



## **Anlage 1 (Anforderungen und Vorgaben zur Leistungserbringung)**

### **EU-Vergabe**

#### **Rahmenvereinbarung zur Beschaffung von Public- und Sovereign-Cloud Service in zwei Losen**

ID: B05-II

Auftraggeber: Deutsche Bundesbank

Auftragnehmer: Provider

Datum: 10.07.2026

Revision: 1.0

Autor: Deutsche Bundesbank

Status: Freigegeben

## DOKUMENTEN HISTORIE

| Datum | Revision | Autor | Status | Kommentar |
|-------|----------|-------|--------|-----------|
|       |          |       |        |           |
|       |          |       |        |           |
|       |          |       |        |           |
|       |          |       |        |           |
|       |          |       |        |           |

**INHALT**

|          |                                                                 |          |
|----------|-----------------------------------------------------------------|----------|
| <b>1</b> | <b>INHALT DIESES DOKUMENTS UND RAHMENBEDINGUNGEN .....</b>      | <b>1</b> |
| 1.1      | Einleitung.....                                                 | 1        |
| 1.2      | Überblick Leistungsinhalt .....                                 | 1        |
| <b>2</b> | <b>ANFORDERUNGEN UND VORGABEN .....</b>                         | <b>3</b> |
| 2.1      | Anforderungen zum Leistungsstandort .....                       | 3        |
|          | (a) Georedundante Standorte für die Cloud Leistungen .....      | 3        |
| 2.2      | Technische Anforderungen.....                                   | 3        |
|          | (a) Unterbrechungsfreie Leistungserbringung .....               | 3        |
|          | (b) Auftragnehmer-Linux Distributionen .....                    | 4        |
|          | (c) Rollenbasierte Zugriffe .....                               | 4        |
|          | (d) Rollen nach dynamischen Gruppen und Strukturen .....        | 5        |
|          | (e) RDBMS as a Service.....                                     | 5        |
|          | (f) Performance Monitoring.....                                 | 6        |
|          | (g) Configuration Management as a Service .....                 | 7        |
|          | (h) Budgetierung und Kostenlimits .....                         | 7        |
|          | (i) Angebot von Schulungs- und Zertifizierungsprogrammen.....   | 7        |
| 2.3      | Anforderungen zum Datenschutz.....                              | 8        |
| 2.4      | Marktgängige Zertifizierungen .....                             | 8        |
| 2.5      | Anforderungen zu IT-Sicherheit.....                             | 8        |
|          | (a) Grundsätzliches.....                                        | 8        |
|          | (b) Verschlüsselung.....                                        | 9        |
|          | (c) Authentifizierung .....                                     | 10       |
|          | (d) Logging .....                                               | 10       |
| 2.6      | Support-Anforderungen .....                                     | 11       |
|          | (a) 24/7h Support und schnelle Antwortzeit .....                | 11       |
|          | (b) Form und Sprache des Supports .....                         | 11       |
|          | (c) Freier Online Support.....                                  | 11       |
|          | (d) Priorisierung von Incidents .....                           | 11       |
|          | (e) Support für Dritt-Anbieter-Software .....                   | 11       |
| 2.7      | Anforderungen zur Souveränität .....                            | 12       |
|          | (a) EU*-basierter Betrieb der Public-Cloud .....                | 12       |
|          | (b) EU*-Dauerbetrieb .....                                      | 12       |
|          | (c) Datenauskunft, Datenzugriff und Portabilität .....          | 12       |
|          | (d) Technische und betriebliche Dokumentation und Hardware..... | 12       |
| 2.8      | Anforderungen zu Schnittstellen .....                           | 13       |

|      |                                                                                |    |
|------|--------------------------------------------------------------------------------|----|
| 2.9  | Anforderungen zu Prozessen.....                                                | 13 |
| 2.10 | Anforderungen zu Netzwerkanbindungen .....                                     | 14 |
| 2.11 | Anforderungen zum IT Service Continuity Management und Disaster Recovery ..... | 14 |
| 2.12 | Anforderung an Dokumentationen und das Reporting .....                         | 14 |
| 2.13 | Anforderungen zur Zusammenarbeit .....                                         | 15 |
| 2.14 | Anforderungen an die Vertragsbeendigung .....                                  | 16 |
|      | (a) Allgemeine Anforderungen .....                                             | 16 |
|      | (b) Einzelne Unterstützungsleistungen .....                                    | 17 |
|      | (c) Vergütung.....                                                             | 17 |

# **1 INHALT DIESES DOKUMENTS UND RAHMENBEDINGUNGEN**

## **1.1 Einleitung**

Diese Anlage beinhaltet die Anforderungen und Vorgaben zur Leistungserbringung durch den Auftragnehmer sowie weitere Rahmenbedingungen zur Zusammenarbeit.

Diese hat der Auftragnehmer im Rahmen der Leistungserbringung einzuhalten. Das konkrete „Wie“ der Umsetzung dieser Anforderungen ist in D04-II „Anlage 5 (Lösungsdokumente)“ zum Vertrag\* und den jeweiligen Anhängen dargestellt.

Grundsätzlich umfasst diese Anlage Anforderungen und Vorgaben zur Leistungserbringung zu folgenden Themen:

- (i) Anforderungen zum Leistungsstandort
- (ii) Technische Anforderungen
- (iii) Anforderungen zum Datenschutz
- (iv) Marktgängige Zertifizierungen
- (v) Anforderungen zu Security und Authentifizierung
- (vi) Support-Anforderungen
- (vii) Anforderungen zur Souveränität
- (viii) Anforderungen zu Schnittstellen
- (ix) Anforderungen zu Prozessen
- (x) Anforderungen zu Netzwerkanbindungen
- (xi) Anforderungen zum IT Service Continuity Management und Disaster Recovery
- (xii) Anforderung an Dokumentationen und das Reporting
- (xiii) Anforderungen zur Zusammenarbeit

## **1.2 Überblick Leistungsinhalt**

Der Auftragnehmer stellt eine Cloud-Plattform\* für zu implementierende Anwendungen des Auftraggebers zur Verfügung. Die vom Auftragnehmer bereitzustellende Cloud-Lösung soll hierbei durch einheitliche Leistungen eine externe (Off-Premises, Public Cloud) Leistungsbereitstellung ermöglichen.

Die Bundesbank übernimmt die Rolle des Integrators der zentralen Cloud-Lösungen und Integrationsleistungen sind nicht Bestandteil der Leistung des Auftragnehmers.

