

---

**Leistungsbeschreibung**  
**für einen Rahmenvertrag „Audit“**  
**für den Informationsverbund nach**  
**ISO 27001 auf Basis**  
**IT-Grundschutz**

in der  
HIL Heeresinstandsetzungslogistik GmbH

---

# **1 Ausgangssituation**

## **1.1 Zum Auftraggeber**

Die Zielsetzung des Auftraggebers (= AG) HIL GmbH ist es, für vertraglich definierte Waffensysteme des Heeres einschließlich der darin befindlichen Baugruppen alle Materialerhaltungsmaßnahmen zu planen, zu steuern und durchzuführen und dabei die Verfügbarkeit der Systeme in der geforderten Höhe sicherzustellen. Die Planung, Steuerung und Durchführung der hierfür erforderlichen Management-, Reparatur- und Instandsetzungsleistungen ist die Kernkompetenz des Unternehmens.

Hierzu stehen die Zentrale in Bonn, die Werke in Darmstadt, St. Wendel und Doberlug-Kirchhain ebenso zur Verfügung wie fünf Niederlassungen samt über 70 zugeordneter Stützpunkte sowie die Vertretung Auslandsunterstützung in Erfurt. Zusammen mit den Auftragnehmern aus der wehrtechnischen Industrie ist der AG somit in der Lage, für die Bundeswehr hochwertige Dienstleistungen aus einer Hand wirtschaftlich zu erbringen.

Der Betrieb dieses IT-Systems erfolgt – mit Ausnahme der Systeme der Bundeswehr sowie der Büro- und Kommunikationstechnik – durch IT-Dienstleister auf der Grundlage entsprechender Verträge und zugehöriger Service Level Agreements (SLA). Zentrales Element ist ein eigenes SAP-System. Die Client-Anwendungen werden aktuell in einer Terminal-Server-Architektur unter CITRIX zentral bereitgestellt und durch einen Servicedesk des IT-Dienstleisters betreut.

## **1.2 Ausgangssituation**

Die HIL GmbH hat Ihren Informationsverbund als geheimschutzbetreutes Unternehmen aufgebaut und unterliegt den folgenden Regelwerken:

- GeheimSchutzhandbuches (GHB), Anlage 4
- IT-Grundschutz Standard 200-1, 200-2, 200-3, sowie 200-4
- Anteilen der ZDV A960/1

Um die Umsetzung der Anforderungen der aufgeführten Regelwerke zu überprüfen, soll ein langfristiger Rahmenvertrag mit einem Auditdienstleister ohne Abrufverpflichtung abgeschlossen werden

# **2 Auftragsleistung und Zeitplanung**

## **2.1 Ziel des Audit-Rahmenvertrages**

Der Informationsverbund der HIL GmbH mit allen darin enthaltenen Applikationen nebst zugehöriger Hardware, sowie allen darin einbezogenen Liegenschaften und der zu berücksichtigenden Prozessen soll im Rahmen der kontinuierlichen Verbesserung regelmäßig auditiert werden.

Dieses soll anhand des noch aufzustellenden Audit-Universes risiko- und auftragsbezogen stattfinden. Strategisches Hauptziel der Auditierungen ist es, Verbesserungspotentiale im Rahmen des BSI IT-Grundschutzes zu identifizieren, partielle Sicherheitskonzepte für Schlüsselapplikationen und -hardware zu bewerten sowie lösungsorientierte Maßnahmen abzuleiten. Durch diese Maßnahmen wird die erfolgreiche Erlangung der für das Jahr 2028 angestrebten ISO

---

27001-Zertifizierung verbindlich sichergestellt. Darüber hinaus wird mithin die Einhaltung des KVP / Audit Prozesse fortlaufend gewährleistet.

