



**Leistungsbeschreibung zur Ausschreibung einer
Rahmenvereinbarung über die Beschaffung einer
integrierten Managementsuite (ISMS, BCMS, DSMS) für die
GKD Recklinghausen und ihre Zweckverbandsmitglieder**



1. Einleitung und Zielsetzung

Die GKD Recklinghausen ist gemeinsamer kommunaler IT-Dienstleister für den Kreis Recklinghausen und acht Städte des Kreises Recklinghausen.

Die GKD beabsichtigt, eine Rahmenvereinbarung über die Beschaffung einer integrierten Managementsuite (ISMS, BCMS, DSMS) für die GKD Recklinghausen und ihre Zweckverbandsmitglieder abzuschließen.

Gegenstand dieser Ausschreibung ist der Abschluss einer Rahmenvereinbarung zur Beschaffung einer integrierten Management Tool Suite zur ganzheitlichen Unterstützung des Informationssicherheitsmanagements (ISMS), des Business Continuity Managements (BCMS) sowie des Datenschutzmanagements (DSMS) für die GKD Recklinghausen und ihre Zweckverbandsmitglieder.

Ziel ist es, eine durchgängige, konsistente und revisionssichere Unterstützung aller relevanten Managementprozesse bereitzustellen und den norm- sowie rechtskonformen Betrieb dieser Managementsysteme sicherzustellen, um von Synergieeffekten bestmöglich zu profitieren.

2. Leistungsumfang

2.1 Allgemeines

Die Rahmenvereinbarung hat eine Laufzeit von vier Jahren, beginnend mit dem **01.08.2026**.

Das maximale Abrufvolumen der Rahmenvereinbarung liegt bei 500.000,00 € netto. Es besteht keine Verpflichtung zum Abruf von Mindestabnahmemengen aus der Rahmenvereinbarung durch den Auftraggeber.

Bei den im Preisblatt aufgeführten Mengen handelt es sich um den geschätzten Bedarf. Auf die Abnahme der geschätzten Mengen erwirbt der Bieter keinen Anspruch. Über- bzw. Unterschreitungen dieser Mengen bleiben ohne Einfluss auf die Preise und die Vertragslaufzeit.

Bei Abrufen während der Vertragslaufzeit soll eine Synchronisierung der Laufzeiten entsprechend der Grundlaufzeit des Erstabrufs erfolgen. Die Preise gemäß Preisblatt sind dabei entsprechend anzupassen.

Mit der Abgabe eines Angebotes verpflichtet sich der Bieter den im Entwurf beigefügten EVB-IT Vertrag nach Individualisierung abzuschließen.

Leistungsgegenstand ist die Bereitstellung, Inbetriebnahme (Einrichtung und Installation) sowie die Pflege einer Integrierten Management Suite im Bereich GRC, nachfolgend GRC-Suite genannt. Diese soll drei dedizierte Tools zur ganzheitlichen Unterstützung des Informationssicherheitsmanagements (ISMS), des Business Continuity Managements (BCMS)



sowie des Datenschutzmanagements (DSMS) für die GKD Recklinghausen und ihre Zweckverbandsmitglieder beinhalten. Eine gemeinsame Datenbasis, d.h. eine aus CMDB und weiteren Tools importierte Asset-Struktur, dient diesen Tools dabei als Grundlage. Ziel ist es, eine durchgängige, konsistente und revisionssichere Unterstützung aller relevanten Managementprozesse bereitzustellen. Dabei ist der norm- sowie rechtskonforme Betrieb dieser Managementsysteme sicherzustellen. Um von Synergieeffekten bestmöglich zu profitieren, muss die anzubietende Lösung als integrierte Gesamtsuite bereitgestellt werden und mindestens die Tools ISMS, BCMS und DSMS umfassen. Zusätzlich wird eine Komponente zur Erfüllung der Anforderungen des NIS-2 Umsetzungsgesetzes gefordert. Es dürfen keine voneinander isolierten Einzellösungen angeboten werden. Sämtliche Module müssen auf einem gemeinsamen, konsistenten Datenbestand basieren, sodass Assets, Prozesse, Rollen, Verantwortlichkeiten und Abhängigkeiten systemübergreifend einheitlich gepflegt und genutzt werden können. Änderungen an der Datenbasis müssen sich unmittelbar und konsistent auf alle Module auswirken. Die Benutzeroberfläche der gesamten Suite sowie die zugehörige System- und Anwenderdokumentation müssen vollständig in deutscher Sprache verfügbar sein.

