



Was ist ein ISMS nach ISO 27001 – Definition, Aufbau & Vorteile

In diesem Fachbeitrag der VOREST AG erfahren Sie, was ein [Informationssicherheitsmanagementsystem \(ISMS\)](#) nach ISO 27001 ist. Ein ISMS bildet die Grundlage für einen systematischen und ganzheitlichen Schutz sensibler Informationen, der alle Aspekte von der Vertraulichkeit über die Integrität bis hin zur Verfügbarkeit abdeckt. Durch die Einführung eines ISMS nach ISO 27001 schützen Organisationen ihre sensiblen Informationen und Daten vor Verlust, Diebstahl oder Missbrauch. Zugleich wird Vertrauen bei Kunden, Partnern und Aufsichtsbehörden geschaffen.

Definition und Zielsetzung eines ISMS ISO 27001

Ein Informationssicherheitsmanagementsystem nach ISO 27001 ist ein strukturierter und ganzheitlicher Ansatz, um die Informationssicherheit in einer Organisation systematisch zu planen, umzusetzen, zu überwachen und fortlaufend zu verbessern. Dabei umfasst ein ISMS sämtliche Richtlinien, Verfahren, Zuständigkeiten sowie technische und organisatorische Maßnahmen, die den Schutz sensibler Informationen gewährleisten. Ziel ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten dauerhaft sicherzustellen und Informationssicherheitsrisiken wirksam zu minimieren.

Die [ISO/IEC 27001](#) ist dabei die international anerkannte Norm für Informationssicherheitsmanagementsysteme. Sie definiert die Anforderungen, die ein ISMS in einem Unternehmen erfüllen muss, um Informationssicherheit nachweislich und strukturiert umzusetzen. Eine [Zertifizierung nach ISO 27001](#) stärkt das Vertrauen von Kunden und Partnern, schafft Wettbewerbsvorteile und unterstützt die Einhaltung gesetzlicher Vorgaben wie der DSGVO.

Video - Was ist Informationssicherheit?

In der digitalen Welt sind Informationen zu einem der wertvollsten Vermögenswerte geworden. Unternehmen sammeln und verarbeiten riesige Datenmengen. Deshalb ist es von entscheidender Bedeutung, dass diese Informationen sicher und geschützt sind. In diesem Video erfahren Sie mehr darüber, was Informationssicherheit ist und wie wertvolle Daten geschützt werden können. Außerdem erhalten Sie einen Überblick über die drei Schutzziele der Informationssicherheit.



