B. 1 Leistungsbeschreibung

Verfahren	**„Business Process Management (BPM) & Governance Risk and Compliance (GRC)Tools als Software as a Service“**
Vergabe-Nr.	

Inhalt

1. Unternehmensprofil und Ausgangslage 2
2. Beschaffungsgegenstand 2
   2.1 Allgemeine Beschreibung 2
      2.1.1 SaaS 2
      2.1.2 Weitere Leistungen 3
   2.2 Laufzeit 4
3. Übergreifende Key Requirements (Kernanforderungen) 4
4. Durch die BPM & GRC-Lösung abzudeckende Funktionsbereiche und Leistungsparameter 8
   4.1 Funktionsbereich Prozessmodellierung/ Prozessworkflow 8
5. Funktionsbereich Information Security Management (ISMS) 8
   5.1 Funktionsbereich Internes Kontrollsystem (IKS) 9
   5.2 Funktionsbereich Business Continuity Management (BCM) 11
6. Weitere Funktionalitäten, die von dem Auftraggeber optional bezogen werden können 13
   6.1 Funktionsbereich Operationelles Risiko (OpRisk) 13
   6.2 Funktionsbereich Audit 13
   6.3 Funktionsbereich KPI-Messung 15
7. Mengengerüst 16

1. Unternehmensprofil und Ausgangslage

Die FMS Wertmanagement AöR (im Folgenden **FMS-WM** oder **Auftraggeber**) ist eine organisatorisch und wirtschaftlich selbstständige, teilrechtsfähige Anstalt des öffentlichen Rechts innerhalb der Bundesanstalt für Finanzmarktstabilisierung (FMSA).

Der Auftraggeber wickelt in einem bankähnlichen Setup die übernommenen Kredite, Wertpapiere und sonstigen Finanzinstrumente ab, ist aber dabei rechtlich keine Bank, kein Finanz- oder Wertpapierdienstleister und auch keine Versicherung nach der Definition des Kreditwesengesetzes oder der EU-Richtlinie 2006/48/EG. Gleichwohl bestehen bestimmte regulatorische Anforderungen an die FMS-WM:

Die FMS-WM unterliegt für ihre Tätigkeit der Aufsicht der BaFin und muss insbesondere die von der BaFin veröffentlichten Mindestanforderungen an das Risikomanagement (MaRisk) erfüllen. Die FMS-WM setzt die Anforderungen des Digital Operational Resilience Acts (Verordnung (EU) Nr. 2022/2554) (nachfolgend „DORA“) für nicht systemrelevante Kreditinstitute um. Die FMS-WM führt kein Informationsregister und unterliegt keinen Meldepflichten aus der DORA.

Weitere Informationen zur FMS-WM befinden sich unter **www.fms-wm.de**.

Die FMS-WM ist aktuell im Begriff, ihr Betriebsmodell zu verschlanken und kostenoptimiert aufzustellen. Hierbei sollen nach Möglichkeit standardisierte Softwareprodukte als SaaS Lösungen genutzt werden.

2. Beschaffungsgegenstand

2.1 Allgemeine Beschreibung

2.1.1 SaaS

Die FMS-WM beschafft vorliegend im Wege einer europaweiten Ausschreibung eine **Software as a Service (SaaS)** mit den **initial zu nutzenden Funktionalitäten**:

1. zum Management ihrer Geschäftsprozesse, sog. Business Process Management (**BPM**),
2. zum Management ihrer Non-Financial-Risikoarten im Wege von (i) **ISMS** als auch (ii) Business Continuity Management (**BCM**) und (iii) Internes Kontrollsystem (**IKS**) und

Darüber hinaus umfasst die zu beschaffende Software as a Service auch die folgenden **Funktionalitäten**, die von der FMS-WM **optional** in Anspruch genommen werden können:

3. zum Management ihrer Non-Financial-Risikoarten mit Funktionalitäten für OpRisk und Audit, sowie die Unterstützung bei der KPI-Messung externer Dienstleister,

Die letztgenannten, in Nr. 3 aufgeführten, Funktionalitäten müssen ebenfalls Teil des Angebots sein. Allerdings wird die FMS-WM diese Funktionalitäten nur optional zu einem Zeitpunkt in der Zukunft (voraussichtlich nicht vor 2028) in Anspruch nehmen.

