verfügung gestellt.	I6c	Für den Service erfolgt eine fortlaufende SBOM Analyse basierend auf den aktuellen Common Vulnerabilities and Exposures (CVEs).	I6d	Die SBOM erfüllt BSI TR-03183 Teil 2.
Datenschutz	**0**		**Noch keine Stufe erreicht**	I7a	Der Service ist DSGVO-konform.					I7b	Wie I7a, zudem sind die hinsichtlich des Services getroffenen technischen und organisatorischen Maßnahmen mindestens für eine Verarbeitung von Daten mit hohem Schutzbedarf ausgelegt.	I7c	Wie I7a, zudem sind die hinsichtlich des Services getroffenen, technischen und organisatorischen Maßnahmen mindestens für eine Verarbeitung von Daten mit sehr hohem Schutzbedarf ausgelegt.

Digitale Souveränität:

Im Bereich Digitale Souveränität werden Anforderungen an den Leistungsort und den Betreiberwechsel gestellt.

	Antwort	Kommentarfeld	Keine Stufe	Stufe 1: Minimalkriterien		Stufe 2		Stufe 3		Stufe 4		Stufe 5: Optimiert	
Leistungsort	**0**		**Noch keine Stufe erreicht**	D1a	Die Speicherung und sonstige Verarbeitung von Daten des Kunden (einschließlich Metadaten) erfolgt ausschließlich innerhalb der EU und des EWR sowie der Schweiz.							D1b	Die Speicherung und sonstige Verarbeitung von Daten des Kunden (einschließlich Metadaten) erfolgt ausschließlich in Deutschland.
Export von Kundendaten	**0**		**Noch keine Stufe erreicht**					D2a	Der Service bietet einen Export der Kunden-Daten und ihrer Beziehungen in einem nachnutzbaren Datenformat wie bspw. CSV oder JSON an, welcher im Self-Service ausgeführt werden kann.	D2b	Der Service bietet eine oder mehrere APIs an, um eine direkte Übernahme der Kunden-Daten und ihrer Beziehungen in eine Nachfolgelösung zu ermöglichen.	D2c	Wie D2b, zudem gibt es für den Service beschriebene Vorgehensweisen und technische Werkzeuge, welche dem Kunden bei einem Anbieterwechsel umfassend unterstützen.
Export von Konfiguration	**0**		**Noch keine Stufe erreicht**							D3a	Der Kunde kann seine Konfigurationen in den jeweils zur Konfiguration gehörenden Datenformaten exportieren.	D3b	Zum Service existiert eine beschriebene Vorgehensweise, um Konfigurationen des Kundens zu exportieren.
Open Source	**0**		**Noch keine Stufe erreicht**					D4a	Sämtliche Bestandteile des Services auf Applikationsebene sind OpenSource.	D4b	Wie D4a, zudem sind alle wesentlichen Infrastrukturkomponenten des Service (Datenbank, Betriebssystem, Server etc.) Open Source.	D4c	Wie D4b, zudem ist der Code der Open Source-Komponenten im Open CoDE Repository hinterlegt.

Erweiterte Dimension für das DVC Stufenmodell (falls HV-Benchmark kompakt nicht vorliegt):

Dieser beinhaltet einige Teile aus dem HV-Benchmark und muss nur ausgefüllt werden, wenn der HV Benchmark nicht komplett ausgefüllt wird

	Antwort	Kommentarfeld	Keine Stufe		Potentialstufe 1		Potentialstufe 2		Potentialstufe 3		Potentialstufe 4		Potentialstufe 5
Indikator I.1 Informationssicherheitsmanagementsystem (ISMS)	**0**		**Noch keine Stufe erreicht**	H1a	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)?	H1b	2.1. 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? 2.2. Sind die dafür notwendigen technischen und personellen Ressourcen vorhanden?	H1c	3. Sind die erforderlichen Dokumentationen (z. B. Sicherheitskonzepte) vollständig, richten sich am BSI IT-Grundschutz oder ISO 27001 aus und umfassen mindestens Folgen- des: 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?	H1d	4.1. Wird im Rahmen von regelmäßigen Sicherheitsaudits die Einhaltung der sicherheits-relevanten Maßnahmen und Prozesse entsprechend ihrer Vorgaben überprüft? 4.2. Werden erkannte Defizite abgestellt?	H1e	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?
Indikator I.3 Notfall- und Krisenmanagement	**0**		**Noch keine Stufe erreicht**	H3a	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?	H3b	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?	H3c	3.1. 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? 3.2. 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?	H1d	4.1. 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? 4.2. Führen die Überprüfungen dazu, dass erkannte Lücken zwischen Soll und Ist geschlossen werden?	H1e	5.1. Erfolgen regelmäßig Reviews und unabhängige Audits des Notfall- und Krisenmanagements insgesamt, insbesondere hinsichtlich seiner Funktionsfähigkeit und Effektivität, unter Einbeziehung der Ergebnisse aus 4? 5.2. Führen die Überprüfungen zu einer Optimierung der Konzepte, Verfahren, Prozesse, Rollen, Maßnahmen, Räumlichkeiten etc. des Notfall- und Krisenmanagements?
Indikator I.5 Infrastruktur, Grundlagen und Planung	**0**		**Noch keine Stufe erreicht**	H5a	1.1. Sind in der Organisation Verantwortliche benannt, die sich um die Berücksichtigung aller in der Kurzbeschreibung genannten Aspekte bei Planung und Betrieb des Gebäudes kümmern? 1.2. Wird eine enge Zusammenarbeit der Verantwortlichen gelebt?	H5b	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?	H5c	3.1. 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? 3.2. Ist dieses Konzept vollständig dokumentiert und umgesetzt?	H1d	4.1. Erfolgt eine regelmäßige Überprüfung, ob die Anforderungen eingehalten werden? 4.2. 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? 4.3. Werden bei Abweichungen von den Vorgaben entsprechende Verbesserungsmaßnahmen eingeleitet und deren Umsetzung nachgehalten?	H1e	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?
Indikator I.18 Ausfallsicherheit/Redundanzkonzept	**0**		**Noch keine Stufe erreicht**	H18a	1.1. 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.] 1.2. Werden für die Erbringung der IT-Services ausschließlich solche Hardware- und Infrastrukturkomponenten verwendet, die für den Betrieb in Rechenzentren und Serverräumen ausgelegt sind?	H18b	2.1. 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? 2.2. Stellen beide räumlichen Bereiche mindestens anforderungskonformen Schutz bereit?	H18c	3.1. 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? 3.2. Sind diese Bereiche hinsichtlich der übrigen Schutzmerkmale anforderungskonform mindestens gleichwertig? 3.3. Findet ein Failover zwischen den redundanten Systemen ohne für den Nutzer relevante Verzögerungen oder sonstige Auswirkungen statt?	H1d	4.1. Sind sowohl die IT-Services als auch die für die Erbringung der IT-Services erforderlichen Infrastrukturen, IT- und Netzwerkkomponenten redundant auf georedundante Standorte verteilt? 4.2. 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).]	H1e	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?
Indikator I.23 Server-Sicherheit	**0**		**Noch keine Stufe erreicht**	H23a	1.1. Sind für alle Server Härtungskonzepte vorhanden (z. B. Sicherheitsmaßnahmen nach IT-Grundschutz „Standardniveau") und umgesetzt? 1.2. Werden aktuelle Sicherheitsupdates zeitnah installiert und ist ein stets aktueller Schutz gegen Schadprogramme aktiv?	H23	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?	H23c	3. Ist die Härtung der Systeme vollständig dokumentiert und gibt es Prozesse, die einen aktuellen Stand der Härtung sicherstellen?	H1d	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?	H1e	5.1. Werden die Härtungskonzepte regelmäßig überprüft? 5.2. Fließen auch die Ergebnisse der Reviews und Pentests in den weiteren Härtungsprozess mit ein, so dass die Härtungsverfahren und -konzepte systematisch verbessert werden?
Indikator I.24 Datensicherheit der Speicher	**0**		**Noch keine Stufe erreicht**	H24a	1. Sind die Speichersysteme gemäß IT-Grundschutz eingerichtet (z. B. eine verschlüsselte Datenablage gemäß Schutzbedarf)?	H24b	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?	H24	3.1. Werden die Systemmeldungen der Speichersysteme automatisiert auf Verletzungen der Datensicherheit überprüft? 3.2. Sind für Zonen mit besonderem Schutzbedarf dedizierte Speichernetze eingerichtet?	H1d	4.1. Erfolgt zwischen (geo-)redundanten Standorten eine automatische Datensynchronisation und werden dabei Sicherheitsmaßnahmen gegen mögliche Verluste der Vertraulichkeit und der Integrität getroffen? 4.2. Ist das Datensicherheitskonzept an allen Standorten gleichermaßen umgesetzt?	H1e	5. Wird die korrekte Umsetzung des Datensicherheitskonzepts für die Speichersysteme regelmäßig durch Reviews und technische Tests überprüft und werden erkannte Schwachstellen eliminiert?

