OM-IT SYSTEME GMBH
Innovation zur digitalen Revolution.

Ergebnisbericht zum Compliance-Check

IT-Sicherheits-Compliance-Report

Erstellt am	Unternehmensgröße	Branche
6. Oktober 2026	Mittelständische Unternehmen (51–250 Mitarbeiter)	Produktion & Industrie

Compliance-Score

45 %

Level

Verbesserungsbedarf

Risiko

Hoch

Erhebliche Compliance-Lücken

Stärkste Kategorie

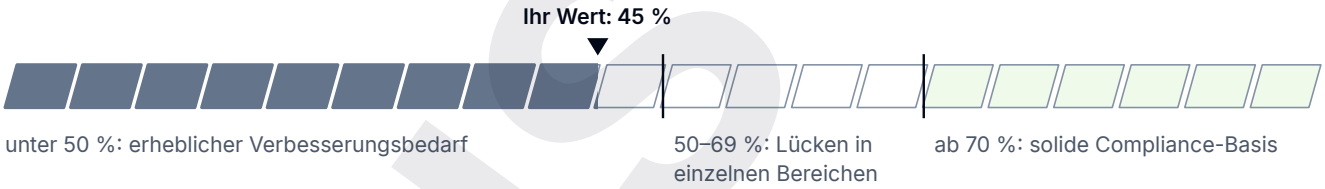
65 %

IT-Sicherheit

Größtes Verbesserungspotenzial

0 %

Business Continuity



Zusammenfassung

Ihr Unternehmen erreicht einen Compliance-Score von 45 % (Verbesserungsbedarf). Dieser Wert basiert auf 7 Compliance-Kategorien, die für Ihr Unternehmen relevant sind, und berücksichtigt Ihre Unternehmensgröße (Mittelständische Unternehmen (51–250 Mitarbeiter)) sowie Ihre Branche (Produktion & Industrie). Einordnung nach der Skala dieses Checks: Ab 70 % besteht eine solide Compliance-Basis, von 50 bis 69 % gibt es Lücken in einzelnen Bereichen, unter 50 % erheblichen Verbesserungsbedarf. Ihr Wert liegt im Bereich unter 50 %.

NIS2/BSIG, vorläufige Einschätzung ohne Rechtsberatung: Betroffenheit bitte prüfen. Details stehen im Abschnitt Bußgeldrisiken. Ihre stärkste Kategorie ist „IT-Sicherheit“ mit 65 %, die größten Verbesserungspotenziale liegen in „Business Continuity“ mit 0 %.

NIS2/BSIG

Betroffenheit bitte prüfen

vorläufige Einschätzung ohne Rechtsberatung. Details stehen im Abschnitt Bußgeldrisiken.

