

Leistungsbeschreibung

für die europaweite Ausschreibung

- Offenes Verfahren -

Softwarelösung „Service Integration and Management (SIAM) Broker“

Auftraggeber:

ITSCare – IT-Services für den Gesundheitsmarkt
Saonestr. 3a
60528 Frankfurt

1 Inhalt

I.	Präambel	4
1.0	Allgemeines	4
1.1	Beschreibung der Ausgangssituation	4
1.2	Zielsetzung	5
1.3	Auftragsgegenstand, Umfang, Laufzeit	5
II.	Leistungsbeschreibung	6
2	Allgemeine Anforderungen	6
2.0	Kommunikation	7
2.1	Rollen und Berechtigungen	7
2.1.1	Berechtigungen	8
2.1.2	Berechtigungsvorlagen	8
2.2	Usability	9
2.3	Anforderungen an den Betrieb	9
2.4	Barrierefreiheit	10
2.5	Incidentmanagement	10
2.5.1	Masterticket	11
2.5.2	Eskalationspfade	11
2.6	Problem- / Notfallmanagement	11
2.6.1	Root Cause Analyse	12
2.6.2	Known Error DB	12
2.7	Changemanagement	12
2.7.1	Risikoanalyse	12
2.7.2	Freigabeworkflow	13
2.8	Eventmanagement	13
2.9	Reporting & Performancemanagement	13
2.10	Administration & Konfiguration	14
2.11	Nichtfunktionale & Technische Anforderungen	15
2.11.1	Interoperabilität & API Management	15
2.11.2	Performance & Skalierbarkeit	15
2.12	Security, Datenschutz & Audit	16
2.13	Migrationskonzept	16
3	Lizenzmodell und Softwareinformationen	17
3.0	Sprache, Dokumentation	17

3.1	Software-/Anwendungs-Lösung	17
3.2	Anzahl Nutzer	17
3.2.1	Funktionale Nutzergruppen	17
3.2.2	Technische User.....	18
3.2.3	Skalierungsoptionen.....	19
4	Wartung und Support.....	19
4.0	Wartung.....	19
4.1	Support	20
4.2	Supportanforderungen.....	20
4.3	Anforderungen an das Störungsmanagement	21
5	Weitere Leistungen	22
5.0	Implementierungsprojekt / Customizing	22
5.1	Schulungen	24
5.2	Weitere Unterstützungsleistungen	24
5.3	Leistungsort	24
6	Governance	25
6.0	Datenschutz.....	25
6.1	Informationssicherheit	25
6.1.1	Informationsklassifizierung	25
6.1.2	Einhaltung bestehender Richtlinien zur Informationssicherheit	25

I. Präambel

1.0 Allgemeines

Die ITSCare – IT-Services für den Gesundheitsmarkt GbR (nachfolgend „ITSCare“) mit Sitz in Frankfurt ist u.a. Betreiber verschiedener zentraler Online-Serviceangebote der gesetzlichen Krankenversicherungen (GKV) AOK Baden-Württemberg, AOK Bayern, AOK Bremen-Bremerhaven, AOK Hessen, AOK Niedersachsen, AOK Nordost, AOK NordWest, AOK PLUS, AOK Rheinland/Hamburg, AOK Rheinland-Pfalz/Saarland, AOK Sachsen-Anhalt (Aufzählung nachfolgend „AOKs“). Als Tochtergesellschaft der AOK Baden-Württemberg, AOK Hessen und AOK Rheinland-Pfalz/Saarland ist die ITSCare als Full-Service-IT-Dienstleister für zentrale IT-Themen zuständig.

Der Auftraggeber ist ausschließlich die ITSCare, eine Gesellschaft des privaten Rechts (GbR), nachstehend als AG bezeichnet.

Der Auftragnehmer (nachstehend als AN bezeichnet) ist das zur Leistungserbringung beauftragte Unternehmen. Leistungen, die durch Unterauftragnehmer erbracht werden, gelten als Leistungen des AN.

Zur besseren Lesbarkeit werden im vorliegenden Dokument personenbezogene Bezeichnungen, die sich zugleich auf Frauen, Männer und Divers beziehen, generell nur in der männlichen Form angeführt, also z.B. „Kunden“ statt „KundInnen“ oder „Kundinnen und Kunden“. Dies soll keinesfalls eine Geschlechterdiskriminierung oder eine Verletzung des Gleichheitsgrundsatzes zum Ausdruck bringen.

1.1 Beschreibung der Ausgangssituation

In einem Umfeld, das durch fortschreitende Digitalisierung und steigende Anforderungen an die IT-Infrastruktur geprägt ist, übernimmt die ITSCare eine Schlüsselrolle als zentrale Betreiberinstanz für strategische Applikationen. Um in dieser dynamischen Systemlandschaft operative Exzellenz zu gewährleisten, stellt die ITSCare ein umfassendes Portfolio an standardisierten und individualisierten Prozessen bereit. Diese bilden das Fundament für ein ganzheitliches Service-Management, das von Incident- und Problem-Management bis hin zu dediziertem Reporting reicht.

Die aktuelle Architektur der Tools und Prozesse im Incident-Management ist dabei durch eine hohe strukturelle Komplexität gekennzeichnet. Zwar sind interne Prozesse und Integrationspunkte zu den bestehenden IT-Dienstleistern der AOKs vereinheitlicht, sie unterliegen jedoch einer starren zentralen Governance, die unter den Bedingungen zunehmender Vernetzung und absehbarer Anforderungen der Anbindung neuer Partner an ihre Grenzen stößt.

1.2 Zielsetzung

Die vom AN bereitzustellende Softwarelösung wird zentraler Bestandteil der Integrationsarchitektur auf Seiten der ITSCare. Sie ermöglicht im Sinne der Funktion einer Middleware und Service Integrators ein effizientes, systematisches und durchgängiges Andocken bestehender sowie zu etablierender Anbindungen an IT Service Management (ITSM) Prozesse und Tools.

Der als zentrales Steuerungsinstrument vorgesehene sog. SIAM Broker wird das Multi-Provider-Management der AOKs systematisch unterstützen und optimieren. Eine durchgängige End-to-End-Steuerung soll die Servicequalität über alle beteiligten Dienstleister hinweg gewährleisten und ein lückenloses Reporting sowie klar definierte Verantwortungsbereiche unterstützen.

Langfristig schafft dieser Ansatz eine standardisierte und belastbare Plattform, die künftige Erweiterungen – insbesondere die Ablösung bestehender Einzelintegrationen sowie die Anbindung weiterer Integrationspartner – proaktiv ermöglicht und steuerbar macht.

1.3 Auftragsgegenstand, Umfang, Laufzeit

Gegenstand der Leistungen des AN ist die Bereitstellung einer Softwarelösung für einen „Service Integration and Management (SIAM) Broker“

- zur Nutzung für im ITSM Umfeld Beschäftigte der ITSCare sowie kooperierender Partner (20 technische Schnittstellenuser / 20 concurrent technische Schnittstellenuser)
- falls abweichend klassifizierbar und nicht in Basis-Lizenz enthalten 10 Administratoren-Lizenzen
- falls abweichend klassifizierbar und nicht in Basis-Lizenz enthalten mit einem Transaktionsvolumen von mindestens 15.000 Einzeltransaktionen p.a., wobei eine Einzeltransaktion als vollständiger Durchlauf eines fachlichen Datensatzes (z.B. Incident) definiert ist, bei dem sämtliche während seines Lebenszyklus anfallenden Statusänderungen und Updates (bidirektional) bereits inkludiert sind und kein erneutes Transaktionskontingent verbrauchen. Die konkrete fiktive Mengenstaffel zur Preisermittlung über die Laufzeit ist dem Preisblatt zu entnehmen.
- Software-Pflege und -Wartung inkl. Remote-Support z.B. bei Störungen und Produktupdates

für eine Laufzeit von 48 Monaten ab Zuschlag.

Als weitere Leistungen sind vom AN zu erbringen:

- Implementierungsunterstützung (Installation, Konfiguration und Inbetriebnahme) – ggf. vor Ort bzw. über einen vom AG bereitgestellten Remotesupportzugang
- Bereitstellung und Unterstützung bei der Erstellung von Dokumentationen und Konzepten (z.B. Installationsdokumentation, Handbücher,

- Sicherheitskonzepte) sowie Bereitstellung von Schulungsunterlagen
- Customizing von Kundenanforderungen und ggf. Schnittstellen
- Schulung von Anwendern (Multiplikatoren) und Administratoren
- Projektunterstützung bei der Einführung

Eine detaillierte Aufstellung der weiteren Leistungen erfolgt in Kapitel 5.

