

## DER ROTE FADEN

# 10 Schritte zur Implementierung eines ISMS nach ISO 27001



# Einführung

Die ISO 27001-Zertifizierung gilt weltweit als einer der wichtigsten Standards für Informationssicherheit. Ganz gleich, ob Sie ein kleines Unternehmen oder ein großer Konzern sind – immer mehr Organisationen setzen auf diese Zertifizierung. Warum? Weil sie das Vertrauen Ihrer Stakeholder in Ihre Cybersicherheitsmaßnahmen stärkt – und immer öfter eine Voraussetzung bei Ausschreibungen ist.

Vielleicht stehen auch Sie gerade vor der Entscheidung, sich nach ISO 27001 zertifizieren zu lassen – wissen aber noch nicht genau, wie Sie starten sollen? Das ist keine Seltenheit. Viele unserer Kunden kommen mit genau dieser Frage auf uns zu. Häufig geben die Anforderungen ihrer eigenen Kunden den Anstoß, um weiterhin erfolgreich zusammenarbeiten zu können. Mit diesem Leitfaden zeigen wir Ihnen in zehn klaren Schritten, wie Sie die ISO 27001-Zertifizierung erfolgreich umsetzen. Ganz praktisch und direkt anwendbar.

# 1. Projektdurchführung

## Warum zertifizieren? Wer sind die Projekttreiber?

Die Zertifizierung eines Managementsystems erfordert erhebliche Ressourcen und Anstrengungen, nicht nur für den Aufbau und die Implementierung, sondern auch für den langfristigen Betrieb und die Pflege des Systems. Die Gründe für eine Zertifizierung können vielfältig sein. Wir unterscheiden hier nach internem und externem Bedarf.

### **Interner Bedarf:**

- Verbesserung der Arbeitsmethoden
- Reduktion von Geschäftsrisiken
- Minimierung von Mängeln oder Vorfällen, die den Ruf des Unternehmens schädigen könnten
- Schaffung interner Anerkennung

### **Externer Bedarf:**

- Vertragsanforderungen von Kunden, die ISO 27001 verlangen
- Schutz vor zunehmender Cyberkriminalität

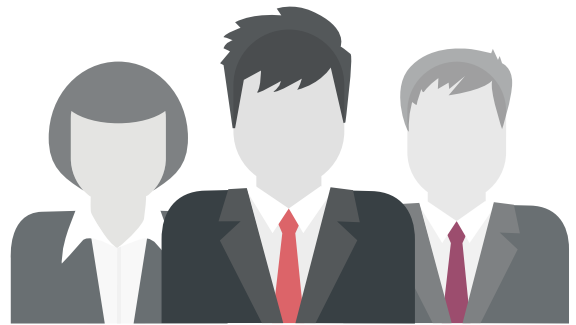
Viele Unternehmen denken über eine ISO-Zertifizierung nach, weil vertragliche Anforderungen oder Kundenerwartungen sie dazu drängen. Dabei lohnt sich der Blick über die reine Erfüllung solcher Pflichten hinaus: Wer die Anforderungen einer ISO-Norm wirklich in die eigenen Prozesse integriert, profitiert von mehr Struktur, Transparenz und Sicherheit im gesamten Unternehmen.

Gerade angesichts der wachsenden Bedrohung durch Cyber-Kriminalität ist das ein entscheidender Faktor. Angriffe werden immer gezielter und professioneller – sensible Daten von Kunden und Mitarbeitenden zu schützen, ist heute wichtiger denn je. Auch ohne Zertifizierung lassen sich Prozesse natürlich an Normvorgaben ausrichten. Doch wer sich gegen den offiziellen Nachweis entscheidet, verzichtet auf wichtige Vorteile – etwa bei Ausschreibungen oder gegenüber potenziellen Geschäftspartnern, die zunehmend auf zertifizierte Sicherheit setzen.

## Einbindung der Geschäftsführung

Ein entscheidender erster Schritt: Sichern Sie sich die Unterstützung Ihrer Führungsebene.

Ohne deren Engagement und die nötigen Ressourcen wird es schwer, ein Information Security Management System (ISMS) erfolgreich aufzubauen und dauerhaft zu betreiben. Binden Sie Ihr Management deshalb von Anfang an aktiv ein – das ist die Grundlage für den späteren Erfolg.



„Wenn die Führungsebene nicht hinter der ISO-Zertifizierung und dem ISMS steht, wird das Projekt scheitern – egal wie gut das Konzept ist.“

Eine erfolgreiche Umsetzung eines Informationssicherheits-Management-systems nach ISO 27001 erfordert mehr als nur technische Maßnahmen und saubere Dokumentation. Ohne echtes Commitment und aktives Mitwirken der Verantwortlichen – besonders im Management – bleibt das ISMS ein Papiertiger. Erst wenn Sicherheitskultur als strategisches Ziel verstanden wird, kann eine Zertifizierung nachhaltigen Mehrwert bringen.

Das bedeutet auch: Informationssicherheit darf kein reines IT-Projekt sein. Sie ist eine gemeinsame Aufgabe – und beginnt mit der Überzeugung, dass Sicherheit ein zentraler Erfolgsfaktor für das Unternehmen ist.

## Entwicklung eines Projektplans

Wie bei jedem großen Projekt ist ein gut durchdachter Plan unerlässlich. Der Plan sollte klare Aufgaben und Verantwortlichkeiten festlegen sowie Zeitpläne und Meilensteine definieren. Eine Person sollte mit der Planung und Koordination der ISO 27001-Implementierung beauftragt werden.

## Einrichtung einer Lenkungsgruppe

Die Zusammensetzung und Größe der Lenkungsgruppe hängt stark von der Organisationsstruktur und dem Einflussbereich des ISMS ab. Ziel sollte es sein, regelmäßige Treffen zu etablieren, um die Umsetzung des ISMS-Plans kontinuierlich zu überwachen und gezielt weiterzuentwickeln.

