Corporate Security nach DIN SPEC 14027.

Einordnung, Aufbau und Anwendung des neuen Standards zur Stärkung physischer Resilienz von Organisationen

Seminar	Zurzeit keine Termine	Teilnahmebescheinigung
Präsenz / Virtual Classroom	8 Unterrichtseinheiten	

Seminarnummer: 32294

Stand: 31.08.2026. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/32294

Für Arbeitsschutz, Datenschutz und IT-Sicherheit bestehen seit Jahren etablierte Standards. Für die Unternehmenssicherheit gab es bislang keinen. Mit der im April 2026 veröffentlichten DIN SPEC 14027 liegt erstmals ein branchen- und größenunabhängiger Standard für die physische Sicherheit von Organisationen vor, initiiert und finanziert durch das Bundesministerium des Innern im Rahmen des Aktionsplans 2024+ zur Nationalen Wirtschaftsschutzstrategie. Das Seminar ist der Einstieg in dieses neue Regelwerk: Es ordnet den Standard ein, erschließt seinen Aufbau und macht die Arbeit mit dem Dokument an einem Fallbeispiel erfahrbar.

Nutzen

- Sie ordnen die DIN SPEC 14027 sicher ein: Entstehung, Auftraggeber, Zielsetzung und Unterschied zu einer DIN-Norm.
- Sie kennen die Abgrenzung zu benachbarten Standards und wissen, wo sich die Anforderungen in ein bestehendes integriertes Managementsystem einfügen lassen.
- Sie lernen die Methodik der Schutzbedarfsermittlung kennen und erproben sie an einem Fallbeispiel.
- Sie überblicken die 16 Handlungsfelder und können einschätzen, welche davon für Ihre Organisation relevant sind.
- Sie wissen, wie Sie mit den Anforderungskatalogen des Anhangs arbeiten, und können sie für Standortbestimmung, interne Reviews und die Steuerung externer Dienstleister nutzen.
- Sie nehmen ein Arbeitsraster mit, mit dem Sie die Standortbestimmung anschließend in Ihrer eigenen Organisation angehen können.

Zielgruppe

Sicherheits- und Security Manager, Informationssicherheits- und IT-Sicherheitsbeauftragte, die ihre Verantwortung über die Informationssicherheit hinaus ganzheitlich ausrichten. Notfall-, Krisen- und Business-Continuity-Verantwortliche. Compliance Officer und Risikomanager mit Berührung zur physischen Sicherheit. Werk-, Standort- und Sicherheitsleitungen sowie Führungskräfte des Werkschutzes. Beratende und auditierende Fachkräfte, die den neuen Standard einordnen und anwenden müssen. Angesprochen sind ebenso Verantwortliche in Organisationen, die eine Sicherheitsfunktion erst aufbauen.

Abschluss

Teilnahmebescheinigung

Teilnahmebescheinigung der TÜV Rheinland Akademie

Inhalte des Seminars

Einordnung und Hintergrund

- DIN-Norm, DIN SPEC und PAS-Verfahren: Unterschiede und praktische Bedeutung
- Auftraggeber, Konsortium und Entstehung des Dokuments
- Vom Wirtschaftsgrundschutz zum Corporate Security Grundschutz
- Zielsetzung, Nutzergruppen und Anwendungsbereich
- Regulatorischer Kontext: Nationale Wirtschaftsschutzstrategie, KRITIS-Dachgesetz, organisatorische Sorgfaltspflichten

Abgrenzung und Einbettung

- Bewusst nicht behandelte Themen und Abgrenzung zum Arbeitsschutz
- Anschlusspunkte zu ISO/IEC 27001, BSI IT-Grundschutz und weiteren Standards
- Einbindung in ein integriertes Managementsystem
- All-Gefahren-Ansatz sowie Zusammenspiel der Rollen von CSO und CISO

Aufbau des Dokuments und Arbeit mit den Anhängen

- Themenübergreifende und themenspezifische Handlungsfelder
- Die wiederkehrende Struktur: Allgemeines, Anforderungen, Schnittstellen
- Die Anforderungskataloge als prüfbare Vorgaben für Standortbestimmung, interne Reviews und Leistungsbeschreibungen
- Informative Hilfsmittel: Bedrohungsszenarien, Lastannahmen, Schutzbedarfskategorisierungen

- Modularer und ganzheitlicher Einsatz des Standards

Schutzbedarfsermittlung als methodischer Kern

- Identifikation und Klassifizierung von Organisationswerten
- Strategische und operative Schutzziele
- Bewertung von Assetkritikalität und Bedrohungsintensität
- Schutzbedarfsmatrix, Bruttobewertung und Netto-Risiko
- Schwellenwerte, nicht akzeptable Gefährdungen und Ableitung des Schutzkonzepts
- Übung am Fallbeispiel

Die 16 Handlungsfelder im Überblick

- Sicherheitslagebild, Sicherheitskultur und Kommunikation, Interne Untersuchung
- Störungs-, Notfall- und Krisenmanagement sowie Business Continuity Management
- Standortsicherheit, Personenschutz, Veranstaltungsschutz, Bedrohungsmanagement, Reisesicherheit
- Integritätsprüfung, Know-how-Schutz, Lieferkettensicherheit
- Auswahl und Steuerung sicherheitsbezogener Dienstleistungen
- Aufbau und Betrieb eines Sicherheitsmanagementsystems
- Arbeit mit ausgewählten Anforderungskatalogen an konkreten Beispielen

Transfer in die eigene Organisation

- Erste Selbsteinschätzung: Welche Handlungsfelder sind für die eigene Organisation relevant?
- Überlegungen zu einem modularen Einstiegspfad
- Schnittstellen zu Informationssicherheit, Business Continuity, Facility Management, Einkauf und Personalwesen
- Ansatzpunkte für die Argumentation gegenüber der Organisationsleitung

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/32294 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.