EDAY 2025 SALZBURG

Zukunft gestalten.
Digitalisierung für Ihr Unternehmen

WKS
Unternehmensberatung · Buchhaltung · IT

EDAY 2025 SALZBURG

Cybersecurity & Compliance
Überblick, Umsetzung aktueller Vorschriften

mIT-Security
powered by 7FREAKS

WKS
Unternehmensberatung · Buchhaltung · IT

NIS2, DORA, CRA, ISO:27001, TISAX und ISMS
Sicherheit und Compliance in der digitalen Welt

Ziel des Vortrags: Kompakte Orientierung zu aktuellen Sicherheitsstandards und Verordnungen

Bedeutung für Unternehmen: Schutz vor Cyberbedrohungen, gesetzliche Compliance, Wettbewerbsvorteile

Warum sind diese Standards & Verordnungen relevant?
Durch den Dschungel navigieren

- Steigende Cyberbedrohungen und regulatorische Anforderungen
- Haftungsrisiken und Strafen bei Nichteinhaltung
- Wettbewerbsvorteil durch zertifizierte Sicherheitsstandards

NIS2 – Network and Information Security Directive 2
Stärkung der Cybersicherheit

NIS2 baut auf NIS(1) auf, erweitert aber die Pflichten

Sanktionen bei NICHT-Compliance – Hohe Bußgelder

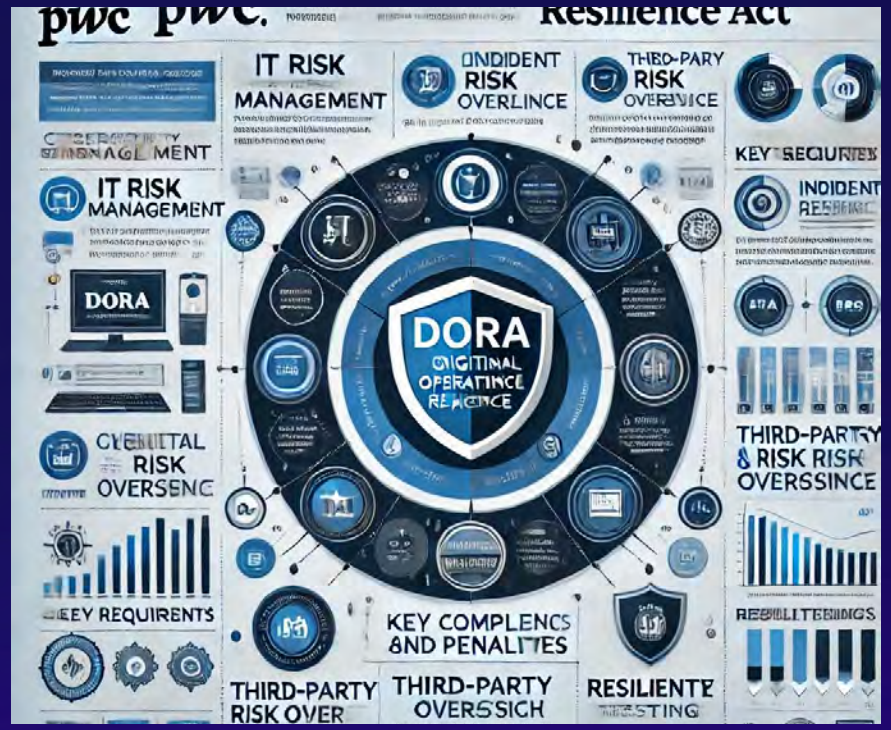
Unternehmen sollten ein ISMS einführen um Anforderungen zu erfüllen