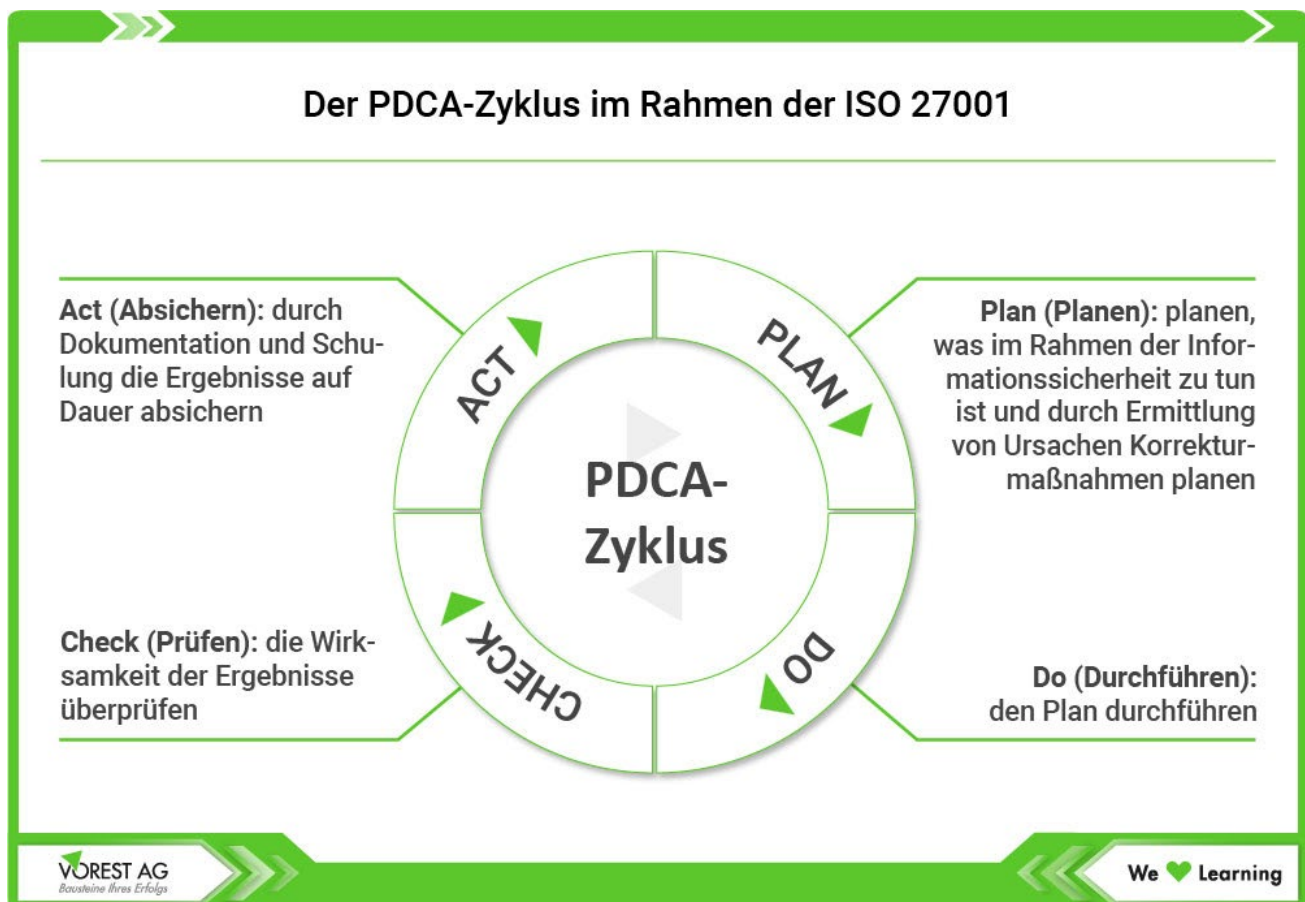
Inhalte:

- Betrachtung der Informationen als Vermögenswerte
- Unterteilung der Schutzziele
- Informationssicherheitsrisiko

Wie wird ein ISMS ISO 27001 aufgebaut?

Der Aufbau eines Informationssicherheitsmanagementsystems nach ISO 27001 folgt, wie andere Managementsysteme auch, dem **PDCA-Zyklus** (Plan – Do – Check – Act). Dieser Zyklus beschreibt einen **kontinuierlichen Verbesserungsprozess**, der sicherstellt, dass Informationssicherheit im Unternehmen strukturiert und nachhaltig umgesetzt wird.

In der **Plan-Phase** werden sicherheitsrelevante Prozesse geplant, Risiken bewertet und geeignete Maßnahmen definiert. Die **Do-Phase** umfasst die Umsetzung dieser Maßnahmen. In der **Check-Phase** wird überprüft, ob die Maßnahmen wirksam sind und die angestrebten Sicherheitsziele erreicht werden. In der abschließenden **Act-Phase** werden erfolgreiche Prozesse standardisiert und Optimierungspotenziale umgesetzt.



PDCA Zyklus im ISMS ISO 27001

Die Implementierung eines ISMS nach ISO 27001 erfolgt schrittweise. Im Folgenden stellen wir Ihnen die wichtigsten Schritte vor, mit denen Sie Ihr ISMS einführen können:

Schritt 1: Anforderungen an die Informationssicherheit identifizieren

Zu Beginn werden alle Anforderungen an die Informationssicherheit ermittelt, sowohl die der ISO 27001 als auch die Ihres Unternehmens sowie die der interessierten Parteien und Behörden. Auf dieser Grundlage wird die Informationssicherheitspolitik definiert. In dieser legt die oberste Leitung die strategischen Ziele und Grundsätze der Informationssicherheit fest.

