A03_V1_GIZ-DSM-_ISM-Tool_Leistungsbeschreibung

Inhaltsverzeichnis

1. Abkürzungsverzeichnis 4

2. Kontext 7
2.1 Zweck des Dokuments 7
2.2 Vorbemerkungen 7
2.3 Über die Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH 7
2.4 Ziel der Ausschreibung 8
2.5 Datenschutz in der GIZ 8
2.6 Informationssicherheit in der GIZ 9
2.7 Vorgehen im Projekt 9
2.8 Lizenzmodalitäten 9
2.9 Systemlandschaft der GIZ 10

3. Liefergegenstände 11
3.1 SaaS-Lösung für ISM und DSM 11
3.1.1 Funktionale Anforderungen (DSM) 11
3.1.2 Funktionale Anforderungen (ISM) 19
3.1.3 Modulübergreifende funktionale Anforderungen 28
3.1.4 Technische Anforderungen 35
3.1.5 Rollen- und Berechtigungskonzept 38
3.1.6 Mengengerüst 45
3.2 Leistungen in den Implementierungsphasen 47
3.2.1 Implementierungsplan 47
3.2.2 Einrichtung der Systemumgebung und Herbeiführung der Betriebsbereitschaft der SaaS-Lösung 47
3.2.3 Datenmodell-Analyse und Modellierung inklusive Update 48
3.2.4 Datenmigration 49
3.2.5 Beratung und Konzeptentwicklung bei der Einrichtung der Rollen- und Berechtigungen für ISM 52
3.2.6 Einrichtung der Rollen und Berechtigungen 52
3.2.7 Einrichtung der Schnittstellenanbindung an bestandsführende Tools der GIZ (CMDB und Prozessdaten) 53
3.2.8 Projektmanagement durch die Projektleitung des AN 53
3.2.9 Schulungen und Betriebsdokumentation 54
3.3 Optionale Leistungen während der Vertragslaufzeit 59
3.3.1 Schnittstellenanbindung 59
3.3.2 Beratungs- und Programmierleistungen 60
3.3.3 Aktivitäten zum Vertragsende 60
3.3.4 Audit-Management Modul (ISM) 60
3.3.5 Datenimport von Prozessdaten als Back-Up Lösung 61

3.3.6 Beratungsleistung Testmanagement....61
3.3.7 Beratungsleistung Projektmanagement....61
3.3.8 Weitere Schulungsleistungen....61

4. Personaleinsatz des AN....61
4.1 Projektleitung....61
4.2 Entwicklungspersonal....62
4.3 Testmanager....62

1. Abkürzungsverzeichnis

AG	Auftraggeber
AN	Auftragnehmer
API	Application Programming Interface
AuV	Auftragsverarbeitung
bmp	Windows Bitmap
BMZ	Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung
BPMN	Business Process Model and Notation
BSI	Bundesamt für Sicherheit in der Informationstechnik
CMDB	Configuration Management Database
CNIL	Commission Nationale de l'Informatique et des Libertés
CSV	Comma-separated values
DHD	Data Helpdesk
DMARC	Domain-based Message Authentication, Reporting and Conformance
DSB	Datenschutz-beauftragte
DSFA	Datenschutz-Folgenabschätzung
DS-GVO	Datenschutz-Grundverordnung
DSM	Datenschutzmanagement
DSMS	Datenschutzmanagementsystem
DSM-T	Datenschutzmanagement-Team
EDSA	Europäischen Datenschutzausschusses
EWR	Europäischer Wirtschaftsraum
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH
IAM	Identity Access Management
ISB	Informationssicherheitsbeauftragter
ISB-T	Informationssicherheitsbeauftragter-Team
ISK	Informationssicherheitskoordinatoren

ISM	Informationssicherheitsmanagement
ISMS	Informationssicherheitsmanagementsystem
ISM-T	Informationssicherheitsmanagement-Team
ISO	Information Security Officer
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission 27001
IT	Informationstechnologie
JDBC	Java Database Connectivity
JSON	JavaScript Object Notation
KPI	Key-Performance-Indicator
ODATA	Open Data Protocol
ODBC	Open Database Connectivity
OE	Organisationseinheit
PDF	Portable Document Format
PL	Projektleitung
Q&A	Questions and Answers
RPO	Recovery Point Objective (Maximal zulässiger Datenverlust nach einem System-Ausfall, gemessen in Zeit)
RTO	Recovery Time Objective (Maximal akzeptable Zeitspanne bis zur erneuten Bereitschaft nach einem Systemausfall)
SaaS	Software-as-a-Service
SAML	Security Assertion Markup Language
SCIM	System for Cross-Domain Identity Management
SLA	Service-Level-Agreement
SPF	Sender Policy Framework
SSO	Single-Sign-On
TIA	Transfer Impact Assessments
TLS	Transport Layer Security

TOM	Technische und organisatorischen Maßnahmen
VVT	Verzeichnis der Verarbeitungstätigkeiten
WBT	Web-based Training
XLSX	Excel Spreadsheet XML

2. Kontext

2.1 Zweck des Dokuments

In der Leistungsbeschreibung sind die Art und der Umfang der zu erbringenden Leistung wie auch die dazugehörigen Rahmenbedingungen beschrieben, welche die Bewerber bzw. Bieter für die Erstellung eines Angebotes und zur Realisierung der Leistungen benötigen. Die Leistungsbeschreibung wird im Anschluss des Vergabeverfahrens Teil des Vertrags zwischen dem AG und dem AN. Aus der Leistungsbeschreibung gehen die Anforderungen an die einzelnen Positionen im Preisblatt hervor. Außerdem verweist die Leistungsbeschreibung auf ergänzende Anforderungen zur Leistungserbringung, wie zum Beispiel auf Datenschutz- oder Sicherheitsbestimmungen.

2.2 Vorbemerkungen

Genderhinweis: Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in diesem Dokument die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

2.3 Über die Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH

Die Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH ist ein weltweit tätiges Bundesunternehmen. Sie unterstützt die Bundesregierung in der internationalen Zusammenarbeit für nachhaltige Entwicklung und in der internationalen Bildungsarbeit.

Als Dienstleister der internationalen Zusammenarbeit für nachhaltige Entwicklung und internationalen Bildungsarbeit engagiert sie sich weltweit für eine lebenswerte Zukunft. Die GIZ hat mehr als 50 Jahre Erfahrung in unterschiedlichsten Feldern, von der Wirtschafts- und Beschäftigungsförderung über Energie- und Umweltthemen bis hin zur Förderung von Frieden und Sicherheit. Das vielfältige Know-how des Bundesunternehmens GIZ wird rund um den Globus nachgefragt – von der deutschen Bundesregierung, Institutionen der Europäischen Union, den Vereinten Nationen, der Privatwirtschaft und Regierungen anderer Länder. Der Auftraggeber (AG) kooperiert mit Unternehmen, zivilgesellschaftlichen Akteuren und wissenschaftlichen Institutionen und trägt so zu einem erfolgreichen Zusammenspiel von Entwicklungspolitik und weiteren Politik- und Handlungsfeldern bei. Der Hauptauftraggeber der AG ist das Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ).

Alle Kooperationspartner schenken der GIZ ihr Vertrauen, Ideen für politische, gesellschaftliche und wirtschaftliche Veränderungen mit ihnen gemeinsam zu entwickeln, konkret zu planen und umzusetzen. Als gemeinnütziges Bundesunternehmen steht der AG für deutsche und europäische Werte. Gemeinsam mit ihren Partnern, den nationalen Regierungen weltweit sowie mit Kooperationspartner aus Wirtschaft, Wissenschaft und

Zivilgesellschaft, arbeitet die AG flexibel an wirksamen Lösungen, die Menschen Perspektiven bieten und deren Lebensbedingungen dauerhaft verbessern.

Die GIZ hat ihren Sitz in Bonn und Eschborn.

2.4 Ziel der Ausschreibung

Ziel der Ausschreibung ist die Beschaffung und Implementierung einer integrierten SaaS-Lösung, welche die aktuell betriebenen SaaS-Lösungen im Datenschutzmanagement (DSM) und Informationssicherheitsmanagement (ISM) ablöst und die in der Leistungsbeschreibung aufgeführten Anforderungen eines Datenschutzmanagementsystem (DSMS) und Informationssicherheitsmanagementsystem (ISMS) erfüllt und integriert.

Die SaaS-Lösung soll als Private Cloud beschafft werden inklusive Wartung Pflege und Support gemäß Kap. 3.1.4.1.7, dient hierbei den Einheiten DSM und ISM als Management Tool. Dabei muss im DSM die Führung des VVT, die Prüfung der TOM der eingesetzten Auftragsverarbeiter sowie Durchführung von DSFA enthalten sein. Im ISM müssen das Asset- und Risikomanagement abgedeckt werden.

In den Kapiteln 3.1.1 und 3.1.2 sind die Anforderungen der Aufgaben DSM und ISM in Form von Anforderungen an das System beschrieben. Die Leistungen in den Implementierungsphasen sind in Kap. 3.2, die Optionalen Leistungen während der Vertragslaufzeit in Kapitel 3.3 beschrieben.

Übergeordnet unterliegt das Tool der Einhaltung der Konformität der gesetzlichen Normen (DSGVO) und der ISO-Normen (ISO/IEC 27001 und ISO/IEC 27005) sowie deren systemische Abbildung.

Die Art der Implementierung sowie die der SaaS-Lösung zugrundeliegende Datenbank stellt sicher, dass der Zugriff auf alle Daten und Informationen durch DSM und ISM für die jeweiligen fachspezifischen Bearbeitungsprozesse jederzeit redundanzfrei möglich ist.

2.5 Datenschutz in der GIZ

Für die Umsetzung der Anforderungen aus der DS-GVO in der GIZ wurde die Gruppe DSM aufgebaut, die sowohl Beratungs- als auch Richtlinienkompetenz vereint, um eine DS-GVO-konforme Verarbeitung in der GIZ sicherzustellen. Zusammen mit dem ISM arbeitet das DSM im In- und Ausland als betriebssichernde Organisationseinheit in der Abteilung Informationssicherheits- und Datenschutzmanagement. Neben normativen Aufgaben im Sinne einer unternehmensweiten Governance, sorgt das DSM zusammen mit den datenverarbeitenden Stellen für die operative Umsetzung des Datenschutzes in der GIZ. Grundlagen des Handelns sind neben den gesetzlichen Regelungen, die Datenschutzleitlinie der GIZ und die innerbetrieblichen Prozesse und Regelungen.

Die GIZ setzt ein extern betriebenes Datenschutzmanagementsystem (SaaS-Lösung) ein, mit dem die gesetzlichen Anforderungen zur Führung eines VVT, der Prüfung der TOM der Auftragsverarbeiter und Durchführung von DSFA erfüllt werden. Über Online-Formulare werden Beratungsanfragen zum Datenschutz erstellt, die im Managementbereich des DSMS als Ticket dokumentiert und bearbeitet werden. Das aktuelle Tool bietet derzeit keinerlei Schnittstellen zu bestehenden Systemen der GIZ.

2.6 Informationssicherheit in der GIZ

Die GIZ beschäftigt sich seit 2020 weltweit mit dem Aufbau eines ISMS gemäß der Norm ISO 27001, welche als Multi-Site-Zertifizierung die Basis des Informationssicherheitsansatzes der GIZ darstellt. Zum gegenwärtigen Zeitpunkt sind das Headquarter der GIZ, ca. 40 Büros und mehrere hundert Projektstrukturen weltweit gemäß ISO/IEC 27001 zertifiziert.

Die anzuschaffende SaaS-Lösung muss daher in der Lage sein, die grundlegenden Anforderungen des genannten Standards zu erfüllen und den dezentralen Unternehmensaufbau abzubilden. Mit der Implementierung des neuen Tools soll die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen durch einen Risikomanagementprozess zur angemessenen Steuerung von Informationssicherheitsrisiken und Maßnahmen weiterhin gewährleistet werden. Zudem soll es ermöglichen, auf Basis der vorhandenen Daten KPIs und Reportings aufzubauen bzw. bestehende Auswertungen nachzubilden.

Im Zuge der ersten ISO-Zertifizierung wurde der Aufbau durch eine temporäre externe Lösung begleitet, in der derzeit das Asset- und Risikomanagement betrieben wird und die nun abgelöst werden soll. Die Audit-Management Prozesse sowie die Maßnahmennachverfolgung erfolgen außerhalb der aktuellen Lösung; Letztere wird zukünftig in der zu beschaffenden SaaS-Lösung abgebildet. Schnittstellen zu anderen Systemen bestehen derzeit in der aktuellen Form nicht und sollen erst im Rahmen der Neubeschaffung in Betrieb genommen werden.

2.7 Vorgehen im Projekt

Aus Projektplanungssicht ist die Umsetzung des Projektes in 2 Releases geplant:

- Release 1: DSM
- Release 2: ISM

Kapitel 3.2 „Leistungen in der Implementierungsphase“ und 3.3 „Optionale Leistungen während der Vertragslaufzeit ist die Zuweisung zu DSM bzw. ISM bei Relevanz erkennbar. Die Implementierungszeiträume sind wie folgt vorgesehen:

- DSM-Release: 2. Halbjahr 2027 bis Ende Januar 2028
- ISM-Release: Januar 2028 bis Ende Juni 2028

Die Angabe dieser Zeiträume dienen als Orientierung für die Bieter und stellen keine verbindliche Ressourcen- und Abrufzusage seitens des AG dar.

Die detaillierten Zeitpläne werden gemeinschaftlich zwischen AN und AG in den Kick-Off-Meetings zu Beginn der Implementierungsphase erarbeitet und abgestimmt – siehe Kapitel 3.2.1 Implementierungsplan.

2.8 Lizenzmodalitäten

Der AG ist interessiert an Unternehmenslizenzen oder Modullizenzen für DMS und ISM, die alle Kosten auf Jahres-Basis abbilden. Sofern ein Bieter ein solches Modell anbietet, ist dieses im Preisblatt einzutragen in den Positionen 1.1. – 1.3. Wenn der AN eine Unternehmenslizenz

und eine Modullizenz für DSM und ISM anbietet, sind die Kosten für die Unternehmenslizenz anzugeben.
Sofern der AG keine Gesamtunternehmenslizenz oder Modulbasierte Unternehmenslizenzen anbietet, können alternativ nutzerbasierte Lizenzen angeboten werden – Positionen 1.4 bis 1.7 im Preisblatt.
Zusätzlich erwartet der AG die Angabe zur Kostensituation der Bereitstellung für einer Staging- bzw. Spiegelumgebung und einer Testumgebung, Positionen 1.9 und 1.10 im Preisblatt gemäß Kapitel 3.1.4.1.5.

2.9 Systemlandschaft der GIZ

Ausstattung der Mitarbeiter

Alle Mitarbeiter verfügen über einen Firmenlaptop. Das Client-Betriebssystem bei der GIZ ist derzeit Windows 11 (Version 24H2 oder aktueller). Der Standard-Browser ist Microsoft Edge 64-Bit in der aktuellen Version (derzeit 145.0.3800.58 oder aktueller), d.h. die SaaS-Lösung muss uneingeschränkt in dieser Microsoft-Umgebung funktionieren. Aufgrund der weltweiten Präsenz der GIZ sowie der Vielzahl und Heterogenität der Projektländer werden auf mobilen Endgeräten die Betriebssysteme Android und iOS in verschiedenen Versionen eingesetzt. Der Minimumstandard (bei Android 12, bei iOS 16.7.8) für die eingesetzten Versionen wird sich an den Vorgaben von Microsoft Intune orientieren.

ERP-System (SAP)

Das ERP-System der GIZ ist seit 05.01.2026 S4Hana, wobei einige Module noch nicht durch S4Hana abgelöst sind. Diese werden sukzessive bis voraussichtlich Ende 2027 auch in S4Hana oder anderen SaaS Lösungen abgebildet werden.

IT-Identitäten

Die GIZ betreibt eine hybride Identitätsumgebung, welche sich derzeit zum größten Teil in der Microsoft Cloud (MS-Entra ID) befindet. Die Synchronisation an Drittsysteme wird durch eine große Anzahl an Protokollen und Konnektoren an die Microsoft Landschaft angebunden. Für einen Single-Sign-On (SSO) werden auch unterschiedliche Technologien angewandt (sowohl SAML 2.0 in Kombination mit SCIM als auch Open ID Connect mit OAuth 2.0).

