	Datum:	Seite
Checkliste zur Selbsteinschätzung ISO/IEC 27001	14.02.2025	1 von 13

Erstelldatum	**13.01.2023**
Update	**14.02.2025**

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

Inhaltsverzeichnis

1. Kontext der Organisation		
1.1 Identifizierung relevanter Faktoren	Umgesetzt	Zufrieden
Haben Sie alle internen und externen Aspekte ermittelt, die für den Zweck Ihres Unternehmens und die Erreichung der ISMS-Ziele entscheidend sind (z. B. Marktanforderungen, technologische Entwicklungen)?	☐	☐
Überwachen und aktualisieren Sie diese Faktoren regelmäßig, um Veränderungen frühzeitig zu erkennen und angemessen zu reagieren?	☐	☐
1.2 Erwartungen relevanter Parteien	**Umgesetzt**	**Zufrieden**
Wurden die Interessen und Anforderungen sämtlicher Stakeholder (Kunden, Lieferanten, Behörden etc.) erfasst, die Einfluss auf das ISMS nehmen könnten?	☐	☐
Überprüfen Sie diese Bedürfnisse in angemessenen Intervallen, um sicherzustellen, dass Ihr ISMS auf aktuelle Rahmenbedingungen ausgerichtet ist?	☐	☐
1.3 Geltungsbereich des ISMS	**Umgesetzt**	**Zufrieden**
Haben Sie den Scope Ihres ISMS schriftlich festgelegt, einschließlich externer und interner Aspekte sowie ausgegliederter Prozesse?	☐	☐
Berücksichtigen Sie dabei sowohl Geschäftsaktivitäten innerhalb des Unternehmens als auch Leistungen, die durch Dritte erbracht werden?	☐	☐
1.4 Risiken und Chancen	**Umgesetzt**	**Zufrieden**
Sind alle mit Ihren internen und externen Faktoren verbundenen Risiken und Chancen identifiziert und dokumentiert?	☐	☐
Nutzen Sie diesen Überblick für kontinuierliche Verbesserungsmaßnahmen und eine vorausschauende Steuerung Ihres ISMS?	☐	☐

2. Führung (Leadership)		
2.1 Verantwortung des Topmanagements	Umgesetzt	Zufrieden
Hat die oberste Leitung die Verantwortung für die Wirksamkeit des ISMS übernommen und diese Bedeutung im gesamten Unternehmen kommuniziert?	☐	☐
Engagieren sich Führungskräfte aktiv und stellen die notwendigen Ressourcen bereit?	☐	☐
2.2 Leitlinien und Ziele	**Umgesetzt**	**Zufrieden**
Existieren klare Sicherheitsleitlinien (Policy) und messbare Ziele für das ISMS, die sich an der strategischen Ausrichtung des Unternehmens orientieren?	☐	☐
Werden diese Ziele regelmäßig auf ihre Aktualität geprüft und unternehmensweit kommuniziert?	☐	☐
2.3 Rollen und Zuständigkeiten	**Umgesetzt**	**Zufrieden**
Sind die Verantwortlichkeiten und Befugnisse für alle relevanten ISMS-Rollen eindeutig definiert, dokumentiert und an die betreffenden Personen weitergegeben?	☐	☐
Verfügen die Rollenträger über ausreichende Kompetenzen, um die Einhaltung und Weiterentwicklung des ISMS sicherzustellen?	☐	☐
2.4 Programm und Zielerreichung	**Umgesetzt**	**Zufrieden**
Besteht ein strukturiertes Vorgehen, um die angestrebten Ergebnisse zu erreichen, die Anforderungen zu erfüllen und das ISMS fortlaufend zu verbessern?	☐	☐

Werden Fortschritte und Meilensteine regelmäßig bewertet und an das Management berichtet?	☐	☐

