

STN	Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Riadenie informačnej bezpečnosti (ISO/IEC 27002: 2022)	STN EN ISO/IEC 27002 97 4172
------------	---	--

Information security, cybersecurity and privacy protection
Information security controls

Sécurité de l'information, cybersécurité et protection de la vie privée
Moyens de maîtrise de l'information

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre
Informationssicherheitsmaßnahmen

Táto slovenská technická norma je slovenskou verziou európskej normy EN ISO/IEC 27002: 2022.
Preklad zabezpečil Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky.
STN EN ISO/IEC 27002 má rovnaké postavenie, ako majú oficiálne verzie.

This standard is the Slovak version of the European Standard EN ISO/IEC 27002: 2022.
It was translated by Slovak Office of Standards, Metrology and Testing.
STN EN ISO/IEC 27002 has the same status as the official versions.

Nahradenie predchádzajúcich dokumentov

Táto slovenská technická norma nahrádza STN EN ISO/IEC 27002 z februára 2019 v celom rozsahu.

136380

Národný predhovor

Tento dokument pripravila spoločná technická komisia ISO/IEC JTC 1 Informačné technológie, subkomisia SC 27, Bezpečnosť informácií, kybernetická bezpečnosť a ochrana súkromia.

Toto tretie vydanie ruší a nahrádza druhé vydanie (ISO/IEC 27002: 2013), ktoré bolo technicky revidované. Zahŕňa aj technické opravy ISO/IEC 27002: 2013/Cor. 1: 2014 a ISO/IEC 27002: 2013/Cor. 2: 2015.

Hlavné zmeny sú tieto:

- názov bol upravený;
- štruktúra dokumentu bola zmenená, pričom ovládacie prvky sú prezentované pomocou jednoduchej taxonómie a súvisiacich atribútov;
- niektoré ovládacie prvky boli zlúčené, niektoré odstránené a bolo zavedených niekoľko nových ovládacích prvkov. Úplná korešpondencia sa nachádza v prílohe B.

Normatívne referenčné dokumenty

Táto slovenská technická norma neobsahuje normatívne odkazy.

Vypracovanie slovenskej technickej normy

Spracovateľ: Ing. Lenka Gondová, Pro Excellence, s. r. o., Bratislava

Technická komisia: TK 37 Informačné technológie

**Informačná bezpečnosť, kybernetická bezpečnosť
a ochrana súkromia
Riadenie informačnej bezpečnosti
(ISO/IEC 27002: 2022)**

Information security, cybersecurity
and privacy protection
Information security controls
(ISO/IEC 27002: 2022)

Sécurité de l'information, cybersécurité
et protection de la vie privée
Moyens de maîtrise de l'information
(ISO/IEC 27002: 2022)

Informationssicherheit, Cybersicherheit
und Schutz der Privatsphäre
Informationssicherheitsmaßnahmen
(ISO/IEC 27002: 2022)

Túto európsku normu schválil CEN 30. októbra 2022.

Členovia CEN a CENELEC sú povinní plniť vnútorné predpisy CEN/CENELEC, v ktorých sú určené podmienky, za ktorých sa tejto európskej norme bez akýchkoľvek zmien priznáva postavenie národnej normy. Aktualizované zoznamy a bibliografické odkazy týkajúce sa takýchto národných noriem možno na požiadanie dostať od Riadiaceho strediska CEN-CENELEC alebo od každého člena CEN a CENELEC.

Táto európska norma existuje v troch oficiálnych verziách (anglickej, francúzskej, nemeckej). Verzia v akomkoľvek inom jazyku, ktorú na vlastnú zodpovednosť vydal člen CEN a CENELEC v preklade do národného jazyka a ktorá bola oznámená Riadiacemu stredisku CEN-CENELEC, má rovnaké postavenie, ako majú oficiálne verzie.

Členmi CEN a CENELEC sú národné normalizačné organizácie Belgicka, Bulharska, Cypru, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Islandu, Litvy, Lotyšska, Luxemburska, Maďarska, Malty, Nemecka, Nórska, Poľska, Portugalska, Rakúska, Rumunská, Severného Macedónska, Slovenska, Slovinska, Spojeného kráľovstva, Srbska, Španielska, Švajčiarska, Švédsko, Talianska a Turecko.