Schritt 2: Beurteilung von Informationssicherheitsrisiken

Im nächsten Schritt erfolgt die Risikobeurteilung. Dabei identifizieren und bewerten Sie Bedrohungen, Schwachstellen und Eintrittswahrscheinlichkeiten, die Ihre Informationswerte betreffen. Die [Methodik der Risikobeurteilung](#) ist in der ISO 27001 frei wählbar, muss aber transparent dokumentiert werden.

Schritt 3: Informationssicherheitsrisiken behandeln

Nun werden die identifizierten Informationssicherheitsrisiken priorisiert und behandelt. Risiken mit geringem Einfluss können akzeptiert, kritische Risiken hingegen müssen durch geeignete Sicherheitsmaßnahmen reduziert werden. Prüfen Sie dabei, ob bereits bestehende Maßnahmen wirken, sodass sich Doppelarbeiten und unnötige Kosten vermeiden lassen.

Schritt 4: Schutzmaßnahmen auswählen und umsetzen

Wählen Sie zielgerichtete Schutzmaßnahmen, um Risiken auf ein akzeptables Niveau zu senken. Dabei sind gesetzliche Vorgaben, interne Ziele und das Kosten-Nutzen-Verhältnis zu berücksichtigen. Wichtig ist dabei auch, dass Sie die zu erwartenden Verluste durch den Eintritt Risiken mit den Umsetzungskosten abwägen. Sind die Investitionskosten der Sicherheitsmaßnahmen um ein Vielfaches höher als die Verlusterwartung, sollten Sie die Maßnahmen nochmals überdenken.

Schritt 5: Überwachung und Bewertung der Leistung des ISMS

Die Leistung des ISMS muss regelmäßig überwacht, analysiert und bewertet werden. Durch interne Audits prüfen Sie, ob Ihr ISMS die Anforderungen der ISO/IEC 27001 erfüllt und ob geeignete Maßnahmen zur Risikobehandlung definiert sind. Stellt der Auditor Nichtkonformitäten fest, müssen Korrektur- und Vorbeugemaßnahmen eingeleitet werden.

Auch die Managementbewertung durch die oberste Leitung ist Teil dieses Prozesses. Dabei beurteilt das Management in festgelegten Abständen die Eignung, Angemessenheit und Wirksamkeit des Systems. Die Ergebnisse der internen Audits dienen als Grundlage, um über die weiteren Maßnahmen zur Informationssicherheit zu entscheiden.

Schritt 6: Fortlaufende Verbesserung des Informationssicherheitsmanagementsystems

Die **kontinuierliche Verbesserung (KVP)** ist ein zentraler Bestandteil der ISO 27001. Auf Basis der Audit-Ergebnisse und der Managementbewertung wird das ISMS stetig weiterentwickelt. Dabei geht es nicht nur darum, Nichtkonformitäten zu beseitigen, sondern auch funktionierende Schutzmaßnahmen zu optimieren und zu standardisieren. So tragen Sie dauerhaft zum Erhalt der Schutzziele bei.

Vorteile und Nutzen des ISMS nach ISO 27001 für Unternehmen

Ein ISMS nach ISO 27001 bietet Unternehmen zahlreiche Vorteile. Im Mittelpunkt steht der systematische Schutz sensibler Informationen und somit die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten.

Die wichtigsten Vorteile im Überblick:

