Datenschutz und Informationssicherheit als Managementsystem etablieren

suhling management consulting

REFERENT PETER SUHLING

VORTRAG: 15.09.2022

Inhalt

Bedeutung ISO 27001 und ISO 27701

Elemente eines Managementsystems

Unterschiede der Standards

Einführung DSMS mit Zertifizierung

Auditierung des DSMS

Kosten eines DSMS

Implementierung und Betrieb eines DSMS nach ISO/IEC 27701

Bedeutung ISO 27001 und ISO 27701

Bedeutung ISO 27001 und ISO 27701

Informationssicherheitsmanagementsystem (ISMS):
Die ISO 27001 beschreibt ein Managementsystem, welches durch eine akkreditierte Zertifizierungsgesellschaft zertifiziert werden kann.

Datenschutzmanagementsystem (DSMS):
Die ISO 27701 heißt: „Sicherheitstechniken - Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Management von Informationen zum Datenschutz - Anforderungen und Leitlinien (ISO/IEC 27701:2019);“ Dieser Standard kann nicht alleine zertifiziert werden, sondern nur als Erweiterung mit der ISO 27001.

Elemente eines Managementsystems

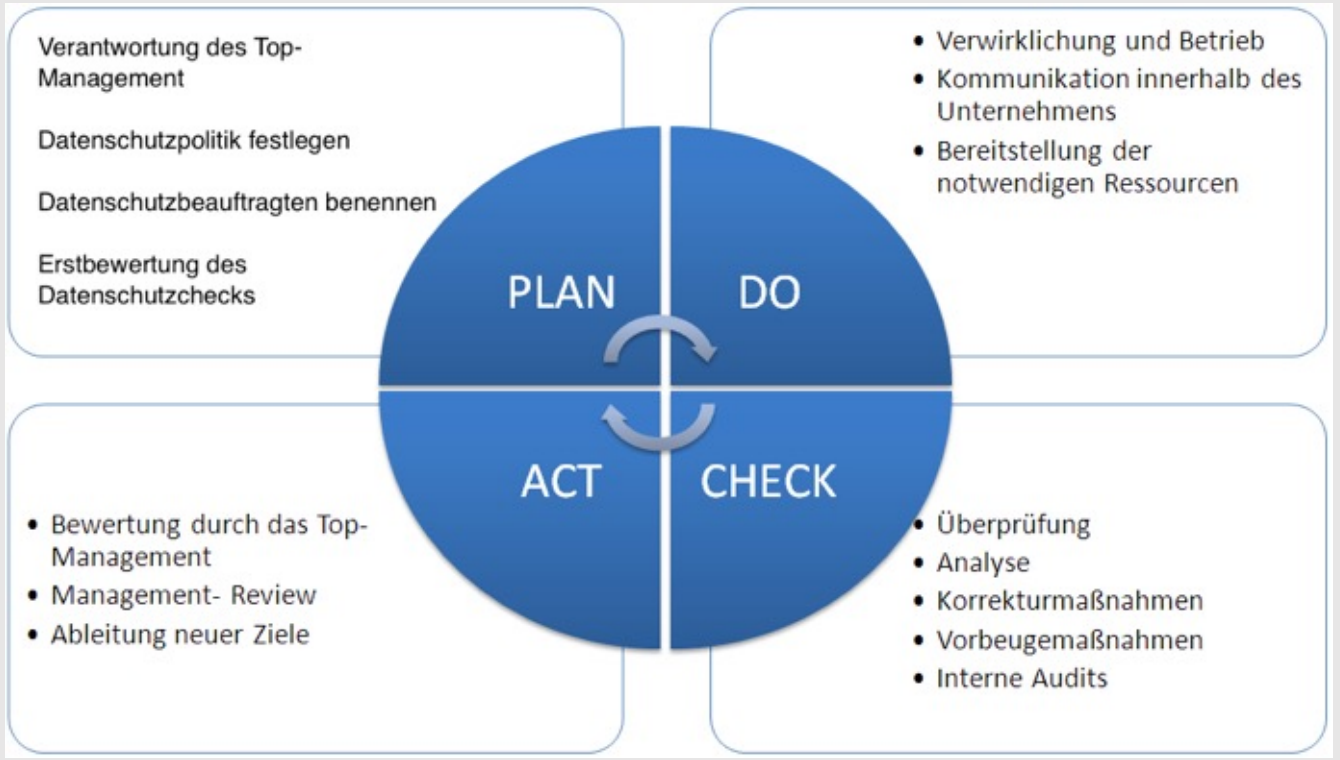
Elemente eines Managementsystems

PDCA - Plan, Do, Check, Act - Demingkreis

Quelle: wikipedia

Elemente eines Managementsystems

PDCA angepasst an den Datenschutz



Quelle: wikipedia

Elemente eines Managementsystems

Normabschnitte am Beispiel der ISO 27001 - Informationsschutz:

Nr.0 Einleitung

Nr.1 Anwendungsbereich

Nr.2 Normative Verweisungen

Nr.3 Begriffe

Nr.4 Kontext der Organisation

Nr.5 Führung

Nr.6 Planung

Nr.7 Unterstützung

Nr.8 Betrieb

Nr.9 Bewertung der Leistung (Interne Auditierung)

Nr.10 Verbesserung

Anhang A (normativ)
Referenzmaßnahmenziele und -maßnahmen

Elemente eines Managementsystems

Was ein IMS ist:

Unterschiedliche Managementsysteme verbinden durch Integrierte Managementsysteme

„…Das integrierte Managementsystem „IMS“ verbindet die ursprünglich getrennten Managementsysteme bzw. Teilmanagementsysteme zu einem einheitlichen Managementsystem, das alle Aspekte und Aufgaben der einzelnen Managementsysteme ganzheitlich umfasst…“