CEN

Európsky výbor pre normalizáciu
European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

**Riadiace stredisko CEN-CENELEC:
Rue de la Science 23, B-1040 Brusel**

CENELEC

Európsky výbor pre normalizáciu v elektrotechnike
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

**Riadiace stredisko CEN-CENELEC:
Rue de la Science 23, B-1040 Brusel**

Obsah

	strana
Európsky predhovor	8
Úvod	9
1 Predmet	13
2 Normatívne odkazy.....	13
3 Termíny, definície a skrátené termíny	13
3.1 Termíny a definície	13
3.2 Skrátené termíny	20
4 Štruktúra tohto dokumentu	22
4.1 Kapitoly	22
4.2 Témy a atribúty	22
4.3 Štruktúra opatrení	24
5 Organizačné opatrenia	24
5.1 Politiky informačnej bezpečnosti	24
5.2 Úlohy a zodpovednosti v oblasti informačnej bezpečnosti.....	27
5.3 Oddelenie právomoci	29
5.4 Povinnosti manažmentu	30
5.5 Kontakt s orgánmi moci	32
5.6 Kontakt so špeciálnymi záujmovými skupinami	33
5.7 Analýza hrozieb	34
5.8 Informačná bezpečnosť v projektovom riadení	36
5.9 Inventárny zoznam informácií a iných súvisiacich aktív	38
5.10 Prijateľné používanie informácií a iných súvisiacich aktív	41
5.11 Vrátenie aktív.....	42
5.12 Klasifikácia informácií	44
5.13 Označovanie informácií.....	46
5.14 Prenos informácií.....	48
5.15 Riadenie prístupov.....	51
5.16 Správa identít	54
5.17 Autentizačné údaje	56
5.18 Prístupové práva	59
5.19 Informačná bezpečnosť vo vzťahoch s dodávateľmi	61

Contents

	Page
European foreword	8
Introduction	9
1 Scope	13
2 Normative references	8
3 Terms, definitions and abbreviated terms	13
3.1 Terms and definitions	13
3.2 Abbreviated terms	20
4 Structure of this document	22
4.1 Clauses	22
4.2 Themes and attributes	22
4.3 Control layout	24
5 Organizational controls	24
5.1 Policies for information security	24
5.2 Information security roles and responsibilities.....	27
5.3 Segregation of duties	29
5.4 Management responsibilities	30
5.5 Contact with authorities.....	32
5.6 Contact with special interest groups	33
5.7 Threat intelligence.....	34
5.8 Information security in project management	36
5.9 Inventory of information and other associated assets.....	38
5.10 Acceptable use of information and other associated assets	41
5.11 Return of assets	42
5.12 Classification of information	44
5.13 Labelling of information	46
5.14 Information transfer	48
5.15 Access control.....	51
5.16 Identity management.....	54
5.17 Authentication information.....	56
5.18 Access rights.....	59
5.19 Information security in supplier relationships	61

