ČESKÁ TECHNICKÁ NORMA

ICS 35.030 **Duben**
2023

Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí –
Opatření informační bezpečnosti

ČSN
EN ISO/IEC 27002

36 9798

idt ISO/IEC 27002:2022

Information security, cybersecurity and privacy protection – Information security controls

Sécurité de l,information, cybersécurité et protection de la vie privée – Mesures de sécurité de l,information

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre – Informationssicherheitsmaßnahmen

Tato norma je českou verzí evropské normy EN ISO/IEC 27002:2022. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the European Standard EN ISO/IEC 27002:2022. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN EN ISO/IEC 27002 (36 9798) ze září 2014.

Národní předmluva

Změny proti předchozí normě

Název normy byl změněn. Byla změněna struktura normy, opatření jsou prezentována pomocí jednoduché taxonomie a souvisejících atributů. Některá opatření byla sloučena, některá opatření byla odstraněna a bylo zavedeno několik nových opatření. Úplná korespondence je uvedena v příloze B.

Souvisící ČSN

ČSN EN ISO 9000 (01 0300) Systémy managementu kvality – Základní principy a slovník

ČSN ISO 55001 (01 0376) Management aktiv – Systémy managementu – Požadavky

ČSN EN ISO/IEC 15408 (soubor) (36 9789) Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT

ČSN ISO 15489-1 (97 1500) Informace a dokumentace – Správa dokumentů – Část 1: Pojmy

a principy

ČSN ISO/IEC 17788 (36 9865) Informační technologie – Cloud computing – Přehled a slovník

ČSN ISO/IEC 17789 (36 9866) Informační technologie – Cloud computing – Referenční architektura

ČSN ISO/IEC 19086 (soubor) (36 9867) Informační technologie – Cloud computing – Rámec dohody o úrovni služeb (SLA)

ČSN ISO/IEC 19770-1 (36 9043) Informační technologie – Správa aktiv IT – Část 1: Systémy správy aktiv IT – Požadavky

ČSN ISO/IEC 20889 (36 9039) Terminologie a klasifikace technik odstranění identifikace dat zvyšujících soukromí

ČSN ISO 21500 (01 0345) Management projektů, programů a portfolií – Kontext a koncepce

ČSN ISO 21502 (01 0346) Management projektů, programů a portfolií – Návod k managementu projektu

ČSN EN ISO 22301 (01 2306) Bezpečnost a odolnost – Systémy managementu kontinuity podnikání – Požadavky

ČSN EN ISO 22313 (01 2316) Bezpečnost a odolnost – Systémy managementu kontinuity podnikání – Pokyny pro používání ISO 22301

ČSN EN ISO/IEC 24760 (soubor) (36 9716) Bezpečnost IT a soukromí – Rámec pro řízení identit

ČSN EN ISO/IEC 27001:2014 (36 9797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky

ČSN EN ISO/IEC 27007 (36 9790) Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Směrnice pro audit systémů řízení bezpečnosti informací

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

ČSN EN ISO/IEC 27017 (36 9710) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002

ČSN EN ISO/IEC 27018 (36 9709) Informační technologie – Bezpečnostní techniky – Soubor postupů na ochranu osobně identifikovatelných informací (PII) ve veřejných cloudech vystupujících jako zpracovatelé PII

ČSN EN ISO/IEC 27019 (36 9719) Informační technologie – Bezpečnostní techniky – Opatření bezpečnosti infor-
mací pro energetický průmysl

ČSN ISO/IEC 27031 (36 9801) Informační technologie – Bezpečnostní techniky – Směrnice pro připravenost informačních a komunikačních technologií pro kontinuitu činnosti organizace

ČSN ISO/IEC 27033 (soubor) (36 9701) Informační technologie – Bezpečnostní techniky – Bezpečnost sítě

ČSN ISO/IEC 27034-1 (36 9703) Informační technologie – Bezpečnostní techniky – Bezpečnost aplikací – Část 1: Přehled a pojmy

