WHITEPAPER

ISO/IEC 27001:2022

Der Weg zum zertifizierten ISMS

Aktuelle rechtliche Grundlagen, Zertifizierungsprozess und Praxis in Österreich und Deutschland

Für Entscheider in KMU

Pragmatischer Leitfaden mit klaren Empfehlungen

Stand: Mai 2026

Herausgeber: Datenschutz Kroes, Alexander Kroes e.U.

Inhaltsverzeichnis

Klicken Sie auf einen Eintrag, um direkt zum jeweiligen Kapitel zu springen. Funktioniert in PDF und Word.

Auf einen Blick

Dieses Whitepaper richtet sich an Geschäftsführer, kaufmännische Leiter und IT Verantwortliche kleiner und mittlerer Unternehmen, die wissen wollen, was ISO 27001 in der aktuellen Fassung von 2022 konkret fordert, welcher Aufwand realistisch ist und wie sich die Praxis in Österreich und Deutschland unterscheidet.

Es ersetzt keine individuelle Prüfung, liefert aber die rechtliche Basis, den Maßnahmenkatalog, den Zertifizierungsablauf und die Aufwandskalkulation, um die Diskussion in der Geschäftsleitung fundiert zu führen.

> **Lesehinweis**
> Wer es eilig hat, liest Kapitel 1, 3 und 6. Das genügt, um die Norm und die Besonderheiten in AT und DE einzuordnen. Wer entscheiden will, ergänzt Kapitel 7 bis 10. Wer umsetzen will, liest das gesamte Dokument.

1. Was ist ISO/IEC 27001

ISO/IEC 27001 ist der international führende Standard für Informationssicherheits Management Systeme, kurz ISMS. Herausgegeben von der International Organization for Standardization gemeinsam mit der International Electrotechnical Commission, definiert die Norm die Anforderungen an Aufbau, Betrieb, Überwachung und kontinuierliche Verbesserung eines ISMS.

Der vollständige Titel der aktuellen Fassung lautet ISO/IEC 27001:2022 Informationssicherheit, Cybersicherheit und Datenschutz, Informationssicherheits Management Systeme, Anforderungen. Der Zusatz Cybersicherheit und Datenschutz ist neu gegenüber 2013 und spiegelt die Verzahnung mit DSGVO und Cyber Compliance wider.

Begriffe, die häufig verwechselt werden

- ISO/IEC 27001, internationale Originalbezeichnung.
- DIN EN ISO/IEC 27001, deutsche Übernahme des internationalen Standards. Inhaltlich identisch.
- ÖNORM EN ISO/IEC 27001, österreichische Übernahme. Ebenfalls inhaltlich identisch.
- ISO 27001, Kurzform. In der Praxis am häufigsten verwendet.

Wer im Vertragstext oder in einer Ausschreibung eine der oben genannten Bezeichnungen findet, kann sicher sein, dass dieselbe Norm gemeint ist. Eine Zertifizierung nach ISO 27001 ist international und in beiden Ländern dieselbe.

Die drei Schutzziele der Informationssicherheit

- Vertraulichkeit. Informationen sind nur für Berechtigte zugänglich.
- Integrität. Informationen bleiben unverfälscht und vollständig.
- Verfügbarkeit. Informationen stehen dann zur Verfügung, wenn sie gebraucht werden.

ISO 27001 macht diese drei Ziele zum messbaren System. Sie bewertet jedes Informationsasset und jeden Prozess gegen diese Ziele und definiert konkrete Maßnahmen für den Fall, dass die Risiken zu hoch sind.

2. Warum jetzt, die aktuellen Treiber

ISO 27001 war bis vor wenigen Jahren ein Thema für Konzerne, Banken und Behörden. Diese Zeit ist vorbei. Vier Treiber schieben die Norm in den Mittelstand und in inhabergeführte Unternehmen.

Treiber 1, Regulatorischer Druck durch NIS 2

Die EU NIS 2 Richtlinie ist in beiden Ländern in nationales Recht überführt. Der Maßnahmenkatalog des Gesetzes orientiert sich erkennbar an ISO 27001. Wer ein zertifiziertes ISMS betreibt, erfüllt nach übereinstimmender Einschätzung der Praxis 65 bis 80 Prozent der NIS 2 Anforderungen ohne Zusatzaufwand. Wer kein ISMS hat, baut faktisch ein solches auf, nur ohne Zertifikat.