Es ist im Rahmen des Vertrages nicht erforderlich, den Briefkopf der jeweiligen Audit-Firma zu verwenden, sowie Testat fähig zu sein. Vielmehr wird die Dienstleistung im Rahmen eines Co-Sourcings durchgeführt, und die vorhandenen HIL-eigenen Ressourcen im Rahmen ihrer Verantwortlichkeiten unterstützt. Die Projektleitung wird durch den Informationssicherheitsbeauftragten oder einen Vertreter der Abteilung Informationssicherheit übernommen. Im Ausnahmefall wird die Prüfung durch das Auditteam des Dienstleisters vollumfänglich eigenständig durchgeführt.

## **2.2 Leistungsumfang**

### **2.2.1 Audit /Prüfungen**

Der Auditor soll im Rahmen des langfristigen Engagements / Vertrages folgende Prüfungen durchführen:

- Bewertung der IT-Sicherheitsmaßnahmen gemäß ISO 27001 und IT-Grundschutz sowie des zugrundeliegenden Reifegrades des ISMS und der damit aufgebauten Prozesse
- Prüfung der Einhaltung der Sicherheitsanforderungen aus dem Geheimschutzhandbuch (GHB) Anlage 4.
- Überprüfung von physischen, technischen und organisatorischen Sicherheitsmaßnahmen; ggf. auch bei externen IT-Dienstleistern und anderen Unterauftragnehmern der HIL
- Identifikation potenzieller Sicherheitsrisiken und Schwachstellen.
- Ableitung von Maßnahmen zur Schließung identifizierter Sicherheitslücken.
- Regelmäßige GAP – Analyse zum aufgestellten Projektplan zur Zertifizierung nach ISO 27000 auf Basis IT-Grundschutz
- Bewertung und Prüfung der aufgestellten und implementierten Prozesse zum Notfall- und Continuitymanagement insbesondere nach DER.4 mit den Schnittstellen (Erweiterungen) zu 200-4 (physisch, technisch und organisatorisch)
- Dokumentation der Ergebnisse u.a. Im SAVe Tool, gesonderten Textberichten nach Vorgabe, Ergebnispräsentationen
- Der Auditor soll die HIL auf die Zertifizierung ISO 27001 nach BSI GS vorbereiten. Alle Bewertungen und Maßnahmen sollen so aufgebaut sein, dass sie einer künftigen Zertifizierung bzw. externen Prüfung Stand halten.

### **2.2.2 Prüfungsnahe Beratung**

Prüfungsnahe Beratung zu ausgewählten Themen im Rahmen des BSI IT-Grundschutzes, des Notfallmanagements und auch für gesonderte Fragestellungen im Bereich von Sicherheitskonzepten soll Bestandteil des Rahmenvertrages sein. Dieses bezieht sich unter anderem auf folgende Punkte:

- Erstellung von Risikoanalysen im Bezug auf den Informationsverbund
- Bewertung von komplexeren Architektur- und Applikationsanforderungen im Rahmen des Changemanagements (Prüfersicht)

**Leistungsbeschreibung  
für die  
Dienstleistung eines Audits des Informations-  
verbundes HIL nach ISO 27001 auf Basis  
IT-Grundschutz**



- Erstellung von einzelnen ausgewählten Richtlinien für das ISMS der HIL GmbH
- Individuelles Coaching des ISB, Projektleitungen und Systemverantwortliche, auch insb. bzgl. wesentlicher Anpassungen im BSI IT-Grundschutz
- Beratung hinsichtlich der potentiellen Weiterentwicklungen im Grundschutz (z.B. Grundschutz ++)
- Planung und Durchführung von mindestens quartalsweisen Statusbesprechungen mit der HIL-Projektleitung / ISB; Protokollierung der Meetings; Grundsätzlich finden diese Meetings vor Ort in Bonn statt.