Wichtiger Hinweis: Dies ist keine Rechtsberatung

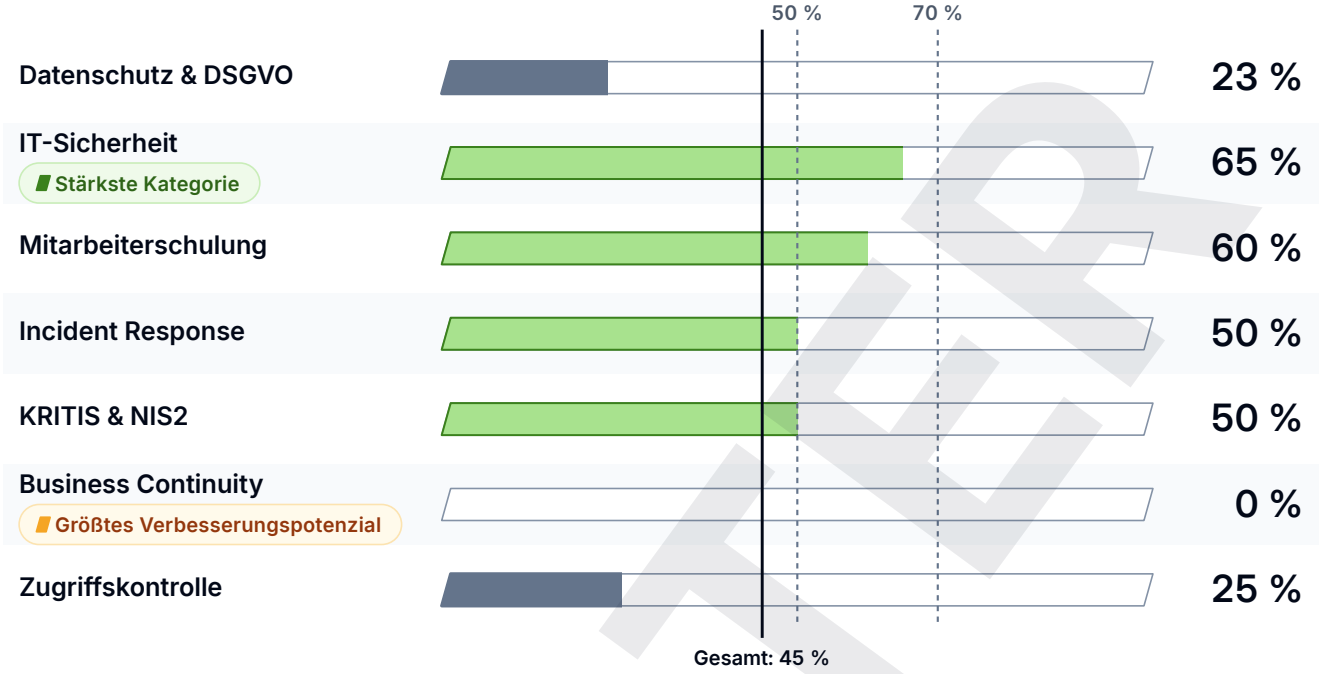
Die Inhalte dieses Reports stellen keine Rechtsberatung dar. Sie dienen ausschließlich zur Orientierung und ersetzen keine individuelle rechtliche Prüfung durch einen Rechtsanwalt oder Datenschutzbeauftragten.

MUSTER

MUSTERBERICHT MIT BEISPIELWERTEN – KEIN ECHTES ERGEBNIS

Detaillierte Bewertung nach Kategorien

Erreichter Anteil je Kategorie, eingeordnet auf der Skala dieses Checks



ab 70 %: solide Compliance-Basis

50–69 %: Lücken in einzelnen Bereichen

unter 50 %: erheblicher Verbesserungsbedarf

Kritische Maßnahmen

Hohe Priorität – Kurzfristig empfohlen

1 von 6

Kritisch

Prüfung und Implementierung grundlegender Sicherheitsmaßnahmen: MFA für alle wichtigen Systeme (E-Mail, VPN, Admin-Konten, Cloud-Dienste) aktivieren, 3-2-1-Backup-Strategie mit täglichen Tests und monatlichen Restore-Übungen einrichten, Firewall-Regeln überprüfen und aktualisieren, Festplattenverschlüsselung (BitLocker/FileVault) auf allen Endgeräten aktivieren – **innerhalb von 2 Wochen** umsetzen

2 von 6

Kritisch

Rechtliche Prüfung, ob ein Datenschutzbeauftragter erforderlich ist (bitte durch Rechtsanwalt prüfen lassen) und bei Verpflichtung **innerhalb von 1 Woche** einen qualifizierten DSB benennen und Ressourcen bereitstellen

Fortsetzung: Kritische Maßnahmen 3–6 auf der nächsten Seite

MUSTERBERICHT MIT BEISPIELWERTEN – KEIN ECHTES ERGEBNIS

3 von 6
Kritisch

Rechtliche Prüfung, ob ein Verarbeitungsverzeichnis erforderlich ist (bitte durch Rechtsanwalt prüfen lassen) und bei Verpflichtung **innerhalb von 2 Wochen** ein vollständiges Verzeichnis aller Datenverarbeitungen mit Zweck, Rechtsgrundlage, Systemen und Löschfristen erstellen

4 von 6
Kritisch

Dokumentation von Incident-Response-Verfahren: Notfallplan mit Ansprechpartnern, Meldeverfahren (DSGVO 72 Stunden, IT-SiG/NIS2 24 Stunden), ersten Maßnahmen, Kommunikationsrichtlinien und Vorlagen für Meldungen erstellen und allen Verantwortlichen zugänglich machen – **innerhalb von 1 Woche**

5 von 6
Kritisch

Security-Awareness-Schulungen durchführen: Jährliche Pflichtschulung für alle Mitarbeiter organisieren, Phishing-Simulationen monatlich durchführen, schriftliche Sicherheitsrichtlinien erstellen und Integration ins Onboarding sicherstellen – **innerhalb von 1 Monat** umsetzen