Indikator I.25 Datenreplikation und -sicherung	**0**		**Noch keine Stufe erreicht**	H25a	1.1. Sind die Daten, die über Replikationsmechanismen und/oder Backup geschützt werden müssen, identifiziert? 1.2. Sind diese Maßnahmen umgesetzt? Wurde anhand von Funktionstests nachgewiesen, ob bei einem Ausfall des (Haupt-)Datenträgers auf den redundanten Datenträger umgeschaltet werden kann? 1.3. Wurde das Wiedereinspielen der Daten aus dem Backup (Restore) getestet?	H25b	2.1. Ist im Rahmen der mit dem Kunden getroffenen Vereinbarungen (z. B. SLA) eine Wiederherstellung von Daten auf Wunsch der Informationseigner möglich? 2.2. 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?	H25c	3. Werden Datensicherungen an externe Orte, die ein gleichwertiges Sicherheitsniveau haben, ausgelagert?	H1d	4.1. Werden die Daten gemäß Fragen 1-3 zwischen mindestens zwei georedundanten Standorten repliziert? 4.2. Und werden diese Daten an beiden Standorten gesichert? 4.3. Ist das gesamte Speichernetz georedundant ausgelegt?	H1e	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)?
Indikator I.26 Energieversorgung: Unterbrechungsfreie Stromversorgung	**0**		**Noch keine Stufe erreicht**	H26a	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.]	H26b	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.]	H26c	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.]	H1d	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.]	H1e	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?
Indikator I.32 Monitoring der technischen Infrastruktur	**0**		**Noch keine Stufe erreicht**	H32a	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?	H32b	2.1. Ist eine automatisch arbeitende Störungsmeldung/-übertragung für die wesentlichen Infrastrukturkomponenten (z. B. Strom, Klima, Wasser) implementiert? 2.2. Werden mindestens technisch sortierte Gruppenmeldungen zu einer 24/7-besetzten Interventionsstelle übertragen, die auf Basis vorgegebener Kriterien angemessen auf die Meldungen reagiert?	H32c	3. Erfolgen die Meldungen für jeden Sensor individuell (also keine Gruppenmeldungen) und erfolgen die Meldungen in klar verständlichem Text mit ersten Handlungsanwei- sungen?	H1d	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.]	H1e	5.1. Gibt es zusätzlich zum lokalen Monitoring an den georedundanten Standorten auch ein zentrales Monitoring, an dem die Meldungen aller Standorte auflaufen? 5.2. Ist die Übertragung der Störungsmeldungen durch redundante, verschlüsselte Leitungen abgesichert?
Indikator I.33 Monitoring auf IT-Sicherheitsvorfälle / Logging	**0**		**Noch keine Stufe erreicht**	H33a	1.1. 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? 1.2. Ist dieser Zeitraum ausreichend, um Vorfälle angemessen aufzuklären?	H33b	2.1. Melden die IT-Systeme sicherheitsrelevante Vorgänge an zentrale Systeme zur Speicherung? 2.2. Sind diese Systeme in die Datensicherung eingebunden? 2.3. 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?	H33c	3.1. 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)? 3.2. Kommt ein IDS zum Einsatz? Sind die Vorgaben zum Monitoring vollständig umgesetzt?	H1d	4.1. Werden die Systeme automatisch auf andere, d. h. außergewöhnliche Sicherheitsvorfälle überwacht (z. B. mittels SIEM)? 4.2. Wird regelmäßig geprüft, ob die Log-Daten den Vorgaben entsprechend im erforderlichen Umfang erhoben und ausgewertet werden?	H1e	5.1. 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? 5.2. Werden die Vorgaben/Anforderungen an das Monitoring regelmäßig überprüft? 5.3. Entsprechen sie dem jeweils aktuellen Stand?
Indikator I.34 Monitoring der IT-Komponenten und -Dienste auf Verfügbarkeit	**0**		**Noch keine Stufe erreicht**	H34a	1. Existiert ein Monitoring zur Messung der Verfügbarkeit der kritischen IT-Komponen- ten und wird das Incident-, Security- oder Continuity-Management über Abweichungen vom Soll informiert?	H34b	2.1 Sind alle zentralen IT-Komponenten im Monitoring enthalten? 2.2 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?	H34c	3.1 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? 3.2 Erfolgt im Falle einer Störung eine automatische Information des Incident-, Security- oder Continuity-Managements zur Behebung der Störung? Sind die 3.3 Vorgaben zum Monitoring vollständig dokumentiert und umgesetzt?	H1d	4.1 Sind für die georedundanten Standorte die Stufen 1 bis 3 erreicht? 4.2 Werden bei signifikanten Abweichungen der gemessenen Werte vom Soll automatisch entsprechende Meldungen verschickt? 4.3 Werden die Soll-Verfügbarkeitsanforderungen aktuell gehalten? 4.4 Wird regelmäßig geprüft, ob das Monitoring der Systeme und Dienste den aktuellen Vorgaben entspricht und werden Defizite behoben?	H1e	5. Sind alle Standorte auch in ein zentrales Monitoring eingebunden und ist das zentrale Monitoring auch bei Wartung eines Standortes und gleichzeitigem Ausfall eines weite- ren Standortes funktionsfähig?

