Titel	**Request for Information**
Ausgabe	1.0
Ausgabe-Datum	04.08.2025
Daten-Klassifizierung	Public

Author	Function	Company
Giselle Laoutoumai	Head of Digital Workplace, Data- and Collaboration Platforms	OHB ITS GmbH
Peter Jänen	Head of Digital Infrastructure and Services	OHB ITS GmbH
Philipp Wehling	Senior IT Consultant Cyber Security	OHB ITS GmbH

INHALT

1 EINLEITUNG

1.1 Beschreibung der OHB

Die **OHB SE** ist der erste börsennotierte Technologie- und Raumfahrtkonzern in Deutschland mit Sitz in Bremen. Sie gehört zu den drei führenden Raumfahrtunternehmen in Europa und gliedert sich in die drei Unternehmensbereiche Space Systems, Aerospace und Digital. Die drei Unternehmensbereiche sind in verschiedene Tochtergesellschaften unterteilt. Insgesamt beschäftigt die OHB SE weltweit rund 3.000 Mitarbeitende an 15 Standorten.

Mit ihrer langjährigen Erfahrung bedient OHB ihre internationalen Kunden mit anspruchsvollen Lösungen und Systemen im Bereich der Hochtechnologie und der Bündelung von Raumfahrt- und Telematikkompetenzen. Daraus resultiert eine hervorragende Positionierung des Konzerns als eine der bedeutenden unabhängigen Kräfte in der europäischen Raumfahrt- und Hightech-Industrie. In den letzten Jahren hat sich das Unternehmen innerhalb Europas geografisch diversifiziert und verfügt über Standorte in wichtigen ESA-Mitgliedsländern. Diese strategischen Standortentscheidungen fördern die Teilnahme an zahlreichen europäischen Programmen und Missionen.

OHB Information Technology Services GmbH ist mit 80 Mitarbeitenden der interne Partner für alle IT-bezogenen Fragen im OHB SE-Konzern. Durch die Bündelung von Know-how und Technologie ermöglicht sie optimale Prozesse, stellt eine leistungsfähige IT-Umgebung und IT-Dienstleistungen bereit und treibt die Digitalisierung im Konzern voran. Darüber hinaus werden für die OHB-Unternehmen IT-Projekte durchgeführt und mit neuen Technologien Impulse gesetzt.

1.1.1 Zustand heute

Aufgrund der gewachsenen Strukturen herrscht für IT Dienstleistungen eine sehr diverse Partnerlandschaft. Das ist unter anderem dem Umstand geschuldet, dass einige OHB Firmen ihre IT Umgebungen noch autark betreiben und es in vielen Fällen kein harmonisiertes IT Service Angebot gibt.

Grundsätzlich unterscheidet OHB heute zwischen Projekt-IT und Corporate IT. Das bedeutet, dass auch in den Fachbereichen IT Experten vorhanden sind, die eigenständig IT Systeme für (Kunden-) Projekte betreiben und somit eigene Partnerschaften eingehen.

Es zeigt sich, dass die Grenzen mehr und mehr aufgehoben werden und die Fachbereiche Expertise aus den IT-Bereichen anfragen und auch innerhalb der IT Systeme für Projekte entwickelt und bereitgestellt werden.

Die ITS arbeitet heute mit verschiedenen IT Partnern in unterschiedlichem Umfang zusammen. Diese werden sowohl für Betriebsunterstützung, Managed Service und Projektunterstützung eingesetzt.

Derzeit wird der Service „IT Security Monitoring“ als Managed Service betrieben mit mehreren Partnern und Technologien betrieben.

Der Automatisierungsgrad ist eher gering.

Offener und eingestufter Bereich (VS-NfD) arbeiten teilweise mit unterschiedlichen Prozessen, Architekturen und Technologien.

Der Service Desk wird inhouse auf Basis von Jira Service Desk betrieben. Die CMDB wird inhouse mit iDoIT betrieben.

Die eingesetzten Technologien werden je Service im nachfolgenden Dokument beschrieben.

1.1.2 Zielsetzung des Vorhabens

1.1.2.1 Strategische Partnerschaft mit einem Lieferanten

Langfristige Zusammenarbeit mit einem zentralen Dienstleister für:

- Steigerung der Effizienz und Stabilität der Service Operation (Betrieb und Support)
- Reduktion der Durchlaufzeiten und Konditionen für Hardwarebeschaffung (z. B. Endgeräte, Infrastrukturkomponenten)
- Reduktion von Komplexität und Kosten durch Standardisierung.
- Ziel: Nahtlos ineinandergreifende Prozesse, reduzierte Schnittstellen, höhere Effizienz.
- Verbesserung der Cyber Defense, u.a. durch Security Monitoring (24/7 SOC, Threat Hunting) inklusive Analyse und ggf. Eskalation.
- Unterstützung bei Projekten zur Einführung neuer Lösungen und Technologien.
- Klar definierte Eskalationspfade und Ansprechpartner für operative und sicherheitsrelevante Themen.
- Optional: Vor-Ort-Präsenz bei kritischen Systemen oder in Hochsicherheitsbereichen.