Im Betrieb ist vorgesehen, dass pro Institution, d.h. für die GKD Recklinghausen sowie jedes Zweckverbandsmitglied, eine eigene Instanz der Toolsuite angelegt wird, auf der ein Mehrbenutzerbetrieb vorgesehen ist. Die Administration jeder Instanz soll von einer zentralen Stelle aus möglich sein. Die Bereitstellung der Tool Suite hat ausschließlich als On-Premise-Lösung mit vollständiger Datenhoheit beim Auftraggeber zu erfolgen. Der Betrieb muss entweder auf einem Windows Server in der Version 2016 oder neuer oder alternativ auf einer Linux-basierten Umgebung beziehungsweise innerhalb einer Docker-Umgebung möglich sein. Zwingende Cloud-Abhängigkeiten sind nicht zulässig. Weitere zum Betrieb der GRC-Suite notwendige Dienste und IT-Komponenten sind durch den Bieter im Rahmen der Einrichtung zu übernehmen. Ein weiterer Teil der Einrichtung ist die Bereitstellung einer Importfunktionalität bzw. Konfiguration der notwendigen Schnittstellen durch den Bieter. Diese umfasst mindestens den Import von Assets aus den CMDB-Systemen i-doit, Matrix42 und docusnap, wobei pro Instanz nur der Import von Assets aus jeweils einem dieser Systeme vorgesehen ist. Die Anwender sollen final in die Lage versetzt werden, mit geringem Aufwand künftig selbst regelmäßige Asset-Importe und Aktualisierungen durchführen zu können. Im Rahmen der Einrichtung sollen die Hauptanwender der Tools In-House geschult werden, um die gängigen Abläufe der Managementsysteme effektiv anwenden zu können.

Im Rahmen der Pflege werden durch den Bieter in regelmäßigen Abständen Updates bereitgestellt. Dies beinhaltet Funktionsupdates, Bug-Fixes und insb. Sicherheitsupdates für kritische Komponenten, die unverzüglich bereitgestellt werden müssen.

Die Tool Suite muss die Anforderungen der einschlägigen Normen und Regelwerke der Informationssicherheit, des Kontinuitätsmanagement und des Datenschutzes vollständig abdecken. Hierzu zählen insbesondere die BSI-Standards 200-1, 200-2, 200-3 und 200-4 sowie die Anforderungen der Datenschutz-Grundverordnung (DSGVO). Die Umsetzung der



normativen Anforderungen muss systematisch, nachvollziehbar und auditfähig unterstützt werden.

2.2 Asset-Import

Die Lösung muss über umfangreiche Import- und Schnittstellenfunktionen verfügen. Insbesondere muss der Import von Daten aus i-doit, Matrix42, Docusnap sowie aus Excel- und CSV-Dateien möglich sein. Sollte für den Import der Assets keine dedizierte low-effort Importfunktionalität bereitgestellt werden, muss die Einrichtung und Konfiguration der entsprechenden Schnittstellen zu den CMDB-Systemen und MS Active Directory durch den Bieter übernommen werden. Zum Abschluss der Einrichtung wird daher gefordert, dass die jeweiligen Toolverantwortlichen bzw. Process-Owner der CMDB-Systeme mindestens dazu in der Lage sind – ohne weitere Programmierkenntnisse – weitere Assetklassen zu importieren, Aktualisierungen durchzuführen, Änderungen zu verwalten und zu mergen sowie neue Zielobjektgruppen in die gemeinsame Datenbasis zu überführen. Zusätzlich sind Schnittstellen zu Macmon NAC und PRTG wünschenswert.

