

# FAQ – Häufig gestellte Fragen zur KRITIS-Prüfung



Sie möchten Ihr Unternehmen vor IT-Ausfällen und unberechtigten IT-Zugriffen schützen und alle Vorgaben gemäß der BSI-Kritisverordnung erfüllen. Aus diesem Grund möchten Sie gern mehr zur **KRITIS-Prüfung** erfahren. Nachfolgend haben wir die häufigsten Fragen und Antworten zum Thema für Sie zusammengefasst.

## 1. Was ist KRITIS?

Basierend auf dem IT-Sicherheitsgesetz (IT-SiG) von 2015 ergänzte das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Verordnung zu den Kritischen Infrastrukturen (KRITIS). Darin wurde festgelegt, dass KRITIS-Betreiber sowohl IT-Systeme als auch KRITIS-Kernkomponenten angemessen zu schützen haben.

Da es bei Störungen und Totalausfällen von KRITIS-Unternehmen zu Versorgungsengpässen und Gefahren für die Sicherheit der Bevölkerung kommen kann, müssen diese höhere gesetzliche Auflagen erfüllen als andere Unternehmen.

## 2. Welche Sektoren sind von der Kritisverordnung betroffen?

Folgende Sektoren werden gemäß der aktuellen Gesetzeslage als kritische Infrastrukturen eingestuft:

- Energie
- IT und Telekommunikation
- Ernährung
- Wasser / Abwasser
- Transport und Verkehr
- Gesundheit
- Finanz- und Versicherungswesen

## 3. Welches Ziel verfolgt die KRITIS-Prüfung?

Mit einer erfolgreich bestandenem KRITIS-Prüfung bestätigen wir Ihnen als unabhängige Prüfstelle, dass Ihr Unternehmen den aktuellen Sicherheitsstandards entsprechend Ihrer Vorgaben entspricht. In diesem Rahmen prüfen wir im Vorfeld mit Ihnen gemeinsam, ob Ihre Prüfziele den derzeitigen Anforderungen des BSI entsprechen.

#### 4. KRITIS-Unternehmen sollen den „Stand der Technik“ einhalten. Was ist damit gemeint und wer legt den aktuellen Stand fest?

Der sogenannte „Stand der Technik“ meint, dass innerhalb eines Unternehmens alle Maßnahmen zum Schutz der IT-Systeme, Komponenten und Prozesse den fortschrittlichsten Verfahren, Ausstattungen und Betriebsweisen entsprechen müssen. Hierbei ist zu beachten, dass der jeweilige aktuelle Stand den entsprechenden nationalen, internationalen und europäischen Normen und Standards entspricht und erfolgreich in der Praxis erprobt wurde.

Konkrete Vorgaben und Leitfäden hierzu werden durch die jeweiligen Branchen im Rahmen der B3S – branchenspezifische Sicherheitsstandards – oder durch das BIS selbst vorgeschlagen veröffentlicht.

#### 5. Welche Vorteile bringt die KRITIS-Prüfung durch DEKRA meinem Unternehmen?

Aufgrund unserer branchenübergreifenden Erfahrung und unseres Expertennetzwerkes bieten wir Ihnen folgende Vorteile:

- **Kosten und Zeitersparnis durch Vermeidung von Mehrfachprüfungen**
- **Verhinderung von Lücken und Mängel der angegebenen Prüfvorgaben**
- **BSI-konformer Nachweis über die Erfüllung der Anforderungen gemäß des IT-Sicherheitsgesetzes**
- **Vermeidung von Bußgeldern durch eventuelle Verstöße**

#### 6. Mein Unternehmen verfügt bereits über eine ISO 27001 Zertifizierung. Ist diese ausreichend?

Nein. Die ISO 27001 Zertifizierung kann lediglich als Grundlage für den Nachweis gemäß §8a BSIG verwendet werden. Sie erfasst nicht automatisch den gesamten

relevanten Geltungsbereich (Scope) und deren zugehörige Umsetzungsmaßnahmen, die für den Nachweis notwendig sind. Es besteht hierbei das Risiko, dass relevante Schutzziele kritischer Infrastrukturen nicht ausreichend oder gar nicht erfasst werden.

Gern unterstützen wir Sie bei Ihrer KRITIS-Prüfung auf Basis einer vorhandenen ISO 27001 Zertifizierung durch unsere Erfahrung mit Prüfungsgrundlagen in Ihrem spezifischen Sektor und dem BSI.

#### 7. Wie ist der konkrete Ablauf einer KRITIS-Prüfung?

Die Prüfung wird in folgenden Schritten durch unsere Experten durchgeführt:

1. **Prüfungsvorbereitung, inklusive der Wahl der Prüfungsgrundlage sowie der Prüfung des Geltungsbereichs**
2. **Erstellung des Prüfplans**
3. **Dokumentationsprüfung**
4. **Vor-Ort-Prüfung**
5. **Nachbereitung der Vor-Ort-Prüfung**
6. **Erstellung des Prüfberichts**

#### 8. Wie lange ist mein Prüfbericht gültig?

Der KRITIS-Prüfbericht ist zwei Jahre gültig und erfordert vor Ablauf von zwei Jahren eine erneute Überprüfung der IT-Sicherheit kritischer Komponenten und Systeme Ihres Unternehmens.

**Sie haben weitere Fragen zur KRITIS-Prüfung? Sprechen Sie unsere Experten noch heute an!**

### Weitere Leistungen, von denen Sie profitieren

Sie haben ebenfalls die Möglichkeit, weitere Zertifizierungen durch unsere erfahrenen Experten durchführen zu lassen, wie z.B. nach **ISO 27001**, **ISO 22301** und **ISO 9001** sowie deren Kombinationen. Über 40 Akkreditierungen beinhaltet unser Portfolio! Darüber hinaus bietet Ihnen die DEKRA Gruppe rund um das Thema Sicherheit:

- **Bewertungen zur Einhaltung eigener Regeln**
- **Trainings und Schulungen**
- **Personen-Zertifizierungen**
- **Produktprüfungen und Zertifizierungen**

### Ausgezeichnet – das DEKRA Siegel



Setzen Sie ein Ausrufezeichen für höchste Qualität und Zuverlässigkeit – branchenübergreifend und international. Das **DEKRA Siegel** leistet beste Dienste als Imageträger, Marketinginstrument und um sich vom Wettbewerb abzuheben. So zeigen Sie Ihren Kunden und Geschäftspartnern, dass Leistung bei Ihnen ihr Geld wert ist. Wir unterstützen Sie gerne dabei.

DEKRA Certification GmbH  
Handwerkstraße 15  
70565 Stuttgart  
Telefon +49.711.7861-2566  
Telefax +49.711.7861-2615  
Mail [certification.de@dekra.com](mailto:certification.de@dekra.com)  
Web [www.dekra.de/audit/](http://www.dekra.de/audit/)