Alternativen zu ISO 27001

Ein Informationssicherheitsmanagementsystem (ISMS) aufzubauen, benötigt viel Zeit und Wissen. Die ISO 27001 ist dazu der Standard, der als Referenz dient. Der erste Teil der Norm beschreibt den Aufbau des ISMS. Darin enthalten sind der Kontext, die Ressourcen, die Risiko-Bewertung, Audits und Verbesserungen. Ergänzt kommen 114 (Version 2013) beziehungsweise 93 Massnahmen (Version 2022) dazu.

Die Norm gilt als komplex in der Umsetzung. Mit mindestens einem Jahr Aufwand ist zu rechnen, bis es zertifiziert werden kann. In Deutschland gibt es die Alternativen CISIS12 und den Standard VdS 10000. Beide werden in der Folge vorgestellt.

CISIS12

Bei CISIS12® handelt es sich um ein Vorgehensmodell zur Einführung eines ISMS. Es richtet sich an kleine und mittlere Unternehmen sowie an Behörden. In zwölf Schritten werden konkrete Umsetzungsmassnahmen und Handlungsempfehlungen aufgezeigt. Es wird vom IT-Sicherheitscluster e.V. entwickelt, herausgegeben, geschult und vertrieben. Informationen zum Modell, Schulungen und Werkzeuge sind unter www.cisis12.de abrufbar. Unter der gleichen Adresse kann das Vorgehensmodell gekauft werden.

Analog dem Vorgehen nach ISO 27001 werden in einem ersten Schritt die Prozesse, Anwendungen, die IT-Infrastruktur und Gebäude erfasst. Ein weiterer wichtiger Punkt ist die Compliance (entspricht dem C im Titel der Norm), welche im gesamten Kontext zu berücksichtigen ist.

Im Standard ist der Zusammenhang zwischen den Themengebieten in Bild 1 festgehalten.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Die Umsetzung von CISIS12 kann durch die Zertifizierungsgesellschaften Deutsche Gesellschaft zur Zertifizierung von Managementsystemen (DQS) oder datenschutz-cert GmbH zertifiziert werden. Für die Schweiz ist dies eine Herausforderung, sind diese Organisationen weniger bekannt. Gemäss Homepage sollen aber weitere Stellen folgen. Wie bei anderen Zertifizierungen gewohnt, ist das Zertifikat drei Jahre gültig, es erfolgen aber ebenfalls jährlich Überwachungsaudits.

Bei der Implementierung stehen folgende Themen im Fokus:

- Rahmenbedingungen, Organisation und Führung
- Personal, Dokumentation und Projektmanagement
- Betrieb und Risikomanagement
- Leistungsbewertung, Kontrolle und Verbesserung

Anhand dieser Themen ist bereits ersichtlich, dass der Aufbau analog der ISO 27001 erfolgt ist. Die zwölf Schritte umfassen folgende Themengebiete:

Schritt 1: Leitlinie erstellen

Die Leitlinie umfasst die Verantwortung der Organisation, Festlegung des Geltungsbereichs, die Gewährleistung der Informationssicherheit, die Definition von Sicherheitszielen, die Umsetzung des Sicherheitskonzepts sowie die Einbindung aller Mitarbeitenden.

Schritt 2: Beschäftigte sensibilisieren

Bereits zu Beginn ist es wichtig, alle Mitarbeitenden miteinzubeziehen. Dazu gehören Schulungen, regelmässige Sensibilisierung und Sicherstellung des Informationsflusses.

Schritt 3: Informationssicherheitsteam aufbauen

Zum Team gehören neben dem Informationssicherheits- (ISB) und Datenschutzbeauftragen (DSB) folgende Rollen: IT-Leiter, Informationssicherheitskoordinator, CISIS12-Berater, Arbeitssicherheit, Gremienvertreter, Facility-Management.

Schritt 4: IT-Dokumentationsstruktur festlegen

Die Norm benennt 15 Pflichtdokumente, zum Beispiel die Leitlinie (Schritt 1), Schulungs- und Sensibilisierung (Schritt 2), ein Betriebshandbuch, Netzplan, Managementbericht, das Risiko-Management und ein Notfallplan. Bei der Umsetzung kommen aber erfahrungsgemäss weitere Dokumente dazu.

Schritt 5: IT-Servicemanagement Prozesse

Dieser Punkt kommt in der ISO 27001 nur am Rande vor, zum Beispiel werden Change Management und Capacity Management erwähnt, weitere Themen fehlen jedoch. Es wird erwartet, dass Wartungsprozesse, Änderungsprozesse oder die Störungsbeseitigung ebenfalls bewertet werden.