2.3 Funktionen allg.

Die GRC-Suite verfügt über eine zentrale Benutzerverwaltung pro Instanz. Den Benutzern können basierend auf ihren globalen oder spezifischen Rollen Zugriffsprofile mit unterschiedlichen Berechtigungen für die Nutzung des Tools zugewiesen werden. Um eine gemeinsame Datenbasis für das ISMS, BCMS sowie DSMS Tool bereitzustellen, verfügt die GRC Suite über ein zentrales Asset Management. Hier werden Assets wie Infrastruktur, Prozesse und Personen tool-übergreifend verwaltet. Die Suite muss die Abbildung hierarchischer Prozess- und Subprozessstrukturen unterstützen. Rollen, Verantwortlichkeiten und Zuständigkeiten müssen sowohl für internes als auch externes Personal abbildbar sein und an Assets geknüpft werden können. Änderungen oder Umstrukturierungen von Assets wirken sich dabei pro Instanz global aus. Darüber hinaus werden Abhängigkeiten von Assets dargestellt. Der Datenbestand soll sowohl manuell als auch automatisiert je Mandant aktualisiert werden können, beispielsweise durch erneute Synchronisation mit angebundenen Quellsystemen. Allgemein unterstützt die GRC-Suite den Benutzer durch geeignete Umsetzungshinweise bei der Nutzung der Tools. Es besteht die Möglichkeit, Dokumente, die mithilfe der GRC-Suite erstellt wurden, als .pdf Dokumente zu exportieren.

2.4 Integriertes Management

Zusätzlich zu den dedizierten Tools ermöglicht die GRC-Suite das tool-übergreifende, effiziente Management von unterschiedlichen Bereichen. Um eine Bindung an einzelne Personen zu vermeiden, ist ein Rollenmanagement bereitzustellen, welches die Zuordnung von Verantwortlichkeiten zu Rollen zu ermöglicht. Der Wechsel von Verantwortlichkeiten oder Mitarbeitenden muss systemseitig unterstützt werden. Zur operativen Umsetzung sind Funktionen für ein Aufgabenmanagement bereitzustellen, die es ermöglichen, Aufgaben an Umsetzungsteams zu vergeben, ohne diesen einen vollständigen Zugriff auf die Tool Suite einräumen zu müssen. Optional stellt das Tool eine Möglichkeit zur Verfügung, Aufgaben und



deren Bearbeitung zeitlich zu planen. Mindestens für das ISMS Tool sollte eine Zeitplanung entsprechend Bestandteil des Aufgabenmanagements sein, um die Umsetzung von Maßnahmen verfolgen zu können, bspw. in Form eines Gantt Diagramms. Darüber hinaus müssen alle Module über ein integriertes Risikomanagement verfügen, das die Definition individueller Risikokriterien, die Durchführung von Risikoanalysen sowie die Risikobehandlung unterstützt. Die Ableitung geeigneter Maßnahmen aus der Risikobewertung muss systemgestützt erfolgen können. Ergänzend ist ein Auditmanagement bereitzustellen, das Anwender bei der Planung, Durchführung, Dokumentation und Nachverfolgung von normativen und prozessualen Audits unterstützt. Ein integriertes Dokumentenmanagementsystem wird vorausgesetzt, um sämtliche Änderungen sowie Freigaben revisionssicher dokumentieren zu können. Der Import eigener Dokumentenvorlagen sollte möglich sein. Darüber hinaus hat der Anbieter vordefinierte Dokumentenvorlagen gemäß den Anforderungen bereitzustellen. Die GRC-Suite verfügt über ein zentrales Sicherheitsvorfall-Management, um Sicherheitsvorfälle zu verwalten. Funktionen zur Aufnahme und Behandlung entsprechender Vorfälle müssen vorhanden sein.

2.5 ISMS-Modul

Das ausgeschriebene ISMS-Tool ermöglicht den Aufbau eines ISMS nach der Methodik des BSI IT-Grundschutzes nach Standard 200-1 sowie 200-2. Ein zentraler Anschaffungsgrund für das Tool ist, dass eine Zertifizierung auf Basis IT-Grundschutz für einzelne Informationsverbünde durchgeführt wird. Entsprechend muss das Tool die Anforderungskataloge und Kompendien auf dem Stand von 2023 oder neuer beinhalten, um den Nutzer erfolgreich durch den Zertifizierungsprozess führen zu können. Neue und notwendige Änderungen am Anforderungskatalog werden vom Anbieter zeitnah bereitgestellt. Ebenfalls wird der fristgemäße Umstieg auf Grundschutz++ gemäß regulatorischer Vorgaben sichergestellt. Idealerweise ermöglicht das Tool die grundschutzkonforme Erstellung aller Referenzdokumente, die für die Zertifizierung benötigt werden (A0 bis A6). Besonderer Fokus wird hierbei auf die BSI-Konformität der möglichen 28 Referenzdokumente gelegt.

