



ISO 27001 einfach erklärt – Definition, Anforderungen und Inhalte

ISO 27001 beschreibt die Anforderungen an ein strukturiertes Informationssicherheitsmanagementsystem (ISMS), mit dem Unternehmen ihre Informationssicherheit systematisch planen, steuern, überwachen und kontinuierlich verbessern. Die Norm schafft klare Verantwortlichkeiten, reduziert Sicherheitsrisiken und schützt sensible Daten unabhängig von Branche, Unternehmensgröße oder Standort. Auf dieser Seite erhalten Sie einen fundierten Überblick über Definition, Aufbau, Anforderungen, Schutzziele und Zertifizierung der ISO/IEC 27001:2022.

Cyberangriffe, zunehmende regulatorische Anforderungen und steigende Abhängigkeit von digitalen Prozessen verändern die Risikolage für Unternehmen grundlegend. Organisationen, die ihre Informationssicherheit nicht aktiv steuern, riskieren Datenverluste, Produktionsausfälle, Reputationsschäden und rechtliche Konsequenzen. Ein strukturiertes Management der Informationssicherheit nach ISO 27001 schafft hier Transparenz, Verlässlichkeit und strategische Kontrolle über sicherheitsrelevante Prozesse.

Wie wird die ISO 27001 definiert?

Die ISO/IEC 27001:2022 ist die international anerkannte Norm für Informationssicherheitsmanagementsysteme (ISMS). Sie wurde gemeinsam von der International Organization for Standardization (ISO) und der International Electrotechnical Commission (IEC) entwickelt. Ziel der ISO 27001 ist es, Unternehmen dabei zu unterstützen, Risiken im Umgang mit Daten systematisch zu erkennen, zu bewerten und angemessen zu behandeln. Unabhängig von Branche, Größe oder Standort kann jede Organisation die Anforderungen der ISO 27001 umsetzen.

Die drei Schutzziele der Informationssicherheit bilden dabei das Fundament der ISO 27001. Sie stellen sicher, dass Informationen vertraulich bleiben, ihre Integrität gewahrt wird und sie für autorisierte Personen jederzeit verfügbar sind. Um diese Schutzziele in der Praxis wirksam umzusetzen, unterstützt die ISO 27001 Unternehmen mit einem strukturierten Informationssicherheitsmanagementsystem (ISMS), das Sicherheitsmaßnahmen gezielt plant, steuert und kontinuierlich verbessert.

Die Norm verfolgt einen risikobasierten Ansatz und orientiert sich an der sogenannten Harmonized Structure (HS), vormals High Level Structure (HLS). Dadurch lässt sich die ISO 27001 optimal mit bestehenden Managementsystemen kombinieren. Als zertifizierbarer Standard bietet sie Organisationen weltweit eine anerkannte Grundlage, Informationssicherheit nachhaltig zu steuern und nachzuweisen.

Video: Die ISO 27001 und ihre Anforderungen einfach erklärt

Die ISO/IEC 27001 ist die international führende Norm für das Informationssicherheitsmanagement. Sie definiert die Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS) und spielt eine zentrale Rolle beim Schutz sensibler Daten und Informationen in Unternehmen weltweit. Ziel der Norm ist es, Informationssicherheitsrisiken systematisch zu erkennen, geeignete Maßnahmen umzusetzen und die Sicherheit kontinuierlich zu verbessern.



In diesem Video erfahren Sie, welche Anforderungen die ISO 27001 stellt, wie ein ISMS aufgebaut sein muss und warum eine [Zertifizierung nach ISO 27001](#) für Organisationen von Vorteil sein kann.

Inhalte des Videos:

- Was ist die ISO 27001?
- Inhalte und Anforderungen der ISO 27001
- Zertifizierung des ISMS in einem Unternehmen

Die Vorteile der ISO 27001 zusammengefasst

Die ISO/IEC 27001 bietet Unternehmen zahlreiche Vorteile, die weit über den reinen Schutz sensibler Daten hinausgehen:

Verbesserte Informationssicherheit: Ein strukturiertes ISMS nach ISO 27001 schützt die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und reduziert Risiken wie Cyberangriffe oder Datenverluste systematisch.

