# SLOVENSKI STANDARD
# SIST EN ISO/IEC 27001:2017

**01-julij-2017**

**Nadomešča:**

**SIST ISO/IEC 27001:2013**

---

**Informacijska tehnologija - Varnostne tehnike - Sistemi upravljanja informacijske varnosti - Zahteve (ISO/IEC 27001:2013, vključno s popravkoma Cor 1:2014 in Cor 2:2015)**

Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)



Informationstechnik - Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015)



Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences (ISO/IEC 27001:2013 y compris Cor 1:2014 et Cor 2:2015)

**Ta slovenski standard je istoveten z: EN ISO/IEC 27001:2017**

---

**ICS:**

| | | |
|---|---|---|
| 03.100.70 | Sistemi vodenja | Management systems |
| 35.030 | Informacijska varnost | IT Security |

**SIST EN ISO/IEC 27001:2017 en,fr,de**

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

# EN ISO/IEC 27001

Februar 2017

ICS 03.100.70; 35.030

Deutsche Fassung

## Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2013 + Cor. 1:2014 + Cor. 2:2015)

Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)

Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences (ISO/IEC 27001:2013 y compris Cor 1:2014 et Cor 2:2015)

Diese Europäische Norm wurde vom CEN am 26. Januar 2017 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.



Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.



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

**CEN-CENELEC Management Centre:**
**Avenue Marnix 17, B-1000 Brussels**

# Inhalt

Seite

# Europäisches Vorwort

Der Text von ISO/IEC 27001:2013 + Cor. 1:2014 + Cor. 2:2015 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als EN ISO/IEC 27001:2017 übernommen.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis August 2017, und etwaige entgegenstehende nationale Normen müssen bis August 2017 zurückgezogen werden.

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

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien, 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 27001:2013 + Cor. 1:2014 + Cor. 2:2015 wurde vom CEN als EN ISO/IEC 27001:2017 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. Internationale Organisationen, staatlich und nichtstaatlich, in Liaison mit ISO und IEC, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames technisches Komitee (JTC, en: joint technical committee), ISO/IEC JTC 1, eingerichtet.

Internationale Normen werden in Übereinstimmung mit den Regeln nach ISO/IEC Direktive, Teil 2 erarbeitet.

Die Hauptaufgabe von Technischen Komitees ist es Internationale Normen zu erarbeiten. Internationale Norm-Entwürfe, die von Technischen Komitees verabschiedet wurden, werden den Mitgliedsorganisationen zur Abstimmung zur Verfügung gestellt. Für die Veröffentlichung als Internationale Norm werden mindestens 75 % Zustimmung der Mitgliedsorganisationen benötigt.

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.



ISO/IEC 27001 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“, Unterkomitee SC 27 „IT Security techniques“, erarbeitet.



Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO/IEC 27001:2005), welche technisch überarbeitet wurde.

# 0 Einleitung

## 0.1 Allgemeines

Diese Internationale Norm wurde erarbeitet, um Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) festzulegen. Die Einführung eines Informationssicherheitsmanagementsystems stellt für eine Organisation eine strategische Entscheidung dar. Erstellung und Umsetzung eines Informationssicherheitsmanagementsystems innerhalb einer Organisation richten sich nach deren Bedürfnissen und Zielen, den Sicherheitsanforderungen, den organisatorischen Abläufen sowie nach Größe und Struktur der Organisation. Es ist davon auszugehen, dass sich alle diese Einflussgrößen im Laufe der Zeit ändern.

Das Informationssicherheitsmanagementsystem wahrt die Vertraulichkeit, Integrität und Verfügbarkeit von Information unter Anwendung eines Risikomanagementprozesses und verleiht interessierten Parteien das Vertrauen in eine angemessene Steuerung von Risiken.

Es ist wichtig, dass das Informationssicherheitsmanagementsystem als Teil der Abläufe der Organisation in deren übergreifende Steuerungsstruktur integriert ist und die Informationssicherheit bereits bei der Konzeption von Prozessen, Informationssystemen und Maßnahmen berücksichtigt wird. Es wird erwartet, dass die Umsetzung eines Informationssicherheitsmanagementsystems entsprechend den Bedürfnissen der Organisation skaliert wird.