Das Tool folgt der BSI IT-Grundschutz Methodik. Dabei nutzt es die in den Standards 200-1 sowie 200-2 benutzten Formulierungen. Dadurch wird dem Nutzer ermöglicht, die einzelnen Schritte der IT-Grundschutz Methodik intuitiv abzuarbeiten. Dabei ist es pro Mandant bzw. Instanz möglich, mehrere Informationsverbünde anzulegen. Für jeden Informationsverbund lässt sich die gewünschte Absicherung nach Vorgehensweise Basisabsicherung, Kernabsicherung oder Standardabsicherung bestimmen. Innerhalb der Strukturanalyse ermöglicht das Tool das Anlegen des Informationsverbundes durch geeignete Zielobjekte. Auch eine Gruppierung einzelner Zielobjekte muss möglich sein. Eine Visualisierung der Zielobjektstruktur ist wünschenswert. Optimalerweise werden durch Auswahl/Markierung eines Zielobjektes alle weiteren Zielobjekte angezeigt. Alternativ werden die Abhängigkeiten mithilfe einer hierarchischen Struktur oder durch visuelle Graphendarstellung ermöglicht.

Im Rahmen der *Schutzbedarfsfeststellung* erfolgt die Schutzbedarfsvererbung nach dem Maximalprinzip, muss aber die Möglichkeit bieten, den jeweiligen Schutzbedarf bei



Abweichungen individuell festlegen zu können. Für die effiziente Modellierung der Sicherheitsanforderungen muss es möglich sein, Prozessbausteine einmalig einem Informationsverbund zuzuordnen. Systembausteine modellieren dann die in der Strukturanalyse festgelegten Zielobjektgruppen. Die Erstellung einer Anwendbarkeitserklärung (Statement of Applicability, SoA) ist Bestandteil des Tools. Die vorher festgelegte Vorgehensweise soll sich auch in der Modellierung widerspiegeln, sodass zum Beispiel im Fall der Basis-Absicherung auch nur die entsprechenden Basis-Anforderungen modelliert werden können. Im Rahmen des Soll-Ist-Vergleich legt der Benutzer fest, ob Anforderungen bereits „erfüllt“, „teilweise erfüllt“, „nicht erfüllt“ oder „entbehrlich“ sind. Die Risikoanalyse folgt dem BSI-Standard 200-3. Es muss möglich sein, eine individuelle Risikomatrix anlegen zu können. Das Tool unterstützt den Benutzer dabei, die Umsetzung der benötigten Maßnahmen effizient zu realisieren. Dazu ermöglicht es, Maßnahmen zu verteilen und deren Umsetzung zu managen, indem Aufgaben an entsprechende Rollen verteilt werden.

Anforderungen nach dem aktuellen NIS-2 Gesetz müssen mit dem Tool ebenfalls abgebildet werden können. Auch hier sind Neuerungen zeitnah bereitzustellen. Um den Benutzer kontinuierlich über den Zustand des ISMS zu informieren, verfügt das Tool über eine Visualisierung des Gesamtfortschritts, mit besonderem Fokus auf den Umsetzungsstand der Maßnahmen. Wünschenswert ist ebenfalls eine Darstellung des Reifegrads des ISMS.

