



# Checkliste: Ihr Weg zur ISO 27001

# Ihre ISO 27001 Roadmap

ISO 27001 ist der globale Goldstandard für Informationssicherheit.

Mit einer Zertifizierung nach ISO 27001 beweisen Sie Kunden und Partnern die Robustheit Ihrer Sicherheitspraktiken – und das weltweit.

Unsere ISO 27001-Checkliste hilft Ihrem Unternehmen bei der erfolgreichen Implementierung eines Informationssicherheits-Managementsystems (ISMS) gemäß der ISO-Norm.

## Schritt 1

### **Projektplan, Anwendungsbereich und Governance-Struktur**

- Projektteam zusammenstellen und Rollen sowie Verantwortlichkeiten definieren.
- ISMS-Anwendungsbereich („Scope“) festlegen und dokumentieren.
- Governance-Struktur etablieren, inklusive der Rollen des Top-Managements.

## Schritt 2

### **Strategie und Erfassen der Vermögenswerte**

- Informationssicherheitsziele und -strategie formulieren.
- Asset-Management-Prozess definieren und ein Asset-Register erstellen.
- Klassifizierungsschema für Informationen und Assets festlegen.

### Schritt 3

## Generierung von Richtlinien

- ISMS-Richtlinien, Prozesse und Verfahren gemäß ISO 27001 entwickeln.
- Dokumentationsrahmen aufbauen und Verwaltungsprozess für Dokumente etablieren.
- Dokumentierte Verfahren für regelmäßige Reviews und Updates einrichten.

### Schritt 4

## Risikomanagement durchführen

- Risikomanagement-Verfahren und -Kriterien für Risikobewertung und -behandlung definieren.
- Risikoidentifikation durchführen und Risikoregister erstellen.
- Risikoanalyse und -bewertung vornehmen und Behandlungspläne erarbeiten.

### Schritt 5

## Management und KPI-Überprüfung

- Festlegen von Key Performance Indicators (KPIs) für das ISMS.
- Durchführung von Managementbewertungen zur Überprüfung der ISMS-Leistung.

### Schritt 6

## Internes Audit

- Entwickeln des internen Auditprogramms gemäß ISO 27001 Anforderungen.
- Auswahl und Schulung interner Auditoren oder Beauftragung externer Auditoren.
- Durchführen von Audits für alle Elemente des ISMS, um Konformität und Effektivität zu prüfen.

### Schritt 7

## Nachbesserung

- Review der Audit-Ergebnisse
- Entwicklung und Umsetzung von Korrekturmaßnahmen zur Adressierung identifizierter Nonkonformitäten.
- Überprüfung der Wirksamkeit der Korrekturmaßnahmen.

### Schritt 8

## Vorbereitung auf Zertifizierungsaudit

- Auswahl eines akkreditierten Zertifizierungsauditors.
- Letzte Nachbesserungen durchführen.
- Organisation auf das vor-Ort Audit vorbereiten.

## Schritt 9

### ISO 27001 Zertifizierungsaudit

- Stage 1 Audit durchführen – Dokumentenprüfung.
- Stage 2 Audit durchführen – Detaillierte Prüfung Ihres ISMS und dessen Wirksamkeit bei Ihnen vor Ort.

## Schritt 10

### Regelbetrieb des ISMS

- Nebenabweichungen des Zertifizierungsaudits beheben.
- ISMS-Dokumentation auf dem neuesten Stand halten.
- Jährliche Überwachungsaudits durchführen.

## Schritt 11

### SECJUR Demo vereinbaren

- Automatisieren Sie die Erstellung und Verwaltung Ihres ISMS mit SECJUR.

## Der bequeme Weg zur ISO 27001

Mit der SECJUR Automatisierungsplattform und unseren TÜV-zertifizierten Experten, bauen Sie Ihr ISMS nach ISO 27001 mühelos und in Rekordzeit – und das ohne jegliches Vorwissen.

[Mehr erfahren](#)



Für eine Welt, in der Unternehmen immer compliant sind, aber nie an Compliance denken müssen.

[secjur.com](https://secjur.com)

[info@secjur.com](mailto:info@secjur.com)