II. Leistungsbeschreibung

2 Allgemeine Anforderungen

Die Softwarelösung dient der einheitlichen Aggregation, Distribution sowie der prozessualen Steuerung und Eskalation von Störungsmeldungen über alle Satelliten-Systeme hinweg. Der SIAM Broker fungiert hierbei als führende Master-Instanz zur Konsolidierung und Harmonisierung sämtlicher Entitäten, wobei die initiale Ausprägung auf Störungsmeldungen fokussiert, jedoch prozessunabhängig zu konzipieren ist.

Um eine effiziente Anbindung der Partnersysteme zu gewährleisten, muss die Lösung über eine intuitive Administrationsumgebung verfügen, die eine technologisch agnostische Integration mittels Low-Code/No-Code-Verfahren ermöglicht.

Die Interoperabilität ist so zu gestalten, dass externe Integrationspartner ihre gewohnten Nutzeroberflächen beibehalten können (Tool-Agnostik), während die Synchronisation und Orchestrierung im Hintergrund erfolgt. Die Lösung muss eine lückenlose Transparenz hinsichtlich der Bearbeitungshoheit (Ownership) über den gesamten Lebenszyklus einer Entität sicherstellen. Änderungen an Datensätzen sind in Echtzeit auf Basis eines definierten Regelwerks an die entsprechenden Satellitensysteme zu replizieren. Die Lösung muss in der Lage sein die prozessuale Bearbeitungsverantwortung dynamisch zuzuweisen und zu steuern. Dies muss auf Basis eines internen wie externen Organisationsmodells erfolgen, welches die verschiedenen Service-Provider-Strukturen abbildet.

Neben der funktionalen Steuerung muss die Lösung höchste Anforderungen an die Betriebssicherheit erfüllen. Dies beinhaltet robuste Mechanismen zum Error-Handling, wie beispielsweise automatisierte Retry-Verfahren und Queueing bei Systemausfällen, um die Datenintegrität zu wahren. Zur Erfüllung von Compliance-Vorgaben ist zudem eine revisionssichere Protokollierung (Audit-Trail) sämtlicher Transaktionen und Feldänderungen erforderlich. Ein integriertes Monitoring-Dashboard soll den Zustand der Schnittstellen sowie die Einhaltung systemübergreifender Service Level Agreements (SLAs) transparent halten.

Die Systemarchitektur muss eine hohe Skalierbarkeit und funktionale Flexibilität aufweisen, um über das Incident-Management hinaus weitere ITSM-Prozesse abbilden zu können. Die Lösung muss somit prozessagnostisch konzipiert sein, um eine perspektivische Erweiterung des Anwendungsbereichs auf zusätzliche ITSM-Disziplinen (z.B. Change-, Problem- oder Request-Management) ohne strukturelle

Anpassungen zu gewährleisten.

2.0 Kommunikation

Die Lösung muss eine hochverfügbare und latenzarme Kommunikation zwischen der Master-Instanz und den Satellitensystemen sicherstellen. Hierbei ist ein bidirektionaler Informationsfluss in Echtzeit zu gewährleisten, der auf modernen Kommunikationsprotokollen (z.B. REST, Webhooks oder Message Queueing) basiert. Zur Wahrung der Datenintegrität auch bei instabilen Verbindungen muss die Kommunikationsschicht über Mechanismen zur Empfangsbestätigung (Acknowledgement) und zur automatisierten Wiederaufnahme des Datentransfers verfügen.

Wesentliches Leistungsmerkmal ist die Synchronisation von kollaborativen Inhalten. Kommentare, Arbeitsnotizen und Anhänge müssen zwischen den beteiligten Systemen so repliziert werden, dass der Kontext der Bearbeitung für alle involvierten Parteien (interne Teams sowie externe Partner) jederzeit vollständig ersichtlich bleibt. Hierbei ist sicherzustellen, dass eine differenzierte Steuerung der Sichtbarkeit (z.B. interne vs. externe Kommentare) systemübergreifend unterstützt wird, um die Vertraulichkeit in Multi-Provider-Umgebungen zu wahren.

Die Plattform muss über eine integrierte Engine für das Benachrichtigungsmanagement verfügen. Diese soll Nutzer und Verantwortliche proaktiv über relevante Ereignisse in Kenntnis setzen. Die Distribution dieser Informationen muss über verschiedene Kanäle (z.B. E-Mail oder Enterprise-Messaging-Systeme) konfigurierbar sein. Ferner muss die Lösung in Notfällen in der Lage sein, dringende Informationen zeitgleich an definierte Stakeholder zu versenden.

Zur prozessualen Sicherheit muss die Lösung eine konsolidierte Sicht auf die Kommunikationshistorie jeder Entität bieten. Diese Historie dient als „Single Source of Truth“ und muss lückenlos dokumentieren, welche Informationen wann und durch wen an welches Satellitensystem übermittelt wurden. In Krisensituationen muss das System zudem eine gezielte Stakeholder-Kommunikation unterstützen, um definierte Nutzerkreise über den aktuellen Lösungsfortschritt automatisiert zu informieren.

2.1 Rollen und Berechtigungen

Die Software-Lösung muss ein flexibles Rollen- und Berechtigungssystem unterstützen, um z.B. Rollen und Berechtigungen für Administrator, Betreiber, technische User, fachliche User usw. abzubilden.

Anwenderrolle	Aufgaben
Technischer Administrator	Administration von Umgebung, Templates, Backup und Update

Anwenderrolle	Aufgaben
Fachlicher Administrator	Definition von Vorgangsarten für Entitäten, Workflows, Rollen- und Berechtigungsvergabe auf Vorgangsarten, Entitäten, Datensegmente, Auswertungen durchführen und auf unterschiedliche Bedarfe anpassen, Schnittstelle/Ansprechperson zum AN bei Anpassung sowie Fehlerbehebung, fungiert zudem auch als ITSM-Prozessverantwortlicher
Technischer User Satellitensystem	Synchronisation definierter Vorgangsarten und Segmente für Entitäten
Reporting	Erstellung und Abruf von Berichten + erweiterte Möglichkeiten im dynamischen Reporting wie Navigation durch einen vordefinierten Datenraum, Filter, Sortierungen, Detaillierung (Drill-Down) usw.
Berichtskonsumenten	Abruf von Berichten

Über die Software soll die Nutzung unterschiedlicher Funktionalitäten / Ausführung verschiedener Aufgabenstellungen über Anwenderrollen steuerbar sein.

2.1.1 Berechtigungen

Jeder Nutzer der Lösung muss individuell berechtigt werden können. Die verfügbaren Berechtigungen müssen sich in „Berechtigungsvorlagen“ gruppieren lassen, die den Nutzern zugeordnet werden. Hierzu sind Strukturen der Zugriffsberechtigung (z.B. Vererbung, Verschachtelung) vorzusehen, mit der die erforderlichen Gruppen dargestellt werden können. Die Rechtevergabe der Mitarbeiter erfolgt über Berechtigungstemplates aus dem SAP Identity Management (IDM) des AG, welches beim AG geführt wird. Zudem können die Berechtigungen für einzelne Mitarbeiter (MA) vom AG eigenständig angepasst und verändert werden.

2.1.2 Berechtigungsvorlagen

Die verfügbaren Berechtigungen müssen sich in „Berechtigungsvorlagen“ gruppieren lassen und den Nutzern zugeordnet werden können. Die Berechtigungsvorlagen sind vom AN bereitzustellen.

Die einzelnen Berechtigungen im Administrationsportal werden den Mitarbeitern nicht per Einzelberechtigung, sondern über Berechtigungsvorlagen vergeben. Die Zuordnung der Profile erfolgt automatisch auf Grundlage der im IDM vergebenen Rollen und Berechtigungen.

Änderungen der Berechtigungsvorlagen müssen sich unmittelbar auch auf die Personen auswirken, denen diese Vorlage zugewiesen wurde.

Widerspricht ein durch den Administrator vergebenes Einzelrecht dem Recht aus dem Berechtigungstemplate, so bleibt das Einzelrecht erhalten und wird durch die Synchronisation nicht überschrieben, solange keine andere Vorlage zugewiesen wird. Die Inhalte der Templates werden im Implementierungsprojekt definiert.

2.2 Usability

Das vom Auftragnehmer (AN) bereitgestellte System sollte dem Auftraggeber (AG) umfangreiche Customizingmöglichkeiten (Konfigurations- und Anpassungsmöglichkeiten) bieten. Diese betreffen speziell optische, jedoch auch inhaltliche und strukturelle Elemente. Des Weiteren gilt dies auch für einen Teil der Prozessabläufe, des Seitenaufbaus und der genutzten Templates.

Das Tool sollte mindestens über folgende Eigenschaften bzw. Funktionen verfügen:

- Intuitives Bedienkonzept einschl. einer benutzerfreundlichen Bedienoberfläche in deutscher Sprache
- Zentrale Datenhaltung
- Workflow- und Aufgabenmanagement sowie Benachrichtigungsfunktionen (Mailanbindung und Mail bei bestimmten Sachverhalten)

Fachliche Anwender werden intuitiv durch das Tool geführt und können weitgehend selbsterklärend Auswertungen und Anpassungen durchführen. Der Nutzer kann die Plattform dadurch weitestgehend so nutzen, wie er es von diversen gängigen Online-Plattformen gewohnt ist.

