>> Digital Operational Resilience Act (DORA)

Wie Banken Cyber-Bedrohungen meistern

EGOS! the education company

DORA enthält Vorgaben für die Resilienz von IKT-Systemen für verschiedene Arten von Finanzunternehmen, wie beispielsweise für Kreditinstitute (Banken) und Versicherungsunternehmen sowie für deren IKT-Dienstleister.

Ihr Nutzen

In diesem spannenden Vortrag erfahren Sie die wichtigsten Eckpunkte und Informationen zu DORA und erhalten Tipps wie Sie Ihre Organisation zur Stärkung der digitalen operationalen Resilienz nach DORA vorbereiten.

Voraussetzungen

keine

Preis pro Teilnehmer

EUR 400,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Tag(e)/Day(s)

Hinweise

Die Inhalte dieser Präsentation können individuell an Rahmenbedingungen und Richtlinien in Ihrer Organisation angepasst werden.

Version: N/A

Seminarinhalte

* Digitalisierung in der Finanzindustrie
- Entwicklung der Finanzbranche im digitalen Zeitalter
- Wichtige IKT-Risikokategorien und Bedeutung in der Bankenwelt

* DORA – Hintergrund, Ziele und Regelungsinhalte
- Zielsetzung des Digital Operational Resilience Act
- Entstehung und Notwendigkeit von DORA

* Regelungsübersicht
- Allgemeine Bestimmungen
- IKT-Risikomanagement
- Behandlung und Berichterstattung von Vorfällen
- Testen der digitalen Resilienz
- Management des IKT-Drittparteienrisikos
- Ergänzende nationale Begleitgesetzgebungen

* Bedeutung für Banken
- Änderungen und Anforderungen DORA konkret für den Bankensektor

* IT-Risikomanagement und Cyber-Bedrohungslage in der Praxis

* IT-Risikomanagement im Bankensektor
- Besonderheiten und Praxisbeispiele aus Finanzunternehmen

* Cyberbedrohungen im Finanzmarkt
- Typische Angriffstechniken und aktuelle Trends
- Herausforderungen bei der Abwehr von Cyberangriffen

* Auswirkungen von DORA auf das Risikomanagement
- Anpassungen und neue Anforderungen, etwa in der Berichterstattung und

* Spezifische Instrumente und Umsetzungsbeispiele

* Threat-Led Penetration Testing (TIBER)
- Vorstellung des TIBER-Ansatzes und dessen Umsetzung
- Praxisbeispiele und Erkenntnisse (TIBER-DE als Exkurs)

* Management des Drittparteienrisikos
- Regulatorische Vorgaben und praktische Lösungsansätze
- Bedeutung der Überwachung kritischer IKT-Drittdienstleister

* Informationsaustausch und Zusammenarbeit
- Mehrwert und Praxisbeispiele (VPN Zero-Day-Vorfall)
- Vorbildfunktion skandinavischer Modelle

* Regulatorischer Rahmen & Aufsichtsmechanismen

* IKT-Risiko-Beaufsichtigung im Bankensektor
- Aufbau der Aufsicht, Vor-Ort-Prüfungen, laufende Kontrollen und Aufsichtsmaßnahmen

* Rechtliche Rahmenbedingungen
- Überblick über angrenzende Rechtsakte (NIS-2-Richtlinie, Cyber Resilience Act, EU-Zertifizierungsrahmen)
- Sanktionsregime und praktische Auswirkungen (u.a. strafrechtliche Aspekte und Verwaltungsstrafen)

* Herausforderungen und Erfolgsfaktoren bei der Umsetzung

* Typische Herausforderungen
- Notwendigkeit neuer Ansätze in der IT-Sicherheitsarchitektur
- Von der Idee zur praktischen Implementierung – Best Practices und Lösungsansätze

* Ausblick und strategische Empfehlungen
- Zukunftstrends im Bereich Cybersecurity und Digitalisierung
- Handlungsempfehlungen für Geschäftsleiter und operative Teams

* Zusammenfassung & Diskussion

Unsere BildungsberaterInnen stehen Ihnen gerne zur Verfügung. Innsbruck +43 (0)512 36 47 77.