Die vorstehend skizzierten und im Weiteren noch detaillierten und in verschiedene Themenbereiche geclusterten Anforderungen an die Funktionalitäten des Beschaffungsgegenstandes werden nachfolgend auch Business Process Management & Governance, Risk and Compliance bzw. **BPM & GRC-Lösung** genannt.

2.1.2 Weitere Leistungen

Sofern nicht ohnehin in der Ausgestaltung als SaaS enthalten, sind folgende weitere Leistungen Gegenstand der Ausschreibung:

- Der Dienstleister stellt die Services gesamtheitlich, also insbesondere inklusive der darunter erforderlichen Infrastrukturen, Lizenzen, dem Betrieb (inkl. 2nd, 3rd Level Support) und der Weiterentwicklung, als SaaS bereit.
- Der 2nd Level-Support erfolgt in deutscher und englischer Sprache
- Das Angebot umfasst während der Vertragslaufzeit Software-Updates bzw. Upgrades oder andere Änderungen, z.B. an der Plattform oder Infrastruktur, wobei ein sog. **Evergreening**-Ansatz verfolgt werden muss. Das Evergreening muss insbesondere die folgenden Tätigkeiten und Aufwendungen auf Seiten des Anbieters enthalten:
    - Notwendige Änderungen/Fixes/Patches am Service,
    - Versions-Upgrades des Services (und aller technischen Komponenten, die zur Erbringung des Services erforderlich sind), unabhängig ob „Major“ oder „Minor“ Upgrades,
    - Durchführung der im Rahmen von Upgrades/Updates notwendigen Änderungen an den ursprünglich vom Anbieter zur Erfüllung der Anforderungen vorgesehenen FMS-WM-spezifischen Konfigurationen, Anpassungen oder Erweiterungskomponenten des Services,
    - Providerseitig durchgeführte Tests aller von ihm zur Verfügung gestellten Funktionalitäten und Vorhalten der Testdokumentation
    - Providerseitiges Change- und Testmanagement (soweit notwendig, ist in Ausnahmefällen der Auftraggeber bei fachlichen Abnahmetests einzubeziehen).
- Zusätzlich zur Bereitstellung der Services kann fallbezogen und auftragsweise die Hinzunahme von Beratungsleistungen durch die FMS-WM angefordert werden (**Professional Services**).
- Der Auftragnehmer ist im Rahmen der **Implementierung** der angebotenen BPM & GRC-Lösung insbesondere verantwortlich für:
    - Konzeptionierung und Durchführung von Schulungen auf Deutsch und auf Englisch (End-User und Service Desk zur Leistung des 1st Level Supports)
    - Erstellung und Abstimmung eines Implementierungsplans für die von ihm angebotene Lösung (Aktivitäten, Verantwortlichkeiten, Ressourcen, Zeit und notwendige Beistellungen seitens der FMS-WM, etc.)
    - Bereitstellung der entsprechenden Systemumgebung, Herstellung der technischen Zugriffe und Einrichtung der User (Basis: gemeinsam abgestimmtes Rollenkonzept der FMS-WM)
    - Schlüsselfertige fachliche Grundkonfiguration/Parametrisierung der Lösung, die die Anforderungen der FMS-WM erfüllt
    - Migration/Input der notwendigen Daten der FMS-WM (im Wesentlichen System – und Organisationsinformationen, ggf. Prozessdaten aus ARIS)
    - Anbindung der notwendigen Schnittstellen (Microsoft Entra ID, ggf. OMADA und Service Now)
    - Fachliche Konfiguration und technische Einrichtung der notwendigen Reports und Workflows
    - Planung, Durchführung und Dokumentation der notwendigen Testaktivitäten (z.B. technische Tests, Datenmigrationstests, funktionale Tests, Integrationstests)

- Durchführung Go-live Support
- kontinuierliche Dokumentation der Implementierungsergebnisse.

Der Auftragnehmer soll sicherstellen, dass die initial zu nutzenden Funktionalitäten der BPM & GRC-Lösung innerhalb von drei Monaten nach Zuschlag und Vertragsstart von der FMS-WM erfolgreich abgenommen und in ihren Regelbetrieb überführt werden können.

Für alle Fragestellungen wird der Auftraggeber mindestens einen Ansprechpartner bereitstellen, um die toolunabhängigen und unterstützenden Vorbereitungen zu treffen. Ferner stellt der Auftraggeber einen Projektleiter auf seiner Seite bei, der die Einführung der Lösung auf Seiten der FMS-WM steuert.

