

2021

Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí -  
Správa a řízení bezpečnosti informací

ČSN  
ISO/IEC 27014

36 9790

Information security, cybersecurity and privacy protection - Governance of information security

Sécurité de l'information, cybersécurité et protection de la vie privée - Gouvernance de la sécurité de l'information

Tato norma je českou verzí mezinárodní normy ISO/IEC 27014:2020. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 27014:2020. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Národní předmluva

Informace o citovaných dokumentech

ISO/IEC 27000 zavedena v ČSN EN ISO/IEC 27000 (36 9790) Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník

Související ČSN

ČSN EN ISO/IEC 27001 (36 9797) Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky

ČSN EN ISO/IEC 27002:2014 (36 9798) Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací

ČSN EN ISO/IEC 27011:2020 (36 9710) Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací pro telekomunikační organizace založený na ISO/IEC 27002

ČSN ISO 37001:2017 (01 0392) Systémy protikorupčního managementu - Požadavky s návodem pro použití

ČSN ISO/IEC 38500:2020 (36 9045) Informační technologie - Správa a řízení IT technologií v organizaci

## Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v člancích „Informace o citovaných dokumentech“ a „Souvisící ČSN“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných evropských/mezinárodních norem (včetně všech změn).

## Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČO 40654419

Technická normalizační komise: TNK 20 Informační technologie

Pracovník České agentury pro standardizaci: Ing. Miroslav Škop

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

ICS 35.030

Obsah

	Strana
Předmluva.....	
..... 5	
Úvod.....	
..... 6	
<b>1.....</b> Předmět normy.....	
..... 7	
<b>2.....</b> Citované dokumenty.....	
..... 7	
<b>3.....</b> Termíny a definice.....	
..... 7	
<b>4.....</b> Zkrácené termíny.....	
..... 8	
<b>5.....</b> Použití a struktura tohoto dokumentu.....	8
<b>6.....</b> Normy v oblasti správy a řízení.....	8
<b>6.1.....</b> Přehled.....	8
..... 8	
<b>6.2.....</b> Činnosti správy a řízení v rozsahu ISMS.....	8
<b>6.3.....</b> Další souvisící normy.....	
..... 9	

<b>6.4.....</b>	Vlákno správy a řízení v organizaci.....	9
<b>7.....</b>	Správa a řízení entity a správa a řízení bezpečnosti informací.....	9
<b>7.1.....</b>	Přehled.....	9
<b>7.2.....</b>	Cíle.....	10
<b>7.2.1... Cíl 1:</b>	Ustanovit integrovanou komplexní bezpečnost informací pro celou entitu.....	10
<b>7.2.2... Cíl 2:</b>	Rozhodovat pomocí přístupu založeného na riziku.....	10
<b>7.2.3... Cíl 3:</b>	Nastavit směr akvizice.....	10
<b>7.2.4... Cíl 4:</b>	Zajistit soulad s interními a externími požadavky.....	10
<b>7.2.5... Cíl 5:</b>	Podporovat kulturu pozitivního vztahu k bezpečnosti.....	10
<b>7.2.6... Cíl 6:</b>	Zajistit, aby výkonnost bezpečnosti splňovala současné a budoucí požadavky entity.....	11
<b>7.3.....</b>	Procesy.....	11
<b>7.3.1...</b>	Obecně.....	11
<b>7.3.2...</b>	Hodnocení.....	12
<b>7.3.3...</b>	Směřování.....	12
<b>7.3.4...</b>	Monitorování.....	12

### 7.3.5...

Komunikace.....  
..... 13

**8**..... Požadavky orgánu správy a řízení na  
ISMS..... 13

**8.1**..... Organizace  
a ISMS.....  
..... 13

**8.2**..... Scénáře (viz příloha  
B).....  
... 14

**Příloha A** (informativní) Vztahy správy  
a řízení..... 15

**Příloha B** (informativní) Typy organizace  
ISMS..... 16

**Příloha C** (informativní) Příklady  
komunikace..... 17

Bibliografie.....  
..... 18

### **DOKUMENT CHRÁNĚNÝ COPYRIGHTEM**

© ISO/IEC 2020

Veškerá práva vyhrazena. Žádná část této publikace nesmí být, není-li specifikováno jinak nebo nepožaduje-li se to v souvislosti s její implementací, reprodukována nebo používána v jakémkoliv formě nebo jakýmkoliv způsobem, elektronickým ani mechanickým, včetně pořizování fotokopii nebo zveřejňování na internetu nebo intranetu, bez předchozího písemného souhlasu. O souhlas lze požádat buď ISO na níže uvedené adrese, nebo členskou organizaci ISO v zemi žadatele.

