

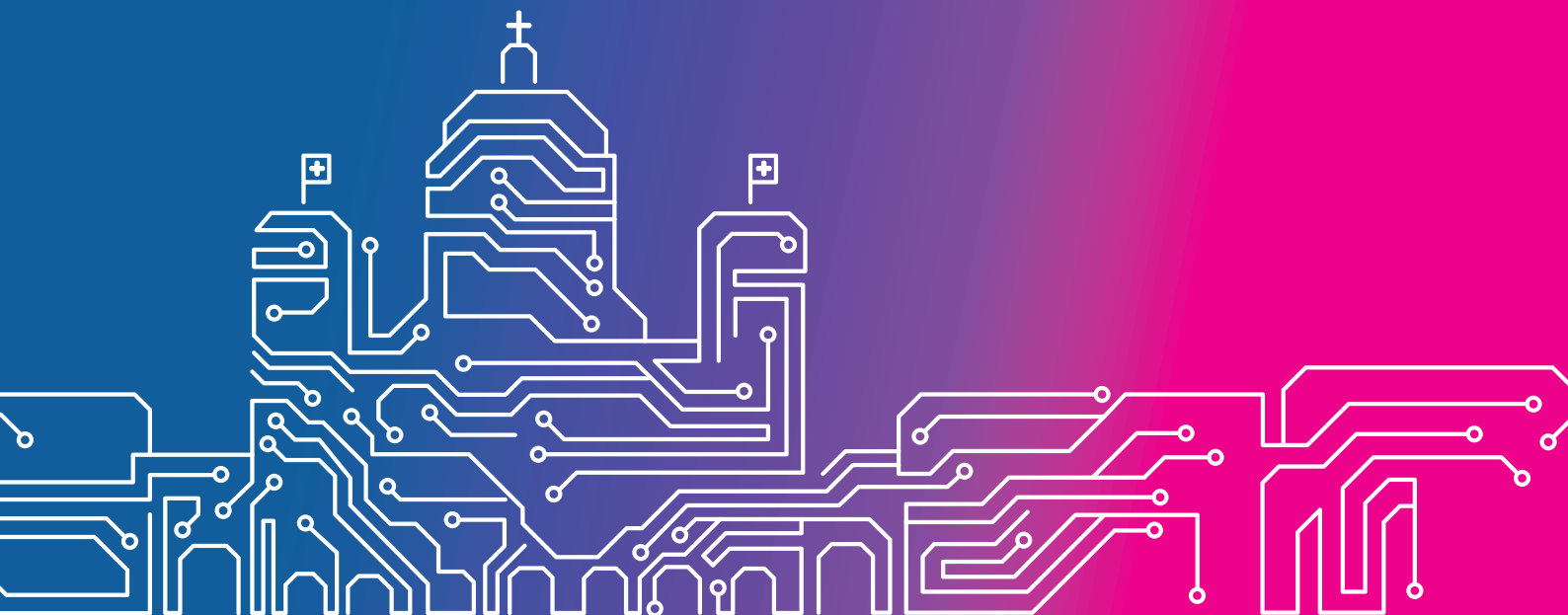


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

Strategie

Rechenzentren der zivilen Bundesverwaltung



Strategie Rechenzentren der zivilen Bundesverwaltung

1. AUSGANGSLAGE

Rechenzentren (RZ) bilden die Grundlage für die Produktion von IKT-Leistungen. Mit dem Ziel, eine Vielzahl dezentraler Serverräume abzulösen und Effizienzsteigerungen zu erreichen, hat der Bundesrat 2014 den RZ-Verbund sowie den Bau des RZ CAMPUS beschlossen. Das neue RZ wurde gebaut und derzeit wird der Bezug vorangetrieben.

Gleichzeitig zeichnen sich wegen Cloud Technologien und anderen Veränderungen in der IKT neue Nutzungsmuster für Rechenzentren des Bundes ab: Während der Bund in der Vergangenheit die IKT-Produktion bundesintern selbst erbrachte, und die RZ deshalb eng mit der eigenen IKT-Produktion verflochten waren, zeigt sich heute ein komplexeres Bild:

- Mit der **Digitalisierung und der digitalen Transformation** nimmt die Nutzung digitaler Systeme zu: Neben zusätzlicher Speicherkapazität führt insbesondere der Bedarf an zusätzlicher Rechenleistung zu einem insgesamt moderaten Mehrbedarf an RZ-Platz.
- Aus der beschleunigten technologischen Entwicklung resultiert auf Stufe RZ ein **Bedarf an strukturierten, standardisierten und schnell verfügbaren RZ-Produkten**. Diese ermöglichen eine schnelle und qualitativ hochstehende Umsetzung von IKT-Innovationen.
- Unter anderem aufgrund der **Public Cloud Technologie** wird die externe Produktion von IT-Leistungen ermöglicht. Dadurch reduziert sich der Bedarf an bundeseigener IKT-Produktion und an RZ-Platz.
- Aus der Digitalisierung entsteht zudem eine zunehmende Abhängigkeit von digitalen Systemen. Daraus resultiert die Forderung nach **Digitaler Souveränität für die Schweizer Bundesverwaltung**: Einzelne IKT-Leistungen sollen unabhängig von Public Cloud, externen Lieferanten oder externen Netzwerken produziert werden können. Auch unter erschwerten Bedingungen müssen Teile der IKT-Produktion mit hoher Sicherheit und Verfügbarkeit aufrechterhalten werden.

Als Grundlage für die eigene IKT-Produktion sind RZ ein zentraler Teil der Digitalisierung. Sie bilden das Gegenstück zur Nutzung der Public Cloud. Die RZ haben deshalb strategische Bedeutung.

2. ZIELE DER RZ-STRATEGIE

Die Strategie Rechenzentren der zivilen Bundesverwaltung, kurz "RZ-Strategie", hat den Zweck, die zivilen Rechenzentren des Bundes am zukünftigen Bedarf der IKT-Leistungserbringer (IKT-LE) des Bundes auszurichten.

Die RZ-Strategie strebt dazu gering gehaltene Veränderungen an, welche insgesamt zu einer **höheren Effektivität** und höheren **Agilität für die Digitalisierung** führen, **IKT-Innovationen und neue Technologien** ermöglichen und fördern, sowie die langfristig notwendige Informationssicherheit erbringen. Die Massnahmen zur Informationssicherheit werden stufengerecht und an den Bedarf angepasst umgesetzt.

Zugunsten der **Digitalen Souveränität** wird ein robuster und auch in Notlagen verlässlicher Betrieb angestrebt. Weiter enthält die Strategie konkrete Anforderungen zur Digitalen Souveränität.

Die RZ sind Bestandteile der Infrastruktur, welche auf die Anforderungen Digitaler Souveränität ausgerichtet werden. Zusammen mit anderen Massnahmen können damit die auf den RZ aufbauenden Systeme, Anwendungen und Dienstleistungen mit erhöhter digitaler Souveränität bereitgestellt werden.

Die unterschiedlichen BCM-Anforderungen von Fachanwendungen werden durch den Verbund der Rechenzentren unterstützt. Während das BCM selbst Bestandteil der technischen Umsetzung der jeweiligen Fachanwendungen ist, nennt die RZ-Strategie für typische IT-Systemarchitekturen mögliche **BCM-Ansätze**, und bildet diese auf RZ-Standorte ab.

