Auditmanagement nach ISO/IEC 27002:2022

Know-how to go – ISO 27001 Novellierung

HiSolutions AG

Jerome Horn

Jerome Horn

Senior Consultant

Fachliche Schwerpunkte

- Beratung zu den Themen Informationssicherheitsmanagement nach BSI IT-Grundschutz sowie nach ISO 27001
- Internes Auditmanagement sowie Auditierung und Zertifizierung von ISMS
- Informationssicherheit im Banken- und Finanzdienstleistungsumfeld

Qualifikationen

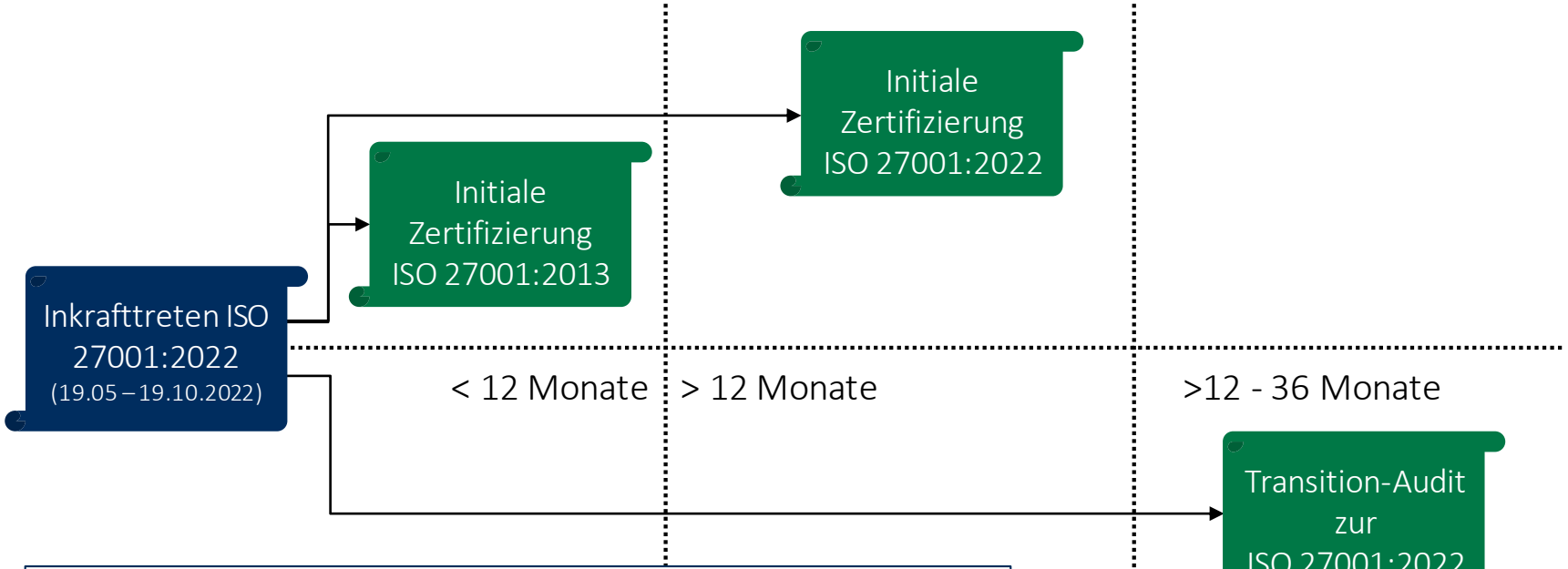
- Zertifizierter ISMS Lead Auditor ISO 27001
- Zertifizierter Auditor nach ISO/IEC 27001 Energiewirtschaftsgesetz
- Zertifizierter ISMS Lead Auditor ISO 22301
- BSI IT-Grundschutz Praktiker
- Zusätzliche Prüfverfahrenskompetenz für § 8a BSIG

Agenda

1. Übergangsfristen und relevante Key Facts
2. Auditierung neuer Controls
3. Auditplanung nach neuer Normstruktur
4. Vorteile der Attributsstruktur bei Reifegradbestimmung

1. Übergangsfristen und relevante Key Facts

Auswirkungen auf bestehende und zukünftige Zertifizierungen



Diese Annahmen basieren auf Erfahrungen vergangener Aktualisierungen. Übergangsperioden können in Abhängigkeit von der Akkreditierungsstelle abweichen. Maßgeblich für den deutschsprachigen Raum ist hierbei vor allem die Bekanntgabe der DAkkS.