- **Erhöhter Schutz sensibler Informationen:** Systematische Sicherstellung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit durch klar definierte Prozesse und Maßnahmen.
- **Vertrauen und Reputation:** Eine ISO 27001-Zertifizierung belegt den verantwortungsvollen Umgang mit Informationen – das stärkt das Vertrauen von Kunden, Partnern und Behörden.
- **Erfüllung gesetzlicher Anforderungen:** Unterstützung bei der Einhaltung von DSGVO, IT-Sicherheitsgesetz und branchenspezifischen Regularien.
- **Strukturiertes Risikomanagement:** Risiken werden frühzeitig erkannt, bewertet und durch geeignete Maßnahmen reduziert. Das verringert Sicherheitsvorfälle und finanzielle Schäden.
- **Kontinuierliche Verbesserung:** Regelmäßige Audits und Managementbewertungen fördern die laufende Optimierung der Informationssicherheit.
- **Kosteneffizienz:** Durch die Vermeidung von Sicherheitsvorfällen, Bußgeldern und Ausfallzeiten lassen sich langfristig Kosten senken.
- **Klare Strukturen und Verantwortlichkeiten:** Prozesse werden dokumentiert, Zuständigkeiten klar geregelt und Sicherheitsmaßnahmen nachvollziehbar gesteuert.
- **Einfache Integration mit anderen Managementsystemen:** Dank der Harmonized Structure (HS) lässt sich das ISMS nahtlos mit bestehenden Systemen wie ISO 9001 oder ISO 14001 verbinden, was Ressourcen spart
- **Wettbewerbsvorteil:** Ein zertifiziertes ISMS signalisiert Sicherheit und Professionalität

Passende Schulungen der VOREST AG zur Einführung und Weiterentwicklung eines ISMS nach ISO 27001

Damit Ihr Unternehmen die Vorteile eines ISMS nach ISO 27001 voll ausschöpfen kann, ist fundiertes Wissen über den Aufbau, die Umsetzung und die kontinuierliche Verbesserung des Managementsystems entscheidend. Mit den ISO-27001-Schulungen der VOREST AG erwerben Sie das nötige Wissen, um ein ISMS in Ihrem Unternehmen umzusetzen und zu auditieren.

Bei der VOREST AG können Sie zwischen verschiedenen Lernformaten wählen. Absolvieren Sie Ihre Informationssicherheitsmanagement Schulungen als Präsenzseminar, Live-Virtual-Classroom oder ganz flexibel als [E-Learning-Schulung](#).

	<p>Kostenloser E-Learning Kurs - Was ist ein ISMS nach ISO 27001?</p> <p>Kostenloser E-Learning Kurs zum Informationssicherheitsmanagement mit erstem Überblick über die Bedeutung eines ISMS sowie über die Funktionsweise und Ziele der Norm ISO 27001.</p> <p>Preis: 0,00 € Kursformat: E-Learning</p>	zum Kurs »
	<p>Basiswissen ISMS ISO 27001</p> <p>Grundlagen Kurs zu den Inhalten und Forderungen der Norm DIN EN ISO/IEC 27001 für Informationssicherheitsmanagementsysteme und zur Einführung & Zertifizierung eines ISMS.</p> <p>Preis: 1099,00 € Kursformat: Präsenz Preis: 1.044,05 € Kursformat: Virtual-Classroom</p>	zum Kurs »
	<p>Interner Auditor ISO 27001</p> <p>Schulung zur Vorbereitung, Durchführung und Nachbereitung von internen Audits nach ISO 19011 im Informationssicherheitsmanagementsystem nach ISO 27001 - Abschluss mit Zertifikat.</p> <p>Preis: 1099,00 € Kursformat: Präsenz Preis: 1.044,05 € Kursformat: Virtual-Classroom</p>	zum Kurs »
	<p>Informationssicherheitsbeauftragter - ISMS Beauftragter ISO 27001</p> <p>Ausbildung zur Rolle und den Aufgaben des ISMS-Beauftragten ISO 27001 mit Qualifikation zur Betreuung & Weiterentwicklung eines Informationssicherheitsmanagementsystems - Abschluss mit Zertifikat.</p> <p>Preis: 1299,00 € Kursformat: Präsenz Preis: 1234,05 € Kursformat: Virtual-Classroom</p>	zum Kurs »
	<p>Informationssicherheitsmanagement Auditor / Leitender Auditor ISO 27001</p> <p>Ausbildung zum Erwerb des fachlichen und persönlichen Know-how zur Durchführung externer Audits und Zertifizierungsaudits im ISMS als (Lead) Auditor ISO 27001 - Abschluss mit Zertifikat.</p> <p>Preis: 2599,00 € Kursformat: Präsenz Preis: 2469,05 € Kursformat: Virtual-Classroom</p>	zum Kurs »
	<p>Kostenloser Gesamtkatalog der VOREST AG zum Download</p> <p>Gesamtkatalog der VOREST AG mit allen Schulungen rund um Managementsysteme, Prozessoptimierung und Methoden zum kostenlosen Download.</p>	Download »

Sie wissen noch nicht, welcher Kurs der richtige ist?

