

Leistungsbeschreibung Beratungsleistung Informationssicherheit ÖPNV

Durchführung interner und Begleitung externer Audits der Informationssicherheit

1 Leistungsgegenstand

Der Auftragnehmer erbringt Beratungs- und Unterstützungsleistungen mit Schwerpunkt auf KRITIS-Anforderungen im IT-/OT-Umfeld des betrieblich-technischen Bereiches der HOCHBAHN.

1.1 Einarbeitung

- Aufbau und Struktur des ISMS
- Richtlinien und Prozesse des ISMS
- Aufbau und Struktur der betrieblich-technischen IT-/OT Systemlandschaften
- organisatorische Strukturen der HOCHBAHN-Technik
- Verantwortlichkeiten und Prozesse der HOCHBAHN-Technik
- informationssicherheitstechnische Besonderheiten der Abteilung Zugsicherungs- und Kommunikationsanlagen
- Ergebnisse der letzten internen und externen Audits sowie Pentests

1.2 Unterstützung bei internen Audits und Gap-Analysen

- Vorbereitung und Durchführung interner Audits gemäß ISO 27001 und VDV440/4400
 - Erstellung von Auditplänen und Checklisten gemäß BSI-Anforderungen
 - Erstellung von Prüfberichten
 - Bewertung von Konformität und Wirksamkeit
- Durchführung von Gap- und Reifegradanalysen im Kontext von Zugsicherungs- und Kommunikationsanlagen
- Prüfung der Maßnahmenumsetzung und Sicherstellung der Konformität mit BSIG, BSI-Vorgaben, ISO 27000er Reihe sowie VDV440/4400

1.3 Unterstützung bei KRITIS-Audits und § 39-Nachweisen

- Vorbereitung und Begleitung externer Audits (Erbringung von Nachweisen gemäß § 39 BSIG) zur Sicherstellung einer gesetzeskonformen Nachweisführung
- Beratung zu:
 - technisch-organisatorischen Maßnahmen zur Umsetzung der Controls
 - Meldepflichten
 - Reifegradbewertung und -erreichung gemäß Reife- und Umsetzungsgradbewertung im Rahmen der Nachweisprüfung (RUN) des BSI
- Begleitung der Audits
- Unterstützung der Nachbereitung

1.4 Erstellung und Qualitätssicherung von Richtlinien und Prozessen

- Erstellung und Weiterentwicklung audit- und prüfungssicherer Informationssicherheitsrichtlinien
- Unterstützung bei der (Weiter-)Entwicklung von Informationssicherheitsprozessen
- Qualitätssicherung der Richtlinien und Prozesse

2 Anforderungen an den Auftragnehmer

2.1 Anforderungen an das Unternehmen

- Nachweisbare Kompetenz und Erfahrung in der Beratung von Kunden im KRITIS-Umfeld bezogen auf die Themen im Leistungsgegenstand
- Zertifizierung der für den Auftraggeber relevanten Unternehmensbereiche in ISO 27001 o.ä.

2.2 Anforderungen an die eingesetzte Person

- Nachweisbare fundierte Normen- und Methodenkompetenz in:
 - BSIG und BSI-KritisV
 - BSI Orientierungshilfe Systeme zur Angriffserkennung
 - BSI-Standards (200-X) und Methoden, auch mit RUN und GAI-N
 - VDV-Schrift 440 und VDV-Mitteilung 4400
- Nachweisbare Prüfkompentenz in:
 - BSI IT-Grundschutz
 - ISO 27000er Reihe (bspw. Lead Implementer, Lead Auditor)
 - IEC 62443
 - Erbringung von Nachweisen gemäß § 39 BSIG in KRITIS-Unternehmen
- Nachweisbare mehrjährige praktische Erfahrung in:
 - KRITIS-Umfeld im ÖPNV
 - ÖPNV-Branchenkenntnisse
 - OT-Systeme im Umfeld von Zugsicherungs- und Kommunikationsanlagen
 - Erbringung von Nachweisen gegenüber dem BSI
 - Erstellung von Informationssicherheitsrichtlinien im IT- und OT-Bereich
 - Erstellung revisionssicherer Dokumentation
 - Durchführung von Reifegradanalysen im IT- und OT-Bereich im ÖPNV
- Persönliche Anforderungen:
 - sehr gute Deutschkenntnisse (C2)
 - hohe Kommunikations- und Moderationsfähigkeit
 - ausgeprägte Beraterkompetenz und die Fähigkeit, Themen im Unternehmen proaktiv voranzutreiben
 - Möglichkeit, voraussichtlich 2 Personentage pro Quartal vor Ort in Hamburg zu sein

Die Nachweise sind in Form von persönlichen Zertifikaten und individuellen Kundenreferenzen zu erbringen, die dem Angebot beizufügen sind.

3 Zeitlicher Rahmen und Umfang

Die Leistungserbringung erfolgt ab Zuschlagserteilung und endet unter Berücksichtigung möglicher Verlängerungen um zweimal 2 Jahre voraussichtlich im Jahr 2034.

Der Auftraggeber prognostiziert, dass eine Verfügbarkeit der Spezialisten von durchschnittlich insgesamt 1 Personentag in der Woche (Montag bis Freitag) erforderlich sein wird. Davon voraussichtlich durchschnittlich 2 Personentage pro Quartal vor Ort in Hamburg beim Auftraggeber. Ein Personentag entspricht 8 Stunden.

Als prognostiziertes Gesamtvolumen wird ein Bedarf von ca. 350 Personentagen (8 Stunden) geschätzt. Ein Anspruch auf Abruf besteht nicht.