2. Auditierung neuer Controls

Neue und überarbeitete Controls, um die Themenvielfalt zu erhalten und den Schutzbereich zu erweitern

Keine einzige Maßnahme wurde unverändert aus der bisherigen Norm übernommen:

Ein Control entfällt (11.2.5 Removal of assets)

Der FDIS listet derzeit 11 „neue“ Controls

Die anderen Controls wurden neu formuliert

56 Controls wurden auf 24 komprimiert

Die Controls der ISO 27002:2021 werden in 4 Themen sortiert, nicht 14 Annexen

Organizational Controls

Physical Controls

People Controls

Technological Controls

A.5.7 Threat intelligence

Informationen bzgl. Informationssicherheits-gefährdungen müssen zur frühzeitigen Bedrohungs-erkennung gesammelt und analysiert werden.

➡ *Permanentes Monitoring der Bedrohungslage (Bedrohungsaufklärung)*

Umsetzungsmöglichkeiten:

a) Sollte auf unterschiedlichen Ebenen (strategisch, taktisch und operativ) betrieben werden
b) Ergreifung geeigneter Abhilfemaßnahmen
c) Systematische Datensammlung und Bewertung
d) Sensibilisierung und Kommunikation

A.5.23 Information security for use of cloud services

Verfahren zur Beschaffung, Nutzung, Steuerung und zum Austritt von Cloud-Diensten im Einklang mit IS-Aspekten sollten etabliert werden.

➡ *Angemessener Umgang mit Informationssicherheit bei der Nutzung von Cloud-Diensten*

Umsetzungsmöglichkeiten:

a) Verfahren für die Verwaltung von Cloud-Diensten in Übereinstimmung mit IS-Anforderungen
b) Cloud Security Richtlinie
c) Sicherheitsrisikomanagement für Cloud-Dienste
d) Regelungen der Verantwortlichkeiten der Cloud-Service-Anbieter/-Kunden
e) Erstellung von spezifischen Cloud Service Agreements

A.5.30 ICT readiness for business continuity

Auf Basis der Kontinuitätszielen ist die IKT-Bereitschaft zu planen, umzusetzen und aufrechtzuerhalten.

Implementierte IKT-Bereitschaft auf Basis von Geschäftskontinuitätszielen und IKT-Kontinuitätsanforderungen

Umsetzungsmöglichkeiten:

a) Erforderliches Verfügbarkeitsniveau der IKT-Dienste auch während Störungen erreichen
b) Business Impact Analyse (BIA) und Risikobewertung für IKT-Dienste
c) IKT- Kontinuitätsstrategien entwickeln

A.7.4 Physical security monitoring

Betriebsgelände sind kontinuierlich auf unberechtigte Zutritte zu überwachen.

Permanente Zutrittskontrolle für Gebäude/Räume, in denen sich kritische Systeme befinden

Umsetzungsmöglichkeiten:

a) Erkennen und Abschrecken von unbefugtem physischen Zugang
b) Nutzung und Verwaltung (extern/intern) von Überwachungssystemen
c) Vorgaben zur Verwaltung und Nutzung von Schlüsseln

A.8.9 Configuration management

(Sicherheits-)Konfigurationen von Assets sind zu definieren und dokumentieren sowie kontinuierlich zu überprüfen.

Kontrollierte Einführung, Dokumentation und Überwachung von Sicherheitskonfigurationen

Umsetzungsmöglichkeiten:

a) Hardware-, Software-, Service- und Netzwerkkonfigurationen sollten IS-Sicherheitsanforderungen unterliegen
b) Standardvorlagen für Sicherheitskonfigurationen
c) Lenkung von Dokumentationen über Sicherheitskonfigurationen (siehe Clause 7.5)

A.8.10 Information deletion

Informationen, die auf jeglichen Systemen und Datenträgern gespeichert sind, sind nach ihrer Nutzungsdauer, zu löschen.

