

# Anlage 1 zum EVB-IT Dienstvertrag 26-2000077114

---

## Leistungsbeschreibung

Externe Unterstützungsleistungen  
für den Betrieb und die Weiterentwicklung von NExt

## Inhaltsverzeichnis

<b>1</b>	<b>Auftragsbeschreibung.....</b>	<b>5</b>
<b>2</b>	<b>Technisches Umfeld.....</b>	<b>7</b>
<b>3</b>	<b>Leistungsorte /-zeiten.....</b>	<b>8</b>
<b>3.1</b>	<b>Leistungsort.....</b>	<b>8</b>
<b>3.2</b>	<b>Arbeiten an den IT-Systemen sowie in den Räumlichkeiten des Auftraggebers .....</b>	<b>9</b>
<b>4</b>	<b>Datenschutz, Geheimhaltung und Sicherheit.....</b>	<b>9</b>
<b>4.1</b>	<b>Personenbezogene Daten.....</b>	<b>9</b>
<b>5</b>	<b>Aufgabenschwerpunkte.....</b>	<b>9</b>
<b>5.1</b>	<b>Allgemeine Einordnung.....</b>	<b>9</b>
<b>5.2</b>	<b>Initiale Einweisung und Übergabe von Arbeitspaketen.....</b>	<b>12</b>
<b>5.3</b>	<b>Entwicklungsprozess und DevSecOps Engineering.....</b>	<b>12</b>
<b>5.4</b>	<b>Betriebsführung und-überwachung (Monitoring, Technical Event- Management).....</b>	<b>13</b>
<b>5.5</b>	<b>Anforderungs- und Change-Management.....</b>	<b>13</b>
<b>5.6</b>	<b>Release-Management.....</b>	<b>14</b>
<b>5.7</b>	<b>Incident-Management.....</b>	<b>15</b>
<b>5.7.1</b>	<b>Incident Reaktionszeiten.....</b>	<b>17</b>
<b>5.7.2</b>	<b>Incident Lösungszeiten.....</b>	<b>17</b>
<b>5.8</b>	<b>Problem-Management.....</b>	<b>18</b>
<b>5.9</b>	<b>Backup-, Restore- und Disaster-Recovery-Management.....</b>	<b>18</b>
<b>5.10</b>	<b>Schwachstellen- und Patch-Management.....</b>	<b>19</b>
<b>5.11</b>	<b>Exit-Management - Bestimmungen für den Fall einer Vertragsbeendigung....</b>	<b>19</b>
<b>5.11.1</b>	<b>Einleitung und Gegenstand.....</b>	<b>19</b>
<b>5.11.2</b>	<b>Herausgabe von Unterlagen und Daten.....</b>	<b>20</b>
<b>5.11.3</b>	<b>Rückgabe von Hard- und Software.....</b>	<b>20</b>
<b>5.11.4</b>	<b>Leistungszeitraum der Anlage Exit Management und Sonderbestimmungen.....</b>	<b>20</b>
<b>5.11.5</b>	<b>Mitwirkungspflichten bei der Migration.....</b>	<b>20</b>
<b>5.12</b>	<b>Weitere Bestimmungen bei Beendigung des Vertrages.....</b>	<b>21</b>
<b>6</b>	<b>Zusammenarbeit &amp; Governance.....</b>	<b>22</b>
<b>6.1</b>	<b>Berichtswesen.....</b>	<b>22</b>
<b>6.2</b>	<b>Planung des Arbeitseinsatzes.....</b>	<b>22</b>
<b>6.3</b>	<b>Finanzcontrolling.....</b>	<b>23</b>
<b>6.4</b>	<b>Steuerungsmeeting.....</b>	<b>23</b>

6.5	Eskalationsprozess .....	23
7	Anforderungen an die durch den Auftragnehmer eingesetzten Personen zur Unterstützung .....	24
7.1	Allgemeine Anforderungen .....	24
7.2	Austausch von Personen zur Leistungserfüllung .....	26
7.3	Infrastruktur-Architekt (A-Kriterien) .....	27
7.4	Anwendungs-Architekt (A-Kriterien) .....	29
7.5	Entwicklungsexperte mit Schwerpunkt Backend (A-Kriterien) .....	31
7.6	Entwicklungsexperte mit Schwerpunkt Frontend (A-Kriterien) .....	32
7.7	Entwicklungsexperte mit Schwerpunkt Cloud-Engineering (A-Kriterien) .....	33
7.8	Tester / Testautomatisierungs-Engineer (A-Kriterien) .....	34
7.9	Application Security Engineer / Security Champion (A-Kriterien) .....	35

Begriffsdefinition:

<b>Begriff</b>	<b>Bedeutung</b>
Erfahrungen	mindestens praktische Tätigkeit nach Ausbildungsabschluss mit in dem jeweiligen Aufgabenumfeld erforderlichen Skills
Praktische Erfahrungen	mindestens einjährige Tätigkeit mit in dem jeweiligen Aufgabenumfeld erforderlichen Skills
Umfangreiche praktische Erfahrungen	mindestens dreijährige praktische Tätigkeit mit in dem jeweiligen Aufgabenumfeld erforderlichen Skills, auch in komplexen Anwendungsfällen
Profunde praktische Erfahrungen	mindestens fünfjährige Tätigkeit mit in dem jeweiligen Aufgabenumfeld erforderlichen Skills, auch in sehr komplexen Anwendungsfällen
Kenntnisse	hat bereits theoretische Kenntnisse in den Techniken und Methoden erworben
Sehr gute Kenntnisse sowie sicherer Umgang mit Techniken, Methoden und Tools	hat sehr gute theoretische Kenntnisse in den Techniken und Methoden sowie bereits praktische Erfahrungen im sicheren Umgang mit den Techniken, Methoden und Tools

## **1            Auftragsbeschreibung**

Die Deutsche Bundesbank beabsichtigt eine Rahmenvereinbarung mit bis zu drei Auftragnehmern über konzeptionelle, implementierende, pflegende und beratende Leistungen im Umfeld der Weiterentwicklung und des technischen Betriebs ihres bereits bestehenden NExt-Portals abzuschließen. Das Portal weist eine erhebliche Größe sowie eine hohe Komplexität auf und ist ein zentrales System für viele Fachbereiche sowie deren Geschäftsprozesse.

Die ausgeschriebenen Leistungen umfassen insbesondere die Bereiche Cloud-native Software-Entwicklung, Cloud-Engineering für Cloud Services sowie Cloud Infrastrukturen als auch deren Betrieb, die aktuell in der Bundesbank Landing Zone, innerhalb der Azure Cloud, betrieben werden. Ziel ist es, Aufgaben in der Wartung, Weiterentwicklung und im Betrieb der Plattform NExt an einen externen Dienstleister zu vergeben.

Um einen reibungslosen Betrieb, die nahtlose Weiterentwicklung sowie die technische Integrität zum bisherigen Entwicklungsfortschritt von NExt zu gewährleisten, wird eine ausgeprägte Expertise sowie langjährige Erfahrung in den o.g. Bereichen als notwendiges Skill-Set erachtet.

Das NExt-Produkt wird derzeit in einem agilen und SCRUM-nahen Setup entwickelt mit vierzehntägigen Sprints, die flexibel in der Umfangdefinition sind. Die Entwicklung ist nach DevSecOps ausgerichtet. Gemäß des „DevSecOps“ Ansatzes sind die Mitarbeiter für die Entwicklung als auch für den (Sicherheits-)Betrieb einzusetzen, um so die notwendige Qualität und Effizienz zu liefern. Die eingesetzten Mitarbeiter des externen Dienstleisters, mit den im Verlauf genannten Profilen, bilden den wesentlichen Teil des Entwicklungsteams und unterliegen der fachlichen Führung der Produktverantwortlichen Stelle der Bundesbank, insb. strategisch vertreten durch den Systemeigner, operativ durch den Product Owner und den (Cloud) Solution Architect.

Die Leistungserbringung erfolgt unter Anwendung der folgenden, integralen Prozesse des Entwicklungs- und Betriebsmodells:

- Entwicklungsprozess im Sinne des DevSecOps-Engineerings
- Betriebsführung und -überwachung (Monitoring, Technical Event-Management)
- Anforderungs- und Change-Management

## Anlage 1 zum EVB-IT Dienstvertrag 26-2000077114

- Release-Management
- Incident-Management
- Problem-Management
- Backup-, Restore- und Disaster-Recovery-Management
- Schwachstellen- und Patch-Management

Ein zentrales Element der Zusammenarbeit ist die kontinuierliche Verbesserung der erbrachten Leistungen. Dies wird durch regelmäßige Retrospektiven und die Analyse von „Lessons Learned“ sichergestellt. Alle involvierten Mitarbeiter werden in diesen Prozess eingebunden, um Feedback zu sammeln, Optimierungspotenziale zu identifizieren und umzusetzen.

Die detaillierte Ausgestaltung der genannten Prozesse, einschließlich konkreter Tätigkeiten, Ergebnisse und Verantwortlichkeiten, wird in den nachfolgenden Kapiteln beschrieben.

Einen Überblick über alle beteiligten Produktbeteiligten, aufgeteilt nach interner und externer Besetzung, gibt die unten aufgeführte Darstellung. Geringfügige Anpassungen sind auch während des Produkt Life Cycles möglich.

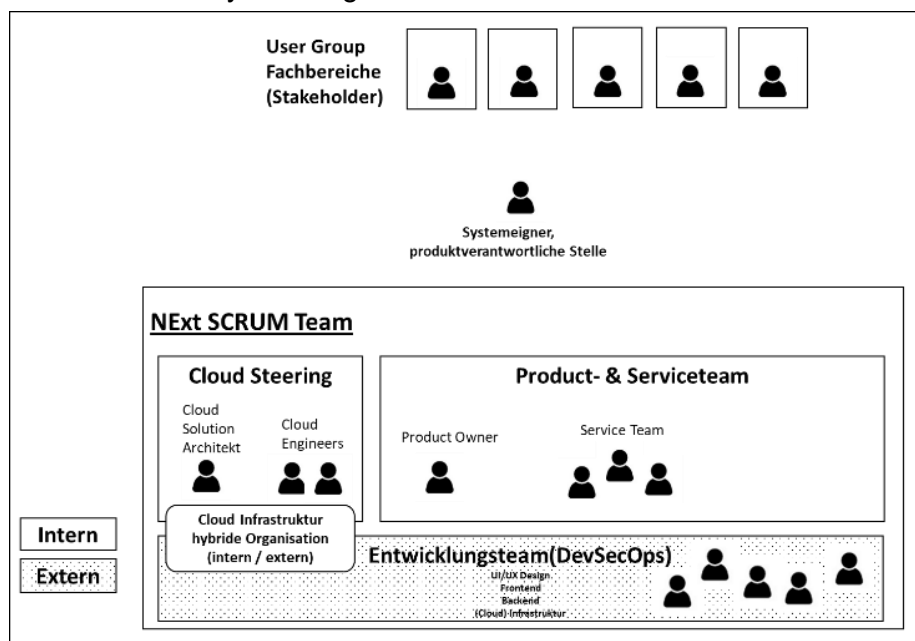


Abbildung 1 Darstellung NNext (Team) Organisation

## 2 Technisches Umfeld

Die im Folgenden aufgeführten technologischen-Komponenten befinden sich aktuell in den Bereichen der NExt-Entwicklung im Einsatz.

