EIN PROJEKT
DES IT-PLANUNGSRATS

DEUTSCHE VERWALTUNGSCLOUD

Eigenerklärung zum DVC Reifegradmodell Version 0.9

NAME des ANBIETERS	Dataport
NAME des Cloud-Services	DIPAS
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 Detailierte Ansicht finden Sie auf den nachfolgenden Seiten.

Was ist das Unterschied zwischen Stufenmodell, HV Benchmark Kompakt und der erweiterten Dimension

Stufenmodell: Das Stufenmodel ist verpflichtend auszufüllen, es beinhaltet unter anderem die Minimalkritierien (Stufe1) welche zwingend erfüllt werden müssen

Erweiterte Dimensionen für das DVC Stufenmodell
Dieser beinhalatet einige Teile aus dem HV-Benchmark und muss nur ausgefüllt werden wenn der HV Benchmark nicht komplett ausgefüllt wird

1) Selbsteinschätzung des Anbieters zum Cloud-Service

Stufenmodell

Name	Stufe
Skalierbarkeit	0
AutoScaling	0
Barrierefreiheit	4
Neuer Programmstand	1
Bereitstellung IaaS	2
Mandantentrennung	1
Verbrauchsmonitoring	n/a
Verbrauchs-Reporting	n/a
Bestellprozess	1
Servicezeiten	2
Störung	1
Benutzerdokumentation	5
Technische Dokumentation	4
Verfügbarkeit	0
Inhalts-Verschlüsselung	n/a
Transport-Verschlüsselung	1
Backups	1
Authentisierung	1
Autorisierung	4
SBOM	2
Datenschutz	1
Leistungsort	5
Export von Kundendaten	5
Export von Konfiguration	4
Open Source	3

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

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**	Keine Skalierung nach NIST aktuell	**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	**4**	Barrierefreiheitsprüfung nach BITV 2.0 im März 2024 erfolgreich durchlaufen - wenige Punkte offen - Prüfbericht auf Anfrage verfügbar	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	**1**		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	**2**		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	**1**		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~~	**n/a**	Keine flexiblen Verbrauchskomponenten	~~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~~	**n/a**	Keine flexiblen Verbrauchskomponenten	~~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	**1**		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	**2**		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	**1**		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	**5**	https://wiki.dipas.org/index.php/Hauptseite	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	**4**	https://wiki.dipas.org/index.php/Hauptseite	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**	95% Verfügbarkeit kann vertraglich garantiert werden - Realbetrieb > 99%	**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~~	**n/a**	Für den Service nicht notwendig	~~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	**1**		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	**1**		Noch keine Stufe erreicht	**I3a**	**Im Service erfolgt ein regelmäßiges Backup der Kundendaten (inkl. 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	**1**		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	**4**		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	**2**		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	**1**		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	**5**		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	**5**		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	**4**		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	**3**		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 beinhalatet einige Teile aus dem HV-Benchmark und muss nur ausgefüllt werden wenn der HV Benchmark nicht komplett ausgefüllt wird

	Antwort	Kommentarfeld	Keine Stufe		Stufe 1: Minimalkriterien		Stufe 2		Stufe 3		Stufe 4		Stufe 5: Optimiert
Indikator I.1 Informationssicherheitsmanagementsystem (ISMS)			**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			**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			**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			**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			**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			**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			**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 Stand- orten 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			**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			**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			**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			**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?