DGI® Deutsche Gesellschaft für Informationssicherheit AG

Vorgehen und Prüfpunkte für die Auditierung eines ISMS gemäß ISO 27001

- Richtlinie -

Inhaltsverzeichnis

1 Angaben zum Audit

Audit-Nummer	
Auditart	
Auditzeitraum	
Auditierter Bereich	

2 Festlegungen zum Audit

2.1 Auditkriterien

Die Auditkriterien ermöglichen eine strukturierte Bewertung der Auditfeststellungen.

Die Auditkriterien werden wie folgt angewendet

1. Status der dokumentierten Regelungen (Lenkung und Steuerung)
2. Vollständigkeit zu einem Referenzmodell
3. Konsistenz zu weiteren Regelungen
4. Akzeptanz der Zielgruppen
5. Wirksamkeit der Maßnahmen

2.3 Festlegung der Prüfkriterien

Die nachfolgende Tabelle zeigt die Prüfkriterien für die Bewertung der Dokumentation und der Maßnahmen auf.

Bewertung	Erläuterung
4	vollständig erfüllt
3	überwiegend erfüllt
2	teilweise erfüllt
1	nicht erfüllt
0	nicht gewürdigt

	Informationssicherheitsmaßnahmen nicht, teilweise zeigen Verbesserungspotentiale auf

3 Hinweise für den Umgang mit der Auditcheckliste

3.1 Allgemeines

Die nachfolgende Tabelle zeigt beispielhaft einen einzelnen Prüfpunkt mit seinem Prüf- und Bewertungsschema auf.

Kürzel und Bezeichnung der Anforderung							
Prüfpunkt	**Auditfeststellung**						
	Geprüft	Dokumentation		Maßnahmen		Bewertung	
		Nachweis	A	Nachweis	A	Abweichung	SFI

Prüfpunkte

In der Spalte „Prüfpunkt“ muss für jede Anforderung oder Prüfgegenstand ein oder mehrere Prüfpunkte für die Konkretisierung der Anforderung aufgeführt werden.

Geprüft

Es müssen alle Prüfpunkte bewertet werden.

In der Spalte „Geprüft“ muss die Auswahl [Ja] oder [Nein] getroffen werden.

Dokumentation

Hier muss angegeben werden, ob zu einem Prüfpunkt eine Dokumentation oder eine dokumentierte Regelung, wie eine Prozessbeschreibung, eine Verfahrensanweisung, ein Konzept, eine Richtlinie, ein Handbuch oder eine Arbeitsanweisung vorgelegt werden kann und ob die Anforderungen an den Prüfpunkt erfüllt werden.

In der Spalte „Nachweis" muss ein Nachweis für die Dokumentation angegeben und unter „Erläuterungen" näher beschrieben werden.

In der dazugehörigen Spalte „A" erfolgt die Bewertung durch den Auditor nach dem festgelegten Prüfschema.

Maßnahmen

In der Spalte "Abweichung" muss die Auswahl Erfüllt (E) / Hauptabweichung (H) / Nebenabweichung (N) getroffen werden.

In der Spalte "SFI" (Scope for Improvement) kann durch das Setzen eines [X] vermerkt werden, dass sich aus dem Prüfpunkt Verbesserungspotentiale für die Organisation ergeben.

Erläuterungen

Hier können ergänzende Angaben zu den Auditfeststellungen näher beschrieben werden.

4 Prüfpunkte

4.1 Allgemeines

Die nachfolgende Gliederung der Anforderungen basiert auf der High Level-Struktur der ISO 27001 sowie dem Anhang A der ISO 27001.

4.2 Prüfpunkte gemäß ISO 27001

Begriffe							
Inwieweit sind die relevanten Begriffe des ISMS organisationsspezifisch definiert und festgelegt?							
Gibt es einen Prozess zur Überwachung einer konsistenten Anwendung der relevanten Begriffe des ISMS?							
Erläuterungen							

Verstehen der Organisation und ihres Kontextes							
Prüfpunkt	**Auditfeststellungen**						
	Geprüft	Dokumentation		Maßnahme		Bewertung	
		Nachweis	A	Nachweis	A	Abweichung	SFI
Inwieweit sind die relevanten externen und internen Themen und Beweggründe zum ISMS organisationsspezifisch eruiert und analysiert?							
Gibt es einen Prozess zur Überwachung der externen und internen Themen zum ISMS?							
[illegible]							
[illegible] eines ISMS?							
Erläuterungen							