2026 CAMPUS TAGE

DSN Akademie

10 Jahre DSGVO

Und jetzt?
Gemeinsam weiterdenken!

2026 CAMPUS TAGE

DSN Akademie

ISMS unter der Lupe:

Was im Zertifizierungsaudit wirklich zählt!

DSN Akademie

Sebastian Meissner
Jurist | Audits und Zertifizierungen

datenschutz cert GmbH
T +49(0)421 69 66 32 567
E-Mail smeissner@datenschutz-cert.de

www.dsn-group.de

Agenda

1. Vorstellung der datenschutz cert
2. Einführung ins Thema
3. Stolpersteine: Typische Schwachstellen
4. Zentrale Erfolgsfaktoren eines ISMS
5. Security by Design

DSN Akademie

1. Vorstellung dsc

Wer ist die datenschutz cert GmbH?

Teil der DSN GROUP

Unsere Akkreditierungen und Anerkennungen

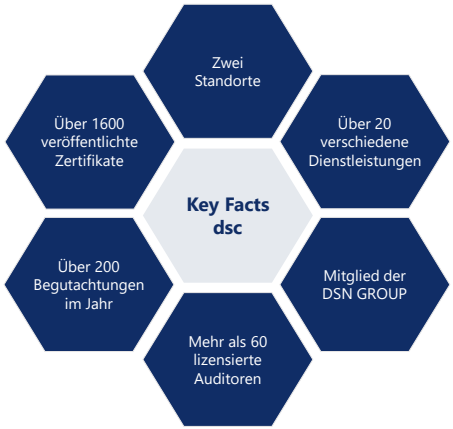
Deutsche Akkreditierungsstelle (DAkkS)
- ISO/IEC 27001
- ISO/IEC 27701
- IT-Sicherheitskatalog §11 (1a) EnWG
- IT-Sicherheitskatalog §11 (1b) EnWG

- eIDAS-Konformitätsbewertungsstelle
- ips – Videosprechstunde – IT
- information privacy standard (DSGVO)

Bundesamt für Sicherheit in der Informationstechnik (BSI)
- IT-Sicherheitsdienstleister
- Prüfstelle für IT-Sicherheit (TR-ESOR)
- IT-Grundschutz /Prüfbegleitung
- TR 03109-6 „GWA"
- TR 03145 „Secure CA Operation"
- TR 03125 „TR-ESOR"

Bundesnetzagentur
- eIDAS-Zertifizierungsstelle

Key Facts



2. Einführung

Was im Audit wirklich zählt

Einführung
Häufige Missverständnisse

Was nicht ausreicht:

- Checklisten abhaken
- Dokumente (nur) für den Audittermin erstellen
- Fokus auf das ISMS (nur) vor dem Audittermin

→ Gefragt ist dauerhafte Wirksamkeit – nicht punktuelle Konformität

Was nicht erforderlich ist:

- Jedes Dokument ist makellos formuliert.
- Jede einzelne Maßnahme aus Anhang A ist implementiert.
- Alle Risiken sind eliminiert oder vollständig behandelt.
- ISMS, das bereits alle Verbesserungsmöglichkeiten ausgeschöpft hat.

→ Perfektion? Nein. Aber: Wirksamkeit.

Einführung
Erwartungshaltung von Auditoren

Das wollen Auditoren sehen:

- Risiken, die systematisch identifiziert, bewertet und nachvollziehbar behandelt sind
- ein ISMS, das zur Organisation passt – in Größe, Komplexität und Risikolage
- eine Organisation, in der Informationssicherheit nicht nur bei IT und CISO ankommt, sondern in allen Bereichen gelebt wird
- Verantwortlichkeiten, die nicht nur dokumentiert, sondern tatsächlich wahrgenommen werden
- ein ISMS, das aus Vorfällen und Audits lernt und sich weiterentwickelt

3. Stolpersteine

Typische Schwachstellen von ISMS in Zertifizierungsaudits

Abschnitt 4.3 ISO/IEC 27001

Alle Normbezüge in dieser Präsentation beziehen sich auf ISO/IEC 27001:2022, © ISO/IEC

Scope

Definition des Geltungsbereichs

- Auf welche Teile der Organisation, welche Prozesse und welche Standorte bezieht sich das ISMS?
- strategische Grundsatzentscheidung: Bestimmt, was im Audit geprüft und später zertifiziert wird – und was nicht