Anforderungen an eine intuitive Usability / Nutzerführung:

- schnelle Ladezeiten
- einfache Navigation (schnelles Auffinden gewünschter Informationen mit wenigen Klicks)
- leichte Lesbarkeit (kurze Textblöcke, relevante und informierende Überschriften, Auflockerungen durch Aufzählungen oder Bilder)
- ansprechendes Design (einheitliches und konsistentes Layout und Farbgestaltung)
- unkomplizierte Formulare (einfache Anwendung bei Kontakt- und ähnlichen Feldern, keine Überfrachtung, keine unnötigen Inhalte)

2.3 Anforderungen an den Betrieb

Die Bereitstellung erfolgt in der Bereitstellungsvariante Software-as-a-Service (SaaS) als Managed Service durch den AN.

Der AN garantiert die Einhaltung der geltenden Datenschutz- und Sicherheitsvorgaben des AG.

Es gelten folgende Anforderungen an Architektur und Integration:

Identitätsmanagement: Die Lösung muss eine nahtlose Anbindung an das Active Directory (via AD-Gruppen) unterstützen. Die Authentifizierung muss über Industriestandards (z. B. SAML 2.0 oder OpenID Connect) erfolgen und kompatibel zu Identity-Providern wie Keycloak sein.

Funktionale Flexibilität: Die Software darf keine geschlossene „Blackbox“ sein. Es muss möglich sein, benutzerdefinierte Funktionen, individuelle fachliche Logiken und Workflows eigenständig zu etablieren und zu konfigurieren.

Skalierbarkeit: Die Architektur muss – unabhängig von der gewählten Variante – prozessdiagnostisch und hochskalierbar ausgelegt sein, um eine spätere Erweiterung über das Incident Management hinaus zu gewährleisten.

2.4 Barrierefreiheit

Die Software soll den Anforderungen der Barrierefreiheit nach den folgenden Bestimmungen, jeweils in ihrer gültigen Fassung entsprechen:

- EU-Richtlinie 2016/2102 (EU-weit),
- WCAG 2.1-Standard (International),
- BITV2.0 (national) und
- L-BGG (Landes-Behindertengleichstellungsgesetz Baden-Württemberg)

Dabei sind die folgenden Anforderungen besonders zu beachten:

- (1) Die Software funktioniert mit einem Screenreader (Vorlesesoftware).
- (2) Die Software ist rein mit der Tastatur bedienbar (ohne Maus).
- (3) Die Software entspricht der Softwareergonomie unter Berücksichtigung der Arbeitsschutzanforderung, insbesondere im Hinblick auf die farbliche Gestaltung und Schriftgröße
- (4) Eine gängige Vergrößerungssoftware lässt sich integrieren und ist ohne Beeinträchtigung in den gängigen Größen (Zoomstufen – bis 300%) nutzbar.
- (5) Buttons, Seitenüberschriften etc. sind mit gängigen Begriffen, möglichst in Deutsch betitelt, um das fehlerfreie Lesen einer Reader-Software zu gewährleisten

Stellt der AG fest, dass z.B. elementare Anforderungen an die Barrierefreiheit nicht erfüllt sind, sichert der AN zu, diesen Mangel in einer angemessenen Zeit zu beheben und über ein Update/Upgrade die SW zu aktualisieren.

Dem AG entstehen weder für die SW-Aktualisierung (Programmierung) und die Bereitstellung noch die Implementierung/Installation irgendwelche Kosten.

2.5 Incidentmanagement

Der AN hat mit dem SIAM Broker eine zentrale Integrationsplattform (Middleware) bereitzustellen, die das Incident Management providerübergreifend orchestriert. Der SIAM Broker muss als zentrale Drehschreibe fungieren, die Störungsmeldungen zwischen den verschiedenen ITSM-Tools der Provider und den internen Systemen des AG routet und synchronisiert.

Die Lösung muss eine konsolidierte Ticketübersicht („Single Pane of Glass“) generieren, die den Status aller offenen, geschlossenen und eskalierten Incidents aus den integrierten Quellsystemen in Echtzeit aggregiert darstellt. Dabei ist sicherzustellen, dass Status-Änderungen und Ticket-Updates (z.B. Kommentare, Anhänge, Statuswechsel) bidirektional mit einer geringen Latenz zwischen den Systemen repliziert werden.

2.5.1 Masterticket

Der SIAM Broker muss über eine Logik zur Bildung und Verwaltung von Mastertickets verfügen. Die Middleware muss technisch in der Lage sein, eingehende Tickets unterschiedlicher Provider und / oder Endanwender (Child-Tickets) mit einem übergeordneten Masterticket logisch zu verknüpfen.

Hierbei muss die Lösung sicherstellen, dass Informationen, wie beispielsweise die Beschreibung eines Lösungswegs oder Workarounds, die im Masterticket hinterlegt werden, automatisiert mit den verknüpften Tickets in den jeweiligen Provider-Systemen synchronisiert werden. Der SIAM Broker fungiert dabei als Verteiler, der redundante Kommunikationswege eliminiert.

2.5.2 Eskalationspfade

Das System soll ein regelbasiertes Eskalationsmanagement als übergeordnete Logikschicht bereitstellen. Es sollen konfigurierbare Eskalationsregeln hinterlegt werden können, die basierend auf Metadaten der durchlaufenden Tickets automatische Aktionen auslösen.

Der SIAM Broker soll in der Lage sein, bei Eintreten definierter Bedingungen eine Eskalation (z. B. Benachrichtigung, Statusänderung oder Routing an eine spezielle Gruppe) sowohl in Richtung der internen Teams als auch an die Schnittstellen der externen Provider zu initiieren und diesen Vorgang revisionssicher zu protokollieren.

2.6 Problem- / Notfallmanagement

Die Middleware soll die Prozesse des Problem- und Notfallmanagements durch providerübergreifende Workflows unterstützen. Im Bereich Problemmanagement soll der SIAM Broker als zentrales Register für Problem-Records dienen, in die Probleme aus verschiedenen Quellen (Provider-Tickets) zusammengeführt und verwaltet werden, um eine zentrale Steuerung der Ursachenforschung über Systemgrenzen hinweg zu ermöglichen.

Für das Notfallmanagement soll der SIAM Broker Mechanismen bereitstellen, um kritische Ereignisse (Major Incidents) zu erkennen und eine Notfallkommunikation (Broadcasts) zu steuern. Die Lösung soll Warnmeldungen oder Statusinformationen simultan an alle angeschlossenen Schnittstellen und definierten Empfängergruppen (Stakeholder, Provider) verteilen, um eine synchrone Informationslage sicherzustellen.

2.6.1 Root Cause Analyse

Zur Unterstützung der nachhaltigen Störungsbehebung soll der SIAM Broker den Prozess der Root-Cause-Analyse (RCA) technisch abbilden können. Die Middleware soll in der Lage sein, RCA-Dokumente oder strukturierte Datenfelder (Ursache, Lösungsweg, Lessons Learned) von den Providern entgegenzunehmen, zu zentralisieren und am entsprechenden Problem-Record zu historisieren.

Es soll ferner gewährleistet sein, dass die Ergebnisse der Analysen zentral abrufbar sind, unabhängig davon, in welchem Provider-System die ursprüngliche Analyse durchgeführt wurde.

2.6.2 Known Error DB

Der SIAM Broker soll eine Funktion zur Aggregation oder Bereitstellung einer Known Error Datenbank (KEDB) bieten. In dieser werden bekannte Fehler und deren Workarounds, die von verschiedenen Providern geliefert werden, in einer zentralen Wissensdatenbank zusammengeführt oder referenziert.

Die Middleware soll sicherstellen, dass diese Information (Known Errors und Workarounds) für den Service Desk und andere beteiligte Parteien zentral durchsuchbar und aufrufbar sind.

2.7 Changemanagement

Zur Sicherstellung der langfristigen Stabilität der IT-Services ist die Lösung so zu konzipieren, dass das Changemanagement als zentrale Säule der Governance perspektivisch integriert werden kann. Der AN soll hierzu ein System bereitstellen, das nicht nur isolierte Änderungen verwaltet, sondern als Broker fungiert, der die Change-Prozesse über verschiedene Provider hinweg harmonisiert und steuerbar gestaltet.

2.7.1 Risikoanalyse

Die Lösung soll Funktionen zur proaktiven Identifikation und Bewertung von Risiken bereitstellen.

Das System soll Abhängigkeiten zwischen IT-Services, Infrastrukturkomponenten sowie beteiligten Providern darstellen können. Zudem sollen sich Zusammenhänge der jeweiligen Servicekomponenten visualisieren lassen.