NAME des ANBIETERS	
NAME des Cloud-Services	
Version des Cloud-Services	
Alle Daten sind korrekt aufgenommen und erfasst worden. Einer Veröffentlichung der Daten stimmen wir zu.	

Identifier	Frage	Erfüllt? Wenn zutreffend, bitte "x" auswählen	Reifegrad	Bemerkung
Domäne Management			0	
Indikator I.1 Informationssicherheitsmanagementsystem ISMS)			0	
	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)?			
	wird, wie ein anforderungsgerechter Schutz aller Informationen und IT-Ressourcen vor Bedrohungen wie Zerstörung, Enthüllung, Modifizierung oder nicht autorisierter Benutzung jederzeit sichergestellt ist?			
	2.2. Sind die dafür notwendigen technischen und personellen Ressourcen vorhanden?			
	3. Sind die erforderlichen Dokumentationen (z. B. Sicherheitskonzepte) vollständig, richten sich am BSI IT-Grundschutz oder ISO 27001 aus und umfassen mindestens Folgen- des: Sicherheitsleitlinie, Klassifizierung von Informationen und Systemen und deren Schutzbedarf, Risikobewertung, ID- und Rechtemanagement, physische Sicherheit, Datensicherheit (inkl.			
	4.1. Wird im Rahmen von regelmäßigen Sicherheitsaudits die Einhaltung der sicherheits- relevanten Maßnahmen und Prozesse entsprechend ihrer Vorgaben überprüft?			
	4.2. Werden erkannte Defizite abgestellt?			
	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?			
Indikator I.2 Risikomanagement im Zusammenhang mit der IT-Dienstleistungserbringung			0	
	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?			
	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?			
	3.1. Sind die Prozesse und Ergebnisse aus den Vorgaben unter 2 in der Organisation vollständig etabliert und umgesetzt?			
	3.2. Existieren vollständige Dokumentationen und Vorgaben?			
	4.1. Wird die Einhaltung der festgelegten Risikomanagement-Prozesse regelmäßig kontrolliert?			
	4.2. Werden die etablierten Methoden und Maßnahmen regelmäßig auf Plausibilität geprüft?			
	4.3. Werden risikorelevante Vorfälle in einer revisionssicheren Art erfasst?			
	4.4. Werden regelmäßig die Meldewege auf Praxistauglichkeit und Aktualität überprüft?			
	4.5. Werden erkannte Defizite abgestellt?			
	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?			
Indikator I.3 Notfall- und Krisenmanagement			0	
	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?			
	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?			
	3.1. 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?			
	3.2. 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?			
	4.1. 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?			
	4.2. Führen die Überprüfungen dazu, dass erkannte Lücken zwischen Soll und Ist geschlossen werden?			
	5.1. Erfolgen regelmäßig Reviews und unabhängige Audits des Notfall- und Krisenmanagements insgesamt, insbesondere hinsichtlich seiner Funktionsfähigkeit und Effektivität, unter Einbeziehung der Ergebnisse aus 4?			

	5.2. Führen die Überprüfungen zu einer Optimierung der Konzepte, Verfahren, Prozesse, Rollen, Maßnahmen, Räumlichkeiten etc. des Notfall- und Krisenmanagements?			

Indikator I.4 Verfahren zur Einhaltung rechtlicher und organisatorischer Vorgaben durch das Personal			0	
	1. Haben alle Mitarbeiter inklusive Fremdpersonal eine Vertraulichkeitsvereinbarung unterzeichnet, welche die relevanten Gesetze, Vorschriften und Regelungen berücksichtigt?			
	2.1. Liegen für Mitarbeiter, die in sicherheitsrelevanten Bereichen eingesetzt werden, unbedenkliche (erweiterte) Führungszeugnisse vor und sind in diesen Bereichen definierte Benutzer-/Zugangsbeschränkungen umgesetzt?			
	2.2. Erfolgt anlassabhängig (z. B. bei Änderung von Gesetzen, Vorschriften und Regelungen) eine Neuverpflichtung der betroffenen Mitarbeiter?			
	2.3. Sind auch hierfür die entsprechenden Prozesse dokumentiert, kommuniziert und umgesetzt?			
	2.4. Nur für behördliche Rechenzentren: Werden Sicherheitsüberprüfungen durchgeführt, die in angemessener Relation zum Schutzbedarf der Daten stehen, mit denen die Mitarbeiter in Kontakt kommen können?			
	3.1. 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?			
	3.2. Erfolgen 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)?			
	4.1. Wird die Einhaltung der Verfahren zur Personalverpflichtung regelmäßig geprüft?			
	4.2. Wird in regelmäßigen Abständen geprüft, ob alle Mitarbeiter angemessen verpflichtet sind?			
	4.3. Werden Diskrepanzen beseitigt?			
	5.1. Wird der Prozess der Personalverpflichtung regelmäßig und anlassabhängig überprüft und verbessert?			
	5.2. 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)?			
Indikator I.5 Infrastruktur, Grundlagen und Planung			0	
	1.1. Sind in der Organisation Verantwortliche benannt, die sich um die Berücksichtigung aller in der Kurzbeschreibung genannten Aspekte bei Planung und Betrieb des Gebäudes kümmern?			
	1.2. Wird eine enge Zusammenarbeit der Verantwortlichen gelebt?			
	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?			
	3.1. 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?			
	3.2. Ist dieses Konzept vollständig dokumentiert und umgesetzt?			
	4.1. Erfolgt eine regelmäßige Überprüfung, ob die Anforderungen eingehalten werden?			
	4.2. 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?			
	4.3. Werden bei Abweichungen von den Vorgaben entsprechende Verbesserungsmaßnahmen eingeleitet und deren Umsetzung nachgehalten?			
	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?			