3. Liefergegenstände

3.1 SaaS-Lösung für ISM und DSM

Dieser Abschnitt beschreibt die unmittelbaren funktionalen und technischen Anforderungen sowie die Anforderungen an das Rollen- und Berechtigungskonzept aus Sicht der Informationssicherheit und des DSM an die SaaS-Lösung.

3.1.1 Funktionale Anforderungen (DSM)

3.1.1.1 Meldungen zum Verzeichnis von Verarbeitungstätigkeiten (VVT)

3.1.1.1.1 Inhalte der Online-Formulare zur Erstellung und Bearbeitung der Meldungen zum VVT

Die SaaS-Lösung stellt ein Web-Interface mit Online-Formular zur Erstellung von Meldungen zum VVT durch die fachlich verantwortliche Stelle bereit. Die Erfassung der nach Art. 30 Abs. 1 DS-GVO erforderlichen Angaben sowie zusätzlicher, frei konfigurierbarer Informationen ist sicherzustellen.

Anforderungen:

- Funktionen zur Erstellung einer Meldung der Verarbeitungstätigkeit durch die datenverantwortliche Stelle (alle Mitarbeitenden der GIZ) per Online-Formular anhand vom AG konfigurierbarer Kriterien müssen vorhanden sein.
- Eine vollständige Erfassung aller nach Art. 30 DS-GVO erforderlichen Angaben muss möglich sein.
- Eine Klassifizierung von Verarbeitungstätigkeiten muss nach frei wählbaren Kriterien des AG möglich sein.
- Die Durchführung und Dokumentation einer Risikobewertung muss möglich sein.
- Die regelmäßige Aktualisierung bestehender Meldungen muss möglich sein.
- Die Bereitstellung der VVT-Meldungen für Prüf- und Nachweiszwecke gegenüber Aufsichtsbehörden muss möglich sein (s. Kapitel 3.1.1.1.7).
- Die Abbildung eines Bearbeitungs- und Freigabeprozesses mit Darstellung der jeweiligen Bearbeitungsphasen (Entwurf, Eingang, in Prüfung, freigegeben) soll vorhanden sein.
- Frei konfigurierbare Felder zur Erfassung von Zusatzinformationen sollen vorhanden sein.
- Es soll eine Mailkommunikation mit der einreichenden Stelle vorhanden sein.
- Die SaaS-Lösung muss die Erfassung, Verwaltung und Aktualisierung von Meldungen zum VVT gemäß Art. 30 DS-GVO über den gesamten Lebenszyklus hinweg unterstützen.

3.1.1.1.2 Entgegennahme und Prüfung der Meldung als Management-Tool

Die SaaS-Lösung stellt Managementfunktionen zur Entgegennahme, Prüfung und Steuerung von Meldungen zu Verarbeitungstätigkeiten bereit.

Anforderungen:

- Annahme der Meldungen: Funktionen, mit denen die zuständige Einheit eingereichte Meldungen initial entgegennimmt und auf Vollständigkeit sowie Plausibilität prüft, müssen vorhanden sein.
- Statussteuerung von Meldungen: Eine Funktion zum Annehmen und Ablehnen von Meldungen einschließlich der entsprechenden Statusänderung muss vorhanden sein.
- Übergeordnete Verarbeitungstypen: Eine Funktion zur Erstellung übergeordneter Verarbeitungstypen („Master-Meldungen“) zur strukturierten Zusammenfassung einzelner Verarbeitungstätigkeiten muss vorhanden sein.
- Kategorisierung und Darstellung: Eine konfigurierbare Kategorisierung-Funktion der eingehenden Meldungen zu den „Master-Meldungen“ soll möglich sein.

3.1.1.1.3 Risikobewertung der Datenverarbeitung (Schwellwertanalyse)

Die SaaS-Lösung stellt Funktionen zur Risikobewertung von Verarbeitungstätigkeiten und zur Feststellung der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DS-GVO bereit.

Anforderungen:

- Risikobewertung und DSFA-Pflicht: Die SaaS-Lösung muss eine Prüffunktion zur Bewertung des Risikoniveaus von Verarbeitungstätigkeiten sowie zur Feststellung der DSFA-Pflicht gemäß Art. 35 DS-GVO bereitstellen.
- Schwellwertanalyse: Die SaaS-Lösung muss die Durchführung einer Schwellwertanalyse nach den Empfehlungen des EDSA ermöglichen.
- Abgleich mit Risiko- und Ausnahmelisten: Die SaaS-Lösung muss Funktionen zum Abgleich der Verarbeitungstätigkeit mit standardisierten Risiko- und Ausnahmelisten der Aufsichtsbehörden (Blacklists und Whitelists) bereitstellen.
- Dokumentation der Ergebnisse: Die Ergebnisse der Schwellwertanalyse müssen vollständig und meldungsbezogen dokumentiert werden.
    - Weiterleitung in einen DSFA-Prozess: Ergibt die Schwellwertanalyse die Erforderlichkeit einer DSFA, muss die SaaS-Lösung eine Funktion zur Initiierung eines eigenständigen Bearbeitungsprozess zur Datenschutz-Folgenabschätzung bereitstellen.
    - Externe DSFA: Die SaaS-Lösung muss die Integration und Anzeige von extern durchgeführten Datenschutz-Folgenabschätzungen (in Office-Formaten sowie PDF) ermöglichen und diese einer Meldung zum VVT

eindeutig zuordnen können.

3.1.1.1.4 Abschluss und Freigabe

Die SaaS-Lösung stellt Funktionen zum Abschluss, zur Freigabe und zur revisionssicheren Aufnahme von Meldungen zum VVT bereit.

Anforderungen:

- Aufnahme von Meldungen in das VVT und Statuskennzeichnung: Nach Abschluss der Risikobewertung und Bearbeitung von Meldungen muss das VVT automatisch aktualisiert und neue Meldungen mit einem eindeutigen Statushinweis versehen werden.
- Abschlussmeldung mit Benachrichtigung: Mit Abschluss der Bearbeitung der finalen Meldung zum VVT muss eine konfigurierbare Abschlussbenachrichtigung erstellt und automatisch an den Melder verschickt werden.
    - Abgeschlossene Meldungen zum VVT müssen zu jedem Zeitpunkt auswählbar und in den unter 3.1.3.5 angegebenen Formaten exportierbar sein.

3.1.1.1.5 Aktualisierung von Meldungen zum VVT

Die SaaS-Lösung stellt Funktionen zur regelmäßigen und anlassbezogenen Aktualisierung von Meldungen zum VVT bereit.

Anforderungen:

- Eigenständiger Aktualisierungsprozess: Die SaaS-Lösung muss zur Aktualisierung bestehender Meldungen zum VVT einen Prozess zur Bearbeitung aller erfassten Angaben bereitstellen.
- Anlassbezogene Änderungen: Die SaaS-Lösung soll einen Prozess zur Durchführung und Dokumentation anlassbezogener Änderungen von Meldungen zum VVT (z.B. bei Änderungen der Verarbeitung oder beim Wechsel von Auftragsverarbeitern) unterstützen.
- Berichtsfunktion (als Report) für durchzuführende Gültigkeitsprüfungen: Die SaaS-Lösung soll Funktionen zur Berichtserstellung für anstehendende Gültigkeitsprüfungen durch das DSM von Meldungen zum VVT bereitstellen. Die Prüfintervalle sollen konfigurierbar sein.

3.1.1.1.6 Prozessmonitoring und Qualitätssicherung

Die SaaS-Lösung stellt Funktionen zu einem Monitoring und der Qualitätssicherung der Bearbeitungsprozesse zu den Meldungen des VVT bereit.

Anforderungen:

- Die SaaS-Lösung muss eine Funktion zur Darstellung und Auswertung (im Excel-Format) der in den Meldungen zum VVT eingesetzten IT-Lösungen bereitstellen.
- Die Visualisierung des Bearbeitungs- und Freigabestands (Prozessdarstellung) sowie die Status- und Fortschrittsanzeige: Der Bearbeitungsstand der Meldung zum VVT soll über den gesamten Prozess hinweg und nach Abschluss jederzeit darstellbar sein.

3.1.1.1.7 Dokumentation und Berichtsfunktionen

Die SaaS-Lösung stellt eine Funktion zur vollständigen und exportierbaren Dokumentation bereit.

Anforderungen:

- Die Archivierung abgeschlossener Meldungen im VVT mit unveränderbarer Speicherung muss möglich sein.

3.1.1.2 Prüfung von Auftragsverarbeitern („Bieterprüfung“)

3.1.1.2.1 Inhalte der Online-Formulare zur Erstellung und Bearbeitung von Bieterprüfungen

Die SaaS-Lösung stellt ein Online-Formular bereit, über das die fachlich verantwortliche Stelle alle für die Prüfung erforderlichen Informationen und Unterlagen vollständig erfassen und einreichen kann.

Anforderungen:

- Ein webbasiertes Online-Formular zur strukturierten Einreichung einer Bieterprüfung durch die fachlich verantwortliche Stelle, einschließlich Pflichtfeldern und Validierungsmechanismen, (Kap. 3.1.3.11.5) nach Vorgaben des AG muss vorhanden sein.
- Der Upload prüfungsrelevanter Dokumente (insbesondere Leistungsbeschreibung, AuV-Dokument inkl. TOM, Angaben zum AN sowie Anforderungen der Informationssicherheit) in gängigen Dateiformaten (bmp, jpg, PDF, Office-Formate) muss innerhalb des Online-Formulars möglich sein.

3.1.1.2.2 Strukturierter Workflow

Die SaaS-Lösung stellt Funktionen zu einer strukturierten und revisionssicheren datenschutzrechtlichen Prüfung von Auftragsverarbeitern der GIZ gemäß Art. 28 DS-GVO

bereit. Die Prüfung der risikobasierten Bewertung ist mit der Kritikalitätsbewertung des ISM verknüpft.

Anforderungen:

- Ein strukturierter Workflow zur Durchführung der datenschutzrechtlichen Prüfung von Auftragsverarbeitern gemäß Art. 28 DS-GVO, einschließlich Erfassung, Bewertung und Nachverfolgung prüfrelevanter Informationen muss vorhanden sein.

3.1.1.2.3 Risikobewertung

Die SaaS-Lösung stellt Funktionen zu einer Risikobewertung im Rahmen der Bieterprüfung bereit. Diese umfassen insbesondere die Erfassung der verarbeiteten Datenkategorien und betroffenen Personengruppen sowie die Prüfung und Bewertung der vom Bieter vorgelegten TOM gemäß Art. 32 DS-GVO.

Anforderungen:

- Ein strukturierter Bewertungsprozess zur Prüfung und Bewertung der vom Bieter vorgelegten TOM gemäß Art. 32 DS-GVO muss vorhanden sein.
- Eine Funktion zur nachvollziehbaren und revisionssicheren Dokumentation der Bewertungsergebnisse der Schutzmaßnahmen, einschließlich Begründungen und Entscheidungsergebnissen muss vorhanden sein.

3.1.1.2.4 Dokumentation und Register der Auftragsverarbeiter

Die SaaS-Lösung stellt Funktionen zur Dokumentation und Darstellung der Ergebnisse aus der Bieterprüfung in einem zentralen Register der Auftragsverarbeiter bereit (gem. Art. 24, 26 sowie Art. 44 ff. DS-GVO).

Anforderungen:

- Ein Verzeichnis der Auftragsverarbeiter mit Dokumentation eingesetzter datenschutzrechtlicher Garantien (z. B. Standardvertragsklauseln, Angemessenheitsbeschlüsse) und deren Bewertung bzgl. der Notwendigkeit eines Transfer Impact Assessments (TIA) muss vorhanden sein.
- Eine Funktion zur strukturierten Erfassung und Darstellung der Erforderlichkeit datenschutzrechtlicher Garantien gemäß Art. 44 ff. DS-GVO, einschließlich Dokumentation der zugrunde liegenden Bewertung muss vorhanden sein.
- Eine Funktion zur übersichtlichen Darstellung der in der GIZ eingesetzten Auftragsverarbeiter muss vorhanden sein.
- Eine Funktion zur Nachverfolgung und Darstellung von Änderungen oder Anpassungen bei Auftragsverarbeitern, insbesondere im Hinblick auf Subdienstleister sowie eingesetzte TOM soll vorhanden sein.

3.1.1.3 Datenschutz-Folgenabschätzungen

Die SaaS-Lösung stellt einen eigenständigen, strukturierten Prozess zur Durchführung von Datenschutz-Folgenabschätzungen (DSFA) gemäß Art. 35 ff. DS-GVO bereit.

3.1.1.3.1 Strukturierter Workflow

Anforderungen:

- Ein eigenständiger, strukturierter Workflow zur Durchführung von Datenschutz-Folgenabschätzungen, einschließlich Beschreibung der Verarbeitung, Risikobewertung und Maßnahmenableitung muss vorhanden sein.
- Eine Funktion zur fortlaufenden Darstellung des Bearbeitungs- und Entscheidungsstands (z.B. „Initiierung“, „Bearbeitung“, „Prüfung“, „Finalisierung“, „Abgeschlossen“) innerhalb des DSFA-Prozesses soll vorhanden sein.

3.1.1.3.2 Eingangsprozesse

Für die Durchführung einer DSFA wird die Erforderlichkeit aus den unten aufgeführten vorgeschalteten Prozessen in der GIZ ermittelt.

Anforderungen:

- Eine Funktion zur direkten Verlinkung zwischen VVT-Modul und dem DSFA-Modul muss bereitgestellt werden, wenn in der Schwellwertanalyse zur eingereichten Meldung zum VVT festgestellt wird, dass Kriterien für eine DSFA erfüllt werden.
- Eine Funktion zur Anlage einer DSFA muss bereitgestellt werden, wenn in der Beratung der Organisationseinheiten des Datenschutzes über die Schwellwertanalyse festgestellt wird, dass Kriterien für eine DSFA erfüllt werden.
- Bei Vorliegen von DSFA, die von extern durchgeführt wurden, müssen diese im DSFA-Modul vollständig angelegt und dokumentiert werden können.
- Eine Funktion zur Anlage von extern durchgeführte DSFA mit Darstellung der Ergebnisse (in Office-Formaten sowie PDF) anhand der im DSFA-Modul verwendeten Methodik soll vorhanden sein.

3.1.1.3.3 DSFA-Methodik

Das DSFA-Modul orientiert sich bei der intern eingesetzten Durchführungs- und Bewertungsmethodik einer DSFA an international anerkannte Verfahren (z. B. EDSA, CNIL).

Anforderungen:

- Ein international anerkanntes Verfahren (EDSA oder CNIL) zur Durchführung und Bewertung von Datenschutz-Folgenabschätzungen muss unterstützt werden.

- Eine Funktion zur Konfiguration und Anpassung der DSFA-Methodik (Bewertungskriterien, Risikostufen und Entscheidungsschwellen) durch die AG soll vorhanden sein.

3.1.1.3.4 Dokumentation und Nachverfolgung der DSFA-Ergebnisse

Die SaaS-Lösung gewährleistet eine vollständige und strukturierte Dokumentation aller Datenschutz-Folgenabschätzungen.

Anforderungen:

- Eine übersichtliche, konsolidierte Darstellung aller laufenden und abgeschlossenen DSFAs soll vorhanden sein,
  dies beinhaltet mindestens:
  - Bearbeitungsstatus (z.B. „in Prüfung“, „Maßnahmen umgesetzt“, „Konsultation erforderlich“ und „abgeschlossen“),
  - Bewertungsergebnis (z.B. niedriges, mittleres und hohes Risiko),
  - und verantwortlicher Bearbeiter / Fachbereich.

3.1.1.3.5 Unterstützung des Konsultationsverfahrens gem. Artikel 36 DS-GVO

Die SaaS-Lösung unterstützt den Prozess der Konsultation der zuständigen Aufsichtsbehörde bei verbleibend hohem Risiko nach Art. 36 DS-GVO technisch.

