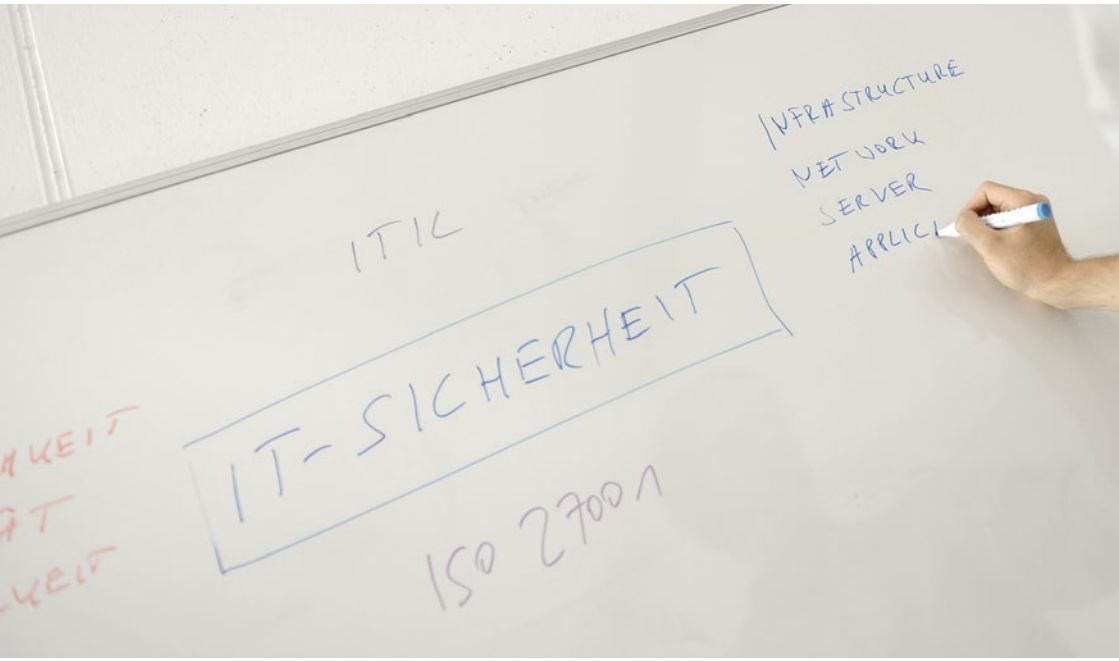


ISMS und Sicherheitskonzepte

ISO 27001 und IT-Grundschutz

datenschutz nord
GRUPPE

Aufbau eines ISMS, Erstellung von Sicherheitskonzepten

Bei jedem Unternehmen mit IT-basierenden Geschäftsprozessen kommt der Informationssicherheit eine große Bedeutung zu. Neben dem eigenen Interesse, die Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten und sensiblen Unternehmensinformationen sicherzustellen, bestehen auch **gesetzliche Vorgaben,** z.B. **das IT-Sicherheitsgesetz** oder das **Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG).** Hierdurch wird Informationssicherheit als Bestandteil des betrieblichen Risikomanagements für die Geschäftsführung verpflichtend.

Um die Sicherheit der Informationen gewährleisten zu können, ist es nicht ausreichend, ausschließlich technische Sicherheitsmaßnahmen umzusetzen. Voraussetzung für ein angemessenes Sicherheitsniveau ist zum einen eine kontinuierliche Planung, Lenkung und Kontrolle der Sicherheitsmaßnahmen. Dieser Prozess wird als **Informationssicherheits-Managementsystem** oder auch kurz als **ISMS** bezeichnet. Zum anderen müssen die umgesetzten Sicherheitsmaßnahmen in einem IT-Sicherheitskonzept ausreichend **dokumentiert** sein. Dabei kann ein IT-Sicherheitskonzept sowohl für alle IT-Komponenten im Geltungsbereich des ISMS, als auch für einzelne Fachverfahren erstellt werden.

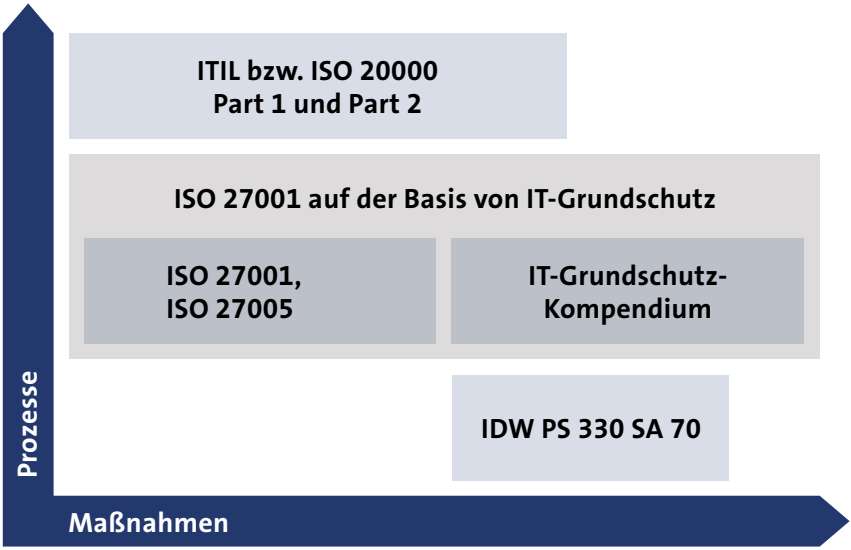
Mit der **ISO-Norm 27001** und dem **IT-Grundschutz** des Bundesamts für Sicherheit in der Informationstechnik (BSI) gibt es seit Jahren **zwei Standards** zur Informationssicherheit, die sich in Unternehmen und öffentlichen Stellen etabliert haben. Darüber hinaus gibt es **branchenspezifische Anforderungen,** beispielsweise hat der Verband der Automobilindustrie (VDA) ein eigenes Information Security Assessment auf der Grundlage der ISO 27001 erstellt. Allerdings ist nicht jedes Unternehmen oder jede Verwaltung, die behauptet, ihre IT sei konform zu ISO 27001 oder IT-Grundschutz organisiert, auch automatisch nach diesen Normen zertifiziert.