ISO copyright office

CP 401 · Ch. de Blandonnet 8

CH-1214 Vernier, Geneva

Tel.: + 41 22 749 01 11

E-mail: [copyright@iso.org](mailto:copyright@iso.org)

Web: [www.iso.org](http://www.iso.org)

Publikováno ve Švýcarsku

# Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětová federace národních normalizačních orgánů (členů ISO). Mezinárodní normy obvykle vypracovávají technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být v této technické komisi zastoupen. Práce se zúčastňují také vládní i nevládní mezinárodní organizace, s nimiž ISO navázala pracovní styk. ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice.

Postupy použité při tvorbě tohoto dokumentu a postupy určené pro jeho další udržování jsou popsány ve směrnících ISO/IEC, část 1. Zejména se má věnovat pozornost rozdílným schvalovacím kritériím potřebným pro různé druhy dokumentů ISO. Tento dokument byl vypracován v souladu s redakčními pravidly uvedenými ve směrnících ISO/IEC, část 2 (viz [www.iso.org/directives](http://www.iso.org/directives)).

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO nelze činit odpovědnou za identifikaci jakéhokoliv nebo všech patentových práv. Podrobnosti o jakýchkoliv patentových právech identifikovaných během přípravy tohoto dokumentu budou uvedeny v úvodu a/nebo v seznamu patentových prohlášení obdržných ISO (viz [www.iso.org/patents](http://www.iso.org/patents)).

Jakýkoliv obchodní název použitý v tomto dokumentu se uvádí jako informace pro usnadnění práce uživatelů a neznamená schválení.

Vysvětlení nezávazného charakteru technických norem, významu specifických termínů a výrazů ISO, které se vztahují k posuzování shody, jakož i informace o tom, jak ISO dodržuje principy Světové obchodní organizace (WTO) týkající se technických překážek obchodu (TBT), jsou uvedeny na [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html).

Tento dokument vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise SC 27 *Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí*, ve spolupráci s ITU-T.

Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na adrese [www.iso.org/members.html](http://www.iso.org/members.html).

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 27014:2013), které bylo technicky zrevidováno. Hlavní změny oproti předchozímu vydání jsou:

- dokument byl uveden do souladu s ISO/IEC 27001:2013;
- byly vysvětleny požadavky ISO/IEC 27001, které představují činnosti v oblasti správy a řízení;
- byly popsány cíle a procesy správy a řízení bezpečnosti informací.

Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na adrese [www.iso.org/members.html](http://www.iso.org/members.html).

# Úvod

Bezpečnost informací je pro organizace klíčovou záležitostí, kterou umocňuje rychlý pokrok v metodikách a technologiích útoků a odpovídající zvýšené regulatorní tlaky.

Selhání opatření organizace v oblasti bezpečnosti informací může mít mnoho nepříznivých dopadů na organizaci a její zainteresované strany, mimo jiné včetně narušení důvěry.

Správa a řízení bezpečnosti informací představuje využití zdrojů k zajištění efektivní implementace bezpečnosti informací a poskytuje záruku, že:

- budou dodržovány směrnice týkající se bezpečnosti informací; a
- orgán správy a řízení obdrží spolehlivé a relevantní zprávy o činnostech souvisejících s bezpečností informací.

To pomáhá orgánu správy a řízení činit rozhodnutí týkající se strategických cílů organizace poskytováním informací o bezpečnosti informací, které mohou tyto cíle ovlivnit. Správa a řízení bezpečnosti informací rovněž zajišťují, že je strategie bezpečnosti informací v souladu s celkovými cíli entity.

Manažeři a další pracující v organizacích potřebují rozumět:

- požadavkům na správu a řízení, které ovlivňují jejich práci; a
- jak splnit požadavky na správu a řízení, které po nich vyžadují, aby jednali.

# 1 Předmět normy

Tento dokument poskytuje pokyny ke koncepcím, cílům a procesům pro správu a řízení bezpečnosti informací, pomocí kterých mohou organizace hodnotit, směřovat, monitorovat a komunikovat procesy související s bezpečností informací v rámci organizace.

Cílovou skupinu tohoto dokumentu představují:

- orgán správy a řízení a vrcholový management;
- osoby odpovědné za hodnocení, směřování a monitorování systému řízení bezpečnosti informací (ISMS) založeného na ISO/IEC 27001;
- osoby odpovědné za řízení bezpečnosti informací, které probíhá mimo rámec ISMS založeného na ISO/IEC 27001, ale v rámci správy a řízení.

Tento dokument je použitelný pro všechny typy a velikosti organizací.

Všechny odkazy na ISMS v tomto dokumentu platí pro ISMS na základě ISO/IEC 27001.

Tento dokument se zaměřuje na tři typy organizací ISMS uvedené v příloze B. Tento dokument však může být používán i v případě jiných typů organizací.

**Konec náhledu - text dále pokračuje v placené verzi ČSN.**