5.20	Riešenie informačnej bezpečnosti v rámci dodávateľských dohôd.....	65	5.20	Addressing information security within supplier agreements	65
5.21	Riadenie informačnej bezpečnosti v dodávateľskom reťazci IKT	68	5.21	Managing information security in the ICT supply chain	68
5.22	Monitorovanie, preskúmanie a riadenie zmien dodávateľských služieb	71	5.22	Monitoring, review and change management of supplier services	71
5.23	Informačná bezpečnosť pri používaní cloudových služieb	73	5.23	Information security for use of cloud services	73
5.24	Plánovanie a príprava riadenia incidentov informačnej bezpečnosti	77	5.24	Information security incident management planning and preparation ...	77
5.25	Posudzovanie a rozhodovanie o udalostiach informačnej bezpečnosti ...	79	5.25	Assessment and decision on information security events	79
5.26	Reakcia na incidenty informačnej bezpečnosti	80	5.26	Response to information security incidents	80
5.27	Poučenie z incidentov informačnej bezpečnosti	82	5.27	Learning from information security incidents	82
5.28	Zhromažďovanie dôkazov	83	5.28	Collection of evidence	83
5.29	Informačná bezpečnosť počas narušenia	84	5.29	Information security during disruption	84
5.30	Pripravenosť IKT na kontinuitu podnikania	85	5.30	ICT readiness for business continuity	85
5.31	Právne, zákonné, regulačné a zmluvné požiadavky	87	5.31	Legal, statutory, regulatory and contractual requirements	87
5.32	Práva duševného vlastníctva	89	5.32	Intellectual property rights	89
5.33	Ochrana záznamov	91	5.33	Protection of records	91
5.34	Ochrana súkromia a osobných údajov....	93	5.34	Privacy and protection of PII	93
5.35	Nezávislé preskúmanie informačnej bezpečnosti	95	5.35	Independent review of information security	95
5.36	Súlad so zásadami, pravidlami a normami pre informačnú bezpečnosť....	98	5.36	Compliance with policies, rules and standards for information security	98
5.37	Zdokumentované prevádzkové postupy....	98	5.37	Documented operating procedures	98
6	Personálne opatrenia	100	6	People controls	100
6.1	Preverovanie	100	6.1	Screening	100
6.2	Podmienky zamestnania	102	6.2	Terms and conditions of employment... ..	102
6.3	Povedomie o informačnej bezpečnosti, vzdelávanie a školenie	103	6.3	Information security awareness, education and training.....	103
6.4	Disciplinárny proces	106	6.4	Disciplinary process	106
6.5	Zodpovednosť pri ukončení alebo zmene zamestnania	107	6.5	Responsibilities after termination or change of employment	107
6.6	Dohody o mlčanlivosti alebo zachovaní mlčanlivosti	108	6.6	Confidentiality or non-disclosure agreements	108
6.7	Práca na diaľku	110	6.7	Remote working	110
6.8	Hlásenie udalostí informačnej bezpečnosti	113	6.8	Information security event reporting	113

7	Fyzické opatrenia	114	7	Physical controls	114
7.1	Perimetre fyzickej bezpečnosti	114	7.1	Physical security perimeters	114
7.2	Fyzický vstup	115	7.2	Physical entry	115
7.3	Zabezpečenie kancelárií, miestností a zariadení	118	7.3	Securing offices, rooms and facilities....	118
7.4	Monitorovanie fyzickej bezpečnosti	119	7.4	Physical security monitoring.....	119
7.5	Ochrana pred fyzickými a environmentálnymi hrozbami	121	7.5	Protecting against physical and environmental threats.....	121
7.6	Práca v zabezpečených oblastiach	123	7.6	Working in secure areas	123
7.7	Čistý stôl a čistá obrazovka	124	7.7	Clear desk and clear screen	124
7.8	Umiestnenie a ochrana zariadení	125	7.8	Equipment siting and protection.....	125
7.9	Bezpečnosť aktív mimo organizácie	126	7.9	Security of assets off-premises	126
7.10	Pamäťové médiá	128	7.10	Storage media	128
7.11	Podporné služby	130	7.11	Supporting utilities	130
7.12	Bezpečnosť kabeláže	132	7.12	Cabling security.....	132
7.13	Údržba zariadení	133	7.13	Equipment maintenance	133
7.14	Bezpečná likvidácia alebo opätovné použitie zariadenia.....	135	7.14	Secure disposal or re-use of equipment	135
8	Technologické opatrenia	136	8	Technological controls	136
8.1	Koncové zariadenia používateľa	136	8.1	User endpoint devices.....	136
8.2	Privilegované prístupové práva	140	8.2	Privileged access rights	140
8.3	Obmedzenie prístupu k informáciám.....	142	8.3	Information access restriction	142
8.4	Prístup k zdrojovému kódu	145	8.4	Access to source code	145
8.5	Bezpečná autentizácia	147	8.5	Secure authentication	147
8.6	Riadenie kapacít.....	149	8.6	Capacity management	149
8.7	Ochrana pred škodlivým softvérom.....	151	8.7	Protection against malware.....	151
8.8	Riadenie technickej zraniteľnosti.....	154	8.8	Management of technical vulnerabilities..	154
8.9	Riadenie konfigurácie	159	8.9	Configuration management.....	159
8.10	Vymazanie informácií	161	8.10	Information deletion.....	161
8.11	Maskovanie údajov.....	163	8.11	Data masking	163
8.12	Prevencia úniku dát.....	166	8.12	Data leakage prevention	166
8.13	Zálohovanie informácií	168	8.13	Information backup.....	168
8.14	Redundancia zariadení na spracovanie informácií	170	8.14	Redundancy of information processing facilities	170
8.15	Logovanie	172	8.15	Logging.....	172
8.16	Monitorovacie činnosti.....	176	8.16	Monitoring activities.....	176
8.17	Synchronizácia času.....	179	8.17	Clock synchronization	179
8.18	Používanie privilegovaných systémových obslužných programov	181	8.18	Use of privileged utility programs.....	181
8.19	Inštalácia softvéru na prevádzkové systémy	182	8.19	Installation of software on operational systems	182
8.20	Sieťová bezpečnosť	184	8.20	Networks security.....	184