Fragen zu Formaten, Förderung oder Inhalten?



Sevil Kaya

Sevil Kaya

Mail: skaya@vorest-ag.de
Telefon: 07231 92 23 91 33



Katharina Reutter

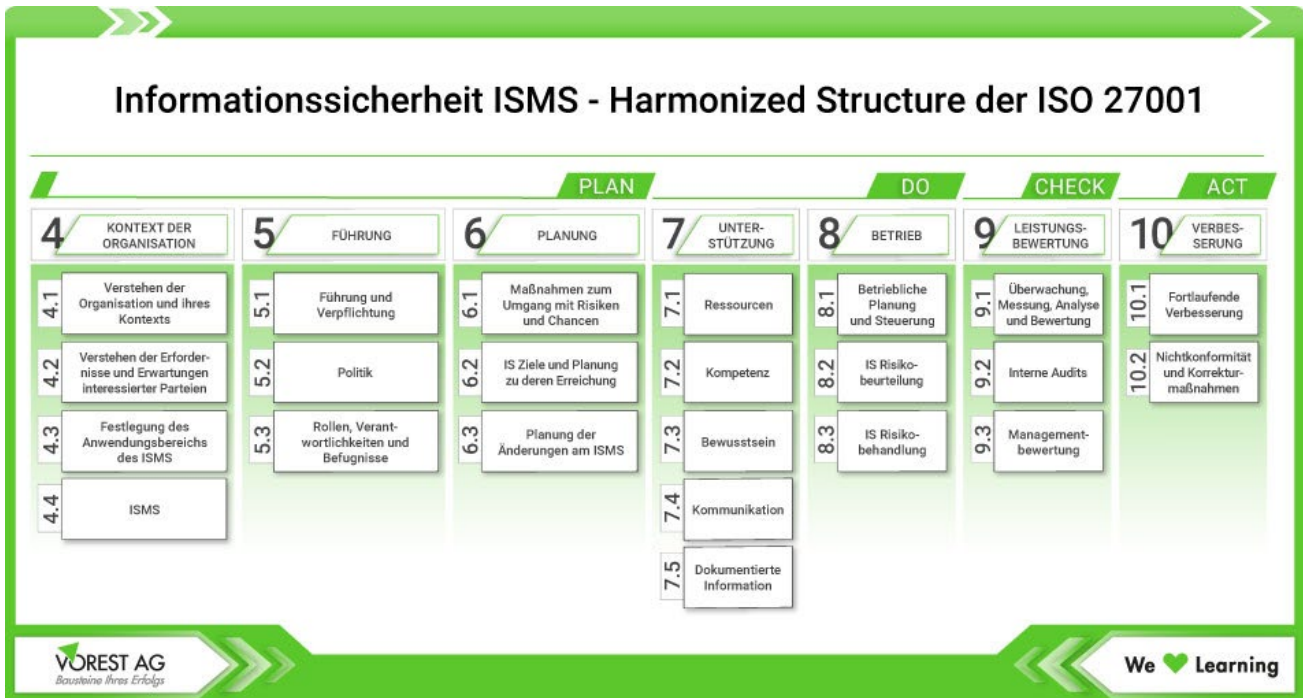
Katharina Reutter

Mail: kreutter@vorest-ag.de
Telefon: 07231 92 23 91 37

Bedeutung und Anforderungen der ISO 270001 für ein ISMS

Die ISO/IEC 27001 ist der international anerkannte Standard für Informationssicherheitsmanagementsysteme. Sie legt die Anforderungen fest, die Unternehmen erfüllen müssen, um Informationssicherheit systematisch und nachweisbar zu managen. Seit der [Revision 2022](#) folgt die Norm der sogenannten Harmonized Structure (HS). Diese einheitliche Struktur gilt für alle aktuellen ISO-Managementsystemnormen, wie z. B. ISO 9001 oder ISO 14001, und erleichtert so die Integration mehrerer Managementsysteme in einem Unternehmen.