Stärkung von Vertrauen und Image: Die ISO 27001 Zertifizierung signalisiert hohe Sicherheitsstandards und stärkt das Vertrauen von Kunden, Partnern und Behörden nachhaltig.

Erfüllung gesetzlicher und regulatorischer Anforderungen: Die Norm unterstützt Unternehmen dabei, regulatorische Vorgaben – etwa DSGVO-Anforderungen – strukturiert umzusetzen und Informationssicherheit mit Compliance zu verbinden.

Effektives Risikomanagement: ISO 27001 etabliert einen risikobasierten Ansatz, mit dem Bedrohungen frühzeitig erkannt, bewertet und gezielt behandelt werden.

Wettbewerbsvorteil: Ein zertifiziertes Unternehmen hebt sich klar vom Wettbewerb ab und kann Informationssicherheit als starkes Argument in Ausschreibungen und Kundengesprächen nutzen.

Kontinuierliche Verbesserung der Informationssicherheit: Durch den PDCA-Zyklus werden Sicherheitsmaßnahmen regelmäßig überprüft und optimiert, sodass das ISMS dauerhaft wirksam bleibt.

Kosteneinsparungen durch Prävention: Die frühzeitige Behandlung von Risiken reduziert die Wahrscheinlichkeit kostspieliger Sicherheitsvorfälle und schützt gleichzeitig Reputation und Betriebskontinuität.

Was sind typische Ziele der ISO 27001?

Die ISO 27001 verfolgt das Ziel, Informationssicherheit systematisch im Unternehmen zu verankern. Im Mittelpunkt stehen der Schutz von Informationen hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit sowie ein strukturiertes Risikomanagement zur frühzeitigen Erkennung und Behandlung von Bedrohungen. Gleichzeitig unterstützt die Norm Organisationen dabei, gesetzliche Anforderungen einzuhalten, Verantwortlichkeiten klar zu regeln und die Sicherheitsmaßnahmen kontinuierlich zu verbessern. So entsteht ein dauerhaft wirksames und nachvollziehbares Informationssicherheitsniveau.

Welche Anforderungen stellt die Norm ISO 27001?

Die Inhalte der ISO 27001 decken mehrere zentrale Bereiche der Informationssicherheit ab. Unternehmen müssen die ISO 27001 Anforderungen erfüllen, um eine effektive Sicherheitsstrategie zu entwickeln und ein erfolgreiches Informationssicherheitsmanagementsystem aufzubauen. In der folgenden Tabelle finden Sie die ISO 27001 Inhalte und welche Anforderungen dabei an ein ISMS gestellt werden:

Anforderung nach ISO 27001	Inhaltliche Schwerpunkte	Ziel für das ISMS
Leitung und Unterstützung	Strategische Verankerung der Informationssicherheit, Bereitstellung von Ressourcen, klare Verantwortlichkeiten durch die oberste Leitung.	Sicherstellung von Führung, Priorisierung und nachhaltiger Umsetzung des ISMS.
Risikoidentifikation und Risikobewertung	Systematische Identifikation und Bewertung von Risiken (technisch, menschlich, physisch, organisatorisch) sowie Planung geeigneter Risikobehandlungsmaßnahmen.	Minimierung von Informationssicherheitsrisiken durch strukturiertes Risikomanagement.

Anforderung nach ISO 27001	Inhaltliche Schwerpunkte	Ziel für das ISMS
Dokumentation des ISMS	Dokumentation aller relevanten Prozesse, Richtlinien und Sicherheitsmaßnahmen.	Nachvollziehbarkeit, Auditfähigkeit und rechtliche Absicherung.
Organisation der Informationssicherheit	Klare Definition und Kommunikation von Rollen und Zuständigkeiten; Benennung z. B. eines ISMS-Beauftragten.	Transparente Verantwortlichkeiten und wirksame Steuerung des ISMS.
Sicherheitsprüfungen und ISO 27001 Audits	Regelmäßige interne Audits und Sicherheitsüberprüfungen zur Bewertung der Normkonformität und Wirksamkeit.	Identifikation von Schwachstellen und kontinuierliche Verbesserung.
Human Resource Security	Schulungen, Sensibilisierungsprogramme und Sicherheitsverantwortung aller Mitarbeitenden.	Stärkung des Sicherheitsbewusstseins im Unternehmen.
Physische und umgebungsbezogene Sicherheit	Zutrittskontrollen, Schutz sensibler Bereiche, regelmäßige Überprüfung physischer Sicherheitsmaßnahmen.	Schutz vor unbefugtem Zugriff, Diebstahl oder Beschädigung von IT-Systemen.
Kommunikationssicherheit	Einsatz von Verschlüsselung, Authentifizierungsverfahren und Netzwerkzugangskontrollen für sichere Datenübertragung und -speicherung.	Sicherstellung der Vertraulichkeit und Integrität sensibler Informationen.