- (i) Das verfügbare Serviceportfolio des Auftragnehmers umfasst mindestens folgende Servicegebiete, die je nach Ausprägung als IaaS und/oder PaaS bzw. als FaaS und/oder SaaS auszuprägen sind:
  - 1. Cloud Compute
    - Virtuelle Server in verschiedensten Ausprägungen (Core, RAM, Performance, Betriebssystem) mit oder ohne Betriebssystem Lizenz
    - Dedizierte Server in verschiedensten Ausprägungen (CPU, RAM, Performance, Betriebssystem) mit oder ohne Betriebssystem Lizenz
    - Verwaltete Container-Orchestrierung mit automatischer Skalierung und Optimierung der zugrundeliegenden Infrastruktur

2. Cloud Storage (Disk/Backup)
  - Managed Storage für Block Storage, File Storage, Object Storage, Backup und Archive in verschiedenen Ausprägungen (Redundanz, Performance)
3. Cloud-Datenbanken
  - Datenbanken in verschiedenen Ausprägungen (Datenbank-Typ, Größe und Performance) mit und ggf. ohne Lizenz
4. Generelle Cloud Services\*
  - Verwaltungs-Services\* für die Cloudumgebung (System Management, Monitoring, Logging, Configuration, Analyse und Automation)
  - Security, Identity und Compliance Services\* zur Umsetzung der Vorgaben der Deutschen Bundesbank, die sich an C5 sowie dem BSI IT-Grundschutz ausrichten
  - Loadbalancing- und Firewall-Services\* für die Cloudinfrastruktur
  - Migrationsservices zur Unterstützung der Cloudtransformation der Deutschen Bundesbank wie z. B. für Discovery Services\*, Servermigration Services\* (P2V und V2V), Datenbankmigration Services\*, Datentransport Services\*
  - Internet Breakout als Backup zum zentralen Internetbreakout der Deutschen Bundesbank aus dem eigenen Netzwerk
  - Container Services\* inkl. Verwaltung und Integration in der Cloudumgebung zur Nutzung von Microservices
  - Managed Services\* für Server, Datenbanken und Middleware in verschiedenen Ausprägungen (Service Level, Betriebszeiten)
  - Technische Möglichkeiten zur Etablierung getrennter Staging-Umgebungen mit entsprechenden Berechtigungen und Netztrennungen für DEV, Test, QA und PROD bis auf Workload-Ebene
  - Administrative Services\* bspw. für Cost Management und Billing (Alerting, Tagging, etc.)
  - Unterstützung von Entwicklungsumgebungen (z.B. interaktiver Notebooks) für Data Engineering und Data Science
5. Automation-, AI- und IoT- Services\*
  - Services\* im Bereich AI (Artificial Intelligence) wie z. B. KI-Stacks (Frameworks, Infrastruktur und Tools), Machine Learning-Plattformen, API-gesteuerte Services\*
  - Services\* im Bereich Automation wie z. B. Data Warehousing, Data Lake und Lakehouse-Szenarien über Business Intelligence, Batch-Verarbeitung sowie Stream- und analytische Compute-Funktionalitäten (Spark oder vergleichbare Technologien), Datenstromverarbeitung und maschinelles Lernen bis hin zur Abstimmung der Daten\* Workflows

- Analysefunktionen auf Daten\* im Lakehouse bzw. Data Lake sowie Services\* im Bereich Analytics, z. B. Data Warehouses, Clickstream-Analysen, Betrugserkennung, Empfehlungsfunktionen, ereignisgesteuertes Extrahieren, Transformieren und Laden, serverlose Datenverarbeitung und IoT-Verarbeitung
- Bereitstellung von Funktionen zur Verwaltung von Metadaten sowie zur Unterstützung von Datenkatalogisierung, Datenklassifikation und Data-Governance, einschließlich der Möglichkeit zur strukturierten Erfassung, Organisation und Nutzung von Datenbeständen.
- Unterstützung der Orchestrierung von Datenpipelines, Workflows und wiederkehrenden Verarbeitungsprozessen

Der Auftragnehmer ermöglicht dem Auftraggeber jederzeit Zugriff auf sein komplettes Cloud Service Portfolio, das der Auftragnehmer in der von dem Auftraggeber gewählten Region seinen Kunden über das Self-Service Portal zugänglich macht.

## 2 ANFORDERUNGEN UND VORGABEN

Die Anforderungen und Vorgaben in diesem Kapitel sind – soweit nicht ausdrücklich anders vermerkt – unverzichtbare Anforderungen, welche der Auftragnehmer im Rahmen der Leistungserbringung einhält.

### 2.1 Anforderungen zum Leistungsstandort

Eine Änderung der servicespezifisch vereinbarten Leistungsstandorte erfordert die Weisung des Auftraggebers in Textform.

#### (a) Georedundante Standorte für die Cloud Leistungen

Der Auftragnehmer erbringt seine Public Cloud Leistungen mindestens an **zwei georedundanten Standorten** in der EU\* mit **jeweils einem (1) Twin-Datacenter\*** mit den folgenden Eigenschaften je Standort:

- (i) Replikation mit max. 20ms Paketlaufzeit zum zentralen Netzknotenpunkt Frankfurt DE-CIX.
- (ii) Ein Twin-Datacenter\* besteht aus mindestens zwei (2) Brandschutzzonen mit redundanter Technik im Sinne zweier getrennter Rechenzentren.
- (iii) Die Daten\* verlassen die EU\* auch für den Transport zwischen den Standorten nicht.

### 2.2 Technische Anforderungen

#### (a) Unterbrechungsfreie Leistungserbringung

Aufgrund von unterschiedlichen Business-Anforderungen benötigt der Auftraggeber die Flexibilität, dass Neustarts von Services\* den Dienst nicht unterbrechen. Daher muss der Auftragnehmer Folgendes sicherstellen:

- (i) Die für den Anwendungsbetrieb bzw. Servicebetrieb erforderlichen Ressourcen und Services\* des Auftragnehmers werden durch Wartungs- und Patch\*-Tätigkeiten nicht unterbrochen, soweit die vom jeweiligen Anbieter bereitgestellten Best Practice Anleitungen genutzt werden.
- (ii) Der Auftragnehmer stellt die Leistungen mit den in Anlage 3 (Servicekatalog und Servicebeschreibung) zugesagten und marktüblichen Service Levels zur Verfügung.

- (iii) Der Auftragnehmer wird die Einhaltung der Service Levels regelmäßig mit abgestimmten Messverfahren messen. Die Messungen erfolgen jeweils in Bezug auf einen definierten Zeitraum („**Bezugszeitraum**“). Der Auftragnehmer wird für die Service Levels jeweils adäquate, marktübliche Bezugszeiträume vorschlagen. Soweit nicht abweichend vereinbart, ist der Bezugszeitraum monatlich.
- (iv) Die Nichteinhaltung der vereinbarten Service Qualität führt zu einem angemessenen Service Credit. Der Service Credit soll eine angemessene monetäre Kompensation für den aufgrund der Nichteinhaltung eines Service Level eingetretenen Minderwert der vom Auftragnehmer nicht vertragsgemäß erbrachten Leistung darstellen. Weitergehende Ansprüche des Auftraggebers bleiben von einem Service Credit unberührt.
- (v) Weiterhin führt der Auftragnehmer alle notwendigen Untersuchungen durch, um die Gründe für den Ausfall zu benennen und ergreift die geeigneten Maßnahmen, um gleichartige Ausfälle zukünftig auszuschließen.
- (vi) Die Cloud-Lösung enthält datenschutzfreundliche Einstellmöglichkeiten (privacy by design/by default).

**(b) Auftragnehmer-Linux Distributionen**

Um das Risiko der Abhängigkeit von bestimmten OS-Distributionen zu minimieren, ist es notwendig, dass der Auftragnehmer verschiedene Distributionen bereitstellt, um unabhängig von möglichen OS-Distributoren (Patch\*-Zyklen, Security Risks) zu sein und parallel eine höhere Qualität zu bieten.