Die Harmonized Structure sorgt für eine klare und einheitliche Gliederung in zehn Hauptkapitel. Damit werden Anforderungen an Aufbau, Verantwortung, Planung, Umsetzung und Verbesserung eines ISMS transparent beschrieben. Die folgenden Kapitel zeigen eine Übersicht der ISO 27001 Anforderungen, wie sie in der Norm festgelegt sind.



Harmonized Structure ISO 27001

- **Kapitel 1–3:** Beschreiben den Anwendungsbereich, relevante Normverweisungen und zentrale Begriffe der Informationssicherheit, wie „ISMS“, „Risiko“ und „Maßnahme“.
- **Kapitel 4 – Kontext der Organisation:** Verlangt, dass interne und externe Einflussfaktoren sowie Erwartungen interessierter Parteien berücksichtigt werden.
- **Kapitel 5 – Führung:** Fordert Verantwortung und Engagement der obersten Leitung, die Einführung einer Informationssicherheitspolitik und die Festlegung klarer Verantwortlichkeiten.
- **Kapitel 6 – Planung:** Behandelt die Erkennung und Bewertung von Risiken und Chancen sowie die Planung geeigneter Maßnahmen zur Risikobehandlung
- **Kapitel 7 – Unterstützung:** Umfasst die Bereitstellung von Ressourcen, Schulungen, Kommunikation und die Dokumentation des ISMS.
- **Kapitel 8 – Betrieb:** Regelt die Steuerung der betrieblichen Prozesse sowie die Durchführung von Risikobewertungen und -behandlungen.
- **Kapitel 9 – Bewertung der Leistung:** Verlangt eine regelmäßige Überprüfung der Wirksamkeit des ISMS, z. B. durch interne Audits und Managementbewertungen.
- **Kapitel 10 – Verbesserung:** Definiert den Umgang mit Nichtkonformitäten und die Einleitung von Korrektur- und Verbesserungsmaßnahmen, um das ISMS fortlaufend zu optimieren.

Anhang A – Maßnahmenziele und Maßnahmen (Controls)

Der Anhang A der ISO/IEC 27001 enthält eine strukturierte Liste von Informationssicherheitsmaßnahmen (Controls), die als Leitfaden für den Aufbau und die Umsetzung eines wirksamen ISMS dienen. Diese Controls unterstützen Organisationen dabei, identifizierte Risiken im Rahmen der Risikobehandlung gezielt zu adressieren und geeignete Schutzmaßnahmen auszuwählen.

Anhang A der aktuellen ISO/IEC 27001:2022 umfasst 93 Maßnahmen, die in vier Hauptkategorien gegliedert sind.

- **Organisatorische Maßnahmen (Organizational Controls):** z. B. Richtlinien zur Informationssicherheit, Rollen und Verantwortlichkeiten, Schulungen, Lieferantenmanagement.
- **Personenbezogene Maßnahmen (People Controls):** z. B. Schulung und Sensibilisierung der Mitarbeitenden sowie Verantwortlichkeiten vor, während und nach dem Arbeitsverhältnis.
- **Physische Maßnahmen (Physical Controls):** z. B. Zutrittskontrollen und Schutz vor unbefugtem Zugriff oder Umwelteinflüssen.
- **Technologische Maßnahmen (Technological Controls):** z. B. Zugriffskontrollen, Kryptografie, Schutz vor Malware, Überwachung und Protokollierung.

Diese Maßnahmen sind nicht verpflichtend vollständig umzusetzen, sondern bilden einen Referenzrahmen. Jede Organisation muss im Rahmen ihrer Risikobewertung und Risikobehandlung individuell festlegen, welche Controls relevant und angemessen sind. Die getroffenen Entscheidungen, einschließlich abgelehnter Controls, müssen im sogenannten Statement of Applicability (SoA) dokumentiert und begründet werden.

Risikomanagement im Rahmen des ISMS nach ISO 27001

Das Risikomanagement bildet das zentrale Element eines ISMS nach ISO/IEC 27001. Ziel ist es, Informationssicherheitsrisiken systematisch zu identifizieren, zu bewerten und mit geeigneten Maßnahmen zu behandeln, um die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit dauerhaft sicherzustellen.

