

## Nutzen Sie die Erfahrung der EnBW AG.

Als Betreiber von Energieerzeugungsanlagen und Netzen hat die EnBW schnell auf die Herausforderungen reagiert, die Digitalisierung und Vernetzung mit sich bringen. Unsere Kernkraftanlagen unterstehen den höchsten Sicherheitsauflagen, auch im IT-Bereich. Die EnBW ist der erste Kernkraftwerksbetreiber Deutschlands, der das IT-Sicherheitsgesetz erfolgreich umgesetzt hat.

## Ihre IT. Sicherer. Machen.

Unser Ziel ist, die IT Ihres Unternehmens sicherer zu machen. Vertrauen Sie auf die EnBW-Kompetenz.

## Branchen im Fokus

Im Fokus unserer Unterstützung stehen Branchen, die als kritische Infrastruktur klassifiziert sind. In den Geschäftsfeldern Energie, Gesundheit und Wasser ist die EnBW selbst schon seit Jahren aktiv, daher konzentrieren wir uns vor allem auf diese Branchen.



Sie können einzelne Leistungen oder alle Services von uns aus einer Hand wählen

- › Unterstützung zur Compliance-Erreichung
- › Audits und Zertifizierung
- › IT-Security-Beratung
- › IT-Betrieb

Mehr Information unter:  
[enbw.com/kritis](http://enbw.com/kritis)

Ihre Daten und Informationen werden natürlich vertraulich behandelt und nicht an Dritte weitergegeben oder für andere Zwecke verwendet.

EnBW Energie Baden-Württemberg AG

Durlacher Allee 93  
76131 Karlsruhe

[kritis@enbw.com](mailto:kritis@enbw.com)



› [enbw.com/kritis](http://enbw.com/kritis)

# Der EnBW Full Kritis Service >



IT.Sicherer.Machen.

— EnBW



Mit der fortschreitenden Digitalisierung und Vernetzung steigt das Risiko für Cyber-Angriffe.

Die Manipulationen führen zu Schäden, die für Unternehmen schwerwiegend bis existenzbedrohend sein können, und die Angriffe nehmen in Anzahl und Intensität zu: Das WannaCry-Virus infizierte im Mai 2017 über 200.000 Systeme in 150 Ländern.

Die Bundesregierung hat mit dem seit Juli 2015 gültigen IT-Sicherheitsgesetz reagiert.

Die BSI-KritisV („Verordnung zur Bestimmung Kritischer Infrastruktur“) regelt, welche Unternehmen die Anforderungen des Gesetzes bis Ende des Jahres 2018 umsetzen müssen. Im Fokus stehen alle Branchen, bei denen Ausfälle der Versorgungsdienstleistung dramatische Folgen für Wirtschaft, Staat und Gesellschaft hätten.

Ist Ihr Unternehmen von den im IT-Sicherheitsgesetz beschlossenen Regelungen betroffen? Mit uns als Partner erreichen Sie Ihre Ziele hinsichtlich IT-Security-Compliance.

- › IT-Sicherheit (IT-SiG)
- › Datenschutz (EU-DSGVO)
- › Umsetzung nach ISO 27001 oder branchenspezifischen IT-Sicherheitsstandards
- › Cybersecurity (in Anlehnung an BSI-Empfehlungen)
- › Organisations- und Prozesssicherheit

Unser Ansatz ist ganzheitlich und hat das Zusammenwirken von Mensch, Technik und Organisation im Blick.



## 1. Quick-Check

Analyse und Handlungsempfehlungen.

Der EnBW Quick-Check für kritische Infrastrukturen gibt Ihnen schnell einen Überblick über den aktuellen IT-Sicherheitsstatus, über Schwachstellen und Handlungsbedarfe in Ihrem Unternehmen. Dabei beraten wir Sie gerne auch zu unseren Produkten wie z. B. IT-Security, Leistungen unserer Rechenzentren oder die Optimierung Ihres IT-Sourcings.

Innerhalb von 48 Stunden nach Abschluss der Analyse erhalten Sie einen elektronischen Bericht. Der erste Baustein auf dem Weg zur vollständigen IT-Security-Compliance Ihres Unternehmens.



## 2. Konformitätsanalyse

Konformitätsprüfung & Gap-Analyse, detaillierter Bericht über Ihren Status-Quo und Roadmap für Ihre Zielerreichung.

Die Ergebnisse des Quick-Checks werden analysiert und die Schwachstellen und Handlungsbedarfe detailliert aufgezeigt. Sie erhalten einen Bericht über den aktuellen Status-Quo und über alle notwendigen Schritte bis zur Zielerreichung.

Auf Basis dieser Informationen können wir Ihnen ein verbindliches Angebot für die Maßnahmenumsetzung zukommen lassen.



## 3. Maßnahmenumsetzung

Planung und Herstellung Ihrer Zertifizierungsreife bis zum Abschluss der formalen Umsetzung und „Testphase“.

Gemeinsam setzen wir alle für die Normerfüllung notwendigen Maßnahmen um und etablieren dabei die entsprechenden Prozesse und Rollen sowie ein maßgeschneidertes Dokumenten-Framework. Wir übernehmen gerne das komplette Projektmanagement für Sie oder alternativ die Qualifizierung Ihrer Mitarbeiter.

Nach Abschluss der formalen Umsetzung beginnt die Testphase im Live-Betrieb. Die dabei gewonnenen Erfahrungen gehen durch unseren kontinuierlichen Verbesserungsprozess direkt in die Arbeitsergebnisse ein



## 4. Betrieb

Kritis-Compliance-Bericht und Übergang in den Betrieb.

Nach erfolgreichem Abschluss der Testphase kann im Rahmen eines externen Audits durch ein akkreditiertes Zertifizierungsunternehmen der Compliance-Nachweis erbracht werden.

Je nach Zielsetzung wird ein einreichungsfähiger Compliance-Bericht erstellt oder die offizielle Zertifizierung durchgeführt. Im Anschluss daran geht Ihr Projekt in den Betrieb über.