Der Auftraggeber stellt Testdaten und Testkapazitäten bei.

2.2 Laufzeit

Die initiale Vertragslaufzeit beträgt fünf Jahre. Die Vertragslaufzeit beginnt mit dem Start der Implementierung, die sich unmittelbar an die Zuschlagserteilung anschließt. An die initiale Vertragslaufzeit schließen sich zwei Verlängerungsoptionen an: Zunächst um drei weitere Jahre und im Anschluss um zwei weitere Jahre. Die maximale Vertragslaufzeit beträgt damit zehn Jahre (5+3+2 Jahre).

Dabei soll es sich um zwei einseitige Verlängerungsoptionen zugunsten des Auftraggebers handeln. Bei Ausgestaltung als einseitige Verlängerungsoptionen zugunsten des Auftraggebers wird dies im Rahmen der vorzunehmenden Bewertung des anzubietenden Vertrags positiv bewertet werden.

Sofern der Auftragnehmer nicht bereit ist, einseitige Verlängerungsoptionen zugunsten des Auftraggebers anzubieten, sind die Verlängerungsoptionen beidseitig (Ausübung der Verlängerungsoptionen nur im beiderseitigen Einverständnis) auszugestalten. Die positive Bewertung im Rahmen der vorzunehmenden Vertragsbewertung entfällt in diesem Fall.

Zu beachten ist, dass Vertrag und Preise für den Verlängerungszeitraum nicht der Neuverhandlung unterliegen dürfen. Preislich kommt für die erste Verlängerung der fixe Preis für das fünfte Vertragsjahr zur Anwendung, der für das sechste Jahr und über den Verlängerungszeitraum jährlich um einen indexbasierten Inflationsausgleich angepasst wird. Für die zweite Verlängerung wird der Preis für das achte Vertragsjahr zugrunde gelegt und wiederum jeweils um einen indexbasierten Inflationsausgleich für das neunte und zehnte Vertragsjahr ergänzt.

3. Übergreifende Key Requirements (Kernanforderungen)

Die nachstehenden Anforderungen, die für sämtliche vertragsgegenständlichen Funktionalitäten erfüllt sein müssen, sind in der Spalte „**MUSS**“ aufgeführt. Darüberhinausgehende Anforderungen für sämtliche vertragsgegenständliche Funktionalitäten sind in der Spalte „**SOLL**“ aufgeführt. Deren Vorliegen wird im Rahmen der Angebotsbewertung **positiv bewertet** werden.

Anforderung	MUSS	SOLL
Hosting/ Bereitstellung der Funktionalitäten	Die zu beschaffenden Funktionalitäten müssen als Software-as-a-Service (SaaS) angeboten werden. Neben einer Produktiv-umgebung muss eine Testumgebung für die Implementierungsphase und während Upgrades sowie auf Anforderung der FMS-WM zur Verfügung gestellt werden. Der Auftragnehmer muss die Funktionalitäten in einer, mit Blick auf die definierten An-forderungen an IT-Security und Datenschutz geeigneten Infrastruktur betreiben	

	und der FMS-WM zur Nutzung bereitstellen. Für diese Cloud Services sind während der gesamten Vertragslaufzeit adäquate Informationssicherheitsvorgaben zu wahren, die insbesondere die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit der Daten sicherstellen. Die FMS-WM geht von einer Integration und Zugriff auf die SaaS über eine marktübliche Windows Standard Umgebung (z.B. über Standard Webbrowser oder Fat-Client) aus.	
Sicherheits-konzept	Im Hinblick auf Cyber-Risiken muss der Auftragnehmer ein hohes Maß an Sicherheit für sein System gewährleisten. Die Absicherung der betriebenen Umgebung(en) ist eine zentrale Leistungsanforderung. D.h. typische IT-Plattform- und Sicherheitsservices sind vom Auftragnehmer zu leisten. Diese umfassen zwingend: - die Betriebssystem- und Plattformhärtung, - Zugriffs- und Identitätsschutz, - Netzwerksicherheit, - Datensicherheit, - Monitoring und Logging. Die oben aufgeführten IT-Plattform- und Sicherheitsservices sind in einem Sicherheitskonzept marktüblich, für einen fachkundigen Dritten nachvollziehbar, zu dokumentieren. Daneben sind auch Schwachstellen- und Penetrationstests durchzuführen sowie eine Security Incident Detection nachzuweisen. Hierzu ist es notwendig, dass Verletzungen der Cybersicherheit systemseitig erkannt und entsprechende Warnungen generiert werden. Die Überwachung der für den Kunden erbrachten Dienstleistungen erfolgt mittels eines SIEM-Systems, einschließlich der Möglichkeit, relevante Alarme weiterzuleiten.	Eine Weiterleitung relevanter Log-Informationen an die SIEM-Systeme des Kunden soll möglich sein.
Kontrollberichte	Damit der Auftraggeber seine gesetzlichen und regulatorischen Anforderungen einhalten kann muss der Auftragnehmer jährliche Kontrollberichte in einem offiziellen Standard wie ISAE 3402 Type II oder	

