ISMS - Risk Register

Das Risk Register ist ein zentrales Dokument im Informationssicherheitsmanagementsystem. Es dient dazu, identifizierte Risiken strukturiert zu dokumentieren, zu bewerten und geeignete Maßnahmen zur Risikobehandlung festzulegen. Es entsteht im Rahmen der Risikoanalyse und bildet die Grundlage für die Steuerung von Informationssicherheitsrisiken innerhalb der Organisation.

In einem Risk Register werden Risiken systematisch erfasst. Für jedes Risiko werden das betroffene Asset, mögliche Bedrohungen sowie vorhandene Schwachstellen dokumentiert. Ergänzend werden die Eintrittswahrscheinlichkeit und die potenziellen Auswirkungen bewertet. Aus dieser Bewertung ergibt sich die Risikoklasse, die als Grundlage für die Priorisierung von Sicherheitsmaßnahmen dient.

Ein typisches Risk Register enthält mehrere Informationsfelder. Dazu gehören eine eindeutige Risiko-ID, das betroffene Informationsasset, die identifizierte Bedrohung sowie die zugrunde liegende Schwachstelle. Zusätzlich werden Eintrittswahrscheinlichkeit und Auswirkung bewertet, um das Gesamtrisiko zu bestimmen. Darüber hinaus werden geplante oder bereits umgesetzte Maßnahmen dokumentiert, ebenso wie die verantwortliche Person und der aktuelle Status der Risikobehandlung.

Risiko-ID	Asset	Bedrohung	Schwachstelle	Wahrschein-lichkeit	Auswirkung	Risiko	Maßnahme	Verantwortlich	Status
R-01	Kundenplattform	Unbefugter Zugriff	Schwache Passwortrichtlinien	Mittel	Hoch	Hoch	Einführung MFA	IT-Security	In Umsetzung
R-02	Cloud-Datenbank	Datenverlust	Fehlende Backup-Tests	Niedrig	Hoch	Mittel	Regelmäßige Backup-Tests	IT-Betrieb	Offen
R-03	E-Mail-System	Phishing-Angriff	Geringe Awareness	Hoch	Mittel	Hoch	Awareness-Training	HR / Security	Geplant
R-04	Webserver	Malware-Infektion	Fehlende Updates	Mittel	Hoch	Hoch	Patch-Management	IT-Betrieb	In Umsetzung
R-05	Entwicklungsumgebung	Datenleak	Fehlende Zugriffsbeschränkung	Niedrig	Hoch	Mittel	Zugriffskontrolle	DevOps	Offen

Beispiel für ein Risk Register.

Das Risk Register ermöglicht eine transparente Übersicht über alle identifizierten Risiken im ISMS. Sicherheitsverantwortliche können so erkennen, welche Risiken besonders kritisch sind und welche Maßnahmen priorisiert umgesetzt werden müssen. Gleichzeitig dient das Dokument als wichtiger Nachweis im Rahmen interner Audits oder externer Zertifizierungsaudits nach ISO/IEC 27001.

Für die Bewertung der Risiken werden häufig einfache Bewertungsmodelle verwendet, bei denen Eintrittswahrscheinlichkeit und Auswirkungen in Kategorien wie niedrig, mittel und hoch eingeteilt werden. Die Kombination dieser Faktoren ergibt eine Risikobewertung, auf deren Grundlage geeignete Maßnahmen definiert werden.

Das Risk Register ist kein statisches Dokument und muss regelmäßig aktualisiert werden. Veränderungen der IT-Infrastruktur, neue Bedrohungsszenarien oder organisatorische Änderungen können dazu führen, dass bestehende Risiken neu bewertet oder zusätzliche Risiken identifiziert werden müssen.

Ein gepflegtes Risk Register schafft Transparenz über Informationssicherheitsrisiken und unterstützt fundierte Entscheidungen im Risikomanagement. Es bildet damit eine zentrale Grundlage für ein wirksames Informationssicherheitsmanagementsystem.

Mehr zum Thema ISMS

Der vollständige Leitfaden „ISMS erfolgreich implementieren – Klappentext: Praxisleitfaden für Unternehmen nach ISO/IEC 27001“

🛒 Jetzt bei Amazon bestellen