

DIN ISO/IEC 27009

ICS 03.100.70; 03.120.20; 35.030

**Informationstechnik –
IT-Sicherheitsverfahren –
Sektorspezifische Anwendung der ISO/IEC 27001 – Anforderungen
(ISO/IEC 27009:2016)**

Information technology –
Security techniques –
Sector-specific application of ISO/IEC 27001 – Requirements
(ISO/IEC 27009:2016)

Technologies de l'information –
Techniques de sécurité –
Application de l'ISO/IEC 27001 à un secteur spécifique – Exigences
(ISO/IEC 27009:2016)

Gesamtumfang 14 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Inhalt

	Seite
Nationales Vorwort.....	3
Nationaler Anhang NA (informativ) Literaturhinweise	4
1 Anwendungsbereich.....	5
2 Normative Verweisungen	5
3 Begriffe	5
4 Übersicht zu dieser Internationalen Norm	6
4.1 Allgemeines	6
4.2 Aufbau dieser Internationalen Norm	7
4.3 Erweiterung von Anforderungen nach ISO/IEC 27001 oder Maßnahmen nach ISO/IEC 27002.....	7
5 Ergänzende, verfeinerte oder interpretierte Anforderungen nach ISO/IEC 27001	8
5.1 Allgemeines	8
5.2 Ergänzende Anforderungen.....	8
5.3 Verfeinerte Anforderungen	8
5.4 Interpretierte Anforderungen.....	9
6 Ergänzende oder geänderte Anleitung nach ISO/IEC 27002.....	9
6.1 Allgemeines	9
6.2 Ergänzende Anleitung.....	9
6.3 Geänderte Anleitung.....	9
Anhang A (normativ) Vorlage für die Erarbeitung sektorspezifischer Normen mit Bezug zu ISO/IEC 27001:2013 oder ISO/IEC 27002:2013.....	10
A.1 Entwurfsanweisungen	10
A.2 Vorlage.....	10
Literaturhinweise.....	14

Nationales Vorwort

Die Internationale Norm ISO/IEC 27009:2016 wurde in der deutschen Sprachfassung unverändert in das Deutsche Normenwerk übernommen. Fachlich zuständig ist für diese Deutsche Norm der Arbeitskreis NA 043-01-27-01 AK „Anforderungen, Dienste und Richtlinien für IT-Sicherheitssysteme“ im DIN-Normenausschuss „Informationstechnik und Anwendungen“ (NIA).

Die, dieser Norm zugrundeliegende Internationale Norm ISO/IEC 27009:2016, wurde von ISO/IEC JTC 1/SC 27 (*International Organization for Standardization/International Electrotechnical Commission – Joint Technical Committee 1 „Information Technology“/Subcommittee 27 „IT Security techniques“*) erarbeitet.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. Das DIN [und/oder die DKE] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Für die in diesem Dokument zitierte Internationale Norm wird im Folgenden auf die entsprechende Deutsche Norm hingewiesen:

ISO/IEC 27000:2016	siehe	DIN ISO/IEC 27000 (in Überarbeitung)
ISO/IEC 27001:2013	siehe	DIN ISO/IEC 27001
ISO/IEC 27002:2013	siehe	DIN ISO/IEC 27002 (in Überarbeitung)

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN ISO/IEC 27000, *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Überblick und Terminologie*

DIN ISO/IEC 27001:2015-03, *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Anforderungen*

DIN ISO/IEC 27002:2014-02, *Informationstechnik — IT-Sicherheitsverfahren — Leitfaden für das Informationssicherheits-Management*

Informationstechnik — IT-Sicherheitsverfahren — Sektorspezifische Anwendung der ISO/IEC 27001 – Anforderungen

1 Anwendungsbereich

Diese Internationale Norm legt die Anforderungen für die Anwendung von ISO/IEC 27001 in jedem spezifischen Sektor (Bereich, Fachgebiet oder Marktsektor) fest. Sie erläutert, wie ergänzende Anforderungen zu den in ISO/IEC 27001 enthaltenen aufgenommen, wie Anforderungen nach ISO/IEC 27001 verfeinert und wie Maßnahmen oder Maßnahmenkataloge in Ergänzung zu ISO/IEC 27001:2013, Anhang A einbezogen werden müssen.

Diese Internationale Norm stellt sicher, dass ergänzende oder verfeinerte Anforderungen nicht im Widerspruch zu den Anforderungen nach ISO/IEC 27001 stehen.

Diese Internationale Norm ist für all diejenigen anwendbar, die sektorspezifische Normen erarbeiten, die in Bezug zu ISO/IEC 27001 stehen.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 27000:2016, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 27000 und die folgenden Begriffe.

3.1

Interpretation

Erklärung (in Form einer Anforderung oder Anleitung) einer Anforderung nach ISO/IEC 27001 in einem sektorspezifischen Kontext, die keine der Anforderungen nach ISO/IEC 27001 außer Kraft setzt

3.2

Verfeinerung

sektorspezifische Festlegung einer Anforderung nach ISO/IEC 27001, die keine der Anforderungen nach ISO/IEC 27001 beseitigt oder außer Kraft setzt