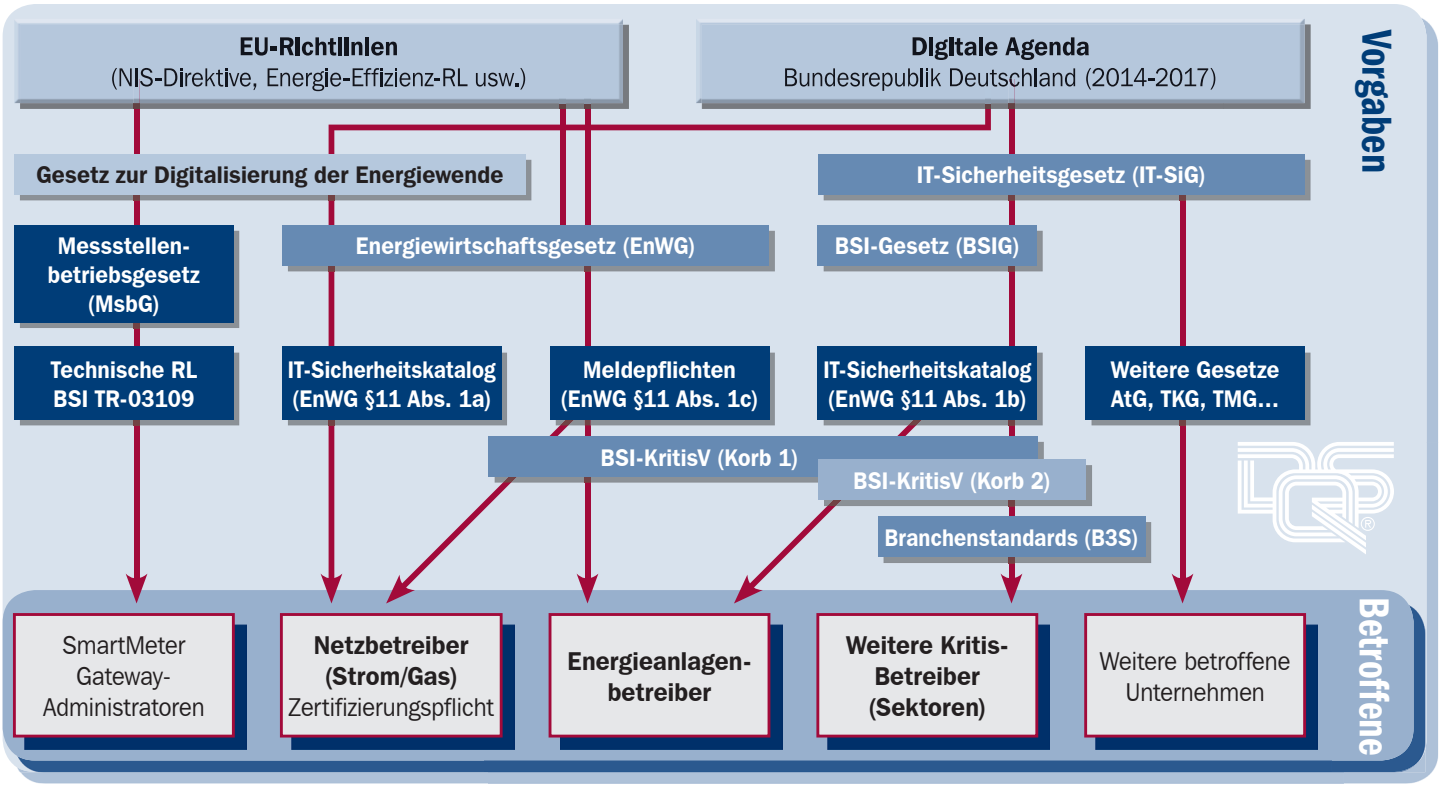
THE AUDIT COMPANY

## KRITIS – Kritische Infrastrukturen

# IT-Sicherheitsgesetz und BSI-KritisV gemäß §8a BSIG




*Gesetzliche Grundlagen*

Das Bedrohungspotenzial aus dem Cyberraum ist beträchtlich. Besonders anfällig sind so genannte **Kritische Infrastrukturen (KRITIS)**. Hier hätte ein Ausfall oder eine Beeinträchtigung der Versorgungsdienstleistungen dramatische Folgen für Wirtschaft, Staat und Gesellschaft.

Als wichtigste Grundlage zu Ihrem Schutz gilt das IT-Sicherheitsgesetz*, das zum 25. Juli 2015 in Kraft getreten ist. Mit diesem Gesetz wird u. a. das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik **(BSI-Gesetz/BSIG)** ergänzt.