Wichtig ist, dass alle relevanten Bereiche vertreten sind – insbesondere Entscheidungsträgerinnen und Entscheidungsträger, die Verantwortung für folgende Themen tragen:

- Entwicklung von Strategien, Verfahren sowie ISMS-Zielen und -Plänen
- Freigabe und Steuerung von Budgets
- Bewertung von Risiken und Auswahl geeigneter Maßnahmen
- Verteilung und Nachverfolgung von Aufgaben

Zentral für den Erfolg ist außerdem eine Sponsorin oder ein Sponsor auf Führungsebene, der/die das ISMS intern vertritt und den Betrieb auf strategischer Ebene unterstützt und vorantreibt.

## Kommunikation ist entscheidend

Es ist von großer Bedeutung, dass alle Mitarbeiterinnen und Mitarbeiter verstehen, warum die Zertifizierung angestrebt wird und dass die Unternehmensleitung das Projekt unterstützt. Eine klare und regelmäßige Kommunikation hilft, das Bewusstsein und die Akzeptanz im gesamten Unternehmen zu fördern.

## Durchführung einer ersten Lückenanalyse

Eine Lückenanalyse hilft dabei, den aktuellen Stand der Konformität mit ISO 27001 zu bewerten. Dies ermöglicht es, die notwendigen Maßnahmen zu identifizieren und den Aufwand für die Zertifizierung abzuschätzen. Regelmäßige Wiederholungen der Lückenanalyse während des Projekts zeigen den Fortschritt und helfen bei der Priorisierung von Aufgaben.

## 2. Umfang, Kontext und interessierte Kreise

### Festlegung des ISMS-Umfangs

Bestimmen Sie, welche Teile der Organisation und welche Prozesse in den Geltungsbereich des ISMS fallen. Dies ist ein kritischer Schritt, da er alle weiteren Aktivitäten beeinflusst. Der Umfang sollte klar dokumentiert und kommuniziert werden.

### Identifikation interessierter Parteien

Die ISO 27001 fordert, dass alle interessierten Parteien identifiziert und berücksichtigt werden, die in irgendeiner Weise relevant für das Informationssicherheits-Managementsystem (ISMS) sind. Doch wer zählt dazu?

#### Typischerweise gehören dazu:

- **Kunden:** Sie stellen häufig vertragliche Anforderungen an Produkte, Dienstleistungen oder Sicherheitsstandards, die direkt in das ISMS einfließen müssen.
- **Behördliche und gesetzliche Stellen:** Ob lokal, regional oder national – gesetzliche Vorgaben beeinflussen maßgeblich, welche Verfahren und Kontrollen Sie implementieren müssen.
- **Zulieferer und Dienstleister:** ISO 27001 legt besonderen Fokus auf die sichere Zusammenarbeit mit externen Partnern. Dabei geht es unter anderem um den Schutz sensibler Informationen und die Kontrolle von Zugriffsrechten – physisch wie digital.

Nehmen Sie sich Zeit, um sowohl interne als auch externe Stakeholder zu identifizieren, die Einfluss auf Ihr ISMS und dessen Wirksamkeit haben können. Verstehen Sie, welche Erwartungen oder Anforderungen sie mitbringen – und überlegen Sie, wie Sie diese durch geeignete Richtlinien, Prozesse und Sicherheitsmaßnahmen adressieren können. Denn: Die Interessen dieser Gruppen können nicht nur Anforderungen mit sich bringen, sondern auch Risiken, die aktiv erkannt und gemanagt werden müssen.

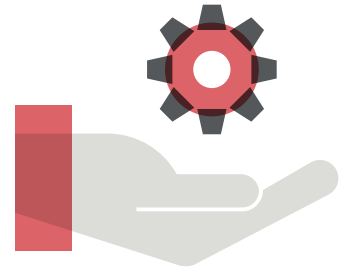
### Dokumentation des Umfangs

Die festgelegten Grenzen des ISMS sollten klar dokumentiert werden, um der Zertifizierungsstelle (RCB) zu zeigen, wo das ISMS beginnt und endet. Dies wird in der sogenannten Statement of Applicability (SoA) hinterlegt.

# 3. Politik, Rollen und Verantwortlichkeiten

## Definition von Rollen und Verantwortlichkeiten

Für ein funktionierendes ISMS braucht es klare Verantwortlichkeiten. Die folgenden Rollen sind zentral für Planung, Umsetzung und Überwachung – je nach Unternehmensgröße können Aufgaben zusammen gefasst oder verteilt werden:



- **Lenkungsgruppe für Informationssicherheit** (siehe Schritt 1): Dieses Gremium begleitet das ISMS auf strategischer Ebene und trifft grundlegende Entscheidungen.
- **Informationssicherheitsmanager** – oft auch als Chief Information Security Officer (CISO) bezeichnet – ist die zentrale Ansprechperson für alle Fragen rund um Informationssicherheit und koordiniert die Umsetzung im Unternehmen.
- **Eigentümer von Informationswerten** tragen die operative Verantwortung für spezifische Informationsgüter, wie sie in der Inventarisierung festgelegt sind.
- **Verantwortliche für Informationssicherheitsrisiken** sind dafür zuständig, definierte Risiken aktiv zu managen – wie im Risikomanagement der Organisation beschrieben.
- **Informationssicherheitsauditoren** übernehmen interne Audits gemäß ISO/IEC 27001 und stellen sicher, dass das ISMS wirksam umgesetzt und kontinuierlich weiterentwickelt wird.
- **Weitere Rollen mit Sicherheitsverantwortung**, z. B.:
  - Abteilungsleiterinnen und Abteilungsleiter
  - IT-Fachkräfte
  - Anwenderinnen und Anwender

Alle Beteiligten leisten ihren Beitrag zur Informationssicherheit – abgestimmt auf ihre jeweilige Rolle und Verantwortung im Unternehmen.

