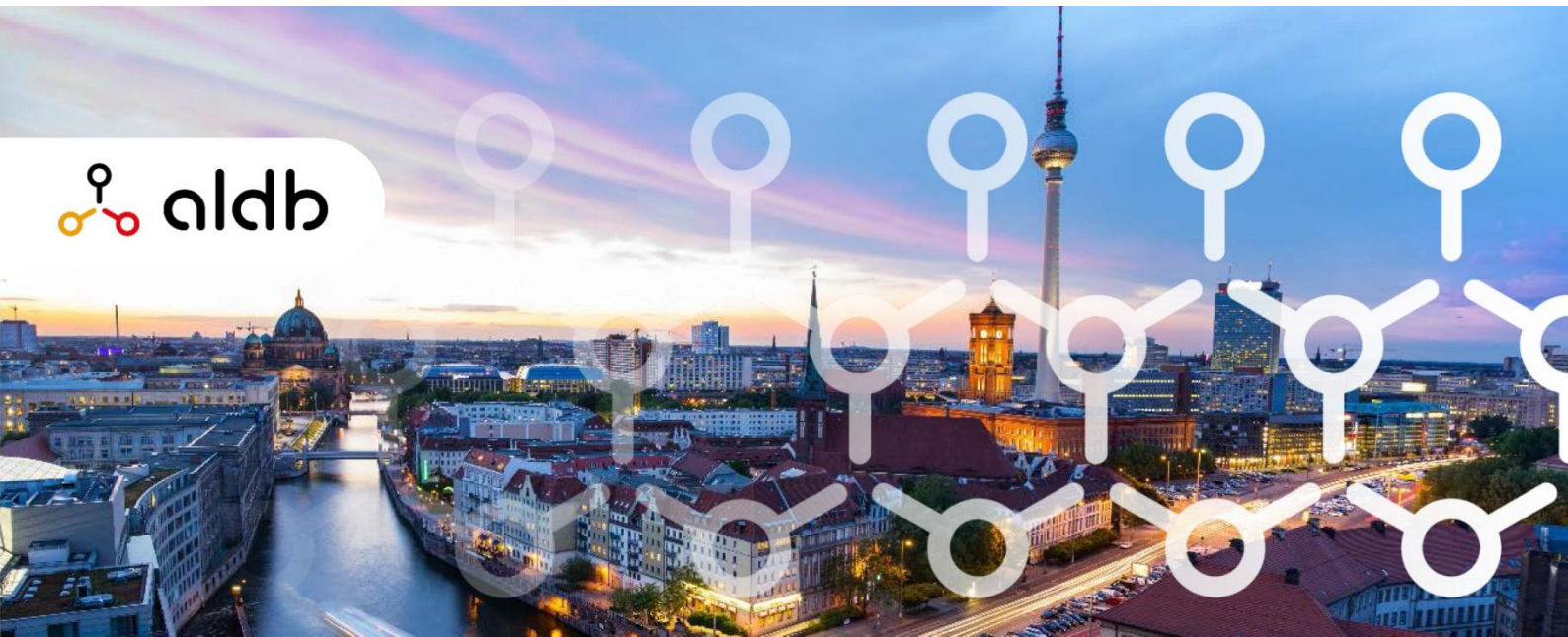




Leistungsbeschreibung Vg-26-030 Identity Access Management (IAM)

Inhaltsverzeichnis

1	Einleitung.....	3
1.1	Ausgangslage und Ziele.....	3
1.2	Aufteilung der Leistung.....	4
2	Backup.....	5
3	Anforderungen an das Identity Access Management System (IAM).....	6
3.1	On-Premise System.....	6
3.2	Datenschutz	6
3.3	Zugang zum IAM-Tool	6
4	Leistungsmerkmale des IAM	7
4.1	Grundlagen der Benutzerverwaltung	8
4.2	Joiner-, Mover- und Leaver-Prozesse	8
4.3	Rollen- und Berechtigungsmanagement	8
4.4	Access Management	9
4.5	Identity Governance	9
4.6	Administration	10
4.7	Workflow Management.....	10
4.8	Compliance, Reporting und Audit.....	11
4.9	Sicherheitsfunktionen.....	12
4.10	Benutzeroberfläche	12
4.11	Verfügbarkeit des IAM	12
4.12	Software-Support.....	13
5	Produktivsetzung	13
6	Exit-Management.....	13

1 Einleitung

Die ALDB GmbH ist eine 100%ige Tochter der BDBOS mit derzeit rund 420 Mitarbeitern.