### 2.2.3 Grobe Abschätzung der Personentage insgesamt

Der ungefähre, sich aktuell abzeichnende Rahmen für eine Aufwandschätzung sieht folgende jährliche Personentage insgesamt vor.

| Jahr | Geschätzter Aufwand in Personentagen (PT) |
|------|-------------------------------------------|
| 2027 | 209                                       |
| 2028 | 209                                       |
| 2029 | 209                                       |
| 2030 | 23                                        |

Diese Aufwandsschätzung bezieht sich auf folgende Grundlage.

| Annahmen gemäß Standard und Vorgaben pro Jahr, abgeschätzt für einen 2-Personen Audit Team (1 HIL + 1 Extern) |                        |                         |                |                                           |                                                                          |
|---------------------------------------------------------------------------------------------------------------|------------------------|-------------------------|----------------|-------------------------------------------|--------------------------------------------------------------------------|
| Thema                                                                                                         | Anzahl                 | Tage total (nur extern) | Summe pro Jahr | Kommentar                                 | Annahmen (in Tagen)                                                      |
| Werk                                                                                                          | pro Jahr ein Werk      | +13 Tage                | 13             |                                           | 2-4 Vorbereitung; 4 Durchführung; 3 Bericht, 2 Abstimmung & Nacharbeiten |
| Bereich-Fläche                                                                                                | pro Jahr zwei Bereiche | +13 Tage                | 26             |                                           |                                                                          |
| IT-Applikation                                                                                                | pro Jahr ~ 8x          | + 5 Tage                | 40             | Top-Down nach Risikobewertung             |                                                                          |
| IT-Dienstleister                                                                                              | pro Jahr ~ 3x          | +5 Tage                 | 15             |                                           |                                                                          |
| Change Requests                                                                                               | pro Jahr ~ 5x          | +5 Tage                 | 25             | Je nach Komplexität                       | 1 Vorbereitung, 2 Durchführung, 1 Bericht, 1 Abstimmung & Nachbereitung  |
| Prozessaudit (Risikobasiert)                                                                                  | pro Jahr ein Prozess   | +10 Tage                | 10             |                                           |                                                                          |
| sonstiges                                                                                                     | pro Jahr 4x            | + 5 Tage                | 20             |                                           |                                                                          |
| <b>Zwischensumme:</b>                                                                                         |                        |                         | <b>149</b>     |                                           |                                                                          |
| HIL GmbH                                                                                                      | pro Jahr einmal        | 30                      | 30             | immer 2x externe Mitarbeiter (je 15 Tage) | 4 Vorbereitung, 5 Durchführung, 4 Bericht, 2 Abstimmung & Nachbereitung  |
| IT-Haupt Dienstleister                                                                                        | pro Jahr einmal        | 15                      | 15             | immer HIL zzgl eine ext. Ressource        |                                                                          |
| Prüfungsnahe, technische Unterstützung (Maßnahmen etc.)                                                       |                        | 15                      | 15             | immer extern                              |                                                                          |
| <b>Zwischensumme:</b>                                                                                         |                        |                         | <b>60</b>      |                                           |                                                                          |
| <b>Summe</b>                                                                                                  |                        |                         | <b>209</b>     |                                           |                                                                          |

## 3 Auditmethodik

Die durchzuführenden Prüfungen sollen durch eine Kombination folgender Methoden durchgeführt werden:

**Scope und Kontrollen:** Der Scope und die Anzuwendenden Kontrollen aus dem Annex A der ISO 27001 ist mit den beidseitigen Stakeholdern abzustimmen und können nach Ermessen angepasst werden.

**Dokumentenprüfung:** Analyse der relevanten Sicherheitsrichtlinien, Prozesse und Verträge sowie der zugehörigen Kontrollen und Reportings.

---

**Systemprüfungen:** Durchführen von technischen Analysen und Bewertung der grundsätzlichen Applikations- und Hardware Härtingsmaßnahmen.

**Technische Prüfungen:** Pentests und oder andere geeignete Mittel zur Substantiven Testung von Hardware- und Konfigurationseinstellungen. Code und/oder Anwendungseinsicht sind je nach Kritikalität bzw. Sensibilität mit dem Abteilungsleiter für Informationssicherheit / ISB abzustimmen und freizugeben.

