

# ISO 27001

## PREISINFORMATIONEN ZUR GRUPPENZERTIFIZIERUNG FÜR MITGLIEDER IM BUNDESVERBAND IT-MITTELSTAND E.V.

Preisstruktur der ISO 27001-Gruppenzertifizierung | Stand: Juli 2024

## Erfolgsfaktor Qualitätsmanagement

Die Norm ISO 27001 beschreibt einen Risikomanagementprozess, an dem Personen, Prozesse und IT-Systeme beteiligt sind und bietet einen ganzheitlichen Ansatz für die Informationssicherheit. Unsere ISO 27001 Gruppenzertifizierung ist speziell für die Anforderungen kleiner und mittlerer IT-Unternehmen konzipiert und bietet Preisvorteile gegenüber einer Einzelzertifizierung. Eine gemeinsame Zertifizierung in der Gruppe ermöglicht es den beteiligten Unternehmen zudem, die Vorteile von QM unter Einhaltung des ISO 27001 Standards zu realisieren, ohne das operative Geschäft zu behindern.

## Zertifizierung im Gruppenverfahren



### Voraussetzungen:

- Mitgliedschaft im Bundesverband IT-Mittelstand e.V. (BITMi)
- vorhandene ISO 9001 (falls nicht vorhanden, kann diese im Zuge der ISO 27001 zu einem Sonderpreis von 4.500 Euro bei einer 3-jährigen Betreuung durchgeführt werden)
- ein Standort in der BRD
- maximal 100 Mitarbeiter



### Beratung durch EuroConsult:

- 20.000 Euro für 3 Jahre
- 1.200 Euro je weiteren Standort für 3 Jahre
- 2.000 Euro / Jahr ab dem 4. Jahr
- 399 Euro / Jahr EASY-QM-Plattform, falls nicht vorhanden
- 180 Euro / Jahr QS-Pool Mitgliedschaft, um an der Gruppenzertifizierung teilnehmen zu können
- 175 Euro / Jahr Reisekostenanteil



### Zertifizierung durch ISOCERT®:

- 2.500 Euro / Jahr bei bis zu 50 Mitarbeiter
- 2.750 Euro / Jahr bei bis zu 99 Mitarbeiter
- 3.000 Euro / Jahr ab 100 Mitarbeiter
- zuzüglich 225 Euro Reisekostenanteil bei Audit vor Ort
- zuzüglich 150 Euro Zertifikatsgebühren, alle 3 Jahre
- zuzüglich 75 Euro je weiterer Standort auf dem Zertifikat



KONTAKT, FRAGEN & ANMELDUNG:

[kontakt@bitmi.de](mailto:kontakt@bitmi.de)

[www.bitmi.de](http://www.bitmi.de)



- In einem **Kombizertifizierungsverfahren** ISO 9001/ISO 27001 reduziert sich der Zertifizierungspreis um 300 Euro.
- Sämtliche **Preise** verstehen sich zzgl. der gesetzlichen Mehrwertsteuer und haben vorerst eine Gültigkeit bei einem **Vertragsabschluss bis 31.12.2024**.
- **Zuschuss:** QS-Pool-Mitglieder können über die „QM-Initiative 2025“ einen Antrag stellen und ohne großen Aufwand einen Zuschuss von 1.250 Euro je Norm erhalten.
- **Projektlaufzeit**
  - a) Einführung und Umsetzung inkl. Zertifizierung ca. 6 - 12 Monate
  - b) Projektlaufzeit zunächst 3 Jahre

## NIS-2 Ergänzung zur ISO 27001

NIS-2 ist für Unternehmen **ab 50 Mitarbeiter** oder 10 Mio. Euro Jahresumsatz **ab Oktober 2024** erforderlich und kommt man diesen Auflagen nicht nach, drohen Geldstrafen. Diese NIS-2 Vorgaben verpflichten die Unternehmen zur Stärkung der Cybersicherheit und zu mehr Kommunikation mit den nationalen Aufsichtsbehörden – in Deutschland ist das das Bundesamt für Sicherheit in der Informationstechnik (BSI).