Wir betreiben das weltweit größte TETRA-Kommunikationsnetz für die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) und die Autorisierten Stellen der Bundesländer und des Bundes.

Zur Verbesserung der Sicherheit der Informationssysteme, zur Automatisierung der Verwaltung von Benutzeridentitäten sowie zur Gewährleistung einer zentralen Steuerung von Zugriffsrechten plant die ALDB die Einführung einer **Identity & Access Management (IAM)-Lösung**.

Die Identity & Access Management-System dient der zentralen Verwaltung des gesamten Lebenszyklus von Benutzeridentitäten. Es ermöglicht die automatisierte Bereitstellung, Änderung und Entziehung von Zugriffsrechten, die Verwaltung von Rollen und Berechtigungen sowie die Unterstützung standardisierter Genehmigungsprozesse für den Zugriff auf IT-Systeme und Anwendungen. Ziel ist es, die Informationssicherheit zu erhöhen, administrative Prozesse zu vereinfachen und eine einheitliche, revisionssichere Verwaltung aller Benutzeridentitäten und Berechtigungen sicherzustellen.

1.1 Ausgangslage und Ziele

Derzeit verwaltet die ALDB-Benutzeridentitäten, Rollen und Zugriffsberechtigungen über verschiedene bestehende Systeme und Dokumentationen. Ein wesentlicher Teil der Daten, Konfigurationen und administrativen Prozesse wird dabei manuell, unter anderem mithilfe von Excel-Dateien und weiteren Verwaltungsdokumenten, gepflegt. Die Verwaltung von Benutzerkonten, die Vergabe, Änderung und Entziehung von Berechtigungen sowie die Pflege von Rollen erfolgen größtenteils manuell. Dies erhöht das Risiko menschlicher Fehler, Inkonsistenzen, redundanter Datenhaltung sowie potenzieller Sicherheitsrisiken.

Ziel der Einführung einer **Identity & Access Management (IAM)-Lösung** ist die Etablierung einer zentralen Plattform zur Verwaltung sämtlicher Benutzeridentitäten, Rollen und Berechtigungen sowie die Standardisierung und Automatisierung aller damit verbundenen Geschäftsprozesse. Durch die Implementierung der IAM-Lösung sollen manuelle Tätigkeiten erheblich reduziert, menschliche Fehler minimiert, die Datenqualität und Konsistenz verbessert sowie die tägliche Administration innerhalb der komplexen Organisations- und IT-Landschaft der ALDB deutlich vereinfacht werden.

Die Lösung muss den gesamten Lebenszyklus von Benutzeridentitäten unterstützen – von der automatisierten Anlage neuer Benutzerkonten über die rollenbasierte Bereitstellung und Anpassung von Berechtigungen sowie organisatorische Änderungen bis hin zur Deaktivierung, Archivierung und endgültigen Löschung von Benutzerkonten. Gleichzeitig muss das System eine vollständige Historisierung sämtlicher Aktivitäten, Änderungen und Entscheidungen im Zusammenhang mit Benutzeridentitäten, Rollen, Berechtigungen, Zielsystemen und Anwendungen gewährleisten. Dadurch sind eine vollständige Revisionssicherheit, lückenlose Nachvollziehbarkeit sowie die Einhaltung aller geltenden Sicherheits-, Compliance- und gesetzlichen Anforderungen

sicherzustellen.