Folgende Anforderungen sind durch den Auftragnehmer bzw. dessen Cloud-Lösung einzuhalten:

- (i) Sicherstellung, dass als Betriebssystemumgebung mehrere Linux Distributionen zur Verfügung stehen, darunter mindestens eine freie Linux Distribution sowie RedHat Enterprise Linux.
- (ii) Optimierung der Linux Distributionen und Integration in die Cloud-Umgebung.
- (iii) Regelmäßige Bereitstellung von Security Patches.

**(c) Rollenbasierte Zugriffe**

Für den IT-Betrieb muss, soweit technisch realisierbar, mindestens ein Basisfunktionsumfang zur Verfügung stehen, um Services\* starten, löschen, neu starten, abschalten und Snapshots machen zu können.

Parallel muss die Möglichkeit bestehen, Rechte mit derselben Detailtiefe wie die Rollen zuzuweisen, um Rollen/Funktionen sicherheitstechnisch zu trennen.

Folgende Anforderungen sind durch den Auftragnehmer bzw. dessen Cloud-Lösung, einzuhalten:

- (i) Die Cloud-Lösung ermöglicht einen rollenbasierten Zugriff.
- (ii) Bereitstellung eines Identity-Management-Systems mit granularen rollenbasierten Autorisierungsmöglichkeiten für Services\* (sowohl für Management Console als auch Service Interface).

- (iii) Möglichkeit der Autorisierung von Usern/Gruppen durch Zuordnung zu einer Rolle auf Assets/Gruppen von Assets.
- (iv) Granulare Rechte für die angebotenen Services\* - mindestens notwendige granulare Rechte für Services\* sind: Erstellen, löschen, neu starten, abschalten, starten und Backups/Snapshots.
- (v) Die Evaluierung und Durchsetzung von Rollen-, Rechte- und Richtlinienentscheidungen erfolgt vollständig innerhalb der EU\*. Identitäts- und Richtlinienmechanismen besitzen keine Abhängigkeiten zu globalen Directory-, DNS- oder Policy-Komponenten außerhalb der EU\*.
- (vi) Trennung zwischen den Konfigurations- und Datenebenen der Services\* soll mit Hilfe der Rollen möglich sein.
- (vii) Möglichkeit der Konfiguration über das Web Interface und API.
- (viii) Einbindung eines externen Verzeichnisdienstes (wie z. B. EntraID, AWS IAM Identity Center, etc.) für die Nutzung der Clouddienste zur Authentifizierung.

**(d) Rollen nach dynamischen Gruppen und Strukturen**

Aufgrund der komplexen Anwendungs- und Verantwortungsstruktur des Auftraggebers muss die Möglichkeit bestehen, IT-Ressourcen mit individuellen Metainformationen zu versehen und innerhalb der Gruppierung von Metainformationen Rollen/Rechte zu vergeben; so besteht zum Beispiel die Möglichkeit, übergreifende Admins von lokalen Admins für bestimmte Kundenbereiche zu trennen sowie nach bestimmten Verfahren, Umgebungen Rechte zu vergeben.

Ferner dient es dazu, den Überblick über eine komplexe Rechtestruktur zu behalten. Durch eine Rollenstruktur nach Metainformationen kann jederzeit festgestellt werden, welchen Usern welche Rollen zugeordnet sind, um so einen strukturierten Überblick zu behalten.

Folgende Anforderungen sind durch den Auftragnehmer bzw. dessen Cloud-Lösung einzuhalten:

- (i) Bereitstellung eines Identity-Management-Systems mit granularen rollenbasierten Autorisierungsmöglichkeiten zu Services\*, Elementen von Services\* sowie ganzen Accounts.
- (ii) Möglichkeit der Vergabe von Zugriffsrechten je Gruppe (individuellen Strukturen von IT-Ressourcen sowie auf individuellen Elementen) auf Basis von Metadaten (bspw. Zugriffsrechte in einer Gruppe von Servern und Services\* für ein Projekt).
- (iii) Möglichkeit der Konfiguration über das Web Interface und API.

**(e) RDBMS as a Service**

Aufgrund der Vielfalt, der von dem Auftraggeber bevorzugt genutzten Datenbank-Varianten sowie der unterschiedlichen Managementstrukturen und Verantwortungsbereiche, werden RDBMS Services\*, welche grundlegende konfigurierbare Datenbank-Funktionen/Features zur Verfügung stellen, gefordert, ohne spezifisches Know-how zu benötigen.

Im Bestand des Auftraggebers werden viele Anwendungen betrieben, die MSSQL-Datenbanken verwenden. Diese Anwendungen lassen sich nicht mit vertretbarem Aufwand auf RDBMS-Systeme anderer Hersteller migrieren.

Folgende Anforderungen werden durch den Auftragnehmer bzw. die Cloud-Lösung erfüllt:

- (i) Der Auftragnehmer hat keinen inhaltlichen Zugriff auf die Daten\* des Auftraggebers, um so eine mögliche Veränderung von Daten\* durch den Auftragnehmer bzw. der von ihm eingesetzten Personen und/oder einen Abfluss von Daten\* durch den Auftragnehmer bzw. der von ihm eingesetzten Personen auszuschließen.
- (ii) Ein oder mehrere Relational Database Management System (RDBMS) as a Service, welche vollautomatisiert im Self Service bedienbar sind; hier ist für den Auftraggeber kein Zugriff auf darunterliegende OS möglich und die Wartung des Service wird komplett durch den Auftragnehmer durchgeführt.
- (iii) Der vollständige technische Betrieb erfolgt ausschließlich innerhalb der EU\*.
- (iv) Mindestens Microsoft SQL Server (MSSQL), PostgreSQL , MySQL sowie NoSQL (Dokumenten-, Key-Value-Datenbanken) und Cloud eigene Datenbanken sind verfügbar.
- (v) Es besteht die Möglichkeit, von dem Auftraggeber selbst erworbene Lizenzen in der Cloud zu nutzen (bring-your-own-licence).
- (vi) Eine georedundante (nach BSI) Replikation ist konfigurierbar.
- (vii) Es muss ermöglicht werden einen eigenen Verschlüsselungsschlüssel (Bring-Your-Own-Key) zur Verschlüsselung der Nutzdaten\* einzusetzen.
- (viii) Es besteht die Möglichkeit Nutzdaten\* verschlüsselt abzulegen, so dass sie nur für den Auftraggeber lesbar sind, insbesondere nicht für den Auftragnehmer ohne vorherige Zustimmung durch den Auftraggeber.

**(f) Performance Monitoring**

Für die aktive Betriebsführung im Sinne der Sicherstellung von Stabilität und Performance ist für den Auftraggeber eine Echtzeitauswertung diverser Betriebsparameter notwendig.

Zur Sicherstellung der zwischen dem Auftragnehmer und dem Auftraggeber vereinbarten Service Levels sowie der Unterstützung in Fehlerfällen bzw. einer Root Cause Analysis sind entsprechende Logging-Funktionen notwendig.