Die folgende Tabelle umreisst konkrete Ziele sowie zugehörige Umsetzungsansätze:

Kundenorientierung	<ul style="list-style-type: none"> - Betrieb der RZ zugunsten und nach Bedarf der IKT-LE - Unterstützung von aktuellem und zukünftigem Bedarf - Neutraler Betrieb mit gleicher Nutzung für alle IKT-LE
Digitale Souveränität	<ul style="list-style-type: none"> - Wahrnehmung der strategischen Bedeutung der RZ: Technisch autarker Betrieb bei RZ der Stufe IV
Business Continuity Management	<ul style="list-style-type: none"> - RZ-Verbund und Standorte unterstützen BCM-Anforderungen - Unterstützung für niedrige Latenzzeiten zwischen RZ - Geschützte Archivstandorte zur langfristigen Datensicherung
Agilität für die Digitalisierung	<ul style="list-style-type: none"> - Vereinfachung der Nutzung: Minimale, bekannte Verfahren - Einfache Teilprodukte frei von Extras - Angemessener Informationsschutz
Qualität	<ul style="list-style-type: none"> - Qualität durch Audits gesichert u.a. auf Basis internationaler Standards
Informationssicherheit	<ul style="list-style-type: none"> - Unterscheidung von zwei RZ-Stufen: Stufe III und Stufe IV - Schutzmassnahmen pro Stufe umgesetzt - Laufende Prüfung der Umsetzung
Innovationen & neue Technologien	<ul style="list-style-type: none"> - RZ-Produkte sind weitgehend generisch - RZ-Produkte sind nicht mit IKT-Produkten gekoppelt - Unterstützung aktueller Vorhaben: BIT SGC - Unterstützung der Secure Private Cloud Bund des EJPD - Unterstützung von Trends: KI, Edge Computing, HPC
Unterstützung etablierter Betrieb	<p>Anerkennung bestehender Bedarfsprofile:</p> <ul style="list-style-type: none"> - RZ-Stufe III mit geringen Änderungen für bisherige Nutzer - RZ-Stufe IV mit geringen Änderungen für bisherige Nutzer
Ökonomische Optimierung	<ul style="list-style-type: none"> - RZ der Stufe III sind vergleichbar mit Industrieprodukten - Einfaches Outsourcing der RZ-Stufe III in kommerzielle RZ - Migration von Serverräumen in die Verbund-RZ - Anforderungen höher als Stufe IV als Spezialfälle ermöglicht
Bedarfsgerechte Dimensionierung	<ul style="list-style-type: none"> - Modulare und flexible Ausgestaltung der RZ-Infrastruktur - Etappierte Umsetzung mit definierten Prüfpunkten - Regelmässige Überprüfung und Anpassung der Bedarfsprognosen
Ökologische Optimierung	<ul style="list-style-type: none"> - RZ entsprechen dem Stand der Technik - Renovation RZ PRIMUS
Langfristige Entwicklung	<ul style="list-style-type: none"> - RZ-Strategie zeigt Weiterentwicklung der RZ auf - Planung Ersatz PRIMUS

3. ZWECK DER RECHENZENTREN UND NUTZER

Die Rechenzentren des Bundes sind Grundlage für die eigene IKT-Produktion. Sie unterstützen dafür insbesondere Anforderungen, welche sich aus den Aufgaben der Bundesverwaltung ergeben und nicht über kommerzielle Angebote abgedeckt werden können.

Primäre Nutzer der Rechenzentren des Bundes sind die IKT-LE des Bundes mit deren IKT-Produktion zugunsten des Bundes. Die RZ des Bundes stehen zudem für Kantone, für Betreiber Kritischer Infrastrukturen sowie für externe IKT-LE für die Departements-Informatik zur Verfügung, unter den Beschränkungen in Anhang 3.

4. DIENSTLEISTUNGSUMFANG

Rechenzentren stellen den Betreibern von IKT-Systemen im wesentlichen Platz, Strom, Kühlung, Zutritt sowie Verbindungen innerhalb des RZ zur Verfügung. Zugehörige RZ-Dienstleistungen umfassen die Logistik, die physische Installation von Geräten, das Schalten von Verbindungen oder Hilfeleistungen bei Fehlersuche oder Unterhalt. Produkte und Dienstleistungen sind in Anhang 1 aufgeführt.

Ausser für den eigenen Bedarf beinhalten die Leistungen der RZ keinen Betrieb von IT- oder Cloud-Plattformen, keine Storage und kein Netzwerkbetrieb. Solche Leistungen werden durch die IKT-LE erbracht – sie bauen dafür auf den Leistungen der RZ auf.

5. SPEZIFISCHE ANFORDERUNGEN DES BUNDES

Der Bund betreibt eine Vielzahl von Informatik-Anwendungen und -Systemen. Während für viele Systeme kommerzielle Anforderungen gelten, führen einzelne Aufgaben des Staates zu erhöhten oder stark erhöhten Anforderungen an die IKT bezüglich Verfügbarkeit oder Informationssicherheit. Auf Stufe der RZ führt dies gegenüber kommerziellen Angeboten zu erhöhten Anforderungen bezüglich physischen Schutzes, Einschränkung des Zutritts oder zusätzlicher Überwachung von Personal, Systemen und Gebäuden.

Zur Wahrung der Wirtschaftlichkeit werden die unterschiedlichen Anforderungen mittels zwei Bedarfsprofilen gewährleistet:

- **RZ Stufe III** entspricht gängigen kommerziellen Rechenzentren, und führt zu einem mit kommerziellen RZ vergleichbaren Informationsschutz. Damit ist der Zugang zu den Systemen sowohl für Personal der IKT LE als auch für externe Firmen in der Regel möglich.
Die RZ Stufe III ist mit der Cloud-Stufe III der Cloud Strategie des Bundes abgestimmt und dient als Grundlage zur Bereitstellung von Diensten auf Cloud Stufe III.
- **RZ Stufe IV** erfüllt höhere Anforderungen in Bezug auf Informationsschutz, Betriebssicherheit, Betriebszeiten und Zertifizierungen, und erlaubt nur stark eingeschränkten Zutritt.
Die RZ Stufe IV bildet die Grundlage für den Betrieb von Systemen auf Cloud Stufe IV sowie von Systemen mit Anforderung für Höchstverfügbarkeit oder für Systeme mit erhöhtem Schutzbedarf.
Die RZ Stufe IV erlaubt unter Nutzung von zusätzlichen Sicherheitsmassnahmen den Betrieb auf Sicherheitsstufe "sehr hoher Schutz" resp. "Sicherheitszone 2".

Die Bedarfsprofile der RZ Stufen III und IV können in einem RZ gleichzeitig betrieben werden unter Trennung der Systeme, Kommunikationsverbindungen und des Zutritts. In diesem Falle werden die gemeinsamen Teile der RZ, insbesondere die Regelung des Zutritts, nach den Anforderungen der RZ Stufe IV betrieben.

Das SEPOS erarbeitet die technischen Vorgaben zum Informationsschutz. Die oben genannten Eigenschaften und Annahmen unterliegen anwendbarem Recht.

Details zur Abgrenzung der beiden RZ-Stufen finden sich in Anhang 2.

6. KAPAZITÄTSPLANUNG UND SOURCING

Während Planung und Bau eines RZ bis zu 15 Jahre in Anspruch nehmen und mit hohen Investitionen verbunden sind, entwickelt sich der Bedarf der Nutzer kurzfristig, und ist zudem von gegenläufigen Tendenzen (zunehmende Nutzung der Public Cloud und kompaktere Systeme vs. zunehmende Digitalisierung) geprägt. Eine Kapazitätsplanung ist deshalb mit grossen Unsicherheiten verbunden. Die RZ-Strategie mitigiert diese Unsicherheiten wie folgt:

- Der Bedarf für RZ-Stufe III kann sowohl durch RZ des Bundes als auch durch RZ von Kantonen oder durch private Anbieter gedeckt werden. Bei externen RZ und externen Dienstleistern ist vorgängig die Durchführung eines Betriebssicherheitsverfahrens nach Art. 49ff ISG zu prüfen. Das externe Sourcing ermöglicht kurzfristiges Wachstum oder auch Reduktion der Nutzung.
- Der Bedarf für RZ-Stufe IV hingegen wird aufgrund der höheren Anforderungen ausschliesslich durch die RZ des Bundes gedeckt und hat deshalb langfristige Priorität.

Die Planung und Dimensionierung neuer RZ-Standorte wie NUBES und NAVIS wird bedarfsgerecht, flexibel und modular gestaltet. Dies ermöglicht eine schrittweise Realisierung und Anpassung an sich verändernden Bedarf über die Zeit. Festgelegte Prüfpunkte in regelmäßigen Abständen (z.B. 2030, 2035) sollen sicherstellen, dass vor weiteren Investitionsetappen der tatsächliche Bedarf neu bewertet wird. Grundlegend betreibt der Bund die RZ für die eigene Leistungserbringung. Die direkte oder indirekte Leistungserbringung gegenüber Dritten soll nicht zu einem wesentlich erhöhten Investitionsbedarf für RZ des Bundes führen.