1.2 Aufteilung der Leistung

Das Projekt umfasst folgende Leistungsbestandteile:

a) Bereitstellung der IAM-Softwarelösung (On-Premise)

Der Auftragnehmer hat die angebotene Identity & Access Management (IAM)-Lösung als **On-Premise-Lösung** bereitzustellen. Hierzu gehören sämtliche Softwarelizenzen einschließlich aller Module und Funktionalitäten, die zur Erfüllung der in dieser Leistungsbeschreibung definierten, fachlichen, technischen und sicherheitsrelevanten Anforderungen erforderlich sind.

Die Lizenzierung muss die Verwaltung der vorgesehenen Anzahl von Benutzeridentitäten, Rollen, Berechtigungen, Zielsystemen und Anwendungen ermöglichen sowie eine bedarfsgerechte Skalierung zur Unterstützung zukünftiger Erweiterungen der IT-Landschaft der ALDB gewährleisten.

b) Beratungsleistungen, Implementierung und Integration

Der Auftragnehmer ist für die vollständige Planung, Implementierung, Konfiguration, Parametrisierung, Integration, Inbetriebnahme, Testunterstützung sowie die fachliche und technische Begleitung während der gesamten Projektlaufzeit verantwortlich.

Der Leistungsumfang umfasst insbesondere die Integration der IAM-Lösung in die bestehende IT-Infrastruktur der ALDB einschließlich der Anbindung aller vereinbarten Quell- und Zielsysteme, Active Directory, Microsoft Entra ID, Kubernetes-Umgebungen sowie weiterer geschäftskritischer Anwendungen. Darüber hinaus sind die Organisationsstruktur, das Rollen- und Berechtigungskonzept, Identity Lifecycle Management, Provisionierungs- und Deprovisionierungsprozesse, Genehmigungsworkflows, Access Requests, Rezertifizierungsprozesse sowie Audit- und Reportingfunktionen zu implementieren und zu konfigurieren.

Alle Implementierungs- und Integrationsarbeiten sind so durchzuführen, dass der laufende Geschäftsbetrieb der ALDB nicht beeinträchtigt wird.

c) Test

Nach der Zuschlagserteilung und vor der Produktivsetzung ist eine Testumgebung bereitzustellen, die der späteren Produktivumgebung weitestgehend entspricht.

Vor dem Go-Live sind umfassende funktionale, technische, integrative, sicherheitsrelevante sowie fachliche Abnahmetests durchzuführen. Erst nach erfolgreichem Abschluss sämtlicher Tests und der schriftlichen Freigabe durch die ALDB darf die Produktivsetzung erfolgen.

d) Migration

Der Auftragnehmer ist für die vollständige Planung, Durchführung und Dokumentation der Migration verantwortlich in Abstimmung mit der Auftraggeberin.

Im Rahmen der Migration sind sämtliche Benutzeridentitäten, Rollen, Berechtigungen, Organisationsstrukturen, Konfigurationen sowie alle für den Betrieb der IAM-Lösung erforderlichen Daten vollständig, konsistent und ohne Datenverlust in das neue System zu übernehmen.

Die Migration ist so durchzuführen, dass Unterbrechungen des Produktivbetriebs auf ein Minimum reduziert werden und die Integrität aller Daten jederzeit gewährleistet bleibt.

e) Customer Support

Der vom Auftragnehmer zu erbringende IAM Customer Service umfasst den technischen Support, den Betrieb, die Wartung sowie die kontinuierliche Weiterentwicklung der implementierten Identity & Access Management-Lösung entsprechend den fachlichen und technischen Anforderungen der ALDB. Der Service erfüllt die Anforderung an KRITIS Anforderungen und ist deutschsprachigen Support.

Der Leistungsumfang umfasst insbesondere Incident- und Problem-Management, Fehleranalyse und Fehlerbehebung, Software-Updates, Hotfixes, Patches und sicherheitsrelevante Aktualisierungen sowie Unterstützung bei Konfigurationsänderungen, Change Requests, Erweiterungen und der Integration zusätzlicher Quell- und Zielsysteme.