Anforderung nach ISO 27001	Inhaltliche Schwerpunkte	Ziel für das ISMS
Kontinuierliche Verbesserung	Regelmäßige Überprüfung und Anpassung des ISMS nach dem PDCA-Zyklus (Plan – Do – Check – Act).	Dynamische Weiterentwicklung des ISMS und Anpassung an neue Bedrohungen.

Zentrale Rollen im ISMS nach ISO 27001

Im Informationssicherheitsmanagement nach ISO 27001 gibt es mehrere zentrale Rollen, die je nach Unternehmensgröße unterschiedlich ausgeprägt sein können. Typischerweise gehören dazu:

Der interne Auditor

Der [interne Auditor](#) plant, führt interne Audits durch und bewertet, ob das ISMS wirksam umgesetzt wird und den Anforderungen der Norm entspricht.

Informationssicherheitsbeauftragter (ISB) / ISMS-Beauftragter

Koordiniert den Aufbau, die Umsetzung und die Weiterentwicklung des ISMS. Er ist zentrale Ansprechperson für Informationssicherheit im Unternehmen.

Oberste Leitung (Top Management)

Trägt die Gesamtverantwortung für das Informationssicherheitsmanagementsystem (ISMS), legt die Informationssicherheitsstrategie fest und stellt notwendige Ressourcen bereit.

Der (externe) Auditor

Werden von einer akkreditierten Zertifizierungsstelle beauftragt und führen im Rahmen der ISO 27001 Zertifizierung unabhängige Audits durch. Sie prüfen, ob das ISMS normkonform implementiert ist und die Anforderungen der ISO 27001 erfüllt.

Aufbau und Struktur der ISO 27001

Der ISO 27001 Aufbau folgt der einheitlichen High Level Structure (HLS), die für moderne ISO-Managementsysteme gilt. Diese international festgelegte Gliederung sorgt dafür, dass sich unterschiedliche Managementsysteme, wie etwa ISO 9001 (Qualitätsmanagement) oder ISO 14001 (Umweltmanagement), leicht miteinander kombinieren lassen.

Die HLS umfasst zehn Hauptabschnitte, die sich am bewährten [PDCA-Zyklus](#) (Plan – Do – Check – Act) orientieren. Dieses Prinzip unterstützt Unternehmen dabei, ihr Informationssicherheitsmanagementsystem (ISMS) systematisch zu planen, umzusetzen, zu überwachen und kontinuierlich zu verbessern.

Video: Struktur der ISO/IEC 27001 – Aufbau & Inhalte der ISMS-Norm einfach erklärt

Die Norm DIN EN ISO/IEC 27001 bietet Organisationen einen strukturierten Rahmen, um Risiken im Bereich der Informationssicherheit zu identifizieren, zu bewerten und geeignete Schutzmaßnahmen zu implementieren. Dabei legt die Norm sowohl Anforderungen an die organisatorische als auch an die technische Umsetzung eine ISMS fest. Der Kern der Norm ist in den Abschnitten 4 bis 10 strukturiert, die dem PDCA-Zyklus folgen.



In diesem Video erfahren Sie, wie die ISO/IEC 27001 aufgebaut ist und welche Anforderungen die ISMS-Norm in ihren einzelnen Abschnitten stellt.

