Kompetenzprofil/Zertifizierungsprüfung „Certified Resilience Expert (CRE)“

Rollenbeschreibung „Certified Resilience Expert (CRE)“	
Ziele	In der heutigen, schnelllebigen Geschäftswelt ist Resilienz entscheidend für den langfristigen Erfolg und die Stabilität von Unternehmen und Organisationen. Durch die RKE und NIS II Richtlinien haben sich auch die rechtlichen Rahmenbedingungen für Unternehmen und Organisationen erheblich geändert. Im Zentrum steht dabei der Schutz von Daten. Mit dem Zertifikat „Certified Resilience Expert (CRE)“ wird ein Standard etabliert, bei dem Personen ein grundlegendes Verständnis für die verschiedenen Aspekte der organisatorischen Resilienz besitzen. Zertifikatsinhaber:innen sind in der Lage, Resilienz in ihrer gesamten Breite zu verstehen und in ihren Organisationen zu leben.
Aufgaben / Verantwortlichkeiten	Certified Resilience Expert verfügen über Grundkenntnisse des Risikomanagements sowie des Business Continuity und Notfall- sowie Krisenmanagements. Sie unterstützen bei der Vermittlung des Bewusstseins für die Bedeutung der physischen Sicherheit und von Informationssicherheit sowie der Cyber Security in der Organisation. Dies umfasst auch die Einhaltung der einschlägigen gesetzlichen Rahmenbedingungen, insbesondere der RKE und der NIS II Richtlinie. Certified Resilience Expert unterstützen den/die Certified Resilience Manager:in dabei, die Mitarbeiter:innen und Führungskräfte zu beraten, um eine Kultur der Resilienz in der Organisation zu schaffen.

Kompetenzprofil/Zertifizierungsprüfung „Certified Resilience Expert (CRE)“

QUALIFIKATIONSBEREICHE UND KOMPETENZFELDER

Die in der nachfolgenden Tabelle angeführten Qualifikationsbereiche und Kompetenzfelder geben einen Überblick über die Kenntnisse, Fertigkeiten und Kompetenzen des nach dem Standard der EN ISO/IEC 17024 erarbeiteten „Certified Resilience Expert (CRE)“.

Kompetenzfeld	**Qualifikationsbereiche** **Kenntnisse - Fertigkeiten - Kompetenzen**
Fachkompetenz/ Kontextkompetenz/ Sozialkompetenz	Certified Resilience Expert (CRE) besitzen ein breites Spektrum an Grundkenntnissen, die notwendig sind, um den gesetzlichen Anforderungen der EU-Richtlinien NIS II und RKE zu entsprechen. **Allgemeines** • Kenntnisse über die Aufgaben und Verantwortlichkeiten eines/einer Certified Resilience Expert **Risikomanagement** • Kenntnisse über die Prinzipien und Techniken des Risikomanagements • Grundkenntnisse über die Entwicklung und Anwendung von Risikomanagementstrategien. • Grundkenntnisse über den Einsatz von Tools und Techniken zur Risikoanalyse und -bewertung **Business Continuity Management** • Kenntnisse über die Grundlagen des Business Continuity Managements und dessen Bedeutung für die Unternehmensresilienz • Grundkenntnisse über die Erstellung und Verwaltung von Business Continuity Plänen (Notfallpläne, Geschäftsfortführungspläne, Wiederanlaufpläne). • Grundkenntnisse über die Durchführung von Business Impact Analysen und Entwicklung von Wiederherstellungsstrategien. **Notfall- & Krisenmanagement** • Kenntnisse über die Prinzipien des Notfall- und Krisenmanagements, einschließlich Vorbereitung, Reaktion und Wiederanlauf in den Normalbetrieb. • Grundkenntnisse über die Koordination von Notfall- und Krisenreaktionsteams. • Grundkenntnisse über die Entwicklung und Implementierung von Notfall- und Krisenreaktionsplänen.

	Physische Sicherheit • Kenntnisse über die Grundlagen der physischen Sicherheit und deren Anwendung in verschiedenen Umgebungen • Grundkenntnisse über die Bewertung und Verbesserung der physischen Sicherheit von Einrichtungen • Kenntnisse über die Möglichkeiten der Implementierung von Perimeterschutz, Überwachungssystemen und anderen Sicherheitsmaßnahmen **Informationssicherheit** • Grundkenntnisse der Informationssicherheit, einschließlich Datenschutzbestimmungen • Grundkenntnisse über die Identifikation und Bewältigung von Bedrohungen für die Informationssicherheit • Grundkenntnisse über Maßnahmen zur Datensicherheit und zum Schutz sensibler Informationen. **Cyber Security** • Kenntnisse über die Grundprinzipien der Cyber Security und aktuelle Bedrohungsszenarien • Kenntnisse über die Erkennung und Abwehr von Cyberangriffen. • Kenntnisse über die Implementierung von Cybersecurity-Maßnahmen, einschließlich Firewalls, Antivirensoftware und Netzwerksicherheit. **Gesetzliche Rahmenbedingungen (NIS II und CER)** • Grundkenntnisse über die Anforderungen und Bestimmungen der NIS II- und CER-Richtlinie.