Treiber 2, Anforderung in der Lieferkette

Über 60 Prozent der Top 1000 Unternehmen im DACH Raum verlangen von strategischen Lieferanten den Nachweis einer ISO 27001 Zertifizierung. Entweder direkt vertraglich oder über ergänzende IT Sicherheits Klauseln. ISO 27001 ist damit für mittelständische B2B Anbieter eine Markteintrittsbarriere geworden, kein Bonus.

Treiber 3, Versicherung und Risiko

Cyber Versicherer setzen ein funktionierendes ISMS oder einen vergleichbaren Nachweis voraus. Ohne Nachweis sinken Deckungssumme und Vertragsbedingungen oder die Police entfällt. Die persönliche Haftung der Geschäftsleitung für Cybersicherheit ist mit NIS 2 explizit gesetzlich verankert. Ein zertifiziertes ISMS ist hier der sauberste Entlastungsnachweis.

Treiber 4, DSGVO und technisch organisatorische Maßnahmen

Art. 32 DSGVO verlangt geeignete technische und organisatorische Maßnahmen, kurz TOM, im Stand der Technik. Die Aufsichtsbehörden, sowohl die österreichische Datenschutzbehörde als auch die deutschen Landesdatenschutzbehörden, akzeptieren ISO 27001 als anerkannten Nachweis. Eine bestehende Zertifizierung verkürzt die Diskussion mit der Behörde im Schadensfall erheblich.

> **Kernaussage**
> Wer ab 2026 in einer regulierten Branche oder als B2B Zulieferer arbeitet, kommt um ein ISMS faktisch nicht mehr herum. Die Frage ist nicht mehr ob, sondern ob mit oder ohne formales Zertifikat.

3. ISO 27001:2022, die aktuelle Version

Die ISO/IEC 27001:2022 wurde am 25. Oktober 2022 veröffentlicht und ersetzt die Vorgängerversion von 2013. Die dreijährige Übergangsfrist endete am 31. Oktober 2025. Seit diesem Stichtag ist die 2022er Fassung die einzige zertifizierungsfähige Basis. Akkreditierte Zertifizierungsstellen dürfen keine Audits mehr nach der alten Norm durchführen.

Wichtiger Hinweis zum Stichtag

Zertifikate nach ISO 27001:2013 sind seit dem 1. November 2025 ungültig. Wer die Übergangsfrist verpasst hat, kann keine reine Transition mehr machen, sondern muss eine vollständige Neuzertifizierung mit Stage 1 und Stage 2 Audit nach der 2022er Fassung durchlaufen. Dauer realistisch vier bis acht Monate, Kosten Faktor 1,5 bis 2,0 gegenüber regulärer Re-Zertifizierung.

Die wesentlichen Änderungen 2022 gegenüber 2013

Aspekt	ISO 27001:2013	ISO 27001:2022
Anzahl Controls im Annex A	114 Controls	93 Controls
Strukturierung Annex A	14 Kategorien	4 Themengebiete
Neue Controls	Keine	11 neue Controls
Normstruktur Hauptklauseln	10 Klauseln	10 Klauseln, identische Struktur, HLS
Datenschutz im Titel	Nein	Ja, Cybersicherheit und Datenschutz neu im Titel
Änderungsmanagement	Standard	Verschärfte operative Anforderungen

Die elf neuen Controls

Die elf neuen Controls adressieren aktuelle Bedrohungslagen, die in der 2013er Fassung nicht oder nur am Rand abgebildet waren.

- Threat Intelligence, also Bedrohungsanalyse, A.5.7.
- Informationssicherheit für Cloud Dienste, A.5.23.
- Bereitschaft der IKT für Business Continuity, A.5.30.
- Physische Sicherheits Überwachung, A.7.4.
- Konfigurationsmanagement, A.8.9.

- Löschung von Informationen, A.8.10.
- Daten Maskierung, A.8.11.
- Data Leakage Prevention, A.8.12.
- Überwachungstätigkeiten, A.8.16.
- Web Filterung, A.8.23.
- Sichere Coding Praktiken, A.8.28.