Anforderungen:

- Die automatische Kennzeichnung einer DSFA, bei denen trotz technischer und organisatorischer Maßnahmen ein hohes Restrisiko besteht, muss vorhanden sein.
- Die Dokumentation eines Konsultationsprozesses direkt aus der DSFA heraus muss möglich sein.
- Die Bereitstellung aller relevanten Dokumente (z.B. DSFA-Bericht, Risikoanalyse, Maßnahmenplan) für die Übermittlung an die Aufsichtsbehörde soll möglich sein.
- Die Dokumentation des Kommunikationsverlaufs mit der Aufsichtsbehörde soll möglich sein.
- Die Erfassung und Zuordnung der behördlichen Stellungnahme zur jeweiligen DSFA muss möglich sein.
- Eine Funktion zur Kennzeichnung „freigegebener“ Verarbeitungen nach Abschluss des Konsultationsprozesses soll vorhanden sein.

3.1.1.3.6 Maßnahmenumsetzung und Risikobewertung

Die SaaS-Lösung stellt Funktionen zur Maßnahmenumsetzung und Risikobewertung der in einer DSFA identifizierten Maßnahmen bereit.

Anforderungen:

- Eine Erfassung, Zuordnung und Nachverfolgung von Maßnahmen zur Risikominderung mit Angaben zu Verantwortlichen, Fristen und Status muss möglich sein.
- Die Verknüpfung der Maßnahmen mit den entsprechenden Verarbeitungstätigkeiten oder Projekten muss möglich sein.
- Die Überwachung und Fortschrittskontrolle der Maßnahmenumsetzung (z.B. durch Projekt-, Statusberichte oder Auditfunktionen) soll möglich sein.

3.1.1.3.7 Überwachung und Re-Evaluierung einer DSFA

Die SaaS-Lösung unterstützt eine kontinuierliche Überwachung und regelmäßige Neubewertung von durchgeführten DSFA und deren Ergebnissen.

Anforderungen:

- Eine Funktion zur systembasierten Neubewertung muss vorhanden sein, wenn:
  - sich der Verarbeitungszweck,
  - die Technologie,
  - die eingesetzten Systeme oder
  - die Sicherheitslage verändern.
- Eine Monitoring- und Auditfunktion zur kontinuierlichen Überprüfung der Wirksamkeit von Risikokontrollen muss vorhanden sein.
- Eine Berichtsfunktion über den Stand und die Ergebnisse laufender Re-Evaluierungen muss vorhanden sein.

3.1.2 Funktionale Anforderungen (ISM)

3.1.2.1 Asset Management

3.1.2.1.1 Rahmenbedingungen

Das Asset Management bildet basierend auf den relevanten primären und sekundären Assets die Grundlage für die Informationssicherheitsrisikoanalyse des Unternehmens. Es umfasst das Asset Inventar als zentrale Datenbank, die Asset-Erfassung, -Pflege und -Verknüpfung sowie deren Schutzbedarfsfeststellung. Im Asset Inventar wird der Unternehmensaufbau der GIZ abgebildet, der in Zentrale, Stabsstellen, Fach- und Regionalbereiche/Regionen, Organisationseinheiten (OEs), Länder bzw. Landesbüros und Projekte untergliedert ist. Die Informationen zu den Assets werden vorrangig über Schnittstellen zu den bestandsführenden Asset-Datenbanken des Unternehmens bezogen, für informationssicherheitsrelevante Aspekte weiterverarbeitet und im Asset Inventar dokumentiert. Die Assets inkl. Schutzbedarfsfeststellungen werden innerhalb OEs durch Zugriffsberechtigte (u.a. Führungskräfte) sowie durch Unterstützung der Informationssicherheitsorganisation (z.B. ISMT, ISK und ISOs) gepflegt. Durch Aufgabendelegationen und Abfragefunktionen kann die Eingabe von Informationen im DSM-/ISM-Tool dezentral erfolgen.

3.1.2.1.2 Asset Management-Prozess

Die SaaS-Lösung bietet ein kollaborationsfähiges Asset-Management mit nutzergeführter Erfassung, Bearbeitung und Schutzbedarfsfeststellung von Assets.

Anforderungen:

- Ein strukturierter Asset-Management-Workflow (Erfassung, Bearbeitung und Schutzbedarfsfeststellung von Assets und Lieferanten) muss vorhanden sein.
- Die Anpassung (z.B. Bearbeitung, Löschung und Erweiterung von Workflows, Datenfelder, Freigabeprozesse, Schutzziele, Bewertungsstufen, Schadenskategorien) der Asset Management-Prozesse muss durch Administratoren möglich sein.
- Die Erstellung und Bearbeitung im Entwurfsstatus mit anschließender Freigabe/Genehmigung (ggf. durch andere Rollen) muss möglich sein (zentrale Auswertbarkeit erst ab wirksamen/veröffentlichtem Status).
- Die SaaS-Lösung soll die Hinterlegung von Incidents zu Assets mit einer eindeutigen ID und Eingabefeld zur Incident-Beschreibung ermöglichen (1:n Zuordnung Incident je Asset und auswertbar).
- Die SaaS-Lösung muss eine Betroffenheitsanalyse der Assets zur Nachverfolgung von Informationssicherheitsvorfällen (Incidents) ermöglichen.

3.1.2.1.3 Asset Inventar

Die SaaS-Lösung bietet die Möglichkeit zur Verwaltung, Kategorisierung und Erfassung von Assets in ein zentrales Asset-Inventar.

Anforderungen:

- Die standardisierte Erfassung von Assets (sowohl direkt im Frontend aber auch als Schnittstellenimport durch andere Systeme, gem. Kap. 3.1.4.1.4 und 3.2.7) und zentrale Ablage in einem Asset Register muss möglich sein.
- Die Kategorisierung von Assets (z.B. Primäre Assets, Sekundäre Assets, Gruppierung zu thematischen Asset Gruppen) muss möglich sein.
- Eine grafische Anzeige- und Navigationsfunktion von Asset-Verknüpfungen soll vorhanden sein.

3.1.2.1.4 Erfassen und Bearbeiten von Assets

Die SaaS-Lösung unterstützt die Erfassung aller Assets des Unternehmens. Die SaaS-Lösung ermöglicht dabei die weitere Bearbeitung von Assets nach deren initialer Erfassung im Asset-Inventar, um sie zu prüfen, aktualisieren oder unverändert fortzuschreiben.

Anforderungen:

- Die Erfassung von Asset-Informationen (z.B. Standort bzw. Region/ Land/ Projekt, Asset Owner, Organisationseinheit) und Hinterlegung relevanter Dokumente oder Verweise (Upload oder Link auf Dateiablage) muss möglich sein.
- Eine vollständige und konsistente Dokumentation der Assets z.B. durch Pflichtfelder, Validierungen und standardisierte Auswahlmöglichkeiten muss möglich sein.
- Eine direkte Verknüpfung von Assets (z.B. untereinander, mit Asset Owner oder Organisationseinheit) während Erfassung/Bearbeitung (inkl. Auswahl und Verknüpfung der Assets per integrierter Such-/Auswahlfunktion „Look-Up“ bei Assets) muss möglich sein.

3.1.2.1.5 Schutzbedarfsfeststellung

Die SaaS-Lösung bietet eine aktive Unterstützung bei der Schutzbedarfsfeststellung, indem Nutzer für jedes erfasste Asset den Schutzbedarf des jeweiligen Assets bewerten, anpassen und dokumentieren können. Dabei werden die Assets anhand der Schutzziele der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) klassifiziert; die Klassifizierung erfolgt für jedes Schutzziel gesondert.

Anforderungen:

- Eine Schutzbedarfsermittlung über Bewertung der Schadensausprägung (=Bewertungsstufe) je Schutzziel (Vertraulichkeit, Integrität, Verfügbarkeit; Bewertung „gering/mittel/hoch/sehr hoch“) muss möglich sein.
- Eine Unterteilung der Schutzziele nach GIZ-spezifisch definierten Schadenskategorien soll möglich sein, die über qualitativer und quantitativer Beschreibung in der Eingabemaske verfügen, z.B. finanzielle Auswirkungen, Reputationsauswirkung, Gesetz-/Vertragsverstöße, Beeinträchtigung der Aufgabenerfüllung, persönliche Unversehrtheit, informationelle Selbstbestimmung, negative Auswirkungen auf Unternehmensstrategie, Auswirkungen auf Mission der meldenden Organisationseinheit.
- Die Anzeige von benutzerdefinierten Orientierungshilfen je Bewertungsstufe (automatische Einblendung der zugehörigen Schadensausprägung abhängig von der gewählten Schadenskategorie) soll möglich sein.
- Eine automatische Schutzbedarfsbewertung nach Maximalprinzip je Asset (höchstes Schadenspotenzial aus den bewerteten Schadenskategorien wird als maßgebliche Schutzbedarfseinstufung übernommen) soll möglich sein.

3.1.2.1.6 Zuordnung von Assets

Die SaaS-Lösung stellt eine Funktion bereit, mit der alle Assets untereinander im Asset Inventar und bei der Asset-Erfassung unmittelbar miteinander verknüpft werden können (bspw. Importierte Prozesse aus der BPMN-Datenbank zu Assets und Risiken). Dabei können Abhängigkeiten zwischen den jeweiligen Objekten eindeutig abgebildet und nachvollziehbar dargestellt werden.

Anforderungen:

- Assets müssen über eine eindeutige ID verfügen, über die Beziehung (zu Assets und Risiken) definiert werden können, die über Schnittstellen ausgetauscht werden können.
- Eine automatisierte Schutzbedarfsvererbung entlang Asset-Verknüpfungen nach Maximalprinzip (zwischen primären und sekundären Assets sowie zwischen sekundären Assets) muss möglich und nachvollziehbar sein.

- Die Darstellung eines Verteilungseffekts bei der Schutzbedarfsermittlung (Reduzierung des Schutzbedarfs der Verfügbarkeit der primären Assets abhängig von Anzahl verknüpfter sekundärer Assets) muss möglich und nachvollziehbar sein.
- Die Unterstützung eines Kumulationseffekts zur Erhöhung des Schutzbedarfs (bei Mehrfachunterstützung: mehrere Assets durch dasselbe Asset bzw. mehrere sekundäre Assets durch ein weiteres sekundäres Asset) muss möglich und nachvollziehbar sein.
- Die manuelle Überschreibung automatisiert abgeleiteter Schutzbedarfswerte (nach automatisierter Ableitung) muss möglich sein.
- Eine Dokumentation der Abweichungen bzw. manuelle Änderungen von automatisch abgeleiteten Schutzbedarfen (Nachvollziehbarkeit von Zeitpunkt und Begründung) muss möglich sein.

3.1.2.1.7 Dokumentation von Lieferanten

Die SaaS-Lösung ermöglicht das Management von Informationssicherheitsrisiken im Kontext von Lieferanten gemäß ISO/IEC 27001-Anforderungen. Eine Abbildung des Lieferanten ist sowohl über die Integration i im Asset-Management als auch als s alleinstehendes Modul möglich.

Anforderungen:

- Die Erfassung von Lieferanten muss sowohl direkt im Frontend als auch über eine noch gemeinsam zu definierende Schnittstelle importiert werden können (gem. Kap. 3.1.4.1.4 und 3.2.7).

  Das zuliefernde System ist derzeit noch nicht bekannt.

- Das Lieferanten-Risk-Assessment muss im gleichen Verfahren wie das Risk-Assessment für Assets durchgeführt werden können und muss dabei an das Risikomanagement angebunden sein (vgl. Kap. 3.1.2.2).
- Es muss eine Schutzbedarfsfeststellung je Lieferant muss möglich sein.
- Die Gruppierung und Zuordnung von Lieferanten und Beschaffungsgegenständen muss möglich sein.
- Ein zentrales Register zur Dokumentation aller Lieferanten/ Dienstleister/ Auftragsverarbeiter im Beschaffungsvorgang (z.B. integriert im Asset-Inventar gem. 3.1.2.1.3) muss vorhanden sein,
  zum Beispiel mit folgenden Datenfeldern:
  - Asset Owner bzw. verantwortliche Person der GIZ
  - Abteilungszuordnung
  - Unternehmensname, Kontaktdaten, Verantwortliche
  - Lieferantenkategorie (z.B. IT-Dienstleister, Cloud-Anbieter, Beratung, Hosting)

- Schutzbedarfsfeststellung des Lieferanten bzw. Dienstes (Vertraulichkeit, Integrität und Verfügbarkeit)
- Risk Assessment des Lieferanten (einschließlich Maßnahmenplan)
- Zugehörige Standorte, Länder, Organisationseinheiten, Projekte
- Sicherheitsvorfälle (Incidents) der Vergangenheit
- Kennzeichnung zur Verarbeitung personenbezogener Daten
- Vormerkung für zukünftige Audits

- Die Anpassung (z.B. Bearbeitung, Löschung und Erweiterung von Workflows, Datenfelder, Freigabeprozesse, Schutzziele, Bewertungsstufen, Schadenskategorien) des Lieferantendokumentationsprozesses muss durch Administratoren möglich sein.
- Die Verlinkung und Ablage relevanter Lieferantendokumente im Lieferantenregister (insbesondere: AuV-Vertragsannex gem. Art. 28 DS GVO inkl. TOM, Sicherheitszertifikate, AuV-Prüfung/ Risikoanalysen, Auditberichte, Penetrationstests, Maßnahmenplan, Leistungsbeschreibungen und SLAs) muss möglich sein.
- Eine formale Dokumentation der Risikoübernahme muss möglich sein.

3.1.2.2 Risikomanagement

3.1.2.2.1 Rahmenbedingungen

Das Informationssicherheitsrisikomanagement stellt einen integralen Bestandteil des ISMS der GIZ dar und dient der wirksamen Behandlung und Reduzierung von Informationssicherheitsrisiken im Unternehmen. Es basiert im Wesentlichen auf den Prozessen der international anerkannten Normen ISO/IEC 27001 und ISO/IEC 27005.

Das eingesetzte DSM-/ISM-Tool ist in der Lage, die dezentral und global verteilte Unternehmensstruktur abzubilden. Diese umfasst organisationale Einheiten der Zentrale in Deutschland, weltweit angesiedelte Landesbüros sowie die daran angebundenen Projekte. Entsprechend dem dezentralen Organisationsaufbau sind auch die Rollen der Informationssicherheit, die den Informationssicherheitsrisikoprozess durchführen oder unterstützen, den jeweiligen Einheiten zugeordnet. Hierzu zählen insbesondere das ISM-T sowie die ISKs der Zentrale sowie die ISOs der Landesbüros. Eine Risikoauswertung ist dabei auf verschiedene Ebenen (Zentrale, Region, Landesbüros, Projekte) möglich.

Darüber hinaus sind Asset Owner und Risk Owner maßgeblich in den Risikomanagementprozess eingebunden. Asset Owner sind in der Regel Mitarbeiter des operativen Tagesgeschäfts, während Risk Owner überwiegend Funktionen auf Gruppen-, Abteilungs- oder Bereichsleiterebene wahrnehmen. Sie tragen die Verantwortung für die Durchführung der Risk Assessments, entweder durch eigenständige Bearbeitung oder im Rahmen von Delegationsprozessen. Entsprechend ist ein rollenbasierter Zugriff (vgl. Kap. 3.1.5) auf das DSM-/ISM-Tool innerhalb des jeweiligen Verantwortungsbereichs notwendig.

3.1.2.2.2 Risk Assessment-Prozess

Die SaaS-Lösung ermöglicht einen standardisierten, vollständigen, und ISO/IEC 27005-konformen Risk-Assessment-Prozess.

Anforderungen:

- Der Risk Assessment-Prozess sowie dessen Folgeschritte muss für Assets als strukturierter Workflow möglich sein und aus folgenden Aktivitäten gemäß ISO/IEC 27005 bestehen:
  - Risikoidentifikation (Kap. 3.1.2.2.3)
  - Risikoanalyse (Kap. 3.1.2.2.4)
  - Risikobewertung (Kap. 3.1.2.2.5)
  - Risikobehandlung & Maßnahmen (Kap. 3.1.2.2.6)
  - Maßnahmennachverfolgung & Review (Kap. 3.1.2.2.7)
- Die Anpassung (z.B. Bearbeitung, Löschung und Erweiterung von Workflows, Datenfelder, Freigabeprozesse, Bedrohungskataloge, Risk Level-Kalkulationslogik, Eskalationslogik etc.) des Risk-Assessment-Prozesses und der Nachfolgeschritte muss durch Administratoren möglich sein.
- Die Erstellung und Bearbeitung im Entwurfsstatus mit anschließender Freigabe/Genehmigung (ggf. durch Delegation an andere Rollen) muss möglich sein (zentrale Auswertbarkeit erst ab wirksamen/veröffentlichtem Status).
- Eine Nutzerführung und bearbeitbare Informationsfelder in den Eingabemasken zur Erläuterung und Anleitung der Prozessschritte des Risk Assessments müssen vorhanden sein.
- Eine zentrale Auslösung von Review-Aufforderungen an Risk Owner nach Triggern (z.B. für ausgewählte Organisationseinheiten/ Länder/ Ländergruppen/ Projekte/ regional veränderter Bedrohungslage) soll möglich sein.