3. Planung		
3.1 Umgang mit Risiken und Chancen	Umgesetzt	Zufrieden
Haben Sie ein Verfahren etabliert, um Risiken und Chancen in Bezug auf Informationssicherheit gezielt zu identifizieren und zu bewerten?	☐	☐
Stellt dieser Prozess sicher, dass die Wirksamkeit des ISMS nachhaltig gewährleistet ist?	☐	☐
3.2 Risikobewertungsprozess	**Umgesetzt**	**Zufrieden**
Gibt es einen wiederholbaren, konsistenten Bewertungsprozess, der realistische Eintrittswahrscheinlichkeiten und potenzielle Auswirkungen für jede Bedrohung ermittelt?	☐	☐
Werden Risikokriterien verwendet, um Sicherheitsrisiken zu priorisieren und geeignete Maßnahmen abzuleiten?	☐	☐
3.3 Risikobehandlung	**Umgesetzt**	**Zufrieden**
Haben Sie konkrete Optionen zur Risikobehandlung definiert und mit den Anforderungen Ihres Unternehmens abgestimmt?	☒	☐
Wurde die Auswahl dieser Maßnahmen in einer Erklärung zur Anwendbarkeit (Statement of Applicability) dokumentiert und mit den kontrollen aus Anhang A der **ISO/IEC 27001:2022** abgeglichen?	☐	☐
3.4 Risikobehandlungsplan und Akzeptanz	**Umgesetzt**	**Zufrieden**
Liegt ein Risikobehandlungsplan vor, in dem Verantwortlichkeiten, Termine und Vorgehensweisen konkretisiert sind?	☐	☐
Sind Restrisiken von den jeweiligen Risikoeigentümern genehmigt und der Prozess entsprechend dokumentiert?	☐	☐
3.5 Ziele des ISMS	**Umgesetzt**	**Zufrieden**
Sind messbare Haupt- und Nebenziele definiert, veröffentlicht und im gesamten Unternehmen bekannt?	☐	☐
Legen Sie in diesem Zusammenhang fest, wer für welche Maßnahmen zuständig ist und welche Zeitrahmen gelten?	☐	☐

4. Unterstützung (Support)		
4.1 Ressourcen	Umgesetzt	Zufrieden
Stellt Ihr Unternehmen alle notwendigen Mittel (Personal, Infrastruktur, Arbeitsumgebung) bereit, um das ISMS erfolgreich einzuführen, zu betreiben und weiterzuentwickeln?	☐	☐
4.2 Kompetenzen und Schulungen	**Umgesetzt**	**Zufrieden**
Gibt es festgelegte Anforderungen an das Know-how der Mitarbeitenden, die für das ISMS wesentliche Aufgaben übernehmen?	☐	☐
Werden Kompetenzen regelmäßig überprüft und durch Schulungen oder Weiterbildungen ausgebaut, damit alle Beteiligten angemessen qualifiziert sind?	☐	☐
4.3 Wissen im Unternehmen	**Umgesetzt**	**Zufrieden**

Wurden alle relevanten Informationen und Prozessdokumentationen identifiziert, die im Rahmen des ISMS benötigt werden?	☐	☐
Werden diese Informationen für die richtigen Personen in passender Form bereitgestellt und gepflegt?	☐	☐
4.4 Dokumentierte Informationen	**Umgesetzt**	**Zufrieden**
Existiert ein Prozess, um Dokumente und Aufzeichnungen des ISMS zu erstellen, zu aktualisieren und vor unbefugtem Zugriff zu schützen?	☐	☐
Werden externe Dokumente, die für Ihr ISMS erforderlich sind, ebenso gelenkt und regelmäßig geprüft?	☐	☐

5. Betrieb (Operation)		
5.1 Betriebliche Steuerung	Umgesetzt	Zufrieden
Belegen dokumentierte Nachweise, dass ISMS-relevante Prozesse so durchgeführt werden, wie sie geplant sind?	☐	☐
Verfügen Sie über einen klaren Prozess, um Änderungen im ISMS strukturiert anzugehen und mögliche negative Folgen zu minimieren?	☐	☐
5.2 Auslagerungen	**Umgesetzt**	**Zufrieden**
Werden sämtliche ausgelagerten Prozesse regelmäßig überprüft und gesteuert, um sicherzustellen, dass externe Dienstleister mit Ihren Sicherheitsanforderungen konform gehen?	☐	☐
5.3 Laufende Risikobewertung	**Umgesetzt**	**Zufrieden**
Finden Risikoüberprüfungen in festgelegten Intervallen oder anlassbezogen statt (z. B. bei signifikanten Veränderungen in der Systemlandschaft)?	☐	☐
Werden die Ergebnisse dokumentiert und direkt in den ISMS-Prozess zurückgespielt?	☐	☐