	PS951 Typ 2 oder vergleichbaren Formaten vorlegen, sofern der Bericht die für FMS-WM erbrachte Dienstleistungen umfasst. Ersatzweise können andere geeignete Nachweise vereinbart werden.	
Funktionsumfang im Standard	Die vertragsgegenständlichen Funktionalitäten müssen im Zeitpunkt des Angebots bereits als SaaS entwickelt und im Standard angeboten werden. Die Funktionalitäten müssen in den Anwendungssprachen Deutsch und Englisch verfügbar sein.	Die vertragsgegenständlichen Funktionalitäten sollen eigenständig durch die FMS-WM entsprechend ihren Bedürfnissen konfiguriert werden können und nicht der Anpassung durch den Auftragnehmer nach Vorgaben des Auftraggebers bedürfen.
Service Management	Der Auftragnehmer betreibt Service Management Prozesse, welche er in die Service Management Prozesse des Auftraggebers integriert. Hinsichtlich der Verfügbarkeit ist die derzeitige Erwartungshaltung wie folgt: • **Recovery Time Objective (RTO)**: 3 Tage (72 Stunden) als maximal zulässige Zeitdauer zur Wiederherstellung der Anwendung bei Ausfall. • **Recovery Point Objective (RPO)**: 1 Tag (24 Zeitstunden) als maximale Zeitspanne des letzten Datenwiederherstellungspunkt bei Ausfall. • Die **Systemverfügbarkeit** ist bei einer Zielerreichung von mindestens 98,0 % im Jahresmittel in der Zeit von Montag bis Freitag, exklusive deutscher Bankfeiertage von 8:00 Uhr bis 16:00 Uhr erfüllt. Sofern es im Einzelfall nicht vermeidbar ist, dass ein Wartungsfenster in der zugesicherten Servicezeit liegt, ist ein solches, mit Ausnahme von Notfall-Patches, mit dem Auftraggeber mit angemessenem Zeitvorlauf vorab abzustimmen. Die Leistungserbringung wird anhand von Service Leveln gemessen.	Die **Servicezeit**, zu der Fehlerbehebungen durchgeführt werden und 2nd und 3rd-Level Support zur Verfügung stehen, sollen von Montag bis Freitag, exklusive deutscher Bankfeier-tage in der Zeit von 08:00 Uhr bis 16:00 Uhr CET gewährleistet sein. Wartungsarbeiten, während derer das System nicht zur Verfügung steht, sollen außerhalb des vertraglich vorgegebenen Zeitfensters der Servicezeit liegen.
Datenhaltung und integrierte Lösung	Alle vertragsgegenständlichen Funktionsbereiche sind entweder in einer einzigen	Die Lösung soll über eine zentrale Datenhaltung verfügen (zentrales Repository).