6 von 6
Kritisch

Schließung aller identifizierten kritischen Lücken: Konkrete Liste mit Verantwortlichen und Fristen erstellen, wöchentliche Status-Updates durchführen und alle kritischen Lücken **innerhalb von 3 Monaten** vollständig beheben

MUSTER

MUSTERBERICHT MIT BEISPIELWERTEN – KEIN ECHTES ERGEBNIS

Empfohlene Maßnahmen

Kurzfristig umsetzen (3–6 Monate)

1 von 5 — Empfohlen

Externe IT-Sicherheitsberatung einholen, Gap-Analyse durchführen lassen und konkreten Umsetzungsplan mit Prioritäten und Fristen erstellen

2 von 5 — Empfohlen

Umfassenden Compliance-Plan mit allen erforderlichen Maßnahmen, Verantwortlichkeiten, Zeitplänen und Erfolgskriterien entwickeln und monatlich überprüfen

3 von 5 — Empfohlen

Vierteljährliche Sicherheitsbewertungen durch interne oder externe Experten durchführen, Ergebnisse dokumentieren und Maßnahmenplan mit Fristen erstellen

4 von 5 — Empfohlen

Vollständige Dokumentation aller IT-Sicherheitsmaßnahmen, Prozesse, Verantwortlichkeiten und Incident-Response-Pläne in einem zentralen System erstellen und wöchentlich aktualisieren

5 von 5 — Empfohlen

Jährliche verpflichtende IT-Sicherheitsschulungen für alle Mitarbeiter durchführen, Phishing-Simulationen monatlich testen und Ergebnisse dokumentieren

Zusätzliche Maßnahmen

Mittelfristig umsetzen – Optimierung für langfristige Compliance

1 von 3 — Zusätzlich

Security-Awareness-Programm einführen: Jährliche Pflichtschulungen, monatliche Phishing-Simulationen, schriftliche Sicherheitsrichtlinien mit Unterschrift, Integration ins Onboarding und Nachschulungen bei Auffälligkeiten umsetzen

Fortsetzung: Zusätzliche Maßnahmen 2–3 auf der nächsten Seite

2 von 3

Zusätzlich

Erweiterte Monitoring-Lösungen implementieren: SIEM-System für zentrale Log-Auswertung, EDR für Endpoint-Überwachung, automatische Alarmierung bei verdächtigen Aktivitäten und tägliche Log-Reviews durch geschultes Personal einrichten

3 von 3

Zusätzlich

Halbjährliche externe Sicherheitsaudits durch zertifizierte Experten durchführen lassen, Audit-Berichte systematisch auswerten, alle identifizierten Schwachstellen **innerhalb von 1 Monat** beheben und Maßnahmen dokumentieren

Bußgeldrisiken

Bei Verstößen gegen IT-Sicherheits- und Datenschutzbestimmungen drohen erhebliche Bußgelder. Die folgenden Beispiele zeigen reale Fälle aus der Praxis und die rechtlichen Grundlagen:

Relevante Gesetze für Ihr Unternehmen

- **DSGVO:** Bis zu 20 Mio. € oder 4 % des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist (Art. 83 Abs. 5 DSGVO)
- **NIS2/BSIG – Betroffenheit bitte prüfen:** Ihre Branche umfasst erfasste und nicht erfasste Tätigkeiten. Erfasst sind: Anlage 2 Nr. 5 Verarbeitendes Gewerbe (Medizinprodukte und In-vitro-Diagnostika, Datenverarbeitungsgeräte, elektronische und optische Erzeugnisse, Elektrische Ausrüstungen, Maschinenbau, Kraftwagen und Kraftwagenteile, Sonstiger Fahrzeugbau); Anlage 2 Nr. 3 Chemie (Herstellung von und Handel mit chemischen Stoffen); Anlage 2 Nr. 4 Produktion, Verarbeitung und Vertrieb von Lebensmitteln (Lebensmittelunternehmen im Großhandel sowie in der industriellen Produktion und Verarbeitung); Anlage 1 Nr. 4 Gesundheit (Gesundheitsdienstleister, Referenzlabore, Arzneimittel-Forschung und -Herstellung, kritische Medizinprodukte). Gehört Ihr Unternehmen dazu, ist es ab 50 Beschäftigten mindestens wichtige Einrichtung. Als wichtige Einrichtung gilt, wer mindestens 50 Beschäftigte hat oder bei wem Jahresumsatz und Jahresbilanzsumme jeweils über 10 Mio. € liegen; als besonders wichtige Einrichtung ab 250 Beschäftigten oder bei über 50 Mio. € Umsatz und über 43 Mio. € Bilanzsumme (§ 28 BSIG). Die Einstufung als besonders wichtige Einrichtung nach Größe gilt nur für die Sektoren der Anlage 1. Unternehmen aus Anlage 2 – etwa Lebensmittelindustrie und Maschinenbau – sind ab 50 Beschäftigten wichtige Einrichtungen, auch mit 250 oder mehr Beschäftigten. Vorläufige Einschätzung, keine Rechtsberatung. Sonderfälle wie Konzernzugehörigkeit, Nebentätigkeiten oder gesetzliche Ausnahmen sind nicht berücksichtigt.
- **§ 65 BSIG (Umsetzung von Art. 34 NIS2-RL):** bis 10 Mio. € bzw. 2 % des weltweiten Umsatzes für besonders wichtige, bis 7 Mio. € bzw. 1,4 % für wichtige Einrichtungen (Prozentwerte erst ab 500 Mio. € Gesamtumsatz)