Unternehmen, die ihr ISMS auf 2022 aktualisiert haben, decken damit Cloud Security, Threat Intelligence und Data Masking explizit ab. Genau diese Bereiche sind in der NIS 2 Pflichtliste enthalten.

4. Aufbau der Norm

ISO 27001:2022 besteht aus zwei eng verzahnten Teilen. Beide Teile sind verbindlich und prüfungsrelevant.

Teil 1, die Hauptklauseln 4 bis 10

Die Hauptklauseln folgen der harmonisierten High Level Structure, die auch ISO 9001 und ISO 14001 verwenden. Wer bereits ein Qualitäts oder Umweltmanagement System betreibt, kann ISO 27001 leichter integrieren.

Klausel	Inhalt	Kernanforderung
4 Kontext	Geltungsbereich und interessierte Parteien	Scope schriftlich definieren
5 Führung	Verpflichtung und Verantwortung der Leitung	Politik verabschieden, Rollen zuweisen
6 Planung	Risiken, Chancen und Ziele	Risikomethodik festlegen
7 Unterstützung	Ressourcen, Kompetenz, Bewusstsein, Doku	Awareness und Dokumentation aufbauen
8 Betrieb	Planung und Steuerung der Maßnahmen	Risikobehandlung umsetzen
9 Bewertung	Überwachung, Audits, Management Bewertung	Jährliches internes Audit, Management Review
10 Verbesserung	Nichtkonformitäten und kontinuierliche Verbesserung	Korrekturmaßnahmen dokumentieren

Teil 2, der Annex A

Der Annex A enthält 93 Sicherheits Controls, die in vier Themengebieten gruppiert sind. Die Auswahl, welche Controls für das eigene Unternehmen anwendbar sind, erfolgt im Statement of Applicability. Nicht zutreffende Controls dürfen ausgeschlossen werden, der Ausschluss muss aber begründet sein.

5. Die 93 Controls in vier Themengebieten

Die 2022er Fassung gruppiert die Controls erstmals nach inhaltlicher Logik, statt nach Bereich. Das vereinfacht die Zuordnung zu anderen Standards wie NIS 2, DORA oder TISAX deutlich.

Themengebiet	Anzahl Controls	Beispiel Themen
A.5 Organisatorische Controls	37	Policies, Rollen, Lieferanten, Vorfallsmanagement, Threat Intelligence, Cloud
A.6 Personenbezogene Controls	8	Hintergrundprüfung, Awareness, Geheimhaltung, Disziplinarverfahren
A.7 Physische Controls	14	Zutritt, Bauliche Sicherung, Schreibtischordnung, Überwachung
A.8 Technologische Controls	34	Zugangskontrolle, Kryptographie, Backup, Logging, Coding, Web Filter

Wichtig zur Auswahl

Nicht jeder Control trifft auf jedes Unternehmen zu. Ein reiner Dienstleister ohne eigene Produktion wird zum Beispiel Coding Controls nur eingeschränkt anwenden. Wesentlich ist, dass jeder Nichtanwendungsfall im Statement of Applicability schriftlich begründet wird.

Statement of Applicability als Herzstück

Das Statement of Applicability, kurz SoA, ist das zentrale Dokument der Zertifizierung. Es listet alle 93 Controls auf, zeigt für jeden Control ob anwendbar oder nicht, mit Begründung, und verweist auf die konkreten Umsetzungsmaßnahmen. Im Audit ist das SoA das erste Dokument, das der Auditor verlangt.

6. Unterschiede zwischen Österreich und Deutschland

Die Norm selbst ist international und in beiden Ländern identisch. Unterschiede gibt es bei den Akkreditierungs und Zertifizierungsstrukturen, beim begleitenden nationalen Recht und bei ergänzenden nationalen Standards. Die folgenden Punkte sind in der Praxis am häufigsten entscheidungsrelevant.

6.1 Akkreditierungsstelle

Wer akkreditiert die Zertifizierungsstellen?

AT **Österreich**

Akkreditierung Austria, angesiedelt im Bundesministerium für Arbeit und Wirtschaft. Eine Akkreditierungsstelle für alle Branchen und Normen. Zentrale Anlaufstelle in Wien.