Domäne IT-Steuerung			0	
Indikator I.6 Availability Management (Verfügbarkeitsmanagement): Messung und Steuerung der Verfügbarkeit			0	
	1. Wird die Verfügbarkeit für die zur Erbringung der Dienstleistung relevanten IT-Komponenten gemessen, mit definierten Soll-Verfügbarkeitsanforderungen verglichen und auf Abweichungen reagiert?			
	2. Werden regelmäßig Auswertungen und Analysen (Soll-Ist-Vergleiche) der gesammelten Verfügbarkeitsdaten nach einem vorgegebenen Verfahren durchgeführt und dokumentiert und wird auf Abweichungen reagiert?			
	3.1. 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].			
	3.2. Sind die Vorgaben zum Monitoring vollständig dokumentiert und kommuniziert?			
	4.1. Werden die Soll-Verfügbarkeitsanforderungen aktuell gehalten?			
	4.2. Werden die Ist-Zustände sowie Abweichungen von den Sollwerten kontinuierlich erfasst und werden automatisiert geeignete Meldungen über Abweichungen verschickt? Wird vorausschau- end auf erkannte Abweichungen so reagiert, dass zu erwartende nachteilige Abweichungen zwischen Soll und Ist verhindert oder zumindest verzögert werden?			
	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?			
Indikator I.7 Capacity Management (Kapazitätsmanagement): Messung und Steuerung der Kapazität			0	
	1. Wird die Kapazität für die zur Erbringung der Dienstleistung relevanten IT-Komponenten gemessen, mit definierten Soll-Kapazitätsanforderungen verglichen und auf Abweichungen reagiert?			
	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?			
	3.1. Sind die Soll-Kapazitätsanforderungen einheitlich und vollständig dokumentiert?			
	3.2. 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.]			
	3.3. Sind die Vorgaben zum Monitoring vollständig dokumentiert und kommuniziert?			
	3.4. Werden die Prozesse zur Messung und Steuerung der Kapazität in der Institution kommuniziert?			
	4.1. 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?			
	4.2. Wird vorausschauend auf Veränderungen der Ist-Werte so reagiert, dass zu erwartende nachteilige Abweichungen zwischen Soll und Ist verhindert oder zumindest verzögert werden?			
	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?			
Indikator I.8 IT-Service Continuity Management: IT-Notfallplanung (ITSCM-Rahmenwerk)			0	
	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?			
	2.1. Sind Rollen, Verantwortlichkeiten und Prozesse des IT-Service Continuity Managements definiert?			
	2.2. Existieren Strukturen und Vorlagen für Entwicklung, Test und Ausführung von Wiederanlauf-, Wiederherstellungs- und IT-Kontinuitätsplänen?			
	3.1. Gibt es ein zentrales Dokument, welches als Rahmenwerk sowohl die Bestandteile, Ver- fahren 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?			
	3.2. Ist dieses ITSCM-Rahmenwerk vollständig umgesetzt und in der Organisation kommuniziert?			
	4.1. 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?			
	4.2. Werden dabei die Erkenntnisse aus den Notfallübungen berücksichtigt?			
	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)?			

Indikator I.9 IT-Service Continuity Management: Datensicherungen			0	
	1. Sind für die kritischen IT-Systeme Datensicherungsmaßnahmen vorhanden und werden Wiederherstellungstests durchgeführt?			
	2.1. 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?			
	2.2. Basieren die Vorgaben auf einem einheitlichen Schema, z. B. auf einer definierten Klassifikation der Daten, die etwa aus dem Schutzbedarf abgeleitet ist?			
	3.1. Existieren vollständig dokumentierte verbindliche Vorgaben und Regeln zur Durchführung und Auslagerung von Datensicherungen (Datensicherungskonzept), inkl. Wiederherstellung?			
	3.2. Ist das Datensicherungskonzept vollständig umgesetzt und innerhalb der Organisation kommuniziert?			
	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?			
	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?			
Indikator I.10 IT-Sicherheitskonzepte: Mandantentrennung			0	
	1.1. Ist der Datenzugriff der Nutzer durch ein Berechtigungsmodell geregelt?			
	1.2. Kommen mandantenspezifische Benutzerkennungen zum Einsatz, die ausschließlich zum Zugriff auf die eigenen Daten der Mandanten verwendet werden?			
	2.1. Werden alle oder mindestens ausgewählte Zugriffe protokolliert und werden datenschutzrechtlich relevante Mängel an den Datenschutzbeauftragten gemeldet?			
	2.2. 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?			
	3.1. 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?			
	3.2. Sind alle sechs der in Frage 2 genannten Mechanismen der Mandantentrennung sowohl konzeptionell als auch technisch mit dem Ziel der Trennung existierender Mandanten umgesetzt?			
	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?			
	5.1. Wird das Konzept zur Mandantentrennung regelmäßig überprüft und aktualisiert?			
	5.2. Unterliegen die übergeordneten Prozesse zur Sicherstellung der Mandantentrennung einem kontinuierlichen Verbesserungsprozess, wobei insbesondere auch die Ergebnisse der Prüfungen gemäß 4 berücksichtigt werden?			
Indikator I.11 IT-Sicherheitskonzepte: ID- und Rechtemanagement			0	
	1.1. Haben alle Nutzer nur die Berechtigungen, die sie auch benötigen (Need-to-know-Prinzip)?			
	1.2. Gibt es Verantwortliche, die für das Berechtigungsmanagement zuständig sind?			
	2.1. Sind der Zugang zu und Zugriff auf Informationen und IT-Ressourcen gemäß den Anforderungen des Auftraggebers (z. B. Schutzbedarf der Daten) abgesichert?			
	2.2. Ist dies an entsprechender Stelle dokumentiert?			
	3.1. Liegt ein vollständig dokumentiertes, rollenbasiertes und auf die Compliance-Anforderungen abgestimmtes Berechtigungskonzept vor?			
	3.2. 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?			
	3.3. Ist das Berechtigungskonzept vollständig umgesetzt und innerhalb der Organisation kommuniziert?			
	4. Wird die Einhaltung des Berechtigungskonzepts und der daraus abgeleiteten Sicherheitsrichtlinien und Sicherheitsmaßnahmen in geeigneter Weise kontinuierlich über- wacht und werden Diskrepanzen umgehend beseitigt?			
	5.1. Werden die Ergebnisse der o. g. Prüfungen in der Weiterentwicklung des Berechtigungskonzepts berücksichtigt?			
	5.2. Wird das Berechtigungskonzept regelmäßig überprüft und aktualisiert?			