Daher wird der Auftragnehmer bzw. die Cloud-Lösung folgende Anforderungen an Monitoring erfüllen:

- (i) Es können über das Web Interface und API auf Monitoring Informationen zurückgegriffen werden. Metriken sind mindestens:
  1. Compute: CPU Utilization und Memory Utilization
  2. Storage: Disk I/O, Storage utilization, IOPS, queue length
  3. Netzwerk: Network I/O, Netzwerkbandbreite, Packet loss, Loadbalancer request latency und Connection count/Sessions
  4. Service-spezifische Kennzahlen wie u.a. dienstabhängige Leistungs-, Verfügbarkeits- und Nutzungsmetriken, wie beispielsweise Response Times, Fehlerraten, Throughput, Request-Volumen, Queue-Längen, Datenbank-Transaktionen, Cache-Hit-Raten oder Auto-Scaling-Ereignisse.

- (ii) Eine Echtzeitauswertung diverser Betriebsparameter ist nach Bedarf des Nutzers konfigurierbar.

**(g) Configuration Management as a Service**

Bisherige Erfahrungen aus dem Cloud-Betrieb zeigen, dass neben reinen eigenen Server-Templates auch weitere Konfigurationen wie FWaaS, LBaaS, IAM, IaC etc. notwendig sind, um standardisierte und lauffähige Umgebungen auf Knopfdruck zur Verfügung zu stellen und so Templates für komplette Umgebungen bzw. Anwendungsumgebungen zu erstellen.

Daher wird der Auftragnehmer bzw. die Cloud-Lösung folgende Anforderungen erfüllen:

- (i) Möglichkeit, im Rahmen eines integrierten Configuration Management Services\* auf Administrationsschnittstellen (Web, Command Line, etc.) zuzugreifen, Konfigurationen für Cloud Komponenten automatisiert zu verarbeiten und zu speichern und Paketierungen von kompletten Infrastrukturen zu automatisieren.
- (ii) IaC: Komplette Infrastrukturen einschließlich darauf installierter Software können als Template bzw. Code erstellt, aktualisiert und gespeichert werden.

**(h) Budgetierung und Kostenlimits**

Erfahrungen durch Nutzung von Cloud-Lösungen zeigen, dass durch die einfache Bereitstellung von Cloud-Services\* schnell Fehlkonfigurationen bzw. überzogenes Nutzungsverhalten entstehen, welche zu möglichen Kostenexplosionen führen. Um das zu verhindern, muss es möglich sein, bewusst Limits oder Einschränkungen zu definieren.

Daher wird der Auftragnehmer bzw. die Cloud-Lösung folgende Anforderungen erfüllen:

- (i) Möglichkeit, einen maximalen Verfügungsrahmen für einen bestimmten Account oder einen bestimmten Service über das Web-Interface oder per API zu erstellen, um mögliche Kostenexplosionen zu vermeiden.
- (ii) Hierbei ist wählbar, ob bei Aufbrauchen des Volumens die Services\* eingestellt werden oder bestimmte Rechte des Accounts eingeschränkt werden.
- (iii) Des Weiteren ist durch die Definition von möglichen Schwellenwerten eine frühzeitige Alarmierung (z. B. per Mail) möglich, um zusätzliche Transparenz für den Kostenverantwortlichen zu schaffen.

**(i) Angebot von Schulungs- und Zertifizierungsprogrammen**

Der Auftragnehmer bietet ein ausgearbeitetes Schulungs- und Zertifizierungsprogramm an, mit dem Mitarbeiter des Auftraggebers qualifiziert und externe Fachkräfte, welche Leistungen für den Auftraggeber erbringen, auf ihre Qualifikation hin geprüft werden können. Die Trainings umfassen insbesondere:

- a. Die Vermittlung von Grundlagenwissen zu Cloud-Konzepten, Kernservices, Governance- und Sicherheitsmechanismen sowie Betriebsmodellen.
- b. Die Durchführung vertiefender, rollenbezogener Schulungen zu Architektur, Administration, Entwicklung, Betrieb, Sicherheit, Datenmanagement und Management-Aufgaben.
- c. Praxisorientierte Übungen, Hands-on-Labs und Vorbereitung auf einschlägige Zertifizierungen.
- d. Die Bereitstellung aller notwendigen Schulungsunterlagen, Lernpfade und unterstützender Materialien.

**(j) Regionale Autonomiefähigkeit der Plattform**

Die Cloud-Plattform\*- muss so ausgelegt sein, dass der Betrieb innerhalb der EU\* für einen angemessenen Zeitraum, mindestens jedoch für zwölf (12) Monate, auch dann aufrechterhalten werden kann, wenn Verbindungen zu globalen Verwaltungs-, Kontroll- oder Infrastrukturkomponenten gestört oder unterbrochen sind. Hierzu zählt insbesondere, dass grundlegende Steuerungs-, Bereitstellungs- und Betriebsfunktionen der Plattform ohne Abhängigkeiten zu außerhalb der EU\* betriebenen Systemen verfügbar bleiben.

**2.3 Anforderungen zum Datenschutz**

Die Anforderungen der Leistungserbringung an den Datenschutz sind in Anlage 4 (Vereinbarung zur Auftragsverarbeitung) zum Vertrag\* über die Bereitstellung EU\*-nativer Cloud-Services\* („**Vertrag\***“) geregelt. Der Auftragnehmer hat die dort festgelegten Vorgaben bei der Erbringung sämtlicher Leistungen nach dem Vertrag\* einzuhalten.

**2.4 Marktgängige Zertifizierungen**

Der Auftragnehmer stellt für seine Leistungserbringung sicher, dass er über nachfolgende Zertifizierungen oder Testate in einem aktuellen Stand und mit relevantem Zertifizierungs- bzw. Testierungsumfang verfügt.

- (i) DIN EN ISO/IEC 27001 (oder IT-Grundschutz) oder vergleichbar
- (ii) C5-Testierung
  - (a) C5-Typ-2-Testierung, durchgeführt durch einen qualifizierten Prüfer, gemäß dem jeweils aktuell geltenden BSI-Anforderungskatalog Cloud Computing Compliance Controls Catalog (C5). Liegt für einen Service bislang ausschließlich eine C5-Typ-1-Testierung vor, welche die Grundlage für eine anschließende Typ-2-Testierung bildet, ist der Auftragnehmer verpflichtet, für den Service eine C5-Typ-2-Testierung spätestens bis zum 31. Dezember 2027 vollständig durchführen zu lassen und dem Auftraggeber die entsprechenden Nachweise unverzüglich vorzulegen.

**2.5 Anforderungen zu IT-Sicherheit**

**(a) Grundsätzliches**

Für alle Leistungen wird der Auftragnehmer in seinem Aufgabenbereich Sicherheitsleistungen erbringen, die von einem professionellen Auftragnehmer nach dem jeweiligen aktuellen Stand der Technik sowie unter Berücksichtigung von allgemein anerkannten Sicherheitsrichtlinien und Standards erwartet werden dürfen.

