Checkliste für ein Notfallmanagement

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. Governance und organisatorische Verankerung		
1.1 Top-Management Unterstützung	Umgesetzt	Zufrieden
Das Top-Management erkennt Notfallmanagement als **strategisch wichtig** an und stellt ausreichend Ressourcen (Budget, Personal) bereit.	☐	☐
Es existiert eine **offizielle Richtlinie** (Policy) für Notfallmanagement, die in das ISMS (ISO 27001) bzw. BCM (ISO 22301) integriert ist.	☐	☐
1.2 Scope und Verantwortlichkeiten	Umgesetzt	Zufrieden
Klare **Zuständigkeiten** (z. B. Notfallmanager, Incident Response Team, Krisenstab) sind benannt.	☐	☐
Der **Umfang** des Notfallmanagements (betroffene Standorte, Geschäftsprozesse, IT-Systeme) ist definiert und dokumentiert.	☐	☐
1.3 Verknüpfung mit Risikomanagement	**Umgesetzt**	**Zufrieden**
Ergebnisse aus der **Risikobewertung** (z. B. aus ISO 27001, branchenspezifischen Risikoanalysen) fließen in die Szenario-Planung des Notfallmanagements ein.	☐	☐
Mögliche **Klimarisiken** (z. B. Extremwetter, Lieferkettenstörung) sind berücksichtigt, seit ab November 2024 in Kraft (Synergie mit ISO 27001-Kap. 4).	☐	☐

2. Business Impact Analysis (BIA)		
2.1 Prozess- und Systemkritikalität	Umgesetzt	Zufrieden
Ermittlung **geschäftskritischer** Prozesse (z. B. Produktion, Logistik, Kundenservice) und zugrunde liegender IT-Systeme.	☐	☐
Bewertung möglicher Auswirkungen (z. B. wirtschaftlich, reputationsbezogen) bei Ausfall oder Störung.	☐	☐
2.2 RTO und RPO	**Umgesetzt**	**Zufrieden**
Definition von **RTO** (Recovery Time Objective) und **RPO** (Recovery Point Objective) für die wichtigsten Prozesse/IT-Systeme.	☐	☐
Dokumentation, welche Maximalen Ausfallzeiten tolerierbar sind und welche Datenstände wiederhergestellt werden müssen.	☐	☐
2.3 Abhängigkeiten und Prioritäten	**Umgesetzt**	**Zufrieden**
Identifikation wichtiger **Schnittstellen** (z. B. Lieferanten, externe Dienstleister, Partner) und **Abhängigkeiten** (z. B. spezifische Maschinen, Software).	☐	☐
Reihung nach Kritikalität, um Notfall- und Wiederanlaufpläne fokussiert zu erstellen.	☐	☐

3. Notfallstrategie und Plankonzepte		
3.1 Notfallstrategien	Umgesetzt	Zufrieden
Festlegen, wie im Ernstfall verfahren wird: **Vermeidung**, **Redundanzen** (z. B. Backup-Rechenzentrum, Ausweichstandort), **schnelle Wiederanlaufprozesse**.	☐	☐
Dokumentation der gewählten Strategien (z. B. Warm-Site, Cloud-Fallback) und Freigabe durch die Geschäftsleitung.	☐	☐

3.2 Geschäftsfortführungsplan (BCP)	Umgesetzt	Zufrieden
Ausführliche Beschreibung, wie **kritische Prozesse** im Notfall aufrechterhalten oder schnell wiederhergestellt werden.	☐	☐
Verantwortlichkeiten (Process Owner, Krisenstab), alternative Verfahren (z. B. manuelle Prozesse) und Prioritäten festhalten.	☐	☐
3.3 IT-Notfallplan	**Umgesetzt**	**Zufrieden**
Technische Verfahren zur **Wiederherstellung** von Daten und Systemen (z. B. Backup-Strategie, DR-Tests) definieren	☐	☐
Detaillierte **Wiederanlaufpläne** mit RTO/RPO, Eskalationsstufen und Kontaktpersonen.	☐	☐
3.4 Szenariobetrachtungen	**Umgesetzt**	**Zufrieden**
Extremwetter, Stromausfall, Cyberangriff, Ausfall wichtiger Lieferanten, Pandemien als potenzielle Szenarien durchspielen.	☐	☐
Rollen verteilen (z. B. Krisenstab, Kommunikationsteam) und vorbereitete Checklisten für Sofortmaßnahmen anlegen.	☐	☐