6. Bewertung der Leistung (Performance Evaluation)		
6.1 Überwachung und Messung	Umgesetzt	Zufrieden
Haben Sie festgelegt, welche Aspekte der Informationssicherheit gemessen oder überwacht werden müssen, wann dies geschieht und mit welchen Methoden?	☐	☐
Werden die Ergebnisse ausgewertet, dokumentiert und für strategische Entscheidungen genutzt?	☐	☐
6.2 Interner Audits	**Umgesetzt**	**Zufrieden**
Führen Sie in regelmäßigen Abständen interne Audits durch, um die Wirksamkeit des ISMS zu überprüfen und potenzielle Schwachstellen aufzudecken?	☐	☐
Liegt ein Auditprogramm vor, das Verantwortlichkeiten, Zeitpläne und Kriterien für Audits definiert?	☐	☐
Werden die Auditergebnisse dem Management berichtet und angemessen archiviert?	☐	☐
6.3 Managementbewertung	**Umgesetzt**	**Zufrieden**
Bewertet das Topmanagement in geplanten Intervallen den Reifegrad des ISMS?	☐	☐

Werden dabei Chancen, Risiken und Verbesserungsmaßnahmen identifiziert und dokumentiert?	☐	☐
Erfolgt eine wirksame Kommunikation der Ergebnisse an alle relevanten Stellen?	☐	☐

7. Verbesserung (Improvement)		
7.1 Umgang mit Abweichungen	Umgesetzt	Zufrieden
Verfügen Sie über Verfahren zur Behandlung von Nonkonformitäten und zur Einleitung von Korrekturmaßnahmen?	☐	☐
Wird im Rahmen dieser Maßnahmen sichergestellt, dass die Ursachen analysiert und beseitigt werden, um ein erneutes Auftreten zu verhindern?	☐	☐
7.2 Kontinuierliche Optimierung	**Umgesetzt**	**Zufrieden**
Überprüfen Sie regelmäßig, ob durchgeführte Korrektur- und Vorbeugemaßnahmen zu einer nachhaltigen Verbesserung des ISMS geführt haben?	☐	☐
Werden die Ergebnisse dokumentiert und intern kommuniziert, um eine Lernkultur zu fördern?	☐	☐
7.3 Veränderungsmanagement	**Umgesetzt**	**Zufrieden**
Ist ein klarer Prozess definiert, um mögliche Änderungsbedarfe im ISMS zu erkennen, deren Auswirkungen einzuschätzen und die notwendigen Anpassungen durchzuführen?	☐	☐
Werden alle Schritte dokumentiert, kontrolliert und schlussendlich bewertet?	☐	☐

8. Neue Kontrollen und Schwerpunkte (ISO/IEC 27001:2022 / ISO/IEC 27002:2022)		
8.1 Threat Intelligence (Bedrohungsaufklärung)	Umgesetzt	Zufrieden
Verfügt Ihr Unternehmen über Prozesse, um laufend Informationen zu aktuellen Bedrohungen (z. B. Zero-Day-Exploits) zu sammeln und zu bewerten?	☐	☐
Werden diese Erkenntnisse systematisch in die Risikoanalyse und Risikobehandlung eingebunden?	☐	☐
8.2 Cloud Services	**Umgesetzt**	**Zufrieden**
Haben Sie Richtlinien und Prozesse definiert, um die Nutzung von Cloud-Diensten (Public, Private, Hybrid) zu steuern und abzusichern?	☐	☐
Überprüfen Sie regelmäßg die Cloud-Anbieter und deren Sicherheitsmaßnahmen (z. B. Zertifizierungen, SLA, Datenschutz)?	☐	☐
8.3 ICT-Bereitschaft für Business Continuity	**Umgesetzt**	**Zufrieden**
Gibt es ein aktuelles Notfallkonzept bzw. Disaster-Recovery-Pläne, die sicherstellen, dass Ihre Geschäftsprozesse im Falle von IT-Ausfällen fortgeführt werden können?	☐	☐
Werden Notfall- und Wiederanlaufprozesse regelmäßig getestet und auf ihre Wirksamkeit überprüft?	☐	☐
8.4 Physische Sicherheitsüberwachung	**Umgesetzt**	**Zufrieden**
Sind Zugangs- und Überwachungskonzepte für kritische Bereiche (Rechenzentrum, Serverräume etc.) vorhanden und aktuell?	☐	☐