Im Rahmen des ISMS erfolgt das Risikomanagement in fünf aufeinander aufbauenden Schritten:

1. **Risikoidentifikation:** Ermittlung der relevanten Informationswerte (Assets), möglicher Bedrohungen (z. B. Hackerangriffe, menschliche Fehler) und Schwachstellen (z. B. fehlende Sicherheitsupdates). Die Risiken werden den betroffenen Systemen, Prozessen oder Personen zugeordnet.
2. **Risikobewertung:** Bewertung der identifizierten Risiken anhand ihrer Eintrittswahrscheinlichkeit und Auswirkung. Daraus wird der Risikograd ermittelt, häufig mithilfe einer Risikomatrix, und die Risiken werden entsprechend priorisiert.
3. **Risikobehandlung:** Auswahl geeigneter Maßnahmen zur Risikominderung
 - Vermeidung (z. B. Prozesse ändern)
 - Verringerung (z. B. technische Schutzmaßnahmen)
 - Übertragung (z. B. Versicherung)
 - Akzeptanz (bei tolerierbaren Risiken)

Grundlage für die Maßnahmenwahl sind die Controls aus Anhang A der ISO/IEC 27001.

4. **Statement of Applicability (SoA):** Dokumentation aller umgesetzten, akzeptierten oder abgelehnten Sicherheitsmaßnahmen. Dabei wird jede Entscheidung, insbesondere die Nichtauswahl bestimmter Controls, begründet und nachvollziehbar dokumentiert.
5. **Überwachung und Verbesserung:** Regelmäßige Überprüfung der Risiken und Wirksamkeit der Maßnahmen. Veränderungen wie neue Technologien, organisatorische Anpassungen oder gesetzliche Vorgaben werden berücksichtigt und fließen in den kontinuierlichen Verbesserungsprozess (KVP) des ISMS ein.

Das Risikomanagement nach ISO 27001 ist nicht starr, sondern muss zur Organisation passen. Der gewählte Bewertungsansatz (qualitativ oder quantitativ) sowie die Dokumentation müssen nachvollziehbar und reproduzierbar sein.

Zertifizierung nach ISO 27001 - Ablauf und Voraussetzung

Die Zertifizierung eines ISMS nach ISO 27001 erfolgt in mehreren klar definierten Schritten. Zunächst bereitet sich das Unternehmen intern vor: Das ISMS wird aufgebaut, relevante Dokumentationen und Nachweise werden erstellt, eine Risikobewertung durchgeführt sowie interne Audits und eine Managementbewertung umgesetzt. Diese Vorbereitungsphase stellt sicher, dass alle Anforderungen der Norm erfüllt sind.

Anschließend wählt das Unternehmen eine akkreditierte Zertifizierungsstelle, die den eigentlichen Zertifizierungsprozess durchführt. Dieser gliedert sich in zwei Audit-Stufen:

- **Stufe 1 – Dokumentenprüfung:** Die Auditoren prüfen die vorhandene ISMS-Dokumentation und bewerten, ob das System die formalen Anforderungen der ISO/IEC 27001 erfüllt.
- **Stufe 2 – Systemaudit:** Im Anschluss erfolgt das Audit vor Ort. Hier wird überprüft, wie wirksam das ISMS in der Praxis umgesetzt ist und ob die geplanten Maßnahmen tatsächlich greifen.

Werden Abweichungen festgestellt, müssen diese vor Erteilung des Zertifikats nachweislich korrigiert werden. Nach erfolgreicher Prüfung erhält das Unternehmen das ISO 27001-Zertifikat, das drei Jahre gültig ist. Zur Aufrechterhaltung der Zertifizierung werden jährliche Überwachungsaudits durchgeführt, in denen die fortlaufende Anwendung und Verbesserung des ISMS kontrolliert wird. Nach Ablauf der Zertifikatslaufzeit ist ein Rezertifizierungsaudit erforderlich, um die Zertifizierung zu verlängern.

Weitere Informationen finden Sie auf unserer [Seite zur ISO 27001-Zertifizierung](#).