Darüber hinaus unterstützt der Auftragnehmer die ALDB bei der Optimierung bestehender Identity- und Access-Management-Prozesse, der Weiterentwicklung des Rollen- und Berechtigungskonzeptes sowie bei der Umsetzung neuer fachlicher und regulatorischer Anforderungen.

2 Backup

Der Auftragnehmer hat ein Backup- und Wiederherstellungskonzept für die Identity & Access Management (IAM)-Lösung bereitzustellen und umzusetzen, um den Schutz, die Verfügbarkeit sowie die Wiederherstellbarkeit sämtlicher System- und Konfigurationsdaten im Falle von Störungen, Datenverlusten oder sonstigen ungeplanten Ereignissen sicherzustellen.

Sämtliche Backup-Daten sind verschlüsselt zu speichern und entsprechend den BSI IT Grundsatz der ALDB gegen unbefugten Zugriff zu schützen. Die Sicherungen sind auf einer physisch oder logisch von der Produktivumgebung getrennten Infrastruktur abzulegen, um auch im Falle eines schwerwiegenden Systemausfalls oder einer Kompromittierung der Produktivumgebung eine Wiederherstellung der IAM-Lösung sicherzustellen.

Die Erstellung der Datensicherungen hat automatisiert und ohne Beeinträchtigung des laufenden Produktivbetriebs zu erfolgen. Dabei muss sowohl eine vollständige Wiederherstellung der gesamten IAM-Plattform als auch die gezielte Wiederherstellung einzelner Systemkomponenten oder Datenbestände möglich sein.

Die Aufbewahrungsfristen, Rotationszyklen und die Löschung von Backup-Daten richten sich nach den Sicherheitsrichtlinien, den gesetzlichen Anforderungen sowie den standardisierten Vorgaben in der EU.

3 Anforderungen an das Identity Access Management System (IAM)

Alle hier beschriebenen Leistungen müssen von der Software ausgeführt. Die genauen Beschreibungen zu allen Anforderungen sind dem Anforderungskatalog zu entnehmen.

3.1 On-Premise System

Die IAM-Lösung ist als **On-Premise-Lösung** innerhalb der IT-Infrastruktur der ALDB zu implementieren.

Der Auftragnehmer kümmert sich um die Installation, Konfiguration, Integration und Inbetriebnahme der Lösung und arbeitet dabei eng mit ALDB zusammen. Zusätzlich ist der Auftragnehmer dafür verantwortlich, die IAM-Lösung an alle vereinbarten Quell- und Zielsysteme anzubinden, die zuvor von ALDB gewährt wurden. Alle von der IAM-Plattform verarbeiteten Daten sind ausschließlich innerhalb der IT-Infrastruktur der ALDB zu speichern und durch geeignete Maßnahmen hinsichtlich Datensicherheit, Datensicherung sowie Zugriffsschutz zu schützen.

3.2 Datenschutz

Die IAM-Lösung muss die Anforderungen der **Datenschutz-Grundverordnung (DSGVO)** sowie der jeweils geltenden nationalen Datenschutzbestimmungen vollständig erfüllen.

Der Zugriff auf personenbezogene und geschäftsrelevante Daten darf ausschließlich auf Grundlage definierter Rollen und Berechtigungen erfolgen und muss den Prinzipien **Need-to-Know** sowie **Least Privilege** entsprechen.

Die Lösung muss sicherstellen, dass Organisationsstrukturen, Rollen, Berechtigungen sowie sonstige vertrauliche Informationen der ALDB vor unbefugtem Zugriff geschützt sind. Der Export von Organisationsstrukturen und sensiblen Daten darf ausschließlich autorisierten Administratoren möglich sein.

3.3 Zugang zum IAM-Tool

Der Zugriff auf die IAM-Lösung ist nur über eine gesicherte webbasierte Benutzeroberfläche und verschlüsselte HTTPS-Kommunikation in eine geschlossene Umgebung (OnPrem) zulässig

Die Lösung muss den Zugriff für alle Benutzergruppen entsprechend ihrer Rollen und Berechtigungen ermöglichen.