Vernichtung nicht benötigter gespeicherter Informationen in Informationssystemen und -geräten

Umsetzungsmöglichkeiten:

a) Vermeidung der Offenlegung schutzbedürftiger Informationen
b) Einhaltung gesetzlicher, behördlicher und vertraglicher Anforderungen zur Datenlöschung
c) Verfahrensanweisungen zur vollständigen Löschung und Vernichtung von Informationen

A.8.11 Data masking

Unter Berücksichtigung gesetzlicher Vorgaben und des Zugriffsschutz ist eine Datenmaskierung zu etablieren.

Einsatz einer Datenmaskierung in Übereinstimmung mit unternehmensinternen Richtlinien zur Zugriffskontrolle und geltenden Gesetzen

Umsetzungsmöglichkeiten:

a) Schutz sensibler und personenbezogener Daten
b) Einhaltung gesetzlicher, behördlicher, betrieblicher & vertraglicher Anforderungen
c) Anwendung von Pseudonymisierungs- oder Anonymisierungstechniken
d) Einschränkung von Zugriffen auf Informationen basierend auf dem Need-to-Know-Prinzip

A.8.12 Data leakage prevention

Für Informationssysteme und Netze sind Maßnahmen zur Vermeidung von Datenabflüssen umzusetzen.

Verhinderung der unbefugten Offenlegung und Extraktion von Informationen

Umsetzungsmöglichkeiten:

a) Maßnahmen zur Verhinderung von Datenlecks auf Systemen, Netzwerken und Endgeräten
b) Klassifizierung von Informationen
c) Überwachung der Kommunikationskanäle
d) Tools zu Verhinderung und Detektion von Datenlecks

A.8.16 Monitoring activities

Netze, Systeme und Anwendungen sind bzgl. Auffälligkeiten zu monitoren, welche auf mögliche Informationssicherheitsvorfälle zu bewerten sind.

➡ *Überwachung der Netze, Systeme und Anwendungen auf anomales Verhalten*

Umsetzungsmöglichkeiten:

a) Erkennen von anomalem Verhalten und potentiellen Informationssicherheitsvorfällen
b) Möglichst automatisierte Auswertungen nach definierten Use Cases (SIEM)

A.8.23 Web filtering

Der Zugang zu externen Webseiten sollte gesteuert werden, um die Bedrohung durch schadhafte Inhalte zu reduzieren.

➡ *Verwaltung des Zugangs zu externen Websites*

Umsetzungsmöglichkeiten:

a) Browser- und Anti-Malware- Technologien
b) Zugang zu bestimmten Websites sperren
c) Regelungen zum Umgang mit externen Websites

A.8.28 Secure coding

Innerhalb der Softwareentwicklung sind sichere Entwicklungsprinzipien zu etablieren.

Anwendung sicherer Grundsätze und Prinzipien bei der Softwareentwicklung

Umsetzungsmöglichkeiten:

a) Es sollten Grundsätze für die Softwareentwicklung festgelegt werden
b) Für unterschiedliche Programmiersprachen sollten Standards entwickelt werden
c) Bekannte Schwächen von Programmiersprachen und Techniken sollten bekanntgemacht werden