Kosten eines ISMS nach ISO 27001

Die Kosten für die Einführung und den Betrieb eines ISMS nach ISO 27001 hängen stark von der Unternehmensgröße, der Branche, der bestehenden IT-Infrastruktur, der internen Expertise sowie vom gewünschten Zertifizierungsumfang ab. Die folgende Kostenübersicht für ISMS ISO 27001 zeigt typische Aufwände und Preisspannen, die bei der Einführung, Zertifizierung und Pflege eines ISMS bei kleinen bis mittleren Unternehmen entstehen können.

Einmalkosten

Die Einmalkosten entstehen bei der Einführung und Implementierung des ISMS. Dazu zählen unter anderem:

- **Gap-Analyse / Reifegradbestimmung:** Ermittlung von Abweichungen zur Norm – ca. 1.000 – 10.000 €
- **Beratung & externe Unterstützung:** Unterstützung durch ISMS-Experten bei Planung, Dokumentation und Risikoanalyse – ca. 5.000 – 50.000 €
- **Schulungen & Awareness-Trainings:** Sensibilisierung und Qualifizierung von Mitarbeitenden und ISMS-Verantwortlichen – ca. 500 – 5.000 €
- **Dokumentation & Tools:** Erstellung von Richtlinien, Prozessen und ggf. Einführung einer ISMS-Software – ca. 1.000 – 10.000 €
- **Technische Maßnahmen:** Sicherheitslösungen wie Firewalls, Backups, Zugriffs- oder Netzwerkschutz – 1.000 – 50.000 €, abhängig von Umfang und Systemlandschaft

Laufende Kosten

Nach der Einführung entstehen regelmäßige Aufwände für Pflege, Überwachung und Verbesserung des ISMS:

- **Interner Personalaufwand:** Pflege des ISMS, Durchführung von Audits, Risikomanagement und Awareness-Maßnahmen – ca. 0,1 – 1 FTE, abhängig von Unternehmensgröße (FTE = Full Time Equivalent)
- **Interne / externe Audits:** Überwachungsaudits durch interne Auditoren oder Zertifizierungsstellen – ca. 3.000 – 15.000 € jährlich
- **Zertifizierungskosten:** Erstzertifizierung, Überwachungs- und Rezertifizierungsaudits (über 3 Jahre) – ca. 10.000 – 30.000 €
- **ISMS-Software (optional):** Tools zur Dokumentation, Risikoanalyse und Maßnahmenverfolgung – ca. 1.000 – 15.000 € pro Jahr

Weitere Kostenfaktoren

Weitere Faktoren, die die Kosten eines ISMS beeinflussen, sind:

- **Komplexität der IT-Landschaft:** Je heterogener Systeme, Netzwerke und Anwendungen sind, desto höher der Implementierungs- und Wartungsaufwand.
- **Anzahl und Standorte der Mitarbeitenden:** Mehr Mitarbeitende und verteilte Teams erhöhen Schulungs- und Sicherheitsaufwand, insbesondere bei Remote-Arbeitsplätzen.
- **Regulatorische Anforderungen:** Unternehmen in sensiblen Branchen (z. B. KRITIS, Finanz- oder Gesundheitswesen) müssen mit zusätzlichen Vorgaben rechnen.
- **Bestehende Managementsysteme:** Ein vorhandenes ISO 9001-Qualitätsmanagementsystem oder andere Normsysteme können Synergien schaffen und die Implementierungskosten deutlich senken.

■ **Sie haben Fragen oder wünschen ein Angebot?**
Ich helfe Ihnen gerne weiter!

Kati Schäfer

Produktmanagement Training & PRO SYS

☎ 07231 92 23 91 - 0

✉ kschaefer@vorest-ag.de



■ **Inhouse Training – Wir kommen zu Ihnen ins Haus!**
Sie wünschen ein Angebot?

Claudia Talmon

Produktmanagement Training

☎ 07231 92 23 91 - 0

✉ ctalmon@vorest-ag.de



Unser Katalog

Laden Sie hier kostenfrei und unverbindlich unseren **Katalog** mit einer Übersicht zu allen unseren aktuellen **Schulungen** und **E-Learning-Kursen** herunter.