Zur Umsetzung des IT-Sicherheitsgesetzes ist am 3. Mai 2016 der erste Teil der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (**BSI-Kritisverordnung – BSI-KritisV**) in Kraft getreten, der Organisationen aus den Sektoren **Energie, Wasser, Informationstechnik und Telekommunikation** sowie **Ernährung** betrifft. Mit der seit 30. Juni 2017 vorliegenden **Änderungsverordnung BSI-KritisV** wird die Vorgabe des § 10 BSIG abschließend umgesetzt. Sie bestimmt die Schwellenwerte für die Sektoren aus Korb 2: **Gesundheit, Finanz- und Versicherungswesen** sowie **Transport und Verkehr**. Zudem wurden erforderliche Ergänzungen und Klarstellungen für die bereits aus dem 1 Korb verabschiedeten Sektoren und Schwellenwerte vorgenommen. Damit liegen für sieben der neun KRITIS-Sektoren verbindliche Schwellenwerte vor, ab denen Einrichtungen und Anlagen in Deutschland als Kritische Infrastruktur gelten und besonders schützenswert sind.

** IT-SiG: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*


**DQS GmbH**
Deutsche Gesellschaft zur Zertifizierung von Managementsystemen
August-Schanz-Straße 21
60433 Frankfurt am Main
Tel. +49 69 95427-0
info@dqs.de
**www.dqs.de**

THE AUDIT COMPANY

Nach **§ 8a BSIG** müssen Betreiber Kritischer Infrastrukturen zum Schutz ihrer IT-Systeme, -Komponenten und -Prozesse Sicherheitsstandards nach dem **Stand der Technik** einführen, um durch angemessene Schutzmaßnahmen unempfindlich gegenüber Störungen der Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität zu sein. Ergänzend müssen dem BSI eine Kontaktstelle benannt und erhebliche IT-Sicherheitsvorfälle gemeldet werden **(§ 8b)**, sofern diese Auswirkungen auf die Verfügbarkeit kritischer Dienstleistungen haben.

Betroffene Betreiber haben zwei Jahre Zeit, die vom BSIG definierten Anforderungen zu erfüllen und ihrer Nachweispflicht gegenüber dem BSI nachzukommen. Stichtag für die Umsetzung aus Korb 2 ist der **30. Juni 2019**. Bei Nichterfüllung sind Bußgelder bis zu einer Höhe von 100.000 Euro für das verantwortliche Management möglich.

## Nachweis gemäß § 8a BSIG

Entsprechende Umsetzungsnachweise können durch **Sicherheitsaudits**, **Prüfungen** oder **Zertifizierungen** erfolgen. Dafür sind internationale Normen und Standards oder alternativ „**B**ranchen**s**pezifische **S**icherheits**s**tandards“ (**B3S**) zugelassen. Es ist davon auszugehen, dass sich betroffene Betreiber nach den entsprechenden Branchenstandards prüfen lassen, sofern diese vorliegen. Anderenfalls kann ein Informationssicherheits-Managementsystem nach **ISO 27001** ein geeigneter **Lösungsansatz** sein, um die gesetzlichen IT-Sicherheitsanforderungen in zuverlässige und sichere Prozesse zu integrieren. Eine reine ISO 27001-Zertifizierung ist allerdings nicht ausreichend, da hierbei die branchenspezifischen Anforderungen fehlen.

## Sektor Energie: Informationssicherheit für Netzbetreiber

Um die Sicherheit informationstechnischer Systeme im Sektor Energie zu erhöhen, veröffentlichte die Bundesnetzagentur (BNetzA) 2015 den IT-Sicherheitskatalog. Dieser fordert gemäß § 11 Abs. 1a Energiewirtschaftsgesetz (EnWG) von Energienetzbetreibern grundsätzlich die Umsetzung eines vollumfänglichen Informationssicherheits-Managementsystems (ISMS) gemäß ISO 27001. Die Anforderungen an das ISMS werden durch die des IT-Sicherheitskatalogs erweitert. Hinzu kommen Anforderungen aus dem Leitfaden ISO/IEC TR 27019, die sich auf spezifische Besonderheiten des Energiesektors beziehen. Das ISMS ist vom Netzbetreiber einzuführen und durch eine DAkkS akkreditierte Zertifizierungsstelle wie der DQS zertifizieren zu lassen.