Nutzen Sie Technologien (z. B. Videoüberwachung, Zutrittskontrollsysteme), um die physische Sicherheit zu gewährleisten, und wie überwachen Sie deren Wirksamkeit?	☐	☐

9. Organisation und personelle Aspekte		
9.1 Personelle Sicherheit	Umgesetzt	Zufrieden
Führen Sie vor der Einstellung von Mitarbeitern, die kritische Rollen übernehmen, angemessene Hintergrundprüfungen durch?	☐	☐
Gibt es klare Prozesse, um Mitarbeiter bei Sensibilisierungsthemen (z. B. Social Engineering, Phishing) laufend zu schulen?	☐	☐
9.2 Vertraulichkeits- und Verhaltensrichtlinien	**Umgesetzt**	**Zufrieden**
Werden im Rahmen des Onboarding-Prozesses schriftliche Vertraulichkeitsvereinbarungen und Sicherheitsrichtlinien kommuniziert und unterzeichnet?	☐	☐
Existieren Offboarding-Prozesse, in denen Zugriffsrechte systematisch entzogen und wichtige Geräte sowie Dokumente zurückgefordert werden?	☐	☐
9.3 Security Awareness und Schulungen	**Umgesetzt**	**Zufrieden**
Sind Schulungskonzepte zu aktuellen Bedrohungen, Richtlinien und Sicherheitsverfahren für alle Mitarbeitenden (inkl. Führungskräfte) vorhanden?	☐	☐
Messen Sie den Erfolg dieser Trainings, z. B. durch Tests, Phishing-Simulationen oder durch Auswertung von Sicherheitsvorfällen?	☐	☐

10. Technologische Aspekte		
10.1 Verschlüsselung und Schlüsselmanagement	Umgesetzt	Zufrieden
Setzen Sie angemessene Verschlüsselungsverfahren zum Schutz sensibler Daten ein (z. B. End-to-End-Verschlüsselung, Festplattenverschlüsselung)?	☐	☐
Gibt es Richtlinien zum Umgang mit kryptografischen Schlüsseln (Erzeugung, Verteilung, Austausch, Ablage und Entsorgung)?	☐	☐
10.2 Endpoint-Security und mobile Geräte	**Umgesetzt**	**Zufrieden**
Sind mobile Endgeräte (Smartphones, Tablets, Laptops) über Richtlinien und technische Maßnahmen (z. B. Mobile Device Management) abgesichert?	☐	☐
Verfügen Sie über Prozesse zum Patch- und Update-Management auf allen Endgeräten und kritischen Systemen?	☐	☐
10.3 Netzwerksicherheit	**Umgesetzt**	**Zufrieden**
Werden Firewalls, Intrusion Detection- bzw. Prevention-Systeme (IDS/IPS) oder Zero-Trust-Architekturen genutzt, um das Netzwerk zu segmentieren und zu schützen?	☐	☐
Wie wird das Netzwerk kontinuierlich auf Sicherheitslücken, auffälligen Datenverkehr oder Malware überprüft?	☐	☐
10.4 Identitäts- und Zugriffsmanagement (IAM)	**Umgesetzt**	**Zufrieden**
Nutzen Sie mehrstufige Authentifizierungsverfahren (z. B. MFA) für alle privilegierten Zugriffe?	☐	☐
Gibt es ein Rollen- und Berechtigungskonzept, das an den tatsächlichen Aufgaben der Nutzer ausgerichtet ist, und wird dieses regelmäßig überprüft?	☐	☐

11. Lieferanten- und Drittanbieter Management		
11.1 Vertragliche Absicherung	Umgesetzt	Zufrieden
Sind in Dienstleistungs- und Lieferantenverträgen alle sicherheitsrelevanten Anforderungen klar definiert und rechtlich abgesichert (z. B. Vertraulichkeitsklauseln, DSGVO-Vorgaben)?	☐	☐
Gibt es abgestimmte Service Level Agreements (SLAs), die Sicherheitsaspekte einschließen?	☐	☐
11.2 Evaluierung und Kontrolle	**Umgesetzt**	**Zufrieden**
Werden Lieferanten bzw. Drittanbieter regelmäßig auditiert oder überprüft, um sicherzustellen, dass sie Ihre Sicherheitsanforderungen weiterhin erfüllen?	☐	☐
Wie wird der Austausch sensibler Daten mit Drittanbietern überwacht und protokolliert?	☐	☐