Schritt 6: Compliance, Prozesse und Anwendungen

In diesem Schritt werden die Geschäftsprozesse erfasst und gemäss ihrem Schutzbedarf bewertet. Analog einer Business Impact Analyse werden der maximal tolerierbare Datenverlust sowie die maximal tolerierbare Ausfallzeit erfasst. Wie beim BSI-Ansatz erfolgt von hier aus die Vererbung auf die weiteren Themenbereiche. Weiter muss ein Unternehmen bei diesem Schritt die gesetzlichen und vertraglichen Anforderungen erfassen.

Schritt 7: IT-Struktur analysieren

Nach der Erfassung der Geschäftsprozesse folgt die Erfassung der IT-Infrastruktur (Server, Clients, Netzwerkkomponenten, usw.).

Schritt 8: Risikomanagement

Ohne eine Risikobewertung kann heute kein ISMS mehr betrieben werden. Bei CISIS kam dies jedoch erst bei der Version 3 mit dazu. Es stellt damit einen zentralen Ansatz dar.

Schritt 9: Soll-Ist-Vergleich

In einer Selbstbewertung werden die Anforderungen mit dem aktuellen Stand verglichen. Dazu verfügt der Standard über einen

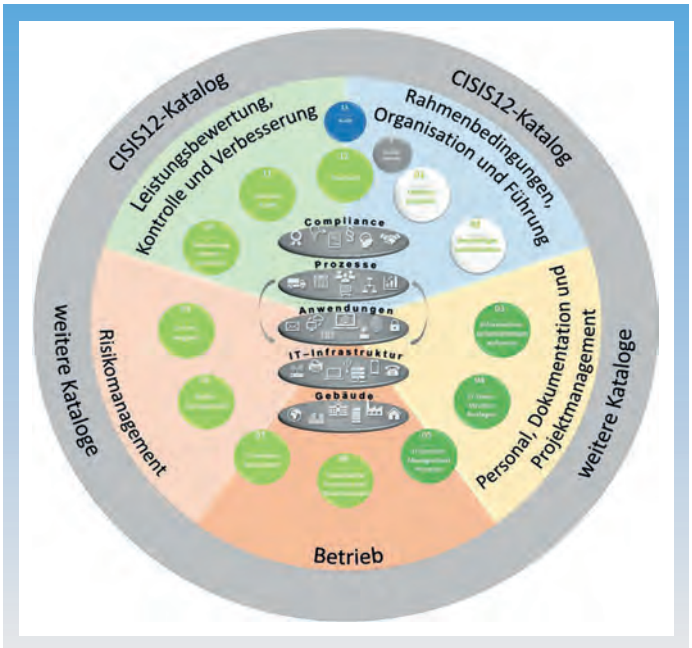

Bild 1: ISIS-Vorgehensmodell und Managementsystemmodell V3.0, Quelle: CISIS-Norm, Seite 5.

	ISO 27001	CISIS12	VdS 10000
Herausgeber	International Standardization Organization ISO	IT-Sicherheitscluster e.V.	VdS Schadenverhütung GmbH
Norm	Ja, 30 Seiten	Ja, 30 Seiten	Nein
Region	International	DACH-Region	Deutschland
Komplexität	Hoch	Hoch	Niedrig
Aufbau/Umfang	Managementsystem, 114 Massnahmen (93 in der Ausgabe 2022)	Vorgehensmodell mit 87 Bausteinen und 1000 Massnahmen	Checkliste
Risikoanalyse	Ja, verpflichtend	Ja, verpflichtend	optional
Zertifizierung	Ja, unabhängige akkreditierte Stelle	Ja, unabhängige akkreditierte Stelle	Ja, durch VdS

Bild 2: Vergleich der drei Standards.

reichhaltigen Bausteinkatalog, der beigezogen werden kann.

Schritt 10: Umsetzung planen und umsetzen
Die Abweichungen aus dem vorherigen Schritt werden erfasst und die Behebung der Mängel geplant und umgesetzt. Gleichzeitig kann ein Reifegrad des Managementsystems erstellt werden.

Schritt 11: Internes Audit
Wie in der ISO 27001 gilt es ein Auditprogramm zu erstellen. Das Ziel dabei ist es, Schwachstellen zu finden und diese zu beheben.

Schritt 12: Revision
Die Schritte 1 bis 11 müssen regelmässig durchlaufen werden. Veränderungen und Ergänzungen sind in diesem Schritt anzubringen. Das Ergebnis ist ein Managementbericht.

VdS 10000

Die VdS 10000 wird von der VdS Schadenverhütung GmbH kostenpflichtig herausgegeben. Sie kann unter https://vds.de/cyber/vds10000 bezogen werden.