3.1.2.2.3 Risikoidentifikation

Die SaaS-Lösung ermöglicht die Risikoidentifikation als Prozessschritt. Die SaaS-Lösung stellt dabei integrierte, anpassbare Bedrohungskataloge bereit, die die für das Unternehmen relevanten Bedrohungen und Bedrohungsszenarien enthalten.

Anforderungen:

- Ein zentrales Risikoregister als führende Datenquelle für alle ISMS-Risiken (Speicherung, Verwaltung, Nachverfolgung, Auswertung inkl. vollständiger Risikodaten) muss vorhanden sein.
- Eine Risikoidentifikation (mit Beschreibung der Bedrohungen, Schwachstellen u. Freitextfeld für Risikoszenarien) für Assets, Asset-Kategorien und -Gruppen muss möglich sein.

- Die Bedrohungsauswahl und Zuordnung per Look-Up/Drop-Down aus zentral gepflegten Bedrohungskatalogen für Risiken mit und ohne Asset-Bezug muss möglich sein.
- Die Auswahl betroffener Schutzziele je Risikoszenario (mindestens Vertraulichkeit, Integrität, Verfügbarkeit; mehrere auswählbar) muss möglich sein.

3.1.2.2.4 Risikoanalyse

Nach Abschluss der Risikoidentifikation ermöglicht die SaaS-Lösung für jedes identifizierte Risiko die Durchführung einer Risikoanalyse als Folgeprozessschritt, um das Risiko Level zu bestimmen.

Anforderungen:

- Die Erfassung bereits umgesetzter Maßnahmen je Risiko (risikoreduzierend) muss möglich sein.
- Die automatische Übernahme der Schutzbedarfe je Schutzziel als Ausgangswert für die Schadenshöhe (Grundlage zur Risikolevel-Berechnung) muss möglich sein.
- Die manuelle Überschreibung der Schadenshöhe je Risiko unter Berücksichtigung vorhandener Maßnahmen muss möglich sein.
- Die Auswahl einer Eintrittswahrscheinlichkeit je Risiko (z.B. „unwahrscheinlich“, „möglich“, „wahrscheinlich“, „sehr wahrscheinlich“) muss möglich sein.
- Die automatische Berechnung des Risk Levels je Risiko (Kalkulation aus Schadenspotenzial und Eintrittswahrscheinlichkeit; z.B. „niedrig“, „mittel“, „hoch“, „sehr hoch“) muss möglich sein.
- Ein Freitextfeld zur Begründung und Kommentierung des Ergebnisses der Risikoanalyse je Risiko muss vorhanden sein.
- Eine standortspezifische Risk-Level-Kalkulation durch regional definierbare Bedrohungslagen soll möglich sein.

3.1.2.2.5 Risikobewertung

Die Risikobewertung gleicht die Analyseergebnisse je Risiko mit den Risikokriterien (Akzeptanz/Grenzwerte) ab, entscheidet über Akzeptanz vs. Behandlungsbedarf, priorisiert und überführt nicht akzeptable Risiken in die Risikobehandlung inkl. dokumentierter Entscheidung und Freigabe.

Anforderungen:

- Ein automatisierter Abgleich des Risk Levels mit Risikobewertungskriterien (u. a. Grenzwerte, Akzeptanzkriterien) zur Ermittlung des Handlungsbedarfs und entsprechendem Vorschlag von Risikobehandlungsstrategien (Risikovermeidung,

Risikoreduzierung, Risikotransfer, Risikoakzeptanz) muss möglich sein (bspw. definierte Schwellwerte initiieren eine erforderliche Managemententscheidung).
- Eine manuelle Änderung der vorgeschlagenen Risikobehandlungsstrategie je Risiko muss möglich sein.
- Ein Freitextfeld zur Begründung und Kommentierung der Risikobehandlungsentscheidung je Risiko muss vorhanden sein.

3.1.2.2.6 Risikobehandlung & Maßnahmen

Die SaaS-Lösung stellt eine standardisierte Dokumentation der Risikobehandlung in einem Maßnahmenplan mit unterstützendem Maßnahmenkatalog bereit.

Anforderungen:

  - Vorbelegte Auswahlfelder (z.B. Dropdown oder funktional gleichwertig) für Risikobehandlungsoptionen (Risikovermeidung, Risikoreduzierung, Risikotransfer, Risikoakzeptanz) müssen vorhanden sein.
  - Die Dokumentation von Risikobehandlungsmaßnahmen in einem individuellen Maßnahmenplan je Asset muss möglich sein.
  - Die Festlegung eines Zielrisikos im Rahmen der Risikobehandlung (erwarteter Risk Level nach Umsetzung geplanter Maßnahmen inkl. Beschreibung der erwarteten Wirkung auf Schadensausmaß und Eintrittswahrscheinlichkeit) muss möglich sein (getrennt vom tatsächlichen Risiko).
  - Eine standardisierte Eingabemaske zur Eingabe und Bearbeitung von Maßnahmen im Maßnahmenplan und im Maßnahmenregister (z.B. Freitext- und Dropdown-Felder) muss vorhanden sein.
  - Die Anlage von Maßnahmen muss auch unabhängig von einem vorhandenen Risiko (z.B. Korrekturmaßnahmen und Verbesserungsmaßnahmen) möglich sein.
  - Die Anlage und Bearbeitung zentraler Maßnahmenkataloge inkl. Maßnahmenvorlagen muss möglich sein.
- Die Dokumentation der Risikoakzeptanz in einem Risikoakzeptanzregister soll vorhanden sein.
- Ein Workflow zur Wirksamkeitsprüfung und Freigabe implementierter Maßnahmen soll vorhanden sein.

3.1.2.2.7 Maßnahmennachverfolgung & Review

Die SaaS-Lösung stellt ein zentrales ISMS-Maßnahmenregister bereit, in dem alle geplanten und implementierten Maßnahmen verwaltet und nachverfolgt werden können.

Anforderungen:

- Die konsolidierte Abbildung aller Maßnahmen im Maßnahmenregister (einschließlich Risikobehandlung/Risk Treatment Plan, Korrekturmaßnahmen aus internen/externen Audits, Verbesserungsmaßnahmen aus dem Continual Improvement Process, Maßnahmen/TOMs aus dem DSM) muss möglich sein.
- Eine Markierung der Maßnahmen mit einer „Vormerkung für zukünftige Audits“ muss möglich sein.
- Regelmäßige Überprüfungen von implementierten Maßnahmen und Maßnahmenwirksamkeit inkl. automatischer Termin- und Benachrichtigungserstellung (Kap. 3.1.3.11.3) müssen möglich sein.
- Ein Statement of Applicability nach ISO 27001 muss sich durch einen Automatisierungsprozess unterstützt auf Basis der Ergebnisse der umgesetzten Maßnahmen erstellen lassen.

3.1.2.2.8 Formularbasierte Datenerfassung

Die SaaS-Lösung ermöglicht eine dezentrale Erfassung und Bearbeitung von Informationen durch Fachverantwortliche über eine Abfragefunktion, ohne dass hierfür ein vollumfänglicher Systemzugriff erforderlich ist. Die konkreten Anwendungsfälle sind mit dem AN zu erarbeiten.

Anforderungen:

- Die Anpassung der Formularstruktur- und -inhalte muss durch Administratoren möglich sein.
- Eingeschränkter Online-Zugriff für Fachverantwortliche zur dezentralen, strukturierten Erfassung, Abfrage und Bearbeitung von Informationen zu Assets/Lieferanten inkl. Schutzbedarfsfeststellung, Risiken und Maßnahmen soll vorhanden sein.
- Die Erstellung und Bearbeitung von Formularen im Entwurfsstatus mit anschließender Freigabe/Genehmigung (ggf. durch andere Rollen) soll möglich sein (zentrale Auswertbarkeit erst ab wirksamen/veröffentlichtem Status).

3.1.3 Modulübergreifende funktionale Anforderungen

3.1.3.1 Modulunabhängige Nutzung der SaaS-Lösung

Unabhängig von den nachfolgenden Anforderungen ist eine sukzessive Nutzung der Funktionalitäten für den DSM- und den ISM-Bereich möglich, ohne dass andere Module bereits genutzt werden. Verknüpfte Inhalte werden in diesem Fall leer angezeigt werden.

Anforderungen:

- Eine modulunabhängige Nutzung der DSM- und ISM-Funktionalitäten muss möglich sein (leere Anzeige verknüpfter Inhalte bei fehlender Umsetzung/Aktivierung des jeweils anderen Moduls).

3.1.3.2 Verknüpfung funktionaler Inhalte von DSM und ISM

Die SaaS-Lösung stellt eine von DSM und ISM gemeinsam genutzte Datenbasis bereit, sodass Inhalte beidseitig in den jeweiligen Prozessen verfügbar sind. Ziel ist die gemeinsame Nutzung von Objekten (Assets, Maßnahmen) für Auswertungen und Analysen im DSM und ISM.

Anforderungen:

- Die SaaS-Lösung muss die Kennzeichnung von Assets und Dienstleistern hinsichtlich Verarbeitung personenbezogener Daten ermöglichen.
- Die SaaS-Lösung muss für den gesamten Arbeitsprozess Sichtbarkeit und Zugriff auf einzelne Objekte sowohl aus der ISM- als auch aus der DSM-Perspektive zulassen. Die Daten liegen übergreifend vor. Das betrifft insbesondere alle Informationen und Ergebnisse der Risikobewertung von Dienstleistern und Assets im Asset-/Lieferantenmanagement (s. Kap. 3.1.2.1.3 und 3.1.2.1.7) sowie im Rahmen der Bieterprüfung erfassten Angaben (s. Kap. 3.1.1.2) (durch die Kennzeichnung/ Checkbox der Verarbeitung personenbezogener Daten).
- Eine prozessuale Verknüpfung von Datenobjekte und Analyseergebnisse zwischen ISM und DSM soll möglich sein

Zum Beispiel durch folgende Funktionen:

- Verknüpfung der Ergebnisse der Bieterprüfung aus dem DSM-Modul mit bestehenden Kritikalitäts- und Risikobewertungen aus dem ISM-Modul
- Sichtbarkeit von TOMs im Datenschutz und implementierter Maßnahmen im ISM-Maßnahmenregister
- Bei der Bewertung der Kritikalität kann eine Aufforderung zur Bewertung des Schutzbedarfs der zugeordneten Assets und Verarbeitungsszenarien im Rahmen der Bieterprüfung angestoßen werden und umgekehrt. (s. Kap. 3.1.1.2).

3.1.3.3 Reporting

Die SaaS-Lösung stellt sowohl für DSM als auch für ISM standardisierte und anpassbare Berichtsgenerierung bereit.

Anforderungen:

  - Standardisierte und anpassbare Berichtsformate (Templates) müssen vorhanden sein,
    zum Beispiel für:
  - Register- und Stammdatenberichte (z. B. Risikoregister, Risikoakzeptanzregister, Maßnahmenregister, Asset-Register)
  - Status-, Fortschritts- und Assessment-Berichte (z. B. Risiken, Workflows, Implementierungsstand von Maßnahmen, Managementberichte zu Prüfungshandlungen
  - Compliance- und Abdeckungsberichte (z. B. Abdeckungsgrad ISO/IEC 27001 Annex-A-Referenzmaßnahmen durch interne Maßnahmen)
  - DSFA- und VVT-bezogene Berichte (z. B. konfigurierbare KPIs zur Auswertung der DSFA-Aktivitäten)

- Eine Berichtsgenerierung anhand ausgewählter Kriterien, Filter, Attribute und definierter Merkmale (z.B. Status „Vormerkung für zukünftige Audits“, Organisationseinheit, Standort, Risk Owner, Asset Owner, Schutzbedarf, Informationssicherheitsrisiko, Risk Level, Audit-Vormerkung, Aufgaben, Deadline, Erstelldatum, Review-Datum, Zeiträume) muss möglich sein.
- Die SaaS-Lösung muss den Export von Reports einschließlich aller Anhänge und grafischen Inhalten in definierten Formaten (z.B. PDF, XLSX, CSV, JSON, JPG) ermöglichen.
- Die SaaS-Lösung muss die Anpassung von Report-Layouts/Berichtsformate und Visualisierungen, grafischen Berichtselementen und Inhalten sowie die Erstellung neuer Berichte durch Administratoren ermöglichen.
- Grafische Berichtselemente zur Darstellung der erfassten Datensätze sollen vorhanden sein.

  Zum Beispiel mit folgenden Darstellungsfunktionen:

  - Risikomatrizen
  - Trenddiagramme
  - Liniendiagramme
  - Balkendiagramme
  - Heat Maps
  - Kennzahlenübersichten
  - Wirksamkeitsanalysen

3.1.3.4 Auswertungs- und Suchfunktion

Die SaaS-Lösung ermöglicht systemübergreifend Funktionen zur Suche und Auswertung fachlicher Datenobjekte.

Anforderungen:

- Die Auswertung erfasster Datensätze im ISM (z.B. Assets, Risiken und Maßnahmen) und DSM (z.B. VVTs, Bieterprüfungen) über alle Datenfelder muss einschließlich Gruppierung, Aggregation, Filterung, Suche, Sortierung und Export/Ad-hoc-Report möglich sein.
  (z.B. Organisationseinheiten, Länder/Regionen, Gesamtübersicht, Gruppierungen nach Systemlandschaft, Risk Owner, Asset Owner, Schutzbedarf, Datenschutz- und Informationssicherheitsrisiko, Audit-Vormerkung, anstehende Deadlines, Erstelldatum, Review-Datum, Zeiträume, Verfahrenszweck oder DSFA-Status, offene/überfällige Wiedervorlagen und Erinnerungen)
- Ein integriertes rollenabhängiges Dashboard für Kennzahlen und Statusinformationen (z.B. Assets, Risiken, Maßnahmen; zugriffsrechtsbasiert; aktuelle Gesamtsicht ISMS-Status) muss vorhanden sein.
- Die SaaS-Lösung muss Suchergebnisse rollen- und berechtigungsbasiert eingeschränkt anzeigen (es werden ausschließlich Daten/Objekte entsprechend der Berechtigung angezeigt).
- Die Visualisierung des Bearbeitungs- und Freigabestands (Prozessdarstellung) sowie die Status- und Fortschrittsanzeige: Der Bearbeitungsstand der Meldung zum VVT sowie des DSFA-Prozesses soll über den gesamten Prozess hinweg und nach Abschluss jederzeit darstellbar sein.
- Die SaaS-Lösung soll eine integrierte globale Volltextsuche über alle relevanten Datenobjekte beinhalten.

3.1.3.5 Import- und Exportfunktion

Die SaaS-Lösung stellt systemübergreifend Funktionen zum Import und Export fachlicher Daten und zugehöriger Informationen bereit.

Anforderungen:

- Unterstützte Import-/Exportfunktionen für fachliche Datensätze (z.B. Risiken im Risikoregister, Maßnahmen, Schutzbedarfsfeststellungen, Meldungen zum VVT, Register der Auftragsverarbeiter) in den Formaten CSV, XLSX, PDF und JSON müssen vorhanden sein.
- Standardisierte Exporte von berechtigten Nutzern für Daten ihres Verantwortungsbereichs (zugriffsrechtsbasiert) müssen möglich sein.

3.1.3.6 Dokumenten-Upload

Die SaaS-Lösung stellt systemübergreifend Funktionen zum Upload und zur Hinterlegung von Dokumenten, Dateien und sonstigen Nachweisen zu fachlichen Datenobjekten bereit.

Anforderungen:

- Der Upload und Verlinkung von Dateien (.doc, .xlsx, .csv und PDF), Links und Ablageorten als Nachweise und zur Dokumentation (z.B. für den DSFA-Prozess, Assets, Risk Assessments und Maßnahmen) muss möglich sein.