Aufgabenumfeld	Technologische Komponenten
<b>Betriebssystem</b>	<ul style="list-style-type: none"> <li>• Linux-basierte Container</li> </ul>
<b>Container-Plattform</b>	<ul style="list-style-type: none"> <li>• Azure Kubernetes Service</li> </ul>
<b>Cloud-Hyperscaler</b>	<ul style="list-style-type: none"> <li>• Microsoft Azure</li> </ul>
<b>IDE</b>	<ul style="list-style-type: none"> <li>• IntelliJ, Visual Studio Code</li> </ul>
<b>Fertigungsstraße</b>	<ul style="list-style-type: none"> <li>• Azure Pipelines</li> <li>• Azure DevOps</li> <li>• Git Repos Azure/Gitlab</li> <li>• CloudAdminVC</li> <li>• ArgoCD</li> <li>• Sonarqube</li> <li>• Azure Container Registry</li> <li>• Terraform</li> </ul>
<b>Frameworks</b>	<ul style="list-style-type: none"> <li>• Quarkus (Backend)</li> <li>• Angular (Frontend)</li> <li>• Typescript (Frontend)</li> <li>• OIDC / OAuth</li> </ul>
<b>Services</b>	<ul style="list-style-type: none"> <li>• Azure Blob Storage, File Storage</li> <li>• Azure MS SQL MI</li> <li>• Postgres Azure Key Vault</li> <li>• Azure Event Hub, Event Grid</li> <li>• Azure Application Gateway</li> <li>• Azure Key Vault</li> <li>• API Gateway Apigee</li> <li>• Microsoft Defender for Storage, Defender for Cloud</li> </ul>
<b>Middleware-Komponenten</b>	<ul style="list-style-type: none"> <li>• Representational State Transfer (REST) APIs</li> </ul>
<b>Logging/Monitoring</b>	<ul style="list-style-type: none"> <li>• Grafana</li> <li>• Prometheus</li> <li>• Loki</li> <li>• Dynatrace</li> <li>• Azure Monitor</li> </ul>
<b>IT-Sicherheit</b>	<ul style="list-style-type: none"> <li>• BSI-Grundschatz</li> </ul>
<b>Web-Entwicklung</b>	<ul style="list-style-type: none"> <li>• SAST, DAST, SCA, CNAPP, Container Scanning</li> </ul>
<b>Tools</b>	<ul style="list-style-type: none"> <li>• Jira</li> <li>• Confluence</li> <li>• Azure Portal</li> <li>• Cloud Admin VC</li> <li>• Virtuelle Clients</li> <li>• NExt Portal</li> <li>• Kubernetes Dashboard</li> </ul>

NExT ist derzeit in der Bundesbank Landing Zone innerhalb der Azure Cloud platziert und ist größtenteils ohne architekturelle Abhängigkeiten und damit ohne „Lock In-Effekte“ in Richtung Microsoft Azure aufgesetzt. Es sollen weiterhin kontinuierlich State-of-the-Art Technologien genutzt werden. Dabei sind präferiert nicht-proprietäre Services zu nutzen und es soll immer auf größtmögliche Portabilität geachtet werden.

Dieser Rahmen ist weiterzuverfolgen, wobei eine Migration auf eine andere Cloud Plattform (Public / Private) oder in das eigene Rechenzentrum der Bundesbank bei Bedarf durchzuführen ist.

Zur Integration in das Bundesbank Rechenzentrum („Private Cloud“) werden darüber hinaus zukünftig ggf. weitere Technologien genutzt.

### **3 Leistungsorte /-zeiten**

#### **3.1 Leistungsort**

Der Einsatzort wird sich am Standort der Auftraggeberin in Frankfurt am Main befinden. Aufgrund der standortübergreifenden Teamzusammensetzung kann ein großer Teil der Leistung ohne Anwesenheit in den Räumlichkeiten der Bundesbank erbracht werden. Hierfür werden Videokonferenzen genutzt (z.B. WebEx). Ein Team-Raum, insbesondere für Projektabstimmungen, befindet sich am Standort der Auftraggeberin in Frankfurt am Main. Alle konzeptionellen und technischen Unterstützungsleistungen können ohne Einschränkung remote bzw. an einem vom Auftragnehmer benannten Standort innerhalb der EU erbracht werden. Mehr-tägige Workshops zum Beispiel für das Onboarding des Auftragsnehmers oder den Wissenstransfer an die internen Mitarbeiter werden nach Absprache in Präsenz stattfinden. Eine kurzfristige Anwesenheit vor Ort, zum Beispiel im Falle von schwerwiegenden andauernden Störungen oder ähnlichen Situationen kann eingefordert werden.

Grundvoraussetzung ist die Bereitstellung der technischen und organisatorischen Zugangsmöglichkeiten, die mit Ausnahme von On-Premise-Komponenten (diese sind in der Verantwortung der Bundesbank und von dieser ggfs. bereitzustellen) wesentlicher Bestandteil der Leistung des Auftragnehmers ist.

Die geforderten Leistungen sowie alle wesentlichen Informationen, die zur Bearbeitung notwendig sind, werden dem Auftragnehmer in Videokonferenzen und vor Ort in Frankfurt am Main übermittelt. Zudem ist die Kommunikation über E-Mail möglich.



### **3.2 Arbeiten an den IT-Systemen sowie in den Räumlichkeiten des Auftraggebers**

Da die Leistungserbringung grundsätzlich an den IT-Systemen (Infrastruktur oder Anwendungen) des Auftraggebers erbracht werden müssen, können diese aus sicherheitsspezifischen sowie technischen Gründen auch nur mit Hardware / Systemzugängen des Auftraggebers erbracht werden. Regelmäßig sind die Zugriffe mit einem Remote-Zugang möglich.

Die hierfür benötigten Zugriffe können im Falle von Vor-Ort-Leistungen nur an den in der Anforderung benannten Standorten, in der Regel zwischen 06:00 und 20:00 Uhr, ermöglicht werden. Im Zuge der konkreten Leistungs-/Arbeitspakete werden dem Auftragnehmer die möglichen Zutrittszeiten zu den Gebäuden des Auftraggebers mitgeteilt.

## **4 Datenschutz, Geheimhaltung und Sicherheit**

### **4.1 Personenbezogene Daten**

Der Auftragnehmer greift auf personenbezogene Daten ausschließlich insoweit zu, wie dies zur Durchführung der in dieser Leistungsbeschreibung beschriebenen Leistungen erforderlich ist. Die Verarbeitung erfolgt im Übrigen gemäß den Regelungen des Auftragsvertrags, s. D4\_Anlage\_7\_zum\_EVB-IT Dienstvertrag\_AV\_26-2000077114.

## **5 Aufgabenschwerpunkte**

### **5.1 Allgemeine Einordnung**

Die Aufgabenschwerpunkte unterteilen sich im wesentlichen auf Unterstützungsleistungen in der Anwendungsentwicklung und des -betriebs.

Grundsätzlich liegen bei der Bundesbank - der produktverantwortlichen Stelle - die Steuerung und Verantwortung für die Anwendungen, notwendige Leistungen im Rahmen der Anwendungsentwicklung und Betrieb der Anwendung gehen auf den Provider über.

Zusätzlich kann die Bearbeitung von zugehörigen Grundsatzthemen erforderlich sein, die der IT-Einheit im Auftrag von zentralen IT-Gremien und IT-Arbeitsgruppen obliegt.

Für den Betrieb und die Weiterentwicklung von NExt sind hochwertige Beratungs-, Implementierungs- und Unterstützungsleistungen notwendig.

Beschreibung der Dienstleistung (nicht abschließend)

## Anlage 1 zum EVB-IT Dienstvertrag 26-2000077114 \_\_\_\_\_

- IT-spezifische Beratung beinhaltet Digitalisierungsexpertise in fachlichen und technischen Themenstellungen, insbesondere bei Fragestellungen in den Bereichen IT-Architektur, IT-Sicherheit, IT-Anwendungsentwicklung, IT-Infrastruktur, Cloud, Bereitstellungs-Szenarien
- Analyse und Sichtung der vorliegenden technischen und fachlichen Anforderungen auf Basis folgender grundlegender Quellen (Baseline):
  - Aktuelles Product Backlog
  - Nicht-funktionale Anforderungen aus der Bundesbank IT
- Bereitstellung, Entwicklung und Konfiguration des zugehörigen Technologie-Stacks (inkl. Middleware, Services, Entwicklungsframeworks, Testtools) bzgl. der vorhandenen Anwendungsbestandteile und des entwickelten Anwendungscodes
- Weiterentwicklung und Bereitstellung der Kernanwendung einschließlich Frontend- und Backend-Entwicklung sowie Cloud-Engineering, basierend auf den fachlichen und technischen Anforderungen
- Ausbau der technischen Integration des externen Cloud-Providers und der Anwendung in die IT-Sicherheits- und Netzwerkinfrastruktur der Bank
- Umsetzung und Evaluierung weiterer technischer und fachlicher Services (z.B. Einbindung interaktive Anwendungen, Portaltechnologie, Archivierungtool)
- Unterstützung bei der Evaluierung von konkreten Software-Produkten (Beispiel: Open Source Monitoring- oder Automatisierungstools, Entwicklungswerkzeuge oder Cloud-Services) sowie kontinuierliche Verbesserung der eingesetzten Software-Produkten oder Technologien
- Sicherstellung der Qualitätsmerkmale der Anwendung gemäß ISO/IEC 25010 (Funktionalität, Leistungseffizienz, Kompatibilität, Benutzbarkeit, Zuverlässigkeit, Sicherheit, Wartbarkeit, Übertragbarkeit)
- Technische Betreuung/Betrieb, Fehlerbehebung und Weiterentwicklung u. a. auf Basis der Tests mit internen und externen Kunden und in Abstimmung mit der produktverantwortlichen Stelle der Bundesbank
- Vollständige Dokumentation des Technologie-Stacks, der technischen Konfiguration, der betrieblichen und IT-sicherheitsrelevanten Einstellungen und Aufgaben und eingesetzten Komponenten und Optimierungsschritte
- Dokumentation aller Tätigkeiten (u. a. Design, Entwicklung, Tests), damit diese ggf. übernommen und weiterentwickelt werden können
- Die Erarbeitung und Umsetzung von Maßnahmen zur Sicherstellung eines zukunftssicheren und stabilen Betriebs der Plattform

## **Anlage 1 zum EVB-IT Dienstvertrag 26-2000077114**

Der Auftragnehmer ist verpflichtet, einen kontinuierlichen Know-how-Transfer an die Mitarbeiter der Deutschen Bundesbank, insb. in der Rolle der „(Cloud/Infrastruktur) Engineer“, sicherzustellen. Dies umfasst insbesondere:

- Einarbeitung von Mitarbeitern in die eingesetzten Technologien, Prozesse und Tools,
- Durchführung regelmäßiger Wissensworkshops
- Bereitstellung von Best-Practice-Dokumenten
- Pairing-/Shadowing-Ansätze im Rahmen der täglichen Arbeit
- Durchführung von Code Reviews

Der Betrieb und die Weiterentwicklung sind in produktneutraler und qualitativ hochwertiger Weise zu erbringen. Die Entwicklung und Implementierung mit Hilfe der Scrum-Prozesse (z.B. Sprints) ist eine Grundvoraussetzung der Zusammenarbeit.

