NIS2 UND ISO/IEC 27001 – EINE SYNERGIE FÜR CYBERSICHERHEIT

Markus Jegelka | DQS GmbH

DQS Group

Zertifizierungen aus einer Hand – national und international

- ✓ Gründung **1985** (einer der ersten Zertifizierer international)
- ✓ weltweit mehr als **2.500** qualifizierte Auditoren
- ✓ Audits und Begutachtungen nach rund **200 nationalen und internationalen** Regelwerken
- ✓ **65.000 zertifizierte Managementsysteme** in 130 Ländern
- ✓ eigener Geschäftsbereich „**Information & Data Security**“
- ✓ internationale Akkreditierungen für **ISO/IEC 27001**
- ✓ DAkkS-Akkreditierungen für **IT-SiKat 1a/1b**
- ✓ **Prüfende Stelle für § 8a BSIG** (kritische Infrastrukturen)
- ✓ unsere **TISAX®-Auditoren** sind auch für ISO/IEC 27001 berufen
- ✓ **erste** Zertifizierungsstelle, die Vehicle Cyber Security (VCS) außerhalb Europas zertifiziert hat

Unsere Zertifikate sind weltweit anerkannt – wir erbringen unsere Auditleistungen dort, wo Sie und unsere Kunden uns brauchen.

§ 30 (1) NIS2UmsuCG (RefE – 22.07.2024)

Verpflichtung zum (dokumentierten) Risikomanagement

Adressierte Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten.

Dabei sind

- ✓ das Ausmaß der Risikoexposition der Einrichtung
- ✓ die Größe der Einrichtung,
- ✓ die Eintrittswahrscheinlichkeit von Sicherheitsvorfällen,
- ✓ die Schwere von Sicherheitsvorfällen sowie
- ✓ ihre gesellschaftlichen und
- ✓ wirtschaftlichen Auswirkungen

zu berücksichtigen.

Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.

ISO/IEC 27001:2022

4.1/interne u. externe Themen

4.2/interessierte Parteien

A.5.31 Juristische, gesetzliche, regulatorische und vertragliche Anforderungen

6.1.2 Informationssicherheitsrisikobeurteilung

6.1.3 Informationssicherheitsrisikobehandlung

8.2 Informationssicherheitsrisikobeurteilung

8.3 Informationssicherheitsrisikobehandlung

§ 30 (2) NIS2UmsuCG (RefE – 22.07.2024)

(Risikomanagement-)Maßnahmen

Maßnahmen nach Absatz (1) sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz (Allgefahrenansatz) beruhen.

NIS2 *Art. 25* Normung

Um die einheitliche Anwendung des Artikels 21 Absätze 1 und 2 zu gewährleisten, fördern die Mitgliedstaaten ohne Auferlegung oder willkürliche Bevorzugung der Verwendung einer bestimmten Technologieart die Anwendung europäischer und internationaler Normen und technischer Spezifikationen für die Sicherheit von Netz- und Informationssystemen.

ISO/IEC 27001:2022

6.1.2/6.1.3 IS-Risikobeurteilung/-behandlung
8.2/8.3 IS-Risikobeurteilung/-behandlung
A.5.29 Informationssicherheit bei Störungen
A.5.30 IKT-Bereitschaft für Business-Continuity

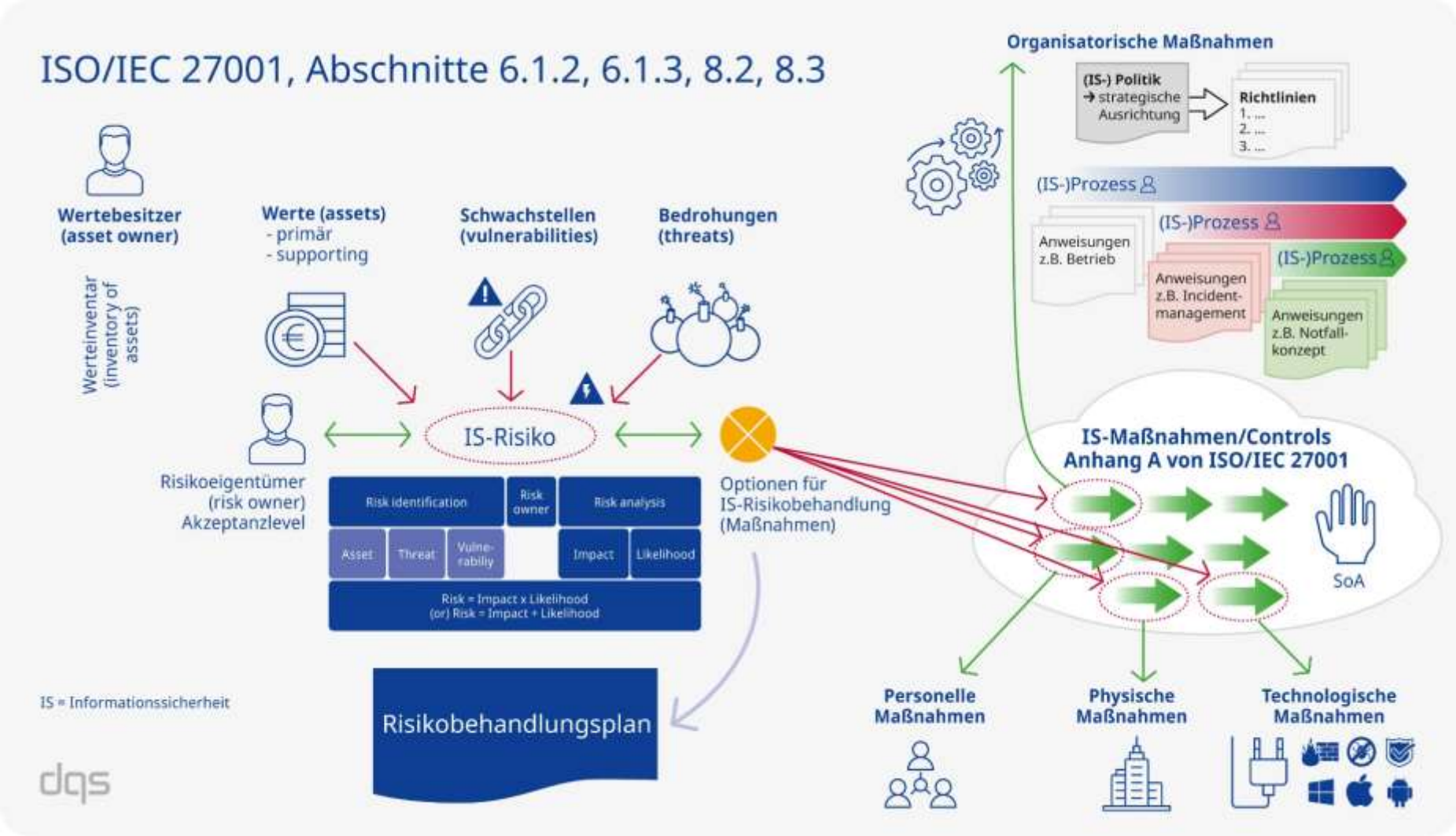
(ISO 27001 auf Basis von IT-Grundschutz)

