Digitale Souveränität und Resilienz Manager (TÜV).

Strategien und Methoden für mehr Unabhängigkeit, Sicherheit und Zukunftsfähigkeit in einer vernetzten Welt

Seminar	4 Termine verfügbar	Zertifikat
Präsenz / Virtual Classroom	24 Unterrichtseinheiten	Online durchführbar

Seminarnummer: 32282

Stand: 03.06.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/32282

IT-Abteilungen stehen heute unter einem doppelten Druck: wachsende technische Abhängigkeiten von globalen Tech-Anbietern auf der einen Seite, ein drastisch verschärfter regulatorischer Rahmen auf der anderen. Wer als IT-Verantwortlicher **digitale Souveränität** und Resilienz aktiv gestalten will, braucht mehr als klassisches IT-Sicherheitswissen. Dieser dreitägige Zertifikatslehrgang vermittelt IT-Fach- und Führungskräften das strategische und technische Handwerkszeug, um technologische Abhängigkeiten zu reduzieren, souveräne Infrastrukturen zu entwerfen und gesetzliche Anforderungen proaktiv zu erfüllen. Schließen Sie den Kurs mit einem anerkannten, zukunftssicheren **TÜV Zertifikat für IT-Sicherheit** ab.

Nutzen

- **Anerkanntes Karriereziel:** Sie erwerben den offiziellen Titel **IT Resilienz Manager** mit einem renommierten **TÜV Zertifikat für IT-Sicherheit** als klaren Nachweis Ihrer strategischen Kompetenz.
- **Handlungsfähigkeit statt Ohnmacht:** Sie lernen den pragmatischen Ansatz „Derisking statt Decoupling“ und entwickeln einen direkt anwendbaren *Digital Sovereignty Action Plan* für Ihr Unternehmen.
- **Rechtssichere Auditierungsbasis:** Sie sind in der Lage, komplexe Vorgaben wie die **NIS2 Umsetzung in der IT-Abteilung** oder die **DORA Compliance in der IT** direkt in technische Architektur- und Beschaffungsentscheidungen zu übersetzen.
- **Exakte Zielgruppen-Ausrichtung:** Maßgeschneidert für IT-Leiter, Cloud-Architekten, Informationssicherheitsbeauftragte (ISBs) sowie Security- & Compliance-Verantwortliche, die Technologieentscheidungen strategisch absichern müssen.

Zielgruppe

- **IT-Leiter und IT-Verantwortliche**, die digitale Souveränität und Resilienz in ihrer Abteilung strukturiert aufbauen und verankern wollen.
- **IT-Architekten und Cloud-Verantwortliche**, die souveräne Architekturen entwerfen und Technologieentscheidungen unter Souveränitätsgesichtspunkten treffen müssen.
- **Security- und Compliance-Verantwortliche in der IT**, die regulatorische Anforderungen (NIS2, CRA, DORA, AI Act, EUCS) in operative IT-Maßnahmen überführen.
- **DSO- und DSR-Manager (in Aufbau oder Funktion)**, die ihre Rolle strategisch in der IT-Organisation positionieren und Schnittstellen zu Datenschutz, Einkauf und Security gestalten wollen.
- **IT-Projektverantwortliche**, die bei Cloud-Entscheidungen, Vendor-Auswahl und technologischen Umbrüchen sicher navigieren möchten.

Abschluss

Zertifikat

Geopolitische und technologische Risikofaktoren für IT-Infrastruktur

Regulatorische Rahmen: Was bedeutet das konkret für die IT-Abteilung

Die Rolle des DSR Managers in der IT-Organisation

Standortbestimmung: Souveränitäts-Assessment

Technische Säulen der Souveränität

Sovereign Cloud

Vendor-Lock und Exit Strategien

KI-Risiken und Sovereign AI

Eintscheidungsrahmen für IT-Verantwortliche

Digital Sovereignity Action Plan

Inhalte des Seminars

Das dreitägige Intensivprogramm bereitet Sie umfassend auf die strategischen Herausforderungen der modernen IT-Governance vor:

- **Tag 1 – Strategische Grundlagen & Regulatorischer Rahmen**
  - **Geopolitische & technologische Risiken:** Umgang mit US-Cloud-Diensten (CLOUD Act), extraterritorialen Abhängigkeiten sowie Zielszenarien für **Krypto-Agilität und PQC** (Post-Quantum Cryptography).
  - **Compliance-Anforderungen übersetzen:** Konkrete Handlungspflichten aus der **NIS2 Umsetzung in der IT-Abteilung**, den **Cyber Resilience Act Anforderungen**, DORA sowie dem EU AI Act.
  - **Das Rollenprofil:** Positionierung des DSR Managers an den Schnittstellen zu Einkauf, Cloud-Architektur und Security; Durchführung eines strukturierten Souveränitäts-Assessments.

- **Tag 2 – Technische Umsetzung & Sovereign AI**
  - **Sovereign Cloud Modelle im Vergleich:** Private, Public und Hybrid-Infrastrukturen; gezielter Einsatz europäischer Anbieter (IONOS, Hetzner, OTC, OVHcloud) für sensitive Workloads.
  - **Abhängigkeiten abbauen:** Methoden zur Vermeidung von Vendor-Lock-in sowie die Entwicklung praxistauglicher **Vendor-Lock-in Exit-Strategien** (Open Source vs. kommerzielle Systeme).
  - **Sovereign AI Architektur:** KI-Workloads souverän und DSGVO-konform betreiben (On-Premise LLMs vs. Corporate Cloud); Abwehr von Shadow AI und Prompt Injections.
  - **Extended Threat Intelligence:** Aufbau eines geopolitischen und regulatorischen Frühwarnsystems für IT-Teams.

- **Tag 3 – Operative Umsetzung & Zertifikatsprüfung**
  - **Digital Sovereignty Action Plan:** Erstellung des zentralen Steuerungsdokuments (Quick Wins, Strukturmaßnahmen und langfristige Transformations-Roadmaps).
  - **Change Management & IT-Governance:** Kommunikation von Souveränitätsrisiken gegenüber der Geschäftsführung und dem internen Team; offizielle TÜV-Zertifikatsprüfung.

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/32282 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang

- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.