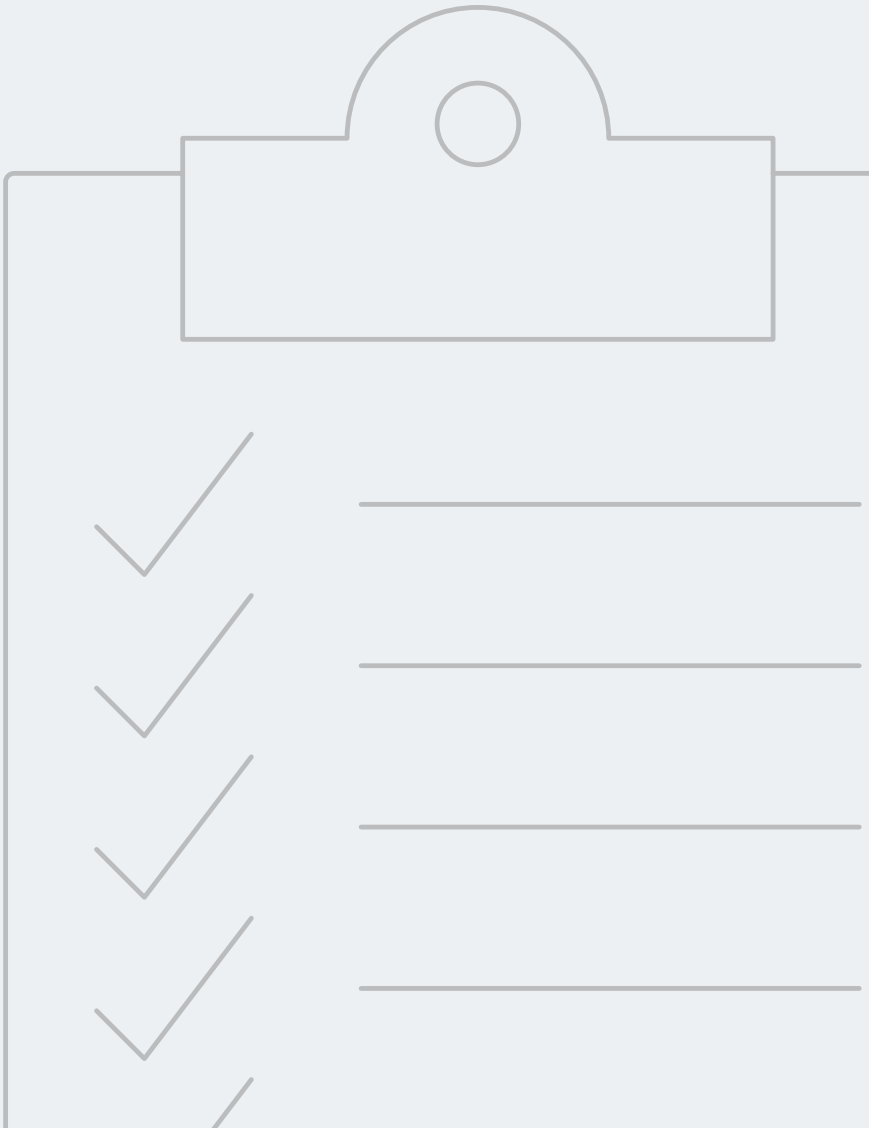
bitbase group

ISO 27001 CHECKLISTE

Januar 2026

ISO 27001 Checkliste

In 10 Schritten zur erfolgreichen Zertifizierung

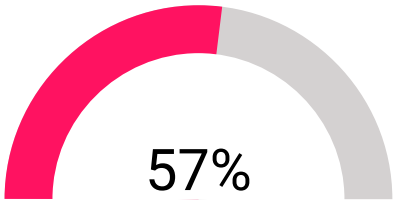


bbg bitbase group GmbH

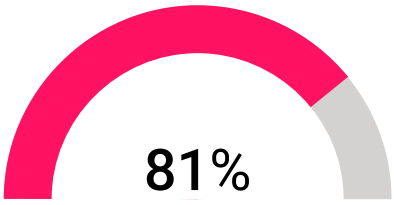
Am Heilbrunnen 47
72766 Reutlingen
mail@bitbasegroup.com

Warum eine **ISO 27001-Checkliste** sinnvoll ist

Informationssicherheit ist kein Zufallsprodukt, sondern das Ergebnis klarer Strukturen und gelebter Prozesse. Ein Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001 bietet Unternehmen einen systematischen Rahmen, um Informationswerte zu schützen, Risiken zu steuern und gesetzliche Vorgaben nachweisbar zu erfüllen.