2.6 BCMS-Modul

Mithilfe des BCMS Tool soll der effektive Aufbau eines BCMS ermöglicht werden. Die Methodik stützt sich hierbei auf den BSI-Standard 200-4. Dabei sollen entsprechend beide Säulen des Business Continuity Managements, sprich Notfallvorsorge und Notfallbewältigung, vorhanden sein. Im Bereich der Notfallvorsorge bietet das Tool die Möglichkeit, eine Business Impact Analyse durchzuführen und Zielobjekten BCM-typische Kennzahlen wie maximale tolerierbare Ausfallzeiten und Wiederanlaufzeiten hinzuzufügen. Des Weiteren muss es mithilfe weniger Klicks möglich sein, aus den Ergebnissen und Erkenntnissen der Tool-gestützten Notfallbewältigung Notfallhandbücher und Wiederanlaufpläne zu generieren. Um Zuständigkeiten in der Notfallbewältigung zu managen, ermöglicht das Tool die Definition eines Notfallstabs und die Zuweisung vorhandener Rollen aus dem Rollenmanagement zu Notfallteams. Mithilfe von Ausfallsimulationen unterstützt das Tool den Benutzer dabei, die Auswirkungen eines ausgefallenen Zielobjekts auf alle davon abhängenden Assets zu visualisieren, um damit beispielsweise Notfallübungen konzipieren zu können.

2.7 DSMS-Modul

Das DSMS Tool muss alle Anforderungen der DSGVO abbilden, es wird also eine DSGVO-Konformität vorausgesetzt. Es muss das strukturierte Anlegen von Verarbeitungstätigkeiten (VVT) ermöglichen und dabei den Anwender insb. in der Erstellung von Datenschutz-Folgenabschätzungen (DSFA) unterstützen. Das Tool bietet eine Möglichkeit auf



Datenschutzvorfälle angemessen zu reagieren. Die Umsetzung von Betroffenenrechten sowie Melde- und Informationspflichten sollen ebenfalls unterstützt werden, um diese organisatorischen Abläufe effektiv zu fördern. Mustervorlagen für Informations- und Meldepflichten, sowie DSFA und weitere organisatorische Maßnahmen sind darüber hinaus wünschenswert.

3. Eignung

Zum Nachweis seiner Eignung hat der Bieter folgende Erklärungen beizubringen:

- Eigenerklärung Ausschlussgründe (F 521)
- Eigenerklärung Sanktionen (F 523 EU)
- Eigenerklärung Subventionen (F 524 EU)

4. Angebotswertung und Zuschlagskriterien

Gem. § 58 VgV wird der Zuschlag nach Maßgabe des § 127 des Gesetzes gegen Wettbewerbsbeschränkungen auf das wirtschaftlichste Angebot erteilt.

Die Bewertung der Angebote erfolgt nach der einfachen Richtwertmethode nach UfAB. Den Zuschlag erhält der Bieter, der bei der Bewertung den höchsten Nutzwert (Z) erzielt:

$$Z = \frac{L}{P} \text{ mit } L = \text{Leistungspunkten}, P = \text{Preis}$$

Der Preis ergibt sich aus den Angaben im Preisblatt. Die Leistungspunkte ergeben sich aus dem Anforderungskatalog. Maximal können 750 Leistungspunkte erreicht werden.

Sollte der höchste Nutzwert Z bei zwei oder mehr Bietern identisch sein, entscheidet das Los.

Es wird vorausgesetzt, dass die Bieter nach entsprechender Aufforderung am nächsten Werktag einen Testzugang zur Verfügung stellen, damit die Angaben im Anforderungskatalog verifiziert werden können.

5. NIS-2 Compliance

Der Bieter, auf dessen Angebot der Zuschlag erteilt werden soll, muss belegen, dass die angebotene Lösung dem aktuellen Stand der Technik entspricht und in einer gesicherten Entwicklungsumgebung (weiter-)entwickelt wird. Eine vollständige Aufstellung aller eingesetzten Software-Komponenten sowie etwaiger externer Abhängigkeiten ist dem Auftraggeber vorzulegen. Der Anbieter verpflichtet sich, die Einhaltung der Anforderungen der Lieferkettensicherheit gem. NIS2UmsuCG nachzuweisen. Im Falle eines erheblichen Sicherheitsvorfalles, welche den sicheren Betrieb der Lösung gefährdet, ist der Auftraggeber



unverzüglich zu informieren. Dabei ist das Recht des Auftraggebers vorbehalten, gezielte, stichprobenartige Audits zur Prüfung von Sicherheit und Konformität durchzuführen. Alle Nachweise und Beschreibungen sind dem Auftraggeber vor Vertragsabschluss zu übergeben.