Die Nutzung der IAM-Lösung muss über aktuelle Webbrowser sowie – soweit durch die angebotene Lösung unterstützt – auch über mobile Endgeräte möglich sein

- a) Passwortschutz

Sofern die IAM-Lösung eine lokale Authentifizierung verwendet, müssen die Vergabe, Änderung und das Zurücksetzen von Passwörtern über Self-Service-Funktionen erfolgen.

Die Lösung muss einen sicheren Prozess zur Initialisierung und Bestätigung von Passwortänderungen bzw. Passwort-Resets unter Verwendung zeitlich begrenzter Einmal-Links oder vergleichbarer sicherer Authentifizierungsmechanismen bereitstellen.

Sofern die IAM-Lösung an die bestehende Authentifizierungsinfrastruktur der ALDB angebunden ist, muss die Passwortverwaltung den Anforderungen des IT-Grundschutz Standards des BSI entsprechen.

b) Log-In

Das IAM muss über eine auditfähige Log-Funktion verfügen und ISO 9001 auditkonform aufgesetzt sein.

Für alle ALDB-Mitarbeiter mit einem Benutzerkonto werden zwei Anmeldeoptionen angeboten: Single-Sign-On (SSO) und eine Anmeldung mit einem generierten Passwort. Für SSO wird das Verfahren „openid connect“ zur Authentifizierung genutzt.

Externe Nutzer verwenden ausschließlich die Anmeldung mit einem generierten Passwort.

Bei der Anmeldung mit einem generierten Passwort besteht die Möglichkeit je nach Zielgruppe (intern und/oder extern) eine 2-fache-Authentifizierung einzurichten.

c) Browser

Als Standardbrowser verwendet die ALDB die Produkte Chrome und Mozilla Firefox, jeweils in der aktuellen Version. Darüber hinaus soll das neue SMS die Browserprodukte Microsoft Internet Explorer, Google Chrome und Apple Safari, ebenfalls in den aktuellen Versionen, als Desktop- und potenziellen Mobilversionen unterstützen.

d) Multiuser

Die IAM-Lösung muss den gleichzeitigen Betrieb durch mehrere Benutzer mit unterschiedlichen Rollen und Berechtigungen ohne Einschränkung der Performance, Stabilität oder Verfügbarkeit unterstützen.

4 Leistungsmerkmale des IAM

Alle geforderten Leistungen und Funktionalitäten der Identity & Access Management (IAM)-Lösung wurden den nachfolgend beschriebenen Funktionsbereichen zugeordnet und sind nachfolgend aufgeführt.

4.1 Grundlagen der Benutzerverwaltung

Diese Kategorie umfasst die zentrale Verwaltung digitaler Identitäten über ihren gesamten Lebenszyklus hinweg. Ziel ist die Konsolidierung, Synchronisierung und Pflege aller Benutzerinformationen aus unterschiedlichen Quellsystemen.

Enthält:

- Identity Lifecycle Management
- Benutzerverwaltung
- Identity Correlation
- Identity Refresh
- Identity Warehouse
- Verwaltung von Identitäten
- Mehrere Identitätsquellen

4.2 Joiner-, Mover- und Leaver-Prozesse

Diese Funktionen automatisieren den Ein- und Austritt von Mitarbeitern sowie organisatorische Veränderungen. Dadurch werden Benutzerkonten und Berechtigungen effizient und regelkonform verwaltet.

Enthält:

- Joiner Workflow
- Mover Workflow
- Leaver Workflow
- Automatische Benutzeranlage
- Automatische Aktualisierung von Benutzerdaten
- Automatische Deaktivierung von Benutzerkonten
- Automatisches De-Provisioning

4.3 Rollen- und Berechtigungsmanagement

Dieser Bereich ermöglicht die strukturierte Verwaltung von Rollen und Zugriffsrechten. Durch Rollenmodelle und automatische Zuweisungen wird die Administration vereinfacht und die Konsistenz der Berechtigungen sichergestellt.