Mehr als die Hälfte dieser Firmen (57 %) berichteten, dass der entstandene Schaden deutlich gestiegen sei.

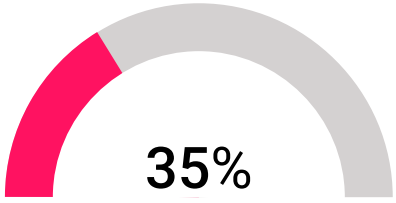


Diese Zahlen zeigen deutlich: Informationssicherheit darf kein isoliertes IT-Thema mehr sein.
Ein funktionierendes ISMS ist heute die Grundlage, um Risiken zu reduzieren, Vertrauen zu schaffen und gesetzliche sowie vertragliche Anforderungen zu erfüllen. Diese Checkliste hilft Ihnen, den Überblick zu behalten. Sie zeigt die wichtigsten Schritte auf dem Weg zur erfolgreichen Zertifizierung – von der Vorbereitung bis zur Auditphase. So können Sie Ihr ISMS gezielt aufbauen, dokumentieren und kontinuierlich verbessern.

266 mrd

Nach Angaben des Branchenverbands Bitkom (2023) beläuft sich der wirtschaftliche **Gesamtschaden durch Datendiebstahl, Spionage und Sabotage** inzwischen auf rund 266 Milliarden Euro jährlich.

Rund 81 % aller Unternehmen in Deutschland waren im selben Zeitraum von Sicherheitsvorfällen betroffen.



Laut einer aktuellen KPMG-Studie (2024) waren mehr als 35 % der deutschen Unternehmen in den vergangenen zwei Jahren Opfer eines Cyberangriffs.

Quellen: KPMG 2024, Bitkom 2023

Für wen ist die Checkliste geeignet?

Für Informationssicherheitsbeauftragte (ISB), IT- und Compliance-Verantwortliche, Dateschutz-beauftragte sowie Führungskräfte, die ihr Unternehmen auditfähig machen oder eine ISO-Zertifizierung vorbereiten möchten. Besonders relevant ist sie für Organisationen mit hohem Schutzbedarf, etwa Cloud-Dienstleistende, Finanzunternehmen, Rechenzentren oder Betreiber kritischer Infrastrukturen.

Die ISO 27001 Checkliste
10 Schritte zum zertifizierten ISMS

Vorbereitung: Bestandsaufnahme und GAP-Analyse

Bevor Sie starten, empfiehlt sich eine strukturierte Bestandsaufnahme. Vergleichen Sie Ihre aktuelle Sicherheitsorganisation mit den Anforderungen der ISO 27001, identifizieren Sie Lücken und priorisieren Sie Maßnahmen. Diese GAP-Analyse schafft Transparenz und bildet die Grundlage für einen realistischen Projekt- und Auditplan.

01

MANAGEMENT-COMMITTMENT SICHERN

Ein ISMS kann nur erfolgreich sein, wenn die Geschäftsführung es aktiv unterstützt. Verankern Sie Informationssicherheit als strategisches Ziel, definieren Sie Verantwortlichkeiten und verabschieden Sie eine unternehmensweite Sicherheitsleitlinie. So entsteht die Grundlage für alle weiteren Schritte.

02

ISMS-ORGANISATION UND ROLLEN AUFBAUEN

Erfolgreiche Informationssicherheit braucht klare Zuständigkeiten.
Benennen Sie zentrale Rollen wie den Informationssicherheitsbeauftragten, das ISMS-Team sowie Verantwortliche in IT, Datenschutz und Fachabteilungen.
Eine gut aufgestellte Organisation sorgt dafür, dass Informationssicherheit in allen Unternehmensprozessen verankert ist.

03

ISMS-STRATEGIE UND HANDBUCH ERSTELLEN

Die Strategie beschreibt, wohin Ihr Unternehmen in Sachen Informationssicherheit will, das Handbuch zeigt, wie Sie dorthin gelangen. Hier werden Prozesse, Ziele und Kontrollmechanismen dokumentiert. Das Handbuch dient intern als Referenz und extern als Nachweis der systematischen Umsetzung.

