Erstelldatum	13.01.2023
Update	16.02.2025

Herausgeber	Teilnehmer der Bewertung zur Selbsteinschätzung	
	Name	Position
SMCT MANAGEMENT concept Stefan Strößenreuther Reuthweg 11 95100 Selb		

Inhaltsverzeichnis

1. Rahmen und Methodik		
1.1 Definition des Scopes	Umgesetzt	Zufrieden
Klarer **Geltungsbereich** (Scope) des ISMS: Welche Standorte, Assets, Abteilungen sind betroffen?	☐	☐
Begründung etwaiger **Ausschlüsse** oder spezieller Bereiche dokumentieren	☐	☐
1.2 Risikomanagement Methodik festlegen	Umgesetzt	Zufrieden
Vorgehensweise (z. B. ISO/IEC 27005, NIST SP 800-30, eigene Matrix) für **Risikoidentifikation, -bewertung** und -behandlung definieren	☐	☐
Kriterien zur Einschätzung von **Auswirkung** (Impact) und **Wahrscheinlichkeit** (Likelihood) festlegen.	☐	☐
1.3 Rollen und Verantwortlichkeiten	**Umgesetzt**	**Zufrieden**
Benennen eines **verantwortlichen Teams** oder Risikomanagers	☐	☐
Klarheit schaffen, wer Entscheidungen über Risikoakzeptanz, -minderung oder -übertragung trifft.	☐	☐

2. Risikoidentifikation		
2.1 Asset Register erstellen	Umgesetzt	Zufrieden
Alle **wichtigen Informationswerte** (Assets) erfassen (Hardware, Software, Datenbanken, kritische Dokumente).	☐	☐
Asset Register erstellen.	☐	☐
Bedrohungen und **Schwachstellen** auflisten	☐	☐
Für jedes Asset / Prozess definieren, wie relevant Vertraulichkeit, Integrität und Verfügbarkeit sind (z. B. hoch, mittel, gering).	☐	☐
Dokumentieren, welche konkreten Konsequenzen (z. B. Datenleck, Manipulation, Systemausfall) sich bei Verletzung eines Schutzziels ergeben können.	☐	☐
Eigentümer (Data Owner) und Standort für jedes Asset festhalten.	☐	☐
2.2 Bedrohungen und Schwachstellen auflisten	**Umgesetzt**	**Zufrieden**
Typische **Bedrohungen** (z. B. Malware, physischen Diebstahl, Social Engineering) für jedes Asset kategorisieren.	☐	☐
Schwachstellen (z. B. ungesicherte Zugänge, fehlende Patches, mangelnde Awareness) dokumentieren	☐	☐
2.3 Berücksichtigung des Klimawandels (seit Nov. 2024)	**Umgesetzt**	**Zufrieden**
Mögliche **Klimarisiken** (z. B. Extremwetterereignisse, Stromausfälle, Lieferkettenstörungen) berücksichtigen, da sie IT-Assets und Infrastruktur beeinflussen können.	☐	☐
Dokumentieren, wie sich klimabezogene Faktoren auf Verfügbarkeit und Integrität von Informationen auswirken	☐	☐

3. Risikobewertung		
3.1 Einschätzung von Eintrittswahrscheinlichkeit und Auswirkung	Umgesetzt	Zufrieden
Festgelegtes Scoring-System verwenden (z. B. Skala 1–5) für **Likelihood** und **Impact**.	☐	☐
Risikowert berechnen (z. B. Eintrittswahrscheinlichkeit × Auswirkung) und Prioritäten ableiten.	☐	☐
Prüfen, **welches Schutzziel** (Vertraulichkeit, Integrität, Verfügbarkeit) durch ein Szenario am stärksten gefährdet ist.	☐	☐
Für die **Auswirkungsanalyse** klar festhalten: Vertraulichkeit verletzt => Datenleck, Integrität verletzt => Datenmanipulation, Verfügbarkeit verletzt => System-/Prozessausfall.	☐	☐
3.2 Risikobewertungsbericht	**Umgesetzt**	**Zufrieden**
Ergebnisse der Bewertung (Übersichtstabelle, Heatmap) zusammenfassen.	☐	☐
Kritische Risiken identifizieren, die umgehend behandelt werden müssen.	☐	☐
3.3 Managementfreigabe	**Umgesetzt**	**Zufrieden**
Bericht dem Top-Management vorlegen, um **Freigaben** (z. B. Budget) und **Risikoeinstufung** zu bestätigen.	☐	☐
Protokollierung von Annahmen und Entscheidungsgrundlagen (z. B. warum bestimmte Risiken höher priorisiert werden).	☐	☐