3.1.3.7 Versionierung und Änderungshistorie

Alle Datensätze werden revisionssicher gespeichert und sind durch eine Änderungshistorie rückwirkend nachvollziehbar.

Anforderungen:

- Eine revisionssichere Dokumentation und Nachverfolgbarkeit aller Änderungen (Historisierung/Versionierung) der fachlichen Datensätze muss möglich sein.

3.1.3.8 Erinnerungs- und Wiedervorlagefunktion

Die SaaS-Lösung bietet Erinnerungen und Wiedervorlagen für definierte Objekte/Prozesse triggerbasiert und fristgesteuert unterstützen, inkl. zentraler Konfiguration und Benachrichtigungskanälen.

Anforderungen:

- Erinnerungs- und Wiedervorlagefunktionen auf Basis von (wiederkehrenden) (Review-)Fristen, Statusänderungen, anstehenden Aufgaben und anlassbezogene Trigger-Ereignissen müssen möglich sein,
  zum Beispiel für:
  - Regelmäßige Prüfung der Gültigkeit von VVT-Meldungen
  - Überfällige oder geänderte Maßnahmen einer DSFA
  - Fristgerechte Prüfungszyklen einer DSFA
  - Regelmäßige Prüfung des Risk Assessments, Maßnahmen und der Schutzbedarfsfeststellung
  - Aufforderungen zum Review der Risikoanalyse bei Änderung der Bedrohungslage (anlassbezogen/Trigger)
  - Regelmäßige Überprüfung der Maßnahmen und Maßnahmenwirksamkeit
  - Delegierte Aufgaben

- Überprüfungszeiträume und Benachrichtigungskanäle müssen frei konfigurierbar sein.
- Eskalationsworkflows auf Basis von Fälligkeiten und Überfälligkeit über E-Mail oder über definierten Kommunikationskanal müssen vorhanden sein (z.B. überfällige Maßnahmen, Review von Risikoanalysen etc.).
- Die SaaS-Lösung soll die Sichtbarkeit von Wiedervorlagen und anstehende Aufgaben in persönlichen Übersichten ermöglichen (z.B. „Meine offenen Punkte“).

3.1.3.9 Sprachen

Die SaaS-Lösung ist mehrsprachig nutzbar sein und die Benutzeroberfläche sowie nutzerrelevante Inhalte sind in mehreren Sprachen verfügbar.

Anforderungen:

- Die SaaS-Lösung muss die Benutzeroberflächen und -dialoge sowie Hilfefunktion mehrsprachig, mindestens in Deutsch und Englisch bereitstellen.
- Die SaaS-Lösung soll die Systemsprache Französisch beinhalten.
- Die SaaS-Lösung soll die Systemsprache Spanisch beinhalten.
- Sprachunabhängige Auswertungsergebnisse (keine abweichenden Ergebnisse durch unterschiedliche Systemsprachen; keine Doppelungen durch Übersetzung einzelner Objekte) müssen möglich sein.
- Die SaaS-Lösung soll eine Übersetzungsmöglichkeit für ein manuell angelegtes Objekt (z.B. Maßnahmen) als Attribut ermöglichen.

3.1.3.10 Vertretungsregelung / Abwesenheitsvertretung

Die SaaS-Lösung unterstützt die Nominierung von Vertretungen, welche während der Abwesenheit der eigentlichen Verantwortlichen, alle oder ausgewählte Objekte (Risiken, Prüfungen, Vorfälle) des vertretenen Nutzers verwalten und bearbeiten können.

Anforderungen:

- Die SaaS-Lösung soll eine befristete Vertretungsregelung bereitstellen (z.B. Vertretung von Risk Owner).

3.1.3.11 Usability

3.1.3.11.1 Barrierefreiheit

Die SaaS-Lösung berücksichtigt Barrierefreiheit gemäß anerkannten Richtlinien und Standards.

Anforderungen:

- Die SaaS-Lösung muss Barrierefreiheit gemäß BITV 2.0 oder gemäß WCAG 2.1 (AA-Standard) oder vergleichbar erfüllen.

3.1.3.11.2 Software-Hilfe

Die SaaS-Lösung stellt Hilfefunktionen bereit und hält diese versionsaktuell. Hilfsinhalte sind kontextbezogen und in den vereinbarten Systemsprachen und (für Admins) konfigurierbar.

Anforderungen:

- Die SaaS-Lösung muss Hilfsinformationen über eine Online-Hilfeplattform, Guided Tours und/oder FAQs bereitstellen.
- Die Hilfsinformationen müssen an die jeweils neueste Version angepasst werden.
- Die SaaS-Lösung muss eine integrierte Kontext-Hilfe durch Informationsfelder im System und schrittweise Nutzerführung in der Eingabemaske für folgende Prozesse erfüllen:
  - Asset Management (gem. Kap. 3.1.2.1)
  - Risikomanagement (gem. Kap. 3.1.2.2)
- Die integrierte Kontext-Hilfe muss von Administratoren bearbeitbar sein (inkl. Ergänzung zusätzlicher Inhalte).
- Die SaaS-Lösung muss eine Hilfsfunktionen mindestens in Deutsch und Englisch sowie in weiteren Systemsprachen nach Vereinbarung beinhalten. (vgl. Kap. 3.1.3.9)
- Die SaaS-Lösung muss eine integrierte Community-Interaktion (z.B. FAQ/ Wiki mit anderen Nutzern innerhalb/außerhalb der Organisation) ermöglichen.

3.1.3.11.3 Systemgenerierte Benachrichtigungen

Die SaaS-Lösung bietet systemgenerierte Benachrichtigungen für Prozesse und Aufgaben und versendet diese zusätzlich per E-Mail, inkl. konfigurierbarer Präferenzen. Der E-Mail-Versand ist dabei technisch abgesichert und in die GIZ-Authentisierungsumgebung integrierbar.

Anforderungen:

- Die SaaS-Lösung muss den Versand systemgenerierter Benachrichtigungen via E-Mail mit Authentisierungstechnologien gemäß Kap. 3.1.4.1.2 gewährleisten.
- Die SaaS-Lösung muss systemgenerierte Benachrichtigungen (und Abschlussbenachrichtigungen) zu Prozessen und Aufgaben bei Statuswechseln und Handlungsaufforderungen (z.B. Risikoanalyse bei hohem Schutzbedarf, regelmäßige/ad-hoc Risikoüberprüfungen, erforderliche Freigaben) sowohl innerhalb der Softwarelösung als auch per E-Mail ermöglichen.
- Die SaaS-Lösung muss konfigurierbare Benachrichtigungspräferenzen bei anstehenden Aufgaben und Handlungsaufforderungen (z.B. Risikoanalyse bei hohem

Schutzbedarf, regelmäßige/ad-hoc Risikoüberprüfungen, erforderliche Freigaben) beinhalten (innerhalb der SaaS-Lösung oder per E-Mail; je Funktionsbestandteil separat aktivier-/deaktivierbar).

- Die SaaS-Lösung muss E-Mail-Benachrichtigungen automatisiert an externe Workflow-Beteiligte versenden können.
- Die SaaS-Lösung muss eine Echtheitsprüfung des E-Mail-Versands mit SPF (Sender Policy Framework) und DKIM (Domain Keys Identified Mail) zusammen mit DMARC (Domain-based Message Authentication, Reporting and Conformance) durchführen.

3.1.3.11.4 Validierung der Dateneingabe

Die SaaS-Lösung validiert Dateneingaben und Pflichtfelder; Umfang und Intensität der Validierung sind dabei konfigurierbar.

Anforderungen:

- Validierungsmöglichkeiten für Eingaben zur Vermeidung falscher/ fehlerhafter/ unvollständig ausgefüllter Felder müssen vorhanden sein.
- Die Konfigurierbarkeit der Datenvalidierung (Pflichtfeldprüfung und Fehlermeldung) bei der Anlage neuer Felder durch GIZ-Administratoren muss möglich sein.

3.1.3.11.5 Templates und Ausfüllhilfen

Um die Arbeitsprozesse zu vereinfachen, bietet das Tool Ausfüllhilfen, wie zum Beispiel webbasierte Formulare zur Datenerfassung durch Nutzer mit beschränktem Zugriff oder kontextbezogene Vorschläge.

Anforderungen:

- Die Nutzung und der automatisierte Vorschlag vordefinierter und anpassbarer Vorlagen/Templates zur Unterstützung standardisierter Erfassungs-, Bewertungs- und Auswahlprozesse soll möglich sein.

  Zum Beispiel in folgenden Anwendungsfällen:

  - Vorausgewählte Assets
  - Asset-Sets
  - Gruppen für Beschaffungsgegenstände
  - Schutzbedarfsfeststellungen
  - Bedrohungen und Schwachstellen bei der Risikoidentifikation
  - Risikoanalysen und -bewertungen
  - Standardmaßnahmen
  - Kategorisierung von Meldungen zum VVT

- Zuordnung von Meldungen zu Standardprozessen und zentralen Dokumentationen
- KI-gestützte Vorschläge zur kontextbezogenen Auswahl von Inhalten sollen möglich sein.
  Zum Beispiel in folgenden Anwendungsfällen:
  - Schwachstellen auf Grundlage ausgewählter Bedrohungen oder vergleichbarer Kontextinformationen
  - Beschreibung von Risikoszenarien

3.1.4 Technische Anforderungen

3.1.4.1 Anforderungen an den Betrieb

3.1.4.1.1 Serverstandort

Aufgrund GIZ-interner Vorgaben ist ein Hosting der SaaS-Lösung und ihrer Redundanzstandorte notwendig.

Anforderungen:

- Die SaaS-Lösung muss auf Servern innerhalb des EWR betrieben werden.
- Die SaaS-Lösung muss örtliche Redundanz innerhalb des EWR nutzen.

3.1.4.1.2 Zugang und Zugriff, Authentisierung

Die SaaS Lösung erfüllt die Anforderungen an die Standardumgebung, Nutzung und Zugang.

Zusätzlich werden Offline-Workflows für eingeschränkte Internetkonnektivität unterstützt.

Anforderungen:

- Die SaaS-Lösung muss in der GIZ-Standardumgebung (derzeit Windows 11, Microsoft Edge) uneingeschränkt nutzbar sein.
- Die SaaS-Lösung muss über eine giz.de-Adresse erreichbar sein.
- Die SaaS-Lösung muss an die GIZ-Systeme zur Authentisierung/Authentifizierung mit SAML 2.0/OAuth 2.0 in Verbindung mit Multifaktor-Authentifizierung (MS-Authenticator-App) (siehe Kap. 2.9) angebunden werden können.
- Der Zugang zur SaaS-Lösung muss über SSO erfolgen.

3.1.4.1.3 SSL-Zertifikate Web-Oberfläche

Die Web-Oberfläche und die gesamte Kommunikation zwischen Client und Systemkomponenten erfolgt mit TLS-Verschlüsselung.

Anforderungen:

- Die SaaS-Lösung muss eine TLS/SSL-Verschlüsselung der Web-Oberfläche gewährleisten.
- Die TLS verschlüsselte Kommunikation muss auf Grundlage von als sicher anerkannten Cipher-Suites erfolgen, gemäß der jeweils gültigen Empfehlungen des BSI während der gesamten Vertragslaufzeit.

3.1.4.1.4 Technische Schnittstellenanforderungen

Die SaaS-Lösung unterstützt den bidirektionalen Datenaustausch mit On-Premise- und Cloud-Systemen (inkl. SQL-Datenbanken).

Anforderungen:

- Die SaaS-Lösung muss eine REST/ODATA-API-Schnittstelle bereitstellen.
- Die SaaS-Lösung muss mindestens folgende Datenaustauschformate unterstützen:
  - XML
  - JSON
  - CSV
  - und TXT.
- Die SaaS-Lösung muss den bidirektionalen Datenaustausch mit On-Premise- und Cloud-Systemen (inkl. SQL-Datenbanken) unterstützen. Dabei sind die in diesem Kapitel beschriebenen Schnittstellenanforderungen zu berücksichtigen.
- Es muss möglich sein, die SaaS-Lösung für zukünftige zusätzliche Datenaustauschformate zu erweitern.
- Die SaaS-Lösung soll eine ODBC-Schnittstelle bereitstellen.
- Die SaaS-Lösung soll eine JDBC-Schnittstelle bereitstellen.
- Die SaaS-Lösung soll das Datenaustauschformat DSN unterstützen.

3.1.4.1.5 Systemumgebung

Der AN stellt während der gesamten Vertragslaufzeit geeignete Betriebsumgebungen bereit.

Anforderungen:

- Der AN muss eine Staging-Umgebung mit technisch und funktional exakter, vollständiger Spiegelung der Produktivumgebung über die gesamte Vertragslaufzeit bereitstellen.

- Die SaaS muss in einem gesicherten Rechenzentrum nach EN 50600 oder vergleichbar (z.B. DIN ISO 27001, NIST SP 800-53, SSAE 16 SOC 2, FedRAMP) betrieben werden.
- Der AN muss insbesondere während Implementierungsphasen, einschließlich späterer Bedarfe, eine zusätzliche Testumgebung zur Verfügung stellen, die keine Produktivdaten, sondern Testdaten enthält. Diese dient der Nachvollziehbarkeit der Abläufe in der SaaS-Lösung und den Entwicklern beim Finden von Fehlern. Es können dort eine Teilmenge der Daten oder auch Testdaten abgebildet werden.

3.1.4.1.6 Incident- und Problemmanagement

Die Leistung des AN umfasst ein Incident- und Problemmanagement gemäß den im Vertrag vereinbarten Servicelevels, inklusive definierter Kommunikationswege und Verfügbarkeitsanforderungen.

Anforderungen:

- Die Störungs-/Request-Kommunikation muss per E-Mail erfolgen und der Status der Meldungen muss nachverfolgt werden können.
- Der AN muss vier Ansprechpartner für die Übermittlung von Vorfallmeldungen benennen.
- Die Kommunikation muss in deutscher oder englischer Sprache erfolgen.
- Es muss eine Störungsbeseitigung zu Servicezeiten gemäß A03-1_GIZ-DSM-_ISM-Tool_Anlage Informationssicherheit inkl. Bereitstellung von Hot-Fixes gewährleistet werden.

3.1.4.1.7 Wartung, Pflege und Support

Wartung, Pflege und Updates und Support sind ab Inbetriebnahme über die gesamte Vertragslaufzeit bereitzustellen, inklusive Release-Management. Es gelten die Reaktions- und Wiederherstellungszeiten/Mängelklassen gemäß „A04_GIZ_DSM-_ISM-Tool_EVB-IT-Cloudvertrag in Ziff. 9 „Sonstige Vereinbarungen“.

Anforderungen:

- Wartung, Pflege und Support ab Inbetriebnahme über die vertraglich vereinbarte Laufzeit (inkl. funktionaler Erweiterungen: Updates, Upgrades, neue Releases/Versionen, Patches, Hot-Fixes) der SaaS-Lösung sowie zugehöriger Schnittstellen muss gewährleistet werden.
- Ein Security-Patch Management welches ad-hoc notwendige Sicherheitsupdates erkennt, um den sicheren Betrieb der SaaS-Lösung sicherzustellen, muss vorhanden sein.

- Neue Updates inkl. Aktualisierung erforderlicher Drittanbieter-Komponenten (Add-Ins etc.) müssen bereitgestellt werden.
- Die Dokumentation neuer Funktionen, Änderungen und durchgeführte Tests von Minor- und Major-Releases müssen auf Deutsch oder Englisch bereitgestellt werden.
- Support auf Deutsch oder Englisch muss zu Servicezeiten innerhalb der Kernarbeitszeit der GIZ-IT (Mo–Fr 08:00–17:00 Uhr Mitteleuropäischer Zeit) bereitgestellt werden (z.B. Ticket, Mail, Telefon).
- Vorabinformation zu Releases müssen mit mindestens 2 Wochen Vorlauf per E-Mail auf Deutsch oder Englisch an benannte Ansprechperson bereitgestellt werden.

3.1.4.1.8 Abschaltung von KI-Funktionalitäten

Die SaaS-Lösung bietet die Möglichkeit, KI-Funktionalitäten zu deaktivieren.

Anforderungen:

- Die SaaS-Lösung muss die **Abschaltung von KI-Funktionalitäten** ermöglichen (sofern vorhanden).

