



Security Governance & Organization

Die zunehmende Komplexität der Bedrohungslandschaft, regulatorische Anforderungen und die rasante Entwicklung neuer Technologien erfordern eine proaktive und umfassende Betrachtung der Informationssicherheit.

In der heutigen digitalen Landschaft reichen technische Maßnahmen allein nicht mehr aus, um komplexe und sich ständig weiterentwickelnde Bedrohungen abzuwehren. Wahre Cyberresilienz entsteht durch eine klare Governance, definierte organisatorische Strukturen und gelebte Prozesse. Eine effektive Security Governance stellt sicher, dass Ihre Sicherheitsinitiativen direkt auf Ihre Geschäftsziele einzahlen und Ihr Unternehmen nachhaltig schützen.

Kommt Ihnen eine dieser Situationen bekannt vor?

- Ihre Sicherheitsstrategie ist nicht klar mit den übergeordneten Unternehmenszielen verknüpft.
- Es existieren keine klar definierten Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit.
- Sicherheitsmaßnahmen wirken reaktiv und unkoordiniert statt proaktiv und strategisch.
- Es fällt Ihnen schwer, den Return on Investment (ROI) für Sicherheitsausgaben nachzuweisen.
- Die Einhaltung regulatorischer Anforderungen (Compliance) ist ein komplexer und manueller Prozess.

Ohne eine solide Governance bleiben Sicherheitsmaßnahmen oft ein reines Cost-Center, anstatt als strategischer Wegbereiter für das Geschäft zu fungieren.

Unser Ansatz: Strategie, Struktur und Erfolg

Wir verstehen, dass jedes Unternehmen einzigartig ist und spezifische Bedürfnisse und Herausforderungen hat. Daher bieten wir **maßgeschneiderte Lösungen**, die auf die individuellen Anforderungen Ihres Unternehmens abgestimmt sind.

Wir arbeiten dabei eng mit Ihrem Team zusammen, um sicherzustellen, dass Ihre Bedürfnisse optimal umgesetzt werden.

Wir helfen Ihnen, Ihre **Sicherheitsausgaben zu optimieren** und sicherzustellen, dass Ihre Investitionen in die Informationssicherheit **maximalen Nutzen** bringen.

Mit unserer umfassenden Beratung und Unterstützung sind wir Ihr Partner in der Entwicklung einer Sicherheitsorganisation, die nicht nur den aktuellen Anforderungen entspricht, sondern auch in der Lage ist, sich an zukünftige Bedürfnisse anzupassen.

Wir verwandeln Ihre Sicherheitsorganisation von einer reaktiven Einheit in einen **proaktiven, strategischen Partner des Unternehmens**.



Aufbau von Informationssicherheits-Governance-Strukturen:

Wir etablieren klare Governance-Strukturen durch die Entwicklung eines umfassenden Policy Frameworks. So stellen wir sicher, dass Ihre Sicherheitsmaßnahmen effektiv gesteuert, überwacht und kontinuierlich an neue Bedrohungen angepasst werden.



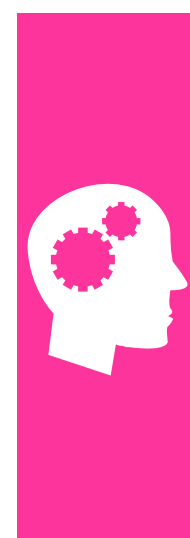
Aufbau und Optimierung der Sicherheitsorganisation:

Wir definieren klare Rollen, Verantwortlichkeiten und Berichtswege (z. B. für die CISO-Rolle und das Sicherheitsteam), um Effizienz und Verantwortlichkeit zu gewährleisten.



Security Cost Management:

Wir sorgen für einen maximalen Return on Security Investment. Durch die Analyse und Optimierung Ihrer Sicherheitsausgaben helfen wir Ihnen, Budgets effizient zu steuern und Ihre Ressourcen gezielt dort einzusetzen, wo sie den größten Nutzen bieten.



CISO as a Service:

Unser CISO as a Service bietet Ihnen flexible, strategische Erfahrungen im Bereich Informationssicherheit zur optimalen Betreuung Ihres Unternehmens hinsichtlich sämtlicher Informationssicherheitsbelange.



Management von Sicherheitsrisiken:

Wir implementieren pragmatische Prozesse zur systematischen Identifizierung, Bewertung und Behandlung von Risiken, damit Sie Ihre Ressourcen dort einsetzen, wo sie am wichtigsten sind.



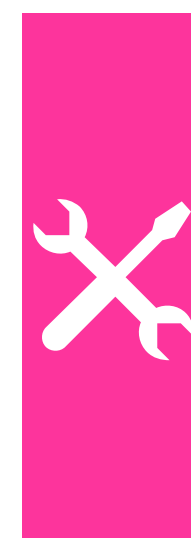
Security KPI Reporting:

Wir machen Sicherheit messbar. Gemeinsam definieren wir relevante Kennzahlen (KPIs) und implementieren ein aussagekräftiges Reporting. So erhalten Sie eine transparente Datengrundlage für fundierte Entscheidungen und die kontinuierliche Optimierung Ihrer Maßnahmen.



Implementierung von Managementsystemen (ISMS):

Wir unterstützen Sie bei der Einführung, dem Betrieb und der Zertifizierung eines Informationssicherheits-Managementsystems nach etablierten Standards wie ISO/IEC 27001 oder BSI IT-Grundschutz.



GRC-Tooling:

Wir unterstützen bei der Auswahl und Implementierung von GRC-Lösungen, um Ihre Governance-, Risiko- und Compliance-Prozesse zu automatisieren, um eine zentrale Datenbasis zu schaffen und die Nachweisbarkeit für Audits sicherzustellen.



**Sind Sie bereit,
Ihre Security
Governance auf
die nächste Stufe
zu heben?**

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).

Thomas Horn
Senior Manager

M +43 664 887 990 10
thorn1@kpmg.at

Lisa Haltmeyer
Senior Managerin

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

Lisa Schumy
Senior Managerin

M +43 664 888 29 193
lschumy@kpmg.at

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



© 2026 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.