8.21	Bezpečnosť sieťových služieb.....	186	8.21	Security of network services	186
8.22	Oddeľovanie sietí	187	8.22	Segregation of networks	187
8.23	Filtrovanie webových stránok.....	189	8.23	Web filtering	189
8.24	Používanie kryptografie.....	190	8.24	Use of cryptography.....	190
8.25	Životný cyklus bezpečného vývoja.....	194	8.25	Secure development life cycle	194
8.26	Požiadavky na bezpečnosť aplikácií	195	8.26	Application security requirements	195
8.27	Bezpečná architektúra systému a zásady vývoja.....	198	8.27	Secure system architecture and engineering principles	198
8.28	Bezpečné kódovanie	201	8.28	Secure coding	201
8.29	Testovanie bezpečnosti pri vývoji a akceptačné testy	205	8.29	Security testing in development and acceptance.....	205
8.30	Vývoj prostredníctvom outsourcingu	207	8.30	Outsourced development.....	207
8.31	Oddelenie vývojových, testovacích a produkčných prostredí.....	209	8.31	Separation of development, test and production environments.....	209
8.32	Riadenie zmien.....	211	8.32	Change management	211
8.33	Testovacie informácie	213	8.33	Test information	213
8.34	Ochrana informačných systémov počas auditného testovania	214	8.34	Protection of information systems during audit testing.....	214
Príloha A (informatívna) – Používanie atribútov			Annex A (informative) – Using attributes		
216			216		
Príloha B (informatívna) – Súlad normy ISO/IEC 270002: 2022 (tento dokument) s normou ISO/IEC 270002: 2013			Annex B (informative) – Correspondence of ISO/IEC 27002: 2022 (this document) with ISO/IEC 27002: 2013.....		
237			237		
Literatúra			Bibliography		
253			253		

Európsky predhovor

Text ISO/IEC 27002: 2022 vypracovala technická komisia ISO/IEC JTC 1 „Informačné technológie“ medzinárodnej organizácie pre normalizáciu (ISO) a bola prevzatá ako EN ISO/IEC 27002: 2022 technickou komisiou CEN-CENELEC/JTC 13 „Kybernetická bezpečnosť a ochrana údajov“, ktorej sekretariát je v DIN.

Tejto európskej norme sa musí priznať postavenie národnej normy buď vydaním identického textu, alebo oznámením najneskoršie do mája 2023 a národné normy, ktoré sú s ňou v rozpore, musia sa zrušiť najneskôr do mája 2023.

Upozorňuje sa na možnosť, že niektoré časti tohto dokumentu môžu byť predmetom patentových práv. CEN-CENELEC nezodpovedajú za identifikáciu ktoréhokoľvek alebo všetkých takýchto patentových práv.

Tento dokument nahrádza EN ISO/IEC 27002: 2017.

Akákoľvek súpätná väzba a otázky k tomuto dokumentu sa majú adresovať národnému normalizačnému orgánu používateľov. Kompletný zoznam týchto používateľov je na webovom sídle CEN-CENELEC.

V súlade s vnútornými predpismi CEN/CENELEC sú túto európsku normu povinné prevziať národné normalizačné organizácie týchto krajín: Belgicka, Bulharska, Cypr, Česka, Dánska, Estónska, Fínska, Francúzska, Grécka, Holandska, Chorvátska, Írska, Island, Litva, Lotyšsko, Luxembursko, Maďarsko, Malta, Nemecko, Nórsko, Poľsko, Portugalsko, Rakúsko, Rumunsko, Severného Macedónska, Slovensko, Slovinsko, Spojeného kráľovstva, Srbsko, Španielsko, Švajčiarsko, Švédsko, Taliansko a Turecko.