Insgesamt lassen sich die Aufgabenschwerpunkte nach dem in der Bundesbank vorhandenen Application-Lifecycle eingliedern:

- Fachliches Anwendungsdesign
  - Mitwirkung beim Anforderungsmanagement
- Technisches Anwendungsdesign
  - Mitwirkung beim Anforderungsmanagement
- Realisierung
  - Konzeption, Design und Implementierung im Rahmen der Weiter- und Neuentwicklung von Anwendungen
  - Eruierung, Bewertung und Ersteinführung von Entwicklungswerkzeugen, sofern diese benötigt werden
  - Mitwirkung beim Releasemanagement
- Abnahme
  - Qualitätssicherung, u. a. (automatisierte) Tests
- Anwendungsbetreuung
  - Incident- und Problem-Management, inklusive Ticketbearbeitung
  - Last-Level Support inkl. möglicher Rufbereitschaften
- Übergreifende Reviews und Tests
  - Qualitätssicherung inklusive Sicherheitsanforderungen, übergreifendes Qualitätsmanagement durch Reviews und (automatisierte) Tests
  - Aufbau und Ausführung Testautomatisierungen, u.a. Lasttests, Regressionstest (vor Inbetriebnahme), E2E-Tests

## 5.2 Initiale Einweisung und Übergabe von Arbeitspaketen

Die Aufnahme der Beratungs-, Konzeptionierungs-, Entwicklungs- und Umsetzungstätigkeit muss direkt im Anschluss an den Vertragsbeginn erfolgen.

Nach der Auftragserteilung wird der Auftraggeber den Auftragnehmer initial in die Anwendung oder das Projekt einweisen und so dass eine selbständige Einarbeitung durch den Auftragnehmer möglich ist. Der Auftragnehmer ist berechtigt, den Zeitraum der Einweisung für die tatsächliche Anzahl an benötigten Personen in Rechnung zu stellen.

## 5.3 Entwicklungsprozess und DevSecOps Engineering

Ein wesentlicher Teil des Entwicklungsprozesses ist das Engineering im DevSecOps-Team. Das DevSecOps-Team arbeitet als **integriertes Engineering-Team** aus internen Mitarbeitenden der Bundesbank und externen Mitarbeitenden des Auftragnehmers. Alle Engineers übernehmen **gemeinsame Verantwortung für Qualität, Sicherheit und Betrieb** der Software- und Plattformkomponenten über den gesamten Lebenszyklus.

Die Zusammenarbeit erfolgt derzeit angelehnt an **Scrum**. Aufgaben werden über gemeinsame Backlogs gesteuert und anhand definierter Qualitäts- und Engineering-Standards der Bundesbank umgesetzt.

Die Softwareentwicklung erfolgt auf Basis eines **durchgängigen CI/CD-basierten Entwicklungsprozesses**. Änderungen werden versioniert entwickelt, automatisiert gebaut, getestet und über standardisierte Pipelines bereitgestellt. Qualität, Sicherheit und Nachvollziehbarkeit werden dabei frühzeitig und kontinuierlich durch automatisierte Prüfungen (z. B. Tests, Code- und Security-Scans) sichergestellt. Deployments sind reproduzierbar, weitgehend automatisiert und folgen dem definierten Releaseprozess.

DevSecOps-Aufgaben werden als integraler Bestandteil der Entwicklungsarbeit verstanden. Ein wesentlicher Bestandteil der Leistung ist der **gezielte Know-how-Transfer**. Dieser erfolgt praxisnah im Arbeitsalltag, z. B. durch Pair Programming, gemeinsame Code-Reviews, technische Dokumentation sowie gezielte Wissenssessions. Ziel ist der nachhaltige Aufbau von DevSecOps-, Betriebs- und Qualitätskompetenzen innerhalb der Bundesbank.

Mit dieser Arbeitsweise ist das DevSecOps Team entsprechend seines Know Hows und der übertragenen Aufgaben in die im Folgenden beschriebenen Prozesse eingebunden

Der Auftragnehmer verpflichtet sich (ohne eine Anpassung des Vertrages) hinsichtlich der oben genannten technologischen Komponenten (Kapitel 2) während der Vertragslaufzeit die Unterstützung auch für Nachfolgeprodukte sicherzustellen sowie den Einsatz neuer Technologien, Frameworks und Tools im NExt-Umfeld durch Beratung und Umsetzung aktiv zu unterstützen. Der Auftragnehmer wird rechtzeitig von der Bundesbank über mögliche Nachfolgeprodukte (bspw. im Fall von Dekommissionierung oder Entscheidung für eine notwendige

Serviceportfolioerweiterung vergleichbar „Loki“) informiert. Ferner stellt der Auftragnehmer sicher, dass jeweils die neuen Produktversionen (bspw. neue Quarkusversion 3.32.x) zeitnah umgesetzt werden, um eine sichere moderne Applikationsarchitektur kontinuierlich zu gewährleisten.

#### **5.4 Betriebsführung und -überwachung (Monitoring, Technical Event-Management)**

Die Betriebsführung und -überwachung erfolgt kontinuierlich und integriert in die DevSecOps-Arbeitsweise. Zentrale Grundlage ist ein **systematisches Monitoring** der Anwendungen und Plattformkomponenten, das relevante technische Metriken, Logs und Zustände erfasst. Ziel ist die frühzeitige Erkennung von Abweichungen, Degradationen oder Fehlentwicklungen, bevor diese zu Incidents führen.

Erkannte **technische Ereignisse (Technical Events)** werden nachvollziehbar erfasst, priorisiert und primär durch das Engineering-Team analysiert und bearbeitet. Dies umfasst insbesondere Performance- und Stabilitätsabweichungen, Ressourcenengpässe, fehlerhafte Konfigurationen, Sicherheitsauffälligkeiten sowie Hinweise aus Logs oder Traces. Die Bearbeitung erfolgt engineering-nah und möglichst zeitnah, einschließlich Ursachenanalyse und nachhaltiger Behebung. Die Bewertung und Priorisierung der sich ergebenden Changes – insbesondere solcher mit erheblicher fachlicher oder technischer Auswirkung bzw. erhöhtem Umsetzungsaufwand – erfolgt ausschließlich durch die hierfür zuständigen Rollen der Deutschen Bundesbank, insbesondere die Cloud Engineers sowie die steuernden Rollen (z. B. Cloud Solution Architect und Product Owner). Monitoring und Event-Management sind eng mit Entwicklungs- und CI/CD-Prozessen verzahnt. Erkenntnisse aus technischen Ereignissen fließen systematisch in Backlog, Architektur- und Qualitätsmaßnahmen ein (z. B. Anpassung von Tests, Pipelines, Konfigurationen oder Monitoring-Regeln). Ziel ist ein **stabiler, transparenter und nachvollziehbarer Betrieb** mit klarer Verantwortung des DevSecOps-Teams für technische Qualität und Betriebsreife.

#### **5.5 Anforderungs- und Change-Management**

Ziel des Anforderungs- und Change-Request-Managements ist es, fachliche und technische Anforderungen sowie Änderungswünsche strukturiert, transparent und nachvollziehbar zu erfassen, zu bewerten, zu priorisieren und umzusetzen. Das Anforderungs- und Change-Management erfolgt auf Basis agiler Methoden und ist eng in den SCRUM-Prozess integriert. Anforderungen sowie Changes werden flexibel und bedarfsorientiert im Rahmen der laufenden SCRUM-Sprints initiiert, typischerweise als User Stories oder Tasks im Product Backlog. Die Priorisierung und Bewertung der eingereichten Anforderungen sowie Changes erfolgt gemeinsam durch Mitarbeiter des Auftragnehmers sowie Vertretern der Bundesbank, primär den Product Owner oder Cloud Solution Architect, im Zuge von Sprint Plannings aber auch auf adhoc Basis bzw. bei notwendigen Anpassungen („Change Requests“).

Die Umsetzung der Changes erfolgt überwiegend durch Ressourcen des Auftragnehmers, die eng mit den internen Cloud Engineers, wo notwendig, zusammenarbeiten. Alle Changes werden Bundesbank-Ticketsystem dokumentiert (u.a. JIRA-Ticket, Confluence oder Ticket-system - zurzeit Service Manager) und nachverfolgt bis zur Abnahme durch die Bundesbank, insbesondere vertreten durch den Product Owner.

Es finden regelmäßige Abstimmungen (z. B. Dailys / Statusmeetings) zwischen internen und externen Mitarbeitern zu den Changes statt, sowie Präsentation der Change Ergebnisse (u. a. Sprint Reviews). Die kontinuierliche Verbesserung des Anforderungs- und Change-Management Prozesses wird durch regelmäßige Reviews und Lessons Learned sichergestellt.

## **5.6 Release-Management**

Die Planung und Durchführung eines Releases beinhalten typischerweise Aktivitäten wie die Definition des Funktionsumfangs, die Priorisierung von Anforderungen, die Entwicklung, Tests und Validierung der Änderungen sowie die Vorbereitung der Produktionsumgebung für die Bereitstellung des Releases. Das Releasemanagement, in der Verantwortung des NExt-Service-Teams der Bundesbank, stimmt dabei mit allen beteiligten Parteien die zeitliche Planung für mögliche Release- und Deployment-Phasen ab. Die gemeinsame Releaseplanung soll insgesamt die Verfügbarkeit der internen und externen Mitarbeiter als auch der technischen Ressourcen sicherstellen.

Das Release-Management steuert die Planung, Vorbereitung und Durchführung von Releases über mehrere Umgebungen hinweg: Entwicklungsumgebung (DEV), Qualitätssicherungsumgebung (QA), Abnahmeumgebung (AT) und Produktionsumgebung (PRD). Die Nutzung der Umgebungen für Test- und Abnahmezwecke erfolgt in Abstimmung mit der Bundesbank, vertreten durch das NExt-Service-Team oder dem Product Owner. Dabei ist durch die Bundesbank sicherzustellen, dass die Umgebungen adäquat genutzt werden können. Der Auftragnehmer verpflichtet sich zu einer kostenoptimierten Nutzung der bereitgestellten Ressourcen.

Die Release-Planung erfolgt in enger Abstimmung mit allen bei der Entwicklung involvierten Personen, um einen reibungslosen Ablauf, auch zwischen internen und externen Mitarbeitern sowie Ressourcen, sicherzustellen. Die Erstellung von Release-Paketen, die Durchführung und Dokumentation der durchzuführenden Maßnahmen sowie Tests in den jeweiligen Umgebungen sowie die Einhaltung der definierten Freigabeprozesse sind fester Bestandteil des Release-Managements. Während des Rollouts in die PRD-Umgebung werden die Systeme überwacht, um bei etwaigen Problemen schnell reagieren zu können; bei Bedarf kann ein Rollback durchgeführt werden. Diese Rollouts finden außerhalb der normalen Geschäftszeiten statt und können in Ausnahmefällen auch am Wochenende eingeplant werden.

Vor einem Release erfolgt eine umfassende Dokumentation der Maßnahmen der durchgeführten Änderungen während der letzten (Software-)Entwicklungsphase, insbesondere in Bezug auf die Software-Architektur. Die produktverantwortliche Stelle der Bundesbank, vertreten durch das NExt-Service-Team, nimmt das Release ab. Erkenntnisse aus dem Release-Prozess werden im Rahmen von Lessons Learned zur kontinuierlichen Prozessverbesserung genutzt.

