BSI-Grundschutz

Audit-Checkliste für KMU

Basierend auf dem IT-Grundschutz-Kompendium des BSI

60 prüfbare Maßnahmen für ein Basis-Audit Ihrer IT-Infrastruktur

Stand: Mai 2026 · Version 1.0

Bereitgestellt von Sat-iTec Systemhaus GmbH

itnetwork-docu.com

Anleitung

Diese Checkliste deckt die wichtigsten Bausteine des BSI IT-Grundschutz-Kompendiums (Edition 2023) für ein KMU-Audit ab. Sie ersetzt keine umfassende Risikoanalyse nach BSI-Standard 200-2, kann aber als Vorbereitung für ein Audit, eine Bestandsaufnahme oder eine ISO-27001-Vorbereitung verwendet werden.

So nutzen Sie die Checkliste

- Drucken Sie die Liste aus oder bearbeiten Sie sie direkt im Word-Dokument.
- Kreuzen Sie pro Prüfpunkt an: J = Ja (erfüllt), T = teilweise erfüllt, N = nicht erfüllt / nicht anwendbar.
- Notieren Sie offene Punkte und planen Sie Maßnahmen mit Verantwortlichen und Frist.
- Wiederholen Sie das Audit jährlich oder nach größeren Infrastruktur-Änderungen.

Wofür die BSI-Bausteine-Spalte?

Die Spalte verweist auf den jeweiligen Baustein des IT-Grundschutz-Kompendiums (z. B. CON.1 = Kryptokonzept, OPS.1.1.3 = Patchen, NET.1.2 = Netzmanagement). Bei Vertragsausschreibungen, Versicherern oder Auditoren können Sie damit die Konformitätsprüfung nachvollziehbar machen.

Tipp: Automatisieren Sie das Inventar

Etwa 70 % der Prüfpunkte (Hardware-Inventar, Software-Stand, AD-Berechtigungen, Server-Rollen, NFS-Shares, Patchstand) lassen sich automatisch aus einem Netzwerk-Audit-Tool ableiten. ITscanner ist eine deutsche Open-Core-Lösung mit Flat-Rate-Lizenz (49,50 € netto/Jahr) und liefert genau diese Daten als Bericht oder Excel-Export. 14 Tage kostenlos testen, ohne Cloud, ohne Asset-Pricing.

1. Sicherheitsorganisation (ISMS.1)

Nr.	BSI-Baustein	Prüfpunkt	Ja	Teilw.	Nein
1.1	ISMS.1	Es existiert eine schriftlich dokumentierte IT-Sicherheitsleitlinie, die von der Geschäftsführung freigegeben ist.	☐ J	☐ T	☐ N
1.2	ISMS.1	Ein IT-Sicherheitsbeauftragter (ISB) ist benannt und der gesamten Organisation bekannt.	☐ J	☐ T	☐ N
1.3	ISMS.1	Sicherheitsvorfälle werden in einem zentralen Register erfasst (Datum, Auswirkung, Maßnahme, Lessons-Learned).	☐ J	☐ T	☐ N
1.4	ORP.2	Mitarbeiter werden mindestens jährlich zu IT-Sicherheit, Phishing und Datenschutz geschult. *Nachweis pro Person + Datum aufbewahren.*	☐ J	☐ T	☐ N
1.5	ORP.3	Bei Eintritt, Wechsel und Austritt von Mitarbeitern werden Zugriffsrechte dokumentiert angepasst.	☐ J	☐ T	☐ N
1.6	ORP.4	Externe Dienstleister haben unterschriebene Vertraulichkeitsvereinbarungen (NDA).	☐ J	☐ T	☐ N