	SaaS Lösung integriert, oder aber es bestehen jedenfalls Schnittstellen zwischen den angebotenen Funktionalitäten/Funktionsbereichen, welche vom Auftragnehmer über die Laufzeit des Vertrags auf-rechterhalten und betreut werden (als Bestandteil der angebotenen Leistung).	
Kollaborations-fähigkeit	Die Lösung muss kollaboratives Arbeiten durch Mehrbenutzer-Zugriffsrechte und Rollenkonzepte, Kommentarfunktionen, Review-Workflows sowie Benachrichtigungssysteme bei Änderungen unterstützen.	
Import /Export von Daten des Auftraggebers	Die vertragsgegenständlichen Funktionalitäten müssen den Im- und Export von Daten des Auftraggebers von/in Excel ermöglichen.	Die vertragsgegenständlichen Funktionalitäten sollen den Im- und Export von Daten des Auftraggebers von/in gängige Formate wie z.B. PDF, Word, XML (z.B. ARIS), BPMN, HTML mit konfigurierbaren Vorlagen ermöglichen. Der Import von Massendaten (bspw. Übernahme aus bestehendem ARIS-System soll möglich sein).
Versionierung	Eine Versionierung der freigegebenen Modelle und Richtlinien/Anweisungen des Auftraggebers muss in sämtlichen vertragsgegenständlichen Funktionalitäten möglich sein.	
Freigabe-prozesse	Das Tool muss über anpassbare Freigabe-prozesse, z.B. Vier-Augenprinzip, für alle vertragsgegenständlichen Funktionalitäten verfügen. Ein integrierter Freigabeprozesse muss sicherstellen, dass Prozessmodelle vor der Veröffentlichung qualitätsgesichert werden. Gleichzeitig dürfen Modelle und Richtlinien vor der finalen Freigabe nicht allgemein für Nutzer sichtbar sein.	Mehrstufige Freigabeprozesse sollen ermöglicht werden können. Die Möglichkeit zur Wiedervorlage soll in den Funktionalitäten integriert sein.
Revisions-sicherheit	Seitens der Benutzer mit Schreibrechten durchgeführte Änderungen müssen revisionssicher für einen Zeitraum von mind. 450 Tagen gelogged werden.	
Performance	Die Software muss fähig sein, mindestens - 1000 Prozesse, - 1000 Dokumente, - 1000 Risiken mit entsprechenden Maßnahmen mit angemessenen Antwortzeiten des	

	Systems zu verwalten.	

4. Durch die BPM & GRC-Lösung abzudeckende Funktionsbereiche und Leistungsparameter

4.1 Funktionsbereich Prozessmodellierung/ Prozessworkflow

Die Funktionalitäten der SaaS zur professionellen Prozessmodellierung müssen die FMS-WM bei der systematischen Erfassung, Analyse, Optimierung und Dokumentation ihrer Geschäftsprozesse unterstützen und bilden die Grundlage für Prozessoptimierung, Digitalisierung und Compliance-Management.

Die folgenden Anforderungen bestehen dabei an die Lösung:

Anforderung	MUSS	SOLL
Grafische Darstellung von Geschäftsprozessen	Die Lösung muss eine der etablierten Notationen BPMN 2.0 oder EPK abdecken. Es müssen hierarchische Prozesslandkarten mit der Möglichkeit eines Drill-downs vom strategischen Überblick bis zur detaillierten prozessualen Arbeitsanweisung erstellt werden können. Die Lösung muss geeignet sein, die Prozesse als Dokumentation für Mitarbeiter lesend zugänglich zu machen.	
Dokumentenmanagement	Die Lösung muss eine Dokumentenmanagement-Funktionalität beinhalten.	

5. Funktionsbereich Information Security Management (ISMS)

Die folgenden Anforderungen bestehen an die Lösung:

Anforderung	MUSS	SOLL
Informationssicherheitsrisiken	Es muss eine Risikoanalyse betreffend die Informationsrisiken ermöglicht werden. Dies beinhaltet mindestens einen Vergleich der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen. Die Risikoanalyse berücksichtigt darüber hinaus z.B. mögliche Bedrohungen, das Schadenspotenzial, die Schadenshäufigkeit sowie den Risikoappetit. Für die durchzuführende Risikoanalyse müssen Soll-Maßnahmen und Ist-Zustände hinterlegbar und anpassbar sein. Anpassungen müssen sowohl hinsichtlich	**Risikoanalyse:** Ermittelte Restrisiken sollen in eine Risikomatrix überführt werden können. Die Lösung soll die Erteilung von Ausnahmegenehmigungen nachhalten und Auswertungen über die Ergebnisse der Risikoanalyse ermöglichen. Die Risikoanalyse soll auch möglich sein für Systeme, die nicht in den Prozessen abgebildet sind.