Diese Internationale Norm kann von internen und externen Parteien dazu eingesetzt werden, die Fähigkeit einer Organisation zur Einhaltung ihrer eigenen Informationssicherheitsanforderungen zu beurteilen.



Die Reihenfolge, in der die Anforderungen in dieser Internationalen Norm aufgeführt sind, spiegelt nicht deren Bedeutung wider noch die Abfolge, in der sie umzusetzen sind. Die Einträge sind lediglich zu Referenzierungszwecken nummeriert.



ISO/IEC 27000 liefert einen Überblick und die Begrifflichkeiten von Informationssicherheitsmanagementsystemen und verweist auf die Informationssicherheitsmanagementsystem-Normenfamilie (einschließlich ISO/IEC 27003 [2], ISO/IEC 27004 [3] und ISO/IEC 27005 [4]), einschließlich deren Begriffe.

## 0.2 Kompatibilität mit anderen Normen für Managementsysteme

Diese Internationale Norm wendet die Grundstrukturen, den einheitlichen Basistext, die gemeinsamen Benennungen und die Basisdefinitionen für den Gebrauch in Managementsystemnormen an, die jeweils im Anhang SL der ISO/IEC-Direktiven, Teil 1, „Consolidated ISO Supplement“ festgelegt sind, und stellt so die Übereinstimmung mit anderen Managementsystemnormen her, die ebenfalls den Anhang SL anwenden.

Die in Anhang SL festgelegte allgemeine Herangehensweise nützt jenen Organisationen, die sich für den Betrieb eines einzigen Managementsystems entscheiden, um die Anforderungen von zwei oder mehr Normen für Managementsysteme zu erfüllen.

# 1 Anwendungsbereich

Diese Internationale Norm legt die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems im Kontext der Organisation fest. Darüber hinaus beinhaltet diese Internationale Norm Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken entsprechend den individuellen Bedürfnissen der Organisation. Die in dieser Internationalen Norm festgelegten Anforderungen sind allgemein gehalten und sollen auf alle Organisationen, ungeachtet ihrer Art und Größe, anwendbar sein. Wenn eine Organisation Konformität mit dieser Internationalen Norm für sich beansprucht, darf sie keine der Anforderungen in den Abschnitten 4 bis 10 ausschließen.

# 2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung des 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, *Information technology — Security Techniques — Information security management systems — Overview and vocabulary*

# 3 Begriffe

Für die Anwendung dieses Dokuments gelten die in ISO/IEC 27000 angegebenen Begriffe.



# 4 Kontext der Organisation

## 4.1 Verstehen der Organisation und ihres Kontextes



Die Organisation muss externe und interne Themen bestimmen, die für ihren Zweck relevant sind und sich auf ihre Fähigkeit auswirken, die beabsichtigten Ergebnisse ihres Informationssicherheitsmanagement-systems zu erreichen.

ANMERKUNG Die Bestimmung dieser Themen bezieht sich auf die Festlegung des externen und internen Kontexts des Unternehmens, wie in ISO 31000:2009 [5], 5.3, beschrieben.

## 4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien

Die Organisation muss:

a) die interessierten Parteien, die für ihr Informationssicherheitsmanagementsystem relevant sind; und

b) die Anforderungen dieser interessierten Parteien mit Bezug zur Informationssicherheit

bestimmen.

ANMERKUNG Die Anforderungen interessierter Parteien können gesetzliche und regulatorische Vorgaben sowie vertragliche Verpflichtungen beinhalten.

### 4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems

Die Organisation muss die Grenzen und die Anwendbarkeit des Informationssicherheitsmanagementsystems bestimmen, um dessen Anwendungsbereich festzulegen.

Bei der Festlegung des Anwendungsbereichs muss die Organisation:

a) die unter 4.1 genannten externen und internen Themen;

b) die unter 4.2 genannten Anforderungen; und

c) Schnittstellen und Abhängigkeiten zwischen Tätigkeiten, die von der Organisation selbst durchgeführt werden, und Tätigkeiten, die von anderen Organisationen durchgeführt werden,

berücksichtigen.

Der Anwendungsbereich muss als dokumentierte Information verfügbar sein.

### 4.4 Informationssicherheitsmanagementsystem

Die Organisation muss entsprechend den Anforderungen dieser Internationalen Norm ein Informationssicherheitsmanagementsystem aufbauen, verwirklichen, aufrechterhalten und fortlaufend verbessern.