3.1.5 Rollen- und Berechtigungskonzept

3.1.5.1 Berechtigungsmanagement

Die SaaS-Lösung beinhaltet ein rollenbasiertes Berechtigungssystem, das für sämtliche Module in der SaaS-Lösung gilt. Dabei werden eine granulare Vergabe und Steuerung von Zugriffsrechten auf Daten, Funktionen und Prozesse ermöglicht.

Anforderungen:

- Der rollen- und berechtigungsabhängige Zugriff auf personenbezogene Daten muss DSGVO-konform erfolgen.
- Die Beschränkung von Zugriffsrechten auf definierte Geltungsbereiche (mind. Organisationseinheiten, Länder, Regionen/Ländergruppen und Projekte) muss möglich sein.
- Eine getrennte Vergabe von Rollen und Geltungsbereichen muss unabhängig von OE/Land/Projekt möglich sein (z. B. ISMT/ISO).
- Objektbezogene Berechtigungen für Datenobjekte und Objektgruppen (mind. Assets, Risiken, Maßnahmen) müssen möglich sein.
- Prozessbezogene Zugriffsbeschränkung jeweils gegliedert nach dem Verantwortungsbereich müssen möglich sein (Es muss die Bearbeitung nur zugeordneter Daten/Vorgänge, wie z.B. Asset- und Risk-Assessment-Prozesse möglich sein).
- Es muss eine Mehrfachzuordnung von Rollen und Geltungsbereichen pro Nutzer möglich sein.

- Auswertungen und Reports müssen geltungsbereichs- und rollenabhängig erstellt werden können.
- Eine rollen- und regelbasierte Delegation von Aufgaben, Verantwortlichkeiten und Bearbeitungsmöglichkeiten soll per systemgenerierter Benachrichtigung gem. Kap. 3.1.3.11.3 möglich sein (inkl. Übergabe von Werten wie z.B. Gültigkeitszeitraum und betroffene Objekte/ Prozesse).
- Die Geltungsbereiche sollen hierarchisch angelegt werden können, sodass Freigabeberechtigungen für übergeordnete Organisationseinheiten auf darunterliegende Organisationseinheiten vererbt werden können (z. B. Regionen/Ländergruppen, Länder, Projekte).

3.1.5.2 Rollenkonzept

3.1.5.2.1 Administration

Rolle	Berechtigungen	Kernaufgaben
Technischer Administrator	○ Anlegen, Ändern und Löschen allgemeiner Systemzugriffsrechte und Inhalte ○ Einschränkung und Erweiterung von Zugriffsrechten auf individuelle Systemfunktionalitäten, Schaltflächen, Objekte, Berichte und Daten ○ Vorgangsbezogene Vergabe von Zugriffsrechten ○ Organisations- und hierarchiebezogene Vergabe von Berechtigungen ○ Geltungsbereich- und vorgangsspezifische Vergabe von Berechtigungen ○ Entzug von Berechtigungsprofilen	○ Technische Systemadministration ○ IAM-Berechtigungs-automatisierung

Rolle	Berechtigungen	Kernaufgaben
	und Zugriffsrechten sowohl nutzerspezifisch als auch mittels Massenzuweisungen ○ Zeitlich befristete Vergabe von Berechtigungen ○ Anlegen, Ändern und Löschen von Inhalten, Templates, Eingabemasken, Berichte und graphischer Elemente ○ Anlegen, Ändern und Löschen von Workflow-Konfigurationen • Anlegen, Ändern und Löschen von Business Rules / Kalkulationslogiken (z.B. Risikobewertung, Vererbungs- und Verteilungsprinzip etc.) ○ Anlegen, Ändern und Löschen der Inhalte der Kontexthilfe	
Fachliche Administration	• Anlegen, Ändern und Löschen allgemeiner Systemzugriffsrechte und Inhalte • Einschränkung und Erweiterung von Zugriffsrechten auf individuelle Systemfunktionalitäten, Schaltflächen, Objekte, Berichte und Daten • Vorgangsbezogene Vergabe von Zugriffsrechten	

Rolle	Berechtigungen	Kernaufgaben
	• Organisations- und hierarchiebezogene Vergabe von Berechtigungen • Geltungsbereich- und vorgangsspezifische Vergabe von Berechtigungen • Entzug von Berechtigungsprofilen und Zugriffsrechten sowohl nutzerspezifisch als auch mittels Massenzuweisungen • Zeitlich befristete Vergabe von Berechtigungen • Konfiguration der Datenvalidierung • Anlegen, Ändern und Löschen der Geltungsbereiche • Anlegen, Ändern und Löschen von Erinnerungen und Wiedervorlagen • Anlegen, Ändern und Löschen von Inhalten, Datenfelder, Templates, Eingabemasken, Berichte und graphischer Elemente • Anlegen, Ändern und Löschen von Workflow-Konfigurationen • Anlegen, Ändern und Löschen von Business Rules / Kalkulationslogiken (z.B. Risikobewertung, Vererbungs- und Verteilungsprinzip etc.) • Anlegen, Ändern und Löschen der Inhalte der Kontexthilfe	

3.1.5.2.2 Standardrollen im Informationssicherheitsmanagement

Das Rollen- und Berechtigungskonzept wird in Zusammenarbeit mit dem AN erarbeitet werden. Folgende ISM-relevante Organisationsrollen existieren in der GIZ:

- ISM-Team (zentrale Einheit des ISMS-Betriebs)
- ISB-T (strategische Rolle im ISM und DSM; siehe Standardrolle im DSM Kap. 3.1.5.2.3)
- ISO (operative Einheit in der Außenstruktur)
- ISK (operative Einheit in der Innenstruktur)
- Führungskräfte als verantwortliche und freigebende Rolle für die Risiken in ihrem Geltungsbereich; Pflege von Assets, Maßnahmen und Risk Assessments werden vorrangig durch Aufgabendelegationen durchgeführt. Diese sollen in der Lage sein, Vertretungen zu benennen.

Das Mengengerüst (Kap. 3.1.6) ist eine grobe Schätzung basierend auf den vorhandenen Funktionen der Informationssicherheitsorganisation sowie Führungskräfte, die zukünftig in der SaaS-Lösung für die dezentrale Datenpflege im Asset- und Risikomanagement verantwortlich sein werden. Die genaue Funktionsbeschreibung der Führungskraft und Umsetzung im Tool sind mit dem AN zu erarbeiten.

3.1.5.2.3 Standardrollen im Datenschutzmanagement

Rolle	Berechtigungen	Kernaufgaben
Melder für Meldungen zum VVT (Eingeschränkter Zugriff)	○ Lesen & Schreiben von Meldungen für das VVT im zuständigen Geltungsbereich	○ Eigenständiges Anlegen von Meldungen für das VVT über Online-Formulare
Melder Bieter-Prüfungen (Eingeschränkter Zugriff)	○ Lesen & Schreiben von Bieterprüfungen im zuständigen Geltungsbereich	○ Eigenständiges Anlegen von Bieterprüfungen über Online-Formulare
Datenschutz-Management-Team (DSMT)	○ Lesen, Erfassen und Bearbeiten von Meldungen im VVT im gesamten Geltungsbereich ○ Lesen, Erfassen und Bearbeiten	○ Unterstützung der Datenverantwortlichen Stellen im Risikobewertungs-Prozess ○ Durchführung von Risikobewertungen

Rolle	Berechtigungen	Kernaufgaben
	von Bieterprüfungen im gesamten Geltungsbereich ○ Lesen, Erfassen und Bearbeiten von Datenschutz-Folgeabschätzungen (DSFA) im gesamten Geltungsbereich ○ Lesen, Erfassen und Bearbeiten von Risikoanalysen und Risikoauswertungen ○ Auswertung und Reporting basierend auf Daten des gesamten Geltungsbereichs	bei Meldungen zum VVT, der Bieterprüfung und der DSFA ○ Durchführung von Risikoanalysen und Risikoauswertungen mit Freigabe ○ Nachverfolgung der Risikobehandlung ○ Reporting
ISB-T	○ Lesen von Meldungen im VVT im gesamten Geltungsbereich ○ Lesen von Datenschutz-Folgeabschätzungen (DSFA) im gesamten Geltungsbereich ○ Lesen von Risikoanalysen und Risikoauswertungen	○ Strategische Rolle, keine operativen Aufgaben

Rolle	Berechtigungen	Kernaufgaben
	○ Lesen von freigegebenen Reports des gesamten Geltungsbereichs	
Data Helpdesk (DHD)	○ Lesen von Meldungen im VVT im gesamten Geltungsbereich ○ Lesen von Bieterprüfungen im gesamten Geltungsbereich ○ Lesen, Erfassen und Bearbeiten von Datenschutz-Folgeabschätzungen (DSFA) im gesamten Geltungsbereich ○ Lesen, Erfassen und Bearbeiten von Risikoanalysen und Risikoauswertungen ○ Auswertung und Reporting basierend auf Daten des gesamten Geltungsbereichs	○ Unterstützung der Projektverantwortlichen (Datenverantwortlichen) Stellen im Beratungsprozess ○ Durchführung von Risikobewertungen im Rahmen der DSFA ○ Reporting
Datenschutz-beauftragte	○ Lesen von Meldungen im VVT im gesamten Geltungsbereich ○ Lesen von Bieterprüfungen	○ Strategische Rolle, operative Aufgaben bei Audits und Betroffenenanfragen.

Rolle	Berechtigungen	Kernaufgaben
	im gesamten Geltungsbereich ○ Lesen und Bearbeiten von Datenschutz-Folgeabschätzungen (DSFA) im gesamten Geltungsbereich ○ Lesen von Risikoanalysen und Risikoauswertungen ○ Auswertung und Reporting basierend auf Daten des gesamten Geltungsbereichs	
Verlängerte Werkbank DSM	○ Lesen, Erfassen und Bearbeiten von Meldungen im VVT im gesamten Geltungsbereich ○ Lesen von Bieterprüfungen im gesamten Geltungsbereich	○ Unterstützung der Datenverantwortlichen Stellen im Risikobewertungs-Prozess ○ Durchführung von Risikobewertungen bei Meldungen zum VVT ○ Durchführung von Risikoanalysen und Risikoauswertungen

3.1.6 Mengengerüst

Die SaaS-Lösung wird unternehmensweit für die im Rollen- und Berechtigungskonzept (Kap. 3.1.5) dargestellten Rollen eingesetzt, für die eine entsprechende Anzahl an Lizenzen benötigt werden. Die Lizenznutzung umfasst Wartung, Pflege, Support und Betrieb durch den Auftragnehmer. Zudem müssen eine spätere Lizenzerweiterung, paralleler Zugriff sowie die

bedarfsgerechte Erweiterung der Systemressourcen bei steigendem Parallelzugriff möglich sein.

Die Lizenz – wenn es sich um nutzergruppenorientierte Lizenzen handelt – muss folgende Anzahl der Nutzer abdecken:

Nutzer-gruppe	**Rolle**	**Usertyp**	Gesamtzahl potenzieller Nutzer je Rolle	**Gesamtzahl je Nutzergruppe**
Administra-toren	Technischer Administrator	Admin	2	4
	Fachlicher Administrator	Admin	2	
ISM-Nutzer	ISM-T	Standardnutzer	45	671
	ISO	Standardnutzer	50	
	ISK	Standardnutzer	15	
	ISB-T	Standardnutzer	3	
	Führungskraft (2 je Organisations-einheit)	Standardnutzer	558	
DSM-Nutzer	DSM-T	Standardnutzer	15	33
	Data Helpdesk (DHD)	Standardnutzer	10	
	Datenschutz-beauftragte (DSB)	Standardnutzer	5	
	Verlängerte Werkbank DSM	Standardnutzer	3	
	Gesamt		708	**708**

Dies gilt auch, wenn eine Unternehmenslizenz zum Einsatz kommt.

<u>Eingeschränkter Zugriff über Online-Formulare/Fragebögen (eingeschränkte Nutzer):</u>

Weiterhin besteht die Anforderung, dass zusätzlich alle GIZ-Mitarbeitenden ca. **25.000** Nutzer mit eingeschränktem Zugriff die Möglichkeit haben eine Meldung zur VVT und Bieterprüfung inkl. der datenverarbeitenden Stellen einreichen (siehe Kap. 3.1.1.1.1) sowie Assets, Risk

Assessments und Maßnahmen via formularbasierte Datenerfassung (Kap. 3.1.2.2.8) pflegen zu können. Dies ist mittels eines vorgeschalteten Web-Formulars umzusetzen.

3.2 Leistungen in den Implementierungsphasen

3.2.1 Implementierungsplan

Der PL des AN erstellt den Implementierungsplan und übernimmt dabei vorher besprochene Teilaufgaben. Der Implementierungsplan enthält Beschreibungen zu Meilensteinen, Zeitbedarf, benötigten Informationen/Ressourcen und die IT-Anbindung an die GIZ-Systemlandschaft. Drittanbieter-Einbindungen müssen durch den AN vollständig verantwortet werden.

Anforderungen an den Inhalt:

- Detaillierter Implementierungsplan inkl. Meilensteinen und erwarteter Zeitdauer für Installation, Konfiguration und Inbetriebnahme (durch den AN) in Abstimmung mit dem AG
- Rollen-/Ansprechpartnerkonzept für die Implementierung (GIZ: 2 fachliche/technische Ansprechpartnerinnen und Entscheidungsträger; Auftragnehmer: bis zu 2 primäre fachliche/technische Ansprechpartnerinnen)
- Phasenbezogene Darstellung benötigter fachlicher und technischer Informationen (je Implementierungsphase)
- Zeitliche Einplanung der IT-Anbindung an die GIZ-Systemlandschaft (Zeitpunkt und Abhängigkeiten)
- Ressourcen- und Kapazitätsplanung für die Implementierung (benötigte Personal-Kapazitäten der GIZ: Anzahl/Qualifikationen; sonstige Ressourcen wie Tester, Testumgebung)

3.2.2 Einrichtung der Systemumgebung und Herbeiführung der Betriebsbereitschaft der SaaS-Lösung

Das Entwicklungspersonal und der Testmanager des AN müssen die SaaS-Lösung einrichten sowie Funktionalität und Performance gemeinsam mit der AG testen und die Tests dokumentieren.

Anforderungen:

- Einrichtung der SaaS-Lösung durch den AN gemäß Kap. 3.1.1 (Funktionale Anforderungen (DSM)) und 3.1.2 (Funktionale Anforderungen (ISM)) sowie notwendige modulübergreifende Funktionen aus Kap. 3.1.3 in der Staging-Umgebung (System-Aufbau), Produktivumgebung (Übernahme nach fachlicher Testabnahme) und Testumgebung (Konfiguration neue Komponenten) gemäß Kap. 3.1.3.1.5.

- Einrichtung Funktionalitäts- und Performance-Tests durch den AN für die technischen Anbindung (einschließlich Dokumentation)

  Testumfang:

  - Zugriff mit Microsoft Edge Chromium auf die Anwendung
  - Anmeldung mit GIZ-Kennung über SAML (SSO)
  - Korrektheit der Rechtezuordnung innerhalb der Anwendung
  - Zugriff auf Produktiv-, Staging- und Testumgebung der SaaS-Lösung
  - Debugging von identifizierten Fehlern im technischen und fachlichen Test

  Abnahmekriterien:

  - Zugriff über den definierten Edge-Browser (gem. Kap. 2.9 und Kap. 3.1.4.1.2)
  - Funktionierende Multifaktor-Authentifizierung (gem. Kap. 3.1.4.1.2)
  - Funktionierendes Rollen- und Berechtigungsmanagement (Kap. 3.1.5)
  - Umsetzung der Anforderungen gemäß Kap. 3.1.4.1.5 in der Staging-Umgebung mit Abnahme ebenda und anschließender Produktivsetzung
  - Zugriff auf die Staging-Umgebung für mindestens 3 Pilotbenutzer je Rolle gemäß Kap. 3.1.5.2
  - Zugriff auf Staging- und Testumgebung gemäß Kap. 3.1.4.1.5

- Begleitung des fachlichen Abnahmetests durch den Fachbereich DSM/ISM:
  - Debugging von Fehlern in der Anwendung
  - Fachlicher und technischer Support im Rahmen des Debuggings

3.2.3 Datenmodell-Analyse und Modellierung inklusive Update

Das Entwicklungspersonal und der Testmanager des AN müssen das bestehende ISMS- und DSMS-Datenmodell analysieren, ein Ziel-Datenmodell im neuen System erstellen und die Migrationstauglichkeit sowie Nutzbarkeit durch Tests nachweisen.