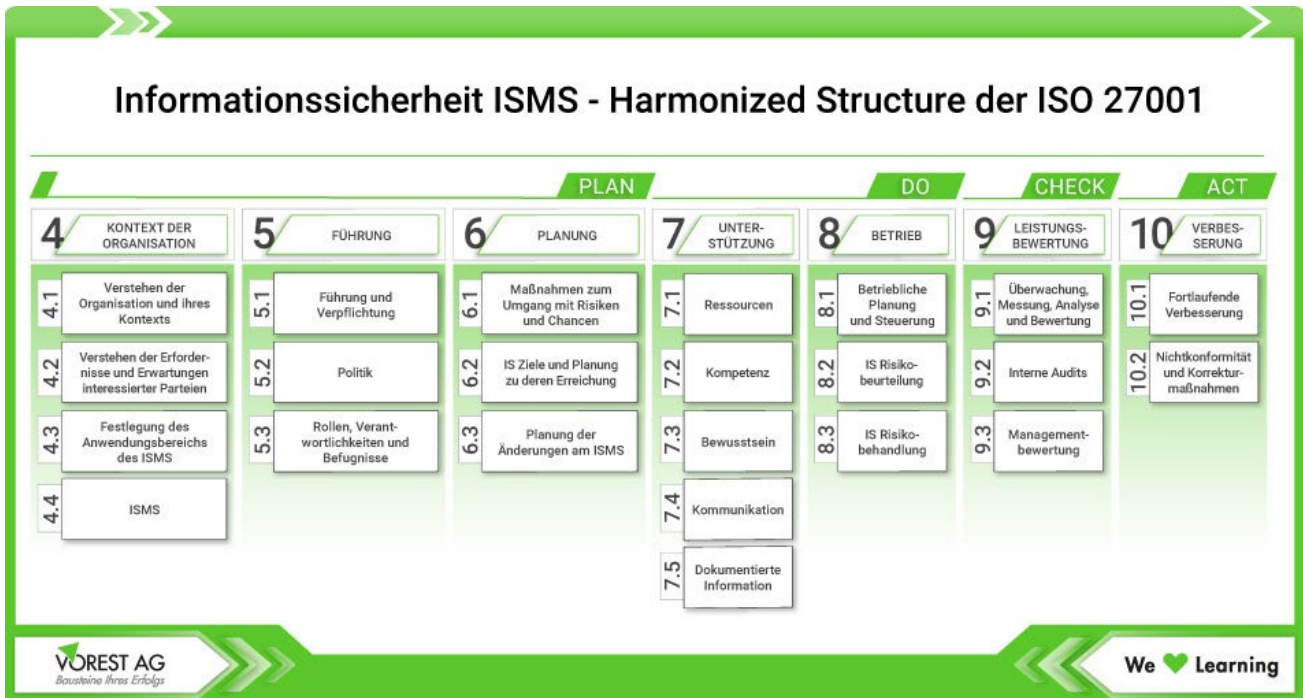
Inhalte dieses Videos:

- Struktur der ISO/IEC 27001
- Abschnitte 0 bis 3
- Abschnitte 4 bis 10

Die 10 Abschnitte der ISO 27001

Der Aufbau der ISO 27001 folgt einer klaren Struktur mit 10 Abschnitten, die in der High Level Structure (HLS) festgelegt sind. Die ersten drei Kapitel dienen als Einleitung und erläutern den Anwendungsbereich, Verweise und Begriffe. In den Abschnitten 4 bis 10 finden sich die konkreten Anforderungen an das Informationssicherheitsmanagementsystem.

Nachfolgend werden die zehn Abschnitte der ISO 27001 im Detail vorgestellt und ihre jeweilige Bedeutung für ein wirksames ISMS erläutert.



Grafische Übersicht der ISO 27001 Anforderungen an ein Informationssicherheitsmanagementsystem in den Abschnitten 4 bis 10 mit Zuordnung zu den einzelnen Phasen des PDCA-Zyklus.

1. Anwendungsbereich

Der erste Abschnitt legt den grundsätzlichen Zweck der ISO 27001 fest. Er beschreibt den Aufbau, die Implementierung und die kontinuierliche Verbesserung eines ISMS. Zudem stellt er klar, dass die ISO/IEC 27001 auf alle Organisationen, unabhängig von Größe, Branche oder Standort, anwendbar ist.

2. Normative Verweisung

Dieser Abschnitt verweist auf weitere Normen, die für das Verständnis und die Anwendung der ISO 27001 Anforderungen relevant sind. Außerdem dient er als Verknüpfung zu ergänzenden Standards, insbesondere zur ISO/IEC 27000, die als Referenzgrundlage für Definitionen und Begrifflichkeiten herangezogen wird.