ČSN ISO/IEC 27035-1 (36 9799) Informační technologie – Bezpečnostní techniky – Řízení incidentů bezpečnosti informací – Část 1: Principy řízení incidentů

ČSN ISO/IEC 27035-2 (36 9799) Informační technologie – Bezpečnostní techniky – Řízení incidentů bezpečnosti informací – Část 2: Směrnice pro plánování a přípravu odezvy na incidenty

ČSN EN ISO/IEC 27037 (36 9846) Informační technologie – Bezpečnostní techniky – Směrnice pro identifikaci, sběr, získávání a uchovávání digitálních důkazů

ČSN EN ISO/IEC 27040 (36 9849) Informační technologie – Bezpečnostní techniky – Zabezpečení úložišť dat

ČSN P ISO/IEC TS 27110 (36 9773) Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Směrnice pro vývoj rámce kybernetické bezpečnosti

ČSN EN ISO/IEC 27701 (36 9770) Bezpečnostní techniky – Rozšíření ISO/IEC 27001 a ISO/IEC 27002 pro řízení ochrany soukromí – Požadavky a směrnice

ČSN EN ISO 27799 (98 2021) Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002

ČSN EN ISO/IEC 29100 (36 9705) Informační technologie – Bezpečnostní techniky – Rámec soukromí

ČSN EN ISO/IEC 29134 (36 9712) Informační technologie – Bezpečnostní techniky – Směrnice pro posuzování dopadu na soukromí

ČSN EN ISO/IEC 29147 (36 9713) Informační technologie – Bezpečnostní techniky – Odhalování zranitelností

ČSN EN ISO/IEC 30111 (36 9706) Informační technologie – Bezpečnostní techniky – Postupy zacházení se zranitelnostmi

ČSN ISO 31000:2018 (01 0351) Management rizik – Směrnice

ČSN EN IEC 31010 ed. 2 (01 0352) Management rizik – Techniky posuzování rizik

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článku „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).

Vysvětlivky k textu převzaté normy

Pro účely této normy je překlad anglického termínu „management“ ponechán v původním tvaru, s ohledem na kontext, v jakém je v textu normy použit.

Upozornění na národní poznámky

Do článků 5.19 a 5.22 a do tabulky A.1 byly doplněny vysvětlující národní poznámky.

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.

EVROPSKÁ NORMA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27002

Listopad 2022

ICS 35.030

Nahrazuje
EN ISO/IEC 27002:2017

Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační 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)

Tato evropská norma byla schválena CEN dne 2022-10-30.

Členové CEN a CENELEC jsou povinni splnit vnitřní předpisy CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se této evropské normě bez jakýchkoliv modifikací uděluje status národní normy. Aktualizované seznamy a bibliografické citace týkající se těchto národních norem lze obdržet na vyžádání v Řídicím centru
CEN-CENELEC nebo u kteréhokoliv člena CEN a CENELEC.

Tato evropská norma existuje ve třech oficiálních verzích (anglické, francouzské, německé). Verze v každém
jiném jazyce přeložená členem CEN a CENELEC do jeho vlastního jazyka, za kterou zodpovídá a kterou notifikuje Řídicímu centru CEN-CENELEC, má stejný status jako oficiální verze.

Členy CEN a CENELEC jsou národní normalizační orgány a národní elektrotechnické komise Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Republiky
Severní Makedonie, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Srbska, Španělska, Švédska, Švýcarska a Turecka.

Řídicí centrum CEN-CENELEC
Rue de la Science 23, B-1040 Brusel

Evropská předmluva

Text ISO/IEC 27002:2022 vypracovala technická komise ISO/IEC JTC 1 *Informační technologie* Mezinárodní
organizace pro normalizaci (ISO) a byl převzat jako EN ISO/IEC 27002:2022 technickou komisí CEN-CENELEC/JTC 13 *Kybernetická bezpečnost a ochrana dat*, jejímž sekretariátem je DIN.

