WHITEPAPER

Informationssicherheits-Management-System (ISMS)

Informationssicherheit für KMU in Deutschland, rechtssicher und praktisch umsetzbar

Variante Deutschland

Erstinformation für Entscheider in KMU

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 in Deutschland, die wissen wollen, was ein Informationssicherheits Management System konkret bedeutet, wofür sie es brauchen und wie ein realistischer Weg zur Einführung aussieht.

Es ersetzt kein Mandat und keine individuelle Prüfung, liefert aber das Vokabular, die Treiber und die Struktur, um die Diskussion auf Geschäftsleitungsebene fundiert führen zu können.

> **Lesehinweis**
> Wer es eilig hat, liest Kapitel 1, 2 und das Sonderkapitel zum jeweiligen Rechtsrahmen. Das genügt für die Einschätzung der Betroffenheit. Wer entscheiden will, liest auch Kapitel 6 bis 10.

1. Worum es geht in 60 Sekunden

Ein ISMS, also Informationssicherheits Management System, ist kein Tool, kein Audit und auch keine IT Lösung. Es ist ein gelebtes Steuerungssystem, das festlegt, wie ein Unternehmen mit Informationen umgeht, welche Risiken es trägt und welche Maßnahmen es nachweislich umsetzt.

Das ISMS macht messbar, was bisher Bauchgefühl war. Wer ein ISMS betreibt, kann gegenüber Kunden, Behörden, Versicherern und Geschäftsführung schriftlich belegen, dass Informationssicherheit nicht passiert, sondern gesteuert wird.

> **Kernaussage**
> Ein ISMS ist die organisatorische Klammer um alle Maßnahmen rund um Vertraulichkeit, Integrität und Verfügbarkeit von Informationen. Es liefert Struktur, Nachweise und Verbesserung in einem geschlossenen Regelkreis.

Die drei Schutzziele

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

Ein ISMS bewertet jede Information und jeden Prozess gegen diese drei Ziele und definiert konkrete Maßnahmen, sofern die Risiken zu hoch sind.

2. Warum ein ISMS heute zur Pflichtübung wird

Bis vor wenigen Jahren war Informationssicherheit ein Thema für Konzerne, Banken und kritische Infrastruktur. Diese Zeit ist vorbei. Drei Treiber schieben das ISMS in jedes mittelständische Unternehmen.

Treiber 1, Gesetz und Aufsicht

Mit dem NIS 2 Umsetzungs und Cybersicherheitsstärkungsgesetz, kurz NIS2UmsuCG, ist seit dem 6. Dezember 2025 die EU NIS 2 Richtlinie in deutsches Recht übersetzt und gilt ohne Übergangsfrist. Es ändert insbesondere das BSI Gesetz, kurz BSIG. Etwa 29.500 Unternehmen aus 18 Sektoren ab 50 Mitarbeitenden oder mehr als 10 Millionen Euro Jahresumsatz fallen in den Anwendungsbereich. Hinzu kommen die DSGVO, das Bundesdatenschutzgesetz, das KRITIS Dachgesetz seit März 2026, branchenspezifische Regelungen und die etablierten Vorgaben des BSI IT Grundschutz.

Treiber 2, Kundenanforderung in der Lieferkette

Große Auftraggeber prüfen ihre Lieferanten auf Informationssicherheit. Kein Nachweis, keine Aufträge. Die ISO 27001 Zertifizierung oder zumindest eine belastbare ISMS Selbsterklärung wird Standard in Vergaben, Ausschreibungen und Rahmenverträgen. Im Automotive Umfeld kommt zusätzlich TISAX als verbindliches Prüfschema.

Treiber 3, Risiko und Haftung

Cyberangriffe treffen Mittelstand und Kleinunternehmen in einer Härte, die früher der Großkonzerne vorbehalten war. Ransomware, CEO Fraud, Lieferketten Angriffe und Datendiebstahl verursachen Betriebsausfälle, Reputationsschäden und Bußgelder. Cyber Versicherer setzen ein funktionierendes ISMS oder eine vergleichbare Struktur inzwischen voraus, sonst sinkt die Deckungssumme oder die Police entfällt.