Stolpersteine:

- nichtssagender/ungenauer Scope: „Relevante Geschäftsprozesse" o.ä. → keine klare Abgrenzung/ Festlegung des Prüfumfangs möglich
- widersprüchlicher Scope: Der Geltungsbereich wird in verschiedenen ISMS-Dokumenten unterschiedlich beschrieben.
- Schnittstellenblindheit: keine Schutzmaßnahmen an Scope-Grenzen
- „Feigenblatt-Scope": bewusstes Aussparen aller kritischen Bereiche

Abschnitt 6.1.2 ISO/IEC 27001

Risikobeurteilung

Papier ist geduldig

- Risikomanagement = Dreh- und Angelpunkt des gesamten ISMS
- Risikobeurteilung ist kein Excel-Sport – sie muss in den Köpfen der Verantwortlichen ankommen.

Stolpersteine:

- Risikobeurteilungen, die erstmalig erstellt und danach trotz Veränderung von Bedrohungslage und Organisation nie aktualisiert wurden
- Risikokataloge mit >100 Einträgen, die alle ein identisches Risikolevel haben: Ein erstaunlicher Zufall? Wohl eher nicht…
- Risikoeigner können die getroffene Bewertung von Eintrittswahrscheinlichkeit und Schadensausmaß nicht erklären.
- Der Risikoeigner eines zentralen Geschäftsprozesses kann das größte Risiko für diesen nicht ad hoc benennen.

Abschnitt 6.1.3 d) ISO/IEC 27001

SoA

Statement of Applicability

- Das SoA macht transparent: Welche der 93 Controls sind relevant, warum – und was ist davon bereits umgesetzt?
- Es ist die nachvollziehbare Brücke zwischen Risikobeurteilung und implementierten Maßnahmen.

Stolpersteine:

- Controls werden ohne jede Begründung als „nicht anwendbar„ bzw. „anwendbar" markiert.
- Verbindung zwischen identifiziertem Risiko und gewähltem Control ist nicht herstellbar.
- Der im SoA dokumentierte Umsetzungsstatus und die tatsächliche Umsetzung stimmen nicht überein.
- Das SoA wird einmalig erstellt und danach nie aktualisiert, obwohl sich Risiken und Organisation verändern.

Abschnitt 5.1 ISO/IEC 27001

Management Commitment

Eine Unterschrift allein genügt nicht…

- Führungsverantwortung ist eine zentrale Voraussetzung für ein wirksames ISMS.
- Sicherheitskultur entsteht top-down – was die Führung nicht vorlebt, wird von Mitarbeitenden nicht ernst genommen.

Stolpersteine:

- Geschäftsführung unterschreibt Informationssicherheitsrichtlinie, und damit endet ihre aktive Beteiligung am ISMS.
- Nicht alle für das ISMS erforderlichen Ressourcen (Personal, Budget, Zeit) stehen zur Verfügung.
- Management-Review existiert nur auf dem Papier: keine echte strategische Überprüfung, sondern jedes Jahr ein nahezu identisches Protokoll

Abschnitt 9.2 ISO/IEC 27001

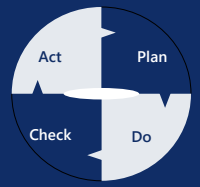
Internes Audit

Selbststeuerung zwischen den externen Audits

- Interne Audits sind ein zentrales Element des kontinuierlichen Verbesserungsprozesses – und damit ein Qualitätsmerkmal eines reifen ISMS.

Stolpersteine:

- kein funktionierendes Auditprogramm: Interne Audits finden unregelmäßig oder gar nicht statt, ein geplantes Auditprogramm existiert nicht.
- fehlende Unabhängigkeit: Mitarbeitende auditieren ihren eigenen Verantwortungsbereich.
- keine dokumentierten Ergebnisse: Auditberichte fehlen, sind inhaltsleer oder nicht auffindbar.
- Befunde führen zu keinen Korrekturmaßnahmen – Nichtkonformitäten werden identifiziert, aber nicht systematisch verfolgt und abgestellt.



Controls 5.31 und 5.34

Compliance

und Datenschutz

- Ein ISMS, das rechtliche und regulatorische Anforderungen nicht kennt, steuert an realen Pflichten vorbei.