2. Inventarisierung & Asset-Management (CON.7)

Nr.	BSI-Baustein	Prüfpunkt	Ja	Teilw.	Nein
2.1	CON.7	Es existiert ein vollständiges Inventar aller Hardware-Assets (Server, Workstations, Drucker, Netzwerkkomponenten) inklusive Hersteller, Modell, Seriennummer, Standort. *ITscanner: Tab 'Hosts' liefert dies via WMI/CIM-Scan.*	☐ J	☐ T	☐ N
2.2	CON.7	Es existiert ein Inventar aller installierten Software-Pakete inklusive Version und Installationsdatum. *ITscanner: Tab 'Software' (agentless WMI-Scan) inklusive Excel-Export.*	☐ J	☐ T	☐ N
2.3	CON.7	Lizenzschlüssel und Aktivierungsstatus für kommerzielle Software werden zentral verwaltet. *ITscanner: Tab 'Lizenzen' aus Win32_SoftwareLicensingProduct.*	☐ J	☐ T	☐ N
2.4	CON.7	Das Inventar wird mindestens vierteljährlich aktualisiert.	☐ J	☐ T	☐ N
2.5	CON.7	Geräte ohne klaren Geschäftszweck werden identifiziert und stillgelegt oder dokumentiert.	☐ J	☐ T	☐ N

3. Identitätsmanagement & Active Directory (ORP.4, APP.2.2)

Nr.	BSI-Baustein	Prüfpunkt	Ja	Teilw.	Nein
3.1	ORP.4	Es existiert ein Konzept für rollenbasierte Zugriffsrechte (RBAC). Jede Rolle hat dokumentierte Berechtigungen. *ITscanner: AD-Tab listet Gruppen, Mitglieder und OU-Hierarchie.*	☐ J	☐ T	☐ N
3.2	APP.2.2	Domain-Admin- und Schema-Admin-Konten werden ausschließlich für administrative Tätigkeiten verwendet (kein E-	☐ J	☐ T	☐ N

		Mail/Web-Browsing).			
3.3	APP.2.2	Inaktive Benutzerkonten (kein Login > 90 Tage) werden regelmäßig identifiziert und deaktiviert. *ITscanner: AD-Audit zeigt 'lastLogonTimestamp' pro User.*	☐ J	☐ T	☐ N
3.4	APP.2.2	Passwort-Richtlinie: mindestens 12 Zeichen, Komplexität, max. 90 Tage Gültigkeit für Admin-Konten.	☐ J	☐ T	☐ N
3.5	APP.2.2	Multi-Faktor-Authentifizierung (MFA) ist für alle privilegierten Konten und externen Zugänge aktiviert.	☐ J	☐ T	☐ N
3.6	APP.2.2	Lokale Administrator-Passwörter sind individuell pro Gerät (LAPS oder vergleichbar).	☐ J	☐ T	☐ N
3.7	APP.2.2	Es existieren mindestens zwei Domain-Controller (Redundanz). *ITscanner: BSI-Bericht warnt bei nur 1 DC.*	☐ J	☐ T	☐ N

4. Patch-Management & End-of-Life-Systeme (OPS.1.1.3)

Nr.	BSI-Baustein	Prüfpunkt	Ja	Teilw.	Nein
4.1	OPS.1.1.3	Sicherheitsupdates für Betriebssysteme werden binnen 14 Tagen nach Verfügbarkeit eingespielt.	☐ J	☐ T	☐ N
4.2	OPS.1.1.3	Es existieren keine produktiv genutzten End-of-Life-Systeme (Windows 7, Server 2008/2012 etc.) ohne dokumentierte Risikoabnahme. *ITscanner: BSI-Bericht markiert EOL-OS automatisch.*	☐ J	☐ T	☐ N
4.3	OPS.1.1.3	Drittanbieter-Software (Browser, PDF-Reader, Office) wird ebenfalls regelmäßig gepatcht.	☐ J	☐ T	☐ N
4.4	OPS.1.1.3	Vor Patches gibt es eine Test-Phase auf nicht-produktiven Systemen.	☐ J	☐ T	☐ N
4.5	OPS.1.1.3	Patch-Status wird zentral überwacht und dokumentiert.	☐ J	☐ T	☐ N