Quelle: Wikipedia

Unterschiede der Standards

Unterschiede der Standards

Übereinstimmungstabelle erarbeiten

Thema	EU-DSGVO	ISO 27001:2017 (ISMS)	ISO 27701:2020 (DSMS)
Risikobewertung / Risk Assessment	Erwägungsgrund 77, Artikel 35	A.8.2.1	A.6.5.2.1
Einhaltung gesetzlicher und vertraglicher Anforderungen / Compliance	Erwägungsgrund 85, Artikel 9	A.18.1.1	A.6.15.1.1
Anzeigepflicht / Breach notification	Artikel 33	A.16.1	A.6.13.1.1
Verwaltung der Werte / Asset Management	Artikel 5, Artikel 7, Artikel 9…	A.8.1.1	A.6.5.11
Datenschutz durch Technikgestaltung und durch daten- schutzfreundliche Voreinstellungen / Privacy by Design	Artikel 25	A.14.1.1	A.6.11.1.1
Lieferantenbeziehungen / Supplier Relationships	Artikel 26	A.15.1.1	A.6.12.1.1

Unterschiede der Standards

Beachtet werden muss die neuestes Ausgabe der ISO 27001 (analog dazu die ISO 27002):

Die Nummerierung und die Inhalte haben sich geändert:

Die neue Version gliedert sich in 93 Maßnahmen, unterschieden in vier Bereiche:

Organizational controls (37 Maßnahmen); People controls (8 Maßnahmen);

Physical controls (14 Maßnahmen); und Technological controls (34 Maßnahmen).

Folge: Die Normabschnitte müssen abgeglichen werden, bevor mit der Implementierung begonnen werden kann.

Einführung DSMS mit Zertifizierung

Einführung DSMS mit Zertifizierung

suhling management consulting

Zertifizierungsmöglichkeiten:
Datenschutzmanagementsystem mittels

ISO 27001 + ISO 27701

1. ISO 27001 - ISMS

2. ISO 27701 - DSMS

3. Zertifizierung nach ISO 27001 – ISMS und 27701 - DSMS

Einführung DSMS mit Zertifizierung

suhling management consulting

Zertifizierungsmöglichkeiten: Datenschutzmanagementsystem mittels

ISO 27001 + ISO 27701

Datenschutz-Zertifizierung mit ISO-Standard:

1. Zertifizierungsgesellschaft anfragen, ob Kombizertifizierung 27001 und Datenschutz möglich ist.

2. Die Anwendbarkeitserklärung (SoA) der ISO 27001 mit den Datenschutz-Normelementen der ISO 27018 oder 27701 oder 29100 auffüllen.