### 5.7 Incident-Management

Die Bundesbank übernimmt in dieser Disziplin die koordinierende Rolle als Incident Manager, überwacht den gesamten Prozess, stellt die Einhaltung der Eskalationswege sicher und fungiert als zentrale Kommunikationsschnittstelle zwischen den Support-Stufen. Alle Incidents werden im zentralen Bundesbank-Ticketsystem dokumentiert, und die Bundesbank erstellt regelmäßige Berichte zur Prozessoptimierung und Service-Level-Monitoring. Zusätzlich erfolgt die Kommunikation immer über ein weiteres Kommunikationstool, um eine effiziente Bearbeitung der Incidents sicherzustellen. Bei der Bearbeitung des Incidents arbeiten interne und externe Mitarbeiter zusammen. Im Falle von Softwareanpassungen überträgt die Bundesbank die Änderungen in das Changemanagement. Nach Abschluss eines Incidents wird die Lösung dokumentiert, ggf. an den oder die betroffenen Nutzer kommuniziert und der Vorgang geschlossen. Kritische Fälle werden darüber hinaus ab ihrem Auftreten für zukünftige Verbesserungen aufgezeichnet und anschließend analysiert.

Die Mitarbeiter der Bundesbank übernehmen grundsätzlich die Aufgaben im First- und Second-Level-Support. Im Rahmen des First-Level-Supports erfolgt die Entgegennahme und Erfassung von Incidents, die durch Anwender gemeldet oder durch automatisiertes Monitoring erkannt werden. Die Bundesbank-Mitarbeiter führen eine Voranalyse und grundlegende Fehlerbehebung (Basic Troubleshooting) durch, um möglichst viele Störungen bereits in dieser Phase zu lösen. Dazu zählen beispielsweise die Überprüfung von Systemstatus, die Durchführung einfacher Konfigurationsänderungen oder die Bereitstellung von Informationen für die Nutzer.

Sollte eine Störung nicht im First-Level gelöst werden können, erfolgt die Weiterleitung an den Second-Level-Support, der ebenfalls durch die Bundesbank abgedeckt wird. Hier werden weiterführende Analysen und vertiefte technische Maßnahmen durchgeführt, um die Ursache des Incidents zu identifizieren und zu beheben. Die Ergebnisse und durchgeführten Schritte werden transparent dokumentiert.

Für komplexe oder produktbezogene Incidents, insbesondere im Zusammenhang mit dem Produkt NExt, wird der Last-Level-Support durch die bereits im Einsatz befindlichen Entwickler, gemäß der DevSecOps-Methode, übernommen. Die externen Mitarbeiter bringen ihre spezifische Expertise ein und sind für die tiefgehende Analyse, Fehlerbehebung und ggf. die Entwicklung von Lösungen verantwortlich.

Die Zusammenarbeit zwischen internen und externen Support-Einheiten erfolgt eng und abgestimmt, um eine schnelle Eskalation und effiziente Lösung sicherzustellen. Alle Incidents



werden in einem zentralen System dokumentiert und nachverfolgt. Erkenntnisse aus der Incident-Bearbeitung fließen in die kontinuierliche Verbesserung der Support-Prozesse und die Prävention zukünftiger Störungen ein.

Im Falle von Problemen oder Eskalationen („Major Incidents“) außerhalb der regulären Arbeitszeiten, insbesondere am Wochenende, steht ein Bundesbank-interner Manager on Duty – außerhalb vom NExt-Serviceteam- als zentrale Ansprechperson für das NExt-Serviceteam, Cloud Engineers und DevSecOps Team zur Verfügung. Dieser fungiert außerhalb der Geschäftszeiten als Eskalationsinstanz als Bindeglied zwischen den verschiedenen Abteilungen.

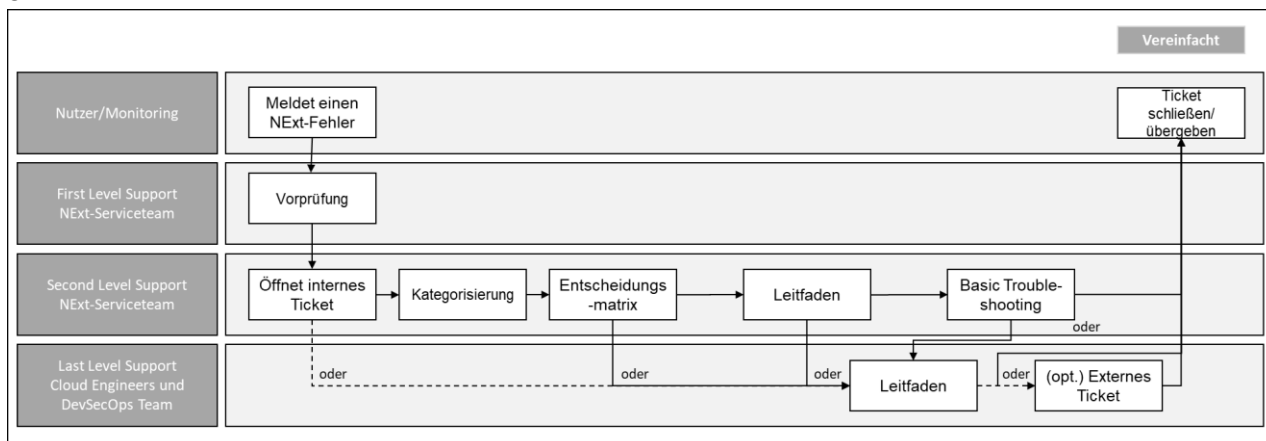


Abbildung 2: Illustration der Support-Level

### First Level Support (FLS) - Bundesbank:

Der First Level Support ist die erste Anlaufstelle für Kunden und Nutzer bei technischen oder organisatorischen Angelegenheiten und wird von dem NExt-Serviceteam und den Fachbereichen der Bundesbank vertreten. Die Hauptaufgabe des FLS besteht darin, einfache Probleme direkt zu lösen (z. B. Nutzerüberprüfungen) oder Anfragen an die zuständigen Stellen weiterzuleiten. Der Kontakt erfolgt zentral über das NExt-Serviceteam, in der Regel schriftlich per E-Mail. Interne Störungsmeldungen können zusätzlich über ein Ticketsystem eingereicht werden. Der FLS dient somit als Schnittstelle zwischen den Nutzern und den nachgelagerten Support-Ebenen.

### Second Level Support (SLS) - Bundesbank:

Der Second Level Support, ebenfalls vertreten durch das NExt-Serviceteam der Bundesbank, übernimmt komplexere technische Probleme, die vom FLS nicht gelöst werden können. Hier arbeiten Experten, die tiefergehende Analysen durchführen und Lösungen für anspruchsvollere Störungen bereitstellen. Incident-Meldungen werden über ein zentrales Ticketsystem an den SLS weitergeleitet. Der SLS agiert als Bindeglied zwischen dem FLS und dem hochspezialisierten Last Level Support.



#### Last Level Support (LLS):

Der Last Level Support ist die höchste Eskalationsstufe im Support-Prozess und wird von hochspezialisierten Fachleuten, sowohl internen Mitarbeitern (insb. Cloud Engineers), aber in erster Linie von externen Mitarbeitern, aus dem Entwicklungsteam/DevSecOps-Team durchgeführt. Diese Experten lösen tiefgehende, seltene oder kritische Probleme, die weder vom FLS noch vom SLS gelöst werden können. Außerhalb der regulären Servicezeiten werden Störungen über die zentrale Business Incident Coordination der Bundesbank gemeldet, insbesondere im Rahmen der Rufbereitschaft. Der LLS stellt sicher, dass auch in Ausnahmefällen eine Lösung gefunden wird, und arbeitet eng mit den vorangegangenen Support-Ebenen zusammen.

Im Folgenden werden die Incident-Reaktionszeiten sowie die Lösungszeiten beschrieben. Diese Zeiten dienen als Grundlage für den Betrieb und können sich im Verlauf der Zusammenarbeit aufgrund geänderter Rahmenbedingungen, technischer Entwicklungen oder betrieblicher Erfordernisse ändern. Anpassungen der Reaktions- und Lösungszeiten bedürfen in jedem Fall der vorherigen Abstimmung beider Vertragsparteien.

#### 5.7.1 Incident Reaktionszeiten

Die Incident Reaktionszeit misst die maximale Zeitspanne zwischen dem Zuweisen eines Tickets an eine Supportgruppe und der Reaktion der entsprechenden Supportgruppe (Start der Bearbeitung). Die Reaktionszeiten werden nach den Ticketprioritäten (1-4) festgelegt, wie sie zum Zeitpunkt der Erstellung des Tickets auf der Grundlage von Informationen des Benutzers im Incident-Ticket erfasst werden. Die Ticket-Priorisierung wird anhand der Auswirkung und Dringlichkeit entsprechend einer Incident Prioritätsmatrix von der Bundesbank definiert.	
Störungen während der <b>Standard</b> supportzeit:	
<b>Priorität 1</b> – Service ist vollständig nicht verfügbar und unternehmenskritisch	10 Minuten
<b>Priorität 2</b> – Service ist teilweise nicht verfügbar. Kurzfristige Wiederherstellung zwingend erforderlich. Der Geschäftsbetrieb der Bundesbank ist beeinträchtigt.	25 Minuten
<b>Priorität 3</b> – Diese Störung betrifft mehrere Anwender. Umgebungslösung ist vorhanden oder Störung liegt außerhalb der Geschäftszeiten.	2 Stunden
<b>Priorität 4</b> – Ein einzelner Benutzer ist von der Störung betroffen	6 Stunden

#### 5.7.2 Incident Lösungszeiten

Die Angaben für die Incident Lösungszeiten beziehen sich darauf, wann der Service wiederhergestellt sein muss. Die Lösungszeiten werden nach den Ticket-Prioritäten (1-4) gemäß der Incident Prioritätsmatrix festgelegt.	
Priorität 1	30 Minuten
Priorität 2	4 Stunden
Priorität 3	12 Stunden
Priorität 4	48 Stunden

## **5.8 Problem-Management**

Das Problem-Management hat das Ziel, die Ursachen wiederkehrender oder signifikanter Störungen im IT-Betrieb systematisch zu identifizieren, zu analysieren und nachhaltig zu beheben. Im Rahmen dieses Prozesses werden auftretende Incidents und Störungen zunächst durch das Incident Management erfasst und klassifiziert. Bei der Identifikation von Problemen, die auf tieferliegende Ursachen oder wiederkehrende Fehler hindeuten, erfolgt eine Übergabe an das Problem-Management. Die Analyse und Bearbeitung des Problems erfolgt in enger Zusammenarbeit zwischen dem NExt-Service-Team sowie internen Cloud-Engineers als auch externen Mitarbeitern aus dem Entwicklungsteam/DevSecOps-Team. Die Dokumentation aller identifizierten Probleme, Analysen und Maßnahmen erfolgt in einem zentralen System. Nach erfolgreicher Ursachenanalyse werden nachhaltige Lösungen (Root Cause Fixes) entwickelt und umgesetzt. Temporäre Workarounds werden dokumentiert und kommuniziert, bis eine dauerhafte Lösung implementiert ist. Die Wirksamkeit der Maßnahmen wird regelmäßig überprüft. Erkenntnisse aus dem Problem-Management fließen in die kontinuierliche Verbesserung der Prozesse ein.

Die Planung der weiteren Bearbeitung erfolgt eng verzahnt mit den agilen Arbeitsprozessen: Identifizierte Probleme werden an die steuernden Rollen des Product Owner oder dem Cloud Solution Architekt adressiert und im Folgenden eingeplant. So wird sichergestellt, dass die Ursachenbehebung zeitnah und strukturiert erfolgt.