Es soll ferner sichergestellt werden können, dass zeitliche Überschneidungen oder technische Abhängigkeiten zwischen verschiedenen Change-Anträgen automatisiert erkannt und / oder den Prozessverantwortlichen gemeldet werden.

Durch die konsolidierte Darstellung der betroffenen Services und Infrastrukturkomponenten sollen potenzielle Risiken für die Serviceverfügbarkeit frühzeitig erkennbar sein.

2.7.2 Freigabeworkflow

Die Lösung soll einen flexibel konfigurierbaren Freigabeworkflow für Freigabe (Change/Genehmigungs-)prozesse bereitstellen.

Hierarchische Genehmigungen: Die Lösung soll Workflows unterstützen, die sowohl interne (AG) als auch externe (Provider) Genehmigungsschritte integrieren.

Automatisierung: Basierend auf definierten Regeln (z. B. Change-Kategorie, Kritikalität oder Risiko-Score) sollen Genehmigungsprozesse angestoßen und / oder Eskalationen eingeleitet werden können.

Revisionssicherheit: Jeder Schritt im Freigabeprozess – von der Beantragung über die Bewertung bis zur finalen Autorisierung – ist lückenlos und auditkonform zu protokollieren, um die Einhaltung der Governance-Vorgaben jederzeit nachweisen zu können.

2.8 Eventmanagement

Das Eventmanagement dient der zentralen Überwachung der Service-Landschaft. Der SIAM Broker muss hierbei als Konsolidierungsschicht agieren, die Events aus heterogenen Quellsystemen zusammenführt und bewertbar macht.

Konsolidierte Ansicht: Es soll eine zentrale, providerübergreifende Ansicht aller Monitoring-Events bereitgestellt werden. Ziel ist ein "Single Pane of Glass", das den aktuellen Status der gesamten Service-Kette in Echtzeit widerspiegelt.

Event-Korrelation: Um die Informationsflut zu bewältigen, soll das System in der Lage sein, zusammengehörige Events automatisiert zu korrelieren. Kritische Ereignisse, die auf dieselbe Ursache zurückzuführen sind, sollen detektierbar sein.

Überführung in Incidents: Die Lösung soll die automatisierte Erstellung von Incident-Tickets aus korrelierten Events unterstützen, um eine schnellstmögliche Störungsbeseitigung einleiten zu können.

Status-Dashboards: Für den internen Betrieb sowie für Berichtskonsumenten sollen Live-Dashboards bereitgestellt werden, die den aktuellen Service-Status transparent und intuitiv visualisieren (z. B. über Ampelsysteme). Der Service-Status des internen Betriebs stellt hierbei Informationen zum SIAM Broker selbst bereit, wohingegen der Status für Berichtskonsumenten Informationen korrelierter Events und Major Incidents konsolidiert darstellt.

2.9 Reporting & Performancemanagement

Das Reporting-Modul des SIAM Brokers stellt ein zentrales Kontrollinstrument zur Überwachung und Steuerung der Servicequalität sowie der vertraglich vereinbarten Leistungen dar. Es muss eine konsolidierte Sicht auf die gesamte Provider-Landschaft ermöglichen.

Die Lösung soll ein automatisiertes Berichtswesen bereitstellen, das über einfache Statusberichte wie folgt hinausgeht:

SLA/OLA/PLA-Monitoring: Das System soll in der Lage sein, Service Level Agreements (SLA), Operational Level Agreements (OLA) und Process Level Agreements (PLA) zu tracken. Hierzu sollen sowohl Einzelnachweise als auch Trendanalysen über definierte Zeiträume, beispielsweise wöchentlich, monatlich oder quartalsweise (von berechtigten Rollen/Nutzern) erzeugt werden können.

Provider-Performance-Vergleich: Um eine objektive Steuerung zu ermöglichen, sollen die Leistungen verschiedener Provider direkt miteinander vergleichbar sein. Dies beinhaltet die Auswertung von Ticket-Volumina, Durchlaufzeiten und Erstlösungsraten.

Langläufer-Analyse: Das System soll proaktiv "Langläufer" identifizieren – d.h. Tickets, deren Bearbeitungszeit kritische Schwellwerte überschreitet. Historische Daten sollen genutzt werden können, um saisonale Trends oder systematische Schwachstellen in der Service-Erbringung aufzudecken.

Interaktive Detailanalyse: Die Lösung muss es ermöglichen, von aggregierten Kennzahlen (Dashboards) direkt per Drill-Down in die zugrundeliegenden Datensätze und vordefinierten Detailfelder abzuspringen, um Ursachenanalysen effizient durchzuführen.

2.10 Administration & Konfiguration

Der SIAM Broker wird als zentrale organisatorische Einheit innerhalb des AG betrieben. Daher muss das System so ausgelegt sein, dass es mit minimalem Konfigurationsaufwand administriert werden kann.

Die Anforderungen an Systemadministration und Anpassungsfähigkeit sind im Folgenden beschrieben:

Low-Code/No-Code-Ansatz: Administrative Aufgaben wie die Anpassung von bestehenden Feldern, Feldinhalten, die Definition neuer Felder und Workflows und / oder die Änderung von Eskalationsregeln sollen vorzugsweise über grafische Oberflächen ohne tiefgreifende Programmierung möglich sein.

Erweiterte funktionale Anpassbarkeit: Über die Standard-Konfigurationsoberflächen hinaus soll die Lösung die Möglichkeit bieten, benutzerdefinierte Funktionen zu etablieren. Um komplexe Sachverhalte abzubilden, die sich nicht über die GUI realisieren lassen, muss das System die Einbindung von Skripten oder kundeneigenem Code (z.B. für komplexe Datenmanipulationen oder spezialisierte Logiken) unterstützen.

Zentrales Rollenmanagement: Die Administration muss die Konfiguration feingranularer Rollenmodelle (z. B. SIAM Broker Manager, Process Owner, Provider Coordinator) ermöglichen. Die Vergabe von Berechtigungen erfolgt nach dem "Need-to-know"-Prinzip.

Multi-Mandantenfähigkeit: Das System muss unterschiedliche organisatorische Einheiten oder Kundengruppen (z. B. verschiedene AOKs) logisch trennen können, während die zentrale Governance gewahrt bleibt.

2.11 Nichtfunktionale & Technische Anforderungen

In diesem Kapitel werden die qualitativen Anforderungen beschrieben, die den stabilen und sicheren Betrieb des SIAM Brokers gewährleisten.

2.11.1 Interoperabilität & API Management

Als zentrale Datendrehscheibe soll der SIAM Broker technologieoffen gestaltet sein.

Integration marktüblicher ITSM-Tools: Der SIAM Broker soll eine aufwandsarme, native Anbindung gängiger Ticket-Systeme unterstützen.

Template-basierte Konfiguration: Für mindestens 3 der folgenden Ticket-Systeme sind vordefinierte Integration-Templates (Konnektoren) bereitzustellen: ServiceNow, Jira Service Management, BMC, USU ITSM, HPSM, KIX. Diese sollen Best-Practice-Mappings für Entitäten (Incidents, Changes, Tasks) enthalten, sodass eine Basiskommunikation zwischen den Systemen ohne aufwendige Individualprogrammierung ("Out-of-the-Box") hergestellt werden kann.

Technologieoffene Schnittstellen: Über die Templates hinaus soll die Plattform über ein API-Gateway verfügen, das alle gängigen Industriestandards (insb. REST, SOAP, JSON und XML) unterstützt. Dies stellt sicher, dass auch proprietäre Lösungen und / oder Legacy-Systeme der Provider flexibel angebunden werden können.

Transformations-Layer: Das System soll in der Lage sein, ein- und ausgehende Datenströme in Echtzeit zu transformieren. Unterschiedliche Datenformate bzw. Feldbezeichnungen der Provider-Tools sollen über ein zentrales Mapping-Tool harmonisiert werden, um eine einheitliche Datenbasis im SIAM Broker zu gewährleisten.

2.11.2 Performance & Skalierbarkeit

Die Lösung muss für den unternehmensübergreifenden Einsatz performant ausgelegt sein.

Statusänderungen an Tickets müssen systemübergreifend in nahezu Echtzeit (mit einer Latenz von maximal 5 Sekunden) systemübergreifend synchronisiert werden. Die Benutzeroberfläche muss auf Nutzerinteraktionen (z.B. Klicks, Eingaben, Tab-Wechsel) mit einer Antwortzeit von maximal 500 Millisekunden reagieren.

Die Architektur soll sowohl horizontal als auch vertikal skalierbar sein, um die Anbindung weiterer Provider sowie steigende Ticket-Volumina ohne Performance-Verlust abzufangen.