> **Wichtig für die Geschäftsführung**
> Die persönliche Haftung der Leitungsorgane für unzureichende Cybersicherheit ist mit den neuen Gesetzen explizit verankert. Eine Delegation ans IT Team reicht nicht. Die Geschäftsführung muss Risikomanagement aktiv überwachen und das nachweislich.

Sonderkapitel, NIS2UmsuCG in Deutschland

Das NIS 2 Umsetzungs und Cybersicherheitsstärkungsgesetz ist seit dem 6. Dezember 2025 in Kraft und gilt ohne Übergangsfrist. Die wesentlichen Pflichten finden sich im neuen BSI Gesetz, insbesondere in den Paragraphen 28, 30, 32, 38 und 65.

Wer fällt unter das NIS2UmsuCG

- Besonders wichtige Einrichtungen ab 250 Mitarbeitenden oder mehr als 50 Millionen Euro Umsatz und mehr als 43 Millionen Euro Bilanz in den Sektoren der Anlage 1.
- Wichtige Einrichtungen ab 50 Mitarbeitenden oder mehr als 10 Millionen Euro Umsatz in den Sektoren der Anlage 1 oder 2.
- Betreiber kritischer Anlagen, also klassische KRITIS, unabhängig von der Größe.
- Erfasst sind unter anderem Energie, Wasser, Gesundheit, Verkehr, Finanz, digitale Infrastruktur, Lebensmittel, Logistik, Maschinenbau, Pharmazie, Chemie, Forschung und Verwaltung.

Bußgeldrahmen nach Paragraph 65 BSIG

Klasse	Beispielhafte Anforderung	Bußgeldrahmen
Besonders wichtige Einrichtung	Proaktive Aufsicht, regelmäßige Prüfung	Bis 10 Mio. Euro oder 2 Prozent des weltweiten Jahresumsatzes
Wichtige Einrichtung	Ex post Aufsicht, anlassbezogene Prüfung	Bis 7 Mio. Euro oder 1,4 Prozent des weltweiten Jahresumsatzes
Geschäftsleitung	Persönliche Haftung bei Pflichtverletzung	Innenhaftung und Reputationsrisiko

Zentrale Fristen

- 6. Dezember 2025, Inkrafttreten ohne Übergangsfrist, also Pflichten ab Tag eins.
- 6. März 2026, ursprüngliches Ende der dreimonatigen Registrierungsfrist beim BSI, verspätete Registrierung weiterhin möglich und dringend zu empfehlen.
- Registrierung über das MUK Portal des BSI, also Melde und Unterrichtungskanal, Voraussetzung ist ein ELSTER Organisationszertifikat.
- 17. März 2026, das ergänzende KRITIS Dachgesetz ist in Kraft.

Meldepflichten nach Paragraph 32 BSIG

- 24 Stunden, Frühwarnung an das BSI.
- 72 Stunden, Folge Meldung mit Sachverhaltsbewertung.
- 1 Monat, Abschlussbericht mit Ursachen, Wirkung und Maßnahmen.

Pflichten der Geschäftsleitung nach Paragraph 38 BSIG

- Aktive Überwachung der Risikomanagementmaßnahmen.
- Verpflichtende Cybersicherheits Schulung der Leitungsorgane.
- Persönliche Haftung der Geschäftsleitung für Pflichtverstöße, Innenhaftung gegenüber dem Unternehmen.
- Delegation ist möglich, entlastet aber nicht von der Überwachungspflicht.

Die zehn Mindestmaßnahmen nach Paragraph 30 BSIG

Nr.	Maßnahmenbereich
1	Konzepte zur Risikoanalyse und Sicherheit der Informationssysteme
2	Bewältigung von Sicherheitsvorfällen
3	Aufrechterhaltung des Betriebs, Backup und Krisenmanagement
4	Sicherheit der Lieferkette und der Dienstleister
5	Sicherheit bei Beschaffung, Entwicklung und Wartung
6	Bewertung der Wirksamkeit der Risikomanagementmaßnahmen
7	Cyberhygiene und Awareness Schulungen
8	Einsatz von Kryptographie und Verschlüsselung
9	Personalsicherheit, Zugriffskontrolle und Asset Management
10	Multifaktor Authentisierung und sichere Kommunikation

Verzahnung mit DSGVO und BSI IT Grundschutz

Wer ein ISMS nach ISO 27001 oder BSI IT Grundschutz betreibt, deckt 70 bis 80 Prozent der NIS 2 Anforderungen ab. Die verbleibenden 20 bis 30 Prozent betreffen die BSI Registrierung, das gestufte Meldeverfahren und die Geschäftsleitungspflichten. DSGVO bleibt parallel anwendbar, ein integriertes Compliance Konzept spart Doppelarbeit.