Indikator I.12 IT-Sicherheitskonzepte: Kryptografie			0	
	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?			
	2.1. Werden nur dem Stand der Technik entsprechende kryptografische Verfahren implementiert, die mit allen anderen IT-Sicherheitskonzepten konform sind?			
	2.2. Werden diese Verfahren sicher installiert und eingesetzt?			
	2.3. 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)?			
	2.4. Werden die Schlüssel ausreichend sicher aufbewahrt und existieren Datensicherungen der Schlüssel zur Wiederherstellung bei Datenverlust?			
	3.1. 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?			
	3.2. 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?			
	3.3. 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?			
	4.1. 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?			
	4.2. Werden ermittelte Diskrepanzen umgehend beseitigt?			
	5.1. Werden die Informationen aus den Überprüfungen und Auswertungen für eine kontinuierliche Optimierung des Einsatzes von kryptografischen Verfahren genutzt?			
	5.2. Werden die o. g. Vorgaben und Verfahren der Kryptografie regelmäßig überprüft, insbesondere die Aktualität und Angemessenheit der ausgewählten Kryptoverfahren (Ab- gleich mit den neuesten Technischen Richtlinien und mit entsprechenden Meldungen in der Fachpresse)?			
Indikator I.13 IT-Sicherheitskonzepte: Sichere Datenlöschung und Aussonderung			0	
	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?			
	2.1. Existiert eine einheitliche, dokumentierte Vorgehensweise (je nach Art des Speichermediums und je nach Schutzbedarf) zum sicheren Löschen von IT-Systemen und Daten- trägern (inklusive Datensicherungen/Archiven) sowie zur Aussonderung von Geräten (Hardware, Peripherie, Datenträger), die zudem sicherstellt, dass keine noch benötigten Daten verloren gehen?			
	2.2. Werden bei der Löschung und Vernichtung die aktuell geltenden Standards eingehalten?			
	2.3. Wird diese Vorgehensweise von den entsprechenden Verantwortlichen befolgt?			
	3.1. 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?			
	3.2. Sind Vereinbarungen mit Dritten abgeschlossen worden, die den internen Regelungen entsprechen, sofern Betrieb oder Wartung an diese ausgelagert wurden?			
	4.1. Wird die Einhaltung des Konzepts zur sicheren Datenlöschung und Aussonderung regelmäßig geprüft, z. B. anhand von regelmäßigen Kontrollen der Ergebnisse von Löschungsvorgängen?			
	4.2. Werden erkannte Lücken geschlossen?			
	5.1. Werden die Vorgaben, Konzepte und Prozesse zur sicheren Datenlöschung und Aussonderung anlassabhängig und regelmäßig hinsichtlich ihrer Eignung bewertet und optimiert?			
	5.2. Wird dabei insbesondere die aktuelle technische Entwicklung von Datenträgern beachtet?			

Indikator I.14 IT-Sicherheitskonzepte: Schutz gegen Schadprogramme und netzbasierte Angriffe			0	
	1. Werden Maßnahmen gegen Schadprogramme getroffen (z. B. Installation eines Virenschutzprogramms) und gibt es hierfür eine verantwortliche Person?			
	2. Sind Maßnahmen, Verpflichtungen und Meldewege (sowohl beim Auftraggeber/Kun- den, 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?			
	3.1. Sind die Sicherheitskonzepte zum Schutz gegen Schadprogramme aktuell und vollständig dokumentiert?			
	3.2. Erfüllen diese die Anforderungen bewährter Standards und werden die Vorgaben innerhalb der Organisation kommuniziert?			
	3.3. 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?			
	4.1. 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)?			
	4.2. Werden erkannte Lücken geschlossen?			
	5.1. Erfolgt eine Weiterentwicklung und Optimierung der übergeordneten Prozesse und Vorgaben zum Schutz vor Schadprogrammen und netzbasierten Angriffen aufgrund der Prüfungsergebnisse gemäß 6 bis 7?			
	5.2. Wird insbesondere das Sicherheitskonzept zum Schutz gegen Schadprogramme und netzbasierte Angriffe regelmäßig angepasst und verbessert?			