4. Dokumentation und Kommunikationsmanagement		
4.1 Pläne und Checklisten	Umgesetzt	Zufrieden
Alle Notfallpläne (BCP, IT-Notfallplan, Kommunikationsplan) in einem zentralen Dokumentationssystem gesichert.	☐	☐
Verwendung von kurzen **Checklisten** für die Erstmaßnahmen, damit die Handlungsleitfäden in Stresssituationen leicht anwendbar sind	☐	☐
4.2 Notfallkommunikation	**Umgesetzt**	**Zufrieden**
Definierte **Kommunikationswege** (z. B. E-Mail-Alternative, Krisenchat, Telefonketten) und Verteilerlisten (Mitarbeitende, Kunden, Medien).	☐	☐
Vorlagen für offizielle Pressemitteilungen, Kundeninformationen oder interne Memos bereitstellen.	☐	☐
4.3 Externe Kontakte und Lieferanten	**Umgesetzt**	**Zufrieden**
Geklärte **Ansprechpartner** (z. B. Cloud-Provider, Lieferanten, Notfall-Dienstleister)	☐	☐
Verträge/SLA, die sicherstellen, dass Notfallunterstützung (z. B. Ersatzteile, Ersatzsysteme) zeitnah verfügbar ist.	☐	☐

5. Testing und Übungen		
5.1 Übungstypen	Umgesetzt	Zufrieden
Verschiedene Szenarien proben: **Schreibtischübungen** (Walkthrough), **technische Wiederherstellungstests** (Disaster Recovery), **Krisenstabsübungen** (Planspiel)	☐	☐
Zeitlicher Rahmen definieren (z. B. jährliche Tests, ggf. zweimal jährlich für kritische Bereiche).	☐	☐
5.2 Protokollierung	**Umgesetzt**	**Zufrieden**

Dokumentation des **Ablaufs**, der Ergebnisse, Feststellungen und Verbesserungsvorschläge nach jeder Übung.	☐	☐
Erstellung eines **Maßnahmenplans**, um gefundene Schwachstellen zu schließen.	☐	☐
5.3 Management Reporting	**Umgesetzt**	**Zufrieden**
Berichtslegung gegenüber Geschäftsleitung: **Zielerreichung**, entstandene Probleme, geplante Verbesserungen.	☐	☐
Regelmäßige Überprüfung und **Aktualisierung** des **Notfallkonzepts** auf Basis der Übungsergebnisse.	☐	☐

6. Rollen und Verantwortlichkeiten		
6.1 Krisenteam / Reaktionsteam	Umgesetzt	Zufrieden
Benennung eines **Stabs** (z. B. IT, HR, Recht, PR, Logistik) mit klaren Rollen (Leiter, Protokollant, Kommunikationsverantwortlicher).	☐	☐
Schaffung eines **Eskalationsstufenmodells** (z. B. Incident, Major Incident, Krisenfall).	☐	☐
6.2 Mitarbeitende	**Umgesetzt**	**Zufrieden**
Grundlagenwissen zu Notfall- und Evakuierungsszenarien, Alarmierungsketten.	☐	☐
Regelmäßige Schulungen/Awareness zu Prozessabläufen im Notfall (z. B. was tun bei Stromausfall, Hackerangriff).	☐	☐
6.3 Management Freigabe	**Umgesetzt**	**Zufrieden**
Dokument, in dem das Management alle Verantwortlichkeiten und Rollen (z. B. Notfallmanager) offiziell bestätigt.	☐	☐

7. Schnittstellen zu anderen Managementsystemen		
7.1 Verknüpfung mit ISO 27001	Umgesetzt	Zufrieden
Risiken aus der **ISMS-Risikoanalyse** (z. B. Data Center-Ausfall, Ransomware) in die Notfallplanung aufnehmen.	☐	☐
Sicherstellung, dass **Vertraulichkeit, Integrität, Verfügbarkeit** der Informationen auch im Notfall gewahrt bleibt.	☐	☐
7.2 Verknüpfung mit ISO 22301	**Umgesetzt**	**Zufrieden**
Überschneidungen im **Business Continuity Management** (BCM) beachten: BIA (Business Impact Analysis), Recovery-Ziele (RTO, RPO).	☐	☐
Abgleich von BCP (Business Continuity Plan) mit IT-spezifischem Notfallplan.	☐	☐
7.3 Synergie Effekte	**Umgesetzt**	**Zufrieden**
Gemeinsame **Übungen** (z. B. Krisensimulation für IT- und allgemeine Geschäftsprozesse).	☐	☐
Einheitliche Kommunikations- und Eskalationswege in beiden Systemen, um Doppelarbeit zu vermeiden.	☐	☐