3. Die wichtigsten Standards im Überblick

Ein ISMS lässt sich nicht aus dem Nichts entwerfen. Etablierte Standards liefern Struktur, Maßnahmenkataloge und international anerkannte Zertifizierungspfade.

Standard	Anwendung	Zertifizierbar
ISO/IEC 27001:2022	Internationaler Leitstandard für ISMS, branchenneutral, weltweit anerkannt	Ja, durch akkreditierte Stellen
ISO/IEC 27002	Maßnahmenkatalog, 93 Controls als Umsetzungshilfe zu ISO 27001	Nein, reiner Leitfaden
BSI IT Grundschutz	Nationale Methodik des Bundesamts für Sicherheit in der Informationstechnik, in Deutschland weit verbreitet, kombinierbar mit ISO 27001	Ja, ISO 27001 auf Basis IT Grundschutz
TISAX	Verbindliches Prüfschema für die Automobilbranche und deren Zulieferer	Ja, durch zugelassene Prüfdienstleister
DORA	Pflicht für Finanzunternehmen und deren IKT Dienstleister seit Januar 2025	Aufsichtspflicht, keine klassische Zertifizierung
ISO/IEC 27017 und 27018	Ergänzungen für Cloud Dienste und Schutz personenbezogener Daten in der Cloud	Ja, ergänzend zu ISO 27001

Für KMU ist ISO 27001 in der Praxis der zentrale Bezugspunkt. Sie ist international anerkannt, deckt 70 bis 80 Prozent der gesetzlichen Cyber Anforderungen ab und ist auch ohne Zertifizierung als Steuerungsmodell sinnvoll.

4. Wie ein ISMS aufgebaut ist

Ein ISMS folgt einem klaren Regelkreis, dem sogenannten PDCA Zyklus, also Plan, Do, Check, Act. Diese Logik wiederholt sich jährlich und sorgt für kontinuierliche Verbesserung statt Einmalprojekt.

Plan, also Planung und Festlegung

- Geltungsbereich definieren. Welche Standorte, Prozesse, Systeme und Mitarbeiter sind erfasst?
- Informationssicherheits Leitlinie verabschieden. Klares Bekenntnis der Geschäftsführung.
- Rollen und Verantwortlichkeiten festlegen, insbesondere Informationssicherheits Beauftragter, ISO oder CISO.
- Asset Verzeichnis erstellen. Welche Informationswerte gibt es, wer ist Eigentümer, wie kritisch sind sie?
- Risikomanagement Methode definieren. Wie werden Risiken identifiziert, bewertet und behandelt?

Do, also Umsetzung

- Risikoanalyse durchführen. Bedrohungen, Schwachstellen und Auswirkungen je Asset bewerten.
- Maßnahmen auswählen und umsetzen. Technisch, organisatorisch und personell.
- Statement of Applicability erstellen. Dokumentierter Maßnahmenkatalog mit Begründung.
- Awareness Schulungen für alle Mitarbeiter durchführen.
- Notfallmanagement und Wiederanlauf Pläne aufbauen.

Check, also Überwachung und Bewertung

- Internes Audit jährlich, das prüft die Wirksamkeit der Maßnahmen.
- Managementbewertung durch die Geschäftsführung, dokumentiert in einem Protokoll.
- Sicherheitsvorfälle erfassen, auswerten und melden, soweit gesetzlich gefordert.
- Kennzahlen und Berichte zur Steuerung.

Act, also Verbesserung

- Korrektur und Vorbeugemaßnahmen ableiten.
- Lessons Learned aus Vorfällen und Audits einarbeiten.
- ISMS Dokumente regelmäßig aktualisieren.

5. Die 14 Themenbereiche nach ISO 27001

Der Maßnahmenkatalog der ISO 27001 deckt diese Themen ab. Sie sind die inhaltliche Substanz jedes ISMS.