12. Governance und Compliance		
12.1 Rechtliche und regulatorische Anforderungen	Umgesetzt	Zufrieden
Sind alle geltenden Gesetze, Vorschriften und Standards (z. B. DSGVO, branchenspezifische Vorgaben) erfasst und in Ihre internen Prozesse integriert?	☐	☐
Verfügen Sie über ein Compliance-Management, das regelmäßig prüft, ob alle Anforderungen erfüllt bleiben?	☐	☐
12.2 Rollen für Governance und Compliance	**Umgesetzt**	**Zufrieden**
Gibt es dedizierte Rollen und Gremien (z. B. Datenschutzbeauftragte, Security Steering Committee), die die Einhaltung der Vorgaben überwachen und kontinuierlich Verbesserungen anstoßen?	☐	☐
Werden Berichte, Auditergebnisse und Compliance-Status regelmäßig an das Management weitergegeben?	☐	☐

13. Business Continuity und Disaster Recovery		
13.1 Notfallprozesse und -dokumentation	Umgesetzt	Zufrieden
Gibt es einen dokumentierten Plan für den Umgang mit größeren Störungen (z. B. Naturkatastrophen, Cyberangriffe)?	☐	☐
Werden in regelmäßigen Abständen Notfallübungen durchgeführt, um die Wirksamkeit der Pläne zu testen und zu optimieren?	☐	☐
13.2 Datensicherung und Wiederherstellbarkeit	**Umgesetzt**	**Zufrieden**
Gibt es Richtlinien und Verfahren zur Datensicherung (Backup-Strategien, verschiedene Sicherungsorte, Verschlüsselung)?	☐	☐
Prüfen Sie regelmäßig, ob die Daten aus Backups tatsächlich wiederhergestellt werden können?	☐	☐
13.3 Rollen und Kommunikation im Krisenfall	**Umgesetzt**	**Zufrieden**
Sind die Zuständigkeiten in Krisensituationen klar festgelegt und sind die relevanten Personen (z. B. Krisenstab) geschult?	☐	☐

Wie stellen Sie die interne und externe Kommunikation (Kunden, Partner, Lieferanten) sicher, falls es zu einer größeren Sicherheitsstörung kommt?	☐	☐

14. Informationssicherheit für Remote- und Hybrid Arbeitsplätze		
14.1 Homeoffice Richtlinie	Umgesetzt	Zufrieden
Existiert eine Richtlinie oder mehrere für die Nutzung privater Geräte (BYOD) und/oder firmeneigener Geräte außerhalb der Unternehmensumgebung?	☐	☐
Werden Sicherheitsanforderungen (z. B. VPN, Multifaktor-Authentifizierung, Verschlüsselung) konsequent umgesetzt und kommuniziert?	☐	☐
14.2 Physische Sicherheit im Homeoffice	**Umgesetzt**	**Zufrieden**
Wie stellen Sie sicher, dass sensible Dokumente oder Geräte im Homeoffice ausreichend vor unbefugtem Zugriff geschützt sind (z. B. abschließbare Schränke, Richtlinien zur Aktenvernichtung)?	☐	☐
Werden Mitarbeitende regelmäßig zum sicheren Umgang mit Unternehmensinformationen im privaten Umfeld geschult?	☐	☐
14.3 Netzwerk- und Applikationszugriff	**Umgesetzt**	**Zufrieden**
Haben Sie technische Vorkehrungen getroffen, um Zugriffe auf Unternehmensnetzwerke und Anwendungen ausschließlich über abgesicherte Verbindungen zu ermöglichen?	☐	☐
Werden remote durchgeführte Updates und Patches kontrolliert, um sicherzustellen, dass alle Geräte auf dem neuesten Stand sind?	☐	☐