→ **Kritische Infrastruktur & wesentliche Unternehmen**

→ **Strikte Sicherheitsanforderungen & Meldepflichten**

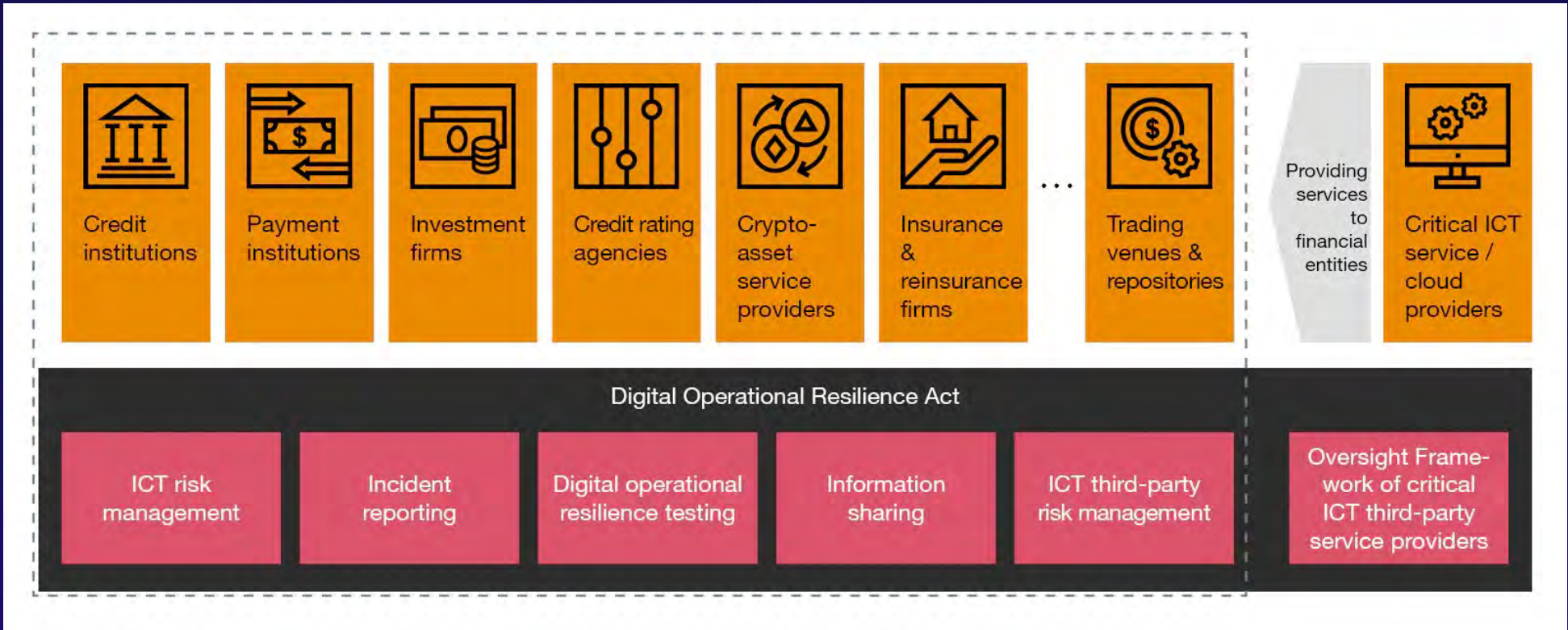
→ **Erweiterter Anwendungsbereich**

DORA - Digital Operational Resiliance Act
Sicherheit und Compliance in der digitalen Welt



- Finanzsektor im Fokus
- Banken, Versicherungen, Zahlungsdienstleister
- Wichtigster Punkt: IT Risiko Management und Resilienz
- Stärkere Kontrolle von Drittanbietern (Cloud, IT Dienstleister)

DORA - Digital Operational Resiliance Act
Sicherheit und Compliance in der digitalen Welt



© PWC.at

CRA – Cyber Resilience Act
Sicherheitsstandards für digitale Produkte

Keine Mindestgröße – auch Startups betroffen

Hersteller müssen Sicherheitsstandards in Entwicklung und Wartung einhalten

Bedeutung für Unternehmen: Nutzung sicherer Produkte und Lieferketten

CRA betrifft auch Unternehmen, die digitale Produkte nutzen und verkaufen

→ **EU Cyber Resilience Act für Hersteller von Hard- & Software**

→ **Sicherh.anford. entlang des gesamten Produktlebenszyklus**

→ **Meldepflicht für Sicherheitslücken**

ISO 27001
Internationaler Standard für Informationssicherheit

- Strukturierter Ansatz zum Schutz sensibler Informationen
- Identifikation, Bewertung und Behandlung von Risiken
- Zertifizierung als Nachweis für Kunden und Partner

TISAX – Trusted Information Security Assessment Exchange
Sicherheisstandard in der Automobilbranche

- Branchenstandard für Informationssicherheit in der Automobilbranche
- Für Zulieferer und Dienstleister verpflichtend
- Vergleichbar mit ISO27001 jedoch mit branchenspezifischen Anforderungen

ISMS – Information Security Management System
DAS Fundament der IT-Sicherheit

- Systematisches Management von Informationssicherheit
- Kontinuierliche Verbesserung durch Monitoring & Audits
- Erforderlich für NIS2, ISO 27001, DORA & TISAX

Praktische Umsetzung – Schritt für Schritt
Stärkung der Cybersicherheit

- **Risikoanalyse durchführen**
- **Sicherheitsrichtlinie definieren**
- **Technische & Organisatorische Maßnahmen implementieren**
- **Schulungen und Sensibilisierung der Mitarbeiter**
- **Regelmäßige Audits und Kontrollen**

Überblick

Kriterien	NIS2	DORA	CRA	ISO 27001	TISAX	ISMS
Gilt für Unternehmen allgemein	✅	❌	❌	✅	❌	✅
Pflicht zur Risikoanalyse	✅	✅	✅	✅	✅	✅
Strenge Meldepflichten	✅	✅	✅	❌	❌	❌
Zertifizierung notwendig	❌	❌	❌	✅	✅	✅
Fokus auf Cybersicherheit	✅	✅	✅	✅	✅	✅
Spezifisch für Finanzsektor	❌	✅	❌	❌	❌	❌
Spezifisch für digitale Produkte	❌	❌	✅	❌	❌	❌
Relevanz für Automobilindustrie	❌	❌	❌	❌	✅	❌
Strafen bei Nichteinhaltung	✅	✅	✅	❌	❌	❌

Fragen und Antworten

www.eday-salzburg.at/download

mIT-Security
powered by 7FREAKS

Danke

Compliance, Cybersecurity &
ISMS Consulting
Security as a Service
Incident Response
office@mit-security.at
0662 202 777 900
mit-security.at

18.03.2025

mIT-Security powered by 7FREAKS

WKS Unternehmensberatung · Buchhaltung · IT