1.1.2.2 Stabilisierung des Betriebs

- Etablierung robuster, standardisierter Betriebsprozesse.
- Minimierung von Störungen durch proaktive Überwachung und automatisierte Reaktionen.
- Sicherstellung eines konsistenten Sicherheitsniveaus über alle kritischen Endpunkte und Netze hinweg.

1.1.2.3 Skalierbarkeit

- Architektur und Prozesse sind so ausgelegt, dass sie mit dem Unternehmenswachstum mitwachsen.
- Flexible Erweiterung auf neue Standorte, Geräteklassen oder Sicherheitsanforderungen ohne Systembrüche.
- Unterstützung hybrider Infrastrukturen (on-prem, cloud, air-gapped).

1.1.2.4 Erhöhung des Automatisierungsgrads

- Automatisierte Bedrohungserkennung und -reaktion (z. B. Isolierung, Quarantäne, Rollback).
- Automatisierte Schwachstellenbewertung und Patch-Empfehlungen.
- Automatisierte Installations- und Konfigurations-, sowie Rollout-Prozesse
- Möglichst gleiche Nutzung von Tools und Prozessen in den unterschiedlichen Netzen (on-prem, air-gapped)

1.1.2.5 Wartungskalender

- Geplanter, transparenter Wartungskalender für Software-Updates, Policy-Anpassungen und Systempflege.
- Minimierung von Downtimes durch abgestimmte Wartungsfenster.
- Dokumentation und Kommunikation über das zentrale Servicemanagement-System.

1.1.2.6 Integration in Service- und Change Management

- Vollständige Einbindung in bestehende ITSM-Prozesse und deren Weiterentwicklung (z. B. über ITIL).
- Automatisierte Ticket-Erstellung bei sicherheitsrelevanten Ereignissen.
- Change Requests für Policy-Änderungen, Rollouts oder Systemanpassungen mit Genehmigungs-Workflows.
- Vollständige Integration in die bestehende CMDB

1.1.2.7 Eingestufte Umgebungen

- Soweit möglich analoge Prozesse, Architekturen und Konzepte im eingestuften Bereich.

2 PROJEKTINFORMATION

2.1 Projektzusammenfassung

Projektbeschreibung	Ziele
Identifizierung und Auswahl eines strategischen IT-Partners zur Bereitstellung skalierbarer, kosteneffizienter und sicherer IT-Dienste mit Schwerpunkt auf Digital Workplace, Infrastruktur und Cybersicherheit.	• Konsolidierung der Anbieter von Workplace- und Infrastrukturdiensten sowie der Hardwarebeschaffungskanäle. • Evaluierung und möglicher Ersatz des derzeitigen SIEM/SOC-Partners. • Steigerung der Kosteneffizienz und Reduzierung der Anbieterkomplexität. • Skalierung des IT-Betriebs für zukünftiges Wachstum. • Vereinheitlichung der Prozesse, Architekturen und Lösungen im offenen und eingestuften Bereich.

2.2 Kontakte

Name	Funktion	E-Mail	Firmenadresse
Giselle Laoutoumai	Head of Digital Workplace, Data- and Collaboration Platforms	giselle.laoutoumai@ohb.de	OHB ITS GmbH Manfred-Fuchs-Platz 2-4 28359 Bremen
Peter Jänen	Head of Digital Infrastructure & Services	peter.jaenen@ohb.de	OHB ITS GmbH Manfred-Fuchs-Platz 2-4 28359 Bremen
Domenic Abb	IT Infrastructure Architect	domenic.abb@ohb.de	OHB ITS GmbH Manfred-Fuchs-Platz 2-4 28359 Bremen
Philipp Wehling	Senior IT Consultant Cyber Security	philipp.wehling@ohb.de	OHB ITS GmbH Manfred-Fuchs-Platz 2-4 28359 Bremen

3 ARBEITSUMFANG UND ERGEBNISSE DES RFIS

3.1 Format und Zeitleiste für Antworten auf dieses RFIs

Phase	Datum
Aufruf zur Teilnahme (RFI)	04.08.2025
Deadline RFI	22.08.2025 16 Uhr
Q&A Runde mit ausgewählten Anbietern	KW 35 – 36 2025
RfP Veröffentlichung	09/2025

3.2 Umfang der erwarteten Antwort

Umfang	Details
Erwartete Leistungen des Lieferanten als Teil des RFIs	• Allgemeine Informationen zum Lieferanten. (Kap. 4) • Informationen zu Prozessen und Technologien hinsichtlich der einzelnen Service Angebote (Kap. 5) • Erfahrungen und Referenzen. (Kap. 6)

4 ALLGEMEINE LIEFERANTENINFORMATIONEN

4.1 Organisation

Bitte geben Sie die folgenden allgemeinen Informationen an	
Vollständiger rechtlicher Name des Unternehmens	
Land und Adresse	
Webseite	
Nächster Bürostandort des Lieferanten zu den Lieferstandorten von OHB (Bremen/Oberpfaffenhofen)	
Primärer Ansprechpartner für die RFI-Reaktion	

Bitte geben Sie einen Überblick über das Unternehmen	
Tätigkeitsbereich des Unternehmens / Geschäftsbereiche	
Wie groß ist das Unternehmen? [Umsatz und Mitarbeiter]	
Kernkompetenzen des Unternehmens	
Anzahl der Mitarbeiter in der abgebenden Einheit	
Was sind die Werte, die Mission und die Vision des Unternehmens?	
Warum sind Sie besser als andere Anbieter? Was macht Sie besonders?	