Bereich	Inhalt in Stichworten
Sicherheitsleitlinien	Strategische Vorgaben und Rahmenrichtlinien
Organisation der Informationssicherheit	Rollen, Verantwortung, Trennung von Aufgaben
Personalsicherheit	Verträge, Hintergrundprüfungen, Awareness, Trennung
Asset Management	Verzeichnis, Eigentümer, Klassifizierung
Zugriffskontrolle	Berechtigungen, Authentisierung, Privileged Access
Kryptographie	Verschlüsselung, Schlüsselmanagement
Physische und umgebungsbezogene Sicherheit	Zutritt, Bauwerk, Notstrom, Brandschutz
Betriebssicherheit	Patch Management, Backup, Logging, Malware Schutz
Kommunikationssicherheit	Netzwerktrennung, sichere Übertragung
Beschaffung, Entwicklung und Wartung	Secure Coding, Test, Change Management
Lieferantenbeziehungen	AVV, Lieferantenaudits, Lieferketten Risiken
Incident Management	Erkennen, Bewerten, Reagieren, Melden, Lernen
Business Continuity	BCM, Notfallpläne, Wiederanlauf
Compliance	Gesetze, Verträge, Audits, Datenschutz

Mit der ISO 27001:2022 Revision wurden die Controls in vier Cluster konsolidiert, also organisatorisch, personell, physisch und technologisch. Inhaltlich bleibt die Substanz der vierzehn Themen erhalten.

6. Implementierung in der Praxis, typische Phasen

Der Aufbau eines ISMS ist kein Tagesprojekt. Ein realistischer Rahmen für ein KMU liegt bei sechs bis zwölf Monaten bis zur Audit Reife. Die Phasen sehen typischerweise so aus.

Phase	Inhalt	Dauer Richtwert
1. Scoping und Kick off	Geltungsbereich, Projektorganisation, Zieldefinition, Kommunikation	2 bis 4 Wochen
2. GAP Analyse	Ist Aufnahme zur Norm, identifizierte Lücken, priorisierter Maßnahmenplan	3 bis 6 Wochen
3. Dokumentation und Policies	Leitlinie, Verfahrensanweisungen, Rollen, Asset Register, SoA	6 bis 10 Wochen
4. Risikomanagement	Methodik, Bewertung, Behandlungsplan, Restrisiken	4 bis 8 Wochen
5. Umsetzung Maßnahmen	Technische und organisatorische Maßnahmen, Schulungen, Notfallplanung	8 bis 16 Wochen
6. Internes Audit	Wirksamkeitsprüfung, Korrekturmaßnahmen, Management Review	3 bis 4 Wochen
7. Zertifizierungsaudit	Stufe 1 Dokumentenprüfung, Stufe 2 Vor Ort durch externe Stelle	6 bis 10 Wochen

> **Realitäts Check**
> Die Norm verlangt kein Perfekt System ab Tag eins. Sie verlangt ein lebendes System mit nachweisbarer Verbesserung. Wer mit einem soliden Risikomanagement, klaren Policies und gelebter Awareness startet, ist auf dem richtigen Weg, auch wenn nicht jede Control sofort auf Stufe fünf steht.

7. Die häufigsten Stolperfallen

Aus Beratungspraxis im Mittelstand wiederholen sich diese Muster. Wer sie kennt, spart Zeit und Geld.

Falle 1, ISMS wird als IT Projekt missverstanden

Ein ISMS ist Managementverantwortung, nicht IT Verantwortung. Wenn die Geschäftsführung delegiert und nicht steuert, wird das System zur Doku Schublade und liefert im Audit nichts.

Falle 2, Geltungsbereich zu groß gewählt

Wer am Anfang alle Standorte und Tochterfirmen einbezieht, schafft den Aufbau nicht in zwölf Monaten. Klüger ist ein eng definierter Geltungsbereich und schrittweise Erweiterung.

Falle 3, Risikomanagement nur auf dem Papier

Wenn die Risikoanalyse einmalig durchgeführt und dann abgeheftet wird, fehlt der Kern des Systems. Risiken müssen mindestens jährlich überprüft werden und nach jeder wesentlichen Änderung im Unternehmen.