15. Datenschutz und Datensparsamkeit		
15.1 Integration von Datenschutz in das ISMS	Umgesetzt	Zufrieden
Haben Sie Datenschutz- und Informationssicherheitsprozesse aufeinander abgestimmt (z. B. Datenschutzfolgeabschätzung in Verbindung mit Risikobewertungen)?	☐	☐
Gibt es einen festen Austausch zwischen Datenschutzbeauftragten und ISMS-Verantwortlichen, um Synergieeffekte zu nutzen?	☐	☐
15.2 Datenminimierung und -löschung	**Umgesetzt**	**Zufrieden**
Werden nur die Daten erhoben und verarbeitet, die tatsächlich für den jeweiligen Zweck benötigt werden (Datensparsamkeit)?	☐	☐
Gibt es eindeutige Regelungen zu Aufbewahrungsfristen und zum sicheren Löschen bzw. Vernichten nicht mehr benötigter Daten?	☐	☐
15.3 Verantwortlichkeiten und Einwilligungen	**Umgesetzt**	**Zufrieden**
Sind Verantwortlichkeiten rund um die Verarbeitung personenbezogener Daten eindeutig festgelegt und dokumentiert?	☐	☐
Wie wird der Prozess zum Einholen, Widerrufen und Dokumentieren von Einwilligungen in Ihrem Unternehmen gemanagt?	☐	☐

16. Software- und Applikationssicherheit		
16.1 Sichere Softwareentwicklung	Umgesetzt	Zufrieden
Gibt es Richtlinien, die Sicherheit über den gesamten Softwareentwicklungszyklus hinweg integrieren (z. B. Code Reviews, Penetrationstests)?	☐	☐

Werden automatisierte Tools zur statischen und dynamischen Codeanalyse eingesetzt, um Sicherheitslücken frühzeitig aufzudecken?	☐	☐
16.2 Third-Party Libraries und Open-Source Komponenten	**Umgesetzt**	**Zufrieden**
Führen Sie ein Inventar der verwendeten Fremdbibliotheken und überwachen Sie diese auf bekannte Sicherheitslücken?	☐	☐
Gibt es Prozesse, um zeitnah Updates oder Patches einzuspielen, wenn Sicherheitslücken in Drittkomponenten gefunden werden?	☐	☐
16.3 Deployment und Betrieb	**Umgesetzt**	**Zufrieden**
Werden produktive und Testumgebungen strikt voneinander getrennt, um versehentliche Freigaben oder Datenlecks zu vermeiden?	☐	☐
Existieren Freigabe- und Rollback-Prozesse, um neue Software- oder Systemversionen risikofrei in Betrieb zu nehmen?	☐	☐

17. Monitoring und Sicherheitsoperationen		
17.1 Sicherheitsüberwachung	Umgesetzt	Zufrieden
Nutzen Sie ein Werkzeuge, um sicherheitsrelevante Ereignisse (Logs, Warnungen, Anomalien) kontinuierlich zu überwachen?	☐	☐
Sind Schwellenwerte für Alarmierungen und Eskalationen definiert und regelmäßig überprüft?	☐	☐
17.2 Incident Management	**Umgesetzt**	**Zufrieden**
Verfügen Sie über einen etablierten Prozess, um Sicherheitsvorfälle (Cyberangriffe, Datenlecks) zu erkennen, zu melden und zu bearbeiten?	☐	☐
Wie schnell reagieren Sie auf Zwischenfälle und wie stellen Sie sicher, dass die Nachverfolgung und Ursachenanalyse vollständig erfolgen?	☐	☐
17.3 Forensische Analysen	**Umgesetzt**	**Zufrieden**
Gibt es ein Verfahren, mit dem forensische Beweise gesichert, dokumentiert und ausgewertet werden können, ohne den normalen Betriebsablauf massiv zu beeinträchtigen?	☐	☐
Werden Mitarbeitende geschult, um bei Verdachtsmomenten oder festgestellten Angriffen korrekt zu handeln (z. B. Beweise nicht zu löschen, Meldung an ISMS-Verantwortliche)?	☐	☐

18. Sicherheitskultur und Kommunikation		
18.1 Feedback Prozesse	Umgesetzt	Zufrieden
Gibt es einen offenen Kommunikationskanal, über den Mitarbeitende mögliche Sicherheitsrisiken oder -verletzungen melden können (z. B. „Security Hotline“ oder „Ticket“-Programm)?	☐	☐
Werden Mitarbeitende für die Meldung potenzieller Sicherheitslücken positiv bestärkt, um eine aktive Sicherheitskultur zu etablieren?	☐	☐
18.2 Security-Updates und Kampagnen	**Umgesetzt**	**Zufrieden**
Informieren Sie Ihr Team regelmäßig über neu aufkommende Sicherheitsbedrohungen (Phishing-Kampagnen, neue Malware-Trends)?	☐	☐