Der Zugang zur Cloudumgebung sowie zu sämtlichen Administrations-, Management- und Abrechnungskomponenten muss ausschließlich durch die Deutsche Bundesbank und den Betreiber der Cloudplattform erfolgen. Betreiber der Cloudplattform im Sinne dieser Leistungsbeschreibung sind der Plattformhersteller selbst sowie mit ihm verbundene Unternehmen. Sofern nicht anders in diesem Vertrag\*, insbesondere dem vorliegenden Dokument, geregelt, ist die Weitergabe von Authentifizierungs- und Zugriffsdaten, einschließlich Benutzerkennungen, Passwörtern, kryptographischen Schlüsseln, Zertifikaten oder vergleichbaren Sicherheitsinformationen ausschließlich an mit dem Betreiber verbundene Unternehmen oder von diesem ausdrücklich beauftragte Dritte

erlaubt, und nur soweit diese unmittelbar dem technischen Betrieb der Cloudplattform zuzurechnen sind. Falls der Auftragnehmer nicht Betreiber der Cloudplattform ist, darf der Auftragnehmer unter keinen Umständen weder unmittelbar noch mittelbar in Zugriff, Betrieb, Support oder Leistungsüberwachung der Cloudplattform eingebunden sein.

- (i) Der Auftragnehmer verfügt über ein Sicherheitskonzept, das die Maßnahmen beschreibt, die der Auftragnehmer im Bereich der Informationssicherheit und den von ihm zu erbringenden Leistungen implementiert hat.
- (ii) Der Auftragnehmer wird dieses Sicherheitskonzept dem Auftraggeber erläutern.
- (iii) Zu diesen Maßnahmen zählen insbesondere die nachfolgenden Punkte unter lit. ((b)) bis ((d)) sowie die an anderen Stellen des Vertrags und dieser D03-II "Anlage 1 (Anforderungen und Vorgaben zur Leistungserbringung)" geforderten Maßnahmen.
- (iv) Das Sicherheitskonzept wird vom Auftragnehmer regelmäßig überprüft und – soweit erforderlich – an aktuelle sicherheitsrelevante Entwicklungen angepasst.

**(b) Verschlüsselung**

Der Auftragnehmer sowie Dritte dürfen keine Möglichkeit haben, ohne vorherige ausdrückliche Zustimmung durch den Auftraggeber, von den Nutzdaten\* des Auftraggebers Kenntnis zu erlangen, diese zu verändern oder weiterzugeben.

Daher wird der Auftragnehmer folgende Anforderung einhalten:

- (i) Sämtliche Kommunikation mit den Services\* des Auftragnehmers wird verschlüsselt durchgeführt. Dabei kommt mindestens TLS v1.2 zur Anwendung. Während der Vertragslaufzeit wird der Auftragnehmer die angewendete Version der Verschlüsselung auf dem Stand der Technik gemäß Empfehlungen des BSI und NIST halten und den Auftraggeber mit angemessenem Vorlauf einem von ihm geforderten Stand der Verschlüsselung anbieten.
- (ii) Ebenso hat die Kommunikation zwischen Services\* verschlüsselt zu erfolgen.
- (iii) Alle Daten\* des Auftraggebers müssen mindestens mit einem vom Auftragnehmer bereitgestellten Key verschlüsselt werden können.
- (iv) Weiterhin muss die Verwendung eines kundeneigenen Verschlüsselungsschlüssel (Bring Your Own Key) unterstützt werden.
- (v) Ein regelmäßiger, ungeplanter oder kurzfristiger Schlüsselwechsel durch oder auf Weisung des Auftraggebers muss möglich sein.
- (vi) Schlüssel, die im Prozess der Sicherung der Daten\* des Auftraggebers verwendet werden, müssen ausschließlich für den Auftraggeber bereitgestellt werden. Der Auftraggeber kann unabhängig vom Auftragnehmer die Schlüssel jederzeit, gezielt löschen.
- (vii) Der Auftragnehmer unterstützt Verschlüsselungsmechanismen, die den aktuellen Empfehlungen des BSI (Bundesamt für Sicherheit in der Informationstechnik) gemäß BSI TR-02102 und der NIST (National Institute of

Standards and Technology) gemäß NIST SP 800-57 bezgl.  
Verschlüsselungsalgorithmen gerecht werden.

**(c) Authentifizierung**

Bezüglich Authentifizierung erfüllt der Auftragnehmer bzw. dessen Cloud-Lösung folgende Anforderungen:

- (i) Die Authentifizierung an der Serviceschnittstelle der Cloud Plattform erfolgt mit Zugangskonten in Verantwortung des Auftraggebers, die über eine Federation Funktion in das Rollen- und Rechtemanagementsystem des Auftragnehmers integriert werden können. Unterstützung einer Federation zum IAM des Auftraggebers mit dem Protokoll SAML 2.0 oder OpenID Connect.
- (ii) Möglichkeit, mittels Federation die Authentifizierungsdaten mit mehreren Hyperscalern zu nutzen.
- (iii) Möglichkeit der Installation eines Domain Controllers (o.ä.) in der Cloud-Umgebung die als managed bzw. Directory-as-a-Service (z. B. Entra ID Domain services, Google managed AD) betrieben wird, um Anwendungsauthentifizierung über Kerberos zu ermöglichen.
- (iv) Das gesamte Rollen- und Rechtekonzept basiert auf dem o. a., um administrative Zugriffe auf Cloud-Ressourcen aus dem On-Premises-Netzwerk heraus steuern zu können.
- (v) Für die Authentifizierung an Cloud-Services\* können On-Premises-Benutzeraccounts aus dem Verzeichnisdienst des Auftraggebers genutzt werden.
- (vi) Für die Authentifizierung an der Self-Service-Schnittstelle muss die Verwendung von Multi-Faktor-Authentifizierung (MFA) möglich und erzwingbar sein.

**(d) Logging**

Security- und Systemevents sind zu protokollieren bzw. zu loggen, daher wird der Auftragnehmer folgende Anforderung einhalten:

- (i) Entsprechende Logging-Funktionen zur Sicherstellung der internen SLAs sowie der Unterstützung in Fehlerfällen bzw. zur Root Cause Analysis.
- (ii) Möglichkeit, Logfiles kontinuierlich und automatisiert zu erhalten und dauerhaft zu archivieren.
- (iii) Möglichkeit, Logfiles automatisch zu löschen nach vorgegebenen Zeiträumen (z. B. aufgrund regulatorischer Vorgaben).
- (iv) Relevante Dimensionen für das Logging sind: Historie, Nachvollziehbarkeit der Einträge sowie Belastbarkeit der Logging-Daten\*.
- (v) Möglichkeit der Anbindung der relevanten Logging-Dienste an die Datenspeicher des Auftraggebers. Die zu loggenden Parameter sind von dem Auftraggeber konfigurierbar. Das Logging (inkl. Datum, Uhrzeiten und Einzelheiten relevanter Ereignisse) muss mindestens folgende Events unterstützen:
  - 1. Nutzeraktivitäten, wie erfolgreiche und abgelehnte Zugriffsversuche

2. Konfigurationsänderungen
3. Aufrufe von Programmierschnittstellen
4. Aufzeichnung von Kommunikationsverbindungen
5. Rechteauserweiterung (privilege escalation)
6. Nutzung privilegierter Rechte
7. Ereignisse im Lebenszyklus kryptographischer Schlüssel

**e) Regionale Control-Plane-Unabhängigkeit**

Der Auftragnehmer stellt sicher, dass Steuerungs-, Verwaltungs- und Kontrollkomponenten der Cloud-Plattform, einschließlich Identitäts-, Richtlinien-, Konfigurations- und Abrechnungsdienste (Control-Plane), ausschließlich innerhalb der EU\* betrieben werden und keine technischen oder operativen Abhängigkeiten zu betriebenen Systemen außerhalb der EU\* bestehen.