7. RZ-DIENSTLEISTUNGEN UND KOOPERATIONSMODELL RZ-BETRIEB

Die RZ-Strategie standardisiert die im RZ-Verbund verfügbaren RZ-Produkte und RZ-Dienstleistungen, um Austauschbarkeit sicherzustellen und langfristig die Kooperation zwischen den beteiligten Organisationseinheiten zu fördern. Die aktuelle Aufgabenteilung zum Betrieb der RZ bleibt dabei weitgehend unverändert:

Bau, Betrieb und Unterhalt von Gebäudehülle, Stromversorgung, Kühlung und Zutrittskontrolle werden weiterhin durch BBL und armasuisse wahrgenommen. Sie teilen RZ-Platz zur Nutzung den bundesinternen IKT-LE zu. Der RZ-Produktkatalog und die RZ-Dienstleistungen sind im Anhang 1 beschrieben. Um die Nutzung von neuen Technologien (HPC, KI-spezifische Systeme, Quantum Computing, etc.) zu ermöglichen, ist dort die dafür notwendige technische Flexibilität beschrieben.

Das Kooperationsmodell der RZ-Strategie beinhaltet, dass in der Regel ein IKT-LE die in einem RZ vor Ort vorhandenen Kräfte für RZ-Dienstleistungen nutzt. Dies insbesondere für kleine Arbeiten, für welche durch die Anfahrt unverhältnismässig hoher Aufwand entstehen würde.

Die bundesinternen IKT-LE erbringen somit RZ-Dienstleistungen für sich selbst sowie, im Rahmen ihrer Möglichkeiten und soweit für die RZ-Stufe zulässig, für andere IKT-LE.

Zur Koordination der Aufträge über den RZ-Verbund wird ein Auftragskoordinations-Werkzeug geschaffen. Dieses wird auf einer besonders gesicherten Infrastruktur betrieben; die Klassifizierung der verarbeiteten Informationen entspricht dabei der RZ-Stufe.

Für definierte Spezialfälle werden die Arbeiten weiterhin durch die IKT-LE selbst durchgeführt. Damit wird die Erfüllung von speziellen Anforderungen ermöglicht, und generell wird die jederzeit notwendige Handlungsfähigkeit der IKT-LE für ihre eigenen Systeme sichergestellt. Spezialfälle beinhalten: Behandlung von Cybervorfällen und Ausfällen, EFK-Prüfungen, geheime Systeme, dringende Fälle (Bereitschaftsdienst), Schengen und Polizei- und Überwachungsmaßnahmen, PKI. Für umfangreiche Arbeiten (Spitzenbedarf) ist ebenfalls absehbar und zulässig, dass diese durch Personal des IKT-LE selbst vorgenommen werden.

Perspektive für die Zukunft: Mit zunehmend harmonisierten und standardisierten Abläufen und Produkten entsteht die Erwartung, dass sich eine zunehmende Zusammenarbeit zwischen den IKT-LE für den Betrieb der Systeme in den RZ ergibt.

Abbildung 1 illustriert das Betriebsmodell und die Nutzung der RZ. Die IKT-LE greifen auf RZ-Dienstleistungen anderer IKT-LE zurück.

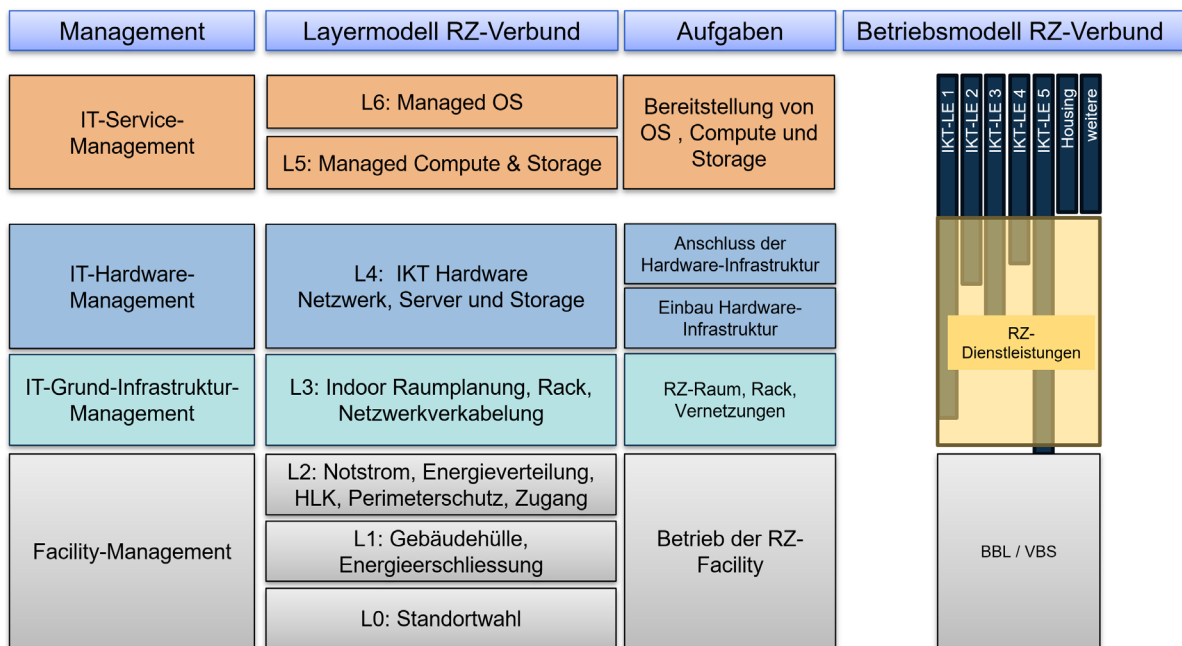


Abbildung 1: Betriebsmodell und Nutzung

8. STANDORTE UND EIGENSCHAFTEN DES RZ-VERBUNDES

Die Zuverlässigkeit von Rechenzentren ist Grundlage für den zuverlässigen Betrieb von IKT-Anwendungen. Während in den heute üblichen «Tier-3» Rechenzentren alle Systeme redundant ausgelegt sind und hohe Anforderungen erfüllen, können grössere Risiken wie Überschwemmung, Brand, grossflächiger Stromausfall, etc. mit einem Rechenzentrum allein nicht ausreichend adressiert werden. Aus diesem Grund werden mehrere Rechenzentren im Verbund betrieben: Georedundante Rechenzentren befinden sich in unterschiedlichen Regionen, womit lokale und regionale Ereignisse kompensiert werden.

Nicht alle IKT-Anwendungen sind jedoch kompatibel mit den Verzögerungen (Latenzzeiten), welche sich aus der Distanz zwischen georedundanten Rechenzentren ergeben. Um die Verfügbarkeit latenzempfindlicher Anwendungen zu verbessern, können diese Standort-redundant in zwei RZ innerhalb einer Metro-Region betrieben werden. Dabei erfolgt der Betrieb in der Regel eng gekoppelt.

IKT-Anwendungen erfordern selten sowohl Standort- als auch Georedundanz. Die Business Continuity Management (BCM) Anforderungen jeder einzelnen Anwendung bestimmen, zusammen mit der Anwendungs-Architektur und den eingesetzten Produkten, welche RZ-Standorte benötigt werden. Die RZ stellen eine technische Komponente des BCM dar. Das BCM ist in der Verantwortung der Anwendungs-Verantwortlichen.

Der RZ-Verbund unterstützt neu Redundanz für Anwendungen, welche geringe **Latenzzeiten** erfordern. Dafür wird das bestehende RZ COMES Bestandteil des RZ-Verbundes. Zudem wird im Raum Frauenfeld unter dem Namen NAVIS Platz in einem **kommerziellen RZ in geringem Umfang angemietet** auf RZ-Stufe III. Damit besteht der RZ-Verbund aus zwei Rechenzentren in je zwei Metro-Regionen – siehe Abbildung 2.

Weiter definiert die RZ-Strategie neu **Archivstandorte**¹: Dabei handelt es sich um Standorte des RZ-Verbundes, welche zur langfristigen Sicherung von Daten ausgelegt sind. Da lediglich die Beherbergung von Band-Archivsystemen (Tape Libraries) ohne wesentliche Rechenleistung vorgesehen ist, sind die Anforderungen gering.

1 Der Begriff wird im Sinne der Informatik ("Backup and Archive") verwendet. Es handelt sich nicht um Archive im Sinne des Bundesgesetzes über die Archivierung (BGA). Siehe Anhang 6: Abkürzungen und Begriffe.