3. Begriffe und Definition

In diesem Abschnitt werden alle wichtigen Begriffe der ISO 27001 festgelegt. Auch hier verweist die Norm auf die ISO/IEC 27000, in der zentrale Begriffe präzise definiert sind. So wird sichergestellt, dass alle Anwender der Norm eine gemeinsame Sprache sprechen und Missverständnisse vermieden werden.

4. Kontext der Organisation

Dieser Abschnitt fordert Unternehmen auf, ihren organisatorischen Kontext im Rahmen der ISO 27001 zu verstehen und zu dokumentieren. Dazu gehören:

- Interne und externe Faktoren, die die Informationssicherheit beeinflussen (z. B. rechtliche, technologische oder kulturelle Rahmenbedingungen)

- Anforderungen interessierter Parteien, wie Kunden, Mitarbeitende, Aufsichtsbehörden oder Geschäftspartner
- Festlegung des Geltungsbereichs des ISMS, also welche Standorte, Abteilungen oder Prozesse abgedeckt werden
- Aufbau eines Informationssicherheitsmanagementsystems nach den ISO 27001 Anforderungen

5. Führung

In diesem Abschnitt wird die zentrale Rolle der Geschäftsleitung bei der Umsetzung der ISO 27001 Anforderungen hervorgehoben. Die oberste Führungsebene trägt die Verantwortung, Informationssicherheit als strategisches Unternehmensziel zu verankern und aktiv vorzuleben.

- Führung und Verpflichtung: Das Management muss sich klar zur Informationssicherheit bekennen, entsprechende Ressourcen bereitstellen und sicherstellen, dass alle Mitarbeitenden die Bedeutung von Informationssicherheit verstehen.
- Informationssicherheitsrichtlinie und Strategie: Entwicklung einer Informationssicherheitsrichtlinie, die die strategischen Unternehmensziele unterstützt
- Rollen, Verantwortlichkeiten und Befugnisse: Klare Definition und Kommunikation aller Zuständigkeiten im Bereich Informationssicherheit, um Verantwortlichkeiten transparent zu gestalten.

6. Planung

Im Kapitel Planung geht es darum, wie Organisationen Sicherheitsziele festlegen und geeignete Maßnahmen zur Risikominderung planen.

- Risiken und Chancen: Systematische Risikoanalyse zur Erkennung und Bewertung potenzieller Bedrohungen, Schwachstellen und Auswirkungen auf die Informationssicherheit.
- Informationssicherheitsziele: Festlegung von konkreten, messbaren und überprüfbaren Zielen auf Basis der Risikoanalyse.
- Planung von Maßnahmen: Definition und Umsetzung geeigneter Maßnahmen, um Risiken zu minimieren und die Schutzziele der Informationssicherheit zu erreichen.

7. Unterstützung

Der Abschnitt Unterstützung definiert alle Ressourcen und organisatorischen Voraussetzungen, die für den Betrieb eines funktionierenden ISMS erforderlich sind.

- Ressourcen: Bereitstellung ausreichender finanzieller, personeller und technischer Mittel für den Betrieb und die Weiterentwicklung des ISMS.
- Kompetenzen: Sicherstellen, dass alle Mitarbeiter die notwendigen Fähigkeiten und Schulungen erhalten, um ihre Aufgaben im Bereich der Informationssicherheit zu erfüllen.

- **Bewusstsein und Kommunikation:** Förderung eines hohen Sicherheitsbewusstseins im Unternehmen sowie eine regelmäßige, transparente Kommunikation über Sicherheitsrichtlinien und -maßnahmen.
- **Dokumentierte Informationen:** Verwaltung und Pflege der Dokumentationen und Aufzeichnungen, die für das ISMS relevant sind.

8. Betrieb

Dieser Abschnitt beschreibt, wie das Informationssicherheitsmanagementsystem (ISMS) im täglichen Betrieb umgesetzt wird.

- **Betriebsplanung und -steuerung:** Sicherstellen der korrekten Umsetzung aller Maßnahmen und kontinuierliche Überwachung des ISMS im laufenden Betrieb.
- **Bewertung von Risiken:** Durchführung von Risikobewertungen und Priorisierung der Risiken.
- **Behandlung von Risiken:** Umsetzung geeigneter Risikobehandlungsmaßnahmen und Entwicklung von Notfallplänen, um bei Sicherheitsvorfällen schnell und wirksam reagieren zu können.

