TÜVNORD

Inspired by Knowledge

ISO/IEC 27001 Zertifizierung

Überblick: Informationssicherheit im aktuellen regulatorischen Umfeld
Informationen sind heute ein zentraler Produktions- und Erfolgsfaktor moderner Organisationen. Durch Digitalisierung, Cloud-Services, mobile Arbeitsformen, vernetzte Lieferketten und zunehmende regulatorische Anforderungen sind Unternehmen immer stärker von der sicheren Verarbeitung und Verfügbarkeit von Informationen abhängig. Gleichzeitig nehmen die Risiken durch Cyberangriffe, Datenschutzverletzungen, Systemausfälle und Compliance-Verstöße zu.

Vor diesem Hintergrund gewinnen die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit weiter an Bedeutung. Informationen sind wertvolle Unternehmenswerte, deren Verlust, Manipulation oder unbefugte Offenlegung erhebliche wirtschaftliche, rechtliche und reputative Schäden verursachen kann. Neben operativen Risiken sind insbesondere Verstöße gegen gesetzliche und regulatorische Vorgaben, beispielsweise aus dem Datenschutz-, IT-Sicherheits- oder Aufsichtsrecht, von zunehmender Relevanz.

Ein wirksames Informationssicherheitsmanagementsystem (ISMS) ist die Grundlage, um diesen Herausforderungen strukturiert zu begegnen. Ein ISMS ermöglicht die systematische Identifikation, Bewertung und Behandlung von Informationssicherheitsrisiken. Es stellt außerdem sicher, dass Informationssicherheit dauerhaft, nachvollziehbar und überprüfbar in der Organisation verankert ist. Dabei werden technische, organisatorische, personelle und physische Aspekte gleichermaßen berücksichtigt.

Die international anerkannte Norm ISO/IEC 27001 definiert die Anforderungen an den Aufbau, die Einführung, den Betrieb, die Überwachung und die kontinuierliche Verbesserung eines dokumentierten Informationssicherheits-Managementsystems (ISMS). Sie folgt konsequent einem risikobasierten Ansatz und ist technologie- sowie branchenneutral gestaltet. Mit einer Zertifizierung nach ISO/IEC 27001 bestätigt TÜV NORD CERT, dass diese Anforderungen wirksam umgesetzt werden und die Informationssicherheit integraler Bestandteil der Unternehmenssteuerung ist.

Kernmerkmale der ISO/IEC 27001 Zertifizierung:

- International anerkannter Standard für Informationssicherheitsmanagementsysteme
- Risikobasierter, ganzheitlicher Ansatz zur Steuerung von Informationssicherheitsrisiken
- Klare Governance-Strukturen mit definierten Rollen und Verantwortlichkeiten
- Kontinuierlicher Verbesserungsprozess durch Audits, Reviews und Maßnahmensteuerung
- Aufbau nach der Harmonized Structure (HS), wie bei nahezu allen modernen Managementsystemnormen, wodurch umfangreiche Synergien mit anderen Normen (z. B. integrierte Dokumentation, gemeinsame Programme für interne Audits und Managementbewertungen sowie insbesondere integrierte Zertifizierungsprogramme und -audits) realisiert werden können

Einordnung im Kontext von Gesetzen und Compliance:

- Unterstützung bei der Einhaltung gesetzlicher und regulatorischer Anforderungen
- Strukturierter Nachweis der Informationssicherheit gegenüber Kunden, Partnern, Aufsichtsbehörden und Auditoren
- Erfüllung vertraglicher Sicherheitsanforderungen in nationalen und internationalen Liefer- und Wertschöpfungsketten

Zielgruppen der Zertifizierung

Die Zertifizierung richtet sich an Organisationen aller Branchen und Größen.

Typische Zielgruppen sind Organisationen, die:

- sensible oder geschäftskritische Informationen verarbeiten (z. B. personenbezogene Daten, Forschungs- und Entwicklungsdaten, geistiges Eigentum)
- gesetzlichen und regulatorischen Anforderungen unterliegen (z. B. kritische Infrastrukturen, Datenschutz, IT-Sicherheit, Aufsichtsvorgaben)
- von Kunden oder Partnern eine ISO/IEC-27001-Zertifizierung als Voraussetzung für eine Zusammenarbeit oder für Ausschreibungen gefordert bekommen
- ihre Cyber-Resilienz, Ausfallsicherheit und Geschäftskontinuität nachhaltig stärken möchten
- Vertrauen bei Kunden, Investoren und weiteren Stakeholdern aufbauen und nachweisen wollen

Die Norm ist sowohl für Organisationen mit bestehenden Managementsystemen als auch für Unternehmen geeignet, die Informationssicherheit erstmals ganzheitlich und strukturiert etablieren möchten.

Ihr Weg zur ISO 27001 Zertifizierung in 5 Schritten

1. Vorbereitung
2. Internes Audit
3. Audit Stufe 1 inkl. Freigabeprozess
4. Audit Stufe 2 inkl. Freigabeprozess
5. Überwachung inkl. Freigabeprozess

Unser Know-how für Ihren Erfolg

TÜV NORD CERT ist ein international anerkannter und zuverlässiger Partner für Prüf- und Zertifizierungsdienstleistungen. Unsere Sachverständigen und Auditoren verfügen über fundiertes Wissen und haben grundsätzlich eine Festanstellung bei TÜV NORD. Hierdurch sind Unabhängigkeit und Neutralität sowie Kontinuität bei der Betreuung unserer Kunden gewährleistet. Der Vorteil für Sie liegt auf der Hand: Unsere Auditoren begleiten und unterstützen die Entwicklung Ihres Unternehmens und geben Ihnen ein objektives Feedback.

Kontakt

TÜV NORD CERT
ISMS Sales &
Projectmanagement

sales.isms@tuev-nord.de
tuev-nord-cert.de

Weitere Informationen und Kontaktformular:

24-0609-02/26