8. Dokumentation und Lenkung		
8.1 Zentrale Ablage	Umgesetzt	Zufrieden
Notfallhandbuch, Evakuierungspläne, Kontaktlisten und Checklisten an einem **gesicherten Ort** (ggf. offline) verfügbar halten	☐	☐
Versionshistorie, Änderungsnachweise (Wer hat wann was freigegeben?).	☐	☐
8.2 Datenschutz und Sicherheit	**Umgesetzt**	**Zufrieden**
Sicherstellen, dass Notfallunterlagen (z. B. wichtige Passwörter, Kundendaten) **vertraulich** und korrekt aufbewahrt werden	☐	☐
Falls **Cloud-Lösungen** genutzt werden, prüfen, ob diese offline oder mobil verfügbar sind (ggf. verschlüsselte Datenträger)	☐	☐
8.3 Regelmäßige Aktualisierung	**Umgesetzt**	**Zufrieden**
Nach jeder Übung, jedem Audit und jeder größeren organisatorischen Veränderung die Dokumentation auf den aktuellen Stand bringen.	☐	☐
Verantwortliche festlegen, die die Aktualität der Notfallpläne prüfen (z. B. jährlich).	☐	☐

9. Kontinuierliche Verbesserung		
9.1 Lessons Learned	Umgesetzt	Zufrieden
Nach realen Vorfällen oder Übungen ein Dokument erstellen: Was lief gut, was war problematisch?	☐	☐
Daraus **Maßnahmen** ableiten, die bei Bedarf in den Notfallplänen und Checklisten eingearbeitet werden.	☐	☐
9.2 Interne Audits	**Umgesetzt**	**Zufrieden**
Notfallmanagement in den Plan für **ISMS-Audits** (ISO 27001) oder **BCM-Audits** (ISO 22301) integrieren.	☐	☐
Auditfeststellungen priorisieren und Korrekturmaßnahmen dokumentieren.	☐	☐
9.3 Managementbewertung	**Umgesetzt**	**Zufrieden**
Management bewerten lassen, ob die Notfallziele (z. B. maximaler Ausfall, RTO, RPO) noch angemessen sind.	☐	☐
Bei Bedarf Entscheidungen zu neuen Investitionen, verbesserten Redundanzen oder Ressourcen treffen.	☐	☐

SMCT MANAGEMENT begleitet Unternehmen dabei, ein fundiertes **Notfallmanagement** zu etablieren oder auszubauen, das sowohl den Anforderungen aus **ISO/IEC 27001** (IT-Sicherheit) als auch **ISO 22301** (Business Continuity) entspricht. Wir identifizieren gemeinsam mit Ihnen die geschäftskritischen Prozesse und IT-Ressourcen, führen eine umfassende Business Impact Analysis durch und entwickeln darauf aufbauend einen Notfall- und Wiederanlaufplan. Dabei berücksichtigen

wir branchenspezifische Risiken ebenso wie neue Herausforderungen, etwa infolge des Klimawandels oder technologischer Umbrüche.

Unser Team unterstützt Sie nicht nur bei der **Dokumentation** und **Zuweisung von Rollen** (z. B. Krisenstab, Incident-Response-Team), sondern gestaltet mit Ihnen gemeinsam **Übungsszenarien**, um das Zusammenspiel im Ernstfall zu testen und potenzielle Schwachstellen frühzeitig aufzudecken. Ergänzend beraten wir zu **Kommunikationsstrategien**und sorgen dafür, dass Mitarbeitende und Führungskräfte in Krisensituationen richtig handeln.

Somit entsteht ein lebendiges Notfallmanagement, das Ihr Unternehmen resilient macht, den Geschäftsbetrieb vor Unterbrechungen schützt und zugleich die Nachweisanforderungen für Zertifizierungen nach ISO 27001 oder 22301 erfüllt.