TECHNISCHE SPEZIFIKATION

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

CEN ISO/IEC/TS 27006-2

November 2022

ICS 35.030; 03.120.20

Deutsche Fassung

Anforderungen an Stellen, die Informationssicherheits-Managementsysteme auditieren und zertifizieren - Teil 2: Datenschutz-Managementsysteme (ISO/IEC TS 27006-2:2021)

Requirements for bodies providing audit and certification of information security management systems - Part 2: Privacy information management systems (ISO/IEC TS 27006-2:2021)

Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management des informations de sécurité - Partie 2: Systèmes de management des informations de sécurité (ISO/IEC TS 27006-2:2021)

Diese Technische Spezifikation (CEN/TS) wurde vom CEN am 30. Oktober 2022 als eine künftige Norm zur vorläufigen Anwendung angenommen.

Die Gültigkeitsdauer dieser CEN/TS ist zunächst auf drei Jahre begrenzt. Nach zwei Jahren werden die Mitglieder des CEN gebeten, ihre Stellungnahmen abzugeben, insbesondere über die Frage, ob die CEN/TS in eine Europäische Norm umgewandelt werden kann.

Die CEN und CENELEC Mitglieder sind verpflichtet, das Vorhandensein dieser CEN/TS in der gleichen Weise wie bei einer EN anzukündigen und die CEN/TS verfügbar zu machen. Es ist zulässig, entgegenstehende nationale Normen bis zur Entscheidung über eine mögliche Umwandlung der CEN/TS in eine EN (parallel zur CEN/TS) beizubehalten.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute und elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Inhalt

Europäisches Vorwort

Der Text von ISO/IEC TS 27006-2:2021 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als CEN ISO/IEC/TS 27006-2:2022 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN-CENELEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN und CENELEC abrufbar.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC TS 27006-2:2021 wurde von CEN-CENELEC als CEN ISO/IEC/TS 27006-2:2022 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents) oder in der IEC-Liste der erhaltenen Patenterklärungen (siehe www.patents.iec.ch).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/TC JTC 1, *Information technology*, Unterkomitee SC 27, *Information security, cybersecurity and privacy protection*, erarbeitet.

Eine Auflistung aller Teile der Normenreihe ISO/IEC 27006 kann auf der ISO-Internetseite abgerufen werden.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

Einleitung

ISO/IEC 27006 legt Kriterien für Stellen fest, die Informationssicherheits-Managementsysteme auditieren und zertifizieren. Falls solche Stellen auch als ISO/IEC 27006-konform akkreditiert werden sollen, mit dem Ziel, Datenschutz-Managementsysteme (PIMS) in Übereinstimmung mit ISO/IEC 27701:2019 zu auditieren und zu zertifizieren, sind einige zusätzliche Anforderungen und Anleitungen in Bezug auf ISO/IEC 27006 erforderlich. Diese werden durch dieses Dokument zur Verfügung gestellt.

Der Text dieses Dokuments folgt der Struktur von ISO/IEC 27006, und die zusätzlichen PIMS-spezifischen Anforderungen und die Anleitung zur Anwendung von ISO/IEC 27006 für die PIMS-Zertifizierung werden durch die Buchstaben „PS“ gekennzeichnet.

Der wesentliche Zweck dieses Dokuments besteht darin, Akkreditierungsstellen zu befähigen, ihre Anwendung von Normen, nach denen sie Zertifizierungsstellen bewerten müssen, effektiver in Einklang zu bringen.