MUSTER

Reale Bußgeldbeispiele

1 **DSGVO-Bußgeld 2020: 35,3 Mio. €**

Systematische Erfassung privater Lebensumstände von Beschäftigten (H&M, Hamburgischer Beauftragter für Datenschutz, 2020). Hinweis: Beispiel aus der Aufsichtspraxis; die Höhe variiert im Einzelfall. Keine Rechtsberatung.

2 **DSGVO-Bußgeld 2020: 1,24 Mio. €**

Gewinnspieldaten ohne wirksame Einwilligung für Werbung genutzt; unzureichende technische/organisatorische Maßnahmen (AOK Baden-Württemberg, LfDI BW, Art. 32 DSGVO, 2020). Hinweis: Beispiel aus der Aufsichtspraxis; die Höhe variiert im Einzelfall. Keine Rechtsberatung.

Rechtlicher Hinweis

Wichtiger Hinweis: Dies ist keine Rechtsberatung

Die Inhalte dieses IT-Sicherheits-Compliance-Reports stellen keine Rechtsberatung dar. Sie dienen ausschließlich zur Orientierung und ersetzen keine individuelle rechtliche Prüfung durch einen Rechtsanwalt oder qualifizierten Datenschutzbeauftragten.

Bei rechtlichen Fragen sollten Sie stets einen spezialisierten Rechtsanwalt oder Datenschutzbeauftragten konsultieren. Die Bewertung basiert auf allgemeinen Compliance-Grundsätzen und kann nicht alle individuellen Umstände Ihres Unternehmens berücksichtigen.

Die Angaben zu Bußgeldern, gesetzlichen Anforderungen und Maßnahmen sind Beispiele und Orientierungshilfen. Die tatsächlichen Anforderungen können je nach Einzelfall, Branche, Unternehmensgröße und weiteren Faktoren erheblich variieren.

MUSTER

> Für eine vollständige Compliance-Prüfung und rechtliche Beratung sollten Sie einen spezialisierten Rechtsanwalt oder Datenschutzbeauftragten konsultieren. OM-IT Systeme übernimmt keine Haftung für die Richtigkeit, Vollständigkeit oder Aktualität der Informationen in diesem Report.

Gemeinsam zur Compliance

Nächste Schritte zu Ihrer IT-Sicherheits-Compliance

Warum mit OM-IT zusammenarbeiten?

- Individuelle Lösungen für Ihre spezifischen Anforderungen
- Erfahrung in IT-Sicherheit und Compliance
- Von der Analyse bis zur Umsetzung – alles aus einer Hand
- Persönliche Betreuung – vor Ort im Oldenburger Münsterland, remote bundesweit

Ihre nächsten Schritte

01 Kostenfreies Erstgespräch vereinbaren (ca. 60 Minuten)

02 Individuelle Compliance-Strategie entwickeln

03 Schritt für Schritt zur Compliance

Kontaktieren Sie uns jetzt:

Erstgespräch anfragen: omit-systeme.de/beratung →

Telefon
04442 888 6190

E-Mail
info@omit-systeme.de

Web
www.omit-systeme.de/beratung

Erreichbarkeit
Mo–Fr 8:00–17:00 Uhr

Anschrift
Gewerbering 35, 49393 Lohne (Oldenburg)

MUSTER