## **2.6 Support-Anforderungen**

Im Rahmen der Integration und Verwendung für Anwendungen im Umfeld der Deutschen Bundesbank ist ein hohes Supportniveau notwendig.

**(a) 24/7h Support und schnelle Antwortzeit**

Der Auftragnehmer leistet einen 24/7h Support mit einer Differenzierung der Antwortzeiten nach Schweregrad auf einem Enterprise-fähigen Level. Dieses beinhaltet bei hoher Beeinträchtigung von geschäftskritischen Systemen der Deutschen Bundesbank eine Reaktionszeit\* von maximal 15 Minuten und einer entsprechenden Abstufung nach sinkender Kritikalität.

**(b) Form und Sprache des Supports**

Der Support erfolgt per

- (i) Service-Portal
- (ii) Chat
- (iii) Mail
- (iv) Telefon

Der für die Support Cases zuständige Support wird in deutscher oder englischer Sprache geleistet.

**(c) Freier Online Support**

Parallel stellt der Auftragnehmer einen kostenfreien Online Support zur Verfügung, welcher FAQs, Wissensdatenbanken, Best Practices und Foren zur Verfügung stellt.

**(d) Priorisierung von Incidents**

Es können bestimmte Incidents beim Auftragnehmer durch den Auftraggeber priorisiert werden (z. B. Notfälle).

Bei Bedarf steht dem Auftraggeber ein dedizierter technischer Ansprechpartner zur Verfügung, welcher entsprechendes Know-How für das Unternehmen des Auftraggebers mitbringt und sich nicht bei jedem Incident erneut einarbeiten muss.

**(e) Support für Dritt-Anbieter-Software**

Im Rahmen des Supports sind über die Cloud-Lösung hinaus Unterstützung für folgende Lösungen gegeben in allen bereitgestellten Versionen:

- (i) RedHat Enterprise Linux Server und mindestens ein lizenzfreies Linux
- (ii) Microsoft Windows Server
- (iii) SSH, OpenVPN
- (iv) VPN-Unterstützung für die Netzkopplung des Premise RZ und der Cloud-Lösung
- (v) Apache, IIS
- (vi) MS SQL Server, PostgreSQL, MySQL

## 2.7 Anforderungen zur Souveränität

### (a) EU\*-basierter Betrieb der Public-Cloud

Der Auftragnehmer verpflichtet sich den vollständigen operativen Cloud-Betrieb und die Administration der eingesetzten Technologien eigenständig innerhalb der EU\* zu gewährleisten. Abhängigkeiten zur Produktwartung einschließlich ggf. notwendigen Herstellersupport, Patch\*-Bereitstellung oder Weiterentwicklung durch Nicht-EU\*-Hersteller sind zulässig, sofern dadurch keine kritische Abhängigkeit im laufenden Betrieb entsteht.

Der Auftragnehmer stellt sicher, dass während der gesamten Vertragslaufzeit sämtliche Betriebs-, Wartungs- und Supportleistungen ausschließlich durch Personal erbracht werden, das seinen gewöhnlichen Aufenthaltsort innerhalb der EU\*/des EWR\* hat. Dies umfasst insbesondere Incident-, Problem- und Change-Management, Sicherheitsüberwachung, Patch\*-Management sowie sämtliche technischen Eskalationsprozesse. Eine Verlagerung oder Ausführung dieser Tätigkeiten durch Personal außerhalb der EU\*/des EWR\* ist unzulässig.

### (b) EU\*-Dauerbetrieb

Der Auftragnehmer gewährleistet, dass die angebotene Cloud-Plattform\* innerhalb der EU\* für einen Zeitraum von mindestens zwölf (12) Monaten ohne zwingende Abhängigkeiten von Infrastruktur, Validierungsmechanismen oder sonstigen betriebskritischen Leistungen außerhalb der EU\* funktionsfähig weiterbetrieben werden kann.

### (c) Datenauskunft, Datenzugriff und Portabilität

Der Auftragnehmer gewährleistet dem Auftraggeber während der gesamten Vertragslaufzeit uneingeschränkten und unmittelbaren Zugriff auf alle eigenen Daten\*. Der Zugriff, Export und die technische Portabilität der Daten\* müssen jederzeit innerhalb der EU\* vollständig gewährleistet sein, ohne dass hierfür Ressourcen oder Systeme außerhalb der EU\* erforderlich werden.

### (d) Technische und betriebliche Dokumentation und Hardware

Der Auftragnehmer verpflichtet sich, sämtliche technische und betriebliche Dokumentation sowie Quellcode während der gesamten Vertragslaufzeit innerhalb der EU\* verfügbar zu halten. Sämtliche technischen und betrieblichen Dokumentationen müssen dauerhaft in deutscher oder englischer Sprache bereitgestellt werden.

Sämtliche eingesetzten Hardware-Komponenten der Cloud-Infrastruktur (inkl. Server, Netzwerk- und Storage-Systeme) stammen ausschließlich aus Ländern, die den EU\*-Sicherheits- und Datenschutzstandards entsprechen und nicht auf den von der

Europäischen Kommission veröffentlichten Listen der Hochrisiko-Drittländer oder sicherheitlich nicht vertrauenswürdigen Herkunftsländer stehen. Komponenten aus Lieferketten, die gemäß EU\*- oder nationalen Sicherheitsbewertungen als kritisch eingestuft wurden, sind ausgeschlossen.

## 2.8 Anforderungen zu Schnittstellen

Es besteht die Möglichkeit, bestehende Incident-Management-Systeme mit der Support API zu integrieren:

- (i) Der Auftragnehmer stellt eine Standard-Schnittstelle zur Verfügung, die eine einfache Integration des Service Management Tools des Auftraggebers ermöglicht.
- (ii) Die Integration von Support Cases ist möglich (create, follow, update, attachments, close).
- (iii) Es kann eine unbegrenzte Anzahl an Cases angelegt werden.

Weiterhin besteht die Möglichkeit, über standardisierte Schnittstellen des Auftragnehmers einen marktüblichen Cloud Broker in die Cloud-Umgebung des Auftragnehmers zu integrieren.

Der Auftragnehmer stellt eine Schnittstelle bereit, um das Regelwerk von Sicherheitsübergängen (z. B. Firewall-Regelwerk, Access Control Lists) auszulesen.

## 2.9 Anforderungen zu Prozessen

Die folgenden Anforderungen gelten für alle Prozesse und werden vom Auftragnehmer akzeptiert und implementiert.