## Erstellung eines Organigramms

Ein Organigramm hilft dabei, die Berichtslinien und Verantwortlichkeiten aller Beteiligten zu visualisieren.

## ISMS-Verantwortungsmatrix

Eine RACI-Tabelle (Responsible, Accountable, Consulted, Informed) kann verwendet werden, um die Verantwortlichkeiten für verschiedene Bereiche der ISO 27001-Norm festzulegen. Diese definiert die Art der Verantwortung jeder Rolle in jedem Bereich, je nachdem, ob die aufgeführte Rolle verantwortlich, rechenschaftspflichtig, konsultiert oder informiert ist.

## 4. Risiko, Chancen und Sicherheit

### Entwicklung eines Risikomanagementprozesses

Bevor Sie mit der eigentlichen Risikobewertung beginnen, sollten Sie zunächst klären, **welchen Risikobewertungsprozess** Sie in Ihrer Organisation anwenden möchten. Es gibt verschiedene Methoden und Vorgehensweisen – entscheidend ist, dass Sie einen Ansatz wählen, der zu Ihrem Unternehmen passt, praktikabel ist und Sie dabei unterstützt, Risiken, deren Auswirkungen und passende Maßnahmen klar und effizient zu erfassen.

#### **Folgende Fragen sollten Sie dabei berücksichtigen:**

- **Welche Methode möchten Sie verwenden?**

Zum Beispiel:

- Qualitative Risikobewertung (Empfohlen): Diese Methode ist eher subjektiv und basiert auf Einschätzungen hinsichtlich der Eintrittswahrscheinlichkeit und der Auswirkungen eines Risikos – in der Regel auf einer Skala, etwa von 1 bis 5.
- Quantitative Risikobewertung: Hier arbeiten Sie mit messbaren, überprüfbaren Daten, um Risiken exakt zu analysieren (z. B. „Risiko A hat eine Eintrittswahrscheinlichkeit von 4/10, also 40 %“).
- Allgemeine Risikobewertung: Ein eher veralteter Ansatz, bei dem Gefahren identifiziert und geeignete Maßnahmen festgelegt werden. Ursprünglich im Bereich Arbeitssicherheit verbreitet, lässt er sich auch auf Informationssicherheit übertragen, wenn Risiken als potenziell schädlich für Ihre Systeme und Prozesse gelten.

- **Welche Dokumente, Vorlagen oder Tools benötigen Sie, um den gewählten Ansatz effizient umzusetzen?**

- **Verfügt Ihr Team über die notwendigen Fähigkeiten und Kenntnisse, um eine fundierte Risikobewertung durchzuführen?**

Gerade bei der strukturierten Umsetzung und kontinuierlichen Pflege eines Risikoprozesses kann ein spezialisiertes Tool wie GRASP sinnvoll unterstützen. Es hilft dabei, Bewertungen transparent zu dokumentieren, Risiken nachvollziehbar zu steuern und Verantwortlichkeiten klar zuzuordnen – ohne dass Sie alles manuell verwalten müssen.



**Wichtig ist: Ihr Risikoprozess sollte nicht nur Risiken identifizieren, sondern auch helfen, diese wirksam zu bewerten und gezielt zu steuern – und das so einfach und effektiv wie möglich.**

## Identifikation organisatorischer Vermögenswerte

Dieser Aspekt ist ein zentraler Bestandteil der ISO 27001-Norm und spielt eine entscheidende Rolle bei der Beantwortung wichtiger Fragen rund um den Schutz von Unternehmenswerten:

- Welche Vermögenswerte besitzt Ihr Unternehmen – sowohl physischer als auch digitaler Natur – und wie können diese wirksam vor Verlust, Diebstahl oder gezielten Angriffen geschützt werden? Besonders im Offboarding-Prozess von Mitarbeiterinnen und Mitarbeitern ist es essenziell sicherzustellen, dass alle überlassenen Ressourcen und Geräte ordnungsgemäß zurückgegeben werden. Diese können in GRASP z.B. leicht und übersichtlich in der Inventarisierung hinterlegt werden.
- Welche Informationswerte gelten als besonders schützenswert, weil sie große Auswirkungen auf die Informationssicherheit haben? Diese „kritischen Informationsbestände“ müssen klar identifiziert und mit entsprechenden Schutzmaßnahmen versehen werden, da sie oft ein lohnendes Ziel für Angriffe darstellen.

Ein strukturiertes Asset- und Informationswertmanagement schafft die Grundlage dafür, Risiken gezielt zu minimieren und den Überblick über alle sicherheitsrelevanten Güter zu behalten – auch im Hinblick auf Verantwortlichkeiten und den Lebenszyklus einzelner Werte.

## Bewertung der Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit (ViV)

Analysieren Sie, wie sich der Verlust oder die Beeinträchtigung von Vermögenswerten auf die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen auswirken würde. Hilfreich sind hier Tools, die eine automatische Vererbung von Schutzbedarfen basieren auf Abhängigkeiten zwischen den Assets beinhalten. GRASP bietet eine solche Möglichkeit.

## Festlegung der Risikobereitschaft

Bestimmen Sie, welche Risiken akzeptabel sind und welche Maßnahmen zur Risikominderung ergriffen werden müssen.

## Risiken bewerten und gezielt behandeln

Ein zentrales Element eines ISO 27001-konformen Managementsystems ist die systematische **Risikobewertung und -behandlung**. Ziel ist es, zu erkennen, welche Maßnahmen erforderlich sind, um Ihre Informationswerte wirksam vor potenziellen Bedrohungen zu schützen – sei es durch externe Angreifer oder durch Schwachstellen innerhalb der eigenen Organisation.