9. Bewertung der Leistung

Die Bewertung der Leistung ist eine zentrale Anforderung der ISO 27001 und entscheidend für die kontinuierliche Verbesserung und Wirksamkeit des ISMS.

- **Überwachung, Messung, Analyse und Bewertung:** Laufende Kontrolle der Informationssicherheitsprozesse
- **Interne Audits:** Regelmäßige interne Audits nach ISO 27001 dienen der Überprüfung, ob alle Normanforderungen erfüllt und die Sicherheitsmaßnahmen wirksam umgesetzt werden.
- **Managementbewertung (Management Review):** Die Geschäftsleitung muss in definierten Abständen eine Bewertung des ISMS durchführen, um Wirksamkeit, Angemessenheit und Verbesserungsbedarf festzustellen.

10. Verbesserung

Der letzte Abschnitt der ISO/IEC 27001 befasst sich mit der kontinuierlichen Verbesserung des Informationssicherheitsmanagementsystems. Ein wirksames ISMS ist kein statisches System, sondern wird regelmäßig angepasst und optimiert.

- **Nichtkonformitäten und Korrekturmaßnahmen:** Werden Abweichungen von den Sicherheitsanforderungen oder Schwachstellen festgestellt, müssen gezielte Korrekturmaßnahmen umgesetzt und dokumentiert werden.
- **Kontinuierliche Verbesserung:** Das ISMS wird laufend überwacht und weiterentwickelt, um auf neue Cyberbedrohungen, gesetzliche Anforderungen und organisatorische Veränderungen reagieren zu können.

Anhang A der ISO 27001: Maßnahmenkatalog

Der [Anhang A der ISO 27001:2022](#) enthält eine Liste von Maßnahmen, die dazu dienen, Sicherheitsrisiken zu behandeln. Unternehmen können diese Maßnahmen als Leitfaden nutzen, um ihre spezifischen Risiken zu bewältigen und ein starkes Sicherheitsmanagement zu etablieren. Die Maßnahmen sind in einzelne Kategorien unterteilt:

- Organisatorische Maßnahmen
- Personenbezogene Maßnahmen
- Physische Maßnahmen
- Technologische Maßnahmen

Grundbegriffe der ISO 27001 einfach erklärt

Um die ISO 27001 Inhalte und Anforderungen richtig zu verstehen und anzuwenden, ist es wichtig, einige grundlegende Begriffe zu kennen. Die nachfolgenden Begriffe bilden die Grundlage für das Verständnis und die Umsetzung der ISO/IEC 27001. Sie helfen dabei, die Normanforderungen klar zu definieren und sicherzustellen, dass alle Aspekte der Informationssicherheit systematisch angegangen werden.

Begriff	Kurzdefinition nach ISO 27001
Informationssicherheitsmanagementsystem (ISMS)	Systematischer Rahmen zur Planung, Umsetzung und Verbesserung der Informationssicherheit im Unternehmen.
Informationssicherheit	Schutz von Informationen zur Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit.
Schutzziele Vertraulichkeit	Zugriff auf Informationen nur für befugte Personen.
Integrität	Schutz vor unbefugter Veränderung oder Manipulation von Daten.
Verfügbarkeit	Informationen und Systeme sind bei Bedarf zugänglich.

Begriff	Kurzdefinition nach ISO 27001
Risiko & Risikoanalyse	Bewertung möglicher Bedrohungen und systematische Behandlung von Informationssicherheitsrisiken.
Sicherheitsmaßnahmen	Organisatorische oder technische Maßnahmen zur Reduzierung von Risiken.
Sicherheitsrichtlinie	Dokumentierte Grundsätze und Regeln zur Informationssicherheit.
Interessierte Parteien	Personen oder Organisationen mit Anforderungen an die Informationssicherheit.
Interne Audits	Interne Prüfung der Wirksamkeit und Normkonformität des ISMS.
Management-Review	Regelmäßige Bewertung des ISMS durch die Geschäftsleitung.
Nichtkonformität & Maßnahmen	Abweichung von Anforderungen sowie Korrektur- oder Präventivmaßnahmen.
Dokumentierte Information	Alle dokumentierten Nachweise und Aufzeichnungen des ISMS.