Oznámenie o schválení

Text medzinárodnej normy ISO/IEC 27002: 2022 schválil CEN-CENELEC ako EN ISO/IEC 27002: 2022 bez akýchkoľvek modifikácií.

Úvod

0.1 Východiská a kontext

Tento dokument je určený pre organizácie všetkých typov a veľkostí. Používa sa ako referencia na určenie a implementáciu opatrení na ošetrovanie rizík informačnej bezpečnosti v systéme riadenia informačnej bezpečnosti (ISMS) založenom na ISO/IEC 27001. Môže sa použiť aj ako usmernenie pre organizácie určujúce a implementujúce všeobecne akceptované opatrenia informačnej bezpečnosti. Tento dokument je navyše určený na použitie pri rozvoji priemyselných alebo organizačných návodov riadenia informačnej bezpečnosti, pričom sa zohľadňujú riziká informačnej bezpečnosti vlastné danému prostrediu. Organizačné alebo prostrediu špecifické opatrenia odlišné od opatrení zahrnutých v tomto dokumente, je možné určiť prostredníctvom posúdenia rizík podľa potreby.

Organizácie všetkých typov a veľkostí (vrátane verejného a súkromného sektora, komerčného a neziskového) vytvárajú, zhromažďujú, spracúvajú, ukladajú, prenášajú a likvidujú informácie v mnohých formách vrátane elektronických, fyzických a verbálnych (napr. konverzácie a prezentácie).

Hodnota informácií presahuje písané slová, čísla a obrázky: vedomosti, koncepty, nápady a značky sú príkladmi nehmotných foriem informácií. V prepojenom svete si informácie a ďalšie súvisiace aktíva zaslúžia alebo vyžadujú ochranu pred rôznymi zdrojmi rizika, či už prírodnými, náhodnými alebo úmyselnými.

Informačná bezpečnosť sa dosahuje implementáciou vhodného súboru opatrení vrátane politík, pravidiel, procesov, postupov, organizačných štruktúr a softvérových a hardvérových funkcií. Na splnenie svojich konkrétnych bezpečnostných a obchodných cieľov by organizácia mala v prípade potreby definovať, implementovať, monitorovať, preskúmať a vylepšiť tieto opatrenia. ISMS, ako sa uvádza v ISO/IEC 27001, má holistický, koordinovaný pohľad na riziká informačnej bezpečnosti organizácie s cieľom určiť a implementovať komplexnú sadu opatrení informačnej bezpečnosti v rámci celkového rámca koherentného systému riadenia.

Mnoho informačných systémov, vrátane ich správy a prevádzky, nebolo navrhnutých tak, aby boli bezpečné podľa ISMS, ako je uvedené v ISO/IEC 27001 a v tomto dokumente. Úroveň bezpečnosti, ktorú je možné dosiahnuť iba technologickými opatreniami, je obmedzená a mala by byť podporená vhodnými riadiacimi činnosťami a organizačnými procesmi. Identifikácia, ktoré opatrenia by mali byť zavedené, si vyžaduje starostlivé plánovanie a detailný prístup pri ošetrovaní rizík.

Introduction

0.1 Background and context

This document is designed for organizations of all types and sizes. It is to be used as a reference for determining and implementing controls for information security risk treatment in an information security management system (ISMS) based on ISO/IEC 27001. It can also be used as a guidance document for organizations determining and implementing commonly accepted information security controls. Furthermore, this document is intended for use in developing industry and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s). Organizational or environment-specific controls other than those included in this document can be determined through risk assessment as necessary.

Organizations of all types and sizes (including public and private sector, commercial and non-profit) create, collect, process, store, transmit and dispose of information in many forms, including electronic, physical and verbal (e.g. conversations and presentations).

The value of information goes beyond written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and other associated assets deserve or require protection against various risk sources, whether natural, accidental or deliberate.

Information security is achieved by implementing a suitable set of controls, including policies, rules, processes, procedures, organizational structures and software and hardware functions. To meet its specific security and business objectives, the organization should define, implement, monitor, review and improve these controls where necessary. An ISMS such as that specified in ISO/IEC 27001 takes a holistic, coordinated view of the organization's information security risks in order to determine and implement a comprehensive suite of information security controls within the overall framework of a coherent management system.