2.12 Security, Datenschutz & Audit

Das System muss alle Vorgaben der DSGVO sowie die besonderen Anforderungen an den Schutz von Sozialdaten gem. Sozialgesetzbuch Zehntes Buch erfüllen, einschließlich verschlüsselter Datenübertragung und spezifischer Reporting-Funktionen zur Datennutzung.

Der AN muss in der Lage sein nach Vertragsabschluss ein Konzept zur Erfüllung datenschutzrechtlicher sowie sicherheitskritischer Vorgaben zu entwickeln und vorzulegen. Dieses umfasst insbesondere technische und organisatorische Maßnahmen sowie Regelungen zum Schutz besonders schützenswerter Daten. Der AN hat einen Datenschutzbeauftragten zu benennen und dessen Kontaktdaten dem AG bereitzustellen. Darüber hinaus sind feste Ansprechpartner für Datenschutz sowie für IT-Sicherheit zu benennen, die während der gesamten Vertragslaufzeit zur Verfügung stehen. Bei Bereitstellung der Lösung durch den AN ist sicherzustellen, dass die Verarbeitung und Speicherung personenbezogener Daten ausschließlich innerhalb der Europäischen Union erfolgt. Der AN hat dies verbindlich zu garantieren und entsprechende Nachweise vorzulegen.

Technisch muss das System zwingend dazu in der Lage sein, eine durchgängige Verschlüsselung der gesamten Kommunikationsstrecke vom Quellsystem über den SIAM Broker bis hin zum Satelliten-System abzubilden. Diese Funktionalität muss pro Schnittstelle optional konfigurierbar sein.

Zur Gewährleistung einer lückenlosen Revisionssicherheit müssen zudem sämtliche Transaktionen, Statusänderungen und administrativen Eingriffe manipulationssicher protokolliert werden, wobei die Auditierbarkeit durch ein feingranulares, rollenbasiertes Zugriffskonzept auf die Protokolldaten geschützt wird.

2.13 Migrationskonzept

Mit dem AN ist ein detailliertes Konzept zur Migrationsstrategie vereinbart, welches beschreibt, wie die Überführung der bestehenden Prozesse, Datenbestände sowie der operativ genutzten Integrationspunkte in den neuen SIAM Broker erfolgen, ohne den laufenden Betrieb zu gefährden.

Hierin ist definiert, welche historischen Daten im Rahmen der Datenmigration (Initial Load) in welcher Form übernommen werden. Der AN hat ferner ein Verfahren zur Harmonisierung von Bewegungsdaten beschrieben.

Während der Migrationsphase hat der AN sicherzustellen, dass die Kommunikation zwischen bereits migrierten und noch nicht migrierten Providern unterbrechungsfrei über Fallback-Szenarien oder temporäre Schnittstellen aufrechterhalten wird.

Der AN erbringt alle im Migrationskonzept (s. o.) beschriebenen sowie zur Zielerreichung notwendigen Migrationsleistungen, ohne den laufenden Betrieb zu gefährden.

3 Lizenzmodell und Softwareinformationen

3.0 Sprache, Dokumentation

Sämtliche Anwendungsdialoge, Benutzeroberflächen, Dokumente (Handbuch, Schulung, Support- und Release-Notes usw.) müssen in deutscher Sprache zur Verfügung gestellt werden.

Die fachlichen und technischen Dokumentationen müssen vom AN unverzüglich nach Zuschlag bereitgestellt werden. Die Dokumentationen sind in elektronischer Form gemäß Abschnitt 5 der EVB-IT Cloud-AGB 01.03.2026 zur Verfügung zu stellen. Für die Software müssen während der gesamten Vertragslaufzeit sowohl fachliche als auch technische Dokumentationen zur Verfügung stehen, die aktuell sind, also den jeweiligen Release-Stand berücksichtigen.

3.1 Software-/Anwendungs-Lösung

Die Lizenzbestimmungen müssen für den AG verständlich und in deutscher Sprache zur Verfügung gestellt werden. Weitergehende Informationen zur Software sollten verfügbar sein.

3.2 Anzahl Nutzer

Da es sich bei der bereitzustellenden Lösung um eine zentrale Service-Integration-Middleware handelt, differenziert sich der Nutzerkreis nach funktionalen Rollen und Zugriffstiefen. Die Software dient als Knotenpunkt zwischen dem AG, den AOKs sowie den beteiligten IT-Dienstleistern und Softwarelieferanten.

Das Lizenzmodell muss die in den folgenden Kapiteln beschriebene Struktur abbilden und hierbei flexibel skalierbar sein.

3.2.1 Funktionale Nutzergruppen

Nutzergruppe	Beschreibung	Anzahl Organisationen	Geschätzte User (Concurrent/Named)
Zentrale Administration & Governance	Vollzugriff auf Systemkonfiguration, API-Management, Master-Workflows und übergreifendes Reporting	1 (Zentraler Betrieb)	2
IT-Dienstleister	Zugriff auf relevante Ticketsystem-Schnittstellen und fachspezifische Abstimmungs-Workflows	5 (IT-Dienstleister)	10
Softwarelieferanten	Zugriff auf relevante Ticketsystem-Schnittstellen und fachspezifische	5 (Softwarelieferanten)	10

	Abstimmungs- Workflows		
Reporting & Stakeholder (AOKs)	Lesender Zugriff auf Status-Dashboards und Performance-Reports zur Steuerung der Servicequalität	12 (AOKs & strategische Partner)	60

3.2.2 Technische User

Neben den personellen Usern muss das Lizenzmodell die technische Kommunikation berücksichtigen:

Es ist von einer initialen Anbindung von mindestens 6 externen ITSM-Instanzen (1 IT-Dienstleister, 5 Softwarelieferanten) auszugehen.

Um künftiges Wachstum abzubilden, muss die Lösung in der Lage sein bis zu 20 Instanzen anzubinden. Für die Preisbewertung wird ein fiktiver Zuwachs auf bis zu 20 Schnittstellen (d.h. Anbindung von bis zu 20 Instanzen) über die Vertragslaufzeit angenommen. Die Mengenstaffel zur Preisermittlung ist dem Preisblatt zu entnehmen.

Zum aktuellen Planungsstand ist für die initiale Anbindung (innerhalb der ersten 12 Monate nach Zuschlag) von folgenden 6 Instanzen auszugehen:

- Monat 3: ServiceNow
- Monat 5: Jira
- Monat 8: Jira
- Monat 9: Jira
- Monat 10: ServiceNow
- Monat 11: Jira

Für den weiteren Projektverlauf (bis Monat 32) sieht die aktuelle Roadmap sukzessive Anbindungen weiterer Instanzen vor. Hierzu zählen nach derzeitigem Stand unter anderem: USU Valuation, Microfocus SMAX, SM4C, KIX, OTRS / TI Messenger, Xurrent 4me, Omnitacker, Novomind iAgent, SAP Fiori Frontend sowie ClickDoc.

Diese explizite Nennung der Zielsysteme und Dienstleister repräsentiert den derzeitigen Projektstand und dient dem AN zur fundierten Kalkulation und Aufwandsabschätzung für die bereitzustellenden Basis-Schnittstellen. Der Auftraggeber behält sich ausdrücklich vor, diese genannten Zielsysteme im Zuge der operativen Projektsteuerung und veränderten Providerlandschaften durch technisch vergleichbare ITSM- oder Umsysteme zu ersetzen oder die zeitliche Reihenfolge der Anbindung zu verschieben. Eine solche Anpassung der Roadmap gilt durch die Pauschalierung der Technologie-Konnektoren und Instanzen im Preisblatt (Positionen 1.1.A und 1.1.B) als vollumfänglich abgegolten.

3.2.3 Skalierungsoptionen

Aufgrund der dynamischen Marktsituation und möglicher Erweiterungen des Lieferantenportfolios muss die Lösung Optionen zur Erweiterung der Nutzerzahlen und Provideranbindungen enthalten.

Insbesondere die optionale Hinzunahme weiterer Softwarelieferanten und die Flexibilität bei der Verschiebung von Nutzerkontingenten sind in diesem Kontext zu berücksichtigen.

Das System muss auf ein automatisierter Transaktionsvolumen von mindestens 15.000 Einzeltransaktionen ausgelegt sein, ohne dass dies zu lizenzrechtlichen Restriktionen führt. Eine Einzeltransaktion ist als vollständiger Durchlauf eines fachlichen Datensatzes (z.B. Incident) definiert, bei dem sämtliche während seines Lebenszyklus anfallenden Statusänderungen und Updates (bidirektional) bereits inkludiert sind und kein erneutes Transaktionskontingent verbrauchen.

4 Wartung und Support

Wartung und Support müssen auf allen Stufen der Servicekette in deutscher Sprache, mindestens auf dem Niveau C1, erfolgen.

Wartung und Support werden für die Dauer von 48 Monaten ab Zuschlag erbracht.