Bei Bedarf, insbesondere bei komplexen oder ressourcenintensiven Problemen, werden externe Mitarbeiter zur Unterstützung hinzugezogen. Die weiterführende Analyse und die Einarbeitung der Problembehebung erfolgen dann in enger Abstimmung zwischen den internen und den externen Experten. Die Aufgabenverteilung richtet sich nach der jeweiligen Problemstellung und den verfügbaren Kompetenzen: Je nach Ergebnis der Analyse und der erforderlichen Maßnahmen übernehmen entweder die internen oder die externen Mitarbeiter die Lösungsumsetzung.

## **5.9 Backup-, Restore- und Disaster-Recovery-Management**

Das Backup-, Restore- und Disaster-Recovery-Management stellt die Verfügbarkeit und Integrität relevanter Daten und Systeme sicher. Regelmäßige, automatisierte Backups werden gemäß den definierten Backup-Strategien und -Zeitplänen durchgeführt und in sicheren, redundanten Speicherorten abgelegt. Die Überwachung der Backup-Jobs sowie die regelmäßige Überprüfung der Backup-Integrität sind fester Bestandteil des Prozesses. Im Bedarfsfall, beispielsweise bei Datenverlust oder Systemausfall, werden Wiederherstellungen (Restores) gemäß den abgestimmten Wiederherstellungsplänen durchgeführt. Die Restore-Prozesse werden regelmäßig getestet, um die Funktionsfähigkeit und Zuverlässigkeit sicherzustellen. Für den Fall schwerwiegender Störungen oder Katastrophen (Disaster) existieren dokumentierte und getestete Disaster-Recovery-Pläne, die eine schnelle Wiederherstellung des Betriebs ermöglichen. Die Koordination der durchzuführenden Maßnahmen erfolgt durch

Vertreter, insbesondere dem NExt-Service-Team, in enger Abstimmung zwischen internen und externen Mitarbeitern. Alle Backup-, Restore- und Disaster-Recovery-Aktivitäten werden gleichermaßen durch interne sowie externe Cloud-Engineers umfassend dokumentiert und regelmäßig im Rahmen von Audits und Reviews überprüft.

## **5.10 Schwachstellen- und Patch-Management**

Das Schwachstellen-Management dient der proaktiven Identifikation, Bewertung und Behebung von Sicherheitslücken.

Das Patch-Management dient darüber hinaus der proaktiven Aktualisierung des Systems und seiner Komponenten zur Verbesserung von Systemstabilität, Systemleistung und zu Funktionserweiterungen.

Eingangsinformationen für den Prozess sind regelmäßige automatisierten Überwachung der Systeme auf bekannte Schwachstellen und verfügbare Patches entsprechend Anforderungen durch die Bundesbank sowie die Auswertung von Herstellerinformationen und weitere benannte Quellen. Die identifizierten Schwachstellen und möglichen Updates werden primär durch das DevSecOps Team, abgestimmt mit der Bundesbank, hinsichtlich ihrer Kritikalität und Relevanz bewertet und in der Planung priorisiert. Basierend auf einer routinierten Abstimmung zwischen Bundesbank internen und externen Mitarbeitern werden die Schritte zur Behebung festgehalten und es findet eine Lösung statt, je nachdem in welcher Komponente die Schwachstelle bzw. das mögliche Updates identifiziert wurde. Die erforderlichen Patches und Updates werden geplant, getestet und zeitnah in den jeweiligen Umgebungen (DEV, QA, AT, PRD) durch interne und externe Mitarbeiter des DevSecOps-Teams ausgerollt. Die Durchführung erfolgt durch das Change-Management, um die Stabilität und Sicherheit der Systeme zu gewährleisten. Kritische Sicherheitsupdates werden im Rahmen von Notfallprozessen priorisiert behandelt. Die Umsetzung und der Status aller Patches werden zentral dokumentiert und überwacht. Erkenntnisse aus dem Schwachstellen- und Patch-Management fließen in die kontinuierliche Verbesserung der Prozesse ein.

## **5.11 Exit-Management - Bestimmungen für den Fall einer Vertragsbeendigung**

### **5.11.1 Einleitung und Gegenstand**

Nachstehende Bestimmungen werden vereinbart, um eine geregelte Überleitung / Migration der IT-Leistungen sowie einen Know-how-Transfer für den Fall einer Beendigung dieses Vertrages oder Teilleistungen dieses Vertrages auf den Auftraggeber und/oder einen hierfür beauftragten Dritten sicherzustellen. Die Bestimmungen aus dieser Anlage einschließlich weiterer einschlägiger Bestimmungen dieses Vertrages gelten, unabhängig davon aus welchem Grund dieser Vertrag – ganz oder teilweise – beendet wird, somit auch im Falle einer Kündigung aus wichtigem Grund durch eine der Vertragsparteien, über das Vertragsende hinaus.

### **5.11.2 Herausgabe von Unterlagen und Daten**

Der Auftragnehmer hat sämtliche Unterlagen und elektronisch gespeicherte Daten, die er im Zusammenhang mit der Vertragserfüllung vom Auftraggeber erhalten oder selbst erstellt hat (z. B. Betriebs- und Systemhandbücher, technische und sonstige Dokumentationen, usw.), an den Auftraggeber auf dessen Verlangen unverzüglich, bedingungslos und kostenfrei herauszugeben oder verschlüsselt online zu übertragen. Sämtliche Dokumente sind in einer lesbaren, strukturierten und verwertbaren Form zu übergeben. Die Übergabe der Daten und Unterlagen ist in einem Protokoll schriftlich festzuhalten. Die Dokumentation ist jederzeit aktuell zu halten. Die Deutsche Bundesbank ist berechtigt, Informationen (einschl. Dokumentation) dem Folgedienstleister offen zu legen, sofern dies für die Weiterentwicklung und den Betrieb des Service relevant ist.

Nach Übergabe sind alle auf den Systemen des Auftragnehmers verbliebenen, auch temporären Daten nicht wiederherstellbar zu löschen. Sie dürfen weder für geschäftliche noch rein interne Zwecke genutzt werden. Der Auftragnehmer weist die Löschung oder Vernichtung der Daten auf Anforderung durch den Auftraggeber schriftlich nach. Von dieser Regelung nicht betroffen sind Daten und Informationen, welche öffentlich und für jedermann frei zugänglich sind oder die aufgrund gesetzlicher Vorschriften einer Aufbewahrungsfrist unterliegen.

### **5.11.3 Rückgabe von Hard- und Software**

Der Auftragnehmer ist verpflichtet, ihm vom Auftraggeber im Zusammenhang mit der vertragsgegenständlichen Leistungserbringung überlassene Hard- und Software nach Beendigung des Gesamtvertrages zurückzugeben.

### **5.11.4 Leistungszeitraum der Anlage Exit Management und Sonderbestimmungen**

Der Auftragnehmer verpflichtet sich, die vertraglich vereinbarten Leistungen bzw. Tätigkeiten auf Wunsch des Auftraggebers auch nach Beendigung des Vertrages für einen Übergangszeitraum von bis zu zwölf Monaten uneingeschränkt zu erbringen, damit die Aufgaben von der Deutschen Bundesbank selbst oder von einem neuen Anbieter übernommen werden können.

### **5.11.5 Mitwirkungspflichten bei der Migration**

Der Auftragnehmer ist verpflichtet, alles zu unternehmen, was für einen geordneten Übergang der Leistungen auf den Auftraggeber oder einen neuen Anbieter erforderlich ist. Der Auftragnehmer wird mit dem neuen Anbieter im Rahmen der Migration eng zusammenarbeiten. Dies schließt auch Leistungen des Auftragnehmers wie die Vermittlung von Kenntnissen zu Systemen, Abläufen und Prozessen ein.

Der Auftragnehmer wird sicherstellen, dass während der Überleitung keine Störungen der vertragsgemäßen Leistungserbringung auftreten und der Auftraggeber oder der von ihm hierzu beauftragte Dritte in der Lage ist, die Durchführung der vertragsgegenständlichen

## **Anlage 1 zum EVB-IT Dienstvertrag 26-2000077114**\_\_\_\_\_

Leistungen aufzunehmen. Dazu ist ein entsprechender Plan für die Migration in Zusammenarbeit zwischen Auftraggeber und Auftragnehmer zu erstellen.

Dabei kann der Auftraggeber verlangen, dass der Auftragnehmer den neuen Anbieter und/oder den Auftraggeber selbst in die zu erfüllenden vertragsgegenständlichen Leistungen bzw. Tätigkeiten einweist.

Der Auftraggeber ist berechtigt, Informationen, die das vorliegende Vertragsverhältnis betreffen, gegenüber Dritten – insbesondere Bietern in einem Ausschreibungs- bzw. Auswahlverfahren zur Übernahme der von der Beendigung betroffenen Leistungen oder dem Folgedienstleister – offenzulegen, soweit dies für eine ordnungsgemäße Überleitung der Leistungen auf diese erforderlich ist.

### **5.12 Weitere Bestimmungen bei Beendigung des Vertrages**

Die Erbringung der Leistungen dieser Anlage erfolgt auf Basis der Konditionen und Bestimmungen des EVB-IT Dienstvertrags\_26-2000077114, dessen jeweilige Bestimmungen somit über das Vertragende hinaus gelten.

Wird das Vertragsverhältnis auf Grund einer Pflichtverletzung des Auftragnehmers durch den Auftraggeber beendet, so hat der Auftragnehmer – vorbehaltlich evtl. Schadensersatzansprüche des Auftraggebers – Anspruch auf eine anteilige Vergütung der von ihm bis zur Kündigung erbrachten vertragsgegenständlichen Leistungen, soweit diese von dem Auftraggeber genutzt werden können. Nicht nutzbare Leistungen werden dem Auftragnehmer, soweit dies möglich ist, ohne eine gesonderte Vergütung zurückgegeben.

Die Rechte aus § 321 BGB bleiben unberührt. Die Geltendmachung eines etwaigen Unternehmerpfandrechts im Sinne von § 647 BGB bei Werkleistungen durch den Auftragnehmer ist ausgeschlossen.

Für die erforderlichen Rückführungsleistungen, Restarbeiten und/oder Hauptleistungen über den Vertrag hinaus erhält der Auftragnehmer, falls nicht anders vereinbart, ein aufwandsbezogenes Entgelt gemäß der vereinbarten Preise. Der Auftragnehmer ist zur Geltendmachung eines darüberhinausgehenden Aufwandes nicht berechtigt, wenn der Auftraggeber aus wichtigem Grund gekündigt hat.

## **6 Zusammenarbeit & Governance**

### **6.1 Berichtswesen**

Zur Sicherstellung einer transparenten und vertrauensvollen Zusammenarbeit sind regelmäßige Berichte und ad hoc Informationen erforderlich. Die nachfolgende Übersicht beschreibt die einzureichenden Berichte und Informationspflichten. Ergänzend behält sich der Auftraggeber vor, nach Absprache mit dem Auftragnehmer, weitere Berichte anzufordern.