Die RZ-Strategie unterscheidet Verwendungszwecke für einzelne Rechenzentren. Die Eigenschaften sind wie folgt:

- **Hauptstandorte (H):** Diese RZ sind primäre Leistungserbringer mit umfangreichem Platz- und Energieangebot. Sie entsprechen dem aktuellen Stand der Technik nach Tier-3. Um Migrationen zu vereinfachen, wird für Hauptstandorte ein einheitlicher und vollständiger Ausbaustandard für Netze und Dienste angestrebt.
- **Nebenstandorte (N):** Diese RZ dienen zur Erfüllung von spezifischem Bedarf (z.B. niedrige Latenzzeiten oder Stufe-IV Betrieb mit Sicherheitszone 2), und der verfügbare Platz ist beschränkt. Nebenstandorte entsprechen dem aktuellen Stand der Technik nach Tier-3. Der Ausbau erfolgt nach Bedarf.
- **Archivstandorte (A)** sind gehärtet und dienen dem Betrieb von Archivsystemen mit geringem Energiebedarf. Der Zutritt ist beschränkt, und die Standorte sind klassifiziert.

Tabelle 1 führt die wesentlichen RZ des RZ-Verbundes auf.

Abbildung 2 zeigt den RZ-Verbund.

Anhang 5 zeigt gängige BCM-Nutzungsmuster als Arbeitshilfe.

Aufgrund der Eigenschaften der Rechenzentren ergibt sich, dass Dienstleistungen der RZ-Stufe III mit Schwerpunkt Ostschweiz erbracht werden, während Dienstleistungen der RZ-Stufe IV im Raum Bern erbracht werden.

Tabelle 1: Wesentliche RZ des RZ-Verbundes

RZ-Name	Verwendungszweck	RZ-Stufe [†]		Bestehend	Beschreibung / Eigenschaften
		III	IV		
PRIMUS	H	Ja*	Ja	Bis 2044	
NUBES	H	Ja	Ja	Ab 2040	Ersatz von PRIMUS
CAMPUS	H	Ja	Ja	Ja	
COMES	N	Nein	Ja	Ja	
NAVIS	N	Ja	Nein	Ab sofort zulässig & bei Bedarf.	Für Bedarf für kleine Latenzzeiten.
CASTELL	A N	Nein	Ja	Ab sofort zulässig	Ein oder mehrere Standorte

* Abnehmende Nutzung

† Die Bedeutung der Unterstützung von RZ-Stufen ist im Anhang 2 detailliert.

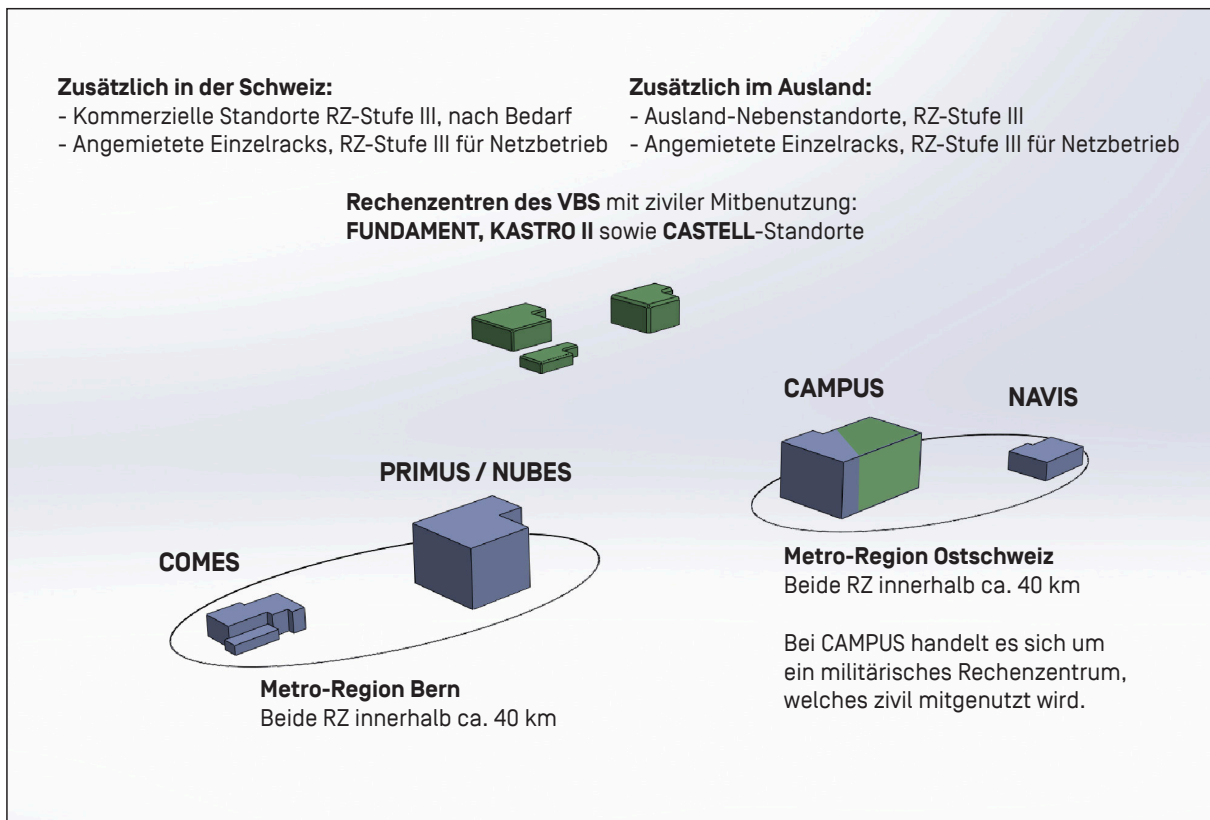


Abbildung 2: Übersicht RZ-Verbund (blau zivil, grün militärisch)

9. ABGRENZUNG DER RZ-STRATEGIE

Bestandteil der RZ-Strategie sind:

Standorte mit RZ-Platz im Ausland: Sie werden durch die jeweilige Organisation vor Ort (in der Regel das EDA) betrieben. Es handelt sich um Nebenstandorte mit bedarfsgerechtem Ausbau, welche teilweise ausländischem Recht unterstehen, und zudem Nutzungsbeschränkungen unterliegen.

Telekommunikations-Racks oder Teilracks an kommerziellen Standorten in der Schweiz oder im Ausland gelten ebenfalls als Nebenstandorte der RZ-Stufe III. Höheneinheiten sind für IKT-LE nutzbar, für Telekommunikationssysteme (Router) und einzelne Server (DNS, Mail, etc.) im Rahmen des tatsächlich verfügbaren Platzes und Strombudgets.

Nicht Bestandteil der RZ-Strategie sind:

Kommunikations- und Technikräume in Gebäuden. Sie können einzelne Systeme enthalten, welche von IKT-LE genutzt werden, z.B. für Edge-Computing. Kommunikations- und Technikräume werden nach Vorgabe des Eigners des Raumes betrieben.

Militärische Rechenzentren: Diese werden in der "Teilstrategie Rechenzentren VBS" behandelt. Das VBS nutzt die Standorte FUNDAMENT, KASTRO II sowie weitere vollgeschützte Standorte für nachfolgende Leistungen zugunsten der zivilen Bundesverwaltung:

- Betrieb des RZ CAMPUS (Bau: armasuisse; Betrieb: Kdo Cy) mit gemeinsamer Nutzung durch VBS und zivile Nutzer
- Betrieb von CASTELL-Standorten, zur Nutzung als Nebenstandorte nach Vorgabe des VBS.
- Betrieb von Archivsystemen

Eine darüber hinaus gehende Nutzung der vollgeschützten Rechenzentren des VBS durch zivile Nutzer ist nicht vorgesehen.

10. TECHNISCHE WEITERENTWICKLUNG

Stand der Technik: Die RZ und die für den Betrieb der RZ genutzten Umsysteme entsprechen dem Stand der Technik und aktuellen Standards.

Fortschritt: Die RZ des Bundes ermöglichen und erleichtern die Anwendung und Nutzung neuer IKT-Technologien. Ihr Betrieb, die verwendete Technik, und Anforderungen an die Sicherheit werden regelmässig an veränderte Anforderungen angepasst.