Der reguläre Support wird an den Arbeitstagen von Montag bis Freitag jeweils von 07.00 bis 17.00 Uhr erbracht („Servicezeiten“). Gesetzliche bundeseinheitliche Feiertage gelten nicht als Arbeitstage. Weitergehende Anforderungen an den Support sind in den Kapiteln 4.1, 4.2 und 4.3 beschrieben.

4.0 Wartung

Für die Software muss über die gesamte Vertragslaufzeit die Wartung sichergestellt sein und erbracht werden. Das umfasst die Weiterentwicklung der Software (neue Versionen). Dies erfolgt über das Einspielen von Patches, Updates und Bugfixes sowie Installationen bei Release- und/oder Versionswechseln.

Der AN ist verpflichtet, folgende Programmstände für die Standardsoftware unaufgefordert und ohne Mehrkosten bereitzustellen, sobald sie am Markt verfügbar sind:

Patches, Updates, Upgrades und Releases.

Mit jeder Systemänderung (neue Version, Release, Patch) muss (vorab) eine entsprechende Dokumentation ausgeliefert werden, aus der die jeweiligen Änderungen und ggf. die sich hieraus ergebenden nötigen Anpassungstätigkeiten hervorgehen. Der AN ist verpflichtet diesbezüglich bei der Aktualisierung betroffener Dokumentationen (z. B. Sicherheitskonzept) ohne Mehrkosten mitzuwirken.

Die Wartung umfasst insbesondere die Bereitstellung von Patches, Updates, Bugfixes sowie neuen Releases oder Versionen.

Die Installation dieser Aktualisierungen muss sowohl durch den AN (nach Freigabe durch den AG) als auch durch den AG selbst durchgeführt werden können.

4.1 Support

Für den laufenden Betrieb der Software erbringt der AN Software-Support sowohl für die Anwendungsadministratoren als auch bei Störungen.

Bei kritischen Fehlern und allgemeingültigen Bugs/Problemen erfolgt eine proaktive Information. Zu kritischen Fehlern und allgemeingültigen Bugs/Problemen informiert der AN zudem anlassbezogen sowie regelmäßig, mindestens jedoch bis zur Behebung in einem Turnus, der den unter 4.2 sowie 4.3 definierten Reaktionszeiten für Supportanfrage- bzw. Störungsklassen entspricht.

Es besteht eine Kontaktmöglichkeit durch den AN an den AG per Telefon, E-Mail und Ticketsystem.

Für kritische Störungen ist eine 24/7 Rufbereitschaft sicherzustellen. Die Entstörung dieser Sachverhalte muss innerhalb von vier Stunden erfolgen.

Die in den Kapiteln 4.2 sowie 4.3 beschriebenen Reaktions- und Wiederherstellungszeiten beginnen mit dem Eingang einer qualifizierten Meldung des Sachverhalts über einen der definierten Support Kanäle.

Die Reaktionszeit ist die Zeitspanne zwischen Meldung des Sachverhalts und Beginn der Störungsbehebung durch einen qualifizierten technischen Supportmitarbeiter. Die Wiederherstellungszeit ist die Zeitspanne zwischen Meldung des Sachverhalts und der vollständigen Behebung der Störung oder Bereitstellung eines Workarounds, der den operativen Betrieb uneingeschränkt ermöglicht.

4.2 Supportanforderungen

Die nachfolgenden Anforderungen gelten für alle Supportanfrageklassen:

- Die Supportanforderung durch den AG erfolgt per E-Mail, über ein Ticketsystem des AN.
- Über Verzögerungen in der Bearbeitung von Supportanfragen informiert der AN den AG unverzüglich.
- Der AN sendet innerhalb der Reaktionszeit eine Eingangsbestätigung per E-Mail oder über ein Ticketsystem des AN.

Die maximalen Reaktionszeiten gliedern sich nach den folgenden Supportanfrageklassen:

Supportanfrageklasse	Beschreibung	Reaktionszeit	Maßgeblicher Zeitraum für Reaktionszeit	Beispiel
Prio 2	Hoch	4 Stunden	Servicezeiten	Unterstützung bei Konfiguration / Administration
Prio 3	Niedrig	8 Stunden	Servicezeiten	Allgemeine Anfragen, Auskünfte, Dokumentation

4.3 Anforderungen an das Störungsmanagement

Die nachfolgenden Anforderungen gelten für alle Störungsklassen:

- Die Meldung von Störungen durch den AN erfolgt per E-Mail, über ein Ticketsystem des AN oder telefonisch. Der AN sendet innerhalb der Reaktionszeit eine Bestätigung der Störungsannahme per E-Mail.
- Behobene Störungen sind als erledigt per E-Mail zu melden. Verzögert sich der Störungsbehebungsprozess, so informiert der AN den AG unverzüglich und teilt die Verzögerungsgründe sowie den voraussichtlichen Termin der Störungshebung mit. Der Adressat bzw. die zu nutzende E-Mail-Adresse wird im Implementierungsprojekt mitgeteilt.
- Der AN ist zu den vereinbarten Servicezeiten (siehe Kap. 4) über eine zentrale Rufnummer telefonisch durchgehend zu erreichen. Über diese Rufnummer müssen Informationen über den Status einer gemeldeten Störung abrufbar sein. Ebenso muss es möglich sein, auf dem beschriebenen Weg weitere Informationen an eine bereits gemeldete Störung (unabhängig davon, ob die Erstmeldung der Störung per E-Mail, per Ticketsystem oder telefonisch aufgegeben wurde) anzuhängen.
- Der AN ist darüber hinaus für Störungen höchster Priorität über eine zentrale Rufnummer telefonisch 24/7 zu erreichen. Über diese Rufnummer müssen Informationen über den Status einer gemeldeten Störung abrufbar sein. Ebenso muss es möglich sein, auf dem beschriebenen Weg weitere Informationen an eine bereits gemeldete Störung (unabhängig davon, ob die Erstmeldung der Störung per E-Mail, per Ticketsystem oder telefonisch aufgegeben wurde) anzuhängen.
- Mängelmeldungen werden wie Störungsmeldungen behandelt.
- Über Verzögerungen in der Bearbeitung von Störungsmeldungen informiert der AN den AG unverzüglich.

Die maximalen Reaktions- und Wiederherstellungszeiten gliedern sich nach folgendem Schema:

Störungs- klasse	Beschreibung	Reaktionszeit	Wiederherstellungs- zeit	Maßgeblicher Zeitraum für Reaktions- & Wiederherstellungs- zeit	Beispiel
Prio 1	Kritisch	2 Stunden	4 Stunden	24/7	Systemausfall, keine Replikation von Entitäten
Prio 2	Hoch	4 Stunden	8 Stunden	Servicezeiten	System- einschränkung mit funktionaler Beeinträchti- gung
Prio 3	Niedrig	8 Stunden	-	Servicezeiten	Sonstige Beeinträchti- gung

5 Weitere Leistungen

Sämtliche im Folgenden beschriebenen Leistungen, einschließlich Workshops, Schulungen, Handbücher, Dokumentationen, sind in deutscher Sprache, mindestens auf dem Niveau C1, zu erbringen.

5.0 Implementierungsprojekt / Customizing

Zur Sicherstellung einer effizienten Projektsteuerung benennt der AN für die gesamte Dauer des Implementierungsprojekts einen zentralen Projektleiter. Dieser fungiert als primärer Ansprechpartner für den AG. Zu seinen Kernaufgaben gehört die proaktive Steuerung und Koordination aller angeforderter Beistelleistungen des AG, um einen reibungslosen Informationsfluss und die Einhaltung des Zeitplans sicherzustellen.

Der im Folgenden skizzierte Zeitplan zur Projekt-Roadmap ist verbindlich.

Nach Zuschlagserteilung beginnt das Implementierungsprojekt, das in mehrere aufeinanderfolgende Phasen unterteilt ist. Die technische Bereitstellung von Konnektoren und Schnittstellen-Templates erfolgt hierbei sukzessive und bedarfsgerecht orientiert an den jeweiligen Pilotierungen bzw. Migrationswellen. Eine vollumfängliche Bereitstellung sämtlicher Konnektoren ab Zuschlagserteilung ist nicht erforderlich.

Das Implementierungsprojekt gliedert sich in folgende Phasen (alle Zeitangaben beziehen sich auf den Zeitpunkt der Zuschlagserteilung = Z:

Phase 1: Vorbereitung & Konzeption (Z bis Z + 3 Monate)

Der AN unterstützt bei der Verabschiedung des Governancemodells und der Erstellung der Feinspezifikation für den „MVP Incident“. Der „MVP Incident“ umfasst die Etablierung eines medienbruchfreien, übergreifenden Incident-Management-Prozesses. Gemeinsam mit dem AG wird bis zum Zeitpunkt Z + 4 Monate das fachliche operative Betriebsmodell final festgelegt.