Gibt es interne Informations- oder Sensibilisierungskampagnen, um das Bewusstsein für Informationssicherheit zu erhöhen?	☐	☐
18.3 Integration in die Unternehmenswerte	**Umgesetzt**	**Zufrieden**
Ist Informationssicherheit als strategischer Wert in Ihrer Unternehmenskultur verankert?	☐	☐
Wie stellt Ihr Führungsteam sicher, dass Sicherheitsaspekte bei allen geschäftlichen Entscheidungen berücksichtigt werden, z.B. bei neuen Projekten?	☐	☐

A. Instandhaltung und Wartung (Maintenance)		
A.1 Wartungsprozesse und Zuständigkeiten	Umgesetzt	Zufrieden
Verfügen Sie über einen definierten Wartungsplan für alle sicherheitskritischen Systeme (Server, Netzwerkinfrastruktur, Firewalls usw.)?	☐	☐
Sind Verantwortlichkeiten für die Wartung klar zugewiesen, und gibt es feste Intervalle oder Kriterien, die eine Wartung auslösen?	☐	☐
A.2 Sicherheit bei Wartungsarbeiten	**Umgesetzt**	**Zufrieden**
Wie stellen Sie sicher, dass nur autorisierte Personen Wartungs- oder Reparaturarbeiten durchführen (z. B. Identitätsprüfung, Begleitung durch internes Personal)?	☐	☐
Werden sensible Daten oder Zugriffsmöglichkeiten während der Wartungsarbeiten angemessen geschützt (z. B. Trennen vom Netzwerk, Nutzung getrennter Konten)?	☐	☐
A.3 Dokumentation der Wartung	**Umgesetzt**	**Zufrieden**
Erfassen Sie die durchgeführten Wartungsarbeiten (z. B. in Wartungsprotokollen oder Ticketsystemen) und überprüfen Sie regelmäßig deren Vollständigkeit und Korrektheit?	☐	☐
Werden sicherheitsrelevante Änderungen (z. B. an Konfigurationen oder Komponenten) dokumentiert und im Rahmen des Change-Management-Prozesses freigegeben?	☐	☐

B. Umgang mit mobilen Geräten und Wechselträgern		
B.1 Richtlinien und Verfahren	Umgesetzt	Zufrieden
Gibt es schriftlich festgelegte Richtlinien für den Umgang mit mobilen Geräten (Smartphones, Laptops, Tablets) und Wechseldatenträgern (USB-Sticks, externe Festplatten)?	☐	☐
Wie wird sichergestellt, dass alle Mitarbeitenden die Richtlinien kennen und verstehen (z. B. Schulungen, Awareness-Kampagnen)?	☐	☐
B.2 Geräteschutz und Verschlüsselung	**Umgesetzt**	**Zufrieden**
Sind alle mobilen Geräte standardmäßig verschlüsselt (z. B. per Full-Disk Encryption) und mit starker Authentifizierung (z. B. PIN/Passwort, biometrische Verfahren) gesichert?	☐	☐
Werden USB-Sticks und sonstige Wechseldatenträger verschlüsselt oder mithilfe eines Passworts geschützt?	☐	☐
B.3 Inventarisierung und Nachverfolgung	**Umgesetzt**	**Zufrieden**
Führen Sie ein Inventar über ausgegebene Geräte (z. B. Laptops, Firmenhandys) und kontrollieren Sie regelmäßig, ob dieses auf dem neuesten Stand ist?	☐	☐
Gibt es einen Prozess zur Rückgabe von Geräten und Wechseldatenträgern (Offboarding), sodass verloren gegangene oder nicht zurückgegebene Geräte zeitnah erkannt werden?	☐	☐

B.4 Fernzugriff und Netzwerksicherheit	Umgesetzt	Zufrieden
Nutzen Sie VPN- oder Zero-Trust-Lösungen, um den Zugriff auf Unternehmensressourcen aus der Ferne abzusichern?	☐	☐
Werden mobile Geräte automatisch mit Sicherheitsupdates (Betriebssystem, Anwendungen) versorgt und sind Richtlinien zum Patch-Management etabliert?	☐	☐
B.5 Verlust, Diebstahl und Vorfallmanagement	**Umgesetzt**	**Zufrieden**
Existiert ein klar definierter Ablauf für den Fall, dass mobile Geräte verloren gehen oder gestohlen werden (z. B. Meldung an IT, Remote-Löschung)?	☐	☐
Wie schnell können kompromittierte Accounts oder Zugriffsrechte gesperrt werden, um weiteren Schaden zu verhindern?	☐	☐

