IT-SICHERHEITSAUDIT CHECKLISTE

Ein IT-Sicherheitsaudit ermöglicht es Unternehmen, die aktuellen Sicherheitsmaßnahmen zu überprüfen, Schwachstellen aufzudecken und die Effektivität der IT-Sicherheitsstrategie zu bewerten. Diese Checkliste ist in acht Bereiche unterteilt:
Vorbereitung, technische Sicherheitsmaßnahmen, organisatorische Maßnahmen, rechtliche Anforderungen, Risikomanagement, Prüfung von Vorgaben, Durchführung von Überprüfungen und Ergebnisanalyse.

1. Vorbereitung des IT-Sicherheitsaudits

Aufgabe	Beschreibung	Status
Auditziele definieren	Welche Bereiche sollen geprüft werden (z. B. Netzwerk, Software, Daten, Mitarbeiter)?	
	Welches Ziel soll erreicht werden (z. B. Verbesserung der IT-Sicherheitsstrategie)?	
Verantwortlichkeiten klären	Benennung eines internen oder externen Auditors	
	Sicherstellen, dass die Geschäftsleitung involviert ist	
Dokumentation sichten	Sicherheitsrichtlinien, Protokolle, Handbücher und Inventar der IT-Infrastruktur prüfen	

2. Technische Sicherheitsmaßnahmen prüfen

Aufgabe	Beschreibung	Status
Netzwerksicherheit	Firewall-Regeln überprüfen	
	Sicherheitsstand der Router, Switches und Transceiver feststellen	
	Erkennen und Beheben offener Ports	
Endpoint-Sicherheit	Antivirensoftware und Passwortmanager einsetzen	
	Zwei-Faktor-Authentifizierung aktivieren	
Datensicherung	Wiederherstellungsplan testen	
	Funktion und Aktualität von Backups überprüfen	
Zugriffsrechte	Analyse von Berechtigungen	
	Überprüfung und Begrenzung von Zugriffen	
Patch-Management	Updates automatisieren und regelmäßig ausführen	

3. Organisatorische Maßnahmen prüfen

Aufgabe	Beschreibung	Status
Schulungen und Awareness	Mitarbeiter regelmäßig zu IT-Sicherheit schulen und Kenntnisse auffrischen	
Interne Kommunikation	Dokumentation von Kommunikationswegen	
	Klare Richtlinie zur internen Meldung von Vorfällen	
Sicherheitsrichtlinien und Prozesse	Sind Richtlinien für die Nutzung von IT-Ressourcen klar definiert?	
	Gibt es ein Prozesshandbuch für den Umgang mit Sicherheitsvorfällen?	
Physische Sicherheit	Zugangskontrollen für sensible Bereiche prüfen	
	Einsatz von Überwachungssystemen	

4. Rechtliche Anforderungen überprüfen

Aufgabe	Beschreibung	Status
Datenschutzgesetze	DSGVO-Konformität überprüfen	
	Sind alle Datenverarbeitungsprozesse dokumentiert?	
Branchenspezifische Vorgaben	Einhaltung von Standards (ISO 27001) sicherstellen	
Meldepflichten bei Sicherheitsvorfällen	Gibt es ein Konzept für die Benachrichtigung der zuständigen Behörden (z. B. BSI)?	
	Sind Verantwortlichkeiten klar definiert?	

5. Risikomanagement bewerten

Aufgabe	Beschreibung	Status
Risikobewertung	Identifikation potenzieller Risiken (z. B. Ransomware, Phishing)	
	Bewertung der Eintrittswahrscheinlichkeit	
Reaktionspläne für Sicherheitsvorfälle	Existieren Handlungsanweisungen für den Ernstfall (z. B. Hackerangriff)?	
	Sind interne und externe Ansprechpartner klar benannt?	
Regelmäßige Sicherheitsaudits	Festlegung eines Auditzyklus (z. B. jährlich)	
	Sicherstellung von Maßnahmen und Verbesserung der Audit-Ergebnisse	

6. Prüfung gesetzlicher und regulatorischer Vorgaben

Aufgabe	Beschreibung	Status
Datenschutz (DSGVO) und Branchenstandards	Werden personenbezogene Daten korrekt verarbeitet und gespeichert?	
	Gibt es ein Verfahren zur Meldung von Datenschutzverletzungen?	
	Sind Meldepflichten im Falle von Cyberangriffen bekannt und dokumentiert?	

7. Durchführung von Sicherheitsüberprüfungen

Aufgabe	Beschreibung	Status
Penetrationstests und Schwachstellenanalysen	Beauftragung von White-Hat-Hackern, um Schwachstellen zu finden	
	Gibt es Berichte über Sicherheitslücken und deren Behebung?	
Simulierte Angriffe und Notfallszenarien	Wie schnell wird reagiert bei simulierten Angriffen?	
	Gibt es klare Prozesse zur Wiederherstellung von Systemen nach einem Vorfall?	

8. Ergebnisanalyse und Dokumentation

Aufgabe	Beschreibung	Status
Auditbericht erstellen	Zusammenfassung der identifizierten Schwachstellen	
	Gibt es priorisierte Handlungsempfehlungen?	
Maßnahmenplan entwickeln und Nachbereitung	Gibt es Schritte zur Behebung von Schwachstellen?	
	Gibt es einen Plan für zukünftige Audits?	

Diese Checkliste hilft, den Zustand der IT-Sicherheit ganzheitlich zu bewerten, Stärken und Schwächen zu erkennen und gezielte Maßnahmen zu ergreifen. Ein regelmäßiges Audit trägt dazu bei, Sicherheitsstandards zu erhöhen und die Widerstandsfähigkeit gegen Cyberangriffe zu stärken.

Tipp: Nutzen Sie Tools und Frameworks wie das BSI-Grundschutz-Kompendium oder ISO 27001 für strukturierte Audits. So stellen Sie sicher, dass Ihre IT-Sicherheit den aktuellen Standards entspricht und potenzielle Risiken minimiert werden.