Této evropské normě je nutno nejpozději do května 2023 udělit status národní normy, a to buď vydáním identického textu, nebo schválením k přímému používání, a národní normy, které jsou s ní v rozporu, je nutno zrušit nejpozději do května 2023.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv.
CEN-CENELEC nelze činit odpovědným za identifikaci jakéhokoliv nebo všech patentových práv.

Tento dokument nahrazuje EN ISO/IEC 27002:2017.

Jakákoli zpětná vazba a otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na webových stránkách CEN a CENELEC.

Podle vnitřních předpisů CEN-CENELEC jsou tuto evropskou normu povinny zavést národní normalizační organizace následujících zemí: Belgie, Bulharska, České republiky, Dánska, Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska, Maďarska, Malty, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Republiky Severní Makedonie, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Srbska, Španělska, Švédska, Švýcarska a Turecka.

Oznámení o schválení

Text ISO/IEC 27002:2022 byl schválen CEN-CENELEC jako EN ISO/IEC 27002:2022 bez jakýchkoliv modifikací.

Obsah

Strana

Strana

Strana

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) tvoří specializovaný systém celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím svých technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oborech společného zájmu. Práce se zúčastňují také další vládní i nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk.

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

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnými 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 obdržených ISO (viz www.iso.org/patents) nebo v seznamu patentových prohlášení obdržených IEC (viz patents.iec.ch).

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), viz www.iso.org/iso/foreword.html. V IEC viz www.iec.ch/understanding-standards.

Tento dokument vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie,* subkomise SC 27 *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí.*

Toto třetí vydání zrušuje a nahrazuje druhé vydání (ISO/IEC 27002:2013), které bylo technicky zrevidováno. To zahrnuje také technické opravy ISO/IEC 27002:2013/Cor. 1:2014 a ISO/IEC 27002:2013/Cor. 2:2015.

Hlavní změny jsou:

- název byl změněn;
- struktura dokumentu byla změněna, opatření jsou prezentována pomocí jednoduché taxonomie a souvisejících atributů;
- některá opatření byla sloučena, některá odstraněna a bylo zavedeno několik nových opatření. Úplnou korespondenci lze nalézt v příloze B.

Jakákoli zpětná vazba nebo otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na www.iso.org/members.html a www.iec.ch/national-committees.

Úvod

0.1 Pozadí a kontext

Tento dokument je určen pro organizace všech typů a velikostí. Slouží jako reference pro určení a zavedení opatření pro ošetření rizik informační bezpečnosti v systému managementu informační bezpečnosti (ISMS) založeném na ISO/IEC 27001. Může být také použit jako pokyny pro organizace, které stanovují a zavádějí obecně uznávaná opatření informační bezpečnosti. Kromě toho je tento dokument určen k použití při vytváření směrnic pro management informační bezpečnosti specifických pro dané odvětví a organizaci, přičemž se zohlední jejich specifické prostředí (specifická prostředí) pro management rizik informační bezpečnosti. Jiná opatření specifická pro organizaci nebo prostředí než ta, která jsou obsažena v tomto dokumentu, mohou být podle potřeby stanovena na základě posouzení rizik.

Organizace všech typů a velikostí (včetně veřejného a soukromého sektoru, komerčních a neziskových organizací) vytvářejí, shromažďují, zpracovávají, ukládají, přenášejí a likvidují informace v mnoha formách, včetně elektronických, fyzických a verbálních (např. rozhovory a prezentace).

Hodnota informací přesahuje psaná slova, čísla a obrázky: znalosti, koncepty, nápady a značky jsou příklady nehmotných forem informací. V propojeném světě si informace a další související aktiva zaslouží nebo vyžadují ochranu před různými zdroji rizik, ať už přírodními, náhodnými nebo úmyslnými.