Falle 4, Lieferketten unterschätzt

Der größte ungeprüfte Risikobereich in der Praxis ist die Lieferkette. Jeder externe Dienstleister mit Zugriff auf Systeme oder Daten ist Teil des Risikoprofils. Auftragsverarbeitungsverträge allein genügen nicht, es braucht regelmäßige Bewertung.

Falle 5, Awareness wird auf E Learning reduziert

Jährliche Online Schulung mit Klickstrecke schafft kein Sicherheitsbewusstsein. Phishing Simulationen, Praxisbezug und Vorbildfunktion der Führung sind nicht verhandelbar.

8. Wirtschaftlicher Nutzen, was Sie davon haben

Ein ISMS ist eine Investition. Der Return ergibt sich aus mehreren Quellen, nicht aus einer einzelnen.

Nutzen Dimension	Konkreter Effekt
Compliance und Bußgeldvermeidung	Erfüllung gesetzlicher Pflichten, dokumentierter Nachweis, geringeres Risiko persönlicher Haftung der Geschäftsführung
Auftrags Sicherung	Zugang zu Ausschreibungen, Lieferkettenfähigkeit, Reduktion verlorener Vergaben durch fehlende Nachweise
Versicherung	Cyber Police bezahlbar und mit voller Deckung, Verhandlungsstärke gegenüber Versicherer
Resilienz	Wirklich funktionierende Backups, geübtes Notfallmanagement, schneller Wiederanlauf, weniger Stillstand
Reputation und Vertrauen	Argument im Vertrieb, in Kundengesprächen, bei Investoren und in Krisenkommunikation
Prozess Klarheit	Saubere Zuständigkeiten, dokumentierte Abläufe, Reduktion von Personenabhängigkeit

Faustregel

Ein gut implementiertes ISMS amortisiert sich in der Regel binnen zwei bis drei Jahren, allein über Aufträge, die ohne den Nachweis nicht gewonnen worden wären, und über vermiedene Vorfälle.

9. Wie Datenschutz Kroes unterstützt

Datenschutz Kroes begleitet KMU bei der Einführung, dem Betrieb und der Auditierung von Informationssicherheits Management Systemen. Der Ansatz ist pragmatisch, dokumentenorientiert und auf Audit Reife ausgerichtet, nicht auf Pseudo Sicherheit.

Leistungsspektrum

- ISMS Quick Check. Strukturierte Erstanalyse Ihres aktuellen Reifegrads gegen ISO 27001.
- GAP Analyse mit priorisiertem Maßnahmenplan und realistischer Zeitachse.
- Aufbau und Dokumentation des ISMS, von Leitlinie bis Statement of Applicability.
- Risikomanagement Methodik, Asset Register, Behandlungsplan.
- Awareness Konzepte, Schulungen und Phishing Simulationen.
- Vorbereitung und Begleitung des Zertifizierungsaudits durch akkreditierte Stellen.
- Betrieb und Pflege des ISMS im Retainer Modell, mit fixen monatlichen Kosten.
- Externer Informationssicherheits Beauftragter, kombinierbar mit der externen Datenschutz Beauftragten Funktion.

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 Tool Plattformen.
- Lokale Präsenz in Österreich und Süddeutschland, Beratung deutsch und auf Augenhöhe.
- Verzahnung mit Datenschutz Beauftragten Leistung, ein Anbieter für beide Compliance Säulen.

10. Wie es weitergeht

Ein ISMS 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 gesetzlicher Pflichten, Einschätzung des sinnvollen Geltungsbereichs und Auswahl des passenden Standards.

Schritt 2, ISMS Quick Check

Strukturierte Reifegradanalyse in der Regel binnen zwei 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 oder als Retainer Modell mit laufender Betreuung.

Datenschutz mit System. Festpreis. Persönlich.

Informationssicherheit ebenso.

Rechtlicher Hinweis

Dieses Whitepaper dient der allgemeinen Information und ersetzt keine individuelle rechtliche oder beraterische Prüfung des Einzelfalls. Die dargestellten gesetzlichen Anforderungen geben den Rechtsstand zum Erstellungsdatum wieder. Änderungen in der Gesetzgebung, in begleitenden Verordnungen und in der Aufsichtspraxis sind möglich und können den dargestellten Inhalt überholt erscheinen lassen. Eine konkrete Betroffenheits und Pflichtenprüfung erfolgt 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/