11. INFORMATIONSSCHUTZ

Die RZ sowie die für die Erbringung der RZ-Dienstleistung erforderlichen Systeme sind Schutzobjekte nach Art. 7 ISV. Sie erfüllen entsprechend ihrer Stufe folgende Anforderungen:

- **RZ Stufe III** erfüllt mindestens den "Grundschutz" Bund nach Art. 17 ISG.
- **RZ Stufe IV:** Neben dem Grundschutz Bund nach Art. 17 ISG erfüllen die RZ mindestens die Sicherheitsstufe "hoher Schutz" nach Art. 17 Abs. 2 ISG. Weiter erfüllen die RZ-Nutzflächen, Kommunikationsräume, Kabelführungen und die technischen Räume der RZ selbst mindestens die Anforderungen als "Sicherheitszonen 1" nach Art. 23 ISG und Art. 35 Abs. 1 Bst. a ISV.
Die RZ Stufe IV erlaubt unter Nutzung von zusätzlichen Sicherheitsmassnahmen abschnittsweise den Betrieb auf Sicherheitsstufe "sehr hoher Schutz" nach Art. 17 Abs. 3 ISG. Für diese Nutzung werden die zugehörigen RZ-Nutzflächen, Kommunikationsräume und Kabelführungen als "Sicherheitszone 2" nach Art. 23 ISG und Art. 35 Abs. 1 Bst. b ISV betrieben.

Sind externe Lieferanten beteiligt oder werden externe RZ genutzt, ist ausgehend von der tatsächlichen Nutzung vorgängig die Durchführung eines Betriebssicherheitsverfahrens nach Art. 49ff ISG zu prüfen.

12. QUALITÄT

Die Qualität der RZ-Produkte und RZ-Dienstleistungen wird mittels Audits gesichert. Nutzer der Produkte nach Anhang 1 haben Anspruch auf die Qualitätsanforderungen nach Anhang 4:

Der Informationsschutz wird regelmässig nach Art. 83 Bst. a, c, d, und e ISG beurteilt und geprüft. Weiter sind Industriestandards anwendbar.

Nutzer werden über den Stand und die Ergebnisse der einzelnen Prüfungen sowie über festgestellte Mängel informiert.

13. TECHNISCHE SOUVERÄNITÄT FÜR RZ STUFE IV

RZ-Produkte und RZ-Dienstleistungen der Stufe IV werden für den Betrieb ohne externe Abhängigkeiten (einschliesslich Internetverbindung, Lizenzcodes, etc.) von mindestens 24 Monaten ausgelegt.

Um zirkuläre Abhängigkeiten zu vermeiden, werden die für den RZ-Betrieb notwendigen IT-Systeme und Umsysteme bundesintern und bundesextern unabhängig betrieben.

14. VERBLEIBENDE RISIKEN

Geopolitische Risiken lassen sich mit den bestehenden RZ-Standorten und bereits gebauten Rechenzentren nicht beantworten. Eine Nachrüstung ziviler RZ für den Betrieb von gehärteten IKT-Systemen ist aus technischen Gründen nicht möglich. Die zivilen RZ des Bundes sind deshalb nicht nach militärischen Kriterien gehärtet. Bei BCM-Anforderungen, welche den RZ-Verbund übersteigen, ist die Nutzung von militärischen RZ in Betracht zu ziehen. Für konkrete technische Risiken wird auf die aktuellen ISDS-Konzepte der RZ verwiesen.

Unterschiedliche Risikoprofile und Eigenschaften der einzelnen RZ reduzieren für die Nutzer die Austauschbarkeit der Standorte.

15. WEITERENTWICKLUNG DER RECHENZENTREN IM RZ-VERBUND

Die Weiterentwicklung der einzelnen Rechenzentren ist unten aufgeführt.

Grundlegend gilt für alle Neubauten und alle Erweiterungsbauten (RZ NUBES, weitere Module von RZ CAMPUS), dass diese modular konzipiert werden und danach in Etappen umgesetzt werden können. Die Dimensionierung richtet sich nach einer quantitativen Bedarfsprognose, die regelmässig evaluiert und aktualisiert wird.

RZ PRIMUS: Das RZ PRIMUS wird gemäss Entscheid D-DTI und Immobilienbotschaft des BBL ab 2026 renoviert, um den Betrieb des RZ bis mindestens 2044 zu gewährleisten. Eine Verzögerung der Renovationsarbeiten von PRIMUS ist wenig praktikabel, weil z.B. Kühltssysteme aufgrund der verwendeten Kältemittel nur bis 2030 betrieben werden dürfen.

Das RZ PRIMUS wird nach 2044 ausser Betrieb genommen. Eine erneute Sanierung von PRIMUS ist danach nicht vorgesehen, weil die maximal nutzbare Kapazität erreicht ist, und weil der Standort in Zukunft nicht mehr den Anforderungen entspricht.

Ersatz des RZ PRIMUS: Standortsuche, Planung und Bau eines RZ erfordern aufgrund von komplexen Anforderungen und Auflagen 13 bis 15 Jahre Zeit. Für den Bezug eines RZ und für die Migration der IKT-Systeme sind zusätzlich mindestens vier Jahre erforderlich.

Die Renovation des RZ PRIMUS schafft Zeit bis 2044. Bis dahin wird der Ersatz des RZ PRIMUS, genannt RZ NUBES, an einem nach aktuellen Kriterien geeigneten Standort geplant, gebaut und in Betrieb genommen. Das künftige RZ NUBES erfüllt alle Anforderungen für den RZ-Betrieb auf Stufe IV, und enthält Bereiche der Sicherheitszonen 1 und 2 nach ISG Art. 23 und ISV Art. 35.

RZ CAMPUS: Dieses RZ wird zusammen mit dem VBS genutzt. Aktuell ist eines von vier möglichen RZ-Gebäuden (Modulen) gebaut. Bei den Modulen handelt es sich nicht um separate RZ, wegen der unmittelbaren Nähe, und weil der Standort CAMPUS gemeinsame Systeme nutzt.

Integration COMES: Das bestehende RZ COMES wird neu Bestandteil des RZ-Verbundes. Es dient zur IKT-Produktion auf RZ Stufe IV und verfügt über beschränkten Platz.

RZ NAVIS: Als Ergänzung zum RZ CAMPUS wird RZ-Platz im Raum Frauenfeld angemietet. Der als NAVIS bezeichnete Standort wird bei Bedarf angemietet und bedient ausschliesslich Anwendungen, welche in CAMPUS betrieben werden, niedrige Latenzzeiten erfordern und aufgrund des BCM einen weiteren Standort erfordern. Die Beschaffungsgrundlage ist noch zu erarbeiten.

RZ CASTELL: Hierbei handelt es sich um einen oder mehrere gehärtete Standorte zur langfristigen Sicherung von Daten oder zur Nutzung als Nebenstandort. Sie werden nach Vorgabe des VBS betrieben. CASTELL wird in bestehenden Anlagen realisiert.

16. KOSTEN

Neu soll mit dem **RZ NAVIS** bei gemeldetem Bedarf kommerzieller RZ-Platz im Raum Zürich-Ostschweiz angemietet werden, um neue Anforderungen für niedrige Latenzzeiten zu erfüllen. Die Mietkosten ergeben sich aus dem tatsächlichen Bedarf.

Die neuen Standorte zur Archivierung resp. Sicherung von Daten (**RZ CASTELL**) verursachen Ausbaurkosten im niedrigen einstelligen Millionenbereich.

Erhebliche Kosten (tiefer dreistelliger Millionenbetrag) ergeben sich für den **Ersatz des RZ PRIMUS**.