	der Anzahl der anzuwendenden Maßnahmen je Anwendungstyp bzw. Schutzbedarf und hinsichtlich der Ausformulierung der Sollmaßnahmen möglich sein. Im Anschluss an die finale Ermittlung der Schutzbedarfe müssen für nicht erfüllte Sollmaßnahmen monetäre Restrisiken ermittelt werden können. Die Lösung muss ein nachvollziehbares Verfahren zur unterjährigen Identifikation, Bewertung und Dokumentation neu auftretender oder wesentlich veränderter IT-Risiken ermöglichen.	
Ermittlung Bedrohungslage		Mithilfe der Lösung soll die spezifische Bedrohungslage anhand eines seitens der FMS-WM individuell definierbaren Bedrohungskatalogs ermittelt werden können.
Abbildung Informationsverbund nach BAIT / DORA	Die Lösung muss die Einrichtung und Pflege eines Inventars aller Informations- und IKT-Assets ermöglichen. Dies beinhaltet: 1. Geschäfts- und Unterstützungsprozesse 2. IT-Systeminventare 3. Schnittstellen zwischen den IT-Systemen 4. Darstellung der Vernetzung des Informationsverbundes mit Dritten (z.B. andere SaaS-Dienstleister) 5. Netz- und Gebäude-Infrastrukturen Die Lösung muss mindestens den Im- und Export der oben angegebenen Daten (z.B. Excel/CSV) ermöglichen. Die manuelle Pflege von Informationen wie Geschäfts- und Unterstützungsprozessen sowie Netz- und Gebäude-Infrastrukturen im System muss möglich sein.	
Risikomaßnahmen	Die Lösung muss die Definition und Dokumentation von Maßnahmen zur Risikobehandlung (Vermeidung, Mitigation, Transfer, Akzeptanz), ermöglichen.	

5.1 Funktionsbereich Internes Kontrollsystem (IKS)

Die Lösung, muss die Dokumentation, Analyse und Verwaltung eines internen Kontrollsystems unter der Einhaltung regulatorischer Anforderungen ermöglichen.

Die folgenden Anforderungen bestehen:

Anforderung	**MUSS**	**SOLL**
Interne Kontrollen	Die systematische Erfassung und Verwaltung interner Kontrollen mit den Attributen - Kontrolltyp (z.B. präventiv, detektiv, korrektiv, manuell, automatisiert), - Kontrollhäufigkeit, - Verantwortlichkeiten, - Wirksamkeit muss möglich sein.	Die Lösung soll die - Definition von Wirksamkeits-kriterien, Kontrollzielen, Prüf-zyklen der Kontrolle, - Erfassung von Kontrolltestings und Ergebnissen - Nachverfolgung von Maßnahmen bei Kontrollschwächen ermöglichen. Risiken und Prozessschritte sollen automatisch mit den Kontrollen vom System verknüpft werden. Die Lösung soll einen integrierten Workflow zur Bestätigung der Durchführung der Kontrollen inkl. Eskalationsmechanismen beinhalten.
IKS-spezifisches Reporting	Die Lösung muss über Auswertungsmöglichkeiten zu Kontrollanpassungen verfügen, um Differenzen in einem Bericht darstellen zu können.	
Kontroll-wirksamkeits-prüfung		Die Lösung soll eine Funktion zum Testmanagement für die Kontroll-wirksamkeitsprüfung beinhalten

5.2 Funktionsbereich Business Continuity Management (BCM)

Die Lösung muss bei der systematischen Planung, Implementierung und Aufrechterhaltung von Maßnahmen zur Geschäftskontinuität unterstützen.

Die folgenden Anforderungen bestehen:

Anforderung	MUSS	SOLL
Regulatorische Anforderungen		Die BCM-Funktionalität soll an einen der folgenden Standards: - ISO 22301 oder - BSI 200-4 angelehnt sein.
Notfalldokumente	Die BCM-Funktionalität muss die zentrale Verwaltung aller - BCM-relevanten Dokumente, - Status-Übersichten, - Reporting-Funktionen mit standardisierten und Ad-hoc-Berichten, - Management- und Audit-Reports umfassen.	Die Lösung soll eine über-sichtliche Darstellung des BCM-Status durch grafische Aufbereitung anbieten,
Krisenpläne	Die BCM-Funktionalität muss die Erstellung von - Plänen zu Business Continuity und Disaster Recovery mit vor-definierten Vorlagen, - Eskalationsprozessen, - Alarmierungsketten, - Handlungsanweisungen, - Checklisten, - Kommunikationsplänen ermöglichen.	
Geschäftsfortführungs-pläne	Mit der BCM-Funktionalität müssen abteilungsspezifische Geschäftsfortführungspläne des Auftraggebers erstellt werden können.	
Wiederanlaufpläne	Die BCM-Funktionalität muss die Erstellung abteilungsspezifischer Wiederanlaufpläne des Auftraggebers abbilden können.	
Kommunikationsmatrix	Die BCM-Funktionalität muss eine zentrale Verwaltung aller kontinuitätsrelevanten Ressourcen, wie z.B. interne/externe Kontaktpersonen, oder Single Points of Failure ermöglichen.	
Notfallkontakte		Die BCM-Funktionalität soll eine