Wie passt Ihr Unternehmen zu OHB?	
Lieferorte/Zeitzone?	
Sprachkenntnisse Deutsch / Englisch	
Möglichkeit der Anreise zu OHB-Standorten	
Referenzen in der Luft- und Raumfahrt und im Verteidigungssektor	

4.2 Zertifikate

Bitte geben Sie Einzelheiten zu den Zertifizierungen an, die Ihr Unternehmen erworben hat (z.B. ISO 9001, ISO 27001, BSI, GDPR, Cobit, ITIL, Partner mit Lieferanten (z.B. SAP, Microsoft, etc.)	
Beispiel 1	
Beispiel 2	
Beispiel 3	
…	
…	
…	

4.3 Projektmanagement

Bitte beschreiben Sie die von Ihnen verwendeten Projektmanagement-Frameworks (z.B. Waterfall, SCRUM, Iterative, Prince2, IPMA usw.)

Mit welchen Methoden des Projektmanagement-Frameworks sind Sie vertraut?	
Projektmanagementmethoden und Zertifizierungen der Mitarbeitenden	
Unterstützte und bevorzugte Werkzeuge (z.B. Jira Software, MS Project, Teams, Confluence…)	

4.4 Sicherung und Qualität

Bitte beschreiben Sie kurz Ihren SW-Qualitätsicherungsansatz.

Welche Mechanismen haben Sie zur Sicherung der Qualität eingerichtet?	
Bitte beschreiben Sie Ihre Qualitätssicherungsmethodik	
Welche Instrumente verwenden Sie?	
Welche Prozesse verfolgen Sie?	
Welche Standarddokumentation erstellen Sie?	

5 SERVICE SCOPE FÜR DEN RFI

Im Zuge der Weiterentwicklung unseres IT-Betriebs suchen wir einen strategischen Partner, der zentrale Infrastruktur-, Workplace und Securityservices ganzheitlich und integriert bereitstellen kann. Der Scope dieses RFI wird im Folgenden je Service beschrieben.

5.1 Endpoint Lifecycle und Configuration Management

Der Service Endpoint Lifecycle & Configuration Management (ELCM) bietet eine umfassende Lösung für das Management des gesamten Lebenszyklus von Endgeräten im Unternehmen. Dies umfasst die Konfigurationsverwaltung, Softwarepaketierung und -verteilung, das Patch-Management sowie die kontinuierliche Überwachung der Compliance. Der Service stellt sicher, dass alle Endgeräte – Desktops, Laptops und mobile Geräte – konsistent konfiguriert, abgesichert und gemäß den Unternehmensrichtlinien sowie regulatorischen Anforderungen aktualisiert werden.

5.1.1 Kernkomponenten

5.1.1.1.1 Endpoint-Konfigurationsmanagement

- Zentrale Verwaltung von Geräteeinstellungen, Richtlinien und Compliance-Baselines.
- Integration mit Verzeichnisdiensten (z. B. Active Directory, Azure AD).
- Unterstützung von Konfigurationsprofilen für mehrere Betriebssysteme.
- Automatisierung von Onboarding- und Bereitstellungsprozessen.

5.1.1.2 Softwarepaketierung und -deployment

- Erstellung, Test und Validierung von Softwarepaketen.
- Verteilung von Anwendungen über zentrale Management-Tools.
- Versionskontrolle und Rollback-Funktionen.
- Unterstützung für benutzerinitiierte und automatisierte Installationen.

5.1.1.3 Patch-Management

- Regelmäßige Bewertung der Patch-Compliance aller Endgeräte.
- Automatisierte Bereitstellung von Betriebssystem- und Drittanbieter-Patches.
- Risikobasierte Priorisierung kritischer Updates.
- Reporting und Benachrichtigung bei Patch-Status und -Fehlern.

5.1.1.4 Software-Patching

- Kontinuierliche Überwachung von Softwareschwachstellen.
- Integration mit Plattformen für Schwachstellenmanagement.
- Geplante und Notfallbereitstellung von Software-Patches.
- Validierung und Rückabwicklung nach der Patch-Installation.

5.1.2 Eingesetzte Technologien

Technologiepartner	Service
SCCM und Intune	Endpoint Management Plattformen
SCCM	Softwarepaketierung und Deployment
SCCM, WSUS, Patch my PC	Patch-Management

Technologiepartner	Service
PowerShell	Scripting & Automatisierung

5.1.3 Benötigte Informationen

Service Funktionalitäten – bitte beschreiben Sie…	
Ihren Ansatz für das Endpoint Configuration Management.	
Details zu Ihrem Prozess der Softwarepaketierung und -verteilung.	
Ihre Methodik und eingesetzten Tools für das Patch-Management.	
Ihre Vorgehensweise beim Software-Patching, insbesondere bei Notfällen.	
Welche Technologien Sie einsetzen und welche Integrationsmöglichkeiten in unsere Systeme es gibt.	
Die Skalierbarkeit Ihres Services in globalen oder hybriden Umgebungen.	
Das Supportmodell, SLAs und Eskalationsverfahren.	
Automatisierungs-, KI- oder Analysefunktionen in Ihrem Service.	
Wie sehen Prozesse, Architekturen und Konzepte in eingestuften Umgebungen aus unter der Maßgabe, dass hier eine standardisierte Lösung betrieben wird.	
Bitte beschreiben Sie beispielhaft mögliche Preis-/Abrechnungsmodelle für diesen Service	

5.2 Endpoint Protection

Der Service Endpoint Protection umfasst den Schutz von Clients und Servern vor Cyberbedrohungen. Ziel ist es, die Integrität, Vertraulichkeit und Verfügbarkeit der Systeme sicherzustellen.