ANHANG 1: RZ-PRODUKTE UND RZ-DIENSTLEISTUNGEN

NORMATIV als Minimalangebot

RZ-Produkte mit wiederkehrenden Kosten:

Kategorie	Bestellung	Nutzung
RZ-Platz luftgekühlt	Eine einzelne Höheneinheit	Platz für das bestellte Produkt wird dem Nutzer zugeteilt. Durch den Nutzer innerhalb des zugeteilten Platzes installierte Verbindungen sind zulässig. Verbindungen ausserhalb des zugeteilten Platzes werden immer durch das RZ installiert. Käfige und Räume erlauben die Platzierung von eigenen Racks oder Systemen. Wasserkühlung ist, wo verfügbar oder installierbar, innerhalb von Räumen möglich.
	Zusammenhängende Höheneinheiten	
	Viertel & Halbrack	
	Einzelnes Rack	
	Aneinander anschliessende Rack(s)	
	Käfig	
	Raum	
Dachplatz	Installation von Antennen oder Systemen auf dem Dach des RZ, inkl. Netzwerk-Verbindungen oder Spezialkabel-Verbindungen.	Nach Abklärung / wo verfügbar
Energie	230/400V AC, redundant, USV-gestützt	
	48V DC, redundant, Batteriegestützt	Nach Abklärung / wo verfügbar

RZ-Produkte mit einmaligen Kosten:

Kategorie	Bestellung	Beschreibung
Zutritt	Person erfassen	Zutrittskontrolle und Auskünfte darüber.
	Person modifizieren	
	Person löschen	
	Gruppe definieren	
	Gruppe modifizieren	
	Gruppe löschen	
	Auszug Personen und Gruppen	
	Auskunft erfolgte Zugänge	

Verbindungen	SMF / MMF schalten	Schalten von Verbindungen. Je nach bestehendem Ausbau können einmalige Kosten zum Ausbau des Racks anfallen.
	RJ45 schalten	
	Coax (Dach) installieren	
	Verbindung entfernen	
Energie	48V DC	Spezialanforderung 48V DC Stromversorgung
Kühlung	Wasserkühlung	Spezialanforderung (nicht standardisiert)
Andere	Sitzungszimmer buchen (wo verfügbar)	
	Übernachtung buchen (wo verfügbar)	
	Mobile Konsole buchen	
	Andere	

RZ-Dienstleistungen („Helping Hands“) mit einmaligen Kosten:

Kategorie	Bestellung	Beschreibung
Systeme Management von Systemen im Rack oder Cage des Kunden.	Systeme Installieren	Einbau von Kundensystemen in ein Rack, nach Vorgabe des Kunden. Für total mehr als 100 Höheneinheiten ist eine „Grosse Bestellung“ zu verwenden.
	Systeme verschieben oder ersetzen	Ersetzen oder verschieben von Kundensystemen innerhalb eines Racks oder zwischen Racks im gleichen RZ, nach Vorgabe des Kunden. Für total mehr als 100 Höheneinheiten ist eine „Grosse Bestellung“ zu verwenden.
	Systeme entfernen	Entfernen von Kundensystemen, nach Vorgabe des Kunden. Für total mehr als 100 Höheneinheiten ist eine „Grosse Bestellung“ zu verwenden.
	Unterhalt von Systemen	Technische Unterstützung für installierte Systeme, z.B.: Überprüfung des Zustandes eines Systems Allgemeine technische Unterstützung Hardware Resets Wichtig: Um wegen einer Fehlfunktion ein System umgehend neu zu starten, die Dienstleistung „Neustart eines Systems“ verwenden.
	Neustart eines Systems	Eröffnen eines dringlichen Tickets wegen Serviceausfall seitens des Kunden. Wichtig: Falls das Anliegen nicht dringlich ist, die Dienstleistung „Unterhalt von Systemen“ verwenden.

Verbindungen Management von Verbindungen von, zu und zwischen Systemen.	Kabel installieren	Installation einer Cross-Connect Verbindung anfordern. Der RZ-Dienstleister kann zusätzlich Patch-Kabel zur Verfügung stellen. Zur Installation von mehr als 24 Kabeln ist eine „Grosse Bestellung“ zu verwenden.
	Kabel verschieben / umstecken	Umstecken eines bestehenden Patch-Kabels an ein anderes Gerät anfordern. Zum Umstecken von mehr als 24 Kabeln ist eine „Grosse Bestellung“ zu verwenden.
	Kabel entfernen	Entfernen eines bestehenden Cross-Connect Patch-Kabels. Zum Entfernen von mehr als 24 Kabeln ist eine „Grosse Bestellung“ zu verwenden.
Logistik Management von Paketen und dem Versand von/zu RZ-Standorten.	Sendung durch RZ empfangen lassen	Den Eingang einer Lieferung ankündigen.
	Material durch RZ versenden lassen	Die Abholung von Material ankündigen.
	Paket im RZ lokalisieren	Ein Paket oder Pakete an einem RZ-Standort lokalisieren lassen. Wichtig: Dieser Auftrag ist nur möglich für Pakete, welche bereits eine Kontrollnummer erhalten haben. Falls das Paket noch keine Kontrollnummer erhalten hat, ist der Auftrag „Sendung durch RZ empfangen lassen“ zu verwenden.
Cage Services Zusätzliche Dienstleistungen im Zusammenhang mit Cages oder zum Audit.	Cage / RZ-Abteil / RZ-Raum aufräumen lassen	Das Entfernen von Abfall oder die Reinigung eines Cage, RZ-Abteils oder RZ-Raumes veranlassen. Wichtig: Es sind keine brennbaren Materialien im Betriebsteil des RZ erlaubt. Ohne Anweisung werden brennbare Materialien entsorgt. Bitte machen Sie Angaben betreffend: Was konkret gereinigt werden soll Was entsorgt werden soll Ist eine Reinigung des Bodens oder Staubsaugen erforderlich? Wie mit brennbarem Material (z.B. Kartonverpackungen oder Papier) umgegangen werden soll. Beispiel: Brennbare Material entsorgen lassen, oder mittels Auftrag „Material durch RZ versenden lassen“ die Rücksendung des Materials veranlassen.
	Fotos erstellen lassen	Fotos von spezifischen Systemen, Verkabelung, Rack, Cage oder Raum erstellen lassen. Die Fotos werden elektronisch zugestellt.
	Physischer Audit	Material und Systeme vor Ort gegenüber einer Materialliste verifizieren, oder ein Inventar oder Angaben zu Systemen (z.B. Stromverbrauch) erstellen lassen. Wichtig: Für Audits zu Qualitätssicherungszwecken den RZ-Dienstleister kontaktieren.
	Besucher eskortieren	Die Begleitung eines Besuchers durch Sicherheitspersonal des RZ-Dienstleisters anfordern, zum Zweck des Zutritts zum Rack, Cage, RZ-Raum des Kunden, oder zum Zugang zu Installationen des Kunden auf dem Dach.

Weitere Dienste Weitere Dienstleistungen im Zusammenhang mit der RZ Nutzung.	Notfallhilfe	Notfallhilfe bei Service-Ausfall seitens des Kunden.
	Strom einschalten oder ausschalten	Das Einschalten oder Ausschalten der Stromversorgung anfordern.
	Grosse Bestellung	Helping Hand Hilfestellung für umfangreiche oder komplexe Arbeiten anfordern, z.B. Kabelinstallationen von mehr als 24 Kabeln. Das Maximum pro Grosse Bestellung beträgt 200 Kabel. Den Aufbau von Systemen mit einem Umfang von mehr als 100 Rack Höheneinheiten verlangen. Das Maximum pro Grosse Bestellung beträgt 500 Höheneinheiten (ca. 10 Racks).
	Zubehör bestellen	Bestellung von Material aus dem Zubehörkatalog des RZ.
	Regelmässiger Bandwechsel	Wechsel oder Rotation von physischen Medien (Backup-Bänder, Festplatten, SSDs etc.) anfordern.
	Entsorgung von Elektronik	Entsorgung von Elektronik veranlassen.
Diagnose / Kabel Testen Diagnose von Verbindungen zu, von oder zwischen Kundensystemen.	Loopback Test	Einen Loopback Test anfordern, zur Funktionsprüfung eines Transceivers oder Ports. Für mehr als 24 Loopback Tests ist eine „Grosse Bestellung“ notwendig.
	Verbindungstest	Die Verbindung zwischen Systemen prüfen lassen: Visuelle Prüfung, ob die Link LEDs grün leuchten; Sicherstellen, dass Glasfaserverbindungen sauber und gereinigt sind; Verifizieren, dass die Steckverbinder ganz eingesteckt sind; Messung der optischen Signalpegel; Verifizieren der Sender (TX) und Empfänger (RX) Status und Statistikinformationen, nachdem die Verbindung wieder hergestellt wurde. Für mehr als 24 Verbindungen ist eine „Grosse Bestellung“ notwendig.
	Remote Console	Einen durch den Kunden zur Verfügung gestelltes Laptop zu einem Rack des Kunden bringen, und mittels Videokonferenz zusammen mit einem Mitarbeiter des RZ-Dienstleisters spezifische Konfigurationsarbeiten ausführen lassen.
Andere Weitere Dienstleistungen für oben nicht aufgeführte Arbeiten.	Helping Hands: Andere Arbeiten	Verwenden Sie diesen Auftrag nur, wenn die spezifische Arbeit oben nicht aufgeführt ist.
	Helping Hands: Andere wiederkehrende Arbeiten	Wiederkehrend ausführen lassen von oben genannten Aufträgen.
	Helping Hands: Report erstellen	Berichte und Abrechnungen zur Nutzung und Verrechnung erstellen lassen.