		Krisenstabsorganisation mit Rollen und Verantwortlichkeiten, sowie workflowgesteuerte Alarmierungs- und Eskalationsprozesse bieten. Darunter fallen z.B. die folgenden Rollen: - Notfallkoordinatoren, - Notfallbeauftragte, - Mitglieder des Krisenmanage-mentteams
Notfallübun-gen/ Mehrjah-resübungsplan	Die BCM-Funktionalität muss eine syste-matische Planung der BCM-Tests er-möglichen.	Es soll die Möglichkeit bestehen, einen Mehrjahresübungsplan er-stellen zu können.
Notfalldoku-mentation		Die Lösung soll im Falle eines Not-falls beim Auftraggeber die Mög-lichkeit bieten, diesen entspre-chend zu dokumentieren.
BCM-spezifi-sches Report-ing		Die BCM-Funktionalität soll Stan-dardberichte (quartärlicher Bericht an die Geschäftsleitung), Dash-boards, Drilldown-Analysen und Exporte von Arbeitsdokumenten aus dem System ermöglichen.
Schutzbedarfs-analyse	Die BCM-Funktionalität muss die erfor-derlichen Funktionalitäten zur Durchfüh-rung der Schutzbedarfs-analyse beinhal-ten. Die Business Impact Analyse und die Schutzbedarfsanalyse müssen auch möglich sein, wenn ein Asset in keinem (im BPM-Modul) abgebildeten Prozess erfasst bzw. abgebildet ist (z.B. techni-sche Anwen-dung).	Die Ermittlung der Schutzbedarfe soll nach dem Maximalprinzip erfol-gen. Das bedeutet, der in den Er-hebungen höchste vergebene Wert wird für die weiteren Bewertungen fort-geschrieben.
Business Im-pact Analyse	Die BCM-Funktionalität muss um-fas-sende Funktionen zur Durchführung von Business Impact Analysen bieten, ein-schließlich - Identifikation und Klassifizierung kriti-scher Geschäftsprozesse, - Ermittlung von MTPD (Maximum Tole-rable Period of Disruption) - RTO (Recovery Time Objective), - Bewertung finanzieller und nicht-finan-zieller Auswirkungen, - Analyse von Abhängigkeiten - Priorisierung von Wiederanlaufmaß-nahmen	
Notfallzugriff		Das Modul soll einen web-basier-ten Zugriff (von außer-halb der FMS-IT-Umgebung) für einen ein-

		geschränkten Benutzerkreis ermöglichen.

6. Weitere Funktionalitäten, die von dem Auftraggeber optional bezogen werden können

6.1 Funktionsbereich Operationelles Risiko (OpRisk)

Die folgenden Anforderungen bestehen:

Anforderung	MUSS	SOLL
Erfassung Risiken/ Maßnahmen/ Schadensfälle	Die Lösung muss folgende Aspekte workflow-basiert abdecken: - Identifikation und Dokumentation von Risiken, - Dokumentation von Schadensfällen, - Verknüpfung von Risiken mit Schadensfällen, - Dokumentation von Maßnahmen, sowie die Verknüpfung von Maßnahmen mit Risiken und/ oder Schadensfällen, - Maßnahmentracking	Die Lösung soll eine Funktionalität zum Managen von operationellen Risiken bereit-stellen.
Eskalationsprozess und Qualitätssicherung	Die Lösung muss folgende Aspekte abdecken: - Abbildung eines Eskalationsprozesses, - Workflows für Qualitätssicherung der Dokumentation von Risiken, Schadensfällen, Maßnahmen, - workflow-basierter Freigabe- und Bestätigungsprozess, - Möglichkeiten zum Reporting für Risiken, Schadensfälle und Maßnahmen, - Backtesting (dokumentierte Risiken versus zugeordnete Schadensfälle)	

6.2 Funktionsbereich Audit

Beschafft wird eine Funktionalität für Audit zur Unterstützung der Internen Revision, die die Planung, Durchführung, Dokumentation und Nachverfolgung von Prüfungen umfassend abbildet und Transparenz über Risiken, Prozesse, Feststellungen und Maßnahmen schafft.