Diese Schutzmaßnahmen werden im Rahmen der Norm als „**Kontrollen**“ bezeichnet. Die ISO 27001 führt in **Anhang A** eine umfassende Liste solcher Referenzkontrollen auf, die als Orientierung dienen können. Dabei ist nicht jede Kontrolle automatisch für jedes Unternehmen relevant – deshalb ist es erforderlich, im Rahmen der sogenannten **Erklärung zur Anwendbarkeit (Statement of Applicability)** genau zu dokumentieren, **welche Kontrollen für Ihre Organisation sinnvoll und notwendig sind** und welche nicht – mit nachvollziehbarer Begründung.

Diese Erklärung zählt zu den wichtigsten Dokumenten bei einem Audit und schafft Transparenz darüber, wie Sie Risiken steuern und welche Sicherheitsmaßnahmen Sie bewusst umgesetzt haben.



## Risikobehandlung

Sobald alle identifizierten Risiken erfasst und bewertet wurden, folgt der nächste Schritt: **die Auswahl passender Maßnahmen**, um diese Risiken zu minimieren oder zu kontrollieren. Dafür greifen Sie auf den Kontrollkatalog aus **Anhang A der ISO 27001** zurück und wählen gezielt diejenigen Kontrollen aus, die zu Ihrer Risikolage passen.

Dabei spielt auch Ihre **individuelle Risikobereitschaft** eine zentrale Rolle – sie beeinflusst, welche Risiken Sie in welchem Umfang akzeptieren und welche **Behandlungsoptionen Sie priorisieren**. So entsteht ein risikobasierter Maßnahmenplan, der genau auf die Bedürfnisse und Sicherheitsziele Ihrer Organisation zugeschnitten ist.



## Genehmigung und Finanzierung von Risikoplänen

Nachdem Sie geeignete **Maßnahmen zur Risikobehandlung** ausgewählt haben, müssen diese auch intern genehmigt und mit den notwendigen Ressourcen ausgestattet werden. Präsentieren Sie den Maßnahmenplan der Geschäftsführung oder dem verantwortlichen Gremium – idealerweise mit einer Bewertung zu Kosten, Wirksamkeit und Dringlichkeit. Priorisieren Sie die Maßnahmen anhand der Risikobewertung und klären Sie, welche Investitionen notwendig sind. Planen Sie dabei auch personelle und technische Ressourcen ein. Nur mit einer abgestimmten Finanzierung und klarer Freigabe können die Maßnahmen effizient umgesetzt werden und ihren vollen Nutzen entfalten.

## Festlegung von Informationssicherheitszielen

Die Festlegung von Informationssicherheitszielen ist entscheidend, um die Implementierung der ISO 27001 gezielt voranzutreiben. Zu Beginn der Einführung eines ISMS konzentrieren sich viele dieser Ziele auf das Erreichen der Zertifizierung und andere wichtige Faktoren für ein erfolgreiches Ergebnis. Allerdings sollten die Ziele eine dynamische, regelmäßig gepflegte Liste darstellen, die sich mit der Zeit weiterentwickelt.

Im Kontext des ISMS gibt es zwei Hauptarten von Zielen: Auf der ersten Ebene stehen die übergeordneten Ziele, die bei der Festlegung des ISMS-Kontexts definiert werden. Auf der zweiten Ebene befinden sich eher praktische, handlungsorientierte Ziele, die an einen bestimmten Zeitrahmen gebunden sind.

Dabei handelt es sich meist um konkrete Ziele, die für ein bestimmtes Geschäftsjahr festgelegt werden, die aufgrund der Anforderungen der Stakeholder zeitlich variieren oder Sicherheitsvorfälle bzw. Verbesserungen betreffen, die innerhalb eines festgelegten Zeitraums angegangen werden müssen. Ein Ziel könnte z.B. die Verbesserung der Passwortsicherheit innerhalb der Organisation sein.



## Beispiel: Passwort-Initiative

Bis zum Ende des nächsten Quartals sollen **100 % der Mitarbeitenden** starke Passwörter gemäß den Unternehmensrichtlinien verwenden.

**Maßnahmen:** Einführung einer Passwortrichtlinie mit Mindestanforderungen (z. B. Länge, Komplexität, regelmäßige Änderung)

**Technische Umsetzung:** Erzwingen der Richtlinie über Active Directory oder ein IAM-System

**Mitarbeiterschulung:** Zur sicheren Passwortverwendung

**Überprüfung & Monitoring:** Quartalsweise Kontrolle der Einhaltung durch interne Audits

**Messbare Erfolgsindikatoren:**

- **100 % der Mitarbeitenden** haben ein konformes Passwort
- **0 Sicherheitsverstöße** aufgrund schwacher Passwörter in den letzten drei Monaten
- **Erfolgreiche Audit-Prüfung** ohne Abweichungen

## 5. Kompetenz und Bewusstsein



### Dokumentation von Rollen und Verantwortlichkeiten

Stellen Sie sicher, dass alle Rollen und Verantwortlichkeiten im Rahmen des ISMS klar definiert und dokumentiert sind. In Tools wie GRASP lassen sich Regelungsdokumente abspeichern und den entsprechenden Bereichen zuordnen, so dass diese im Falle eines Audits schnell auffindbar sind.

### Schulung und Entwicklung

Die Norm fordert lediglich, dass ausreichende Ressourcen bereitgestellt werden, damit das ISMS wirksam betrieben werden kann. Das bedeutet, dass die Unternehmensleitung bewerten muss, welche internen Ressourcen zur Verfügung stehen, um die notwendigen Aufgaben zur Unterstützung des ISMS zu erfüllen – und ob es Lücken gibt, die geschlossen werden müssen.