## 5 Führung



### 5.1 Führung und Verpflichtung

Die oberste Leitung muss in Bezug auf das Informationssicherheitsmanagementsystem Führung und Verpflichtung zeigen, indem sie:



a) sicherstellt, dass die Informationssicherheitspolitik und die Informationssicherheitsziele festgelegt und mit der strategischen Ausrichtung der Organisation vereinbar sind;

b) sicherstellt, dass die Anforderungen des Informationssicherheitsmanagementsystems in die Geschäftsprozesse der Organisation integriert werden;

c) sicherstellt, dass die für das Informationssicherheitsmanagementsystem erforderlichen Ressourcen zur Verfügung stehen;

d) die Bedeutung eines wirksamen Informationssicherheitsmanagements sowie die Wichtigkeit der Erfüllung der Anforderungen des Informationssicherheitsmanagementsystems vermittelt;

e) sicherstellt, dass das Informationssicherheitsmanagementsystem sein beabsichtigtes Ergebnis bzw. seine beabsichtigten Ergebnisse erzielt;

f) Personen anleitet und unterstützt, damit diese zur Wirksamkeit des Informationssicherheitsmanagementsystems beitragen können;

g) fortlaufende Verbesserung fördert; und

h) andere relevante Führungskräfte unterstützt, um deren Führungsrolle in deren jeweiligen Verantwortungsbereichen deutlich zu machen.

## 5.2 Politik

Die oberste Leitung muss eine Informationssicherheitspolitik festlegen, die:

a) für den Zweck der Organisation angemessen ist;

b) Informationssicherheitsziele (siehe 6.2) beinhaltet oder den Rahmen zum Festlegen von Informationssicherheitszielen bietet;

c) eine Verpflichtung zur Erfüllung zutreffender Anforderungen mit Bezug zur Informationssicherheit enthält; und

d) eine Verpflichtung zur fortlaufenden Verbesserung des Informationssicherheitsmanagementsystems enthält.

Die Informationssicherheitspolitik muss:

e) als dokumentierte Information verfügbar sein;

f) innerhalb der Organisation bekanntgemacht werden; und

g) für interessierte Parteien verfügbar sein, soweit angemessen.

## 5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation



Die oberste Leitung muss sicherstellen, dass die Verantwortlichkeiten und Befugnisse für Rollen mit Bezug zur Informationssicherheit zugewiesen und bekannt gemacht werden.

Die oberste Leitung muss die Verantwortlichkeit und Befugnis zuweisen für:



a) das Sicherstellen, dass das Informationssicherheitsmanagementsystem die Anforderungen dieser Internationalen Norm erfüllt; und

b) das Berichten an die oberste Leitung über die Leistung des Informationssicherheitsmanagementsystems.

ANMERKUNG Die oberste Leitung darf auch Verantwortlichkeiten und Befugnisse für das Berichten der Leistung des Informationssicherheitsmanagementsystems innerhalb der Organisation zuweisen.

# 6 Planung

## 6.1 Maßnahmen zum Umgang mit Risiken und Chancen

### 6.1.1 Allgemeines

Bei der Planung für das Informationssicherheitsmanagementsystem muss die Organisation die in 4.1 genannten Themen und die in 4.2 genannten Anforderungen berücksichtigen sowie die Risiken und Chancen bestimmen, die betrachtet werden müssen, um:

a) sicherzustellen, dass das Informationssicherheitsmanagementsystem seine beabsichtigten Ergebnisse erzielen kann;

b) unerwünschte Auswirkungen zu verhindern oder zu verringern; und

c) fortlaufende Verbesserung zu erreichen.

Die Organisation muss planen:

d) Maßnahmen zum Umgang mit diesen Risiken und Chancen; und

e) wie

1) die Maßnahmen in die Informationssicherheitsmanagementsystemprozesse der Organisation integriert und dort umgesetzt werden; und

2) die Wirksamkeit dieser Maßnahmen bewertet wird.