## Kritische Infrastrukturen nach Sektoren und Fristen

| Sektoren | Bereiche | BSI-KritisV | Frist* gemäß BSI-KritisV |
|---|---|---|---|
| **Energie** | Elektrizität, Gas, Mineralöl | Teil I vom 3. Mai 2016 | Mai 2018 |
| **Informationstechnik und Telekommunikation** | Informationstechnik und Telekommunikation | Teil I vom 3. Mai 2016 | Mai 2018 |
| **Wasser** | öffentliche Wasserversorgung, öffentliche Abwasserbeseitigung | Teil I vom 3. Mai 2016 | Mai 2018 |
| **Ernährung** | Ernährungswirtschaft, Lebensmittelhandel | Teil I vom 3. Mai 2016 | Mai 2018 |
| **Finanz- und Versicherungswesen** | Banken, Börsen, Versicherungen, Finanzdienstleister | Änderungsverordnung vom 30. Juni 2017 | Juni 2019 |
| **Gesundheit** | medizinische Versorgung, Arzneimittel und Impfstoffe, Labore | Änderungsverordnung vom 30. Juni 2017 | Juni 2019 |
| **Transport und Verkehr** | Luftfahrt, See- und Binnenschifffahrt, Straßen- und Schienenverkehr, Logistik | Änderungsverordnung vom 30. Juni 2017 | Juni 2019 |
| **Staat und Verwaltung** | Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall-/Rettungswesen inkl. Katastrophenschutz | | |
| **Medien und Kultur** | Rundfunk, gedruckte / elektronische Presse, Kulturgut, symbolträchtige Bauwerke | | |

*Quelle: www.bsi.de*

* *Betroffene Unternehmen müssen zwei Jahre nach Veröffentlichung der BSI-KritisV (Korb 1 und Korb 2) nachweisen, dass sie ihre IT angemessen nach dem Stand der Technik abgesichert haben.*

THE AUDIT COMPANY

## Bei der DQS in guten Händen

Für die „prüfende Stelle“ und deren Auditoren empfiehlt das BSI eine sogenannte **„Spezielle Prüfverfahrenskompetenz für § 8a BSIG“** als Qualifikationsnachweis. Die DQS ist anerkannte Prüfstelle und akkreditierte Zertifizierungsstelle, u. a. für ISO 27001. Gerne stellen wir Ihnen alle geforderten Kompetenzen für eine BSI-konforme Prüfung gemäß § 8a BSIG zur Verfügung:

- spezielle Prüfverfahrenskompetenz
- Auditkompetenz
- IT-Sicherheitskompetenz
- Branchenkompetenz

Der Ablauf der KRITIS-Prüfung basiert auf der BSI-Orientierungshilfe zu Nachweisen gemäß § 8a BSIG. Unser Angebot wird entsprechend diesen Vorgaben aufgebaut und mit Auditaufwänden versehen. Aufgrund unserer Erfahrungen bieten wir Ihnen eine **KRITIS-Prüfung** im Rahmen eines **zweistufigen Verfahrens**.

In Stufe 1 erfolgen insbesondere die Prüfung der Eignung des Scopes sowie die Abstimmung und Erstellung des Prüfplans. Die weiteren Prüfschritte erfolgen in der Stufe 2. Nach der Prüfung erhalten Sie die entsprechenden **BSI-Nachweise**. Bei Interesse verknüpfen wir die KRITIS-Prüfung mit einer Zertifizierung gemäß ISO 27001. In diesem Fall erhalten Sie zusätzlich ein weltweit anerkanntes **DQS-Zertifikat**.

## Schritte einer KRITIS-Prüfung


*Orientierung zum relativen Zeitaufwand einer BSI-konformen Prüfung gemäß § 8a (3) BSIG, Quelle: BSI, www.bsi.de*

## Ihr Vorteil

- BSI-konformer Nachweis über die Erfüllung der Anforderungen aus dem IT-Sicherheitsgesetz
- erhöhte Sicherheit Ihrer IT-Systeme, -Prozesse und -Komponenten durch branchenspezifische Absicherung nach dem Stand der Technik
- verbesserte Versorgungssicherheit Ihrer kritischen Dienstleistung
- gute Verknüpfungsmöglichkeit mit einer Zertifizierung nach ISO 27001 und dem damit verbundenen, international anerkannten DQS-Zertifikat

KRITIS in zwei Minuten.
Der DQS-Videoclip unter www.dqs.de

Sprechen Sie mit uns.
Wir stehen Ihnen gern zur Verfügung.