Anforderungen:

- Analyse des aktuellen Datenmodells (bestehende DSMS- und ISMS-Datenbank und CSV-Datenablagen) gemeinsam mit dem AG am Anfang der Implementierung und Update zu Beginn der Implementierung für die ISM-Daten
- Beratung zur Überführung bisheriger Datenmodelle in das neue System gemäß Bedarfen
- Modellierung des künftig genutzten Datenmodells im neuen System auf Basis der Analyse
- Tests zur Prüfung der Datenmodell auf folgende Funktionalität:
  - Kompatibilität zwischen altem und neuem Datenmodell (CSV)
  - Nutzbarkeit des neuen Datenmodells im neuen System

- Unterstützung durch den AN bei der Datenbereinigung
- Fehlerhafte Daten identifizieren
- Bereinigung des bereitgestellten Datenexportes

Abnahmekriterien des Datenmodells:

- Erfolgreiche Überführung der Bestandsdaten
- Nutzbarkeit und Einsehbarkeit der Bestandsdaten

Update Datenmodell-Analyse und Modellierung für ISM

Das Entwicklungspersonal und der Testmanager des AN müssen erstelle Datenmodellanalyse in der Implementierungsphase für DSM auf die Aktualität des aktuellen Anforderungstand der ISM-Funktionalität überprüfen und ggf. anpassen.

Anforderungen:

- Überprüfung und Anpassung des Datenmodells für die ISMS-Funktionalitäten
- Tests zur Prüfung der Datenmodell auf folgende Funktionalität:
  - Kompatibilität zwischen altem und neuem Datenmodell
  - Nutzbarkeit des neuen Datenmodells im neuen System
  - Unterstützung durch den AN bei der Datenbereinigung
  - Fehlerhafte Daten identifizieren
  - Bereinigung des bereitgestellten Datenexportes

Abnahmekriterien des Datenmodells:

- Problemlose Überführung der Bestandsdaten
- Nutzbarkeit und Einsehbarkeit der Bestandsdaten

3.2.4 Datenmigration

3.2.4.1 Allgemein

Das Entwicklungspersonal des AN muss die Migration der Daten aus dem DSM- und ISM-Altsystem (auf Grundlage eines CSV-Exports) in die neue SaaS-Lösung vollständig, konsistent und nachvollziehbar planen, durchführen, qualitätssichern und dokumentieren. Die Migration ist abgestimmt mit GIZ-Ansprechpartnern und dem externen Dienstleister durchzuführen und muss Betriebsunterbrechungen minimieren.

Anforderungen:

- Datenmigration aus dem bestehenden DSM- und ISM-Altsystemen in die Datenbank der neuen SaaS-Lösung (Vollständige, konsistente und nachvollziehbare Übernahme relevanter Daten für Datenschutz und des ISM)

- Größe der zu migrierenden Datenbasis für DSM: ca. 800 MB, ca. 3,5 Mio. Datensätze (CSV-Exporte)
- Größe der zu migrierenden Datenbasis für ISM: 7 GB relevante Daten (CSV-Exporte)
- Die Verantwortung für Planung, Durchführung, Qualitätssicherung und Dokumentation der Migration liegt beim AN in enger Abstimmung mit den technischen und fachlichen Ansprechpartnern der GIZ

3.2.4.2 Datenqualität und -konsistenz

Das Entwicklungspersonal des AN muss vor der Migration eine Datenkompatibilitätsanalyse durchführen und ein Datenbereinigungskonzept vorlegen; die Migration muss fachlich korrekt und ohne Datenverlust/-verfälschung erfolgen.

Anforderungen:

- Datenkompatibilitätsanalyse vor Migration auf Basis bereitgestellter Testdatensätze
- Konzept zur Datenbereinigung (z.B. Dublettenprüfung, Plausibilitätsprüfungen, Pflichtfeldprüfungen). Die Durchführung der Datenbereinigung liegt in der Verantwortung des AG. Der AN steht für Rückfragen während der Datenbereinigung für den AG zur Verfügung.
- Korrekte fachliche Zuordnung der Daten in der Zielanwendung
- Ausschluss von Datenverlusten und Datenverfälschungen (Backup und Rollback Verfahren)

3.2.4.3 Migrationsverfahren und -durchführung

Das Entwicklungspersonal des AN muss Migration und Abnahme über ein detailliertes Migrationskonzept/-plan mit Datenmapping, Testläufen und revisionssicherer Dokumentation steuern. Die Migration ist erst nach formaler Abnahme abgeschlossen.

Anforderungen:

- Vor jedem Migrationslauf ist sicherzustellen, dass eine Sicherung des bereits bestehenden Datenbestands (Backup) vorhanden ist, auf welche im Fehlerfall zurückgegangen werden kann (Rollback)
- Detailliertes Migrationskonzept und vollständiger Migrationsplan (Meilensteine, Zeitdauer) in Abstimmung mit dem AG
- Migration in Test- und Produktivläufen auf Basis eines Migrationsplans mit definiertem Datenmapping (Mapping der Datenstrukturen der Bestandssysteme auf die Datenstruktur der SaaS-Lösung zur Importfähigkeit)
- Kennzeichnung nicht importierbarer Datensätze
- Überführung importierter Daten (Verzeichnis der Verarbeitungstätigkeiten, TOM-Prüfung Auftragsverarbeiter „Bieterprüfung“, durchgeführte DSFAs) in die jeweiligen

Funktionsmodule des DSM (s. Kap. 3.1.1) und in die jeweiligen ISM-Funktionsmodule (s. Kap. 3.1.2)

- Manuelles Datenfeld-Mapping, Testmigrationen zur Prüfung von Vollständigkeit/Konsistenz/Plausibilität, revisionssichere Dokumentation, formale Abnahme der finalen Übernahme und Rollback-Konzept (Test- und Produktivumgebung; Abnahme durch fachliche GIZ-Ansprechpartner)
- End-to-End-Tests vor Datenmigration inkl. Dokumentation zur Prüfung von Vollständigkeit, Verfügbarkeit und Integrität der migrierten Daten in der SaaS-Lösung
- Fachliche und technische Prüfungen nach Migration inkl. Unterstützung der Abnahmetests sowie Dokumentation/Behebung von Abweichungen und Fehlern; Migrationsabschluss erst nach formaler Abnahme.

  Abnahmekriterien:

  - Migration der Daten gemäß Datenanalyse/-modellierung Kap. 3.2.3
  - Vollständige Einträge;
  - Verfügbarkeit Sprachen gemäß Kap. 3.1.3.9
  - Verfügbarkeit aller zu migrierenden DSM-Daten und Datenkategorien
  - Rollen- und berechtigungskonforme Verfügbarkeit und Nutzbarkeit migrierter Daten (Daten sind je Rolle/Berechtigung einsehbar, bearbeitbar, löschbar und exportierbar)
    - Unterstützte Migrationsdateiformate (weitere Formate nach Abstimmung):
  - .xls,
  - .xlsx
  - .csv,
  - .json,
  - .xml
    - Migration referenzierter Anhänge und Mediendateien mit Abrufbarkeit am Ursprungsobjekt (Datenformate der Anhänge: .docx, .pdf, .xlsx, .xlsm, .jpg, .png, .bmp)
    - Bereitstellung vollständiger Migrationsdokumentation (geeignet für spätere Audits und erneute Migration) bestehend aus:
  - Migrationskonzept
  - Datenmapping
  - Transformationsregeln
  - Testergebnissen
  - Abnahmeprotokollen
  - Manuelle Migration technisch nicht migrierbarer Datensätze durch AN

3.2.5 Beratung und Konzeptentwicklung bei der Einrichtung der Rollen- und Berechtigungen für ISM

Vorgeschaltet zur Einrichtung der Rollen- und Berechtigungen im ISM-Modul entwickelt der PL oder das Entwicklungspersonal des AN gemeinsam mit dem Fachbereich der GIZ das konkrete Rolle- und Berechtigungskonzept zur Umsetzung in der SaaS Lösung.

Anforderungen:

- Beratung Einrichtung von Rollen und Berechtigungen im System basierend auf Kap. 3.1.5 und 3.1.6
    - Das konkrete Rollen- und Berechtigungskonzept zur Umsetzung in der SaaS für ISM ist erarbeitet und vom GIZ-Fachbereich zur Umsetzung in der SaaS Lösung freigegeben. Die Erarbeitung erfolgt basierend auf den Kap. 3.1.5 und 3.1.6

3.2.6 Einrichtung der Rollen und Berechtigungen

Das Entwicklungspersonal des AN muss Rollen und Berechtigungen gemäß den Anforderungen einrichten, testen und anschließend die Rollenverwaltung an die GIZ-Administratoren übergeben.

Anforderungen:

- Einrichtung von Rollen und Berechtigungen im System gemäß Kap. 3.1.5. (DSM-Rollen und gemeinsam von AN und AG erarbeitetes ISM-Rollen- und Berechtigungskonzept)
- Übergabe der Rollen- und Berechtigungsverwaltung an Administratoren der GIZ
- Durchführung von Tests der Rollen und Berechtigungen. Zu prüfen sind:
    - Einrichtung von Rollen und Berechtigungen gem. Anforderungen aus Kap. 3.1.5 (DSM-Rollen und gemeinsam erarbeitetes ISM-Rollen- und Berechtigungskonzept)
    - Vergabe von Rollen und Berechtigungen für Nutzer durch fachliche und technische Administratoren und Automatisierung über IAM
    - Übereinstimmung der Nutzeransicht mit eingerichteten Rollen und Berechtigungen

  Abnahmekriterien:

    - Rollen und Berechtigungen gemäß Kap. 3.1.5 sind umgesetzt
    - Funktionsfähige Rollen-/Berechtigungsvergabe durch die GIZ-Administration
    - Rollen- und berechtigungskonforme Sicht- und Bearbeitbarkeit von Daten je Nutzerin/Nutzerinnengruppe

3.2.7 Einrichtung der Schnittstellenanbindung an bestandsführende Tools der GIZ (CMDB und Prozessdaten)

Für die Abbildung des Asset-Inventar sollen Schnittstellen zur CMDB (beinhaltet IT-Asset-Informationen) und zum BPNM-Tool (beinhaltet Prozessinformationen) mit automatisierter Aktualisierung eingerichtet werden.

Das Entwicklungspersonal des AN muss je Datenbank eine Test- und eine Produktivschnittstelle einrichten und die Abnahme über definierte Testfälle und Synchronisationskriterien sicherstellen.

Anforderungen:

- Einrichtung je Quellsystem einer Test- und einer Produktivschnittstelle durch AN für den Datenaustausch gem. Kap. 3.1.4.1.4
- Schnittstellenanbindung an IT-Assets-Datenbank (CMDB, Inhouse SQL-Datenbank) gem. Kap. 3.1.4.1.4
- Schnittstellenanbindung an Prozessmanagement-Datenbank (BPMN, SaaS-Lösung im Aufbau) gem. 3.1.4.1.4
- Durchführung von Tests der Schnittstellenanbindung in der Staging- und Testumgebung (sofern eingeführt) gemäß Anforderungen aus Kap. 3.1.4.1.5

  Abnahmekriterien:

  - Abnahme vordefinierter Fallbeispiele im Testsystem (durch technischen und/oder fachlichen GIZ-Administration)
  - Import/Synchronisation nach vorgegebenem Zeitplan (durch technischen Systemverantwortlichen)
  - Kostenneutrale Anpassung der Import-/Synchronisationszeiten mit keiner oder sehr geringer Ausfallzeit (unter 10 Minuten)

3.2.8 Projektmanagement durch die Projektleitung des AN

Der AN stellt ein PL für die Kommunikation mit der GIZ-PL und zur Koordination des Projektteams auf der AN-Seite.

Anforderungen:

- Projekt- und Terminsteuerung: Backlog mit AG-Seite erstellen, nachhalten der Aufgaben, des AG-Abhängigkeiten zwischen Projektaktivitäten pflegen, Meilensteine nachhalten, Abweichungen früh adressieren. Genutzt wird hierzu Azure DevOps der AG-Seite.

- Koordination & Kommunikation: Abstimmungen moderieren, Verantwortlichkeiten klären, Entscheidungen protokollieren, Statusberichte bereitstellen.

- Budget- und Kostenkontrolle: Aufwände und Kosten (z. B. Lizenzen, Betrieb, Implementierung) planen, überwachen und berichten.

- Qualitätssicherung in der Implementierungsphase: Testkonzept und -pläne koordinieren, Testdurchführung und Fehlernachverfolgung steuern, Abnahmekriterien prüfen und Abnahmen organisieren.

- Rollout, Schulung und Übergabe: Rollout- und Cutover-Plan umsetzen, Schulungen koordinieren, Betriebs-/Support-Übergabe mit Dokumentation sicherstellen.

3.2.9 Schulungen und Betriebsdokumentation

Das Entwicklungspersonal des AN muss während der gesamten Vertragslaufzeit auf Einzelabruf des AG rollenbezogene Schulungen zur Nutzung der SaaS-Lösung durchführen. Die Schulungen sind als live moderierte Webinare/Online-Schulungen mit Aufzeichnung, über Microsoft Teams bereitzustellen. Ziel ist die zielgruppengerechte Vermittlung der Kenntnisse, die für das Arbeiten in der jeweiligen Rolle erforderlich sind. Die Schulungen müssen grundsätzlich in deutscher Sprache und bei Bedarf auch in englischer Sprache durchgeführt werden können. Ausbildungskonzepte, Schulungsinhalte und Schulungsmaterialien sind je Zielgruppe mit dem AG abzustimmen und durch den AN regelmäßig an neue Funktionen, geänderte Prozesse und sonstige relevante Anpassungen der SaaS-Lösung anzupassen.

3.2.9.1 Benutzerhandbücher

Das Entwicklungspersonal des AN muss für die SaaS-Lösung ein rollenbezogenes Standard-Benutzerhandbuch für die nachfolgenden Zielgruppen als ausführliche Nutzungsdokumentation und Handlungsanweisung bereitstellen. Das Benutzerhandbuch muss die relevanten Funktionen, Prozesse und Arbeitsschritte nachvollziehbar beschreiben. Das Benutzerhandbuch ist dauerhaft zur internen Nutzung, Weitergabe und Nachschulung bereitzustellen.

Das Benutzerhandbuch ist je Zielgruppe in deutscher und/oder englischer Sprache (siehe Tabelle in Kap. 3.2.9.2) bereitzustellen. Es muss aktuelle Screenshots, verständliche Schritt-für-Schritt-Beschreibungen und Hinweise zur produktiv betriebenen Version enthalten. Der AN muss während der Vertragslaufzeit fortlaufend die jeweils aktuelle digitale Handbuchversion (ggf. als Online-Dokumentation oder PDF) bereitstellen.

Abweichungen vom Standard sowie GIZ-spezifische Sonderkonfigurationen und Anpassungen sind separat zu dokumentieren und bei Änderungen zu aktualisieren. Die GIZ erhält das Eigentum an dieser separaten Dokumentation.

3.2.9.2 Zielgruppen und Lernziele der Schulungen

Die Schulungen richten sich an unterschiedliche User entsprechend der Rollenbeschreibungen aus Kap. 3.1.5.2.