Laufend:

- Probleme und Vorschläge zu Verbesserungen
- Entwicklung und Fluktuation des eingesetzten Personals

Jährlich:

- Schulungs- und Qualifikationsnachweise der Mitarbeiter
- Nachweis über die Einhaltung der Versicherungspflichten
- Allgemeine Unternehmensentwicklung und Geschäftsergebnisse

Ad hoc:

- Meldung von Vertragsverstößen (z. B. bei Verstößen gegen Compliance-Vorgaben).
- Meldung von wesentlichen Änderungen in der Eigentümerstruktur oder Geschäftsführung.
- Meldung von behördlichen Prüfungen oder Sanktionen (z. B. durch Datenschutzbehörden, Aufsichtsbehörden).
- Meldung von gravierenden Qualitätsmängeln oder Reklamationen durch Dritte.
- Fristlose Kündigungen von für die Bundesbank tätigen Mitarbeitern
- Anmeldung von Insolvenz

### **6.2 Planung des Arbeitseinsatzes**

Die Steuerung und Koordination des Ressourceneinsatzes erfolgen in enger Abstimmung zwischen Auftraggeber und Auftragnehmer. Der Auftragnehmer benennt hierfür einen zentralen Ansprechpartner, der die Kommunikation zu allen relevanten Aspekten der vertraglichen Auftragsabwicklung übernimmt. Die fachliche Hoheit über die zu erbringenden Leistungen und die Priorisierung der Aufgaben verbleiben beim Auftraggeber. Der Auftragnehmer nimmt hierbei eine beratende Rolle ein und unterstützt den Auftraggeber bei der fachlichen Organisation. Der Auftragnehmer stellt sicher, dass für die ordnungsgemäße und fristgerechte Durchführung der beauftragten Leistungen ausreichend qualifizierte Ressourcen zur Verfügung stehen. Die eingesetzten Personen unterliegen ausschließlich dem Weisungsrecht des Auftragnehmers. Eine Eingliederung in die Arbeitsorganisation des Auftraggebers sowie eine fachliche oder

disziplinarische Weisungsbefugnis des Auftraggebers gegenüber den Mitarbeitenden des Auftragnehmers sind ausdrücklich ausgeschlossen.

### **6.3 Finanzcontrolling**

Im Rahmen der Beauftragung verpflichtet sich der Auftragnehmer regelmäßig einen Finanzreport hinsichtlich der beauftragten Arbeitspakete zur Verfügung zu stellen. Das Intervall sowie die Nachvollziehbarkeit der aufgestellten Kennzahlen wird dabei im Rahmen der jeweiligen Beauftragung abgestimmt.

### **6.4 Steuerungsmeeting**

Auf Verlangen der Bundesbank verpflichtet sich der Auftragnehmer zur Teilnahme der erforderlichen Rollen an Steuerungsmeetings mit der jeweiligen Leitung der in der IT verantwortlichen Stellen. In den Steuerungsmeetings wird die Planung und Steuerung der Ressourcen, die Abschätzung und Kalkulation des Gesamtaufwandes sowie die Koordination aller Termine hinsichtlich der zeitlichen Planung, ggf. u. a. im Sinne eines Multi-Projektmanagements, für die fachlichen und technischen Projekte sowie der Wartung vorgenommen. Eine eventuelle Ansetzung von Steuerungsmeetings erfolgt dabei in Abhängigkeit des jeweiligen beauftragten Volumens. Im Einzelfall ist es erforderlich auf beiden Seiten Personen des Top-Managements (z. B. Eskalationsinstanzen) hinzuzuziehen.

### **6.5 Eskalationsprozess**

Sofern im Rahmen der Zusammenarbeit Meinungsverschiedenheiten auftreten und/oder eine wesentliche vertragliche Verpflichtung nicht erfüllt wird (im folgenden Konflikt), werden die Vertragspartner versuchen, dies unverzüglich partnerschaftlich zu lösen.

Kann der Konflikt nicht innerhalb einer angemessenen Frist beigelegt werden, so kann jeder Vertragspartner dem anderen gegenüber dem Eintritt des im folgenden beschriebenen Eskalationsmechanismus in Schrift- oder Textform (d.h. per E-Mail) verlangen.

Mit Zugang dieses Verlangens beginnt die erste Eskalationsstufe. Diese besteht aus jeweils zwei verantwortlichen Vertretern einer jeden Vertragspartei, die innerhalb von 24h nach Zugang des Verlangens gegenseitig zu benennen sind. Diese Personen versuchen innerhalb einer Frist von sieben Kalendertagen ab Zugang des Verlangens den Konflikt einvernehmlich beizulegen.

Gelingt dies nicht, so beginnt die zweite Eskalationsstufe. Diese kann durch jede Vertragspartei initiiert werden durch Mitteilung einer der beiden Verantwortlichen aus der ersten Eskalationsstufe. Beide Vertragsparteien müssen daraufhin innerhalb von 24h nach Beendigung der ersten Eskalationsstufe jeweils einen verantwortlichen Vertreter (Geschäftsführung



des Auftragnehmers bzw. Abteilungsleitung des Auftragnehmers) für die zweite Eskalationsstufe benennen. Die verantwortlichen Vertreter für die zweite Eskalationsstufe versuchen, den Konflikt innerhalb einer Frist von weiteren 14 Kalendertagen beizulegen.

## **7 Anforderungen an die durch den Auftragnehmer eingesetzten Personen zur Unterstützung**

Die Leistungserbringung muss durch mehrere Personen des Auftragnehmers erfolgen. Der Auftragnehmer verpflichtet sich dazu, dass alle geforderten Aufgaben vollumfänglich und qualifiziert durch das eingesetzte Team erfüllt werden.

Darüber hinaus verpflichtet sich der Auftragnehmer nur Personen einzusetzen, die über hinreichende Qualifikationen und Erfahrungen zur Erbringung der Leistung, vor allem auch hinsichtlich zu nutzender Technologien und Tools, verfügen.

Des Weiteren verpflichtet sich der Auftragnehmer, für die nachfolgenden Rollen ausschließlich Personen einzusetzen, welche die jeweiligen Mindestqualifikationen erfüllen.

### **7.1 Allgemeine Anforderungen**

Die folgenden allgemeinen Qualifikationen (A-Kriterien) sind Kenntnisse und Erfahrungen, die für alle eingesetzten Personen gemäß Kapitel 7 dieser Leistungsbeschreibung vorausgesetzt werden. Die Erfüllung der allgemeinen Anforderungen (s. Kap. 7.1) sowie der geforderten Profile s. Kap. 7.2-7.9) ist bei der Angebotsabgabe in Form der Eigenerklärung in der Bewertungsmatrix, Reiter „Mindestanforderungen (A-Krit)“ darzulegen.

#### **Allgemeine Qualifikationen (A-Kriterien):**

*Folgende Kenntnisse und Erfahrungen sind bei jeder einzelnen eingesetzten Person erforderlich:*

- schnelle Auffassungsgabe
- ausgeprägtes logisches sowie analytisch-mathematisches Denkvermögen
- sicheres Auftreten und Überzeugungsfähigkeit
- Kommunikationsfähigkeit
- Sprachkenntnisse
  - Beherrschung der **deutschen Sprache** in Wort und Schrift inkl. des technischen Fachvokabulars gemäß **C2** des europäischen Referenzrahmens (CEFR)
  - Beherrschung der **englischen Sprache** in Wort und Schrift inkl. des technischen Fachvokabulars gemäß **B1** des europäischen Referenzrahmens (CEFR)



- selbstständige, kunden- und zielorientierte Arbeitsweise
- Fähigkeiten und Bereitschaft zum laufenden Know-how-Transfer
- praktische Erfahrungen in der Präsentation unter Einsatz unterschiedlicher Medien
- hohe Einsatzbereitschaft, Flexibilität und Belastbarkeit
- Theoretische und praktische Erfahrung mit Prozessen, Methoden und der Rolle eines DevSecOps-Teams
- Umfangreiche praktische Erfahrung im Arbeiten nach dem agilen Framework Scrum und der Entwicklungsarbeit nach Scrum
- Persönliche und fachliche Fähigkeiten in der Zusammenarbeit mit interdisziplinären Teams (kommunikativ, offen, konstruktiv, fokussierte, kollaborativ), didaktische Fähigkeiten der Wissensvermittlung und Sicherstellung des Wissenstransfers im DevSecOps-Team und gegenüber den internen Teammitgliedern
- Umfangreiche praktische Erfahrung in übergreifender Projektzusammenarbeit, auch im Zentralbankwesen
- Zusätzlich fachliches Spezialwissen im Bereich Meldewesen und Regulatorik, Erfahrungen im Zentralbankwesen und Erfahrungen im Aufbau eines Meldewesen-Portals in einer Cloudumgebung im B2B (business to business) Kontext

Die folgenden geforderten Qualifikationen und Erfahrungen müssen vollumfänglich und qualifiziert durch das vom Auftragnehmer eingesetzte Team, d.h. jeweils von mindestens einer Person, erfüllt werden:

**Allgemeine Qualifikationen (A-Kriterien):**

*Folgende Kenntnisse und Erfahrungen sind insgesamt im eingesetzten Team erforderlich:*

- Umfangreiche praktische Erfahrung in der Cloud agnostischen Entwicklung
- Umfangreiche praktische Erfahrungen im Einsatz von „CIAM“ Systemen, d. h. zentralen Benutzer- und Rechtemanagement inkl. Zugriffssicherheit, modernen Authentifizierungsverfahren und Self Services
- Kenntnisse in der Umstellung sowie Migration von „CIAM“ Systemen
- Erfahrungen bei der „Daten-Sanitisierung“ zwischen Cloud- und „on prem“ Umgebung (Digitale Souveränität)
- Erfahrungen in den verschiedenen Bereitstellungsszenarien von IT-Services (IaaS, PaaS, SaaS, hybride Konzepte, On-Premise)
- Erfahrungen in der erfolgreichen Migration von Applikationen aus einer Public Cloud zu einer anderen Cloudplattform, in eine Private Cloud oder ein eigenes Rechenzentrum

- Erfahrungen in fachlichen und technischen Services: ereignisgetriebene Mehrwertdienste zur Orchestrierung der Kundenerfahrung, Daten und Interaktionen (Microservices, Containerverwaltung, Anwendungsentwicklung)
- Kenntnisse im produktivitätssteigernden und datenschutzkonformen Einsatz von KI gestützten Tools zur Aufgabenerfüllung

Zusätzlich sind die weiteren jeweiligen folgenden Mindestqualifikationen für die nachstehenden Rollen zu gewährleisten.

## **7.2 Austausch von Personen zur Leistungserfüllung**

Ergänzend zu Ziffer 8 der EVB-IT Dienstleistungs-AGB gilt:

Der Auftragnehmer hat für die ordnungsgemäße Erbringung der vertraglich vereinbarten Leistungen im Regelbetrieb wie in Krisenzeiten quantitativ und qualitativ ausreichende Personalressourcen bereitzustellen. Er stellt kontinuierlich sicher, dass das von ihm eingesetzte Personal stets über den aktuellen Stand der Technik verfügt, sowie hinreichend bzgl. der aktuellen Gesetzes- und Risikolage (insb. IT-Sicherheit und –Bedrohungen, Datenschutz, Compliance- und Fraud-Problematiken) geschult ist.

Erfüllt eine vom Auftragnehmer eingesetzte Person die an sie gestellten Anforderungen nicht oder bestehen Zweifel an deren Zuverlässigkeit, kann der Auftraggeber vom Auftragnehmer den Austausch der Person verlangen.

Der Auftragnehmer stellt eine hohe personelle Kontinuität sicher. Fällt jedoch eine in die Aufgaben eingearbeitete Person des Auftragnehmers längerfristig oder dauerhaft aus und muss deshalb oder wegen eines Wechsels nach dem erstgenannten Grund der Auftragnehmer eine andere Person einsetzen, wird die Einarbeitung für diese neue Person nicht in Rechnung gestellt, solange der Auftragnehmer die ordnungsgemäße Erbringung der vertragsgemäßen Leistungen nicht gewährleisten kann. Diese Ersatzperson muss spätestens nach 15 Bankarbeitstagen die Arbeit aufnehmen.