Phase 2: MVP (Z + 2 Monate bis Z + 4 Monate)

Technische Installation: Die Bereitstellung und Erreichbarkeit der SIAM Broker-Instanz muss bis zum Zeitpunkt Z + 3 Monate abgeschlossen sein. In dieser Phase erfolgt das Customizing gemäß den Anforderungen des AG (Konfiguration, Workflows, Felder). Die Bereitstellung des notwendigen Konnektors zum ITSM-System des AG sowie dessen technische Anbindung muss bis zum Zeitpunkt Z + 5 Monate implementiert, die Datenmigration abgeschlossen und der Datenaustausch aufgenommen sein.

Phase 3: Pilotierung (Z + 4 Monate bis Z + 6 Monate)

Anbindung von einem weiteren Provider und Migration bis zum Zeitpunkt Z + 5 Monate unter Produktivsetzung des ersten spezifischen Provider-Konnektors. Aktivierung des Basis-Reportings (SLA/OLA-Dashboards) bis zum Zeitpunkt Z + 6 Monate. Der Pilotbetrieb endet mit der Abnahme und dem Abschluss der Hypercare-Phase zum Zeitpunkt Z + 7 Monate.

Phase 4: Rollout (Z + 7 Monate bis Z + 19 Monate)

Anbindung und Migration der direkten IT-Dienstleister Welle A bis Z + 10 Monate und der IT-Dienstleister Welle B bis Z + 13 Monate. Die hierfür notwendigen technischen Schnittstellen-Templates sind jeweils 6 Wochen vor Beginn der jeweiligen Welle durch den AN bereitzustellen. Die vollständige Ablösung der Altintegrationen muss bis zum Zeitpunkt Z + 19 Monate abgeschlossen sein.

Phase 4: Rollout (Z + 20 Monate bis Z + 48 Monate)

Anbindung und Migration weiterer IT-Dienstleister Welle C bis Z + 48 Monate. Die hierfür notwendigen technischen Schnittstellen-Templates sind jeweils 6 Wochen vor Beginn der jeweiligen Welle durch den AN bereitzustellen.

Im Rahmen eines Implementierungsprojektes erfolgt nach Beauftragung der Leistung die Installation der Softwarelösung und nachgelagert bzw. zeitgleich das Customizing.

Die Erstdokumentation (inkl. Rollen- / Berechtigungs- und Sicherheitskonzept) ist spätestens zur technischen Installation mit belastbarem Inhalt und einem Fertigstellungsgrad von 70% vorzulegen sowie bis zur produktiven Pilotierung zu finalisieren.

Der AN muss im Rahmen eines Einführungsworkshops die Customizing-Möglichkeiten beratend und nach der Methode „Best Practices“ gemeinsam mit den Administratoren des AG erarbeiten und definieren. Der AN führt anschließend Customizing gemeinsam mit den Administratoren des AG durch und dokumentiert die Durchführung entsprechend. Das schließt gleichzeitig eine Schulung der Administratoren ein (siehe auch Kapitel 5.1 Modul 1). Der Termin für den Einführungsworkshop wird 5 Arbeitstage nach Zuschlagserteilung durch den AN abgestimmt. In diesem Komplex werden auch Inhalte für adressatengerechte Schulungsunterlagen (siehe Kapitel 5.1 Module 2 und 3) abgestimmt.

Parallel zum Customizing muss die Dokumentation der umgesetzten Konfiguration und Parametrisierung sowie des eingeführten und umgesetzten Rollen- und

Berechtigungskonzeptes erstellt und spätestens mit der produktiven Pilotierung in elektronischer Form zur Verfügung gestellt werden.

5.1 Schulungen

Der AN erbringt Schulungen, die auf die jeweiligen Projektphasen abgestimmt sind.

Zu den Schulungen und den verschiedenen Modulen müssen Schulungsunterlagen, Handbücher oder Vergleichbares (soweit möglich je Modul) bis zum Zeitpunkt der Schulungen und vor der produktiven Pilotierung zur Verfügung gestellt werden, die in einer digitalen Ausführung im PDF-Format zu liefern sind. Der AN schult das im Folgenden näher beschriebene Modul 2 nach der Konzeptionierung des Systems. Für die Endanwender soll ein FAQ mit den Inhalten der Funktionalitäten der Softwareanwendung zur Verfügung gestellt werden. Teilnehmer, Inhalte, Umfang und Terminierung der Schulungen erfolgen in Absprache mit dem AG. Die im Folgenden genannte Aufgliederung ist als Orientierung zu verstehen und im Schulungskonzept durch den AN näher zu beschreiben.

Modul 1: Administratorenschulung (Z + 3 Monate – 3 Termine à 4 Stunden):
Durchführung im Rahmen der technischen Installation und des MVP-Customizings.
Ziel ist die Befähigung zur eigenständigen Verwaltung von Rollen, Berechtigungen, Import/Export von Daten sowie der Bedienung und Konfiguration der Anwendung.

Modul 2: Multiplikatorenschulung (Z + 3 Monate – 3 Termine à 2 Stunden):
Ausbildung von Key-Usern auf AG-Seite, um die Toolfunktionalitäten in die Breite zu tragen.

Modul 3: Providerschulung (laufend ab Phase 3 – 10 Termine à 2 Stunden):
Ausbildung von Key-Usern auf Provider-Seite. Bereitstellung von Materialien (Handbücher, FAQs, digitale Unterlagen im PDF-Format).

5.2 Weitere Unterstützungsleistungen

Nach Abschluss des Implementierungsprojekts / Customizings gemäß Kapitel 5.0 und der initialen Schulungen gemäß Kapitel 5.1 muss der AN weitere Unterstützungsleistungen (z. B. spätere Customizing- und/oder Schulungsleistungen) auf Anforderung des AG erbringen. Der AG stellt hierzu ein Abrufkontingent von 240 Beratungsstunden bereit, welches während der Vertragslaufzeit anlassbezogen durch den AG abgerufen werden kann. Dieses Kontingent stellt einen voraussichtlichen Bedarf an Präsenz oder Remote-Stunden dar und gilt als fiktive Schätzung als Grundlage für die Preisermittlung. Der tatsächliche Abruf sowie die zeitliche Verteilung der Leistungen innerhalb der Vertragslaufzeit erfolgen anlassbezogen durch den AG.

5.3 Leistungsort

Die Leistungen gemäß Kapitel 5.0 bis 5.2 werden, soweit nicht anders vereinbart, remote bzw. mittels Webkonferenzen erbracht.

Für den Fall, dass zur Leistungserbringung die Präsenz des AN in den Räumlichkeiten des AG bzw. der AOK erforderlich oder besser geeignet ist, wird die Leistungserbringung vor Ort

- im Fall von Kapitel 5.0 und 5.1 vom AN ohne Mehrkosten durchgeführt
- im Fall von Kapitel 5.2 gesondert vom AG beauftragt.

Etwaige Vor-Ort-Termine finden schwerpunktmäßig an den Standorten Frankfurt, Stuttgart oder Ludwigsburg statt.

6 Governance

6.0 Datenschutz

Die Anforderungen sind im EVB-IT Cloud Vertrag und dessen Anlagen beschrieben.

6.1 Informationssicherheit

Die erforderlichen Formulare für die Informationssicherheit müssen unterzeichnet sein, bevor z.B. Installationsarbeiten durch den AN durchgeführt werden. Die initiale Dokumentation muss bis zum Installationsabschluss finalisiert sein. Zu Beginn der Implementierung muss mindestens eine belastbare initiale Dokumentation vorgelegt werden.

6.1.1 Informationsklassifizierung

Die in die Anwendungen eingebrachten Dateninhalte werden aufgrund möglicher Sozialdaten u.a. personenbezogener Daten als ‚Vertraulich‘ klassifiziert. Entsprechend der gegebenen Informationsklassifizierung hat der AN sowohl für die Installations-, Support-, Wartungs- und Reparaturarbeiten für jede hier involvierten Personen eine Verschwiegenheitserklärung (NDA) gegenüber dem AG zu vereinbaren.

Die Verschwiegenheitserklärung muss vor Einsatz der betreffenden Personen im Fall des Vertragsschlusses in Textform (d.h. per Fax oder per eingescanntem unterschriebenem PDF-Dokument per E-Mail) vorliegen. Das unterschriebene Original ist in jedem Fall nachzureichen.

6.1.2 Einhaltung bestehender Richtlinien zur Informationssicherheit

Aufgrund der ISO 27001-Zertifizierung des AG muss die eingesetzte Software die auf ISO 27001 basierenden Informationssicherheitsrichtlinien des Auftraggebers erfüllen. Der AN hat dies im Rahmen der Abnahme nachzuweisen. Insbesondere sind nachfolgende Anforderungen zur Informationssicherheit zu erfüllen:

6.1.2.1 Schwachstellenmanagement

Der AN betreibt für alle bereitgestellten Hard- und Softwarekomponenten ein wirksames und etabliertes Schwachstellenmanagement. Die Bewertung der Schwachstellen hat nach dem CVSS (common vulnerability scoring system) oder einem vergleichbaren Standard zu erfolgen.