3. Von einer Zertifizierungsgesellschaft zertifizieren lassen. Vorher Angebot einholen.

Einführung DSMS mit Zertifizierung

suhling management consulting

Stand 15.09.2022:

Von der DAkks (Deutsche Akkreditierungsstelle) ist bisher noch kein Standard für Zertifizierungsgesellschaften akkreditiert, nachdem sich Unternehmen und Organisationen über eine Zertifizierungsgesellschaft zertifizieren lassen können.

Auditierung des DSMS

Auditierung des DSMS

Auditarten im Überblick:

First-Party-Audit: Interne Auditierung:

Mindestens jährliche Wiederholung bei einer angestrebten Zertifizierung.

Second-Party-Audit: Lieferantenaudit

Jährliche Wiederholung angepasst an Bedarfe (ABC-Kunden, Aufwände)

Third-Party-Audit: Audits von der Zertifizierungsgesellschaft:

1. Zertifizierungsaudit, 2. Überwachungsaudit, 3. Wiederholungsaudit, und so weiter...

Auditierung des DSMS

Welche Audits können erwartet werden?

First-Party-Audit: Interne Auditierung durch den Datenschutzbeauftragten

Second-Party-Audit: Lieferantenaudit durch den Datenschutzbeauftragten (Prüftourismus)

Third-Party-Audit: Zertifizierungsaudits durch externe Auditoren

Achtung: Das „Interne Audit“ ist eine Voraussetzung für eine Zertifizierung im Datenschutz – DSMS (ISO 27701) oder nach Informationssicherheit - ISMS (ISO 27001)!

Kosten eines DSMS

Kosten eines DSMS

Start auf grüner Wiese:

Erfahrungen aus Projekten zur Einführung von ISO 27001: DSMS ca. 20-30 Tage für den Implementierer (Ist-Aufnahme und Workshoptage). Die Mitarbeit vom Unternehmen wird angenommen.

Ebenfalls abhängig vom ISO-Team (Mitarbeiter, die aktiv an dem Aufbau der Dokumentation mitwirken).

Mit oder ohne vorhandenem Managementsystem:

Abhängig, ob Unternehmen bereits Managementsystem einsetzt oder nicht.

Externe und interne Mitarbeit:

Abhängig, ob externer Projektleiter oder interner Mitarbeiter die Projektleitung (DSB) übernimmt.

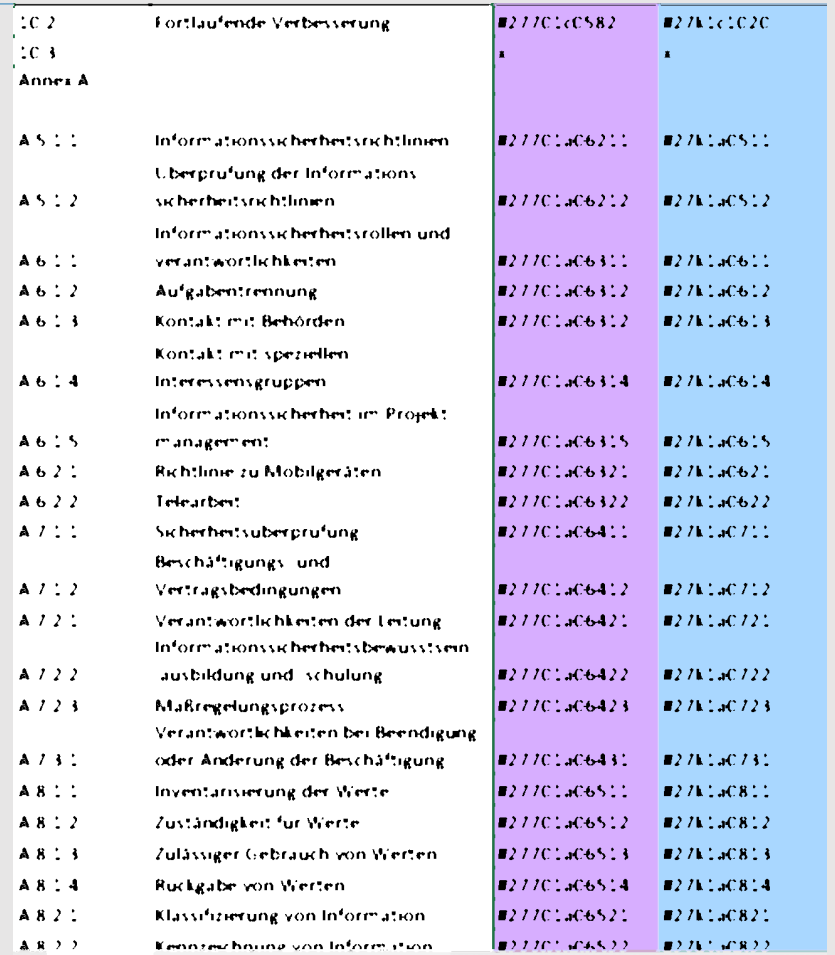
Implementierung und Betrieb eines DSMS nach ISO/IEC 27701