Bis hierhin ist es oftmals ein beschwerlicher Weg, bei dem wir – die datenschutz nord Gruppe – Sie gerne unterstützen. Zunächst ein Überblick über die beiden wichtigsten Normen.

ISO 27001

ISO 27001 hat sich international als Standard für Informationssicherheit in **Unternehmen** und **Behörden** etabliert. Ganzheitlich werden alle Aspekte zur Informationssicherheit analysiert und zertifiziert, die zum Funktionieren eines Unternehmens oder einer Behörde notwendig sind. Dies umfasst neben **technisch-organisatorischen Maßnahmen** auch eine **Risikoanalyse,** in der die jeweils relevanten Bedrohungen bewertet und priorisiert werden.

Im Focus der Norm ISO 27001 steht ein sogenanntes **Informationssicherheits-Managementsystem (ISMS);** die Norm ist im Vergleich zu IT-Grundschutz eher prozessorientiert. Ein nach **ISO 27001** organisiertes ISMS ist vollständig kompatibel zu anderen Managementsystemen wie **ISO 9001** oder **ISO 20000** und kann auch als Basis für Prüfungen nach dem Standard **IDW PS 330** oder **SA 70** bzw. **Sarbanes-Oxley Act (SOX)** dienen.



IT-Grundschutz

Während sich der Standard ISO 27001 in Unternehmen durchgesetzt hat, kommt IT-Grundschutz häufig in **Behörden** und **öffentlichen Stellen** zum Einsatz. IT-Grundschutz ist ein nationaler Standard des BSI, konform zur ISO 27001-Norm und eingebettet in ein ganzheitliches Informationssicherheits-Management-system (ISMS). Hierzu existieren zahlreiche Standards:

- **BSI 200-1:** Managementsysteme für Informationssicherheit (ISMS)
- **BSI 200-2:** IT-Grundschutz-Vorgehensweise
- **BSI 200-3:** Risikoanalyse
- **BSI 100-4:** Notfall-Management

Typisch für IT-Grundschutz ist die Vorgehensweise: Zunächst werden im Rahmen einer **IT-Strukturanalyse,** einer **Schutzbedarfsfeststellung** sowie einer **Modellierung** der IT-Grundschutz-Bausteine der zu betrachtende Informationsverbund umfangreich dokumentiert. Danach wird in einem **IT-Grundschutz-Check** die Ist-Situation gegen das IT-Grundschutz-Kompendium geprüft und der über einen Grundschutz hinausgehende Schutzbedarf analysiert.

Wie können wir Ihnen hierbei behilflich sein?

Wir – die datenschutz nord Gruppe – können Sie beim Aufbau eines ISMS und der Erstellung von IT-Sicherheitskonzepten nach ISO 27001 oder IT-Grundschutz umfassend unterstützen.

Erstellung eines IT-Sicherheitskonzepts

Mit Ihnen gemeinsam ein ISMS etablieren und geeignete IT-Sicherheitskonzepte erstellen, dies würde – je nach geografischer Lage Ihres Unternehmens – entweder von der datenschutz nord GmbH oder der datenschutz süd GmbH wahrgenommen. Hierbei gehen wir pragmatisch vor und beschränken uns auf die wesentlichen Aspekte der Informationssicherheit.

Im Rahmen des ISMS wird ein IT-Sicherheitskonzept erstellt, welches die notwendigen Sicherheitsmaßnahmen definiert. Zu diesem Zweck werden in der **Strukturanalyse**

- die **Infrastruktur** (Gebäude, Serverräume);
- die **Netzkomponenten** (Firewall, Switches, Router) und Verbindungen (Ethernet, Backbone-Technik, Internet- und Remote-Anbindung);
- die **IT-Systeme** (Client, Server, Laptop, Smartphones);
- und die **Anwendungen** erfasst.