Many information systems, including their management and operations, have not been designed to be secure in terms of an ISMS as specified in ISO/IEC 27001 and this document. The level of security that can be achieved only through technological measures is limited and should be supported by appropriate management activities and organizational processes. Identifying which controls should be in place requires careful planning and attention to detail while carrying out risk treatment.

Úspešné ISMS vyžaduje podporu od všetkých zamestnancov v organizácii. Môže tiež vyžadovať účasť iných zainteresovaných strán, ako sú akcionári alebo dodávatelia. Môžu byť potrebné aj rady od odborníkov.

Vhodný, primeraný a efektívny systém riadenia informačnej bezpečnosti poskytuje uistenie vedeniu organizácie a iným zainteresovaným stranám, že ich informácie a ďalšie súvisiace aktíva sú primerane zabezpečené a chránené pred hrozbami a škodami, čím umožňujú organizácii dosiahnuť stanovené obchodné ciele.

0.2 Požiadavky na informačnú bezpečnosť

Je nevyhnutné, aby organizácia určovala svoje požiadavky na informačnú bezpečnosť. Existujú tri hlavné zdroje požiadaviek na informačnú bezpečnosť:

- a) posúdenie rizík organizácie, pričom sa zohľadňuje celková obchodná stratégia a ciele organizácie. To sa dá uľahčiť alebo podporovať prostredníctvom hodnotenia rizík informačnej bezpečnosti. Výsledkom by malo byť určenie opatrení potrebných na zabezpečenie toho, aby zostatkové riziko organizácie spĺňalo jej kritériá pre akceptáciu rizika;
- b) právne, zákonné, regulačné a zmluvné požiadavky, ktoré organizácia a jej zainteresované strany (obchodní partneri, poskytovatelia služieb atď.) musia dodržiavať a ich sociálno-kultúrne prostredie;
- c) súbor zásad, cieľov a obchodných požiadaviek pre všetky kroky životného cyklu informácií, ktoré organizácia vyvinula na podporu svojej prevádzky.

0.3 Opatrenia

Opatrenie je definovaná ako opatrenie, ktoré modifikuje alebo zachováva riziko. Niektoré z opatrení v tomto dokumente sú opatrenia, ktoré modifikujú riziko, zatiaľ čo iné zachovávajú riziko. Napríklad politika informačnej bezpečnosti môže zachovávať iba riziko, zatiaľ čo súlad s politikou informačnej bezpečnosti môže modifikovať riziko. Niektoré opatrenia navyše opisujú rovnaké generické opatrenie v rôznych rizikových kontextoch. Tento dokument poskytuje všeobecnú kombináciu organizačných, ľudských, fyzických a technologických opatrení informačnej bezpečnosti odvodených z medzinárodne uznávaných osvedčených postupov.

A successful ISMS requires support from all personnel in the organization. It can also require participation from other interested parties, such as shareholders or suppliers. Advice from subject matter experts can also be needed.

A suitable, adequate and effective information security management system provides assurance to the organization's management and other interested parties that their information and other associated assets are kept reasonably secure and protected against threats and harm, thereby enabling the organization to achieve the stated business objectives.

0.2 Information security requirements

It is essential that an organization determines its information security requirements. There are three main sources of information security requirements:

- a) the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. This can be facilitated or supported through an information security-specific risk assessment. This should result in the determination of the controls necessary to ensure that the residual risk to the organization meets its risk acceptance criteria;
- b) the legal, statutory, regulatory and contractual requirements that an organization and its interested parties (trading partners, service providers, etc.) have to comply with and their socio-cultural environment;
- c) the set of principles, objectives and business requirements for all the steps of the life cycle of information that an organization has developed to support its operations.

0.3 Controls

A control is defined as a measure that modifies or maintains risk. Some of the controls in this document are controls that modify risk, while others maintain risk. An information security policy, for example, can only maintain risk, whereas compliance with the information security policy can modify risk. Moreover, some controls describe the same generic measure in different risk contexts. This document provides a generic mixture of organizational, people, physical and technological information security controls derived from internationally recognized best practices.