ANHANG 2: DETAILS ZUR ABGRENZUNG RZ-STUFE III VS. RZ-STUFE IV

Die Hauptunterschiede zwischen RZ Stufe III und RZ Stufe IV sind nachfolgend aufgeführt. Einzelne Anforderungen können, baulich bedingt, in bestehenden Rechenzentren nachträglich nur mit Einschränkungen erfüllt werden.

Merkmal	Stufe III	Stufe IV
Kontrolle und Transparenz	Sicherheitsgeprüftes Personal Eigenes und externes Personal	Eigenes sicherheitsgeprüftes Personal - Erweiterte Prüfung. Zentrale Kontrollinstanz / Zutrittslisten / Zugriffslisten.
Betriebssoeveränität	Einzelne Layer des tech. Stacks können an Dritte ausgelagert werden/sein. Bundeseigene RZ und angemietete RZ im geschützten Bereich.	Sämtliche Layer des tech. Stacks werden selbständig verwaltet / betrieben. Bundeseigene RZ, internes Standortpersonal (PSP geprüft).
Abhängigkeit von Drittparteien	Stärkere Abhängigkeiten (siehe oben) Flexibilität der personellen Auslastung.	Weniger Abhängigkeiten (ev. Multi-Vendor Strategie, Vorrat von Komponenten usw.) int. Standortpersonal (Full Stack Ansatz)
Zutritts- und Zugriffskontrolle	Zutritt + physischer Zugriff bis und mit RZ-Raum / Cube.	Mindestens RZ-Raum / zusätzlich bis Cube und Racks.
Ressourcennutzung	Geteilt / nicht vollständig unter eigener Kontrolle.	dediziert / volle Kontrolle. physische Trennung, dedizierte Cubes / überwachte Racks.
Sicherheitsniveau	Zutritt nach Stufen	Max (sehr hoch) Zutritt nach Stufe, mehrstufige Identifikation (Biometrie), begleiteter RZ-Zutritt, zusätzliche Raumüberwachung.
Serviceumfang	Fokus auf "Standardlösungen"	Fokus auf "Individuallösungen", "Erhöhte Sicherheitsanforderungen", Leib und Leben, WK2-Schränke, gehärtete Racks.
Abhängigkeit von Dritten	Sicherheitsgeprüftes Personal - Grundprüfung.	Eigenes sicherheitsgeprüftes Personal. Zentrale Kontrollinstanz / Zutrittslisten.

Beispiel-Vorgaben, nicht abschliessend.

Abgrenzung: Physische Infrastruktur:

Aspekt	Stufe III	Stufe IV
Raumtrennung	Getrennte Räume durch Standardtrennwände	Dedizierte Räume, hochsichere Trennwände
Zutrittskontrolle	Standardisierte elektronische Zugangssysteme	Mehrstufige Zutrittskontrollen (z.B. Biometrie, Schleusen)
Brandschutz	Feuerfestigkeit, automatische Löschsysteme (z.B. Gaslöschung)	
EM-Schutz	Kein oder minimaler elektromagnetischer Schutz	Erhöhter Schutz gegen elektromagnetische Einflüsse (EM-geschützte Räume) [gilt für Neubauten]
Überwachung	Kameras und Alarmsysteme für den gesamten Bereich	Zusätzliche Raumüberwachung (z.B. Bewegungssensoren, redundante Kameras)
Energieversorgung	Erhöhte Redundanz (2N), separate Energieversorgung innerhalb des Raumes. Wo möglich zwei unabhängige Energieversorger.	
Physische Sicherheit	Verstärkte Bauweise (z.B. Schutz gegen Explosionen, Erdbeben), Umzäunung, Arealüberwachung	Verstärkte Bauweise bei Bundes-RZ (z.B. Schutz gegen Explosionen, Erdbeben), Umzäunung, Arealüberwachung. Räume mit erweiterten Anforderungen (siehe Raumtrennung)
Umgebungsbedingungen	Einfache Temperatur- und Feuchtigkeitsregelung	Präzise Steuerung mit höherer Redundanz und erweiterten Umgebungsmonitoren.

Beispiel-Vorgaben, nicht abschliessend.

ANHANG 3: NUTZUNG DER RZ DES BUNDES DURCH DRITTE

Die RZ des Bundes stehen unter den unten aufgeführten Beschränkungen zur Verfügung².

Die Grundlagen für eine weitergehende Nutzung werden durch DTI geprüft. Die Ergebnisse sind Voraussetzung für die Dimensionierung von RZ-Neubauten.

Für Kantone sowie Betreiber kritischer Infrastruktur:

RZ-Stufe III: Die Nutzung der RZ-Produkte des Bundes auf RZ-Stufe III ist nicht vorgesehen.

RZ-Stufe IV: Nutzung bis zu einem Umfang von maximal zwei Racks, sofern verfügbar. Um die Anzahl zutrittsberechtigter Personen klein zu halten, werden Installation, Betrieb und Unterhalt der Systeme ausschliesslich durch IKT-LE des Bundes als RZ-Dienstleister vorgenommen. Der Zutritt zum RZ ist für externe Nutzer nicht möglich.

Für IKT-LE der Privatwirtschaft:

Für IKT-LE der Privatwirtschaft, welche in erheblichem Umfang Leistungen der Anwendungs-Informatik zugunsten eines Departementes erbringen:

RZ-Stufe III: Die Nutzung der RZ-Produkte des Bundes auf RZ-Stufe III ist nicht vorgesehen.

RZ-Stufe IV: Nutzung im notwendigen Umfang, ausschliesslich für die Erbringung der Leistung gegenüber dem Departement. Um die Anzahl zutrittsberechtigter Personen klein zu halten, werden Installation, Betrieb und Unterhalt der Systeme ausschliesslich durch zugelassenes Personal des Departements oder durch einen IKT-LE Bundes als RZ-Dienstleister vorgenommen. Der Zutritt zum RZ ist für externe Nutzer nicht möglich.

2 Die Leistungserbringung zugunsten Dritter (Kantone, Gemeinden) unterliegt rechtlichen Rahmenbedingungen, insbesondere:

Artikel 11 Absatz 3 Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG) und Artikel 41a Absatz 2 Finanzhaushaltsgesetz (FHG): Die Erfüllung der Hauptaufgaben darf nicht beeinträchtigt werden und es dürfen keine bedeutenden zusätzlichen sachlichen und personellen Mittel erforderlich sein.

Artikel 57 Absatz 2 FHG: Kredite der Verwaltungseinheiten dürfen nur für unerlässliche Bedürfnisse verwendet werden.

ANHANG 4: QUALITÄTSSICHERUNG

Die folgenden Standards, Zertifizierungen oder Prüfberichte werden minimal erbracht. Die Qualitätssicherungsanforderungen gelten zusätzlich zu gesetzlichen oder anderen regulatorischen Anforderungen an Rechenzentren des Bundes.