Enthält:

- Business Roles
- IT Roles
- Birthright Roles
- Entitlements
- Rollenhierarchien
- Automatische Rollenzuweisung
- Rollenverwaltung
- Berechtigungsverwaltung

4.4 Access Management

Das Access Management steuert den Prozess der Beantragung, Genehmigung und Vergabe von Zugriffsrechten. Es unterstützt Self-Service-Funktionen sowie zeitlich begrenzte und kontrollierte Berechtigungen.

Enthält:

- Access Request
- Self-Service Access Request
- Approval Workflow
- Mehrstufige Genehmigungsprozesse
- Delegation von Genehmigungen
- Zeitlich begrenzte Berechtigungen

4.5 Identity Governance

Identity Governance sorgt für Transparenz, Kontrolle und Compliance im Umgang mit Identitäten und Berechtigungen. Regelmäßige Überprüfungen und Risikoanalysen unterstützen die Einhaltung von Sicherheits- und Governance-Anforderungen.

Enthält:

- Identity Governance
- Identity Governance Platform
- Access Governance

- Identity Security
- Access Certification
- Access Reviews
- Rezertifizierung
- Role Mining
- Risikoanalyse (Risk Score)

4.6 Administration

Diese Kategorie umfasst die technische und fachliche Administration der IAM-Lösung. Administratoren können Benutzer, Rollen, Schnittstellen, Richtlinien und Systemeinstellungen zentral verwalten.

Enthält:

- Benutzerverwaltung
- Rollenverwaltung
- Connector-Verwaltung
- Workflow-Konfiguration
- Policy-Verwaltung
- Systemkonfiguration

4.7 Workflow Management

Workflow Management ermöglicht die Modellierung und Automatisierung von IAM-Prozessen. Genehmigungen, Provisionierung, Eskalationen und Benachrichtigungen können standardisiert und effizient gesteuert werden.

Enthält:

- Workflow Designer
- Approval Workflows
- Provisioning Workflows
- Lifecycle Workflows
- Eskalationen
- Benachrichtigungen Integrationen

Integrationen stellen die Anbindung des IAM-Systems an bestehende IT-Landschaften sicher. Dadurch können Identitäten, Berechtigungen und Benutzerdaten systemübergreifend verwaltet werden.

Enthält:

- Active Directory
- LDAP
- REST API
- CSV-Import/Export
- SAP
- Oracle Database
- SQL-Server
- Kubernetes (Containers basiert)
- HR-Systeme (z. B. REXX)

4.8 Compliance, Reporting und Audit

Dieser Bereich unterstützt die Einhaltung regulatorischer Anforderungen und schafft Transparenz durch nachvollziehbare Berichte, Dokumentationen und Audit-Nachweise.

Enthält:

- DSGVO-Unterstützung
- ISO 27001 Zertifizierung
- Audit-Unterstützung
- Revisionssicher
- Dokumentation aller Genehmigungen
- Standard Reports
- Audit Reports
- Support (deutschsprachigen)
- Export von Reports (PDF, CSV, Excel)

4.9 Sicherheitsfunktionen

Die Sicherheitsfunktionen schützen Identitäten und Zugriffsrechte vor Missbrauch. Sie unterstützen Sicherheitsrichtlinien, Compliance-Anforderungen und das Prinzip der minimalen Rechtevergabe.

Enthält:

- Role-Based Access Control (RBAC)
- Segregation of Duties (SoD)
- Audit Logs (Protokolldaten zur Weiterverarbeitung an das SIEM (IBM QRadar))
- Audit Logs Dokumentation
- Audit Logging (Lückenlose Protokollierung aller relevanten Aktivitäten und Änderungen)
- Least-Privilege-Prinzip

4.10 Benutzeroberfläche

Die Benutzeroberfläche bietet eine intuitive und effiziente Interaktion mit dem IAM-System. Self-Service-Funktionen und übersichtliche Dashboards erhöhen die Benutzerfreundlichkeit und Akzeptanz. [

Enthält:

- Webbasierte Benutzeroberfläche
- Self-Service Portal
- Dashboard
- Suchfunktion
- Intuitives Design als User Experience (einfach)
- Service Level und Kennzahlen

4.11 Verfügbarkeit des IAM

Die IAM-Lösung ist grundsätzlich für einen Betrieb von **24 Stunden an sieben Tagen pro Woche (24/7)** auszulegen.