Stolpersteine:

- Es gibt keine dokumentierte Zusammenstellung der für die Organisation geltenden rechtlichen, regulatorischen und vertraglichen Anforderungen („Rechtskataster").
- Eine Übersicht existiert, wird aber nicht fortlaufend aktualisiert: Rechtsänderungen wie z. B. NIS-2 oder neue vertragliche Verpflichtungen werden nicht erfasst.
- Die Übersicht existiert, es ist aber nicht nachvollziehbar, welche Controls/Maßnahmen aus welcher Anforderung abgeleitet wurden.
- Datenschutzanforderungen sind im SoA formal erfasst – die Risikobeurteilung enthält aber keine datenschutzrelevanten Risiken.

Abschnitt 7.3 und Control 6.3

Sicherheitskultur

Wenn der Mensch zur Schwachstelle wird

- Technische Maßnahmen und Regelwerke alleine reichen nicht: Entscheidend ist, ob Sicherheit im Arbeitsalltag wirklich gelebt wird.

Stolpersteine:

- Awareness-Maßnahmen beschränken sich auf eine jährliche Pflichtschulung ohne Überprüfung der Wirksamkeit und ohne Bezug zum Arbeitsalltag der Mitarbeitenden.
- Sicherheitsrichtlinien sind vorhanden, werden aber nicht ausreichend kommuniziert und geschult: Mitarbeitende wissen nicht, was von ihnen erwartet wird.
- Sicherheitsvorfälle werden nicht gemeldet, weil unklar ist, was meldepflichtig ist, oder weil eine Meldekultur fehlt.
- Neue Mitarbeitende werden nicht oder nur unzureichend in Sicherheitsanforderungen eingewiesen: Diese sind kein fester Bestandteil des Onboardings.

Controls 5.19 bis 5.22

Lieferanten- & Dienstleistersteuerung

Hoffentlich keine blinden Flecken

- betrifft etwa Anbieter von Cloud-Diensten, externe IT-Dienstleister, Softwareanbieter, BPO-Dienstleister und Wartungsunternehmen
- Sicherheitsanforderungen an Dienstleister müssen klar definiert und vertraglich verankert sein sowie laufend überprüft werden.

Stolpersteine:

- Verträge mit Dienstleistern enthalten keine oder nur pauschale Sicherheitsanforderungen („Treffen angemessener Maßnahmen").
- Fachabteilungen führen Tools und Cloud-Dienste ein, ohne dass dies den Weg ins ISMS findet („Shadow IT").
- Sicherheitsanforderungen werden vereinbart, aber nie überprüft – ob Dienstleister sie einhalten, bleibt offen.
- Es fehlen klare vertragliche Pflichten und Eskalationswege für den Fall eines Sicherheitsvorfalls beim Dienstleister.

Controls 5.29 und 8.13

Business Continuity

Im Ernstfall handlungsfähig bleiben

- Informationssicherheit muss nicht nur im Normalfall funktionieren – sondern gerade auch dann, wenn etwas schiefgeht.
- Ein gut gesichertes System nützt wenig, wenn es im Ernstfall nicht wiederhergestellt werden kann.

Stolpersteine:

- Notfall- und Wiederherstellungspläne existieren auf dem Papier – werden aber nie getestet: Der Ernstfall wäre die Premiere hierfür.
- Backups werden erstellt, aber nie auf Vollständigkeit und Wiederherstellbarkeit geprüft – ob sie im Ernstfall tatsächlich funktionieren, bleibt offen.
- Business Continuity wird als IT-Thema behandelt: Verantwortlichkeiten im Ernstfall sind unklar, Geschäftsprozesse und deren Wiederanlaufreihenfolge nicht definiert.

Controls 5.24 bis 5.28

Incident Management

Das leere Vorfallsregister

- Wie eine Organisation auf Sicherheitsvorfälle reagiert, ist einer der zuverlässigsten Indikatoren für den Reifegrad ihres ISMS
- Ein wirksames Incident Management erkennt Vorfälle, behandelt sie strukturiert und zieht Konsequenzen.

Stolpersteine:

- Es gibt keine dokumentierte, kommunizierte Vorgehensweise für Erkennung, Meldung und Behandlung von Sicherheitsvorfällen.
- Vorfälle werden registriert und geschlossen, ohne Ursachenanalyse und ohne Konsequenzen für das ISMS.
- Keine dokumentierten Vorfälle trotz aktiver IT-Nutzung und realer Bedrohungsexposition.
- Der Vorfallmanagementprozess enthält keine Prüfung, ob ein Vorfall externe Meldepflichten auslöst (etwa gemäß DSGVO oder NIS-2).