Standard / Zertifizierung / Prüfbericht	Beschreibung	Anwendung auf RZ	
		Stufe III	Stufe IV
Sicherheits- verfahren Bund nach ISG	Erstellung / Erneuerung ISDS-Konzepte pro RZ	Ja	Ja
Audit nach Art. 83 Bst. a, c, d, und e ISG	Audit nach ISG: Das ISG definiert in Art. 83 die Aufgaben der Fachstelle des Bundes für Informationssicherheit, welche auf Antrag Überprüfungen durchführt. Die Anwendung bedeutet, dass die Überprüfung für die betreffenden RZ-Bereiche tatsächlich beantragt wird.	Nein	Ja
ISO 27001	Informationssicherheits-Managementsystem (ISMS) für das Rechenzentrum selbst	Nein	Ja
ISO 50001	Energiemanagementsysteme (EnMS)	Ja	Ja
ISO 22301	Business Continuity Managementsysteme (BCMS) für das BCM des Rechenzentrums selbst	Nein	Ja
ISO 27701	Privacy Information Managementsysteme (PIMS). Die Anforderung nach ISO27701 kann gegebenenfalls durch eine Weisung des SEPOS ersetzt werden.	Nein	Ja
Tier 3	Umfassende Qualifikation (Uptime Institute)	Nein	Ja

ANHANG 5: BCM UND RZ-STANDORTE (INFORMATIV)

Die Standorte und Eigenschaften von Rechenzentren haben grossen Einfluss auf das Business Continuity Management [BCM]. Die Business Continuity Management [BCM] Anforderungen jeder einzelnen Anwendung bestimmen, zusammen mit der Anwendungs-Architektur und den eingesetzten Produkten, welche RZ-Standorte benötigt werden. Die RZ stellen eine technische Komponente des BCM dar. Das BCM ist in der Verantwortung der Anwendungs-Verantwortlichen.

Nicht alle IT-Systemarchitekturen sind empfindlich auf Latenzzeiten. Deshalb sind die nachfolgend ausgewählten Kombinationen für Latenz-empfindliche, sowie separat für Latenz-unempfindliche Anwendungsarchitekturen aufgeführt.

RZ-Verbund: Nutzung der Standorte für Latenz-unempfindliche Anwendungen

Ansatz	Vorschlag Standorte	BCM-Auswirkung
Nicht georedundant	Betrieb: CAMPUS	Ausfall des RZ führt zu Ausfall der Anwendung. Bei physischem Schaden kann die Anwendung nicht wieder hergestellt werden, Daten gehen verloren.
Nicht georedundant mit Archivkopien	Betrieb: CAMPUS oder NUBES Archiv: CASTELL	Ausfall des RZ führt zu Ausfall der Anwendung. Bei physischem Schaden kann die Anwendung kurzfristig nicht wieder hergestellt werden. Die Daten bleiben zur späteren Verwendung erhalten.
Active/Active oder auch Active/Passive, georedundant, mit Archivkopien*	Betrieb: CAMPUS & PRIMUS/NUBES Archiv: CASTELL Bei Active/Passive RZ CAMPUS als Active-Standort.	Bei Ausfall eines RZ bleibt die Anwendung in Betrieb oder wird nur kurz unterbrochen. Archivkopien ermöglichen eine robuste Wiederherstellung auch nach technischen Problemen oder Cyber-Vorfällen.

* empfohlen

RZ-Verbund: Spezialfall Nutzung der Standorte für Latenz-empfindliche Anwendungen

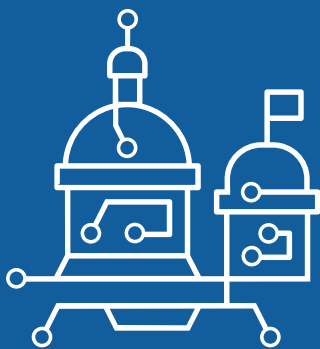
Ansatz	Vorschlag Standorte	BCM-Auswirkung
Betrieb in einem RZ	Betrieb: CAMPUS oder NUBES, inklusive ähnlicher Varianten mit Betrieb an nur einem Standort.	Ausfall des RZ führt zu Ausfall der Anwendung. Bei physischem Schaden kann die Anwendung nicht wiederhergestellt werden, Daten gehen verloren.
Betrieb in einem RZ, mit Archivkopien.	Betrieb: CAMPUS oder NUBES, inklusive ähnlicher Varianten mit Betrieb an nur einem Standort. Archiv: CASTELL	Ausfall des RZ führt zu Ausfall der Anwendung. Bei physischem Schaden kann die Anwendung kurzfristig nicht wiederhergestellt werden. Die Daten bleiben zur späteren Verwendung erhalten.
Active/Active in gleicher Metro-Region betrieben, RZ-Stufe III, mit Archivkopien.	Betrieb: CAMPUS & NAVIS Archiv: CASTELL	Bei Ausfall eines RZ bleibt die Anwendung in der Regel in Betrieb. Archivkopien ermöglichen eine Wiederherstellung innert Monaten nach einem Grossereignis, nach technischen Problemen oder nach Cyber-Vorfällen.

Active/Active in gleicher Metro-Region betrieben, RZ-Stufe IV, mit Archivkopien.	Betrieb: PRIMUS & COMES Archiv: CASTELL	
Active/Active und georedundant, RZ-Stufe III, mit Archivkopien*	Betrieb: CAMPUS & NAVIS Betrieb alternativ in PRIMUS/NUBES Archiv: CASTELL	Bei Ausfall eines RZ bleibt die Anwendung in Betrieb. Ein Zweitstandort (PRIMUS für Stufe III, CAMPUS für Stufe IV) erlaubt die Wiederaufnahme des Betriebes mit hoher Verlässlichkeit auch nach technischen Problemen oder bei einem Grossereignis. Zusätzlich sichern Archivkopien Daten langfristig oder nach Cyber-Vorfällen.
Active/Active und georedundant, RZ-Stufe IV, mit Archivkopien*	Betrieb: PRIMUS/NUBES & COMES Betrieb alternativ in CAMPUS Archiv: CASTELL	

* empfohlen

ANHANG 6: ABKÜRZUNGEN UND BEGRIFFE (INFORMATIV)

Begriff	Bedeutung
Archiv	Der Begriff "Archiv" wird im Sinne der Informatik ("Backup and Archive") verwendet, und bezeichnet eine langfristige Datensicherung mit dem primären Zweck der Fortführung des Betriebes. Aufgrund des Zweckes werden die Daten in der Regel nicht in langfristige Formate (z.B. PDF/A, TIFF, etc.) umgewandelt, obwohl eine zusätzliche Ablage in solchen Formaten unterstützend wirkt. Es handelt sich nicht um Archive im Sinne des Bundesgesetzes über die Archivierung (BGA).
BCM	Business Continuity Management oder „Betriebskontinuitätsmanagement“. BCM bezeichnet die Entwicklung von Strategien, Plänen und Handlungen, um die Fortführung von wichtigen Tätigkeiten oder Prozessen zu schützen, und so Schaden abzuwenden.
DTI	Der Bereich Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei.
HPC	High Performance Computing
IKT	Informations- und Kommunikations-Technologien, d.h. digitale Computer-, Netzwerk- und Telekommunikationssysteme und Technologien.
IKT-LE	IKT-Leistungserbringer.
ISG	Informationssicherheitsgesetz vom 18. Dezember 2020, AS 2022 232
ISV	Informationssicherheitsverordnung vom 8. November 2023, AS 2023 735
PKI	Public Key Infrastructure. In den RZ werden zum Betrieb von PKI besonders gehärtete Systeme und Module verwendet. Wesentliche Arbeiten sind auf Grund von Sicherheitsanforderungen oft nur vor Ort möglich, und werden nur durch besonders geprüfetes und geschultes Personal vorgenommen.
RZ	Rechenzentrum. Der Begriff wird im Sinne der Informatik verwendet: Der Betrieb der Computer-, Netzwerk-, und Speichersysteme ist nicht Bestandteil der RZ, sondern baut auf den Leistungen der RZ auf.
Secure Private Cloud Bund	Cloud-Plattform des EJPD: Platform as a Service, erbringt Dienstleistungen auf Cloud Stufe IV für das EJPD und für die Bundesverwaltung.
SGC	Cloud-Plattform des BIT: „Swiss Government Cloud“, erbringt Dienstleistungen auf Cloud Stufe III für das BIT und für die Bundesverwaltung.
Tier-3	Industrieübliche Bewertung von Rechenzentren nach dem amerikanischen Uptime Institute. Tier-3 bedeutet u.a. volle Redundanz, Tier-4 bedeutet u.a. volle Redundanz auch während Wartungsarbeiten. Siehe uptimeinstitute.com. Hinweis: Die "Tier"-Stufen des Uptime Institute haben keinen Zusammenhang mit den in diesem Dokument definierten RZ-Stufen III und IV der Bundesverwaltung. Siehe auch Anhang 4 (Qualitätssicherung).
Tier-4	
USV	Unterbrechungsfreie Stromversorgung.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

Gültig per 9. Juni 2025

info.dti@bk.admin.ch
+41 (0)58 463 46 64

bk.admin.ch/rz-strategie