DE **Deutschland**

Deutsche Akkreditierungsstelle, kurz DAkkS, mit Sitz in Berlin. Bundesweit zuständig, mehrere Außenstellen. Größerer Markt mit deutlich mehr akkreditierten Zertifizierungsstellen.

6.2 Marktrelevante Zertifizierungsstellen

Bei wem zertifiziere ich konkret?

AT **Österreich**

Marktführer in Österreich sind Quality Austria, CIS Certification and Information Security Services, TÜV Austria Cert und TÜV SÜD Landesgesellschaft Österreich. Auch die Österreichische Computer Gesellschaft, kurz OCG, ist aktiv. Ausländische, im EWR akkreditierte Stellen können in Österreich ebenfalls zertifizieren.

DE **Deutschland**

Im deutschen Markt führend sind TÜV Süd, TÜV Nord, TÜV Rheinland, DEKRA, DQS und GUTcert. Weitere Anbieter wie Bureau Veritas oder SGS sind ebenfalls präsent. Die Auswahl ist deutlich größer als in Österreich, die Preise dadurch tendenziell etwas niedriger.

6.3 Nationale Ergänzungsstandards

Welche nationalen Standards ergänzen ISO 27001?

AT **Österreich**

Die ÖNORM A 7700 ist eine ältere österreichische Norm zur Informationssicherheit, in der Praxis durch ISO 27001 abgelöst. Austrian Standards veröffentlicht ergänzende Leitlinien, eine eigenständige Pflichtmethodik wie der BSI Grundschutz existiert nicht.

DE **Deutschland**

Der BSI IT Grundschutz ist eine eigenständige Methodik des Bundesamts für Sicherheit in der Informationstechnik. Er ist mit ISO 27001 kombinierbar in der Variante ISO 27001 auf Basis IT Grundschutz. Diese Kombination ist in der öffentlichen Verwaltung und bei KRITIS Betreibern oft Pflicht. Für KMU im freien Markt meist nicht erforderlich.

6.4 Verzahnung mit dem nationalen NIS 2 Recht

Wie verzahnt sich ISO 27001 mit NIS 2?

AT **Österreich**

Das österreichische Netz und Informationssystemsicherheitsgesetz 2026, kurz NISG 2026, tritt am 1. Oktober 2026 in Kraft. Die zuständige Behörde ist das neue Bundesamt für Cybersicherheit im Innenministerium. Registrierung bis 31. Dezember 2026, Selbstdeklaration binnen zwölf Monaten nach Registrierungspflicht. Eine bestehende ISO 27001 Zertifizierung deckt 70 bis 80 Prozent der NISG 2026 Anforderungen ab.

DE **Deutschland**

Das NIS 2 Umsetzungs und Cybersicherheitsstärkungsgesetz, kurz NIS2UmsuCG, ist seit dem 6. Dezember 2025 in Kraft, ohne Übergangsfrist. Pflichten ab Tag eins. Aufsichtsbehörde ist das Bundesamt für Sicherheit in der Informationstechnik, kurz BSI. Registrierung im MUK Portal mit ELSTER Zertifikat. Eine bestehende ISO 27001 Zertifizierung deckt ebenfalls 70 bis 80 Prozent der Anforderungen ab, ergänzt um die BSI spezifischen Pflichten.

6.5 Datenschutzaufsicht und ISO 27001

Wie bewertet die Datenschutzbehörde eine ISO Zertifizierung?

AT **Österreich**

Die österreichische Datenschutzbehörde, DSB, akzeptiert ISO 27001 als anerkannten Nachweis der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO. Eine bestehende Zertifizierung wirkt im Verfahren milderungswirksam und verkürzt die Diskussion bei Datenpannen.

DE **Deutschland**

Die Landesdatenschutzbehörden, jeweils zuständig nach Sitz des Unternehmens, akzeptieren ISO 27001 ebenfalls als anerkannten TOM Nachweis. Speziell für Bayern hat das Bayerische Landesamt für Datenschutzaufsicht, BayLDA, mehrfach öffentlich auf den Wert einer Zertifizierung hingewiesen.