5.2.1 Kernkomponenten Client

- Malware- und Ransomware-Schutz: Echtzeitüberwachung und -abwehr gegen Schadsoftware.
- Verhaltensbasierte Erkennung: Analyse von Nutzer- und Prozessverhalten zur Erkennung verdächtiger Aktivitäten.
- Angriffsflächenreduktion (ASR): Kontrolle von Makros, Skripten, USB-Geräten etc.
- Gerätekontrolle: Verwaltung von USB-Zugriff, Druckern und anderen Peripheriegeräten.
- Schwachstellenmanagement: Identifikation und Priorisierung sowie Patchen von Schwachstellen auf Endgeräten.
- Automatisierte Reaktion: Isolierung infizierter Geräte, Beendigung schädlicher Prozesse.
- Integration mit Microsoft 365 Defender: Zentrale Sicht auf Bedrohungen und Korrelation mit anderen Microsoft-Sicherheitsdiensten.

5.2.2 Kernkomponenten Server

- Schutz geschäftskritischer Systeme: Fokus auf Verfügbarkeit und Integrität.
- Anpassung an Serverrollen: Spezifische Konfigurationen für z. B. Domain Controller, File Server, Applikationsserver.
- Überwachung von PowerShell und WMI: Erkennung von Missbrauch durch Angreifer.
- Integration in SIEM/SOAR: Weiterleitung von Alerts an zentrale Systeme wie Microsoft Sentinel.
- Patch- und Schwachstellenmanagement: Unterstützung bei der Priorisierung sicherheitsrelevanter Updates.
- Netzwerküberwachung: Erkennung lateraler Bewegungen und ungewöhnlicher Verbindungen.

5.2.3 Eingesetzte Technologien

Technologiepartner	Service
Microsoft Defender for Endpoint	Endpoint Protection Client und Server
Sentinel One	Endpoint Protection Client und Server im VS-NfD Umfeld

5.2.4 Benötigte Informationen

Service Funktionalitäten – bitte beschreiben Sie…	
Ihren Ansatz für Endpoint Protection.	
Welche Betriebssysteme und Plattformen Sie unterstützen.	
Ihre Methodik im Kontext Verschlusssachen, z.B. Air-Gap Szenarien, BSI-Konformität.	
Integrationsmöglichkeiten in bestehendes SOC/SIEM.	

Die Skalierbarkeit Ihres Services in globalen oder hybriden Umgebungen.	
Das Supportmodell, SLAs und Eskalationsverfahren.	
Automatisierungs-, KI- oder Analysefunktionen in Ihrem Service.	
Die Integration in Patchmanagement Prozesse.	
Wie sehen Prozesse, Architekturen und Konzepte in eingestuften Umgebungen aus unter der Maßgabe, dass hier eine standardisierte Lösung betrieben wird.	
Bitte beschreiben Sie beispielhaft mögliche Preis-/Abrechnungsmodelle für diesen Service	

5.3 Microsoft M365

Microsoft 365 ist eine cloudbasierte Plattform für moderne Zusammenarbeit, Kommunikation, Sicherheit und Geräteverwaltung. Sie vereint zentrale Dienste wie Entra ID (Identitäts- und Zugriffsmanagement), Microsoft Teams, OneDrive for Business, SharePoint Online sowie Microsoft Defender für umfassenden Schutz vor Bedrohungen.

Der aktuelle Schwerpunkt bei OHB liegt auf der intensiven Nutzung der Kollaborationsfunktionen, insbesondere für die Zusammenarbeit mit internen und externen Teilnehmern. Teams dient dabei als zentrale Kommunikations- und Meeting-Plattform, während OneDrive und SharePoint für das Teilen und gemeinsame Bearbeiten von Dokumenten genutzt werden.

Parallel dazu befinden sich weitere Dienste in Planung/im Rollout, darunter:

- Microsoft Teams Telefonie für moderne Unternehmenskommunikation,
- Microsoft Intune für Modern Endpoint Management,
- sowie Mobile Device Management (MDM) zur sicheren Verwaltung mobiler Endgeräte.

Ziel ist der Aufbau einer ganzheitlich integrierten, sicheren und benutzerfreundlichen Arbeitsumgebung auf Basis von Microsoft 365.