5. Netzwerk-Sicherheit (NET.1.1, NET.1.2)

Nr.	BSI-Baustein	Prüfpunkt	Ja	Teilw.	Nein
5.1	NET.1.1	Das Netzwerk ist segmentiert: separate VLANs/Subnetze für Server, Clients, Gäste, Drucker. *ITscanner: Tab 'Subnetze' liefert eine Übersicht aktiver IP-Bereiche.*	☐ J	☐ T	☐ N
5.2	NET.1.1	Nicht benötigte Netzwerk-Dienste sind auf allen Hosts deaktiviert (Telnet, FTP unverschlüsselt, SMBv1).	☐ J	☐ T	☐ N
5.3	NET.1.1	Offene Ports werden regelmäßig per Port-Scan überprüft. *ITscanner: führt automatischen Port-Probe für RDP/SSH/SMB/NFS durch.*	☐ J	☐ T	☐ N
5.4	NET.1.2	Eine Firewall trennt internes Netz vom Internet, mit dokumentiertem Regelwerk.	☐ J	☐ T	☐ N
5.5	NET.1.2	VPN-Zugänge sind ausschließlich mit MFA und nicht ungeschützt aus dem Internet erreichbar.	☐ J	☐ T	☐ N

5.6	NET.1.2	Externe RDP-Zugänge (TCP 3389) sind grundsätzlich nicht aus dem Internet erreichbar. *ITscanner: BSI-Bericht warnt bei sichtbaren RDP-Ports.*	☐ J	☐ T	☐ N

6. Backup & Wiederherstellung (CON.3, OPS.1.1.5)

Nr.	BSI-Baustein	Prüfpunkt	Ja	Teilw.	Nein
6.1	CON.3	Eine Backup-Software ist auf allen kritischen Servern installiert und aktiv. *ITscanner: Tab 'Software' zeigt Backup-Tools (Veeam, Bareos, Acronis u.a.).*	☐ J	☐ T	☐ N
6.2	CON.3	Es existiert ein dokumentiertes Backup-Konzept mit RPO und RTO pro Geschäftsfunktion.	☐ J	☐ T	☐ N
6.3	CON.3	Mindestens eine Backup-Kopie liegt offline / off-site (3-2-1-Regel).	☐ J	☐ T	☐ N
6.4	CON.3	Backup-Restore wird mindestens halbjährlich auf Test-Systemen durchgespielt.	☐ J	☐ T	☐ N
6.5	OPS.1.1.5	Datenbank-Backups (SQL Server, MariaDB, PostgreSQL) sind separat konfiguriert und konsistent.	☐ J	☐ T	☐ N
6.6	CON.3	Backups sind verschlüsselt, sowohl in Transit als auch at rest.	☐ J	☐ T	☐ N

7. Logging & Monitoring (DER.1, OPS.1.1.6)

Nr.	BSI-Baustein	Prüfpunkt	Ja	Teilw.	Nein
7.1	DER.1	Sicherheitsrelevante Ereignisse (Login-Fehlversuche, Privilegien-Änderungen, AD-Änderungen) werden zentral geloggt.	☐ J	☐ T	☐ N
7.2	DER.1	Logs werden mindestens 12 Monate aufbewahrt (für DSGVO-Nachweispflichten ggf. länger).	☐ J	☐ T	☐ N
7.3	DER.1	Logs werden mindestens wöchentlich auf Auffälligkeiten geprüft (manuell oder per SIEM/Alerting).	☐ J	☐ T	☐ N
7.4	DER.1	Verfügbarkeit kritischer Server wird per Monitoring überwacht (z. B. Nagios, Zabbix, Checkmk).	☐ J	☐ T	☐ N

8. Endpoint-Sicherheit (SYS.2.1, SYS.2.2)

Nr.	BSI-Baustein	Prüfpunkt	Ja	Teilw.	Nein
8.1	SYS.2.1	Auf allen Windows-Endgeräten ist ein aktueller Antivirus / EDR aktiv (Defender AV oder Drittanbieter).	☐ J	☐ T	☐ N
8.2	SYS.2.1	Festplatten-Verschlüsselung (BitLocker / LUKS) ist auf Notebooks und mobilen Geräten aktiv.	☐ J	☐ T	☐ N
8.3	SYS.2.1	USB-Datenträger sind durch Endpoint-Policy auf 'read-only'	☐ J	☐ T	☐ N

		oder gar nicht erlaubt.			
8.4	SYS.2.2	Mobile Geräte (Smartphones, Tablets) werden über MDM verwaltet und können remote gelöscht werden.	☐ J	☐ T	☐ N