6.6 Sprachfassung und Vertragsfragen

In welcher Sprachfassung gilt die Norm?

AT **Österreich**

ÖNORM EN ISO/IEC 27001:2022, deutschsprachige Übernahme durch Austrian Standards. Inhaltlich identisch mit der internationalen Originalfassung. Zertifikate gelten EU weit.

DE **Deutschland**

DIN EN ISO/IEC 27001:2022, deutschsprachige Übernahme durch das Deutsche Institut für Normung. Inhaltlich identisch mit der internationalen Originalfassung. Zertifikate gelten EU weit.

Praxisempfehlung für grenzüberschreitend tätige KMU

Wer in beiden Ländern Mandanten oder Standorte hat, lässt sich einmal nach ISO 27001 zertifizieren, vorzugsweise bei einer Zertifizierungsstelle mit Akkreditierung in beiden Ländern. Das Zertifikat gilt EU weit und wird beidseitig anerkannt. Eine doppelte Zertifizierung ist nicht erforderlich. Lediglich die ergänzenden NIS 2 Pflichten müssen für jeden Standort national gesondert erfüllt werden.

7. Verzahnung mit anderen Standards

Eine ISO 27001 Zertifizierung ist selten Selbstzweck. In der Praxis ist sie die Compliance Wirbelsäule, an die sich weitere Anforderungen anlehnen. Die Abdeckungsgrade sind empirisch belegt und unterscheiden sich nach Standard.

Standard oder Rahmen	Abdeckung durch ISO 27001	Zusätzlicher Aufwand
NIS 2 in AT und DE	65 bis 80 Prozent	Registrierung, Meldeverfahren, Geschäftsleitungspflichten ergänzen
DSGVO TOM nach Art. 32	Hoch, anerkannt als Nachweis	VVT und DSFA bleiben außerhalb von ISO 27001
TISAX im Automotive	circa 75 Prozent	Prototypenschutz und Branchenanforderungen ergänzen
DORA für Finanzbranche	Grundlage	IKT Drittparteienrisiko und Resilienztests ergänzen
BSI IT Grundschutz	Kombinierbar	Bausteinkatalog zusätzlich umsetzen
ISO 9001 Qualität	Strukturidentisch	Inhaltlich getrennt, aber leicht integrierbar

Strategischer Hebel

Wer ISO 27001 als Compliance Wirbelsäule aufbaut, erfüllt NIS 2 mit 65 bis 80 Prozent Abdeckung, erreicht TISAX in sechs bis acht Wochen statt zwölf bis sechzehn Wochen, und liefert der Datenschutzaufsicht einen anerkannten TOM Nachweis. Eine Plattform, mehrere Compliance Ziele.

8. Der Zertifizierungsprozess

Der Weg zur Erstzertifizierung folgt einem etablierten Ablauf. Die Schritte sind in beiden Ländern identisch, die Akteure sind landesspezifisch.

Phase	Inhalt	Dauer Richtwert
1. Readiness Check	Reifegradanalyse durch Berater oder Zertifizierungsstelle	1 bis 2 Wochen
2. ISMS Aufbau	Scope, Risikomanagement, SoA, Dokumentation, Awareness	4 bis 8 Monate
3. Internes Audit	Wirksamkeitsprüfung und Korrekturmaßnahmen	3 bis 4 Wochen
4. Management Review	Bewertung und Freigabe durch die Geschäftsleitung	1 bis 2 Wochen
5. Stage 1 Audit	Dokumentenprüfung durch externe Zertifizierungsstelle	1 bis 3 Tage vor Ort
6. Stage 2 Audit	Wirksamkeitsprüfung vor Ort, Hauptaudit	3 bis 8 Tage vor Ort
7. Zertifikatsausstellung	Nach erfolgreichem Stage 2, gültig 3 Jahre	2 bis 4 Wochen
8. Überwachungsaudits	Jährlich, reduzierter Umfang	1 bis 3 Tage jährlich
9. Re Zertifizierung	Vollaudit nach 3 Jahren	3 bis 6 Tage

Drei Jahres Zyklus im Überblick

Das Zertifikat ist drei Jahre gültig. In den beiden Folgejahren findet jeweils ein Überwachungsaudit statt, das den Fortbestand des ISMS prüft. Nach Ablauf der drei Jahre erfolgt ein Vollaudit mit erneuter Zertifizierung. Wer ein Audit verpasst oder gravierende Abweichungen nicht behebt, verliert das Zertifikat. Nachzertifizierung ist dann nicht möglich, es bedarf einer Neuzertifizierung.