DSM

Gruppe / Zielgruppe	**Fachliche und technische Administratoren**	**DSM-T/DHD**
Format / Qualifikation der Schulungs-leitung	Interaktives, live moderiertes Webinar; Durchführung durch einen fachlichen und einen technischen Experten	Interaktives, live moderiertes Webinar
Umfang / Dauer	**2 Schulungstermine** • Umfang je Schulungstermin: 3 Schulungstage à 8 Stunden • Gesamtumfang je Schulungstermin: 24 Stunden • Gesamtumfang Schulungen: 48 Stunden **4 zusätzliche vertiefende Frage-/Antwort-Termine** ○ Umfang je Termin: 4 Stunden ○ Gesamtumfang Frage-/Antwort-Termine: 16 Stunden **Gesamtumfang: 64 Stunden**	**2 Schulungstermine** ○ Umfang je Schulungstermin: 2 Schulungstage à 8 Stunden ○ Gesamtumfang je Schulungstermin: 16 Stunden ○ Gesamtumfang Schulungen: 32 Stunden **4 zusätzliche vertiefende Frage-/Antwort-Termine** ○ Umfang je Termin: 4 Stunden ○ Gesamtumfang Frage-/Antwort-Termine: 16 Stunden **Gesamtumfang: 48 Stunden**
Sprache der Schulung	Deutsch	Deutsch
Teilnehmende	4	25
Lernziel	Schulung von DSM- und ISM-Inhalten zur eigenständigen fachlichen und technischen Administration sowie	Schulung zum Funktionsumfang, zur Systembedienung und zur eigenständigen

	Befähigung zur internen Wissensweitergabe („Train the Trainer“) an weitere Nutzergruppen.	Anwendung der Datenschutzprozesse gem. Kap. 3.1.1.
Unterlagen / Handouts	Administratorenhandbuch zur internen Nutzung und Nachschulung (Sprache: Deutsch und Englisch)	Rollenübergreifendes Standard-Benutzerhandbuch (Sprache: Deutsch)
Aufzeichnung	Die Sessions werden aufgezeichnet und der AN erklärt sich einverstanden, dass eine Aufzeichnung über das Konferenzsystem der GIZ erfolgt.	Die Sessions werden aufgezeichnet und der AN erklärt sich einverstanden, dass eine Aufzeichnung über das Konferenzsystem der GIZ erfolgt.

Die Meldenden der VVT-Meldungen, der Bieterprüfungen, der verlängerten Werkbank und die Datenschutzbeauftragten erhalten interne Schulungen aus dem DSM-T Team.

Weitere Schulungen bzw. Anpassungen können im Bedarfsfall während der Vertragslauzeit abgerufen werden.

ISM

Gruppe / Zielgruppe	ISM-T & ISB-T	ISOs	ISKs	Führungskräfte*
Format / Qualifikation der Schulungsleitung	Interaktives, live moderiertes Webinar	Interaktives, live moderiertes Webinar	Interaktives, live moderiertes Webinar	WBT oder Online-Streamcast (als Mitwirkungs-leistung des AN)
Umfang / Dauer	**2 Schulungstermine** ○ Umfang je Schulungstermin: 3 Schulungstage à 8 Stunden ○ Gesamtumfang je Schulungstermin: 24 Stunden ○ Gesamtumfang Schulungen: 48 Stunden **4 zusätzliche vertiefende Frage-/Antwort-Termine** ○ Umfang je Termin: 4 Stunden ○ Gesamtumfang Frage-/Antwort-	**6 Schulungstermine** ○ Umfang je Schulungstermin: 1 Schulungstag à 4 Stunden ○ Gesamtumfang Schulungen: 24 Stunden **3 zusätzliche vertiefende Frage-/Antwort-Termine** ○ Umfang je Termin: 4 Stunden ○ Gesamtumfang Frage-/Antwort-Termine: 12 Stunden **Gesamtumfang: 36 Stunden**	**2 Schulungstermine** ○ Umfang je Schulungstermin: 2 Schulungstage à 8 Stunden ○ Gesamtumfang je Schulungstermin: 16 Stunden ○ Gesamtumfang Schulungen: 32 Stunden **4 zusätzliche vertiefende Frage-/Antwort-Termine** ○ Umfang je Termin: 4 Stunden ○ Gesamtumfang Frage-/Antwort-	**Erstellung der Schulungsunterlagen** ○ Keine Livepräsentation bzw. Durchführung eines Schulungstermins ○ Umfang für die Erstellung: 1 Arbeitstag

	Termine: 16 Stunden **Gesamtumfang: 64 Stunden**		Termine: 16 Stunden **Gesamtumfang: 48 Stunden**	
Sprache Schulung	Deutsch	Englisch	Deutsch	Deutsch und Englisch
Teilnehmende	bis zu 48	bis zu 50	15	-
Lernziel	Schulung zum Funktionsumfang, zur Systembedienung und zur eigenständigen Anwendung der Informationssicherheitsprozesse (u.a. Asset-Management, Schutzbedarfsfeststellung, Risk Assessment, Maßnahmenplanung, Maßnahmennachverfolgung, Reporting, Datenauswertung) gem. Kap. 3.1.2.	Schulung zum Funktionsumfang, zur Systembedienung und zur eigenständigen Anwendung der Informationssicherheitsprozesse (u.a. Asset-Management, Schutzbedarfsfeststellung, Risk Assessment, Maßnahmenplanung, Maßnahmennachverfolgung, Reporting, Datenauswertung) gem. Kap. 3.1.2.	Schulung zum Funktionsumfang, zur Systembedienung und zur eigenständigen Anwendung der Informationssicherheitsprozesse (u.a. Asset-Management, Schutzbedarfsfeststellung, Risk Assessment, Maßnahmenplanung, Maßnahmennachverfolgung, Reporting, Datenauswertung) gem. Kap. 3.1.2.	Schulung von Führungskräften in ihrer Rolle als Asset-, Risiko- und Maßnahmenverantwortliche zum eigenständigen Management von Risiken im eigenen Verantwortungsbereich, insbesondere zur Schutzbedarfsfeststellung und zum Risk Assessment gemäß Kap. 3.1.2. Die Schulungsinhalte sind mit dem AG abzustimmen.
Unterlagen / Handouts	Rollenübergreifendes Standard-Benutzerhandbuch (Sprache: Deutsch)	Rollenübergreifendes Standard-Benutzerhandbuch (Sprache: Englisch)	Rollenübergreifendes Standard-Benutzerhandbuch (Sprache: Deutsch)	Rollenübergreifendes Standard-Benutzerhandbuch (Sprache: Deutsch und Englisch)
Aufzeichnung	Die Sessions werden aufgezeichnet und der AN erklärt sich einverstanden, dass eine Aufzeichnung über das Konferenzsystem der GIZ erfolgt.	Die Sessions werden aufgezeichnet und der AN erklärt sich einverstanden, dass eine Aufzeichnung über das Konferenzsystem der GIZ erfolgt.	Die Sessions werden aufgezeichnet und der AN erklärt sich einverstanden, dass eine Aufzeichnung über das Konferenzsystem der GIZ erfolgt.	-

Weitere Schulungen bzw. Anpassungen können im Bedarfsfall während der Vertragslauzeit abgerufen werden.

3.2.9.3 Betriebshandbuch

Das Entwicklungspersonal des AN muss ein Betriebshandbuch in deutscher Sprache zur SaaS-Lösung in editierbarer Form bereitstellen, gemeinsam mit der GIZ pflegen und bei Änderungen zeitnah aktualisieren. Das Betriebshandbuch muss die Basisversion der SaaS-Lösung vollständig beschreiben und insbesondere SaaS-bedingte administrative, technische und betriebliche Besonderheiten hervorheben.

Aktualisierungen sind unaufgefordert bereitzustellen und Änderungen nachvollziehbar zu kennzeichnen, insbesondere durch Hervorhebung geänderter, ergänzter oder gestrichener Passagen sowie durch eine Änderungsübersicht. Der AN muss die GIZ bei der Adaption des Betriebshandbuchs auf GIZ-spezifische Inhalte, Konfigurationen und Schnittstellen unterstützen und Änderungen genehmigen.

Der AN wirkt nach Vorgaben des technischen Systemverantwortlichen und unter Nutzung der GIZ-Vorlagen an der Erstellung und Pflege mit. Dies umfasst insbesondere Rollen und Verantwortlichkeiten, technische Beschreibungen einschließlich Systemlandschaft, Schnittstellen, Backup und Wiederherstellung, Notfallkonzept sowie Systemsicherheit. Weitere Inhalte sind bei Bedarf der GIZ zu unterstützen. Die angepassten Betriebshandbücher sind Eigentum der GIZ.

3.3 Optionale Leistungen während der Vertragslaufzeit

3.3.1 Schnittstellenanbindung

Das Entwicklungspersonal des AN muss zukünftig auf Abruf folgende weitere als „muss“-Anforderung deklarierten Schnittstellen in Kap. 3.1.4.1.4 in der Produktiv- und Staging sowie der Testumgebung für den Datenaustausch einrichten:

- Lieferantenmanagement-Software (zukünftige Ausschreibung): Die Anwendung stellt der SaaS-Lösung Lieferanteninformationen bereit, damit diese im ISM-Asset-Management gemäß Kap. 3.1.2.1 redundanzfrei dokumentiert und weiterverwendet werden können.
- Unternehmensrisikomanagement-Software: Die SaaS-Lösung liefert aggregierte Informationssicherheitsrisiken an die Unternehmensrisikomanagement-Software. Derzeit ist MIRAI (Corporator) im Einsatz.
- Raum- und Gebäudemanagement-Software: Die Anwendung stellt der SaaS-Lösung Raum- und Gebäudemanagementdaten redundanzfrei bei der Asset-Erfassung zur Verfügung (Kap. 3.1.2.1) bereit. Derzeit ist WaveWare im Einsatz.
- ITSM-, Change- und Incident-Management-Software: Der AN muss in der Produktiv-, Staging- und Testumgebung (Kap. 3.1.4.1.5) eine Schnittstelle zwischen der SaaS-Lösung als Single Source of Truth und der ITSM-, Change- und Incident-Management-Anwendung für den Datenaustausch einrichten. Es soll eine bidirektionale Schnittstelle eingerichtet werden, in der Datenfelder ausgetauscht werden oder mit Hilfe von Workflows systemwechselseitig weiterverarbeitet werden können. Derzeit ist ServiceWare im Einsatz.

- GRC-Suite: Die SaaS Lösung stellt der GRC-Suite Informationen aus dem Risiko- und Asset-Management nach vorheriger Definition zur Verfügung.

3.3.2 Beratungs- und Programmierleistungen

Bei Bedarf können während der Vertragslaufzeit optionale Beratungs- und Programmierleistungen u.a. zu folgenden Punkten abgerufen werden:

- Anpassung von Auswertung-, Reporting- und Dashboard-Funktionalitäten
- Anpassung der eingeführten Schnittstellen aufgrund von technischen Änderungen der SaaS-Lösung
- Datenmodellierung
- Datenmigration
- Einrichtung von Rollen und Berechtigungen
- Integration in bestehende Systeme
- Ggf. Einrichtung weiterer Schnittstellen
- Unterstützung bei der Behebung von Problemen und Durchführung von Optimierungen
- Unterstützungsleistungen bei Release-Wechsel
- Unterstützung bei der Anpassung des Systems an neue Anforderungen, die während der Vertragslaufzeit auftauchen, z.B. das Hinzufügen von neuen Funktionen oder Modulen
- Weitere Customizing-Leistungen, falls Bedarf besteht (z.B. Delegationsfunktionen, Eskalationslogik, Kalkulationsfunktionen).
- Updates der Dokumentationen (Betriebshandbuch, Benutzerhandbuch)

3.3.3 Aktivitäten zum Vertragsende

Der AN stellt sicher, dass die AG nach Vertragsende seine im System gespeicherten Daten und Konfigurationen vollständig und ohne unzumutbare Einschränkungen in eine andere Lösung migrieren kann.

Der PL und das Entwicklungspersonal des AN ist verpflichtet, die Daten der AG zum Vertragsende ohne zusätzliche Vergütung verfügbar zu machen. Dies umfasst folgende Daten:

- Datenmodell
- API-Dokumentation und Schnittstellenbeschreibungen
- Customizing-Dokumentation
- Audit-Logs

Der Export muss in offenen und dokumentierten Formaten erfolgen. Sind zusätzliche Unterstützungsleistungen zum Vertragsende (z.B. bei der Datenmigration) notwendig, können diese gemäß Preisposition 5.7 B02_GIZ-DSM-_ISM-Tool_Preisblatt abgerechnet werden.

Der AN stellt sicher, dass die Daten nach Übergabe vollständig gelöscht werden.

3.3.4 Audit-Management Modul (ISM)

Der AN stellt ein Audit-Management im ISM-Modul bereit bzw. schaltet Audit-Funktionalitäten frei. Dies umfasst folgende Funktionen:

- Audit-Planung
- Checklisten zur Audit-Durchführung
- Auswertungsfunktionalitäten von Audit-Findings
- Dokumentation der Abweichungen
- Maßnahmennachverfolgung im Maßnahmenregister (Kap. 3.1.2.2.6 und 3.1.2.2.7)

3.3.5 Datenimport von Prozessdaten als Back-Up Lösung

Der AN importiert manuelle Prozessdaten aus einer CSV-Datei nach Durchlauf der Aktivitäten der Datenmigration gem. den Anforderungen in Kap. 3.2.4

3.3.6 Beratungsleistung Testmanagement

Der AN stellt Beratungsleistungen / Personal für die Rollen im Testmanagement insbesondere für die Rolle Testmanager zur Verfügung gemäß den Anforderungen der aus Kap. 4.3.

3.3.7 Beratungsleistung Projektmanagement

Der AN stellt Beratungsleistungen/Personal für di Rollen im Projektmanagement, insbesondere für die Rolle PL zur Verfügung gemäß den Anforderungen aus Kap. 4.1.

3.3.8 Weitere Schulungsleistungen

Der AN stellt optional weitere Schulungen für die einzelnen Zielgruppen gemäß Kap. 3.2.9.2 bereit.

4. Personaleinsatz des AN

4.1 Projektleitung

Der AN stellt für die Implementierungsphase des neuen Systems eine PL. Die Leistung umfasst die Projektplanung für die einzelnen Abrufe und das Projektmanagement sowie die fachliche und technische Beratung durch die PL von AN-Seite. Diese stellt die Schnittstelle zur GIZ-PL dar.

Die zukünftig eingesetzte PL seitens des AN soll die folgenden spezifischen Berufserfahrungen mitbringen und mittels des Dokuments B0X_GIZ-DSM-_ISM-Tool_Erfahrungsiwssen_Projektleitung“ nachweisen.

- 3 Jahre Berufserfahrung in der Beratung und Begleitung bei der Einführung von SaaS-basierten Tools, davon mindestens 1 Jahr mit einem SaaS-basieren Tool mit Funktionalitäten DSM/ISM., idealerweise mit dem angebotenen Tool.
- 3 Jahre Erfahrung im Projektmanagement, insbesondere mit agilen Methoden (z.B. Scrum, SAFE), klassischen oder hybriden Vorgehensmodellen
- Grundlegendes Verständnis von Integrations- und Schnittstellenkonzepten (z.B. APIs, Schnittstellenarchitektur) und die Fähigkeit, technische Themen zwischen Fachbereich, AG (IT und GIZ-PL) und AN (Entwicklungsteam) zu koordinieren

Die PL stimmt die mit der AG festgelegten Aufgaben und Termine des Projekts ab und nimmt außerdem an den gemeinsamen Arbeitssitzungen teil. Darüber hinaus berät die PL zur technischen und fachlichen Umsetzung des DSM-/ISM-Tools und stimmt das Vorgehen mit

der AG ab. Nach Erfordernis sind für diese Beratungsleistungen weitere fachverantwortliche Personen des AN hinzuzuziehen. Zusätzlich erstellt die PL des AN Projektpläne zur Implementierung der SaaS-Lösung.

Der AN stellt sicher, dass es für die PL eine Stellvertretung gibt, die im Falle der Abwesenheit der PL die Projektplanung und das Projektmanagement, sowie die Beratungsleistungen übernimmt. Die Stellvertretung muss über vergleichbare fachliche und technische Qualifikationen verfügen.

4.2 Entwicklungspersonal

Wenigstens 2 Personen des Entwicklungspersonals müssen mindestens 1 Jahre Entwicklungserfahrung haben. Die eingesetzten Entwickler müssen Kenntnisse in folgenden Datenstrukturen vorweisen:

- KPI-Definition,
- Reporting-Aufbau,
- Dashboarding
- Historisierung

Die personellen Ressourcen sollen für die komplette Projektlaufzeit geplant werden.

4.3 Testmanager

Testmanagement ist eine optionale Rolle, die der AG bei Bedarf abruft. Der Testmanager unterstützt die fachliche GIZ-PL in allen Belangen des Testmanagement (vom Testkonzept bis Testplanung und -Überwachung). Die Person soll 2 Jahre Erfahrung im Testmanagement haben, und Kenntnisse in folgenden Themen mitbringen:

- Erstellung von Testkonzepten,
- Schätzung von Testaufwänden,
- Testplanung für Releases / Sprints
- Risikoanalyse des Tests
- Unterstützung in der Testdurchführung und Fehlernachverfolgung
- Prüfung und Organisation von Abnahmen