

Security Regulatory Compliance

Die Einhaltung gesetzlicher Vorschriften stellt sicher, dass Unternehmen branchenspezifische Sicherheitsstandards und gesetzliche Anforderungen einhalten, um die Verfügbarkeit ihrer Dienste aufrecht zu halten, sensible Daten zu schützen, Risiken zu minimieren und Vertrauen zu wahren.



Compliance

- Sind die definierten Anforderungen erfüllt und wirksam umgesetzt?
- Wird die Maßnahmen-erfüllung dokumentiert?
- Sind die Maßnahmen auch durch Dritte prüfbar (z. B. qualifizierte Stelle)?

Compliance ist für Unternehmen, die in regulierten Branchen wie Finanzen, Energieversorgung, kritischer Infrastruktur und Technologie tätig sind, von entscheidender Bedeutung. Die Nichteinhaltung dieser Standards kann zu Strafen, finanziellen Verlusten und Reputationsschäden führen.

Die regulatorischen Anforderungen an österreichische Unternehmen im Bereich IT- und Cybersicherheit steigen von Jahr zu Jahr. Die bestehende IT- und Security-Organisation sowie Fachbereiche verfügen meist nicht über ausreichende Ressourcen und internes Know-how, um die neuen An-

Security

- Sind die Systeme und Anwendungen auch tatsächlich vor Bedrohungen geschützt?
- Sind wir in der Lage, die Angriffe zeitnah zu erkennen und zu berichten?
- Kann schnell und wirksam reagiert werden?

forderungen zu identifizieren und in der Organisation umzusetzen.

Unser Ansatz:

Unsere Expert:innen für Security Regulatory Compliance unterstützen Sie dabei, die regulatorischen Anforderungen mittels einer klaren IT-Governance und eines wirksamen IKT-Risikomanagementrahmens zu erfüllen. Gleichzeitig helfen wir Ihnen bei der Definition und Umsetzung von konkreten und zielgerichteten organisatorischen und technischen Maßnahmen, um das Sicherheitsniveau in der Organisation zu erhöhen und alle internen und externen Stakeholder miteinzubeziehen.



Wir helfen Ihnen, sowohl compliant als auch sicher zu werden!

Wir bieten Ihnen unsere Expertise zu folgenden Regulatorien:

- NIS-2
- RKE (Resilienz kritischer Einrichtungen)
- DORA (Digital Operational Resilience Act)
- AI Act
- CRA (Cyber Resilience Act)
- DSGVO

Ihre Vorteile:

- Aktives Wahrnehmen der Managementverantwortung und proaktive Umsetzung stärkt Vertrauen der Kunden
- Reduzierung des Bußgeld- und Haftungsrisikos
- Aktuelles Expert:innenwissen ohne internen Ressourcenaufbau
- Effiziente externe Umsetzungsbegleitung verringert Aufwand für interne Teams
- Höheres Sicherheitsniveau

Unsere Leistungen im Überblick:



Durchführung von Gap-Assessments / Readiness-Checks:

Durch Dokumentenreviews und Interviews/Workshops mit ausgewählten Ansprechpartner:innen in der Organisation erheben wir den derzeitigen Umsetzungsstand der regulatorischen Anforderungen sowohl auf Vorgaben- als auch auf operativer Umsetzungsebene.



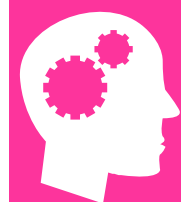
Management-Berichterstattung:

Wir zeigen vorhandene Lücken und Nicht-Compliance mit regulatorischen Vorgaben auf und geben klare Handlungsempfehlungen.



Roadmap-Planung:

Auf Basis der Handlungsempfehlungen erstellen wir gemeinsam mit Ihnen eine strukturierte und priorisierte Maßnahmenliste und Zeitplanung.



Umsetzungsbegleitung der Roadmap:

Wir begleiten sowohl mittelständische und große Unternehmen als auch Gruppen und Konzerne bei der operativen Implementierung der Roadmap. Wir stehen Ihnen sowohl mit unserer Fachexpertise als auch der Bereitstellung externer Projektmitarbeiter:innen zur Verfügung.



Begleitung bei aufsichtlichen Prüfungen:

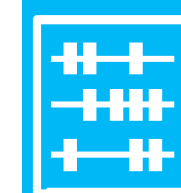
Wir unterstützen unsere Kunden in allen Prüfungsphasen:

- Prüfungsvorbereitung und -begleitung
- Erarbeitung und Qualitätsreview von Stellungnahmen nach Berichtzustellung
- Roadmap-Planung und Umsetzungsbegleitung bei den definierten Maßnahmen.



Training für Führungskräfte:

Wir schulen die Managementebene hinsichtlich der regulatorischen Anforderungen von DORA, NIS-2 und Co. und befähigen sie, IT- und Informationssicherheitsrisiken und die Auswirkungen auf die Geschäftstätigkeit ihres Unternehmens verstehen und bewerten zu können.



Third Party (Risk) Management:

Sichere Lieferketten, die regulatorische Anforderungen an Auswahl und Monitoring der Lieferanten sowie Erkennen und schnelle Reaktionen auf Supply-Chain-Angriffe ermöglichen, sind überlebensnotwendig für Unternehmen.



Cyber Resilience Act:

Wir führen eine Betroffenheitsanalyse für relevante Produkte durch und begleiten anschließend bei der Erstellung der notwendigen Dokumentation und Umsetzung der Anforderungen.

KPMG.
Make the
Difference.

Kontakt

Für weitere Informationen wenden Sie sich bitte an unsere Expert:innen oder besuchen Sie uns unter [kpmg.at](https://www.kpmg.at).

Lisa Schumy
Managerin

M +43 664 888 291 93
lschumy@kpmg.at

Lisa Haltmeyer
Managerin

M +43 664 266 84 41
lhaltmeyer@kpmg.at

Max Schwinger
Manager

M +43 664 816 10 24
mschwinger@kpmg.at

[kpmg.at](https://www.kpmg.at)



© 2025 KPMG Austria GmbH Wirtschaftsprüfungs- und Steuerberatungsgesellschaft, eine österreichische Gesellschaft mit beschränkter Haftung und ein Mitglied der globalen KPMG Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer private English company limited by guarantee, angeschlossen sind. Alle Rechte vorbehalten.