Der angefragte Managed Service soll den vollständigen Lebenszyklus der Microsoft 365-Dienste abdecken – von der technischen Betriebsführung über den 3rd Level Support bis hin zur strategischen Weiterentwicklung und Optimierung der Plattform. Dabei stehen insbesondere die Entlastung interner IT-Ressourcen, die Sicherstellung eines stabilen und sicheren Betriebs sowie die kontinuierliche Anpassung an neue Microsoft-Funktionalitäten im Fokus.

5.3.1 Kernkomponenten

- SharePoint Online (Dokumentenmanagement, Kollaboration mit Externen, Datenaustausch, Intranet)
- OneDrive for Business (persönlicher Cloud-Speicher)
- Microsoft Teams (Zusammenarbeit, Chat, Meetings)
- Microsoft 365 Apps for Enterprise (Office-Anwendungen)
- Microsoft Entra ID (Identitäts- und Zugriffsmanagement)
- Microsoft Defender for Office 365 (Sicherheitsfunktionen)
- Intune / Endpoint Manager (Geräteverwaltung teilweise, Mobile Device Management)

Geplant für 2026

- Purview Compliance & Information Protection (Informationssicherheit, DLP, Archivierung)
- Power Platform (Power BI, Power Apps, Power Automate, Copilot Studio)
- Exchange Online (E-Mail, Kalender, Kontakte)
- Microsoft Teams Telefonie

5.3.2 Eingesetzte Technologien

Technologiepartner	Service
Microsoft 365	Plattform
ShareGate	SharePoint Administration
EasyLife 365	Governance und Automation
Entra ID Connect	AD/Entra Synchronisation

Technologiepartner	Service
Adaxes	Anlage von on premises User und Gruppen

5.3.3 Benötigte Informationen

Service Funktionalitäten – bitte beschreiben Sie…	
Ihren Ansatz für das Management von M365 Umgebungen.	
Details zu Ihrem Prozess zur Bewertung und Freischaltung von automatisch eingespielten Changes.	
Ihre Methodik und eingesetzten Tools für das Monitoring der Microsoft Roadmap.	
Ihre Vorgehensweise bei der Behandlung von Message Center Enträgen und Microsoft Incidents.	
Die Skalierbarkeit Ihres Services in globalen oder hybriden Umgebungen.	
Das Supportmodell, SLAs und Eskalationsverfahren.	
Automatisierungs-, KI- oder Analysefunktionen in Ihrem Service.	
Wie Sie zusätzliche Supportanfragen (durch IT) für die Konzeption und/oder Bereitstellung neuer Lösungen mit in den Service einbringen können.	
Wie berücksichtigen Sie Adoption- & Change Maßnahmen für diesen Service?	
Bitte beschreiben Sie beispielhaft mögliche Preis-/Abrechnungsmodelle für diesen Service	

5.4 IT Security Monitoring Service

Der IT Security Monitoring Service dient der kontinuierlichen, proaktiven Überwachung unserer IT-Infrastruktur mit dem Ziel, sicherheitsrelevante Ereignisse frühzeitig zu erkennen, retrospektiv zu sehen, zu analysieren und geeignete Gegenmaßnahmen einzuleiten. Dabei liegt der Fokus nicht nur auf der allgemeinen Bedrohungserkennung, sondern insbesondere auf der Abbildung und Überwachung unternehmensspezifischer Use Cases, die auf unsere Geschäftsprozesse und IT-Landschaft zugeschnitten sind.

5.4.1 Kernkomponenten

5.4.1.1 Log- und Eventdatenerfassung

- Erfassen sicherheitsrelevante Daten von Endpunkten, Servern, Firewalls, Cloud-Diensten etc.
- Log Normalisierung: Vereinheitlichung unterschiedlicher Logformate zur besseren Analyse
- Weiterentwicklung des bestehenden Datenmodells
- Möglichkeit zur Korrellation zur Suche von Informationen über verschiedene Datenquellen hinweg

5.4.1.2 Zentrale Analyseplattform

- Security Information and Event Management zur Sammlung, Korrellation und Analyse von sicherheitsrelevanten Ereignissen

5.4.1.3 Use Case Management

- Definition und Pflege von Erkennungsregeln: Abbildung individueller Bedrohungsszenarien (z. B. verdächtige Anmeldungen, Datenabflüsse)
- Use Case Library: Sammlung standardisierter und kundenspezifischer Use Cases

5.4.1.4 Alarmierung, Behandlung und Eskalation

- Alerting Engine: Generierung von Alarmen bei Erkennung von Anomalien oder Regelverstößen
- Voranalyse durch Diensleister SOC inklusive Abgleich zu bisherigen Erkenntnissen und Whitelists
- Eskalationsprozesse: Automatisierte oder manuelle Weiterleitung an zuständige Stellen IT Security Team der OHB

5.4.1.5 Incident Response Unterstützung

- Playbooks / Runbooks: Mithilfe bei der Erstellung von Vorgehensweisen zur Reaktion auf bestimmte Vorfälle

5.4.1.6 Dashboard und Reporting

- Visualisierung: Übersichtliche Darstellung von Sicherheitsstatus, KPIs und Trends
- Compliance-Reporting: Berichte für Audits und regulatorische Anforderungen (z. B. DSGVO, ISO 27001)
- Regelmäßiger Abgleich des Dienstleister SOCs mit dem IT Security Team der OHB