Für den so definierten Informationsverbund werden die **Sicherheitsziele** unter Berücksichtigung der relevanten gesetzlichen Regelungen, Vorschriften und Richtlinien – etwa zur Internet- oder E-Mail-Nutzung – auf die Werte der untersuchten Institution abgestimmt und dokumentiert. Auf der Basis der Sicherheitsziele wird der **Schutzbedarf** der zentralen Anwendungen und Daten definiert.

In der **Risikoanalyse** werden die relevanten Gefährdungen ermittelt und bewertet. Dies umfasst die oben genannten Bereiche Infrastruktur, Netzwerk, Systeme und Anwendungen sowie den Bereich Personal und Organisation. Dabei muss für jede Gefährdung eingeschätzt werden, welche Eintrittswahrscheinlichkeit die Gefährdung für den gegebenen Informationsverbund hat. Die durch die datenschutz nord GmbH erstellte Risikoanalyse orientiert sich am BSI Standard 200-3 und der empfohlenen Vorgehensweise nach ISO 27005.

Darüber hinaus werden **Verbesserungsvorschläge** formuliert. Die Verbesserungsvorschläge umfassen in der Regel neu oder anzupassende technische Maßnahmen und zu erstellende Regelungen und Prozessabläufe. Hierbei orientieren wir uns an ISO 27002, ITIL und dem IT-Grundschutz-Kompendium.

Auditierung/Zertifizierung

Für die Auditierung und Zertifizierung nach ISO 27001 bzw. IT-Grundschutz sind entweder Zertifizierungsstellen zuständig, die bei der Deutschen Akkreditierungsstelle GmbH (DAkkS) gemäß ISO 27006 akkreditiert sind, oder das Bundesamt für Sicherheit in der Informationstechnik (BSI). Die datenschutz nord GmbH verfügt über lizenzierte Lead-Auditoren und Auditoren, die beim BSI als ISO 27001-Auditteamleiter lizenziert sind.

Der Ablauf einer typischen Auditierung und Zertifizierung gestaltet sich wie folgt:

- Zu Beginn wird ein **Kick-Off-Meeting** durchgeführt: Hierbei werden die weitere Vorgehensweise und der Zeitplan abgestimmt.
- Die Auditierung nach IT-Grundschutz bzw. ISO 27001 besteht im Wesentlichen aus der **Sichtung von Referenzdokumenten** und dem **Site Visit** vor Ort. Dazu übergeben Sie zunächst die Referenzdokumente (u.a. ISMS, IT-Sicherheitskonzept), die gemäß BSI-Grundschutz bzw. ISO 27001 erforderlich sind.
- Anschließend erfolgt die **Prüfung der Referenzdokumente.**
- Nach der Dokumentationsprüfung erfolgen die **Auditvorbereitung** sowie der Site Visit vor Ort.
- Das gesamte Audit wird in einem **Auditreport** dokumentiert und der Zertifizierungsstelle vorgelegt.
- Mit der Abnahme des finalen Auditreports kann die **Erteilung des Zertifikats** auf der Basis von IT-Grundschutz oder ISO 27001 erfolgen.

datenschutz nord Gruppe

Zu der datenschutz nord Gruppe gehören die **DSN Holding GmbH,** deren Tochterunternehmen **datenschutz nord GmbH,** die **datenschutz süd GmbH,** die **datenschutz cert GmbH,** die international tätige **FIRST PRIVACY GmbH** sowie die **PRIVACY Central GmbH.**

Die datenschutz nord Gruppe ist einer der bundesweit führenden Dienstleister im Bereich Datenschutz. Bei mehr als 500 Unternehmen sind wir als externer betrieblicher Datenschutzbeauftragter tätig. Darunter sind klein- und mittelständische Unternehmen sowie Großkonzerne, sowohl Dienstleister als auch Produktionsunternehmen. Als Datenschutzbeauftragter sind wir zudem bei zahlreichen öffentlichen Stellen und kirchlichen Einrichtungen tätig.

Darüber hinaus beraten unsere IT-Sicherheitsexperten – lizenzierte ISO 27001- bzw. IT-Grundschutz-Auditoren – in allen Bereichen der Informationssicherheit. Wir erstellen **Sicherheitskonzepte,** führen **Penetrationstests** durch und entwickeln mit Ihnen gemeinsam ein für Ihr Unternehmen maßgeschneidertes **Informationssicherheits-Management.**

- **preislich kalkulierbar**
- **direkte Ansprechpartner**
- **zeitlich kalkulierbar**
- **ganzheitliches Projektmanagement**
- **transparent**
- **verständlich**

datenschutz nord GmbH

Hauptsitz Bremen
Konsul-Smidt-Straße 88
28217 Bremen
Tel.: +49 (0) 421 69 66 32-0

office@datenschutz-nord.de
www.datenschutz-nord-gruppe.de

datenschutz süd GmbH

Hauptsitz Würzburg
Wörthstraße 15
97082 Würzburg
Tel.: +49 (0) 931 30 49 76-0

office@datenschutz-sued.de
www.datenschutz-nord-gruppe.de

Weitere Niederlassungen der datenschutz nord Gruppe siehe **www.datenschutz-nord-gruppe.de/standorte**

datenschutz nord

datenschutz süd