Der Auftragnehmer:

- (i) ist zuständig für die Definition, Einführung, Pflege und Umsetzung von Prozessen, Richtlinien, Systemen und Tools auf Seite des Auftragnehmers. Die Prozesse des Auftragnehmers müssen im Rahmen der zu erbringenden Services\* dem „Best Practice“ für den jeweiligen Prozess entsprechen und im Einklang mit dem ITIL V4 Framework bzw. dem bei dem Auftraggeber jeweils eingesetzten ITIL-Framework stehen;
- (ii) ist für die Erbringung von hochwertigen Services\* verantwortlich, die mit den jeweils geltenden Industrie-Standards konform sind;
- (iii) testet in marktüblichen Intervallen den Ausfall von hochverfügbaren (redundanten) Systemen;
- (iv) stellt sicher, dass revisionssichere Protokollierungs- und Archivierungsverfahren (Audit Trails) für alle Prozesse und Tätigkeiten im Rahmen der zu erbringenden Leistungen eingesetzt werden;
- (v) berichtet über Prozessstatus und -ergebnisse an den Auftraggeber in den relevanten Governance Gremien;
- (vi) steuert und überwacht die Prozesse im Rahmen der zu erbringenden Leistungen;
- (vii) nutzt abhängig von den Anforderungen und der erteilten schriftlichen Zustimmung des Auftraggebers kostenneutral ein eigenes Service Management System inkl. Bereitstellung bidirektionaler Schnittstellen mit synchronem Datenaustausch.
- (viii) stellt sicher, dass Administrations-, Zugriffs-, Support- und Sicherheitsprozesse ausschließlich durch Personal durchgeführt werden, dessen gewöhnlicher Aufenthaltsort innerhalb der EU\*/des EWR\* liegt. Für sicherheitsrelevante Vorgänge besteht kein Zugriff durch Personal mit gewöhnlichem Aufenthaltsort

außerhalb der EU\*/des EWR\*, sofern dies durch den Auftraggeber nicht abweichend angewiesen wurde.

- (ix) erlaubt dem Auftraggeber, nach vorheriger Ankündigung und Genehmigung, die Durchführung von Penetrationstests durch von dem Auftraggeber beauftragte, unabhängige Dritte. Der Auftragnehmer stellt sicher, dass entsprechende Tests ohne unzulässige Einschränkung durchgeführt werden können. Außerdem unterstützt er die Planung, Durchführung und Nachbereitung dieser Tests, einschließlich der Bereitstellung aller erforderlichen technischen Informationen, Protokolle und Zugänge, soweit dies zur ordnungsgemäßen Durchführung der Prüfungen erforderlich ist.

## **2.10 Anforderungen zu Netzwerkanbindungen**

- (i) Der Auftragnehmer wird zusammen mit dem Auftraggeber im Rahmen der Herstellung der Leistungsfähigkeit für die Cloud Services\* alle notwendigen Planungs- und Durchführungsleistungen unterstützen, so dass diese Services\* aus dem Netz der Deutschen Bundesbank unterbrechungsfrei nutzbar sind. Der Auftragnehmer verpflichtet sich zu aktiver und professioneller Zusammenarbeit mit dem Dienstleister des Auftraggebers zur Erbringung der Netzanbindung, insbesondere für Private Endpoints, VPN-Verbindungen, IPsec-basierten Tunneln sowie Direkt-Anbindungen.
- (ii) Die Verantwortung des Auftragnehmers umfasst die technische Unterstützung bei der Dimensionierung der Netzanbindung und der Definition technischer Spezifikationen der Netzanbindung, sowie, falls von dem Auftraggeber gefordert, die Unterstützung bei der Beschaffung der Netzanbindung.
- (iii) Die Integration des eigenen IP-Adressschemas der Deutschen Bundesbank in die Cloud-Netzwerkumgebung muss technisch unterstützt werden.

## **2.11 Anforderungen zum IT Service Continuity Management und Disaster Recovery**

IT Service Continuity Management ist ein übergreifender Prozessansatz des Auftragnehmers, der ihn dazu befähigt, die kritischen, unternehmensweiten Geschäftsfunktionen im Fall interner oder externer Ereignisse aufrecht zu erhalten oder zeitgerecht wiederherzustellen, so dass bei Eintreten unerwarteter Notfälle geeignete Notfallvorsorgemaßnahmen vorhanden sind, um die Leistungen im Rahmen der Vereinbarungen kontinuierlich zu erbringen und zu liefern.

Die Verantwortung des Auftragnehmers umfasst:

- (i) die Erstellung und Dokumentation eines IT Service Continuity Management Plans für die vom Auftragnehmer gegenüber des Auftraggebers zu erbringenden Leistungen;
- (ii) die Pflege und kontinuierliche Weiterentwicklung des IT Service Continuity Management Plans über die Vertragslaufzeit;
- (iii) ein mindestens jährliches Planen und Testen aller Komponenten des IT Service Continuity Management Plans in Zusammenarbeit mit dem Auftraggeber;
- (iv) die Ausführung des IT Service Continuity Management Plans in Abstimmung mit dem Auftraggeber.

## **2.12 Anforderung an Dokumentationen und das Reporting**

Als Dokumentationen und Reports werden alle Aufzeichnungen und Darstellungen (unabhängig vom genutzten Medium) verstanden, die im Zusammenhang mit den vom Auftragnehmer zu

erbringenden Leistungen stehen und durch den Auftragnehmer erstellt bzw. von dem Auftraggeber zur Nutzung der Leistungen benötigt werden.

Der Auftragnehmer erstellt und pflegt eine stets aktuelle Übersicht der von ihm zu liefernden Dokumentationen und Reports und stellt diesem dem Auftraggeber monatlich zur Verfügung. Der Auftragnehmer gewährleistet die Nachvollziehbarkeit von Änderungen.

Der Auftragnehmer stellt während der gesamten Laufzeit des Vertrages dem Auftraggeber ein umfangreiches Reporting zur Verfügung. Dieses Reporting beinhaltet mindestens folgende tagesaktuellen Informationen in Form eines Online-Reporting:

- (i) Verbrauch und Nutzung von Services\*
- (ii) Auslastungskennzahlen für Server, Datenbanken in notwendigen Parametern (CPU, RAM, Storage, etc.)
- (iii) Detaillierte Rechnung - auf Basis eines Asset-basierenden Tagging
- (iv) Incident, Problem, Change und Release & Deployment Reports
- (v) Status zu Beauftragungen
- (vi) Übersicht der eingetragenen Anwender und Berechtigungen
- (vii) Einhaltung/Nichteinhaltung von Service Levels
- (viii) Lizenzübersicht
- (ix) Compliance- und Risiko-Berichte

Vorbehaltlich längerer Zeiträume aufgrund von rechtlichen Anforderungen, sind die Berichte mindestens für die zurückliegenden zwölf (12) Monate einsehbar.

Zusätzlich besteht eine Meldepflicht des Auftragnehmers für schwerwiegende Vorfälle, insbesondere solche Ereignisse, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit der für die Leistungserbringung wesentlichen Systeme oder Daten\* spürbar beeinträchtigen oder beeinträchtigen können. Der Auftragnehmer verpflichtet sich die vorgenannten Ereignisse dem Auftraggeber unverzüglich und unaufgefordert mitzuteilen.

Im Falle einer Beendigung des Vertrags wird der Auftragnehmer dem Auftraggeber die gesamten relevanten, vollständigen und detaillierten Dokumentationen und Reports in dem jeweils aktualisierten Stand überlassen.