4. Risikobehandlung		
4.1 Strategien festlegen	Umgesetzt	Zufrieden
Für jedes identifizierte Risiko eine Behandlungsoption definieren: • **Akzeptieren** (z. B. geringes Risiko, akzeptable Kostennutzen-Relation) • **Minderung** (z. B. Maßnahmen zur Reduzierung von Wahrscheinlichkeit/Auswirkung) • **Vermeiden** (z. B. Einstellen einer risikoreichen Aktivität) • **Übertragen** (z. B. Versicherungen, Outsourcing	☐	☐
4.2 Maßnahmenplan (Risikobehandlungsplan)	**Umgesetzt**	**Zufrieden**
Konkrete Maßnahmen (z. B. technische Kontrollen, Schulungen, Prozessänderungen) mit Verantwortlichen, Ressourcen und Zeitrahmen definieren.	☐	☐
Priorisierung (z. B. kurzfristige, mittelfristige) und Kosten-Nutzen-Betrachtung dokumentieren.	☐	☐
4.3 Statement of Applicability (SoA)	**Umgesetzt**	**Zufrieden**
In Bezug auf ISO 27001 Anhang A festhalten, welche **Controls** angewendet werden und warum.	☐	☐
Nicht angewendete Controls kurz begründen (z. B. Ausnahmen, Risikoakzeptanz, irrelevante Szenarien).	☐	☐

5. Implementierung und Dokumentation

5.1 Umsetzung der definierten Maßnahmen	Umgesetzt	Zufrieden
Risikoanalyse, Risikobewertungsbericht, Risikobehandlungsplan und SoA im **ISMS-Dokumentationssystem** sicher ablegen.	☐	☐
Versionierung und Freigabestand eindeutig kennzeichnen.	☐	☐
5.2 Schulung und Awareness	**Umgesetzt**	**Zufrieden**
Mitarbeitende über neue Sicherheitsmaßnahmen oder Prozesse informieren (z. B. Sicherheitsschulungen, E-Learning).	☐	☐
Anwenderfeedback einholen (z. B. Umfragen, Team-Meetings), um Umsetzungsprobleme früh zu erkennen.	☐	☐

6. Kontrolle und Überwachung		
6.1 Monitoring der Maßnahmen	Umgesetzt	Zufrieden
Regelmäßig prüfen, ob implementierte **Kontrollen** (z. B. Firewalls, Zugriffsrechte, Backup-Routinen) in der Praxis funktionieren.	☐	☐
Incidents, Audit-Feststellungen oder Log-Analysen als **Echtzeitindikatoren** für Wirksamkeit nutzen.	☐	☐
6.2 Interner Audits und Managementbewertung	**Umgesetzt**	**Zufrieden**
Risikoanalyse und -behandlung in interne Audits einbeziehen; Auditergebnisse dokumentieren.	☐	☐
Im **Management-Review** (z. B. jährlich) Hinterfragen, ob alle wichtigen Risiken angemessen adressiert wurden und ob Anpassungen nötig sind.	☐	☐

7. Abschluss und RE-Evaluierung		
7.1 Aktualisierung der Risikoanalyse	Umgesetzt	Zufrieden
Nach **wesentlichen Änderungen** (z. B. neue IT-Systeme, Standortverlagerungen, Personalwechsel) die Risikoanalyse anpassen.	☐	☐
Periodische **Neubewertung** (z. B. jährlich oder halbjährlich) durchführen, um neue Bedrohungen oder Schwachstellen zu berücksichtigen.	☒	☐
7.2 Verbesserung des Risikomanagement Prozess	**Umgesetzt**	**Zufrieden**
Lessons Learned aus Audits, Incidents und Tests in die Methodik einfließen lassen (z. B. verfeinerte Bewertungsskala, bessere Dokumentation).	☐	☐
Schulungen oder Tools für Risikoanalyse und -behandlung ggf. modernisieren.	☐	☐
7.3 Management Freigabe	**Umgesetzt**	**Zufrieden**
Risikoanalyse, -bewertung, -behandlung und abschließende Maßnahmen dem Top-Management vorstellen, Beschlüsse protokollieren.	☐	☐
Sicherstellen, dass **Budgets, Ressourcen** und Prioritäten für neue oder geänderte Maßnahmen freigegeben sind.	☐	☐

SMCT MANAGEMENT begleitet Unternehmen dabei, ein effektives Risikomanagement zu etablieren oder auszubauen – von der ersten Bestandsaufnahme bis hin zur strategischen Verankerung im Unternehmensalltag. Wir unterstützen Sie bei der Auswahl einer geeigneten Methodik zur Risikoanalyse, übernehmen die strukturierte Erfassung und Bewertung Ihrer Assets und Bedrohungen und erarbeiten gemeinsam einen Risikobehandlungsplan.

Dabei berücksichtigen wir nicht nur Ihre individuellen Geschäftsziele und Compliance-Anforderungen, sondern auch aktuelle Einflüsse wie den Klimawandel, neue Technologien oder Marktentwicklungen. Durch maßgeschneiderte Schulungs- und Awareness-Programme sorgen wir zudem für ein unternehmensweites Risikobewusstsein.

So entstehen nicht nur formale Nachweise für Audits und Zertifizierungen, sondern auch ein lebendiges Risikomanagement, das aktiv zur Sicherheit, Resilienz und Wettbewerbsfähigkeit Ihres Unternehmens beiträgt.

Hinweis: Die drei **Schutzziele C,I,A** bilden das **Rückgrat** des Informationssicherheitsmanagements. Durchgängig im Risikomanagementprozess verankert, gewährleisten sie, dass alle wesentlichen Aspekte von Informationssicherheit adressiert werden, um ein wirksames und normkonformes ISMS zu etablieren.