Die 27000-Familie der ISO-Normen

Die ISO 27000-Familie umfasst eine Reihe internationaler Normen, die gemeinsam den Rahmen für ein wirksames ISMS bilden. Jede Norm der ISO/IEC 27000-Reihe behandelt dabei einen spezifischen Aspekt der Informationssicherheit und ergänzt die Anforderungen der ISO 27001.

- **ISO/IEC 27000 – Grundlagen und Begriffe**
Diese Norm liefert die zentralen Definitionen, Fachbegriffe und Grundlagen der Informationssicherheit. Sie dient als Referenzdokument für alle weiteren Normen der ISO-27000-Reihe und sorgt für ein einheitliches Verständnis der Terminologie.
- **ISO/IEC 27001 – Anforderungen an das ISMS**
Die ISO 27001 bildet den Kern der gesamten Normenfamilie. Sie definiert die Anforderungen an Aufbau, Umsetzung und kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems und ist die einzige Norm der Reihe, die zertifizierbar ist.
- **ISO/IEC 27002 – Leitfaden für Sicherheitsmaßnahmen**
Diese Norm ergänzt die ISO 27001 um praktische Empfehlungen und konkrete Maßnahmen zur Informationssicherheit.
- **ISO/IEC 27005 – Risikomanagement in der Informationssicherheit**
Die ISO 27005 beschreibt detailliert den Risikomanagement-Prozess, der im Rahmen eines ISMS erforderlich ist. Sie liefert Methoden und Vorgehensweisen zur Identifikation, Bewertung und Behandlung von Risiken.

Video: Die Standards der ISO/IEC 27000 Reihe im Überblick

In diesem Video erhalten Sie einen Überblick über die wichtigsten Standards der ISO/IEC 27000 Reihe und wie sie Unternehmen helfen können ihre Informationssicherheit zu verbessern. Die Informationssicherheit wird in der heutigen Zeit immer wichtiger und Unternehmen müssen sicherstellen, dass ihre Daten und Systeme vor Bedrohungen geschützt sind. Einen auf international anerkannten Standards basierenden Rahmen dafür bildet die ISO/IEC 27000 Reihe.



Inhalte dieses Videos:

- Bestandteile der ISO 27001
- Bestandteile der ISO 27006
- Bestandteile weiterer informativer Normen
- Begriffsnorm – Abschnitt 5.2
- Anforderungsnormen – Abschnitt 5.3
- Leitfadennormen – Abschnitt 5.4
- Sektorenspezifische Leitfadennormen – Abschnitt 5.5
- Maßnahmenbezogene Leitfadennormen

Die Zertifizierung nach ISO 27001

Sobald das Informationssicherheitsmanagementsystem erfolgreich implementiert wurde, kann das Unternehmen die ISO 27001 Zertifizierung anstreben. Hierzu führt eine unabhängige Zertifizierungsstelle ein externes Audit durch. Dabei wird geprüft, ob das ISMS den ISO 27001 Anforderungen gerecht wird. Besteht das Unternehmen dieses Audit, erhält es das ISO 27001 Zertifikat, das in der Regel drei Jahre gültig ist. Während dieser Zeit finden jährliche Überwachungsaudits statt, um sicherzustellen, dass das ISMS weiterhin den Anforderungen entspricht und kontinuierlich verbessert wird. Nach Ablauf des Zertifikats erfolgt ein Rezertifizierungsaudit, mit dem die Gültigkeit des Zertifikats um weitere drei Jahre verlängert werden kann.

Zukunft der Informationssicherheit

Das große Stichwort lautet: **KI**. Die Zukunft der Informationssicherheit und Cybersecurity wird zunehmend von KI, automatisierten Angriffen und strengeren Regulierungen geprägt. Angreifer setzen zunehmend auf KI-gesteuerte Phishing-Angriffe, Deepfakes und Schadsoftware ([Google Threat Intelligence 2025](#)).