0.4 Určenie opatrení

Určenie opatrení závisí od rozhodnutí organizácie po posúdení rizika s jasne definovaným rozsahom. Rozhodnutia týkajúce sa identifikovaných rizík by sa mali zakladať na kritériách pre prijatie rizika, možnosti ošetrenia rizika a prístupu k riadeniu rizika, ktorý organizácia uplatňuje. Určenie opatrení by malo zohľadniť aj všetky príslušné národné a medzinárodné právne predpisy a nariadenia. Určenie opatrení tiež závisí od spôsobu, akým opatrenia vzájomne pôsobia, aby poskytovali obranu do hĺbky.

Organizácia môže podľa potreby navrhnúť opatrenia alebo ich identifikovať z akéhokoľvek zdroja. Pri špecifikovaní takýchto opatrení by organizácia mala zväžiť zdroje a investície potrebné na implementáciu a prevádzku opatrení s realizovanou obchodnou hodnotou. Pre usmernenie o rozhodnutiach týkajúcich sa investície do ISMS a ekonomických dôsledkov týchto rozhodnutí v kontexte konkurenčných požiadaviek na zdroje odporúčame prejsť normu ISO/IEC TR 27016.

Mala by existovať rovnováha medzi zdrojmi nasadenými na implementáciu opatrení a potenciálnym vplyvom bezpečnostných incidentov pri absencii týchto opatrení na podnikanie. Výsledky posúdenia rizík by mali pomôcť usmerňovať a určiť vhodné kroky, priority pre riadenie rizík informačnej bezpečnosti a na implementáciu opatrení nevyhnutných na ochranu pred týmito rizikami.

Niektoré z opatrení v tomto dokumente možno považovať za hlavné zásady pre riadenie informačnej bezpečnosti a platné pre väčšinu organizácií. Viac informácií o určovaní opatrení a iných možnostiach ošetrenia rizík je možné nájsť v ISO/IEC 27005.

0.5 Tvorba špecifického návodu pre organizáciu

Tento dokument možno považovať za východiskový bod pre tvorbu špecifického návodu pre organizáciu. Nie všetky opatrenia a usmernenia v tomto dokumente sa môžu vzťahovať na všetky organizácie. Na riešenie konkrétnych potrieb organizácie a identifikovaných rizík, ktoré boli identifikované, je možné tiež vyžadovať ďalšie opatrenia a usmernenia, ktoré nie sú zahrnuté v tomto dokumente. Ak sa vypracúvajú dokumenty obsahujúce ďalšie usmernenia alebo opatrenia, môže byť užitočné zahrnúť do kapitol krížové odkazy pre budúce použitie.

0.4 Determining controls

Determining controls is dependent on the organization's decisions following a risk assessment, with a clearly defined scope. Decisions related to identified risks should be based on the criteria for risk acceptance, risk treatment options and the risk management approach applied by the organization. The determination of controls should also take into consideration all relevant national and international legislation and regulations. Control determination also depends on the manner in which controls interact with one another to provide defence in depth.

The organization can design controls as required or identify them from any source. In specifying such controls, the organization should consider the resources and investment needed to implement and operate a control against the business value realized. See ISO/IEC TR 27016 for guidance on decisions regarding the investment in an ISMS and the economic consequences of these decisions in the context of competing requirements for resources.

There should be a balance between the resources deployed for implementing controls and the potential resulting business impact from security incidents in the absence of those controls. The results of a risk assessment should help guide and determine the appropriate management action, priorities for managing information security risks and for implementing controls determined necessary to protect against these risks.

Some of the controls in this document can be considered as guiding principles for information security management and as being applicable for most organizations. More information about determining controls and other risk treatment options can be found in ISO/IEC 27005.

0.5 Developing organization-specific guidelines

This document can be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this document can be applicable to all organizations. Additional controls and guidelines not included in this document can also be required to address the specific needs of the organization and the risks that have been identified. When documents are developed containing additional guidelines or controls, it can be useful to include cross-references to clauses in this document for future reference.

0.6 Úvahy o životnom cykle

Informácie majú životný cyklus, od vytvorenia po likvidáciu. Hodnota informácií a riziká s nimi súvisiace, sa môžu v rámci tohto životného cyklu líšiť (napr. neoprávnené zverejnenie alebo krádež finančných účtov spoločnosti nie sú po zverejnení významné, ale integrita zostáva kritická), preto je informačná bezpečnosť do istej miery dôležitá vo všetkých etapách.