### Die wichtigsten Maßnahmen sind:

- Es müssen Prozesse für Risikoanalyse und -management, Informationssicherheit und die Bewältigung von Cyber-Vorfällen festgelegt werden. Diese orientieren sich an den Kriterien der ISO 27001 für ein ISMS.
- Für die Bewältigung eines Notfalls müssen Business Continuity- und Wiederherstellungspläne vorliegen.
- Erhebliche Vorfälle müssen innerhalb sehr kurzer Fristen – in manchen Fällen 24 Stunden – an das BSI gemeldet werden.
- Der Einsatz von Verschlüsselungstechnik und Multi-Faktor-Authentifizierung ist unternehmensweit gefordert.
- Regelmäßige Schulungen des gesamten Personals, die über Verhaltensregeln zur Informationssicherheit und Veränderungen in der Risikolandschaft aufklären, müssen dem BSI nachgewiesen werden.

ISO 27001 bestätigt den Unternehmen, dass sie die NIS-2 Anforderungen bereits zu 70 % erfüllen. Die Anforderungen der NIS-2 können in die ISO 27001 mit einem zusätzlichen Beratungsaufwand, falls gewünscht, von ca. 8.500 Euro mit integriert werden. Mit einem Kostenfaktor von 250 Euro könnte auf dem ISO27001-Zertifikat im Geltungsbereich mit aufgenommen werden, dass die NIS-2 Anforderungen erfüllt werden.

Alle genannten Preisangaben sind ohne Gewähr.



## Mitgliedschaft im Bundesverband IT-Mittelstand e.V.



Die Mitgliedschaft im BITMi ist obligatorisch für die Teilnahme an der ISO 27001 Gruppenzertifizierung. Ist das Unternehmen noch nicht Mitglied im BITMi, kommen deswegen die Kosten der Mitgliedschaft hinzu. Diese setzen sich zusammen aus dem jährlichen Mitgliedsbeitrag und einer einmaligen Aufnahmegebühr in Höhe eines jährlichen Mitgliedsbeitrags. Im ersten Jahr erfolgt die Berechnung des jährlichen Mitgliedsbeitrags ggf. unterjährig. Die grundsätzlichen Möglichkeiten einer Mitgliedschaft ergeben sich gemäß § 5 der Satzung des BITMi. Die vorliegende Beitragsordnung betrifft die Ordentliche Mitgliedschaft und die Fördermitgliedschaft als natürliche oder juristische Person.

Die Höhe des Mitgliedsbeitrags im BITMi richtet sich gemäß der Beitragsordnung nach der **Anzahl der beschäftigten Mitarbeiter**.



Beitragsgruppe	Mitarbeiter	Beitrag
A	1	250 EUR
B	2 – 5	490 EUR
C	6 – 20	750 EUR
D	21 – 50	1.250 EUR
E	51 – 100	2.500 EUR
F	101 – 1000	3.500 EUR

## Mitmachen. Vernetzen. Gestalten

**MITGLIED WERDEN  
UND QUALITÄT  
SICHTBAR MACHEN!**

### Profitieren Sie von zahlreichen BITMi-Vorteilen:

- Erhalt der Siegel *Software Made in Germany* / *Software Hosted in Germany* soweit die Voraussetzungen erfüllt sind
- Sichtbarmachen Ihrer Themen in der Politik
- Gemeinschaftsstände und Speakerslots auf Messen
- Veranstaltungen, Meet-Ups zum Netzwerken und Wissenstransfer
- Austausch zu relevanten Themen in aktuell acht Fachgruppen
- Mitwirken in nationalen und internationalen Forschungs- und Entwicklungsprojekten
- Platzierung in unseren Newslettern, auf Social-Media-Kanälen sowie in Presseartikeln unserer Medienpartnern



KONTAKT, FRAGEN & ANMELDUNG:

[kontakt@bitmi.de](mailto:kontakt@bitmi.de)

[www.bitmi.de](http://www.bitmi.de)