Aktuelle Analysen, wie etwa von [McKinsey](#) zeigen: KI ist zugleich die größte Bedrohung und die stärkste Verteidigung in der Cybersecurity. Während Angreifer KI nutzen, um Angriffe realistischer, schneller und schwerer erkennbar zu machen, eröffnet dieselbe Technologie enorme Chancen für Unternehmen, ihre Abwehr zu stärken.

Für Unternehmen bedeutet das: Investieren Sie jetzt in proaktive Sicherheitsstrategien und schulen Sie Ihre Mitarbeiter, um auf die kommende Entwicklung in der Informationssicherheit vorbereitet zu sein.

Ihre ISO 27001 Schulungen bei der VOREST AG - die Basis für ein wirksames ISMS


Um auch in Zukunft auf die Entwicklung in der Informationssicherheit vorbereitet zu sein, braucht es fundiertes Wissen und ein gemeinsames Verständnis für die Anforderungen der ISO 27001. Eine professionelle [Ausbildung im Informationssicherheitsmanagement nach ISO 27001](#) schafft dafür die optimale Grundlage. Die VOREST AG begleitet Sie als erfahrener Weiterbildungspartner bei der Einführung, Umsetzung und kontinuierlichen Verbesserung Ihres ISMS. Wir bieten Ihnen die Möglichkeit, sich vom Grundlagenwissen bis hin zum Informationssicherheitsbeauftragten weiterzubilden.


Sie wünschen sich ein extra auf Ihre Bedürfnisse ausgerichtetes Seminar zur ISO/IEC 27001 und deren Prozesse in Ihrem Unternehmen? Mit unseren [Informationssicherheitsmanagement Inhouse Schulungen](#) kommen wir zu Ihnen und schulen Sie zu Ihrem Wunschthema. Wir stehen dabei auch gerne beratend zur Seite – sprechen Sie uns einfach an.

- 

Kostenloser E-Learning Kurs - Was ist ein ISMS nach ISO 27001?



★ Kostenloser E-Learning Kurs zum Informationssicherheitsmanagement mit erstem Überblick über die Bedeutung eines ISMS sowie über die Funktionsweise und Ziele der Norm ISO 27001.


 Preis: 0,00 € | Kursformat: E-Learning

[zum Kurs »](#)
- 

Basiswissen ISMS ISO 27001



1 Grundlagen Kurs zu den Inhalten und Forderungen der Norm DIN EN ISO/IEC 27001 für Informationssicherheitsmanagementsysteme und zur Einführung & Zertifizierung eines ISMS.


 Preis: 1099,00 € | Kursformat: Präsenz  Preis: 1044,05 € | Kursformat: Virtual-Classroom

[zum Kurs »](#)
- 

Interner Auditor ISO 27001



2 Schulung zur Vorbereitung, Durchführung und Nachbereitung von internen Audits nach ISO 19011 im Informationssicherheitsmanagementsystem nach ISO 27001 - **Abschluss mit Zertifikat**.


 Preis: 1099,00 € | Kursformat: Präsenz  Preis: 1044,05 € | Kursformat: Virtual-Classroom

[zum Kurs »](#)
- 

Informationssicherheitsbeauftragter - ISMS Beauftragter ISO 27001



3 Ausbildung zur Rolle und den Aufgaben des ISMS-Beauftragten ISO 27001 mit Qualifikation zur Betreuung & Weiterentwicklung eines Informationssicherheitsmanagementsystems - **Abschluss mit Zertifikat**.


 Preis: 1299,00 € | Kursformat: Präsenz  Preis: 1234,05 € | Kursformat: Virtual-Classroom

[zum Kurs »](#)
- 

Informationssicherheitsmanagement Auditor / Leitender Auditor ISO 27001

4 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**.

 Preis: 2599,00 € | Kursformat: Präsenz  Preis: 2469,05 € | Kursformat: Virtual-Classroom

[zum Kurs »](#)
- 

Kostenloser Gesamtkatalog der VOREST AG zum Download

+ Gesamtkatalog der VOREST AG mit allen Schulungen rund um Managementsysteme, Prozessoptimierung und Methoden zum kostenlosen Download.

[Download »](#)

Sie wissen noch nicht, welcher Kurs der richtige ist?

Fragen zu Formaten, Förderung oder Inhalten?



Sevil Kaya

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



Katharina Reutter

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

■ **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.

