0800 400 510 1

AKTUELLE INFORMATION WAS IST EINE SOA?

Prozessmanagement - Nr. 05/2021

Prozessmanagement

Wir entlasten Führungskräfte und schützen Mitarbeiter. Seit 1997.

Was ist eine SOA? - ISO 27001 Statement of Applicability verstehen und umsetzen

Heute widmen wir uns in der Reihe rund um das Informationssicherheitsmanagement um die sog. „Erklärung zur Anwendbarkeit", auch kurz SOA oder Statement of Applicability genannt. Was verbirgt sich hinter der SOA und weshalb ist sie solch ein wichtiges zentrales Instrument im Informationssicherheitsmanagementsystem (ISMS)?

Grundsätzlich listet die SOA Maßnahmen zur Risikobehandlung aus dem Anhang A der ISO 27001 auf und erlaubt so deren Kontrolle. Sie stellt also somit die wesentliche Verknüpfung zwischen der Risikoeinschätzung und -behandlung und den Maßnahmen der Informationssicherheit dar.

Maßnahmen für die Informationssicherheit

In einem ersten Schritt werden alle Maßnahmen gelistet und hinsichtlich ihrer Anwendbarkeit unter Angabe des jeweiligen Grundes der Zulassung oder auch Ausschluss unter Berücksichtigung des organisatorischen Kontextes beurteilt. Hier erfolgt somit also eine Beurteilung wie Assets / Werte eines Unternehmens durch welche Maßnahmen geschützt werden.
Des Weiteren werden hier Maßnahmen benannt, welche ggf. aus anderen Gründen erforderlich sind. Dies kann gesetzlicher, regulatorischer oder vertraglicher Natur oder auch prozessbedingt sein. Hier lohnt auch der Blick in den Katalog des IT-Grundschutzkataloges des BSI.

Zweitens kann eine Beurteilung der Risikoeinschätzung, durchaus einen größeren Umfang erreichen. Für den täglichen Betrieb ist dies unter Umständen nicht wirklich hilfreich. Für die Kommunikation mit dem Management hat man mit der SOA ein geeignetes Instrument, um klar und übersichtlich Informationen über den Status vorzulegen und eventuelle Handlungsbedarfe zu argumentieren.

Drittens (mit höchster Priorität!) dokumentiert die SOA, ob jede Maßnahme bereits umgesetzt wurde. Auch hier ist es ein Zeichen von „Best Practice“, dass Maßnahmen gut beschrieben werden, so z. B. durch Verweis auf Arbeitsverfahren, Richtlinien, Arbeitsanweisungen etc.
Daher wird das Hauptaugenmerk des Prüfers beim Audit immer auf der SOA sein!
Bei einem Prozessaudit ist für den Auditor der Produktionslenkungsplan PLP das wichtigste Dokument für den Auditprozess. Mit dem PLP auditiert der Auditor

Leistungsangebot Prozessmanagement

AKTUELL & WICHTIG!

Krisenmanagement- und Prozessmanagement Beratung

Potentiale identifizieren & analysieren

Strukturen entwickeln & gestalten

Prozesse festlegen & zielgerichtet steuern

Lifecycle & nachhaltige Entwicklung

Managementsysteme - QHSE

WIE KÖNNEN WIR IHNEN HELFEN?

FKC CONSULT GmbH
Eschenburgstr. 5
23568 Lübeck
www.fkc-gmbh.de

prozessmanagementanfrage@fkc-gmbh.de

0800 400 510 1

AKTUELLE INFORMATION
WAS IST EINE SOA?

Prozessmanagement - Nr. 05/2021

Prozessmanagement

entlang des Materialflusses den Produktionsprozess. Im ISMS Audit nimmt sich der Auditor die Anwendbarkeitserklärung und auditiert entlang der SOA, um sicherzustellen, wie die Kontrollen installiert worden sind.

Wie erstellt man eine SOA?

- Auflistung aller Kontrollen (mind. 114 aus dem Anhang A der ISO 27001)
- Definition und Einschätzung ob anwendbar oder nicht anwendbar
- Argumentation für die Entscheidung
- Ziele festlegen, welche mit den Kontrollen dieser Punkte erreicht werden sollen
- Beschreibung wie und mit welchen Maßnahmen diese erreicht werden sollen

Beispiel:

ID	Maßnahmen gemäß ISO/IEC 27001	Anwendbarkeit (JA/NEIN)	Grund für Auswahl/ Ausschluss	Maßnahmenziele	Umsetzungsmethode	Status: Geplant Teilw. umgesetzt* umgesetzt
A.9.3	Verantwortlichkeiten der Benutzer			Benutzer sind für den Schutz ihrer Authentisierungsinformation verantwortlich gemacht.		
A.9.3.1	Verwaltung der geheimen Authetifizierungsinformation der Benutzer	JA			Beschreibung in den Dokumenten: 2019-02-02_A08-Werte_20_Sicherheitspolitik_V1.0.docx 2019-02-02_A09-Zugangssteuerung_10_Zugangssteuerung-Richtlinie_V1.0.docx 2019-02-02_A09-Zugangssteuerung_20_Passwort-Richtlinie_V1.0.docx	Vollständig umgesetzt

Für das Thema Zugangssteuerung (A9) gibt es zum Punkt „Verantwortlichkeiten der Benutzer“ (A9.3) eine Maßnahme, nämlich A9.3.1 „Verwaltung der geheimen Authentifizierungsinformationen der Benutzer“.
In der SOA legen Sie somit fest, ob diese Maßnahmen einbezogen werden oder nicht. Wenn das nicht der Fall ist, muss dies kurz begründet werden. Weiterhin sollten Sie neben den Maßnahmenzielen auch die Methode der Umsetzung kurz beschreiben. In unserem Beispiel wird auf drei Dokumente verwiesen, in denen das im Detail beschrieben ist. Kein MUSS aber ein gern gesehenes KANN ist die Darstellung des Status der Umsetzung.

Haben wir Ihr Interesse daran geweckt, wie Sie IHRE Informationen hinsichtlich Integrität, Vertraulichkeit und Verfügbarkeit schützen können? Gerne stehen Ihnen unsere Experten zur Verfügung. Wir bieten Ihnen die optimale Betreuung zur Implementierung und Pflege eines Informationssicherheitsmanagementsystem nach DIN ISO/IEC 27001 oder auch anderer Normen aus der Informationssicherheit, wie z.B. den BSI Grundschutzkatalog, TISAX und weitere.

Weitere Informationen erhalten Sie unter prozessmanagementanfrage@fkc-gmbh.de

Bilder von Canva.