Partielle Zertifizierung

Der Geltungsbereich kann nach Klausel 4.3 auf bestimmte Standorte, Abteilungen oder IT Systeme begrenzt werden. Das Zertifikat gilt dann nur für diesen Scope. In der Praxis sinnvoll, wenn nur Teile des Unternehmens einer regulatorischen Anforderung unterliegen oder wenn der Aufbau schrittweise erfolgen soll.

9. Kosten und Zeitaufwand

Die Kosten einer Erstzertifizierung schwanken stark nach Unternehmensgröße, Komplexität des Scope und Vorzertifizierungsstand. Die folgenden Richtwerte basieren auf Marktdurchschnitten im DACH Raum und sind als Orientierung zu verstehen, nicht als Festpreis.

Unternehmensgröße	Erstzertifizierung gesamt	Davon externe Auditkosten
KMU bis 25 Mitarbeiter	25.000 bis 45.000 EUR	4.000 bis 8.000 EUR
KMU 25 bis 100 Mitarbeiter	45.000 bis 80.000 EUR	8.000 bis 14.000 EUR
Mittelstand 100 bis 500	80.000 bis 180.000 EUR	14.000 bis 28.000 EUR
Mittelstand 500 bis 1000	180.000 bis 250.000 EUR	28.000 bis 45.000 EUR
Konzerne über 1000	individuell, ab 250.000 EUR	45.000 EUR aufwärts

Kostenkomponenten im Detail

- Externe Beratung beim Aufbau, Tagessätze 1.300 bis 1.900 EUR netto, je nach Spezialisierung.
- Interne Personalkosten, häufig der größte Posten, abhängig von der bereitgestellten Kapazität.
- Audit Kosten, Stage 1 und Stage 2, abhängig von Mitarbeiterzahl und Standorten.
- Tool und Software Lizenzen, falls eine ISMS Plattform eingeführt wird, ab 10.000 EUR jährlich.
- Awareness und Schulungen, in der Regel 2.000 bis 8.000 EUR initial.
- Laufende Kosten in den Folgejahren, etwa zehn bis fünfzehn Prozent der Erstkosten pro Jahr.

Zeitlicher Rahmen

- Erstzertifizierung von Null auf, sechs bis achtzehn Monate, je nach Größe und Vorzertifizierungsstand.
- Erstzertifizierung mit Vorarbeit, drei bis sechs Monate.
- Wenn die Übergangsfrist verpasst wurde, vier bis acht Monate plus Faktor 1,5 bis 2 bei den Kosten.

Realistischer Erwartungswert für ein typisches KMU

Ein KMU mit 50 Mitarbeitern, ohne nennenswerten Vorzertifizierungsstand, sollte mit zwölf bis fünfzehn Monaten Projektdauer und Gesamtkosten zwischen 50.000 und 70.000 EUR rechnen, externe Beratung eingeschlossen.

10. Umsetzungsfahrplan

Der praxisbewährte Fahrplan für ein KMU folgt sieben Phasen, die sich über sechs bis zwölf Monate erstrecken. Die Phasen können überlappend laufen, sollten aber nicht parallel gestartet werden.

Phase 1, Vorbereitung und Scope

- Geschäftsleitung verpflichtet sich schriftlich zum ISMS Projekt.
- Projektleitung benennen, idealerweise mit direkter Berichtsfunktion an die Geschäftsleitung.
- Scope definieren, Standorte, Prozesse, IT Systeme.
- Zertifizierungsstelle ausschreiben und vorauswählen.

Phase 2, GAP Analyse

- Ist Aufnahme gegen die Norm, Reifegradbewertung pro Klausel und pro Control.
- Priorisierter Maßnahmenplan mit Zeitachse und Verantwortlichkeiten.