### 6.1.2 Informationssicherheitsrisikobeurteilung

Die Organisation muss einen Prozess zur Informationssicherheitsrisikobeurteilung festlegen und anwenden, der:

a) Informationssicherheitsrisikokriterien festlegt und aufrechterhält, welche:

1) die Kriterien zur Risikoakzeptanz; und

2) Kriterien für die Durchführung von Informationssicherheitsrisikobeurteilungen

beinhalten;

b) sicherstellt, dass wiederholte Informationssicherheitsrisikobeurteilungen zu konsistenten, gültigen und vergleichbaren Ergebnissen führen;



c) die Informationssicherheitsrisiken identifiziert:



1) den Prozess zur Informationssicherheitsrisikobeurteilung anwendet, um Risiken im Zusammenhang mit dem Verlust der Vertraulichkeit, Integrität und Verfügbarkeit von Information innerhalb des Anwendungsbereichs des ISMS zu ermitteln; und

2) die Risikoeigentümer identifiziert;

d) die Informationssicherheitsrisiken analysiert:

1) die möglichen Folgen bei Eintritt der nach 6.1.2 c) 1) identifizierten Risiken abschätzt;

2) die realistischen Eintrittswahrscheinlichkeiten der nach 6.1.2 c) 1) identifizierten Risiken abschätzt; und

3) die Risikoniveaus bestimmt;

e) die Informationssicherheitsrisiken bewertet:

1) die Ergebnisse der Risikoanalyse mit den nach 6.1.2 a) festgelegten Risikokriterien vergleicht; und

2) die analysierten Risiken für die Risikobehandlung priorisiert.

Die Organisation muss dokumentierte Information über den Informationssicherheitsrisikobeurteilungsprozess aufbewahren.

### 6.1.3 Informationssicherheitsrisikobehandlung

Die Organisation muss einen Prozess für die Informationssicherheitsrisikobehandlung festlegen und anwenden, um:

a) angemessene Optionen für die Informationssicherheitsrisikobehandlung unter Berücksichtigung der Ergebnisse der Risikobeurteilung auszuwählen;

b) alle Maßnahmen, die zur Umsetzung der gewählte(n) Option(en) für die Informationssicherheitsrisikobehandlung erforderlich sind, festzulegen;

ANMERKUNG Organisationen können Maßnahmen nach Bedarf gestalten oder aus einer beliebigen Quelle auswählen.

c) die nach 6.1.3 b) festgelegten Maßnahmen mit den Maßnahmen in Anhang A zu vergleichen und zu überprüfen, dass keine erforderlichen Maßnahmen ausgelassen wurden;

ANMERKUNG 1 Anhang A enthält eine umfassende Liste von Maßnahmenzielen und Maßnahmen. Anwender dieser Internationalen Norm werden auf Anhang A verwiesen, um sicherzustellen, dass keine wichtigen Maßnahmen übersehen wurden.

ANMERKUNG 2 In den ausgewählten Maßnahmen sind implizit Maßnahmenziele enthalten. Die Liste der Maßnahmenziele und Maßnahmen in Anhang A ist nicht erschöpfend und weitere Maßnahmenziele und Maßnahmen könnten erforderlich sein.

d) [AC] eine Erklärung zur Anwendbarkeit zu erstellen, welche

— die erforderlichen Maßnahmen (siehe 6.1.3 b) und c));

— Gründe für deren Einbeziehung;

— ob sie umgesetzt sind oder nicht; sowie

— Gründe für die Nichteinbeziehung von Maßnahmen aus Anhang A

enthält; [AC]

e) einen Plan für die Informationssicherheitsrisikobehandlung zu formulieren; und

f) bei den Risikoeigentümern eine Genehmigung des Plans für die Informationssicherheitsrisikobehandlung sowie ihre Akzeptanz der Informationssicherheitsrestrisiken einzuholen.

Die Organisation muss dokumentierte Information über den Informationssicherheitsrisikobehandlungsprozess aufbewahren.

ANMERKUNG Der in dieser Internationalen Norm genannte Prozess für die Informationssicherheitsrisikobeurteilung und -behandlung steht im Einklang mit den Grundsätzen und allgemeinen Leitlinien in ISO 31000 [5].

## 6.2 Informationssicherheitsziele und Planung zu deren Erreichung

Die Organisation muss Informationssicherheitsziele für relevante Funktionen und Ebenen festlegen.

Die Informationssicherheitsziele müssen:

a) im Einklang mit der Informationssicherheitspolitik stehen;

b) messbar sein (sofern machbar);