Die monatliche Verfügbarkeit der produktiven IAM-Lösung muss mindestens **95 %** betragen. Die Verfügbarkeit ist anhand der vereinbarten Betriebszeit zu messen und nachvollziehbar zu dokumentieren.

Bei der Berechnung der Verfügbarkeit dürfen ausschließlich im Voraus abgestimmte und angekündigte Wartungsfenster unberücksichtigt bleiben. Ungeplante Ausfälle, Störungen einzelner

zentraler Komponenten sowie Einschränkungen wesentlicher IAM-Funktionen gelten als Nichtverfügbarkeit.

4.12 Software-Support

Abgedeckte Bereiche: Der Support-Service stellt technischen Remote-Support bereit. Es müssen Ansprechpartner benannt werden, die im Ernstfall direkt kontaktiert werden können, um Fehler zu lösen

5 Produktivsetzung

Vor der Produktivsetzung der IAM-Lösung ist eine vollständige Test- und Abnahmephase gemäß der in Kapitel **1.2 Aufteilung der Leistung** beschriebenen Projektphasen durchzuführen. Der Auftragnehmer übergibt einen Projektplan.

Die Produktivsetzung wird vom Anbieter unter Begleitung von Projektverantwortlichen der ALDB DevSecOps (IAM), IT-Entwicklung, Active Directory Team, etc.) durchgeführt und geplanter Go-Live-Termin spätestens 01.12.2026

Vor der Inbetriebnahme muss der Auftragnehmer in einem von dem Auftragnehmer erstellten Abnahmeprotokoll nachweisen, dass sämtliche vereinbarten Funktionen, Integrationen, Schnittstellen, Workflows, Rollenmodelle, Berechtigungskonzepte sowie Sicherheits- und Compliance-Anforderungen erfolgreich implementiert, getestet und abgenommen wurden.

Vor der Produktivsetzung muss der Auftragnehmer sicherstellen, dass sämtliche Administratoren und IAM-Verantwortlichen geschult werden.

Helpdesk-Mitarbeiter, Role Owner, Application Owner, Business Owner sowie weitere berechtigte Benutzer entsprechend ihrer jeweiligen Rolle müssen bis Ende 2026 geschult werden. Ziel der Schulungen ist es, alle beteiligten Personen in die Lage zu versetzen, ihre administrativen und fachlichen Aufgaben selbstständig und sicher wahrzunehmen.

Für die jeweiligen Rollen müssen durch den Anbieter im Rahmen der Integration des IAM-Lösung digitale Trainingsunterlagen bereitgestellt werden, welche für die Aufgleisung neuer Mitarbeiter/Nutzer in den jeweiligen Rollen im Nachgang an die Produktivsetzung verwendet werden können. Die Schulungsunterlagen werden in elektronischer Form in einem weiterbearbeitbaren Format (z.B. Word) bereitgestellt.

6 Exit-Management

Der Auftragnehmer erstellt ein Exit-Konzept. In Abhängigkeit künftiger strategischer Entscheidungen des Auftraggebers muss das Exit-Konzept die Möglichkeiten bieten, das Identity Access Management System (IAM) zum Ende der Vertragslaufzeit in ein anderes System zu migrieren (zum Beispiel: alternativ die Bestandsdaten in einem offenen Format, z.B. XML, zur Übernahme in eine andere Lösung)

Die verlustfreie Übernahme, aller bis dahin erfassten Daten ist durch den Auftragnehmer ohne Beeinträchtigung der Leistungsmerkmale zu gewährleisten.