Dabei erfordern manche Aufgabenbereiche eine gezielte Schulung, um die Anforderungen der ISO27001 und deren Auslegung zu verstehen. Andere hingegen benötigen lediglich ein grundlegendes Bewusstsein für die relevanten Richtlinien und Prozesse, die eingehalten werden müssen.

### Förderung eines kontinuierlichen Bewusstseins

Stellen Sie sicher, dass alle Mitarbeitenden regelmäßig über den Stand und die Fortschritte des ISMS-Entwicklungsprogramms informiert werden. Noch wichtiger ist es, das Bewusstsein für zentrale Informationssicherheitsthemen zu stärken – speziell für jene, die im Unternehmensalltag relevant sind. Dazu zählen unter anderem Schulungen zu Richtlinien, Risiken, Sicherheitsmaßnahmen, allgemeinem Sicherheitsbewusstsein sowie Einführungsformate für neue Kolleginnen und Kollegen.

### Kommunikationsprotokolle

Erstellen Sie einen klaren Kommunikationsplan, aus dem hervorgeht, welche Kommunikationskanäle zur Verfügung stehen, wer für die jeweiligen Inhalte verantwortlich ist und auf welche Weise Informationen im Rahmen des ISMS effektiv weitergegeben werden sollen.

## 6. Dokumentierte Informationen

### Dokumentenreferenzierung

Alle ISMS-Dokumente sollten eindeutig nummeriert und referenziert werden, um eine einfache Identifikation zu gewährleisten.

### Dokumentenmanagement

Die ordnungsgemäße Steuerung Ihrer ISMS-Richtlinien, -Verfahren und -Dokumente ist eine zentrale Anforderung jeder Managementsystemnorm. Sie sollten sicherstellen, dass definierte und dokumentierte Verfahren zur Dokumentenkontrolle vorhanden sind, die den gesamten Lebenszyklus der dokumentierten Informationen abdecken.

Auch Aufzeichnungen müssen dabei berücksichtigt werden. Ihr Lebenszyklus sollte klar definiert sein – einschließlich der Methoden zur Identifikation, Speicherung, zum Schutz, Abruf, zur Aufbewahrung und zur ordnungsgemäßen Entsorgung.

„Die sorgfältige Dokumentenkontrolle ist eine grundlegende Voraussetzung für ein funktionierendes Informationssicherheitsmanagementsystem.“

### Erstellung von Richtlinien und Verfahren

In diesem Schritt erstellen Sie alle relevanten Grundsatzdokumente sowie weitere unterstützende Unterlagen, die später Teil Ihres ISMS sein werden. Es ist sinnvoll, sich frühzeitig Gedanken darüber zu machen, wie Sie die ISMS-Dokumente strukturieren und kontrollieren möchten.

Abhängig von der Größe und Komplexität Ihrer Organisation kann der Umfang der benötigten Dokumente variieren. Das hat direkten Einfluss auf die Entscheidung, wie Sie die Verwaltung und Kontrolle dieser Dokumente gestalten – sei es über eine einfache Ordnerstruktur im Netzwerk oder mithilfe von Tools wie SharePoint oder spezialisierten ISMS-Managementlösungen.

# 7. Operativer Betrieb

## Planungsprozesse

In dieser Phase müssen Sie die Kontrollen aus Anhang A identifizieren, die auf spezifische Risiken angewendet werden sollen. Zudem gilt es festzulegen, welche dieser Kontrollen die Entwicklung neuer ISMS-Richtlinien, -Prozesse oder -Verfahren notwendig machen.

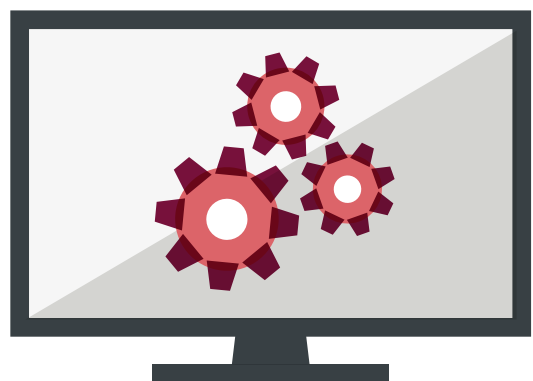
## Durchführung von Maßnahmen

Die Norm fordert von Ihnen, zu analysieren, wie externe und interne Faktoren die Fähigkeit Ihres Unternehmens beeinflussen können, die angestrebten Ziele des Informationssicherheitsmanagementsystems zu erreichen. Viele dieser Faktoren lassen sich im Rahmen der Risikobewertung erfassen, es können jedoch auch weitere Aspekte relevant sein, die zusätzlich berücksichtigt werden sollten.

Auch die Bedürfnisse und Erwartungen relevanter Interessengruppen wirken sich auf das ISMS aus – ebenso wie die identifizierten Risiken und deren Behandlung.

## Überprüfung der Risikobewertung

Die Organisation muss im Rahmen ihrer Risikopolitik und ihrer Verfahren festlegen, in welchen Abständen Risikobewertungen sowie der zugehörige Behandlungsplan überprüft werden. Ebenso ist sicherzustellen, dass der Fortschritt von Abhilfemaßnahmen und die Wirksamkeit der umgesetzten Kontrollen regelmäßig überwacht wird.