Informačné systémy a iné aktíva relevantné pre informačnú bezpečnosť majú životné cykly, v rámci ktorých sú koncipované, špecifikované, navrhnuté, vyvinuté, testované, implementované, používané, udržiavané a prípadne vyradené z používania a zlikvidované. Informačná bezpečnosť by sa mala brať do úvahy v každej fáze. Nové projekty vývoja systému a zmeny v existujúcich systémoch poskytujú príležitosti na zlepšenie bezpečnostných opatrení a zároveň zohľadňujú riziká a ponaučenia organizácie získané z incidentov.

0.7 Súvisiace medzinárodné normy

Aj keď tento dokument ponúka usmernenie týkajúce sa širokého spektra opatrení informačnej bezpečnosti, ktoré sa bežne uplatňujú v rôznych organizáciách, ďalšie dokumenty z radu noriem ISO/IEC 27000 poskytujú doplňujúce informácie alebo požiadavky na ďalšie aspekty celkového procesu riadenia informačnej bezpečnosti.

Všeobecný úvod do ISMS a príbuzných dokumentov nájdete v ISO/IEC 27000. ISO/IEC 27000 poskytuje slovník, ktorý definuje väčšinu výrazov používaných v rámci dokumentov ISO/IEC 27000 a opisuje predmet a ciele pre každú normu z tohto radu.

Existujú normy špecifické pre odvetvie, ktoré obsahujú ďalšie opatrenia, ktorých cieľom je riešiť konkrétne oblasti (napr. ISO/IEC 27017 pre cloudové služby, ISO/IEC 27701 pre ochranu osobných údajov, ISO/IEC 27019 pre energetický priemysel, ISO/IEC 27011 pre telekomunikačné služby a ISO 27799 pre oblasť zdravotníctva). Takéto normy sú zahrnuté v použitej literatúre a niektoré z nich sú uvedené v usmerneniach a ďalších informačných sekciách v kapitolách 5-8.

0.6 Life cycle considerations

Information has a life cycle, from creation to disposal. The value of, and risks to, information can vary throughout this life cycle (e.g. unauthorized disclosure or theft of a company's financial accounts is not significant after they have been published, but integrity remains critical) therefore, information security remains important to some extent at all stages.

Information systems and other assets relevant to information security have life cycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained and eventually retired from service and disposed of. Information security should be considered at every stage. New system development projects and changes to existing systems provide opportunities to improve security controls while taking into account the organization's risks and lessons learned from incidents.

0.7 Related International Standards

While this document offers guidance on a broad range of information security controls that are commonly applied in many different organizations, other documents in the ISO/IEC 27000 family provide complementary advice or requirements on other aspects of the overall process of managing information security.

Refer to ISO/IEC 27000 for a general introduction to both ISMS and the family of documents. ISO/IEC 27000 provides a glossary, defining most of the terms used throughout the ISO/IEC 27000 family of documents, and describes the scope and objectives for each member of the family.

There are sector-specific standards that have additional controls which aim at addressing specific areas (e.g. ISO/IEC 27017 for cloud services, ISO/IEC 27701 for privacy, ISO/IEC 27019 for energy, ISO/IEC 27011 for telecommunications organizations and ISO 27799 for health). Such standards are included in the Bibliography and some of them are referenced in the guidance and other information sections in Clauses 5-8.

1 Predmet

Tento dokument poskytuje referenčný súbor všeobecných opatrení informačnej bezpečnosti vrátane návodu na implementáciu. Tento dokument je určený na použitie organizáciami:

- a) v kontexte systému riadenia informačnej bezpečnosti (ISMS) založeného na norme ISO/IEC 27001;
- b) na implementáciu opatrení informačnej bezpečnosti na základe medzinárodne uznávaných osvedčených postupov;
- c) na vypracovanie návodov pre riadenie informačnej bezpečnosti špecifických pre danú organizáciu.

2 Normatívne odkazy

V tomto dokumente nie sú žiadne normatívne odkazy.

1 Scope

This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:

- a) within the context of an information security management system (ISMS) based on ISO/IEC 27001;
- b) for implementing information security controls based on internationally recognized best practices;
- c) for developing organization-specific information security management guidelines.

2 Normative references

There are no normative references in this document.

koniec náhľadu – text ďalej pokračuje v platenej verzii STN