**Interviews:** Gespräche mit Verantwortlichen des Informationsverbundes durchführen und auf Prozessebene auf Plausibilität prüfen. Die Gespräche gilt es zu dokumentieren und ggf. als Arbeitsergebnisse vorzuweisen.

**Vor-Ort-Begehung:** Inspektion der relevanten Räumlichkeiten und Infrastrukturen.

**Testverfahren:** Testverfahren zu der Kontrolle der umgesetzten Sicherheitsmaßnahmen / Kontrollen sollen je nach Ermessen in einer Voll- oder Stichprobenprüfung überprüft werden. Die einzelnen angewandten Testverfahren sollen in der Beurteilung beschrieben und plausibilisiert werden.

**Berichtswesen:** Übersichtlicher Bericht, mit Management Summary der Anforderungen und Umsetzungstand mit risikoevaluierten Maßnahmen beschreibt.

Etwaige sonstige Bewertungen und Stellungnahmen sollen die Auditmethodik antizipieren jedoch sachlogisch und effizient umsetzen.

## **4 Zeitplanung / Rahmenbedingungen**

Der Rahmenvertrag soll grundsätzlich den Zeitraum von Q1 2027 – Q1 2030 als Leistungszeitraum berücksichtigen. Verbindlich wären 4 Jahre ab Zeichnung des Vertrages.

Für die Leistungserbringung soll zunächst ein Audit-Universe aufgebaut werden. Dieses wird konsultativ zu erbringen sein. Ferner soll dann danach eine Grundlast der angenommenen PTs von 50% pro Jahr fest geplant werden. Die Planung mit Freigabe durch den ISB soll jeweils im Q1 des jeweiligen Jahres abgeschlossen sein. Die verbleibenden Tage werden gesondert zwischen AG und AN geplant. Hierfür wird eine Lead-Time von maximal vier Wochen für Auditprojekte von Beauftragung bis Beginn der Prüfung wesentlich sein. Ressourcen sollen dahingehend aus dem Personenportfolio angeboten werden. Es ist davon auszugehen, dass die Prüfungen nicht länger als 15 Kalendertage dauern werden, inkl. vorläufiger Abschlussempfehlungen. Gesonderte Leistungen wie z.B. prüfungsnahe Beratung werden individuell abgestimmt.

Zusätzlich sollen die gesamten Prüf- und Beratungstätigkeiten nur auf der von der HIL GmbH zur Verfügung gestellten Soft- und Hardwareumgebung bearbeitet und evaluiert werden. Eine Nutzung von Systemen außerhalb der HIL GmbH zur Dokumentation- und weiterverarbeitungszwecken ist strengstens untersagt.

---

## 5 Ergebnisse und Bericht

### Statusbericht und Entwicklungsübersicht:

- **aktueller Reifegradstatus:** Erfassung des Ist-Zustands im Hinblick auf das angestrebte Ziel
- **fortlaufende Entwicklungsübersicht:** Dokumentation der Fortschritte im Vergleich zu vorherigen Audits
- **Ziel-Tracking 2028:** Status und Trendanalyse zur Erreichung der ISO 27001-Zertifizierungsreife
- **Targetdates:** Die entsprechenden Berichte und Entwicklungsübersichten sind zweiwöchentlich vorzulegen.

Am Ende eines jeden Audits/Prüfung wird ein schriftlicher Bericht mit Handlungsempfehlungen für den ISB erstellt, die folgenden Inhalte umfasst:

### Zusammenfassung der Auditdurchführung:

- Scope / Rahmenbedingungen
- Management Summary
- Bewertung der Sicherheitsmaßnahmen gemäß ISO 27001 auf Basis IT-Grundschutz.
- Identifizierte Schwachstellen und Risiken.
- Empfehlungen zur Verbesserung der IT-Sicherheit.

Diese Berichtsformat soll grundsätzlich auch bei Prüfungen von Ad-Hoc Themen und auch etwaiger Penetrationstests Anwendung finden.