Phase 3, Risikomanagement und SoA

- Asset Register aufbauen, jedes Informationsasset mit Eigentümer und Klassifizierung.
- Risikoanalyse durchführen, Bedrohungen und Schwachstellen je Asset bewerten.
- Behandlungsplan ableiten, Statement of Applicability erstellen.

Phase 4, Dokumentation und Maßnahmen

- Informationssicherheits Leitlinie verabschieden.
- Verfahrensanweisungen, Arbeitsanweisungen, Vorlagen erstellen.
- Technische und organisatorische Maßnahmen umsetzen.
- Awareness Schulungen für alle Mitarbeiter durchführen.

Phase 5, Internes Audit und Management Review

- Wirksamkeitsprüfung durch interne oder externe Auditoren.
- Korrekturmaßnahmen für identifizierte Abweichungen.
- Management Bewertung, dokumentiert in einem Protokoll mit Unterschrift.

Phase 6, Externes Audit

- Stage 1 Audit, Dokumentenprüfung.
- Mögliche Lücken vor Stage 2 schließen.
- Stage 2 Audit, Vor Ort Prüfung.
- Korrekturmaßnahmen bei Findings.

Phase 7, Zertifikat und laufender Betrieb

- Zertifikatsausstellung.
- Übergang in den laufenden Betrieb mit jährlichen Überwachungsaudits.
- Kontinuierliche Verbesserung über Lessons Learned, KPI Monitoring und Awareness Maßnahmen.

11. Die häufigsten Stolperfallen

Aus der Praxis von Aufbauprojekten in KMU wiederholen sich diese Muster. Wer sie kennt, spart Zeit, Geld und Audit Findings.

Falle 1, Scope zu groß gewählt

Der Geltungsbereich wird am Anfang zu breit definiert, alle Standorte, alle Töchter, alle Prozesse. Folge, das Projekt schafft die Erstzertifizierung in zwölf Monaten nicht. Klüger ist ein eng definierter Scope mit klarem Erweiterungsplan in den Folgejahren.

Falle 2, ISMS als IT Projekt missverstanden

Die Geschäftsleitung delegiert an die IT, die IT delegiert an einen einzelnen IT Mitarbeiter. Folge, im Audit fällt durch, dass kritische Themen wie Awareness, Lieferantenmanagement und Notfallplanung im Unternehmen nicht verankert sind. ISO 27001 ist Managementverantwortung, nicht IT Verantwortung.

Falle 3, Risikomanagement nur einmal durchgeführt

Die Risikoanalyse wird zu Projektbeginn erstellt und dann abgeheftet. Bei der Re Zertifizierung nach drei Jahren ist sie veraltet. Risiken müssen mindestens jährlich überprüft und nach jeder wesentlichen Änderung im Unternehmen aktualisiert werden.

Falle 4, SoA unsauber gepflegt

Das Statement of Applicability listet alle Controls auf, aber Begründungen für Nichtanwendung fehlen oder sind pauschal. Ein guter Auditor erkennt das in fünf Minuten. Folge sind Findings, die das Audit verzögern.

Falle 5, Awareness auf E Learning reduziert

Jährliches Online Training mit Klickstrecke schafft kein Sicherheitsbewusstsein. Phishing Simulationen, fallbasierte Schulungen und Vorbildfunktion der Führung sind nicht verhandelbar. Auditoren prüfen Awareness gezielt durch Interviews mit zufällig ausgewählten Mitarbeitern.

Falle 6, Lieferanten unterschätzt

Lieferantenmanagement nach Annex A wird oft auf das Vorhandensein eines AVV reduziert. Ein guter Auditor verlangt eine systematische Bewertung der Lieferantenrisiken, regelmäßige Reviews und Vor Ort Audits bei kritischen Dienstleistern.

Falle 7, Übergangsfrist verschlafen

Wer als Bestandszertifikatsinhaber die Frist zum 31. Oktober 2025 verpasst hat, kann nicht mehr nachzertifizieren, sondern braucht eine vollständige Neuzertifizierung. Aufwand und Kosten steigen um Faktor 1,5 bis 2.