André Säckel
DQS Produktmanager
informationssicherheit@dqs.de

THE AUDIT COMPANY

# BSI-KritisV – Schwellenwerte

**Betreiber Kritischer Infrastrukturen können anhand der festgelegten Schwellenwerte prüfen, ob sie unter die Regelungen des IT-Sicherheitsgesetzes fallen und somit von der Umsetzung betroffen sind.**

## *Korb 1*
### *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz vom 22. April 2016*

#### *Sektor Energie*
- *Stromerzeugung: > 420 MW installierte Netto-Nennleistung/Jahr*
- *Stromübertragung: > 3.700 GWh/Jahr*
- *Gasversorgung: > 5.190 GWh/Jahr*
- *Rohölförderung und Transport: > 4,4 Mio. Tonnen/Jahr*
- *Fernwärmeerzeugung: > 2.300 GWh ausgeleitete Wärmeenergie/Jahr*

#### *Sektor Wasser*
- *Trinkwasserversorgung: > 22 Mio. m³ Wasser/Jahr*
- *Abwasserbeseitigung: > 500.000 angeschlossene Einwohner/Jahr*

#### *Sektor Ernährung*
- *Lebensmittelversorgung: > 434.500 t Speisen oder 350 Mio. l Getränke/Jahr*

#### *Sektor Informationstechnik und Telekommunikation*
- *Sprach- und Datenvermittlung: > 300 angeschlossene Systeme/Jahr*
- *Sprach- und Datensteuerung: > 2.5 Mio. abgefragte IP-Adressen pro Tag (Jahresdurchschnitt)*
- *Rechenzentrum: > 5 MW vertraglich vereinbarter Leistung am 30. Juni eines Kalenderjahres)*

## *Korb 2*
### *Erste Verordnung zur Änderung der BSI-KritisV vom 21. Juni 2017*

#### *Sektor Finanz- und Versicherungswesen*
- *Autorisierungssysteme für Bargeldabhebungen und Systeme zur Anbindung an ein Autorisierungssystem: > 15 Mio. Transaktionen/Jahr*
- *Clearing- und Settlement-Systeme: > 18 Mio. Transaktionen/Jahr*
- *Kontoführungssysteme: > 15 Mio. Transaktionen/Jahr*
- *Cash-Center und Systeme zur Bargeldlogistik: > 93,5 Mio. Banknoten/Jahr*
- *Kartengestützter Zahlungsverkehr: > 21 Mio. Transaktionen/Jahr*
- *Konventioneller Zahlungsverkehr: > 100 Mio. dienstleistungsbezogene Transaktionen/Jahr*
- *Systeme zur Verrechnung und Abwicklung von Wertpapier- und Derivat-Geschäften: > 850.000 Transaktionen/Jahr*
- *Systeme in Verbindung mit Lebensversicherungen: > 500.000 Leistungsfälle/Jahr*
- *Systeme in Verbindung mit privaten Krankenversicherungen: > 2 Mio. Leistungsfälle/Jahr*
- *Systeme in Verbindung mit gesetzlichen Krankenversicherungen: > 3 Mio. Leistungsfälle/Jahr*

#### *Sektor Transport/Verkehr*
- *Abfertigungsanlagen und Flughäfen: > 20 Mio. Passagiere/Jahr bzw. 750.000 t Fracht/Jahr*
- *Flugsicherung und Luftverkehrskontrolle: > 17.500 Flugbewegungen/Jahr*
- *Güter- und Zugbildungsbahnhöfe: > 23.000 Züge/Jahr*
- *Schienennetze, Stellwerke und Leitzentralen im ÖSPNV: > 125 Mio. beförderte Personen/Jahr oder > 500.000 Einwohner in der überwachten Region*
- *Logistikzentren und Umschlaganlagen: > 17 Mio. t Güter/Jahr*

#### *Sektor Gesundheit*
- *Krankenhäuser: > 30.000 stationäre Patienten/Jahr*
- *Medizinprodukte (Produktionsstätten/Abgabestellen): > 90,68 Mio. Euro Umsatz/Jahr*
- *Produktionsstätten, Betriebs-/Lagerräume, Vertriebsanlagen für verschreibungspflichtige Arzneien und Apotheken: > 4,65 Mio. Packungen/Jahr*
- *Labore, Transport- und Kommunikationssysteme zur Auftrags-/Befundübermittlung: > 1,5 Mio. Aufträge/Jahr*
- *Blutspende-Einrichtungen: > 34.000 Produkte/Jahr*

informationssicherheit@dqs.de