Ein Austausch von Mitarbeiter ist dem Auftraggeber rechtzeitig anzuzeigen. Der Auftragnehmer stellt sicher, dass bei einem Personalwechsel eine geordnete Übergabe und ein vollständiger Know-how-Transfer erfolgen. Eine höhere Qualifikation der Austausch- oder Ersatzperson begründet keinen Anspruch auf eine Erhöhung der Vergütung.

Des Weiteren weist der Auftragnehmer nach, dass er über ein Konzept zur Mitarbeitergewinnung und zum verbundenen Onboarding Prozess verfügt.

## Anlage 1 zum EVB-IT Dienstvertrag 26-2000077114 \_\_\_\_\_

Die angebotenen Mitarbeiter müssen vom Auftragnehmer zwingend mit dem Zuschlag zur Verfügung gestellt werden und der Bundesbank mindestens ein halbes Jahr nach Zuschlag weiterhin zur Verfügung stehen. Ein spontaner Abzug der Personen ist zu vermeiden und mit einem angemessenen zeitlichen Vorlauf vom Auftragnehmer anzukündigen, so dass eine adäquate Nachbesetzung möglich ist. Ausgenommen davon sind Umstände, die der Auftragnehmer nicht zu vertreten hat (z.B. Krankheit, Kündigung).

Zum Zwecke der Einarbeitung kann der Auftraggeber den Personen des Auftragnehmers Zutritt zu bestimmten Räumlichkeiten und ggf. Daten vor Beginn der Leistungserbringung ermöglichen. Im Einzelfall kann von dieser Regelung im Einvernehmen zwischen Auftraggeber und Auftragnehmer abgewichen werden.

### 7.3 Infrastruktur-Architekt (A-Kriterien)

Zur Unterstützung im Bereich der **Infrastruktur-Architektur** wird ein Experte mit mindestens fünfjähriger relevanter konzeptioneller und praktischer Berufserfahrung (belegt durch Betreuung entsprechender Projekte) in folgenden Bereichen benötigt:

- Mindestens praktische Erfahrung in der Modernisierung von Infrastrukturen auf der Grundlage von Cloud- und Container-Technologie
- Umfangreiche praktische Erfahrungen in den derzeit verwendeten und „State-of-the-Art“ einzusetzenden Anwendungsentwicklungsmethoden
- Umfangreiche praktische Erfahrung in der Implementierung vielschichtiger Infrastruktur-Architekturen
- Praktische Erfahrung in der Analyse und Optimierung der Anwendungs- und Infrastruktur-Performance
- Zur Klärung produktspezifischer Fragen schnellen und unkomplizierten Know-how-Austausch in einem entsprechenden Netzwerk
- Umfangreiche praktische Erfahrung mit Microservice-Architekturen sowie Containerisierung und Container-Orchestrierungstechnologien, die je nach den spezifischen Anforderungen eingesetzt werden
- Praktische Erfahrung in der Modernisierung von Anwendungen, z. B. auf eine Java-basierte Cloud-Plattform und/oder SPA Applikation
- Zugang zu einem Netzwerk zur schnellen und unkomplizierten Diskussion über architekturelle Fragen
- Umfangreiche Kenntnisse und umfangreiche praktische Erfahrungen hinsichtlich der eingesetzten Hardware bzw. der Zielhardware gem. jeweiliger Anforderung

- Umfangreiche Kenntnisse und umfangreiche praktische Erfahrungen hinsichtlich der eingesetzten Technologien/Frameworks bzw. der Zieltechnologien/Frameworks gem. jeweiliger Anforderung
- Umfangreiche Kenntnisse und umfangreiche praktische Erfahrungen hinsichtlich der eingesetzten Tools bzw. der vorgesehenen Tools gem. jeweiliger Anforderung
- Umfassende praktische Erfahrung mit der Entwicklung nativer Cloud-Anwendungen
- Umfangreiche praktische Erfahrungen in Konzeption, Aufbau und Einführung von Informationssystemen (z.B. SQL und NoSQL-Datenbanken)
- Umfangreiche praktische Erfahrungen in Konzeption und Umsetzung von CI/CD Pipelines (Build und Deployment auf Azure Kubernetes Service)
- Praktische Erfahrungen zur Konzeption und Integration von Mechanismen zur Historisierung, Archivierung bzw. Versionsverwaltung
- Mindestens umfangreiche praktische Erfahrungen in: Datenbanken (z.B. SQL-Server), Cloud Storage (z.B. Azure Blob Storage), Datenbereitstellung (z.B. WebDAV)
- Umfangreiche praktische Erfahrungen mit GIT
- Umfangreiche praktische Erfahrungen bei der Entwicklung und Bewertung von Durchführungsszenarien der Anwendungsmigration und Data Migration auf alternativen Plattformen
- Umfangreiche praktische Erfahrungen in der Anwendungssicherheit (z.B. OpenID/OAuth)"
- Umfangreiche praktische Erfahrungen in der Implementierung von Infrastrukturkomponenten (z.B. mit Terraform auf Azure)
- Umfangreiche praktische Erfahrungen Sicherheit von Infrastrukturkomponenten (z.B. API-Gateway, Network Security, VPN, RBAC, Rewrite Proxy, NGINX, Firewall)
- Praktische Erfahrung in Projekten mit Cloud-Technologien (Public/ Private/ Hybrid) unter Nutzung der jeweils angegebenen Technologien/Tools (z.B. auf Azure)
- Praktische Erfahrung im Bereich DevOps (z.B. Azure DevOps)
- Praktische Erfahrung im Bereich DevSecOps
- Konzepte und nachweisbare Umsetzungsarbeiten mit State-of-the-art-Ansätzen und innovativen Techniken in der IT-Infrastruktur, oder -Architektur oder der Anwendungsentwicklung

#### 7.4 Anwendungs-Architekt (A-Kriterien)

Zur Unterstützung im Bereich der **Anwendungsarchitektur** wird ein Experte benötigt, welcher seit mindestens zehn Jahren in diesem Bereich tätig ist und über etwa fünf Jahre relevante konzeptionelle und praktische Berufserfahrung verfügt, nachgewiesen durch die Betreuung entsprechender Projekte in folgenden Bereichen:

- Praktische Erfahrungen bei der Modernisierung von Anwendungen (z.B. Process Optimization, Performance Optimization)
- Umfangreiche praktische Erfahrung in der Konzeption und Implementierung von Microservices
- Umfangreiche praktische Erfahrungen in den derzeit verwendeten und proaktives Einbringen künftig einzusetzender Anwendungsentwicklungsmethoden
- Umfangreiche praktische Erfahrungen in der Entwicklung und Anpassung von vielschichtigen Softwarearchitekturen
- Praktische Erfahrungen in der Analyse und Optimierung der Anwendungsperformance unter Berücksichtigung der eingesetzten Infrastruktur
- Praktische Erfahrungen bei der Modernisierung von Anwendungen (z.B. Process Optimization, Performance Optimization)
- Profunde praktische Erfahrung in der Konzeption und Implementierung von Restful Microservices
- Umfangreiche praktische Erfahrungen in den derzeit verwendeten und „State-of-the-Art“ einzusetzenden Anwendungsentwicklungsmethoden
- Umfangreiche praktische Erfahrungen in der Entwicklung und Anpassung von vielschichtigen Softwarearchitekturen
- Praktische Erfahrungen in der Analyse und Optimierung der Anwendungsperformance
- Zugang zu einem Netzwerk zum schnellen und unkomplizierten Know-how-Austausch für die Klärung produktspezifischer und architektureller Fragen
- Praktische Erfahrungen bei der Modernisierung von Anwendungen unter Berücksichtigung einer neuen Zielplattform
- Umfangreiche praktische Erfahrungen hinsichtlich der eingesetzten Technologien/Frameworks bzw. der Zieltechnologien/Frameworks gem. jeweiliger Anforderung
- Umfangreiche praktische Erfahrungen hinsichtlich der eingesetzten Tools bzw. der vorgesehenen Tools gemäß jeweiliger Anforderung
- Umfangreiche praktische Erfahrungen in der Anwendungsentwicklung

- Praktische Erfahrungen zur Konzeption und Integration von Mechanismen zur Historisierung, Archivierung bzw. Versionsverwaltung
- Umfangreiche praktische Erfahrungen in der Datenmodellierung, Datenkonsolidierung, Datenbereinigung
- Erfahrungen in der Geschäftsprozessmodellierung inkl. Geschäftsprozessmodellierungsmethoden
- Umfangreiche praktische Erfahrungen bei der Entwicklung und Bewertung von Durchführungsszenarien der Anwendungsmigration und Data Migration auf alternative Plattformen
- Umfangreiche praktische Erfahrungen in der Anwendungssicherheit
- Erfahrungen in der Implementierung von Infrastrukturkomponenten
- Umfangreiche praktische Erfahrungen in Sicherheit von Infrastrukturkomponenten
- Praktische Erfahrung in Projekten mit Cloud-Technologien (Public/ Private/ Hybrid) unter Nutzung der jeweils angegebenen Technologien und/oder Tools
- Praktische Erfahrung im Bereich DevOps
- Praktische Erfahrung im Bereich DevSecOps
- Umfangreiche praktische Erfahrungen in der Erstellung von Konzepten und Umsetzung mit State-of-the-art-Ansätzen und innovativen Techniken in der IT--Architektur und der Anwendungsentwicklung
- Erfahrungen zu Konzeption und Umsetzung von Event getriebene Microservice Architekturen u.a. mit RESTful APIs und GraphQL Schnittstellen
- Umfangreiche praktische Erfahrungen zu Konzeption und Integration von verschiedenen asynchronen Kommunikationsprotokollen
- Praktische Erfahrungen zu Konzeption und Umsetzung von KAFKA Failure Strategien
- Praktische Erfahrungen zu Konzeption und Umsetzung von KAFKA Streaming Strategien
- Umfangreiche praktische Erfahrungen zur Konzeption von Microservice Architekturen mit Aspekten aus dem Domain Driven Design (DDD)
- Praktische Erfahrungen bei der Mitarbeit an technischen Gesamtarchitekturen
- Praktische Erfahrungen in der Konzeption, Evaluierung und fortlaufenden Verbesserung von Anwendungsarchitekturen
- Praktische Erfahrungen bei der Anleitung von Entwicklerteams
- Praktische Erfahrungen bei der stetigen technologischen Weiterentwicklung von Anwendungen

## 7.5 Entwicklungsexperte mit Schwerpunkt Backend (A-Kriterien)

Zur Unterstützung im Bereich **Programmierung/Entwicklung** werden externe Entwickler mit umfangreicher praktischer Erfahrung in folgenden Bereichen benötigt:

