

**Vorgehen und Prüfpunkte
für die Auditierung
eines ISMS gemäß ISO 27001**

- Richtlinie -

Inhaltsverzeichnis

Prüfung und Freigabe	2
Änderungshistorie	3
Dokumentensteuerung und Verteilerkreis	4
1 Angaben zum Audit	7
2 Festlegungen zum Audit	8
2.1 Auditkriterien	8
2.2 Auditprüfpunkte	8
2.3 Festlegung der Prüfkriterien	9
2.4 Festlegung der Bewertungskriterien	9
3 Hinweise für den Umgang mit der Auditcheckliste	10
3.1 Allgemeines	10
3.2 Umgang mit den Auditfeststellungen	10
4 Prüfpunkte	12
4.1 Allgemeines	12
4.2 Prüfpunkte gemäß ISO 27001	12
Begriffe	12
Verstehen der Organisation und ihres Kontextes	13
Verstehen der Erfordernisse und Erwartungen interessierter Parteien	14
Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems	15
Informationssicherheitsmanagementsystem	16
Führung und Verpflichtung	17
Politik	18
Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	19
Maßnahmen zum Umgang mit Risiken und Chancen	20
Informationssicherheitsziele und Planung zu deren Erreichung	21
Ressourcen	22
Kompetenz	23
Bewusstsein (Awareness)	24
Kommunikation	25
Dokumentierte Information (Dokumentation)	26
Betriebliche Planung und Steuerung	27
Informationssicherheitsrisikobeurteilung	28
Informationssicherheitsrisikobehandlung	29
Überwachung, Messung, Analyse und Bewertung	30
Internes Audit	31
Managementbewertung	32
Nichtkonformität und Korrekturmaßnahmen	33
Fortlaufende Verbesserung	34

4.3 Prüfpunkte zum Anhang A gemäß ISO 27001	35
A.5 Informationssicherheitsrichtlinien	35
A.6 Organisation der Informationssicherheit	36
A.7 Personalsicherheit	37
A.8 Verwaltung der Werte	38
A.9 Zugangssteuerung	39
A.10 Kryptographie	41
A.11 Physische und umgebungsbezogene Sicherheit	42
A.12 Betriebssicherheit	44
A.13 Kommunikationssicherheit	46
A.14 Anschaffung, Entwicklung und Instandhalten von Systemen	47
A.15 Lieferantenbeziehungen	49
A.16 Handhabung von Informationssicherheitsvorfällen	50
A.17 Informationssicherheitsaspekte beim Business Continuity Management	51
A.18 Compliance	52

1 Angaben zum Audit

Audit-Nummer

Auditart

Auditzeitraum

Auditierter Bereich

DGI®

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

DGI[®]

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	wird geprüft

DGI®

Informationssicherheitsmanagement (ISM, ISO 27001) 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

DGI®

ist.

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

DGI®

In der Spalte „Abweichung“ muss die Auswirkung (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							
							
feststellungen							
Inwieweit sind die relevanten Begriffe des ISMS organisationspezifisch 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?							
Inwieweit werden die Geschäftsrisiken zum ISMS eruiert und analysiert?							
Inwieweit werden die Geschäftsrisiken zum ISMS eruiert und analysiert?							
Inwieweit werden die Geschäftsrisiken zum ISMS eruiert und analysiert?							
Inwieweit werden die Geschäftsrisiken zum ISMS eruiert und analysiert?							
Erläuterungen							