5.4.1.7 Threat Intelligence Integration

- Bedrohungsdatenfeeds: Anbindung externer Quellen oder Erstellung von Referenzlisten zur Erkennung bekannter Angreifer, IPs, Hashes etc.
- Threat Enrichment: Anreicherung von Events mit Kontextinformationen sowohl automatisiert als auch in der Event Analyse durch das Dienstleister SOC

5.4.1.8 Infrastruktur und Betrieb

- Managed Security Operations Center (SOC): Team zur Überwachung, Analyse und Reaktion

- Service Management: SLAs, Onboarding, Change Management, kontinuierliche Verbesserung
- Operational Management: Vollständiger operationeller Betrieb von Infrastruktur auf dem OHB Gelände

5.4.2 Eingesetzte Technologien

Technologiepartner	Service
JIRA Service Management	ITSM/ Ticket-Tool
iDoIt	CMDB
VMRay	Sandboxing
ASGARD	Endpoint Forensics
DCSO Threat Detection and Hunting	Network Monitoring
IBM QRadar OnPrem	SIEM

5.4.3 Benötigte Informationen

Service Funktionalitäten – bitte beschreiben Sie…	
Wie sieht das Use Case Lifecycle Management aus?	
Welche Reports/Dashboards werden bereitgestellt?	
Wie viel Mitwirkung hat die OHB auf die Erkennungsregeln und deren Behandlung?	
Wie wird die Qualität von sicherheitsrelevanten Events, welche nicht an den Kunden eskaliert werden, gesichert?	
Wie sieht das Log Source Lifecycle Management aus?	
Welche variablen Kosten können anfallen und wie werden diese berechnet?	
Welche Informationen werden durch das SOC benötigt, um eine hochwertige Erst-analyse durchzuführen?	
Wie werden Log sources erkannt und behandelt, die keine Events mehr schicken?	
Welches Datenmodell wird verwendet?	
Was passiert mit den OHB-spezifischen Inhalten, wenn ein Provider Wechsel erfolgt?	

Wie wird mit Log Sources umgegangen, die proprietäre oder sich schnell ändernde Log-Formate haben?	
Welchen Zugriff und welche Rechte bekommt die OHB im SIEM?	
Wie weit kann das SOC in der aktive Abwehr gefundener Bedrohungen mitwirken?	
Wie sehen Prozessem Architekturen und Konzepte in eingestuften Umgebungen aus unter der Maßgabe, dass hier eine standardisierte Lösung betrieben wird.	
Bitte beschreiben Sie beispielhaft mögliche Preis-/Abrechnungsmodelle für diesen Service	

5.5 Infrastructure Monitoring Service

Der Infrastructure Monitoring Service bietet eine ganzheitliche Überwachung der IT-Infrastruktur über lokale, cloudbasierte und hybride Umgebungen hinweg. Der Dienst ermöglicht eine proaktive Erkennung von Problemen, unterstützt bei der Ursachenanalyse und stellt die optimale Leistung geschäftskritischer Systeme sicher.

Der Infrastructure Monitoring Service nutzt moderne Monitoring-Plattformen wie z. B. Zabbix und Grafana, um Echtzeit-Einblicke, automatisierte Benachrichtigungen und intelligente Analysen bereitzustellen. Der Service ist in unsere bestehende ITSM-Umgebung bereits integriert und bietet anpassbare Dashboards für verschiedene Zielgruppen. Über diese Schnittstelle werden (Security-) Events automatisiert in die bestehende ITSM Umgebung übertragen.

5.5.1 Kernkomponenten

5.5.1.1 Infrastrukturüberwachung

- Überwachung von Servern, Speicher, Netzwerkgeräten und Virtualisierungsplattformen.
- Unterstützung für Cloud-Infrastrukturen (IaaS, PaaS) und containerisierte Umgebungen.
- Leistungsmetriken in Echtzeit, Verfügbarkeitsprüfungen und Kapazitätsplanung

5.5.1.2 Alarmierung und Incident Management

- Konfigurierbare Schwellenwerte und automatische Benachrichtigungen.
- Integration mit Incident-Management-Plattformen (z. B. Jira).
- Eskalationsprozesse und Benachrichtigungskanäle

5.5.1.3 Berichte und Dashboards

- Anpassbare Dashboards für technische und geschäftliche Nutzer.
- Historische Trendanalysen und SLA-Berichte.
- Management-Zusammenfassungen und Compliance-Reports.

5.5.1.4 Wartung & Lifecycle-Management

- Einspielen regelmäßiger Updates, Patches und Release-Management der eingesetzten Systeme

5.5.2 Eingesetzte Technologien

Technologiepartner	Service
JIRA Service Management	ITSM/ Ticket-Tool
iDoIt	CMDB
Zabbix, Grafana	Monitoring

5.5.3 Benötigte Informationen

Service Funktionalitäten – bitte beschreiben Sie…	
Bitte beschreiben Sie das Betriebsmodell und den Serviceumfang.	
Welche Plattformen und Hersteller unterstützen Sie?	