4.

Zentrale Erfolgsfaktoren eines ISMS

Worauf es wirklich ankommt

Zentrale Erfolgsfaktoren

Was einen Auditor wirklich überzeugt

Die vier Säulen eines wirksamen ISMS:

- Risikoorientierung: Entscheidungen basieren auf einer fundierten, aktuellen Risikobeurteilung – nicht auf Bauchgefühl, Tradition oder dem, was andere Organisationen machen.
- Wirksamkeit: Maßnahmen werden nicht nur implementiert, sondern auch auf ihre tatsächliche Wirkung hin überprüft und gegebenenfalls angepasst.
- Managementverantwortung: Die Führungsebene trägt die Letztverantwortung für das ISMS und steuert dieses aktiv und nachweisbar – sie kann Aufgaben delegieren, nicht aber die Verantwortung.
- Kontinuierliche Verbesserung: Das ISMS entwickelt sich durch Vorfälle, Audits und veränderte Rahmenbedingungen weiter.

Zentrale Erfolgsfaktoren

Was einen Auditor wirklich überzeugt

Weitere Kennzeichen eines reifen ISMS:

- Verhältnismäßigkeit: Das ISMS passt in Größe, Komplexität und Risikolage zur Organisation (das ISMS eines KMU sieht anders aus als das eines großen Konzerns)
- Organisatorische Verankerung als Querschnittsaufgabe: Informationssicherheit ist nicht die alleinige Domäne von IT und CISO; sie muss vielmehr in Prozesse, Verantwortlichkeiten und Kultur der gesamten Organisation eingebettet sein
- Ehrlichkeit im Umgang mit Schwächen: Organisationen, die Lücken offen benennen und aktiv daran arbeiten, überzeugen mehr als solche, die alles schönreden
- Verantwortlichkeiten, die gelebt werden: Risikoeigner kennen ihre Risiken, ohne in der Risikobeurteilung nachschlagen zu müssen

5. Security by Design

Sicherheit als Gestaltungsprinzip – nicht als Korrekturmaßnahme

Controls 5.8 und 8.25 bis 8.29

Security by Design

Von Anfang an sicher

- Gemeinsame Wurzel vieler der vorgestellten Stolpersteine: Informationssicherheit wird nicht als inhärenter Bestandteil der Organisation verstanden, sondern als externe Anforderung, auf die man reagiert (etwa nach einem Audit oder einem Vorfall).
- Security bei Design folgt einem gänzlich anderen Ansatz: Sicherheitsanforderungen werden nicht am Ende eines Projekts geprüft, sondern von Beginn an in die Konzeption von Systemen, Prozessen und Architekturen eingebaut.
- Die ISO/IEC 27001 greift den Gedanken von Security by Design in den Controls 5.8 und 8.25-8.29 auf: Sicherheit als fester Bestandteil von Projekten, Entwicklungsprozessen und Systemarchitektur.
- Was Security by Design für die Informationssicherheit ist, ist Privacy by Design für den Datenschutz – zwei Seiten derselben Medaille → mehr dazu gleich im nächsten Vortrag!

Controls 5.8 und 8.25 bis 8.29

Security by Design

in a nutshell

Die wichtigsten Prinzipien hinter Security by Design:

- Least Privilege: Jeder Nutzer, jedes System, jeder Prozess erhält nur die Rechte, die er für seine Aufgabe tatsächlich benötigt.
- Defence in Depth: Sicherheit wird nicht auf eine einzelne Maßnahme gestützt, sondern auf mehrere unabhängige Schutzschichten; so kompromittiert kein einzelner Fehlerpunkt das gesamte System.
- Fail Secure: Wenn ein System versagt oder in einen Fehlerzustand gerät, fällt es in den sicheren Zustand – nicht in den offenen.
- Security by Default: Systeme werden so konfiguriert, dass die sicherste Einstellung die Standardeinstellung ist, nicht die bequemste.

Vielen Dank
für Ihre
Aufmerksamkeit!
Konsul-Smidt-Straße 88 • 28217 Bremen
T +49 (0) 421 69 66 32-298
Mail: akademie@dsn-group.de
www.dsn-group.de/dsn-akademie