Indikator I.15 Incident Management: Sicherheitsvorfallbehandlung			0	
	1.1. Gibt es eine für die Sicherheitsvorfallbehandlung verantwortliche Person?			
	1.2. Ist ein Sicherheitsvorfall eindeutig definiert und hinreichend gegenüber anderen Ereignissen abgegrenzt?			
	1.3. Werden Sicherheitsvorfälle in den Bereichen der IT und der physischen Infrastruktur zumindest in Ansätzen erfasst, analysiert und behandelt?			
	2.1. Wird sichergestellt, dass bei einem Sicherheitsvorfall die notwendigen Maßnahmen kurzfristig ergriffen werden können?			
	2.2. Werden die im Rahmen der Vorfallbehandlung durchgeführten wesentlichen Aktionen dokumentiert?			
	2.3. Sind die Erfassung, die Behandlung sowie die Nachbereitung von Sicherheitsvorfällen innerhalb eines dokumentierten Prozesses definiert?			
	2.4. Erfolgen Schulungen zur Behandlung von Sicherheitsvorfällen?			
	3.1. Schließt der Prozess die Erkennung, zeitnahe Eskalation und Reaktion sowie die voll- ständige Dokumentation von Sicherheitsvorfällen aller Bereiche (IT und physische In- frastruktur) mit ein?			
	3.2. Ist er allen an der Sicherheitsvorfallbehandlung beteiligten Personen bekannt, vollständig dokumentiert und vollständig umgesetzt?			
	3.3. Erfolgt eine zentrale Auswertung der Sicherheitsvorfälle?			
	4.1. 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?			
	4.2. Wird die Einhaltung der Vorgaben für den Prozess regelmäßig geprüft und werden Diskrepanzen beseitigt?			
	5.1.Werden aufgedeckte Sicherheitslücken zur (bereichsübergreifenden) Optimierung der Sicherheit genutzt?			
	5.2. Werden regelmäßige und anlassabhängige Überprüfungen (unter Berücksichtigung der Ergebnisse gemäß 4) durchgeführt, um die Prozesse zur Sicherheitsvorfallbehandlung zu verbessern?			
Indikator I.16 Patch- und Releasemanagement (Software)			0	
	1. Werden alle Patches, Updates und Releases von mindestens einer verantwortlichen Person entsprechend der Sicherheitsvorgaben identifiziert, gesteuert und kontrolliert?			
	2.1. Werden Patches oder Updates mit hoher Priorität (Notfall-Changes, z. B. sicherheitsrelevante Patches, die eine kritische Sicherheitslücke schließen) vorrangig bearbeitet?			
	2.2. Ist dieses Vorgehen eindeutig definiert und wird dieses Vorgehen in jedem Einzelfall dokumentiert?			
	3.1. 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?			
	3.2. Sind die Vorgaben für solche Tests vollständig dokumentiert und kommuniziert?			
	3.3. Werden die Ergebnisse der Tests vollständig dokumentiert?			
	4.1. Wird regelmäßig überwacht, dass das Einspielen von Patches, Updates und Releases nur nach vorherigen Tests erfolgt?			
	4.2. Werden die in 3 genannten Verfahren eingehalten?			
	5. Erfolgt anhand der Ergebnisse von Reviews und Auswertungen eine Weiterentwicklung und Optimierung des Patch- und Releasemanagements?			
Indikator I.17 Trennung von Entwicklungs-, Test- und Produktionsumgebungen			0	
	1. Werden separate, vom Produktionsbetrieb – mindestens virtuell – getrennte Systeme für Tests von Patches, Updates, Releases, Konfigurationsänderungen etc. einerseits und die Entwicklung andererseits eingesetzt?			
	2.1. Sind die Testumgebungen funktional äquivalent zu den Produktionsumgebungen aufgebaut?			
	2.2. Sind die Test- und Entwicklungsumgebungen bezüglich der Datenverarbeitung und Berechtigungsvergabe strikt von den Produktionsumgebungen getrennt?			
	2.3. Existieren dokumentierte Vorgaben, wie derartige Trennungen zwischen allen Umgebungen zu gewährleisten sind?			
	3.1. Sind die Vorgaben gemäß 2 und 3 vollständig dokumentiert?			
	3.2. 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?			
	3.3. Sind alle diese Vorgaben und Regelungen in der Institution kommuniziert und umgesetzt?			
	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?			
	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)?			

Domäne Technische Umsetzung				0
Indikator I.18 Ausfallsicherheit/Redundanzkonzept				0
	1.1. 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.]			
	1.2. Werden für die Erbringung der IT-Services ausschließlich solche Hardware- und Infrastrukturkomponenten verwendet, die für den Betrieb in Rechenzentren und Serverräumen ausgelegt sind?			
	2.1. 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?			
	2.2. Stellen beide räumlichen Bereiche mindestens anforderungskonformen Schutz bereit?			
	3.1. 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?			
	3.2. Sind diese Bereiche hinsichtlich der übrigen Schutzmerkmale anforderungskonform mindestens gleichwertig?			
	3.3. Findet ein Failover zwischen den redundanten Systemen ohne für den Nutzer relevante Verzögerungen oder sonstige Auswirkungen statt?			
	4.1. Sind sowohl die IT-Services als auch die für die Erbringung der IT-Services erforderlichen Infrastrukturen, IT- und Netzwerkkomponenten redundant auf georedundante Standorte verteilt?			
	4.2. 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).]			
	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?			

Indikator I.19 Netzwerk-Segmentierung			0	
	1.1. Ist das Netzwerk in verschiedene Segmente unterteilt, die dem Schutzbedarf der Komponenten des Segments entsprechen (z. B. Office-Netz, DMZ)?			
	1.2. Werden Daten, welche über Wege transportiert werden, die nicht im Einflussbereich des RZ-Betreibers liegen, geeignet verschlüsselt?			
	2. Sind Netzsegmente mit Verbindungen in öffentliche Netze durch Sicherheitskompo- nenten (dem Schutzbedarf genügend, mindestens durch Paketfilter) von rein intern genutzten Segmenten getrennt?			
	3.1. 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?			
	3.2. Werden die Protokollierungsdaten regelmäßig und zusätzlich anlassbezogen ausgewertet?			
	4. Sind auch die Netze an den georedundanten Standorten entsprechend Fragen 4 und 5 segmentiert und ist die Kommunikation zwischen diesen Standort-Segmenten geeignet verschlüsselt?			
	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)?			
Indikator I.20 Sicherheit der aktiven Netzwerkkomponenten			0	
	1.1. Ist ein Härtungskonzept für Netzwerkkomponenten vorhanden und umgesetzt?			
	1.2. 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.)?			
	2.1. Wird das Management der Netzwerkkomponenten in einem dedizierten Management- Netz durchgeführt?			
	2.2. Findet eine ständige Überwachung der sicherheitsrelevanten Meldungen der Komponenten (Monitoring) mit geeigneter Reaktion statt?			
	3.1. Geschieht das Management „Out of Band", d. h. über ein eigenes, physisch getrenntes Netzwerk?			
	3.2. Erfolgt eine regelmäßige Überprüfung der Einhaltung der Sicherheitsvorgaben sowie der Umsetzung der Sicherheitsmaßnahmen?			
	3.3. Erfolgt eine zeitnahe Beseitigung der gefundenen Schwachstellen?			
	4. Sind alle Sicherheitsmaßnahmen an allen Standorten umgesetzt und werden Ausfälle und Fehlermeldungen zentral zusammengeführt und ausgewertet (Soll-Ist-Abgleich)?			
	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?			
Indikator I.21 Ausgestaltung der WAN-Anbindung zwischen den IT-Standorten			0	
	1. Sind vorhandene WAN-Anbindungen durch Verschlüsselung abgesichert (mindestens Software-Verschlüsselung) und entsprechen die SLA den Anforderungen?			
	2. Werden vorhandene WAN-Anbindungen durch Monitoring auf Ausfall oder Störung überwacht und wird im Bedarfsfall angemessen reagiert?			
	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?			
	4. Verfügen die redundanten Verbindungen über eine gleichwertige Kapazität (z. B. 2 x 1 GBit/s)?			
	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)?			
Indikator I.22 Sicherheit der Internet-Anbindung			0	
	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?			
	2.1. Ist die Sicherheitsgateway-Architektur mehrstufig und werden die übertragenen Inhalte auf Schadsoftware kontrolliert?			
	2.2. Kontrolliert das Sicherheitsgateway auf Applikationsebene (soweit möglich, z. B. Mail, HTTP, FTP u. a.) die übertragenen Inhalte auch auf Protokollkonformität?			
	3. Sind die Komponenten des Sicherheitsgateways vollständig redundant ausgelegt (z. B. Paketfilter, Application Level Gateway, Intrusion Detection System)?			
	4. Werden an den Standorten mit eigener Internet-Anbindung gleichwertige Sicherheitsmaßnahmen (für die Internet-Anbindung) auf dem gleichen Sicherheitsniveau georedundant umgesetzt?			
	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)?			