Die folgenden Anforderungen bestehen an das Tool:

Anforderung	MUSS	SOLL
Zuordnung Verantwortlichkeiten	Auditfeststellungen müssen durch den Bearbeiter den verantwortlichen Personen auf Basis der hin-	

	terlegten Unternehmensorganisation zugeordnet werden können.	
Verwendung als Feststellungs-Datenbank	Die Verwendung als Feststellungs-Datenbank, d.h. eine Erfassung und Nachverfolgung von Feststellungen, muss möglich sein.	
Individualisierung	Es muss eine Anpassung an FMS-Spezifika mindestens hinsichtlich folgender Merkmale möglich sein: - Herkunft von Auditfeststellungen (bspw. FMS-WM intern, FMS-WM extern, Dienstleister A, B, etc.) - Einstufung von Feststellungen (z.B. als geringfügig, bemerkenswert, bedeutend, etc.)	Anpassung an weitere FMS-Spezifika soll möglich sein.
Berechtigungs-konzept	Es muss ein Berechtigungskonzept zur Sicherstellung des Least Privilege/ Need to know Prinzips existieren.	Die Rechtevergabe soll so aus-gestaltbar sein, dass der verantwortliche Fachbereich bestimmte Feststellungen (z.B. geringfügig) im Tool selbst schließen kann.
Uploadfunktion		Es soll eine Uploadfunktion für Dateianhänge an Feststellungen sowie eine Uploadfunktion von Feststellungen selbst in die Lösung auf Basis gängiger Dateiformate (z.B. Excel) existieren.
Änderungshistorie	Änderungen an Auditfeststellungen müssen in einer Änderungshistorie durch Audit-Mitarbeiter nachvollzogen werden können.	
Auswertung/ Reporting/Export	Grundlegende Auswertungsmöglichkeiten für Auditfeststellungen (z. B. Dashboard nach Status, Verantwortliche etc.) müssen gegeben sein und die Ergebnisse in gängigen Dateiformaten (z. B. Excel) exportiert werden können.	
Reminderfunktion		Es soll die Einrichtung und der Versand von automatisierten Erinnerungsmails an eine oder mehrere Verantwortliche von Feststellungen möglich sein.
Abbildung Auditprozess		Es soll die Abbildung des gesamten Auditprozesses mit den klassischen Phasen (Planung, Durchführung, Dokumentation, Bericht) im Tool möglich sein.

6.3 Funktionsbereich KPI-Messung

Die Lösung ermöglicht die zentrale Verwaltung von KPIs gegenüber externen Dienstleistern.
Die folgenden Anforderungen bestehen an die Lösung:

Anforderung	MUSS	SOLL
KPI-Erfassung	Die KPI-Messung von externen Dienstleistern muss möglich sein.	Die Messung soll in verschiedenen Intervallen erfolgen können. Variierende Messgrößen sollen möglich sein: Prozentuale, absolute sowie numerische Messgrößen. Das Modul soll einen Import (Upload) der Werte aus Excel ermöglichen. Das Modul soll einen Export der Werte nach Excel ermöglichen. Ein geeignetes Reporting der KPIs soll möglich sein

7. Mengengerüst

Die folgenden Informationen zur FMS-WM sind für Zwecke der Angebotsvorbereitung zugrunde zu legen.

Produktivumgebung:

Anzahl Lizenzen	200 User, die alle Leserechte besitzen, die die Nutzung aller Funktionalitäten erlauben
Administratoren	Ca. 7 der 200 User benötigen zusätzlich Administratorenrechte über alle angefragten Funktionalitäten (BPM & GRC) und Zugriff auf alle lösungsseitig angebotenen technischen und fachlichen Konfigurationsmöglichkeiten für End User.
Prozessmodellierer	Ca. 10 der 200 User benötigen Lizenzen mit dem Recht zur BPM-Prozessmodellierung.
Freigeberechte	Ca. 20 der 200 User benötigen Freigaberechte bezogen auf die BPM-Funktionalitäten. Ca. 130 der 200 User benötigen Freigaberechte hinsichtlich GRC-Funktionalitäten.
Notfallzugänge	Ein vom Auftraggeber definierter Benutzerkreis von 5 Personen soll die Möglichkeit haben, sich von extern (außerhalb des IT-Systems des Auftraggebers) in die vertragsgegenständliche SaaS einloggen zu können (z.B. via Zwei-Faktor-Authentifizierung).

Testumgebung:

Zugriffsrechte	Ca. 7 der 200 User benötigen Zugriff auf die Testumgebung.