Welche Monitoring- und Management Tools setzen Sie ein?	
Gibt es eine ITSM-Integration zu unserem bestehenden JIRA Service Management?	
Gibt es eine Integration in unsere bestehende CMDB?	
Welche Automatisierungsmöglichkeiten nutzen Sie?	
Bitte beschreiben Sie die Service Levels & Reporting Umfang.	
Bitte beschreiben Sie das Sicherheits- und Datenschutzkonzept.	
Wie sieht eine Integration in unser bestehendes SOC/SIEM aus?	
Was sind Risiken und Lessons Learned aus früheren Projekten?	
Gibt es Schulungskonzepte für interne Teams?	
Wie sehen Architekturen und Konzepte in eingestuften Umgebungen aus unter der Maßgabe, dass hier eine standardisierte Lösung betrieben wird.	
Bitte beschreiben Sie beispielhaft mögliche Preis-/Abrechnungsmodelle für diesen Service	

5.6 Network Operation Center (NOC)

Das Network Operation Center (NOC) ist ein zentralisierter, professionell betriebener Netzwerkbetriebsdienst, der die Überwachung, Steuerung und Optimierung der gesamten Unternehmensnetzwerkinfrastruktur sicherstellt. Ziel ist es, eine hohe Verfügbarkeit, Sicherheit und Performance aller Netzwerkdienste zu gewährleisten – sowohl in lokalen als auch in global verteilten Umgebungen.

Die Netwerkkomponenten werden zentral über unser SOC / SIEM auf sicherheitsrelevante Events überwacht. Störungen, u.a. aus dem Monitoring und den zentralen Managementsystemen werden über eine Schnittstelle in das bestehende JIRA Servicemanagement übertragen.

5.6.1 Kernkomponenten

5.6.1.1 LAN (Local Area Network)

- Betrieb und Überwachung von Core-, Distribution- und Access-Switches
- VLAN-Management, Port-Security, QoS-Konfiguration
- Lifecycle-Management (Firmware, Konfigurations-Backups, Hardwareaustausch)
- Integration in NAC-Lösungen (z. B. 802.1X)

5.6.1.2 WLAN (Wireless LAN)

- Verwaltung von Access Points und Wireless Controllern
- Heatmap-Analysen, Roaming-Optimierung, Kanalplanung
- Gastzugangskontrolle und BYOD-Management
- Monitoring von Signalstärke, Interferenzen und Clientverhalten

5.6.1.3 Firewall-Services

- Zentrale Verwaltung von Next-Generation Firewalls, inkl. virtuellen Firewalls unterschiedlicher Hersteller
- Regelwerksmanagement, Zonen- und Segmentierungskonzepte
- Intrusion Detection/Prevention (IDS/IPS)
- Regelmäßige Sicherheitsreviews und Policy-Audits

5.6.1.4 Remote Access

- Betrieb von VPN-Gateways
- Multi-Faktor-Authentifizierung (MFA), Device Compliance Checks
- Monitoring von Zugriffsmustern und Anomalieerkennung
- Unterstützung für mobile Endgeräte und Homeoffice-Umgebungen

5.6.1.5 WAN (Wide Area Network)

- Verwaltung von Internet-VPN- und SD-WAN-Verbindungen
- Traffic Engineering, Pfadoptimierung, Failover-Strategien
- Performance-Monitoring (Latenz, Jitter, Paketverlust)

5.6.2 Eingesetzte Technologien

Technologiepartner	Service
Aruba, AirWave, ClearPass	LAN / WLAN
PaloAlto, FortiGate, Genua, SINA	Firewall

Technologiepartner	Service
Global Protect, Aruba, ECOS, Genua	Remote Access
FortiGate, SINA	WAN
JIRA Service Management	ITSM/ Ticket-Tool
iDoIt	CMDB
Zabbix, Grafana	Monitoring

5.6.3 Benötigte Informationen

Service Funktionalitäten – bitte beschreiben Sie…	
Bitte beschreiben Sie das Betriebsmodell und den Serviceumfang.	
Welche Plattformen und Hersteller unterstützen Sie?	
Welche Monitoring- und Management Tools setzen Sie ein?	
Gibt es eine ITSM-Integration zu unserem bestehenden JIRA Service Management?	
Gibt es eine Integration in unsere bestehende CMDB?	
Welche Automatisierungsmöglichkeiten nutzen Sie?	
Bitte beschreiben Sie die Service Levels & Reporting Umfang.	
Bitte beschreiben Sie das Sicherheits- und Datenschutzkonzept.	
Wie sieht eine Integration in unser bestehendes SOC/SIEM aus?	
Was sind Risiken und Lessons Learned aus früheren Projekten?	
Gibt es Schulungskonzepte für interne Teams?	
Wie sehen ihre Dokumentationsanforderungen aus?	

Wie werden vor Ort Einsätze organisiert, bzw. übernommen?	
Wie sehen Architekturen und Konzepte in eingestuften Umgebungen aus unter der Maßgabe, dass hier eine standardisierte Lösung betrieben wird.	
Bitte beschreiben Sie beispielhaft mögliche Preis-/Abrechnungsmodelle für diesen Service	

5.7 Hardwarebeschaffung

Gegenstand dieses Servicebereichs ist die ganzheitliche Beschaffung und Bereitstellung von Infrastrukturkomponenten und Endgeräten. Der Lieferant übernimmt die Erstellung von Angeboten auf Basis definierter Anforderungen, die Beschaffung und teilweise Konfiguration der Hardware sowie die termingerechte Bereitstellung an den jeweiligen Einsatzorten.