04

GELTUNGSBEREICH UND SCHUTZOBJEKTE FESTLEGEN

Definieren Sie, welche Bereiche, Systeme, Standorte und Informationswerte in das ISMS einbezogen werden. Ergänzen Sie Ihre Beschreibung um Dokumente wie Organigramme, Netzpläne oder Prozesslandkarten. Der Geltungsbereich sollte regelmäßig überprüft und durch die Geschäftsführung formal freigegeben werden.

05

RISIKOANALYSE DURCHFÜHREN

Bewerten Sie, welche Risiken Ihre Informationswerte gefährden könnten und wie wahrscheinlich deren Eintreten ist. Die Analyse bildet die Grundlage für gezielte Sicherheitsmaßnahmen und einen priorisierten Risikobehandlungsplan.

Ziel ist nicht absolute Sicherheit, sondern ein angemessenes und kontrollierbares Schutzniveau.

SICHERHEITSRICHTLINIEN UMSETZEN

Leiten Sie aus der SoA operative Richtlinien ab, beispielsweise für Zugriffsrechte, Netzwerksicherheit, Patch-Management, Backup oder Notfallmanagement. Die Richtlinien müssen klar dokumentiert, kommuniziert und regelmäßig überprüft werden. So stellen Sie sicher, dass Sicherheitsmaßnahmen im Alltag angewendet und verstanden werden.

06

ERKLÄRUNG DER ANWENDBARKEIT (SOA) ERSTELLEN

Die SoA (Statement of Applicability) übersetzt Ihre Risikoanalyse in konkrete Maßnahmen. Darin wird festgelegt, welche Sicherheitskontrollen der ISO 27001 für Ihr Unternehmen gelten und welche bewusst ausgeschlossen werden. Sie ist eines der zentralen Dokumente im Zertifizierungsaudit.

07

08

DOKUMENTATION UND NACHWEISE PFLEGEN

Ein ISMS lebt von Nachvollziehbarkeit. Pflegen Sie alle relevanten Dokumente zentral, versioniert und revisionssicher. So können Sie im Audit jederzeit belegen, dass Ihr ISMS funktioniert und regelmäßig überprüft wird.

SCHULUNG UND AWARENESS FÖRDERN

Technische Sicherheit ist nur ein Teil der Lösung. Schulen Sie Mitarbeitende regelmäßig, um das Bewusstsein für Informationssicherheit zu stärken – von der Passwortpolitik bis zum Umgang mit sensiblen Daten. Ein hohes Sicherheitsbewusstsein senkt Risiken und stärkt die Sicherheitskultur im Unternehmen.

09

10

INTERNE AUDITS UND KONTINUIERLICHE VERBESSERUNG

Ein ISMS ist kein Projekt mit Enddatum, sondern ein fortlaufender Prozess. Interne Audits und Managementbewertungen zeigen, wo Prozesse funktionieren und wo Verbesserungsbedarf besteht.
So entwickeln Sie Ihr System kontinuierlich weiter und bleiben langfristig auditfähig.