## **2.13 Anforderungen zur Zusammenarbeit**

Im Rahmen der Zusammenarbeit zwischen Auftraggeber und Auftragnehmer wird nach Vertragsschluss ein Zusammenarbeitsmodell umgesetzt, welches folgende Anforderungen erfüllt bzw. die Erreichung folgender Ziele ermöglicht:

- (i) Auftraggeber und Auftragnehmer vereinbaren zur Koordination ihrer Zusammenarbeit und zur Steuerung des Auftragnehmers die Einrichtung einer Struktur mit drei verschiedenen, hierarchisch angeordneten Ebenen der Zusammenarbeit (strategisch, taktisch und operativ) mit folgenden Schwerpunkten:
  1. Auf der strategischen Ebene stehen die Durchsetzung von strategischen Zielen und die Schaffung von Werten im Vordergrund.
  2. Auf der taktischen Ebene stehen das Management der Dienstleistungsbeziehung zwischen den Vertragsparteien und das Management der Services\* im Vordergrund.

3. Auf der operativen Ebene stehen die Lieferung und die Unterstützung von Services\* durch den Auftragnehmer im Vordergrund.
- (ii) Auftraggeber und Auftragnehmer werden zu Vertragsbeginn für jede Ebene der Zusammenarbeit Gremien in Form von Boards und Meetings sowie Rollen und Verantwortlichkeiten festlegen. Dies umfasst mindestens die Einrichtung eines gemeinsamen Executive Steering Boards auf strategischer Ebene, eines gemeinsamen Governance- und Architekturboards auf taktischer Ebene und eines gemeinsamen Service- und Betriebsreview-Boards auf operativer Ebene mit jeweils definierten Rollen, festgelegten Teilnehmern und regelmäßigen Sitzungen.
  - (iii) Soweit einzelne Zuständigkeiten nicht ausschließlich einem anderen Gremium zugewiesen sind, sind die Kontaktpersonen auf der operativen Ebene die zentralen Ansprechpartner für alle Themen, die den Vertrag\* betreffen.
  - (iv) Der Auftraggeber und der Auftragnehmer stellen für die Dauer der Zusammenarbeit kontinuierlich jeweils ein eigenes Team für die Zusammenarbeit bereit und besetzen die einzelnen, unter den vorstehenden Ziffern beschriebenen, Gremien mit fachlich geeigneten und autorisierten Mitarbeitern. Die Parteien werden darauf achten, dass die jeweilige personelle Besetzung möglichst für die gesamte Dauer der vereinbarten Vertragslaufzeit Bestand hat und nur aus wichtigem Grund verändert wird. Sie verpflichten sich in diesem Zusammenhang zudem, bereits vor Aufnahme der vertragsgegenständlichen Leistungserbringung die zuständigen Mitarbeiter sowie deren jeweilige Stellvertreter namentlich zu benennen. Bei Änderungen der Verantwortlichkeiten werden die Parteien einander unverzüglich darüber informieren und sicherstellen, dass eine inhaltliche Übergabe die weitere Zusammenarbeit unterbrechungsfrei ermöglicht.
  - (v) Der Auftragnehmer stellt einen dedizierten Ansprechpartner zur Verfügung, welcher entsprechendes Know-How für das Unternehmen des Auftraggebers mitbringt und Incidents effizient und ohne redundante Einarbeitungsaufwände bearbeitet (vergleichbar mit einem Technical Account Manager).

## **2.14 Anforderungen an die Vertragsbeendigung**

### **(a) Allgemeine Anforderungen**

- (i) Der Auftragnehmer wird im Zusammenhang mit der Planung und Durchführung der Überleitung der Leistungen auf einen/mehrere Nachfolgedienstleister jegliche zumutbare Unterstützung erbringen, die von der Deutschen Bundesbank angefordert wird (insgesamt „Exit-Unterstützungsleistungen“). Der Auftragnehmer verpflichtet sich zu aktiver und professioneller Zusammenarbeit mit der Deutschen Bundesbank sowie dem bzw. den (möglichen) Nachfolgedienstleister(n).
- (ii) Die Überleitung ist so auszuführen, dass (i) etwa damit verbundene operationelle Risiken so weit wie möglich ausgeschlossen oder minimiert werden, (ii) die Qualität der überzuleitenden Leistungen vor und nach dem Überleitungszeitpunkt unbeeinträchtigt bleibt und (iii) die Deutsche Bundesbank bzw. der/die Nachfolgedienstleister in der Lage ist/sind, die überzuleitenden Leistungen ab dem Überleitungszeitpunkt in einem stabilen Zustand zu übernehmen.

- (iii) Der Auftragnehmer erbringt die Exit-Unterstützungsleistungen unabhängig vom Grund der Vertragsbeendigung. Dies gilt auch im Fall einer Kündigung aus wichtigem Grund durch den Auftragnehmer.
- (iv) Exit-Unterstützungsleistungen können in mehreren nachfolgenden Schritten erbracht werden.

**(b) Einzelne Unterstützungsleistungen**

Die vom Auftragnehmer zu erbringenden Exit-Unterstützungsleistungen umfassen, je nach Anforderung der Deutschen Bundesbank, insbesondere das Folgende:

- (i) Der Auftragnehmer wird alle Daten\* und Informationen (einschließlich etwaiger Datenumwandlungen und Interface Spezifikationen) bereitstellen, die für die Planung und die Durchführung der Überleitungsleistung erforderlich sind;
- (ii) Der Auftragnehmer führt einen Wissenstransfer zur Erlangung eines tiefgreifenden Verständnisses der überzuleitenden Leistungen durch;
- (iii) Zum Überleitungszeitpunkt wird der Auftragnehmer der Deutschen Bundesbank und, soweit von der Deutschen Bundesbank gewünscht, dem/den Nachfolgedienstleister(n) sämtliche der Deutschen Bundesbank zustehenden Daten\*, soweit diese nicht bereits in geeigneter Form in Systeme der Deutschen Bundesbank oder eines Nachfolgedienstleisters überspielt worden sind, in einem vereinbarten oder – wenn nichts vereinbart wurde – in einem marktüblichen Format zur Verfügung stellen, das es der Deutschen Bundesbank und dem/den Nachfolgedienstleistern ermöglicht, die Daten\* der Deutschen Bundesbank in ein marktgängiges System zu übertragen.
- (iv) Weitere Einzelheiten im Zusammenhang mit dem Exit Management ergeben sich aus D04.4-II „Anhang 5.4 (*Exitmanagement*)“.

**(c) Vergütung**

- (i) Der Auftragnehmer ist berechtigt, für die von ihm zu erbringenden Exit-Unterstützungsleistungen eine gesonderte Vergütung zu verlangen, soweit es sich um Leistungen handelt, die
  1. durch den Auftragnehmer nach dem Zeitpunkt erbracht werden, in dem die Bundesbank dem Auftragnehmer förmlich mitgeteilt hat, dass er die endenden Leistungen auf einen oder mehrere Nachfolgedienstleister überleiten wird;
  2. Projektcharakter haben und die vom Auftragnehmer nicht bereits als Teil der laufenden vertraglich geschuldeten Leistungen zu erbringen sind.
- (ii) Soweit der Auftragnehmer für die Exit-Unterstützungsleistungen eine gesonderte Vergütung verlangen kann, bedarf dies einer separaten Beauftragung durch die Deutsche Bundesbank.