# 8. Leistungsbewertung

## Interne Audits

Die Aufrechterhaltung der Prozesskonformität und die kontinuierliche Verbesserung sind zentrale Elemente eines erfolgreichen ISMS. Nachdem Sie Zeit, Engagement und finanzielle Mittel in die ISO-Zertifizierung investiert haben, besteht eine der größten Herausforderungen darin, dieses Niveau dauerhaft zu sichern. Interne Audits sind ein wirkungsvolles Instrument, um sicherzustellen, dass die festgelegten Prozesse weiterhin korrekt umgesetzt werden und Anpassungen widerspiegeln, die etwa durch neue Technologien, geänderte Geschäftsabläufe oder personelle Veränderungen notwendig wurden.

Bereits in der Umsetzungsphase sollte ein umfassendes Auditprogramm entwickelt werden, das alle Anforderungen der Norm sowie alle Richtlinien, Prozesse und Verfahren im Geltungsbereich abdeckt. Diese müssen nachweislich intern geprüft worden sein, bevor Sie Ihr Zertifizierungsaudit durch die ausgewählte Zertifizierungsstelle (RCB) durchführen lassen können.

Die internen Audits können entweder von qualifizierten Mitarbeitenden innerhalb Ihrer Organisation oder durch externe Dienstleister durchgeführt werden. Ein zusätzliches internes Vorzertifizierungsaudit kann sinnvoll sein, um zu prüfen, ob Sie bereit für die formale Zertifizierung sind und ob es noch Lücken bei der Normerfüllung gibt.

### Ein interner Auditprozess sollte unter anderem folgende Schritte umfassen:

- Schulung der internen Auditoren
- Erstellung eines internen Auditplans
- Durchführung und Abschluss der internen Audits

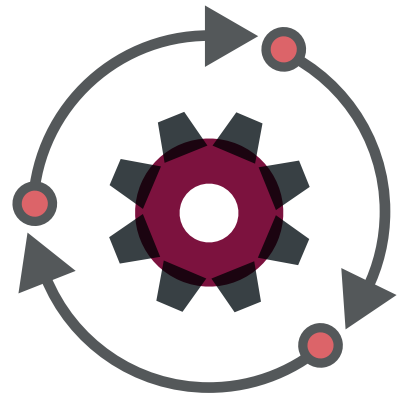
Dabei sollten die internen Audits eine sorgfältige und systematische Überprüfung der Unternehmensprozesse sicherstellen.

## Überprüfung der Ziele

In dieser Phase Ihres Umsetzungsprogramms ist es entscheidend, die Ziele der ISO 27001-Norm nochmals zu überprüfen, zu bekräftigen und bei Bedarf anzupassen. Gleichzeitig sollten die Fortschritte bei der Zielerreichung regelmäßig aktualisiert und nachvollziehbar dokumentiert werden.

## Management-Review

Falls Sie noch kein Management-Review-Meeting durchgeführt haben, sollten Sie unbedingt – idealerweise sogar mehrere – vor dem Zertifizierungsaudit einplanen. Diese Bewertungen sind ein zentraler Bestandteil der ISO 27001-Zertifizierung und tragen wesentlich zur kontinuierlichen Verbesserung des ISMS bei.



### **Achten Sie dabei auf folgende Punkte:**

- Die Managementbewertung muss mindestens die Anforderungen aus Abschnitt 9.3 der Norm abdecken, insbesondere die Unterpunkte 9.3a bis 9.3f.
- Wichtige Interessengruppen sollten aktiv in die Bewertung einbezogen werden und die oberste Führungsebene sollte an der Sitzung teilnehmen oder zumindest auf der Tagesordnung berücksichtigt werden.
- Stellen Sie sicher, dass das Protokoll der Sitzung sowie alle beschlossenen Maßnahmen sorgfältig dokumentiert und aufbewahrt werden.

### **Zu den Inhalten der Managementbewertung gehören unter anderem:**

- Durchführung eines Management-Review-Meetings
- Identifikation und Analyse von ISMS-Nichtkonformitäten
- Entwicklung eines konkreten Maßnahmenplans zur Behebung dieser Abweichungen

Die regelmäßige Durchführung von Managementbewertungen stärkt die Wirksamkeit des ISMS und ist eine wesentliche Voraussetzung für eine erfolgreiche Zertifizierung nach ISO 27001.

## Korrekturmaßnahmen

Nichtkonformitäten und die daraus resultierenden Korrekturmaßnahmen können unterschiedliche Ursachen haben, wie zum Beispiel:

- Ergebnisse interner Audits
- Sicherheitsvorfälle
- Rückmeldungen von externen Kunden oder anderen interessierten Parteien
- Vorschläge und Hinweise aus dem eigenen Team
- Erkenntnisse aus Management Reviews und weiteren internen Überprüfungen

Stellen Sie sicher, dass Sie über klare Verfahren und geeignete Mechanismen verfügen, um Nichtkonformitäten sowie die dazugehörigen Korrekturmaßnahmen systematisch zu erfassen und nachzuverfolgen. Diese Aufzeichnungen zählen zu den zentralen Nachweisen, die im Rahmen der Anforderungen des Managementsystems verpflichtend sind.

# 9. Pläne und Maßnahmen zur Defizitbewertung

- **Aktualisierung der Lückenanalyse**

Stellen Sie sicher, dass die ursprünglich durchgeführte Lückenanalyse für alle bewerteten Bereiche des Standards möglichst vollständig abgeschlossen ist – idealerweise mit 100 % Abdeckung.

- **Verantwortlichkeiten zuweisen**

Alle identifizierten Maßnahmen im Rahmen der Defizitanalyse sollten klar verantwortlichen Personen zugewiesen werden. Diese Personen müssen über die nötige Kompetenz verfügen, um die Aufgaben erfolgreich umzusetzen.

- **Offene Maßnahmen adressieren**

Prüfen Sie, ob alle identifizierten Maßnahmen aus der Lückenanalyse angegangen und abgeschlossen wurden. Überzeugen Sie sich zudem, dass alle daraus entstandenen neuen ISMS-Richtlinien und -Verfahren fertiggestellt und vollständig im ISMS-Repository hinterlegt sind.