TeleTrust „Handreichung Stand der Technik“

§ 30 (2) NIS2UmsuCG (RefE – 22.07.2024) – ISO/IEC 27001:2022

Die Maßnahmen nach § 30 Absatz 1 NIS2UmsuCG müssen zumindest Folgendes umfassen:		ISO/IEC 27001:2022
§ 30 (2) 1.	Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme	6.1.2, 6.1.3 bzw. 8.2, 8.3, A.5.31 A.5.01-A.5.04, A.5.37, [A.5.09, A.5.12, A.5.13]
§ 30 (2) 2.	Bewältigung von Sicherheitsvorfällen (inkl. Systeme zur Angriffserkennung SzA)	A.8.24, A.5.25, A.5.26, A.5.27, A.5.28, A.6.08, A.8.15, A.8.16, A.8.17
§ 30 (2) 3.	Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement	A.5.29, A.5.30, A.8.06, A.8.13, A.8.14, 7.4
§ 30 (2) 3.	Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern	A.5.19, A.5.20, A.5.21, A.5.22, A.5.23
§ 30 (2) 5.	Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen	A.5.08, A.8.25, A.8.26, A.8.27. A.8.28, A.8.29, A.8.30, A.8.31, A.8.32, A.7.13, A.5.07, A.8.08, A.8.09
§ 30 (2) 6.	Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit	9.1, 9.2, 9.3, A.5.35, A.5.36, A.8.34
§ 30 (2) 7.	grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik	7.2, 7.3, A.6.03, A.7.07
§ 30 (2) 8.	Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung	A.5.01; A.5.14; A.5.31; A.8.24
§ 30 (2) 9.	Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Konzepte für das Management von Anlagen	A.6.01, A.6.02, A.6.04 – A.6.06, A.5.15, A.5.18, A.5.09 – A.5.13, A.6.07, A.7.09, A.8.01, A.7.10, A.7.14
§ 30 (2) 10.	Verwendung von Lösungen zur MFA oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- u. Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung	A.5.16, A.5.17, A.8.05, A.8.20, A.8.21, A.8.12, A.8.14, A.5.30

Risikomanagement nach ISO/IEC 27001 - ISO/IEC 27005



DQS-Praxistag Informationssicherheit

Das sind die Highlights am 13. November 2024!

- ✓ **Regulatorische Einblicke:** Unsere Experten geben einen praxisnahen Überblick über aktuelle Entwicklungen in der IT-Regulierung und deren Auswirkungen auf Ihr Unternehmen.
- ✓ **ISO/IEC 27001 als Compliance-Hilfe:** Erfahren Sie, wie die Norm Ihre Compliance-Anforderungen unterstützt und Optimierungen im Unternehmen ermöglicht.
- ✓ **Methodische Ansätze für den Alltag:** Entdecken Sie konkrete Methoden zur Umsetzung von ISMS und zur effizienten Integration neuer Regularien in Ihre Sicherheitsprozesse.

Warum teilnehmen?

- ➢ Wenn Sie **IT-Sicherheitsverantwortliche**, **IT-Manager**, **Compliance-Beauftragte** oder an **Informationssicherheit** interessiert sind, bietet dieser Online-Kongress praxisnahe Einblicke und Strategien für moderne Cybersecurity. Lernen Sie von Experten und vernetzen Sie sich mit unseren Fachleuten!

dqs

Halle 7 | Stand 604

www.dqsglobal.com