Wichtige Unterlagen für Ihre **ISO 27001-Zertifizierung**

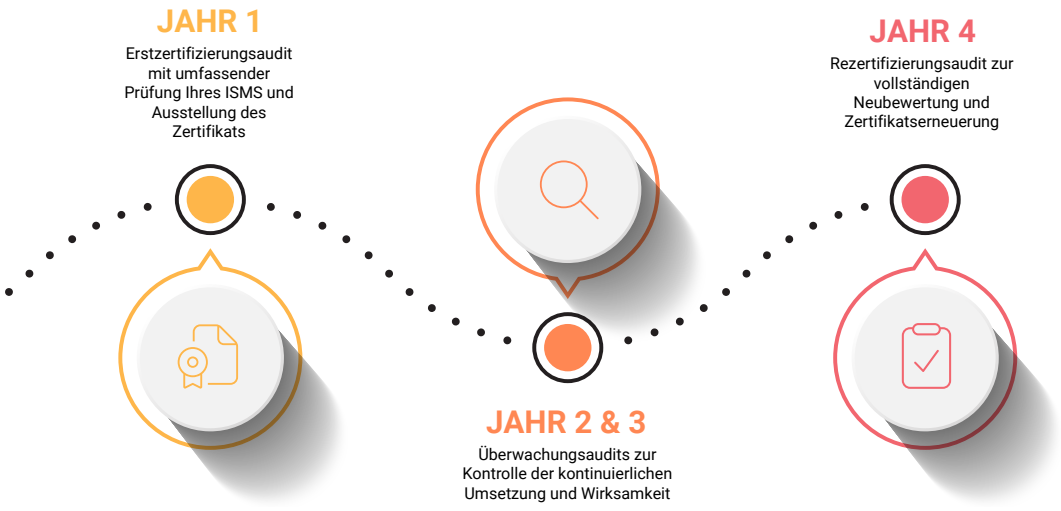
Damit Ihr Zertifizierungsaudit reibungslos verläuft, sollten Sie folgende Nachweise bereithalten:

- Informationssicherheitsleitlinie
- ISMS-Handbuch und SoA (Statement of Applicability)
- Risikoanalyse und Risikobehandlungsplan
- Sicherheitsrichtlinien und Prozessbeschreibungen
- Schulungs- und Awareness-Nachweise
- Interne Audits und Managementbewertungen

Eine vollständige und gepflegte Dokumentation ist der Schlüssel für eine erfolgreiche Auditierung. Interesse an einer Beratung dazu? Das Expertenteam der bbg bitbase group unterstützt Unternehmen beim gesamten Prozess bis zum zertifizierten ISMS.

Zertifizierungszyklus verstehen

Die ISO 27001-Zertifizierung erfolgt in einem dreijährigen Zyklus:



Regelmäßige Audits fördern die Stabilität des Systems und sichern langfristig Ihre Compliance.

Fazit –Checkliste abhaken, Zertifizierung sichern

Informationssicherheit ist kein einmaliges Projekt, sondern ein fortlaufender Managementprozess.
Mit einer strukturierten Vorgehensweise nach ISO 27001 schaffen Sie die Grundlage für Vertrauen, Resilienz und Wettbewerbsfähigkeit. Dass der Standard längst etabliert ist, zeigt auch der Blick auf die Zahlen: Weltweit sind heute **mehr als 50.000 Unternehmen** nach ISO 27001 zertifiziert, in Deutschland **rund 13.000** – Tendenz steigend. Damit gehört Deutschland zu den führenden europäischen Ländern bei der Umsetzung eines zertifizierten Informationssicherheitsmanagementsystems.

Diese Checkliste unterstützt Sie dabei, Ihr ISMS Schritt für Schritt aufzubauen, Zuständigkeiten zu klären und die Zertifizierung gezielt vorzubereiten – effizient, nachvollziehbar und auditfähig.

Quellen: (ISO Survey 2024 / Deura InfoSec 2024)

Konnten wir Ihr Interesse wecken?

Sprechen Sie uns an.

Gerne beraten wir Sie rund um die Themen ISO 27001, Informationssicherheitsmanagement (ISMS) und Compliance. Ob Einführung, Audit-Vorbereitung oder Zertifizierung – unsere Expertinnen und Experten begleiten Sie Schritt für Schritt auf dem Weg zu einem sicheren und auditfähigen Managementsystem.
Alle unsere Beraterinnen und Berater verfügen über fundiertes Know-how in den Bereichen IT-Sicherheit, Governance, Risk & Compliance sowie langjährige Erfahrung in der praktischen Umsetzung von ISMS-Projekten in Unternehmen aller Größen.

José Enrique Gómez Asbeck
Managing Director
bbg bitbase group GmbH

Markus Vatter
Head of Compliance
bbg bitbase group GmbH

bitbase group

ISO 27001 CHECKLISTE

Weiterführende Links

- Unsere Compliance-Services im Überblick
- Interessantes zum Thema NIS2 und Cybersicherheit
- Unser Webinarkanal
- Beratungstermin direkt buchen

bbg bitbase group GmbH

Am Heilbrunnen 47
D-72766 Reutlingen

T. +49 (0) 7121 68 08 49-0
F. +49 (0) 7121 68 08 49-99
mail@bitbasegroup.com
www.bitbasegroup.com