Phase 2 – Rechtliche und organisatorische Anforderungen

> *„Ein ISMS muss die tatsächlichen Pflichten des Unternehmens kennen.“*

Einleitung

Phase 2 – Rechtliche und organisatorische Anforderungen ist ein Baustein auf dem Weg zu einem belastbaren ISMS für KMU. Die Phase verbindet organisatorische Sicht, technische Realität und die Anforderungen der Geschäftsführung.

Ziel der Phase

Ziel ist es, die relevanten Informationen strukturiert zu erfassen, verständlich zu dokumentieren und als Grundlage für die nächsten Schritte nutzbar zu machen.

Benötigte Teilnehmer

- Geschäftsführung oder IT-Entscheider
- Interner oder externer IT-Verantwortlicher
- Fachabteilungen nach Bedarf
- Datenschutz oder Qualitätsmanagement, falls vorhanden

Arbeitsergebnisse der Phase

- Dokumentierte Ergebnisse der Bestandsaufnahme
- Offene Fragen und Risiken
- Erste Prioritäten für spätere Maßnahmen
- Grundlage für die nächste Phase

Checkliste

Gesetzliche Anforderungen

Ziel

DSGVO, BDSG und ggf. branchenspezifische Vorgaben werden geprüft. Nicht jede Norm ist relevant, aber relevante Pflichten müssen dokumentiert werden.

Warum ist das wichtig?

Dieser Punkt sorgt dafür, dass Entscheidungen nicht auf Annahmen beruhen. Gerade in kleinen Unternehmen sind viele Informationen nicht dokumentiert, sondern nur einzelnen Personen bekannt. Durch die strukturierte Erfassung entsteht Transparenz und eine belastbare Grundlage für Risikoanalyse, Maßnahmenplanung und spätere Audits.

Vertragliche Anforderungen

Ziel

Kundenverträge, Lieferantenverträge, Geheimhaltungsvereinbarungen und Serviceverträge können Sicherheitsanforderungen enthalten. Diese Anforderungen werden oft erst bei Audits sichtbar.

Warum ist das wichtig?

Dieser Punkt sorgt dafür, dass Entscheidungen nicht auf Annahmen beruhen. Gerade in kleinen Unternehmen sind viele Informationen nicht dokumentiert, sondern nur einzelnen Personen bekannt. Durch die strukturierte Erfassung entsteht Transparenz und eine belastbare Grundlage für Risikoanalyse, Maßnahmenplanung und spätere Audits.

Kundenanforderungen

Ziel

Manche Kunden verlangen Sicherheitsnachweise, Fragebögen, Mindeststandards oder Zertifizierungen. Diese Anforderungen bestimmen häufig die Priorisierung.

Warum ist das wichtig?

Dieser Punkt sorgt dafür, dass Entscheidungen nicht auf Annahmen beruhen. Gerade in kleinen Unternehmen sind viele Informationen nicht dokumentiert, sondern nur einzelnen Personen bekannt. Durch die strukturierte Erfassung entsteht Transparenz und eine belastbare Grundlage für Risikoanalyse, Maßnahmenplanung und spätere Audits.

Cyberversicherung

Ziel

Versicherer verlangen oft MFA, Patchmanagement, Backups, EDR oder Notfallpläne. Der tatsächliche Versicherungsvertrag sollte geprüft werden.

Warum ist das wichtig?

Dieser Punkt sorgt dafür, dass Entscheidungen nicht auf Annahmen beruhen. Gerade in kleinen Unternehmen sind viele Informationen nicht dokumentiert, sondern nur einzelnen Personen bekannt. Durch die strukturierte Erfassung entsteht Transparenz und eine belastbare Grundlage für Risikoanalyse, Maßnahmenplanung und spätere Audits.

Auftragsverarbeitung

Ziel

AV-Verträge und Datenschutzrollen müssen geklärt werden. Besonders wichtig ist die Abgrenzung zwischen Verantwortlichem, Auftragsverarbeiter und Unterauftragnehmer.

Warum ist das wichtig?

Dieser Punkt sorgt dafür, dass Entscheidungen nicht auf Annahmen beruhen. Gerade in kleinen Unternehmen sind viele Informationen nicht dokumentiert, sondern nur einzelnen Personen bekannt. Durch die strukturierte Erfassung entsteht Transparenz und eine belastbare Grundlage für Risikoanalyse, Maßnahmenplanung und spätere Audits.

Datenschutzorganisation

Ziel

Datenschutzbeauftragter, Verzeichnis der Verarbeitungstätigkeiten, Löschkonzepte und Betroffenenrechte werden betrachtet. Datenschutz und Informationssicherheit überschneiden sich stark.

Warum ist das wichtig?

Dieser Punkt sorgt dafür, dass Entscheidungen nicht auf Annahmen beruhen. Gerade in kleinen Unternehmen sind viele Informationen nicht dokumentiert, sondern nur einzelnen Personen bekannt. Durch die strukturierte Erfassung entsteht Transparenz und eine belastbare Grundlage für Risikoanalyse, Maßnahmenplanung und spätere Audits.

Interne Richtlinien

Ziel

Vorhandene Regeln zu Passwörtern, Homeoffice, mobilen Geräten oder E-Mail werden gesammelt. Fehlen sie, entsteht daraus später ein Maßnahmenbedarf.

Warum ist das wichtig?

Dieser Punkt sorgt dafür, dass Entscheidungen nicht auf Annahmen beruhen. Gerade in kleinen Unternehmen sind viele Informationen nicht dokumentiert, sondern nur einzelnen Personen bekannt. Durch die strukturierte Erfassung entsteht Transparenz und eine belastbare Grundlage für Risikoanalyse, Maßnahmenplanung und spätere Audits.

Rollen und Verantwortlichkeiten

Ziel

Es wird geklärt, wer Informationssicherheit steuert, Entscheidungen trifft und Maßnahmen freigibt. Ohne klare Rollen bleibt das ISMS wirkungslos.

Warum ist das wichtig?

Dieser Punkt sorgt dafür, dass Entscheidungen nicht auf Annahmen beruhen. Gerade in kleinen Unternehmen sind viele Informationen nicht dokumentiert, sondern nur einzelnen Personen bekannt. Durch die strukturierte Erfassung entsteht Transparenz und eine belastbare Grundlage für Risikoanalyse, Maßnahmenplanung und spätere Audits.

Typische Feststellungen

In KMU fehlen häufig aktuelle Dokumentationen, eindeutige Verantwortlichkeiten und regelmäßige Prüfungen. Das ist kein Vorwurf, sondern der Ausgangspunkt für den Aufbau eines ISMS.

Hinweise für den IT-Berater

Wichtig ist eine pragmatische Sprache. Geschäftsführung und Fachbereiche müssen verstehen, welchen Nutzen die Phase für den Betrieb hat. Technische Details sind wichtig, sollten aber immer mit Geschäftsrisiken verbunden werden.

Praxistipp

Am Ende jeder Phase sollte eine kurze Zusammenfassung erstellt werden: Was wurde erkannt, was ist kritisch, was ist offen und welche Entscheidung wird als nächstes benötigt?

Ergebnis der Phase

Die Phase ist abgeschlossen, wenn die Ergebnisse so dokumentiert sind, dass eine andere fachkundige Person die Ausgangslage nachvollziehen und mit der nächsten Phase fortfahren kann.

Revision #5
Created 1 July 2026 08:10:44 by Stefan Kittel
Updated 1 July 2026 08:34:39 by Stefan Kittel