- **Fortschritt des Implementierungsplans**

Die Person, die die ISO27001-Einführung verantwortet, sollte regelmäßig den aktuellen Stand des Implementierungsplans sowie den Fortschritt aller offenen Maßnahmen der Lückenanalyse überprüfen. Hindernisse oder Probleme, die den Projektfortschritt gefährden, sollten zeitnah mit der Lenkungsgruppe und – falls nötig – mit dem Executive Sponsor besprochen werden.

- **Veröffentlichung obligatorischer Verfahren**

Die ISO27001-Norm verlangt bestimmte Verfahren, darunter z. B. die Anwendbarkeitserklärung und die Vermögensinventarisierung. Alle vorgeschriebenen Verfahren sollten veröffentlicht sein – so wenige wie möglich sollten sich zum Zeitpunkt des Stage-1-Audits noch im Entwurfsstatus befinden.

- **Überprüfung der Defizitbewertung**

Gehen Sie nochmals alle Bereiche durch, in denen Defizite festgestellt wurden, und prüfen Sie, ob alle identifizierten Lücken bewertet und bearbeitet wurden.

- **Aktionsplan zur Vervollständigung der noch offenen Bereiche**

Erstellen Sie einen klaren Plan, wie die verbliebenen offenen Punkte zügig geschlossen werden können.

- **Alle Aktionen abgeschlossen**

Stellen Sie sicher, dass sämtliche Maßnahmen abgeschlossen und dokumentiert wurden – keine offenen Aufgaben sollten mehr bestehen.

- **Projektplan aktualisiert**

Bringen Sie den Projektplan auf den neuesten Stand und dokumentieren Sie alle erledigten Maßnahmen sowie offene Themen.

- **Risiken und Maßnahmen – Abschließende Überprüfung**

Vergewissern Sie sich, dass der Risikobehandlungsplan aktuell ist und alle Maßnahmen dokumentiert, überwacht und weiterverfolgt werden.

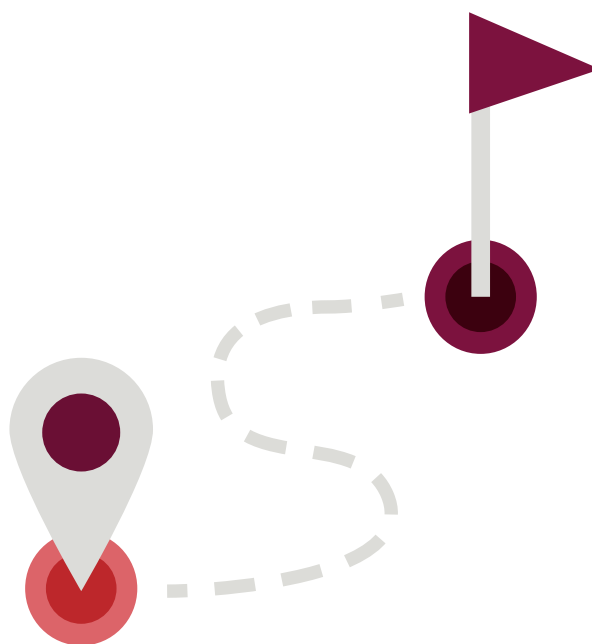
- **Ausgabe und Genehmigung**

Prüfen Sie, ob alle ISMS-Dokumente zum gegebenen Zeitpunkt veröffentlicht und offiziell genehmigt sind. Es ist in Ordnung, wenn sich einzelne Dokumente noch im Arbeitsentwurf befinden – ein Großteil des ISMS sollte jedoch zum Audit vollständig vorliegen.

- Alle vorgeschriebenen Verfahren, Dokumente und Formulare sind vorhanden.
- Das Risikoregister und alle zugehörigen Maßnahmen wurden abschließend überprüft und aktualisiert.
- Alle relevanten Unterlagen sind datiert und durch befugte Personen freigegeben.

- **Liste der Vermögenswerte überprüft und auf den neuesten Stand gebracht**

Kontrollieren Sie, ob die Asset-Liste vollständig und aktuell ist. Fügen Sie ggf. neu hinzugekommene Vermögenswerte oder Informationswerte hinzu, die während der Umsetzung identifiziert wurden.



# 10. Planung der Zertifizierung

## Auswahl einer Zertifizierungsstelle

Zu diesem Zeitpunkt empfiehlt es sich, Kontakt mit einer akkreditierten Zertifizierungsstelle (RCB) aufzunehmen, die das spätere Zertifizierungsaudit durchführen wird. Entscheiden Sie sich möglichst frühzeitig für eine passende RCB und klären Sie wichtige Rahmenbedingungen wie Verfügbarkeit, Abläufe und Kosten. So vermeiden Sie unangenehme Überraschungen im weiteren Verlauf.

## Kosten und Budget

Die Gesamtkosten für die Erstzertifizierung hängen von verschiedenen Faktoren ab – etwa der Anzahl Ihrer Standorte, der Unternehmensgröße sowie der Branche, in der Sie tätig sind. Zusätzlich sollten Sie die wiederkehrenden Kosten für die Aufrechterhaltung der Zertifizierung einplanen.

Idealerweise sind Sie nun so weit, Ihre bevorzugte RCB verbindlich auszuwählen und die Terminplanung für das Audit in Angriff zu nehmen.

## Durchführung von Audits und Bewertungen

Ein zentrales Element von ISO 27001 ist die Durchführung interner Audits Ihres Informationssicherheitsmanagementsystems (ISMS). Vor der offiziellen Bewertung durch eine Zertifizierungsstelle sollten Sie sicherstellen, dass alle relevanten Bereiche Ihres ISMS intern geprüft wurden – oder dass Sie sich zumindest in der finalen Umsetzungsphase befinden.