Die VdS 10000 stellt ein Managementsystem für KMU, Verwaltungen, Verbände und sonstige Organisationen anwendbar. Ergänzend stehen die Dokumente VdS 10005 (Mindestanforderungen an die IT-Sicherheit für Klein- und Kleinstunternehmen), VdS 10010 (Datenschutz für KMU gemäss DSGVO) sowie VdS 10020 (Leitfaden zur Interpretation für industrielle Automatisierungssysteme). Diese Dokumente werden an dieser Stelle aber nicht weiter vertieft. Die VdS 10000 hat folgenden Aufbau:

- Im Kapitel 3 werden diverse Begriffe erläutert, die in diesem Dokument genutzt werden.
- Das Kapitel 4 behandelt die Organisation der Informationssicherheit. Dies beinhaltet die Verantwortlichkeiten (Zuweisung und Dokumentation, Funktionstrennungen, zeitliche Ressourcen), Anforderungen an das Topmanagement, den Informationssicherheitsbeauftragten (ISB), das Informationssicherheitsteam, IT-Verantwortliche, Administratoren, Vorgesetzte, Mitarbeiter, Projektverantwortliche und Externe.
- Im Kapitel 5 wird die Leitlinie zur Informationssicherheit beschrieben. Dieses Kapitel umfasst lediglich allgemeine Anforderungen und Inhalte.
- Ergänzend werden im Kapitel 6 Richtlinien zur Informationssicherheit gefordert. Dazu gehören Regelungen für Nutzer, mobile IT-Systeme, mobile Datenträger, IT-Outsourcing und Cloud Computing, Datensicherung, Störungen und Ausfälle sowie Sicherheitsvorfälle.
- Das Kapitel 7 betrifft die Mitarbeitenden und verlangt Verfahren für die Aufnahme, Wechsel und Beendigung.
- Einen wichtigen Aspekt bildet das Wissen. Dieses wird in Kapitel 8 berücksichtigt. Dazu gehören Schulung und Sensibilisierung.
- Im Kapitel 9 werden die Prozesse und die kritischen IT-Ressourcen identifiziert, im Kapitel 10 folgen die IT-Systeme. Dazu gehören auch ein Basisschutz (Software, Beschränkung des Netzwerkverkehrs, Protokollierung, externe Schnittstellen und Laufwerke, Schadsoftware, fremde Medien, Authentifizierung, Zugänge und Zugriffe) sowie Massnahmen bei der Nutzung von mobilen oder kritischen Systemen. Im Kapitel 11 folgen die Netzwerke und Verbindungen, in Kapitel 12 mobile Datenträger, in Kapitel 13 die Umgebung sowie in Kapitel 14 IT-Outsourcing und Cloud Computing.
- Weitere wichtige Punkte sind in Kapitel 15 die Zugänge und Zugriffsrechte sowie in Kapitel 16 die Datensicherung und Archivierung
- Das Kapitel 17 behandelt Störungen und Ausfälle und das Kapitel 18 Sicherheitsvorfälle.

Die VdS 10000 kann nicht durch eine unabhängige Stelle zertifiziert werden. Als Start in das komplexe Thema ist das Vorgehen aber eine solide Unterstützung.

Vergleich

Bild 2 zeigt einen Vergleich der drei Standards. Diese erweiterte und korrigierte Tabelle orientiert sich an Frank Moses (unabhängiges Datenschutzzentrum Saarland) und Thomas Rehbohm (CISO der Freien Hansestadt Bremen).

Fazit

Der Aufbau eines ISMS benötigt viel Zeit und solides Wissen. Rein nach einer Norm wie die ISO 27001 vorzugehen, lässt viele Fragen offen. Die Norm beschreibt zwar, wie das Ergebnis auszusehen hat, der Weg dahin ist aber offen. CISIS12 und VdS 10000 können dabei ein hilfreiches Werkzeug sein, das Ziel erfolgreich zu erreichen. Die Checklisten-Form der VdS 10000 leitet schrittweise durch den Prozess, die 87 Bausteinen mit 1000 Massnahmen der CISIS12 helfen, die notwendigen Massnahmen umzusetzen. Zusammen sind sie ein wertvolles Werkzeug zur Erreichung einer erfolgreichen Zertifizierung.

Entdecke die Welt grenzenloser Produktentwicklung

INNEO ermöglicht es Ihnen, Beeindruckendes zu erschaffen!

Mit unserem grossartigen Spektrum für ineinandergreifende CAD/PLM/IoT-Lösungen in allen Phasen und mit allen Beteiligten erhöhen Sie Ihre Effizienz.
Steigern Sie Ihre Innovationskraft!

Jetzt mehr erfahren:
www.inneo.ch/pe

INNEO®
That's IT.