Indikator I.23 Server-Sicherheit			0	
	1.1. Sind für alle Server Härtungskonzepte vorhanden (z. B. Sicherheitsmaßnahmen nach IT-Grundschutz „Standardniveau“) und umgesetzt?			
	1.2. Werden aktuelle Sicherheitsupdates zeitnah installiert und ist ein stets aktueller Schutz gegen Schadprogramme aktiv?			
	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?			
	3. Ist die Härtung der Systeme vollständig dokumentiert und gibt es Prozesse, die einen aktuellen Stand der Härtung sicherstellen?			
	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?			
	5.1. Werden die Härtungskonzepte regelmäßig überprüft?			
	5.2. Fließen auch die Ergebnisse der Reviews und Pentests in den weiteren Härtungsprozess mit ein, so dass die Härtungsverfahren und -konzepte systematisch verbessert werden?			
Indikator I.24 Datensicherheit der Speicher			0	
	1. Sind die Speichersysteme gemäß IT-Grundschutz eingerichtet (z. B. eine verschlüsselte Datenablage gemäß Schutzbedarf)?			
	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?			
	3.1. Werden die Systemmeldungen der Speichersysteme automatisiert auf Verletzungen der Datensicherheit überprüft?			
	3.2. Sind für Zonen mit besonderem Schutzbedarf dedizierte Speichernetze eingerichtet?			
	4.1. Erfolgt zwischen (geo-)redundanten Standorten eine automatische Datensynchronisation und werden dabei Sicherheitsmaßnahmen gegen mögliche Verluste der Vertraulichkeit und der Integrität getroffen?			
	4.2. Ist das Datensicherheitskonzept an allen Standorten gleichermaßen umgesetzt?			
	5. Wird die korrekte Umsetzung des Datensicherheitskonzepts für die Speichersysteme regelmäßig durch Reviews und technische Tests überprüft und werden erkannte Schwachstellen eliminiert?			
Indikator I.25 Datenreplikation und -sicherung			0	
	1.1. Sind die Daten, die über Replikationsmechanismen und/oder Backup geschützt werden müssen, identifiziert?			
	1.2. Sind diese Maßnahmen umgesetzt? Wurde anhand von Funktionstests nachgewiesen, ob bei einem Ausfall des (Haupt-)Datenträgers auf den redundanten Datenträger umgeschaltet werden kann?			
	1.3. Wurde das Wiedereinspielen der Daten aus dem Backup (Restore) getestet?			
	2.1. Ist im Rahmen der mit dem Kunden getroffenen Vereinbarungen (z. B. SLA) eine Wiederherstellung von Daten auf Wunsch der Informationseigner möglich?			
	2.2. 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?			
	3. Werden Datensicherungen an externe Orte, die ein gleichwertiges Sicherheitsniveau haben, ausgelagert?			
	4.1. Werden die Daten gemäß Fragen 1-3 zwischen mindestens zwei georedundanten Stand- orten repliziert?			
	4.2. Und werden diese Daten an beiden Standorten gesichert?			
	4.3. Ist das gesamte Speichernetz georedundant ausgelegt?			
	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)?			
Indikator I.26 Energieversorgung: Unterbrechungsfreie Stromversorgung			0	
	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.]			
	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.]			
	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.]			
	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.]			
	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?			

Indikator I.27 Energieversorgung: Einsatz einer Netzersatzanlage			0	
	1. Ist eine ortsfeste Netzersatzanlage (oNEA) vorhanden oder kann eine mobile Netzersatz- anlage (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?			
	2. Ist eine USV vorhanden, deren Überbrückungszeit (Autonomiezeit) bis zur Betriebsbe- reitschaft der NEA gemäß 1 ausreicht?			
	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?			
	4. Ist an jedem von mindestens zwei georedundanten Standorten mindestens eine oNEA gemäß 3 vorhanden, deren Betriebsmittelvorrat für mindestens 72 h ausreicht?			
	5.1. 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?			
	5.2. Reicht der Betriebsmittelvorrat an jedem der Standorte für mindestens 120 h aus?			
	5.3. Wurden die Betriebsgrenzwerte der eingesetzten NEAs auf Basis der technischen und betrieblichen Anforderungen des RZ individuell vorgegeben, womit die NEAs der Aus- führungsklasse G4 nach ISO 8528-5:2022-06 entsprechen?			
	5.4. Gibt es einen definierten Prozess, der sicherstellt, dass die Betriebsgrenzwerte der NEAs dauerhaft den technischen und betrieblichen Anforderungen genügen?			
Indikator I.28 Technischer Brandschutz des Rechenzentrums			0	
	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?			
	2.1. Wird das gesamte Rechenzentrum (IT-Betriebsbereich und Supportbereich) sowie dessen Umfeld durch eine BMA überwacht?			
	2.2. Wird die Meldung der BMA auf eine angemessen reaktionsfähige hilfeleistende Stelle (Feuerwehr, Haussicherheitsdienst etc.) weitergeleitet?			
	2.3. Besteht mindestens die Möglichkeit, die Stromversorgung im Brandfall gezielt per Hand abzuschalten?			
	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.]			
	4.1. 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?			
	4.2. 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.]			
	5. Werden zusätzlich auch die unmittelbaren Nachbarbereiche (vertikal und horizontal) des RZ mit einer Brandfrühesterkennungsanlage überwacht und werden diese Nachbar- bereiche durch eine reaktive Löschanlage (oder eine mindestens gleichwertige andere technische Einrichtung) geschützt und wird in den Räumen der IT-Betriebsflächen de RZ der Sauerstoff-Anteil der Luft auf ≤17 Vol.-% gehalten?			
Indikator I.29 Gebäudesicherheit: Schutz gegen Einbruch und Sabotage			0	
	1. Sind bauliche Maßnahmen für den Einbruchschutz umgesetzt, bei denen alle raumbil- denden Teile (Wände, Decken, Böden, Türen, Fenster etc.) der Widerstandsklasse RC 3 nach DIN EN 1627:2021 genügen?			
	2.1. Werden mindestens alle für den ordnungsgemäßen Betrieb des RZ erforderlichen Bereiche, also auch die Supportbereiche, durch Kontrollgänge bestreift?			
	2.2. 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?			
	3.1. Ist eine Einbruchmeldeanlage (EMA) installiert?			
	3.2. 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.]			
	4.1. 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?			
	4.2. Ist es möglich, den Meldeort einer EMA oder anderer Meldeeinrichtungen mittels zu- schaltbarer Videotechnik zum Zweck der Einsatzoptimierung einzusehen? [Hinweis: Durchsetzungsfähige Reaktion bedeutet hier, dass hinreichend ausgerüstetes und ausgebildetes Sicherheitspersonal eingreift.]			
	5.1. Ist eine auf die automatische Erkennung unzulässiger Ereignisse ausgelegte Videoüber- wachung der RZ-Hülle sowie der Supportbereiche mit sofortiger Meldung (entsprechend Fragen zu 4) vorhanden?			
	5.2 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)?			

