Dokumententyp:	Standard	Version:	1.0
Geltend für:	CONSUST GmbH	Gültig ab:	01.12.2025

STA.IT.003

Statement of Applicability (SoA) – ISO/IEC 27001:2022

Dokumenteninformationen

Erstellt von:	Arno Thenhausen / GF	Neue Version:	1.0
Erstellt am:	19.11.2025	Gültig ab:	01.12.2025
Freigegeben von:	Arno Thenhausen / GF	Ersetzt Version:	
Freigegeben am:	28.11.2025	Gültig ab:	
Verantwortlich:	CISO	Referenz:	ISO/IEC 27001:2022
Freigabenachweis:	A. Thenhausen	S. Kerkhoff-Mann	

Dokumententyp:	Standard	Version:	1.0
Geltend für:	CONSUST GmbH	Gültig ab:	01.12.2025

Inhaltsverzeichnis

1 Präambel 3
1.1 Zweck des Dokuments 3
1.2 Geltungsbereich 3
1.3 Rollen & Verantwortlichkeiten 3
1.4 Dokumentenhistorie 3
1.5 Ablageort und Verweise 3
2 Einleitung 3
3 Annex A Kontrollen 4

1 Präambel

1.1 Zweck des Dokuments

Dieses Dokument definiert die Anwendbarkeit der Sicherheitskontrollen aus Anhang A der Norm und die Begründung bei Nicht-Anwendbarkeit.

1.2 Geltungsbereich

Dieses Dokument ist verbindlich für das gesamte Unternehmen und alle Mitarbeitenden.

Das Dokument tritt mit dem Datum der Freigabe in Kraft und ist für unbegrenzte Zeit gültig.

1.3 Rollen & Verantwortlichkeiten

Dieses Dokument umfasst folgende Rollen und Verantwortlichkeiten:

Rolle	Verantwortlichkeit
Geschäftsleitung	Legt ISMS-Ziele fest, stellt Ressourcen bereit, entscheidet über Risiken und integriert ISMS in Geschäftsprozesse.
CISO / ISMS-Beauftragter	Steuert ISMS, koordiniert Audits und Zertifizierungen, überwacht Compliance und Sicherheitsvorfälle.

1.4 Dokumentenhistorie

Version	Datum	Editor	Beschreibung
1.0	19.11.2025	CISO	SoA in der Ursprungsform

1.5 Ablageort und Verweise

Name	Ort
OneDrive	\consust - General\09_Richtlinien\ISO 27001

2 Einleitung

Das Statement of Applicability (SoA) ist ein zentrales Dokument des Informationssicherheits-Managementsystems (ISMS) nach ISO/IEC 27001:2022. Es dient als verbindliche Übersicht aller relevanten Sicherheitskontrollen aus Anhang A der Norm und dokumentiert deren Anwendbarkeit, die Begründung für die Nicht-Anwendbarkeit sowie den Implementierungsstatus (siehe Anhang A).

Das SoA erfüllt folgende Zwecke:

- Nachweis der risikobasierten Auswahl von Sicherheitsmaßnahmen gemäß ISO 27001.
- Transparenz gegenüber internen und externen Stakeholdern (z. B. Auditoren, Kunden, Partner).
- Grundlage für die Umsetzung, Überwachung und kontinuierliche Verbesserung des ISMS.

Die Anwendbarkeit der einzelnen Kontrollen wird auf Basis des definierten ISMS-Scopes, der Ergebnisse der Risikobewertung, sowie gesetzlicher, regulatorischer und vertraglicher Anforderungen festgelegt.

Dieses Dokument wird regelmäßig überprüft und aktualisiert, insbesondere bei Änderungen des ISMS-Scopes, neuen Risiken oder geänderten Risikobewertungen sowie Anpassungen gesetzlicher oder regulatorischer Anforderungen.

3 Annex A Kontrollen