Implementierung und Betrieb eines DSMS nach ISO/IEC 27701

Umsetzung der ISO 27701 angelehnt an die ISO 27001:

Der Normenkörper (Klauseln / Clauses) von 4-10, sowie die 114 Maßnahmenziele (Controls) müssen umgesetzt werden...

...bis auf die begründeten Ausschlüsse.



:C 2	Fortlaufende Verbesserung	#27/C1:C582	#27k1:C2C
:C 3		x	x
Annex A			
A 5 : 1	Informationssicherheitsrichtlinien	#277C1:aC621:	#27k1:aC5:1
A 5 : 2	Überprüfung der Informations sicherheitsrichtlinien	#277C1:aC621:2	#27k1:aC5:2
A 6 : 1	Informationssicherheitsrollen und verantwortlichkeiten	#277C1:aC631:	#27k1:aC61:
A 6 : 2	Aufgabentrennung	#277C1:aC631:2	#27k1:aC61:2
A 6 : 3	Kontakt mit Behörden	#277C1:aC631:2	#27k1:aC61:3
A 6 : 4	Kontakt mit speziellen Interessensgruppen	#277C1:aC631:4	#27k1:aC61:4
A 6 : 5	Informationssicherheit im Projekt management	#277C1:aC631:5	#27k1:aC61:5
A 6 2 :	Richtlinie zu Mobilgeräten	#277C1:aC6321:	#27k1:aC621:
A 6 2 2	Telearbeit	#277C1:aC6322	#27k1:aC622
A 7 : :	Sicherheitsüberprüfung	#277C1:aC641:	#27k1:aC71:
A 7 : 2	Beschäftigungs und Vertragsbedingungen	#277C1:aC641:2	#27k1:aC71:2
A 7 2 :	Verantwortlichkeiten der Leitung	#277C1:aC6421:	#27k1:aC721:
A 7 2 2	Informationssicherheitsbewusstsein ausbildung und schulung	#277C1:aC6422	#27k1:aC722
A 7 2 3	Maßregelungsprozess	#277C1:aC6423	#27k1:aC723
A 7 3 :	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	#277C1:aC643:	#27k1:aC73:
A 8 : :	Inventarisierung der Werte	#277C1:aC651:	#27k1:aC81:
A 8 : 2	Zuständigkeit für Werte	#277C1:aC651:2	#27k1:aC81:2
A 8 : 3	Zulässiger Gebrauch von Werten	#277C1:aC651:3	#27k1:aC81:3
A 8 : 4	Rückgabe von Werten	#277C1:aC651:4	#27k1:aC81:4
A 8 2 :	Klassifizierung von Information	#277C1:aC6521:	#27k1:aC821:
A 8 2 2	Kennzeichnung von Information	#277C1:aC6522	#27k1:aC822

Quelle: ISO/IEC 27001:2017

Fragerunde

Ihre Fragen bitte!

Vielen Dank

Peter Suhling - suhling management consulting

Website: suhling.biz - E-Mail: info@suhling.biz

Urheberrechtshinweise

Diese Unterlagen sind als Begleitmaterial zum „Zertifikatskurs Datenschutzmanagement“, sowie zum Kurs „Erfolgreiches Datenschutzmanagement nach DSGVO“ von suhling management consulting, Peter Suhling, gedacht und nicht zum Selbststudium geeignet.