Indikator I.30 Gebäudesicherheit: Technische/bauliche Maßnahmen zum Zutrittsschutz			0	
	1.1. 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.]			
	1.2. 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?			
	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?			
	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!]			
	4. Erfolgt der Zutritt über eine Vereinzelungsanlage – mindestens für das Gesamt-RZ, in Abgrenzung zu Bereichen, die nicht zum RZ gehören?			
	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")?			
Indikator I.31 Sicherheit der Verzeichnisdienste			0	
	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?			
	2. Werden den Kennungen Rollen zugewiesen, über die die Rechte auf den IT-Systemen und Anwendungen geregelt sind?			
	3.1. Ist die Anzahl der fehlgeschlagenen Anmeldeversuche einer einzelnen Kennung be- grenzt?			
	3.2. 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?			
	3.3. Ist die Dauer der Anmeldungen über den Verzeichnisdienst ausreichend limitiert?			
	4.1. Werden die hinterlegten Kennungen und die ihnen zugewiesenen Rollen regelmäßig mit den entsprechenden Personalverwaltungen abgeglichen und auf unnötige Rollenzuweisungen kontrolliert?			
	4.2. Werden erkannte Defizite abgestellt?			
	5. Werden die Kontrollen des Verzeichnisdienstes (beispielsweise von fehlgeschlagenen Anmeldungsversuchen) durch Personen außerhalb der regulären Verwaltung des Verzeichnisdienstes durchgeführt?			
Indikator I.32 Monitoring der technischen Infrastruktur			0	
	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?			
	2.1. Ist eine automatisch arbeitende Störungsmeldung/-übertragung für die wesentlichen Infrastrukturkomponenten (z. B. Strom, Klima, Wasser) implementiert?			
	2.2. Werden mindestens technisch sortierte Gruppenmeldungen zu einer 24/7-besetzten Interventionsstelle übertragen, die auf Basis vorgegebener Kriterien angemessen auf die Meldungen reagiert?			
	3. Erfolgen die Meldungen für jeden Sensor individuell (also keine Gruppenmeldungen) und erfolgen die Meldungen in klar verständlichem Text mit ersten Handlungsanwei- sungen?			
	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.]			
	5.1. Gibt es zusätzlich zum lokalen Monitoring an den georedundanten Standorten auch ein zentrales Monitoring, an dem die Meldungen aller Standorte auflaufen?			
	5.2. Ist die Übertragung der Störungsmeldungen durch redundante, verschlüsselte Leitungen abgesichert?			

Indikator I.33 Monitoring auf IT-Sicherheitsvorfälle / Logging			0	
	1.1. 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?			
	1.2. Ist dieser Zeitraum ausreichend, um Vorfälle angemessen aufzuklären?			
	2.1. Melden die IT-Systeme sicherheitsrelevante Vorgänge an zentrale Systeme zur Speicherung?			
	2.2. Sind diese Systeme in die Datensicherung eingebunden?			
	2.3. 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?			
	3.1. 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)?			
	3.2. Kommt ein IDS zum Einsatz? Sind die Vorgaben zum Monitoring vollständig umgesetzt?			
	4.1. Werden die Systeme automatisch auf andere, d. h. außergewöhnliche Sicherheitsvorfälle überwacht (z. B. mittels SIEM)?			
	4.2. Wird regelmäßig geprüft, ob die Log-Daten den Vorgaben entsprechend im erforderlichen Umfang erhoben und ausgewertet werden?			
	5.1. 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?			
	5.2. Werden die Vorgaben/Anforderungen an das Monitoring regelmäßig überprüft?			
	5.3. Entsprechen sie dem jeweils aktuellen Stand?			
Indikator I.34 Monitoring der IT-Komponenten und -Dienste auf Verfügbarkeit			0	
	1. Existiert ein Monitoring zur Messung der Verfügbarkeit der kritischen IT-Komponen- ten und wird das Incident-, Security- oder Continuity-Management über Abweichungen vom Soll informiert?			
	2.1 Sind alle zentralen IT-Komponenten im Monitoring enthalten?			
	2.2 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?			
	3.1 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?			
	3.2 Erfolgt im Falle einer Störung eine automatische Information des Incident-, Security- oder Continuity-Managements zur Behebung der Störung? Sind die			
	3.3 Vorgaben zum Monitoring vollständig dokumentiert und umgesetzt?			
	4.1 Sind für die georedundanten Standorte die Stufen 1 bis 3 erreicht?			
	4.2 Werden bei signifikanten Abweichungen der gemessenen Werte vom Soll automatisch entsprechende Meldungen verschickt?			
	4.3 Werden die Soll-Verfügbarkeitsanforderungen aktuell gehalten?			
	4.4 Wird regelmäßig geprüft, ob das Monitoring der Systeme und Dienste den aktuellen Vorgaben entspricht und werden Defizite behoben?			
	5. Sind alle Standorte auch in ein zentrales Monitoring eingebunden und ist das zentrale Monitoring auch bei Wartung eines Standortes und gleichzeitigem Ausfall eines weite- ren Standortes funktionsfähig?			