5.7.1 Kernkomponenten

- Technologieberatung
- Angebotserstellung auf Basis definierter Anforderungen
- Beschaffung der Hardware
- Vorkonfiguration, Aufnahme ins Managementsystem für Endgeräte
- Überwachung des Lifecycles von der Inbetriebnahme, über Wartung und Austausch bis hin zu Aussonderung.
- Optional: Konfiguration und Installation
- Optional: Dokumentation und Integration in bestehendes Asset Mmanagement System oder CMDB

5.7.2 Eingesetzte Technologien

Technologiepartner	Service
Aruba	LAN, WLAN, Data Center Network
Palo Alto	Firewall, RAS, VPN
FortiGate	Firewall, SD-WAN
InfoBloxx	DNS, DHCP, DDI
Sentinel One / Microsoft Defender	EDR
Microsoft	Digital Workplace, Hosting Windows
Dell Technologies	Digital Backbone
VMWare	Virtualization, Virtual Desktop
Veeam, FastLTA	Backup
RedHat	Hosting Linux, Container,
IBM	SOC/SIEM
itWatch	Datenschleuse
Genua	3rd Party Remote Access, Secure Firewall, Secure RAS
ProofPoint	Mail Gateway, AntiSpam
Semperis	ADFR
F5	Web Application Firewall

Technologiepartner	Service
Kemp	Loadbalancer
OpSwat, TightGate	Managed File Transfer, Secure Internet
JFrog	Software Supply Chain
SINA	Secure WAN
ECOS	Secure RAS
IDpendent	PKI
Meinberg	NTP

5.7.3 Benötigte Informationen

Service Funktionalitäten – bitte beschreiben Sie…	
Welche Infrastrukturkomponenten und Endgeräte können beschafft werden (z. B. Server, Netzwerkkomponenten, Notebooks, mobile Geräte)?	
Welche Herstellerpartnerschaften/-bindungen haben Sie und mit welchem Status? Können herstellerunabhängige Angebote erstellt werden?	
Wie erfolgt die Angebotserstellung? Gibt es standardisierte Kataloge, Self-Service-Portale oder individuelle Beratung?	
Können bestehende Asset Management, Service Management und CMDB-Systeme angebunden werden?	
Lifecycle-Management: Wie wird der Lebenszyklus der Hardware überwacht und dokumentiert (z. B. Garantie, Wartung, Austausch, Aussonderung)?	
Bereitstellung und Rollout: Welche Leistungen sind im Rahmen der Bereitstellung enthalten (z. B. Imaging, Konfiguration, Versand, Vor-Ort-Installation)?	
Nachhaltigkeit und Entsorgung: Welche Konzepte bestehen für Rücknahme, Recycling und nachhaltige Beschaffung?	

Wie werden vor Ort Einsätze organisiert, bzw. übernommen?	
Bitte beschreiben Sie beispielhaft mögliche Preis-/Abrechnungsmodelle für diesen Service	

6 ERFAHRUNGEN UND REFERENZEN

6.1 Referenzen für eingestufte Umgebungen

Bitte beschreiben Sie Ihre Erfahrungen in der Implementierung und dem Management von Services, in eingestuften Umgebungen (VS-NfD). Geben Sie drei vergleichbare[1] Referenzprojekte / Kunden an.	
Beispiel 1	
Beispiel 2	
Beispiel 3	

6.2 Referenzen

Bitte beschreiben Sie Ihre Erfahrungen in der Implementierung von Managed Services, die in den Rahmen unseres RFI fallen. Geben Sie nach Möglichkeit drei vergleichbare Referenzprojekte / Kunden an.	
Beispiel 1	
Beispiel 2	
Beispiel 3	

6.3 Vertragsarten

Bitte beschreiben Sie, welche Vertragsarten Sie willen sind mit uns abzuschließen. (z.B. Werkvertrag)	
Beispiel 1	
Beispiel 2	
Beispiel 3	

[1] Firmengröße, Geschäftsmodell Engineering-to-Order / Configure-to-Order, Industriesektor

7 BEDINGUNGEN

7.1 Es gilt Deutsches Recht.

7.2 Geheimhaltungsvereinbarung

Für die Implementierung ist eine gesonderte Geheimhaltungserklärung zu unterzeichnen, welche aufgrund des Zugriffs auf sensitive Daten der OHB System AG eine Vertragsstrafe von 50.000€ für jede Form der Verletzung unter Umkehr der Beweislast vorsieht.

7.3 Geistiges Eigentum & Nutzungsrechte

Die Rechte an den im Rahmen des Projektes vorgenommenen Anpassungen und Programmierungen (inkl. Konfiguration der Standardanwendungen) liegen alleine bei OHB. Insbesondere genießt OHB kostenfrei, unbeschränkte, weltweite und übertragebare Rechte an allen für OHB vorgenommenen Anpassungen.

Sämtliches im Rahmen des Projektes durch OHB zur Verfügung gestellten Dokumente & Informationen verbleiben Eigentum von OHB.