## Vorbereitung auf die Prüfung

Sobald alle Vorbereitungen abgeschlossen sind, können Sie sich auf den Besuch der Auditoren Ihrer gewählten Zertifizierungsstelle einstellen. Dieser Prüfprozess erfolgt in zwei Phasen:

- **Stufe 1:** Überprüfung Ihrer Dokumentation und des ISMS-Geltungsbereichs. Hier wird eingeschätzt, wie gut Sie vorbereitet sind.
- **Stufe 2:** Detaillierte Bewertung der Umsetzung. Dieser Schritt findet nur statt, wenn bei Stufe 1 keine schwerwiegenden Mängel festgestellt wurden.

Wenn beide Prüfungen erfolgreich verlaufen, erhalten Sie die Zertifizierung – und Ihre investierte Arbeit hat sich ausgezahlt.

# Wie GRASP-IRM Ihre ISO 27001-Implementierung unterstützt



## Integriertes ISMS-Modul

Das ISO 27001-Modul von GRASP-IRM vereint alle notwendigen Komponenten für eine erfolgreiche Zertifizierung. Es unterstützt Sie bei der Definition des Organisationskontexts, der Durchführung von Risikobewertungen und der Implementierung von Sicherheitsmaßnahmen. Durch die zentrale Verwaltung aller relevanten Informationen wird die Einhaltung der Normanforderungen erleichtert.

## Effizientes Risikomanagement

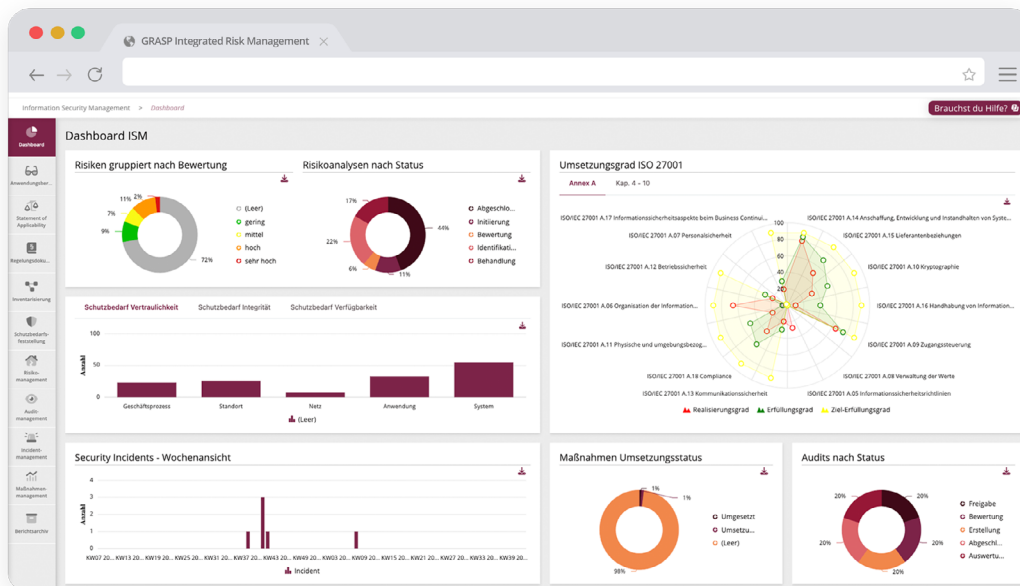
GRASP-IRM bietet eine strukturierte Plattform für die Identifikation, Analyse und Behandlung von Informationssicherheitsrisiken. Die Software ermöglicht eine konsistente Bewertung von Risiken und unterstützt bei der Entwicklung effektiver Strategien zur Risikominimierung.

## Benutzerfreundliche Oberfläche und Anpassungsfähigkeit

GRASP-IRM zeichnet sich durch eine benutzerfreundliche Oberfläche aus, die eine einfache Navigation und Bedienung ermöglicht. Die Software ist flexibel anpassbar und kann ohne Programmierkenntnisse an die spezifischen Anforderungen Ihrer Organisation angepasst werden.

## Integration mit bestehenden Systemen

Die Plattform unterstützt die Integration mit verschiedenen Authentifizierungsdiensten wie LDAP und Azure AD. Zudem können bestehende IT-Assets automatisch importiert und im Kontext des ISMS bewertet werden, was die Effizienz und Genauigkeit der Sicherheitsbewertung erhöht.



## Unterstützung durch ein starkes Partnernetzwerk

Obwohl GRASP-IRM selbst keine Beratungsdienste anbietet, verfügen wir über ein umfangreiches Partnernetzwerk von erfahrenen Fachleuten, die Sie bei der Implementierung und dem Betrieb Ihres ISMS unterstützen können. Diese Partner bieten maßgeschneiderte Beratungsleistungen an, um sicherzustellen, dass Ihre Organisation die ISO 27001-Anforderungen effektiv erfüllt.

# Jetzt 30 Tage **kostenlos** testen!



Hier klicken oder QR Code scannen und loslegen



### **MADE IN GERMANY**

GRASP ist zu 100 % DSGVO-konform. Alle Bestimmungen hinsichtlich Einwilligung, Transparenz und Datensicherheit sind gewährleistet.



### **BASIERT AUF ISO- UND BSI-STANDARDS**

GRASPs Standardmodule Datenschutzmanagement, Informationssicherheitsmanagement und Business Continuity Management basieren auf ISO- und BSI-Standards und können nach Bedarf angepasst werden.



### **ISO 27001 ZERTIFIZIERT**

GRASP wird unter hohen Sicherheitsstandards in Berlin und Essen entwickelt. Die Entwicklerumgebung besitzt eine ISO/IEC 27001-Zertifizierung.