- Nutzung von etablierten Technologien in der Softwareentwicklung wie Windows, Linux, Docker, SQL Datenbanken, Cloud Plattformen, eventgetriebene und messagebasierte asynchrone Kommunikation, synchrone APIs, Storages u.a.
- Programmiertechnische Umsetzung der o.g. Anforderungen mit modernen Entwicklungsframeworks, -umgebungen (z.B. IntelliJ, Visual Studio Code) und –sprachen (z.B. JAVA, Python)
- Umfangreiche praktische Erfahrung mit dem Java Microservice Frameworks Quarkus
- Umfangreiche praktische Erfahrung beim Einsatz und Verwendung von cloud-basierten Produkten und Programmiertechniken
- Umfangreiche praktische Erfahrung in der Entwicklung und Nutzung von Microservices und eines Event-Hubs (z.B. Kafka) sowie von Message Queues
- Praktische Erfahrung von Versionsverwaltung über SVN, Git, Jenkins oder vergleichbaren Tools
- Praktische Erfahrung im Umgang mit Kubernetes, Docker, OpenShift oder vergleichbaren Container-Plattformen
- Umfangreiche praktische Erfahrungen in der Umsetzung von Anforderungen der IT-Sicherheit (inkl. Verschlüsselung) und in der Umsetzung dieser Komponenten im Software-Design
- Umfangreiche praktische Erfahrung bei der Implementierung von OAuth2 / OIDC Security Flows
- Umfangreiche praktische Erfahrung in der Verarbeitung großer, strukturierter Datenmengen über verschiedene Interaktionskanäle und technische Schnittstellen (API mit REST, Portal, Batch via FTP und API)
- Erfahrungen bei der Umsetzung von Service Mesh Ansätzen wie z.B. SideCars
- Umfangreiche praktische Erfahrung im Einsatz von SOAP oder RESTful-Webservices inkl. API-Management
- Praktische Erfahrungen in der Verarbeitung von XML-/XSD/XBRL-Dateien mit containerisierten Ansätzen
- Sehr gute Kenntnisse im Cloud-Computing und in relevanten Plattformen (z. B. AZURE, AWS, GCP)



- Umfangreiche praktische Erfahrung mit relationalen (z. B. SQL, PL-SQL, T-SQL etc), nicht-relationalen (z. B. Redis, Cassandra etc.) Datenbanken sowie Datenbankverwaltungssystemen (z. B. MS SQL-Server, MySQL, Oracle etc.)
- Umfangreiche praktische Erfahrung in der Entwicklung und Orchestrierung von Microservices, Containern (sowie Container-Ressourcen und -Deployment) und dem Docker- und Kubernetes-Stack
- Sehr gute Kenntnisse des SDLC (Software Development Life Cycle)
- Erfahrung im Umgang mit automatisierten CI/CD Pipelines sowie den zugehörigen DevSecOps-Tools

#### **7.6 Entwicklungsexperte mit Schwerpunkt Frontend (A-Kriterien)**

Zur Unterstützung im Bereich **Programmierung/Entwicklung** werden externe Entwickler mit umfangreicher praktischer Erfahrung in folgenden Bereichen benötigt:

- Nutzung von etablierten Technologien in der Softwareentwicklung wie Windows, Linux, Docker, SQL Datenbanken, Cloud Plattformen, synchrone APIs, Storages u.a.
- Programmiertechnische Umsetzung der o.g. Anforderungen mit modernen Entwicklungsframeworks (z.B. Angular), -umgebungen (z.B. IntelliJ, Visual Studio Code) und -sprachen (z.B. Angular, TypeScript)
- Umfangreiche praktische Erfahrungen im Entwicklerframework Angular
- Praktische Erfahrungen zum Einsatz von Microfrontend-Technologien
- Sehr gute Kenntnisse zum Einsatz und Verwendung von cloud-basierten Produkten und Programmieretechniken
- Umfangreiche praktische Erfahrungen in der Entwicklung von interaktiven User Interfaces inkl. Benutzerführung und API-Integration
- Erfahrungen in der Versionsverwaltung über SVN Git, git, Jenkins oder vergleichbaren Tools
- Kenntnisse von Kubernetes, Docker, OpenShift oder vergleichbaren Container-Plattformen
- Praktische Erfahrung in der Berücksichtigung von IT-sicherheitstechnischen Maßnahmen und Zugriffssicherheit bei der Programmierung und im Programmcode („secure-by-design“)
- Erfahrung bei der Integration von OAuth2 / OIDC Security Flows
- Praktische Erfahrung bei der Integration von SOAP oder RESTful-Webservices



- Kenntnisse im Cloud-Computing und in relevanten Plattformen (z. B. AZURE, AWS, GCP)
- Kenntnisse von relationalen (z. B. SQL, PL-SQL, T-SQL etc), nicht-relationalen (z. B. Redis, Cassandra etc.) Datenbanken sowie Datenbankverwaltungssystemen (z. B. MS SQL-Server, MySQL, Oracle etc.)
- Praktische Erfahrungen in der Umsetzung von Anforderungen der IT-Sicherheit (inkl. Verschlüsselung) und in der Umsetzung dieser Komponenten im Software-Design
- Sehr gute Kenntnisse des SDLC (Software Development Life Cycle)

## 7.7 Entwicklungsexperte mit Schwerpunkt Cloud-Engineering (A-Kriterien)

Zur Unterstützung im Bereich **Programmierung/Entwicklung** werden externe Entwickler mit umfangreicher praktischer Erfahrung in folgenden Bereichen benötigt:

- Nutzung von etablierten Technologien in der Softwareentwicklung wie Windows, Linux, Docker, SQL Datenbanken, Cloud Plattformen, synchrone APIs, Storages u.a.
- Erfahrung im Einsatz und Verwendung von cloud-basierten Produkten und Programmier-techniken
- Erfahrungen mit Microservice-Architekturen sowie Containerisierung und Container-Orchestrierungstechnologien, die je nach den spezifischen Anforderungen eingesetzt werden.
- Sehr gute Kenntnisse von Versionsverwaltung über SVN Git, git, Jenkins oder vergleichbaren Tools
- Umfangreiche praktische Erfahrung im Umgang mit Kubernetes, Docker, OpenShift oder vergleichbaren Container-Plattformen
- Berücksichtigung von IT-sicherheitstechnischen Maßnahmen und Zugriffssicherheit („secure-by-design“)
- Kenntnisse bei der Implementierung von OAuth2 / OIDC Security Flows
- Sehr gute Kenntnisse im Einsatz von SOAP oder RESTful-Webservices inkl. API-Management
- Praktische Erfahrung in der Entwicklung von hochverfügbaren Systemen sowie fundierte Grundkenntnisse derer Konzepte (z. B. Redundanz etc.)
- Praktische Erfahrung in Projekten mit Cloud-Technologien (Public/ Private/ Hybrid) unter Nutzung der jeweils angegebenen Technologien/Tools (z.B. auf Azure)

- Praktische Erfahrung mit relationalen (z. B. SQL, PL-SQL, T-SQL etc), nicht-relationalen (z. B. Redis, Cassandra etc.) Datenbanken sowie Datenbankverwaltungssystemen (z. B. MS SQL-Server, MySQL, Oracle etc.)
- Erfahrung im Umgang mit Cloud Storage (z.B. Azure Blob Storage), Datenbereitstellung (z.B. WebDAV)
- Praktische Erfahrung in Networking, Computer-Networks sowie der Entwicklung von Lösungen mit Client-Server-Architekturen
- Praktische Erfahrung in verteilten Systemen
- Erfahrung in der Analyse und Optimierung der Anwendungs- und Infrastruktur-Performance
- Sehr gute Kenntnisse des SDLC (Software Development Life Cycle)
- Praktische Erfahrung im Design, Aufbau und Betrieb automatisierter CI/CD Pipelines sowie im Umgang mit den zugehörigen DevSecOps-Tools

#### 7.8 Tester / Testautomatisierungs-Engineer (A-Kriterien)

Zur Unterstützung im Bereich **Implementierung und Durchführung von Testautomatisierungen** werden externe Tester mit umfassender praktischer Erfahrung in folgenden Bereichen benötigt:

- Praktische Erfahrung in der Konzeption, Implementierung und Wartung von Testautomatisierungs-Frameworks
- Sehr gute Kenntnisse im Bereich Standards zu Qualitätsmanagement und Softwaremanagement
- Sehr gute Kenntnisse in u. a. Java, Typescript für die Testautomatisierung
- Praktische Erfahrungen in Tools für Lasttests (Load Testing) und Performance-Tests, insb. Apache JMeter, Azure Load Testing
- Sehr gute Kenntnisse in Testautomatisierungsplattformen (bspw. Katalon Studio) zur Durchführung von funktionalen Tests
- Sehr gute Kenntnisse in Skriptsprachen (z. B. Bash, PowerShell) zur Integration in Build- und Deployment-Pipelines
- Erfahrung in der Integration automatisierter Tests in Build- und Deployment-Prozesse (Smoke-, Regression-, Integrationstests) sowie Integration der Tests in CI/CD-Pipelines und Sicherstellung einer stabilen Testausführung
- Kenntnisse in Container-Technologien und Orchestrierung (insb. Kubernetes) für testnahe Umgebungen

- Sehr gute Kenntnisse in Regressionstest-Strategien und Testdatenmanagement
- Umfangreiche praktische Erfahrungen in der Erstellung von Teststrategien, Testplänen und Testkonzepten
- Praktische Erfahrungen in agilen Methoden (insb. Scrum) und deren Testintegration
- Kenntnisse in der Erstellung von Test-Auswertungen durch Definition von Metriken und KPIs zur Messung der Test- und Produktqualität

## **7.9 Application Security Engineer / Security Champion (A-Kriterien)**

Zur Unterstützung im Bereich **Anwendungssicherheit** wird ein Entwickler oder Spezialist mit umfassender praktischer Erfahrung in folgenden Bereichen benötigt:

- Praktische Erfahrungen in BSI IT-Grundschutz (inkl. IT-Grundschutz-Kompendium, Bausteine, Risikoanalyse) und deren praktischer Umsetzung in Projekten
- Praktische Erfahrungen im Hinblick auf BSI-Vorgaben, Datenschutz (DSGVO) und weitere regulatorische Anforderungen
- Praktische Erfahrungen im Nachweis der Umsetzung von Sicherheitsanforderungen (z.B. durch Testing, Dokumentation oder Toolunterstützung)
- Sehr gute Kenntnisse in weiteren Rahmenwerken wie u. a. OWASP SAMM, NIST Cyber Security Framework
- Sehr gute Kenntnisse der OWASP Top 10 und des OWASP ASVS zur Absicherung von Webanwendungen und APIs
- Praktische Erfahrungen moderner Web-/Portalarchitekturen (Microservices, Container, API-Gateways, Event-getriebene Architekturen)
- Praktische Erfahrung im sicheren Design von Authentifizierungs- und Autorisierungslösungen (z. B. OAuth2, OpenID Connect, SAML) inkl. Integration in bestehende IAM-Landschaften
- Praktische Erfahrung in Infrastructure as Code (z. B. Terraform) mit besonderem Augenmerk auf Security- und Compliance-Anforderungen
- Sehr gute Kenntnisse in der Nutzung von Cloud-Sicherheitsdiensten (z. B. IAM, KMS, WAF, Secrets Manager, Security Center/Defender, Logging)
- Praktische Erfahrung im Einsatz von SAST-, DAST-, SCA- und IaC-Scanning-Tools sowie deren Integration in den Entwicklungsprozess sowie Toolchain
- Sehr gute Kenntnisse in der Auswertung und Priorisierung von Scan-Ergebnissen sowie in der Ableitung konkreter Maßnahmen für Entwicklungsteams

- Sehr gute Kenntnisse in der Softwareentwicklung (z. B. Java) und in der Zusammenarbeit mit Entwicklungsteams auf Code- und Architektur-Ebene (z.B. durch Code- und Architektur-Reviews)