12. Wie Datenschutz Kroes unterstützt

Datenschutz Kroes begleitet KMU bei Aufbau, Betrieb und Zertifizierung eines ISMS nach ISO 27001:2022. Der Ansatz ist pragmatisch, dokumentenorientiert und auf Audit Reife ausgerichtet, nicht auf theoretische Vollständigkeit.

Leistungsspektrum

- ISO 27001 Quick Check, strukturierte Reifegradanalyse Ihres aktuellen Stands gegen die 2022er Fassung.
- GAP Analyse mit priorisiertem Maßnahmenplan und realistischer Zeitachse.
- Aufbau und Dokumentation des kompletten ISMS, von Leitlinie bis Statement of Applicability.
- Risikomanagement Methodik, Asset Register, Risikobewertungsmatrix, Behandlungsplan.
- Vorbereitung und Begleitung des Stage 1 und Stage 2 Audits durch akkreditierte Stellen.
- Begleitung im laufenden Betrieb, Überwachungsaudits, Management Reviews.
- Externer Informationssicherheits Beauftragter im Retainer Modell.
- Verzahnung mit Datenschutz Beauftragter Leistung und NIS 2 Pflichten in einem integrierten Compliance Konzept.

Warum Datenschutz Kroes

- Spezialisierung auf KMU mit zehn bis einhundert Mitarbeitern, keine Konzern Schablone.
- Festpreis Modelle, keine Stundenfallen, kalkulierbares Budget.
- Persönlicher Ansprechpartner mit Stellvertreter Regelung, keine anonymen Plattform Hotlines.
- Lokale Präsenz in Österreich und Süddeutschland, Beratung auf Deutsch und auf Augenhöhe.
- Integrierte Beratung für ISO 27001, NIS 2, DSGVO und externe DSB Funktion aus einer Hand.

13. Wie es weitergeht

Ein ISO 27001 Projekt beginnt nicht mit dem Kauf eines Tools, sondern mit einer ehrlichen Bestandsaufnahme. Wir empfehlen den folgenden Einstieg.

Schritt 1, Erstgespräch, 30 Minuten kostenfrei

Klärung der Ausgangslage, Identifikation der Treiber, Einschätzung des sinnvollen Scope, Auswahl zwischen Vollzertifizierung und schrittweisem Aufbau.

Schritt 2, ISO 27001 Quick Check

Strukturierte Reifegradanalyse Ihres aktuellen Stands gegen die 2022er Fassung. In der Regel binnen zwei bis drei Wochen. Schriftlicher Bericht mit klaren Empfehlungen, Aufwandsschätzung und Zeitachse.

Schritt 3, Angebot mit Festpreis

Verbindliches Angebot für den Aufbau Ihres ISMS, gestaffelt nach Mitarbeiterzahl und Geltungsbereich. Wahlweise als einmaliges Projekt mit klarem Ende oder als Retainer Modell mit laufender Betreuung.

Informationssicherheit mit System. Festpreis. Persönlich.

Datenschutz Kroes, Ihr Partner für ISO 27001 in AT und DE.

Rechtlicher Hinweis

Dieses Whitepaper dient der allgemeinen Information und ersetzt keine individuelle rechtliche oder beraterische Prüfung des Einzelfalls. Die dargestellten Inhalte zur ISO/IEC 27001:2022 und zu den nationalen Regelungen geben den Stand zum Erstellungsdatum wieder. Änderungen in der Normung, in Akkreditierungsregeln, in begleitenden Gesetzen und Verordnungen sowie in der Aufsichtspraxis sind möglich und können den dargestellten Inhalt überholt erscheinen lassen. Konkrete Zertifizierungs und Pflichtenprüfungen erfolgen im Rahmen eines individuellen Beratungsmandats. Eine Haftung für die Vollständigkeit und Richtigkeit der Inhalte wird im Rahmen der gesetzlichen Vorgaben übernommen.

Anbieter und Kontakt

Datenschutz Kroes

Alexander Kroes e.U.

Inhaber: Alexander Kroes

Firmensitz

(Geschäftsanschrift)

Glatzham 19

6252 Breitenbach am Inn

Österreich

Büro

(Kontaktanschrift)

Unterer Stadtplatz 11

6330 Kufstein

Österreich

Kontakt

E Mail: info@datenschutz-kroes.at

Web: https://datenschutz-kroes.at/