C. Softwarelizenzen und Softwareinventar		
C.1 Lizenzmanagement	Umgesetzt	Zufrieden
Verfügen Sie über einen Prozess zur Beschaffung, Verwaltung und regelmäßigen Überprüfung aller genutzten Softwarelizenzen?	☐	☐
Wie stellen Sie sicher, dass keine illegalen oder abgelaufenen Lizenzen im Unternehmen eingesetzt werden?	☐	☐
C.2 Inventarisierung von Software	**Umgesetzt**	**Zufrieden**
Gibt es ein aktuelles Software-Inventar, in dem sämtliche Anwendungen (inkl. Versionsnummern) aufgelistet sind?	☐	☐
Wer ist verantwortlich für die Pflege und Aktualisierung dieser Liste und gibt es feste Intervalle oder Anlässe, um das Inventar zu überprüfen?	☐	☐
C.3 Automatisierte Tools	**Umgesetzt**	**Zufrieden**
Nutzen Sie Tools oder Systeme (z. B. Software Asset Management-Systeme, Patch-Management-Lösungen), um Lizenzen und Versionsstände zu überwachen?	☐	☐
Werden bei Verstößen (z. B. unlizenzierte Software, fehlende Updates) automatisierte Alerts oder Berichte generiert?	☐	☐
C.4 Lizenz Compliance	**Umgesetzt**	**Zufrieden**
Prüfen Sie regelmäßig, ob die tatsächliche Nutzung Ihrer Software mit den Lizenzbestimmungen des Herstellers übereinstimmt (Audit-Anforderungen)?	☐	☐
Gibt es verbindliche Richtlinien, die regeln, wie und wo neue Software beschafft werden darf (z. B. Freigabeprozess, zentrale Einkaufseinheit)?	☐	☐

D. Vermögenswerte (Assets)		
D.1 Identifikation und Klassifizierung	Umgesetzt	Zufrieden
Haben Sie sämtliche relevanten Vermögenswerte (z. B. Hardware, Software, Datenbanken, Dokumente) identifiziert und kategorisiert (z. B. in Bezug auf Schutzbedarf)?	☐	☐
Existiert eine Richtlinie zur Einstufung von Assets (z. B. „öffentlich“, „intern“, „vertraulich“, „streng vertraulich“) und wird diese durchgesetzt?	☐	☐
D.2 Asset-Register und Verantwortlichkeiten	**Umgesetzt**	**Zufrieden**

Führen Sie ein zentrales Asset-Register, in dem Eigentümer, Standort, Wert und Schutzbedarf vermerkt sind	☐	☐
Sind für alle Assets eindeutige Verantwortlichkeiten (Asset Owner) definiert und kommuniziert?	☐	☐
D.3 Lebenszyklus Management	**Umgesetzt**	**Zufrieden**
Verfolgen Sie den kompletten Lebenszyklus eines Assets (Beschaffung, Betrieb, Wartung, Austausch/Entsorgung) und dokumentieren Sie relevante Aktionen?	☐	☐
Gibt es klare Prozesse für das Aussortieren oder die sichere Entsorgung von Assets (z. B. sichere Datenlöschung, Entwertung vor dem Recycling)?	☐	☐
D.4 Überwachung und Schutzmaßnahmen	**Umgesetzt**	**Zufrieden**
Wie überwachen Sie den Zustand Ihrer Assets (insbesondere kritische Infrastrukturen)?	☐	☐
Werden proaktive Kontrollen durchgeführt, um unautorisierte Änderungen oder Manipulationen an Assets zu erkennen?	☐	☐
D.5 Asset-Bewertung und Risikoeinschätzung	**Umgesetzt**	**Zufrieden**
Wird regelmäßig überprüft, ob die Klassifizierung des Assets nach wie vor korrekt ist (z. B. durch Veränderung der Geschäftsprozesse)?	☐	☐
Stellt Ihr Risikomanagement sicher, dass Änderungen an Assets (z. B. Standortwechsel, neuer Besitzer) in die Risikoanalyse einfließen?	☐	☐