3. Auditplanung nach neuer Normstruktur

Einführung von Attributen
als grundsätzliche Neuerung der ISO 27002:2021

Control Type
#Preventive

Security domains
#Governance_and_Ecosystem
#Protection

Information security properties
#Confidentiality
#Integrity
#Availability

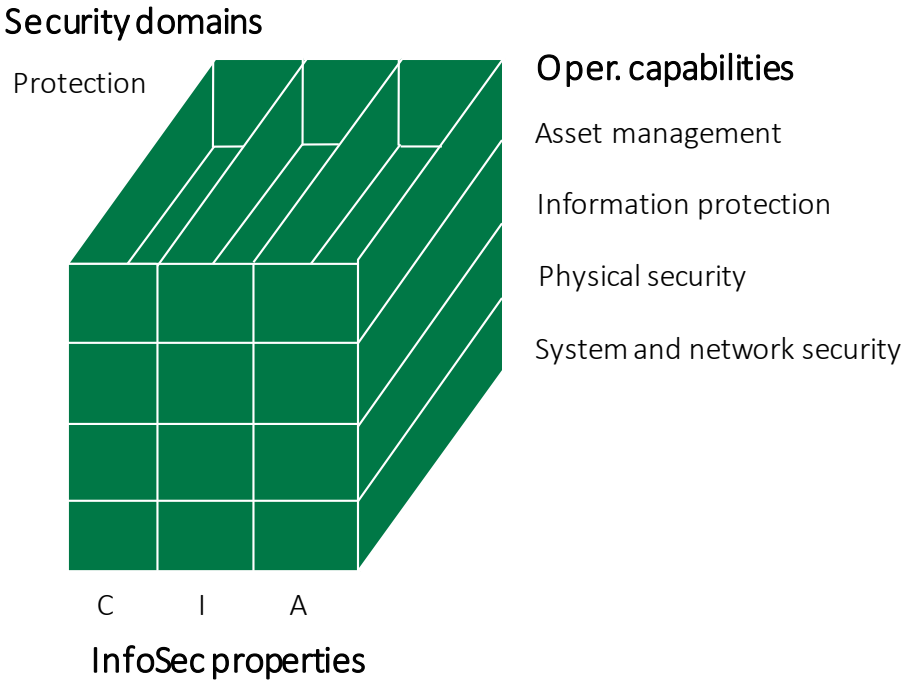
Operational capabilities
#Supplier_relation-ships_security

Cybersecurity Concepts
#Protect

Die Attribute brechen Fachthemen-Silos auf

4. Vorteile der Attributsstruktur bei Reifegradbestimmung

Attributsstruktur erlaubt präzisere Identifizierung offener Flanken



A. 6.7 Remote working

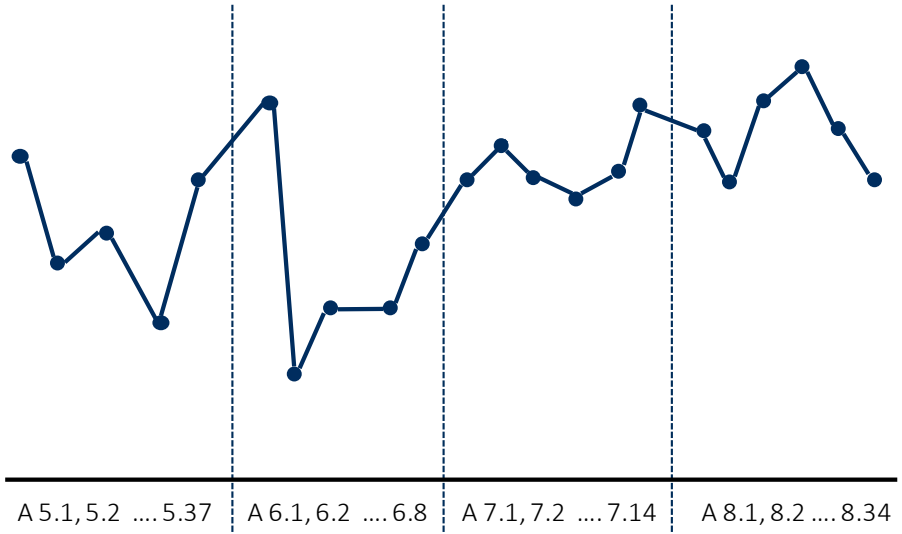
Für den Fall von Remote-Tätigkeiten sind Sicherheitsmaßnahmen zu etablieren, die den Schutz von Informationen außerhalb des Betriebsgeländes sicherstellen.

Mögliche Fragestellungen anhand der Attributsstruktur:

a) Sind meine physischen Sicherheitsmaßnahmen ausreichend, um einen sicheren Home-Office-/ Remote-Betrieb zu gewährleisten?

b) Unterstützt die Verfügbarkeit meiner Unternehmensinfrastruktur einen stabilen Home-Office-/Remote-Betrieb?

Spezifische Reifegradbestimmung von Informationssicherheits-zielen und -Fähigkeiten



<u>Mögliche Ableitungen auf Basis von Auditergebnissen und Reifegradbestimmungen:</u>

a) Wie stark sind die jeweiligen Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität in meinem Kontext abgesichert?
b) Liegen die größten Handlungsbedarfe im technologischen oder organisatorischem Handlungsfeld?
c) Wie stark sind meine detektiven vs. reaktiven Fähigkeiten im Incident-Management?
d) Haben technologische Änderungen einen Einfluss auf den Reifegrad?

Haben Sie Fragen?

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com