Der AG wird über das Auftreten von Schwachstellen seitens des AN unverzüglich informiert und der AN wird – soweit möglich – kompensierende Maßnahmen vorschlagen und setzt diese nach Abstimmung mit dem AG um. Der Meldeprozess ist abzustimmen.

6.1.2.2 Sichere Verschlüsselungsverfahren und Zertifikate

Es dürfen ausschließlich sichere Verschlüsselungsverfahren eingesetzt werden, deren Funktionstüchtigkeit und Sicherheit sich im breiten Einsatz bewährt haben. Die eingesetzten Verschlüsselungsverfahren müssen sicher und zuverlässig sein.

Sichere Verschlüsselungsverfahren sind insbesondere solche Verfahren, die gemäß den aktuellen Krypto-Richtlinien des BSI (insb. TR-02102, TR-03109-3) eingesetzt werden dürfen und bei denen ein praktikabler Angriff unwahrscheinlich ist.

Jedes digitale Zertifikat muss von der PKI des AG signiert werden. Selbstsignierte Zertifikate sind nicht zulässig.

6.1.2.3 Erstellung und Pflege notwendiger Konzepte und Dokumentationen

Im Rahmen der Implementierungsphase mit Customizing sind diverse Dokumentationen und Konzepte (siehe Kapitel 5.0) zu erstellen.

Alle Konzepte müssen nach Erstellung regelmäßig, mindestens halbjährlich, überprüft und aktualisiert werden. Bei wesentlichen Änderungen ist eine vorzeitige Aktualisierung durchzuführen. Der AN verpflichtet sich zur aktiven Mitarbeit bei der Erstellung und Pflege der Dokumente.

6.1.2.4 Aufrechterhaltung relevanter Zertifizierungen

Führt der AN zur Erfüllung relevanter Anforderungen System-, Unternehmens- oder Personenzertifizierungen an (bspw. ISMS nach ISO27001 zertifiziert, Partnerzertifizierung zu einem Hersteller), hat der AN diese über die gesamte Laufzeit aufrecht zu erhalten. Wird ein Zertifikat nicht verlängert oder zurückgezogen, ist der AG unverzüglich zu informieren.

6.1.2.5 Software-Aktualisierungsmanagement

Der AN ist verpflichtet, für die eingesetzte Softwarelösung „Service Integration and Management (SIAM) Broker“ ein kontrolliertes, etabliertes, dokumentiertes und wirksames Software-Aktualisierungsmanagement (Planung, Bewertung, Freigabe, Implementierung und Dokumentation von Softwareänderungen) zu betreiben.

Sämtliche Aktualisierungen – unabhängig davon, ob es sich um funktionale Erweiterungen, Fehlerbehebungen (Bugfixes), Sicherheitsaktualisierungen (Security Fixes) oder sonstige Änderungen handelt – sind dem AG mindestens zehn (10) Werktage vor ihrer Durchführung anzukündigen.

Abweichend hiervon sind Sicherheitsaktualisierungen zur Behebung kritischer Sicherheitslücken dem AG mindestens 24 Stunden vor ihrer Durchführung anzukündigen, soweit dies aufgrund der jeweiligen Gefährdungslage möglich und zumutbar ist. Erfordert eine akute Sicherheitsgefährdung eine unverzügliche Umsetzung der Sicherheitsmaßnahme, informiert der AN den AG hierüber unverzüglich unter Darlegung der Gründe; die Information erfolgt nach Möglichkeit vor der Durchführung, andernfalls unverzüglich nach deren Umsetzung.

Der AN stellt dem AG im Rahmen der Ankündigung Informationen in Textform zu den Auswirkungen der Änderungen, insbesondere im Hinblick auf Datenschutz, Informationssicherheit sowie relevante Änderungen an Schnittstellen oder Integrationen, zur Verfügung. Nach Durchführung der Aktualisierung übermittelt der AN dem AG die finalen Change-Logs.

Die Bereitstellung der Informationen kann auch über eine hierfür geeignete Portalfunktion erfolgen, sofern der AG über die Einstellung neuer oder aktualisierter Informationen unverzüglich in Textform (z. B. per E-Mail) benachrichtigt wird.

6.1.2.6 Informationssicherheit bei erforderlichen Zugängen und Zugriffen auf die Systeme

Für Installations-, Customizing-, Schulungs-, Support-, Wartungs- und Reparaturarbeiten müssen ggf. externe Personen und Dienstleister Zugang oder Zugriff auf die Systeme erhalten. Die auf den Systemen enthaltenen Daten des AG müssen vor dem Zugriff von Unbefugten geschützt werden. Zur Geheimhaltung und zur Überwachung der Fernzugriffe sind zwischen AN und AG vertragliche Regelungen zu treffen, insbesondere ist ein Fernzugriff nur temporär herzustellen für die Beseitigung einer Störung oder gegebenenfalls zur Durchführung einer Software-Aktualisierung. Der AN benennt alle zum Fernzugriff berechtigten Personen und zeigt Veränderungen an.

Im Bedarfsfall stellt der AG dem AN entsprechende Werkzeuge und Zugangsinformationen für einen sicheren Fernzugriff zur Verfügung, die dann vom AN zwingend einzusetzen sind. Eventuelle Abstimmungen erfolgen im Rahmen des Installations-, Implementierungs- und Customizing-Projekts.

6.1.2.7 Regelung zu Benutzerkonten und Passwörtern

Benutzerkonten des AG sowie des AN sind in das zentrale Identitäts- und Accountmanagement (IAM) des AG einzubinden. Die Anbindung an getrennte Systeme ist zulässig, sofern der AN eine sichere Identitätsverwaltung nachweist. Für Benutzerkonten des AG ist das Identitätsmanagement des AG zu verwenden. Ausnahmen sind grundsätzlich nur für Notfallkonten zulässig, um beispielsweise bei Ausfall des IAM weiterhin Systemzugriff zu erlangen.

Die Anbindung an getrennte Systeme ist zulässig, sofern der AN eine sichere Identitätsverwaltung nachweist. Für Benutzerkonten des AG ist das Identitätsmanagement des AG zu verwenden.

Für Passwörter zu Konten der Software sind die Anforderungen gemäß den aktuellen Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Insbesondere einzuhalten:

- Passwörter müssen eine ausreichende Mindestlänge aufweisen (mindestens 14 Zeichen) Die Mindestlänge für administrative Passwörter beträgt 20 Zeichen. Das Passwort muss folgende Zeichenarten enthalten: Großbuchstaben, Kleinbuchstaben, Ziffern, Sonderzeichen (nicht-alphanumerische Zeichen).
- Die Verwendung leicht zu erratender oder häufig verwendeter Passwörter ist zu verhindern (z. B. durch Abgleich mit bekannten Passwortlisten / Blacklists).
- Eine erzwungene regelmäßige Passwortänderung ohne konkreten Anlass ist nicht erforderlich.
- Für privilegierte Konten sowie für Zugriffe mit erhöhtem Schutzbedarf ist zusätzlich eine Multi-Faktor-Authentifizierung verpflichtend umzusetzen.

Bei Komponenten mit Kundenbezug können diese untereinander abweichen und müssen individuell umgesetzt werden können.

6.1.2.8 Schutz vor Schadsoftware

Der AN ist für die Absicherung der bereitgestellten Software gegen Schadsoftware verantwortlich; er stellt sicher, dass jede Softwareaus- und -nachlieferung im Vorfeld der Lieferung mit gängigen Prüfverfahren auf Schadsoftware kontrolliert wird.

6.1.2.9 Sicherheit von Anwendungen und Diensten

Der AN hat vor jedem ausgelieferten Release die eingesetzte Software und der von ihr initiierten Dienste auf Sicherheitsrisiken zu testen. Der AN wird dazu seine Software und die von ihr initiierten Dienste mindestens nach der OWASP Top 10 prüfen.

Sofern sich aus vorgenannten Tests Schwachstellen in der bereitgestellten Software und der von ihr initiierten Dienste ergeben, verpflichtet sich der AN diese aktiv zu beseitigen.

6.1.2.10 Zulässigkeit von Penetrationstests

Der AG behält sich vor, die installierten Komponenten im Rahmen eines Penetrationstests zu überprüfen. Der AN verpflichtet sich, aktiv an der Beseitigung der ermittelten Schwachstellen im Rahmen des Schwachstellenmanagements mitzuwirken. Sofern sich die Schwachstellen nicht auf die bereitgestellten Komponenten bezieht beschränkt sich die Mitwirkung auf entsprechende Hinweise.