9. Datei-Server & Berechtigungen (APP.3.3, ORP.4)

Nr.	BSI-Baustein	Prüfpunkt	Ja	Teilw.	Nein
9.1	APP.3.3	SMB-Freigaben sind dokumentiert mit Zweck, Verantwortlichem und Berechtigungs-Konzept. *ITscanner: Tab 'Freigaben' listet Shares + ACL je Host.*	☐ J	☐ T	☐ N
9.2	APP.3.3	Berechtigungen folgen dem Need-to-Know-Prinzip; 'Jeder' / 'Authenticated Users' Vollzugriff ist die Ausnahme.	☐ J	☐ T	☐ N
9.3	APP.3.3	NFS-Shares werden ebenfalls inventarisiert und sind nicht unbeschränkt zugänglich (no_root_squash, *). *ITscanner v2.08.11+: NFS-Detection für Linux-Hosts.*	☐ J	☐ T	☐ N
9.4	APP.3.3	Quotas verhindern das Volllaufen von Datei-Servern durch einzelne User.	☐ J	☐ T	☐ N

10. Notfallvorsorge (DER.4)

Nr.	BSI-Baustein	Prüfpunkt	Ja	Teilw.	Nein
10.1	DER.4	Es existiert ein schriftliches Notfallhandbuch (Wer ruft wen an? Wo liegen Backup-Tapes? Wie wird das System wiederhergestellt?).	☐ J	☐ T	☐ N
10.2	DER.4	Notfallkontakte (intern, externe Dienstleister, BSI/CERT) sind aktuell und allen Schlüsselpersonen bekannt.	☐ J	☐ T	☐ N
10.3	DER.4	Mindestens jährlich findet eine Notfallübung statt (Tabletop oder echtes Failover).	☐ J	☐ T	☐ N
10.4	DER.4	Eine Cyber-Versicherung ist abgeschlossen oder ein bewusster Verzicht ist dokumentiert.	☐ J	☐ T	☐ N

Auswertung & nächste Schritte

Zählen Sie die ‚Nein'- und ‚Teilweise'-Antworten und priorisieren Sie nach Risiko (vertrauliche Daten, Verfügbarkeit, gesetzliche Pflichten).

Empfohlene Reihenfolge der Umsetzung

- Quick Wins (≤ 1 Tag): MFA für Admin-Konten, RDP aus dem Internet schließen, EOL-Systeme identifizieren, Backup-Restore-Test durchspielen.
- Mittelfristig (1-3 Monate): Vollständige Inventarisierung (Hardware + Software + Lizenzen), Patch-Prozess etablieren, Berechtigungs-Audit auf Datei-Servern.
- Strategisch (6-12 Monate): ISMS-Struktur aufbauen, Notfallhandbuch erstellen und proben, Cyber-Versicherung verhandeln, ggf. ISO-27001-Vorprojekt.

Inventarisierung automatisieren – mit ITscanner

Etwa 25 der 60 Prüfpunkte oben (Hardware-Inventar, Software-Stand, AD-Audit, Lizenzen, Server-Rollen, SMB- und NFS-Freigaben, EOL-Erkennung) liefert ITscanner automatisch aus einem 30-Minuten-Scan. Der eingebaute BSI-Grundschutz-Bericht weist Sie direkt auf offene Punkte hin (EOL-OS, offene RDP-Ports, fehlende Backup-Software, nur 1 Domain-Controller, alte Lizenz-Aktivierungen).
Flat-Rate-Lizenz: 49,50 € netto/Jahr — egal wie viele Geräte. Lokal, ohne Cloud, DSGVO-konform. 14 Tage kostenlos testen ohne Kreditkarte: itnetwork-docu.com

Quellen & Weiterführendes

- BSI IT-Grundschutz-Kompendium (offizielle Quelle)
- BSI IT-Grundschutz Edition 2023 (PDF)
- ITscanner vs. Docusnap & Co. — Vergleich
- ITscanner kostenlos herunterladen (Windows + Linux)