Informační bezpečnosti je dosaženo zavedením vhodného souboru opatření, včetně politik, pravidel, procesů, postupů, organizačních struktur a funkcí softwaru a hardwaru. Aby organizace splnila své specifické cíle bezpečnosti a činnosti, má tato opatření definovat, zavést, monitorovat, přezkoumávat a v případě potřeby zlepšovat. Systém ISMS, jako je systém specifikovaný v ISO/IEC 27001, zaujímá holistický, koordinovaný pohled na rizika informační bezpečnosti organizace s cílem určit a zavést komplexní soubor opatření informační bezpečnosti v celkovém rámci koherentního systému managementu.

Mnoho informačních systémů, včetně jejich managementu a provozu, nebylo navrženo tak, aby byly bezpečné z hlediska ISMS, jak je specifikováno v ISO/IEC 27001 a v tomto dokumentu. Úroveň bezpečnosti, které je možné dosáhnout pouze technologickými opatřeními, je omezená a má být podpořena vhodnými řídicími činnostmi a organizačními procesy. Určení, která opatření mají být zavedena, vyžaduje pečlivé plánování a pozornost věnovanou detailům při ošetření rizik.

Úspěšný ISMS vyžaduje podporu všech pracovníků organizace. Může také vyžadovat účast dalších zainteresovaných stran, jako jsou akcionáři nebo dodavatelé. Může být také zapotřebí poradenství od odborníků na danou problematiku.

Vhodný, přiměřený a efektivní systém managementu informační bezpečnosti poskytuje vedení organizace a dalším zainteresovaným stranám záruku, že jejich informace a další související aktiva jsou přiměřeně zabezpečeny a chráněny před hrozbami a škodami, což organizaci umožňuje dosáhnout stanovených cílů vyplývajících z činnosti organizace.

0.2 Požadavky informační bezpečnosti

Je nezbytné, aby organizace stanovila své požadavky na informační bezpečnost. Existují tři hlavní zdroje požadavků na informační bezpečnost:

a) posouzení rizik organizace s přihlédnutím k celkové strategii a cílům organizace vyplývajících z činnosti organizace. To je možné usnadnit nebo podpořit prostřednictvím posouzení rizik specifických pro informační bezpečnost. Výsledkem má být stanovení opatření nezbytných k zajištění toho, aby zbytkové riziko pro organizaci splňovalo její kritéria přijatelnosti rizik;

b) zákonné, statutární, regulatorní a smluvní požadavky, které musí organizace a její zainteresované strany (obchodní partneři, poskytovatelé služeb atd.) splňovat, a jejich sociokulturní prostředí;

c) soubor zásad, cílů a požadavků vyplývajících z činnosti organizace pro všechny kroky životního cyklu informací, které organizace vytvořila pro podporu svého provozu.

0.3 Opatření

Opatření je definováno jako kroky, které modifikují nebo zachovávají riziko. Některá opatření v tomto dokumentu jsou opatření, která riziko modifikují, zatímco jiná riziko zachovávají. Například politika informační bezpečnosti může riziko pouze zachovávat, zatímco dodržování politiky informační bezpečnosti může riziko modifikovat. Některá opatření navíc popisují stejné obecné opatření v různých kontextech rizika. Tento dokument poskytuje obecnou směsici organizačních, personálních, fyzických a technologických opatření informační bezpečnosti odvozených z mezinárodně uznávaných osvědčených postupů.

0.4 Stanovení opatření

Stanovení opatření závisí na rozhodnutích organizace po posouzení rizik s jasně definovaným rozsahem. Rozhodnutí týkající se identifikovaných rizik mají vycházet z kritérií pro přijatelnost rizika, možností ošetření rizika a přístupu k managementu rizik uplatňovaného organizací. Stanovení opatření má rovněž zohlednit všechny
relevantní národní a mezinárodní právní předpisy a nařízení. Stanovení opatření závisí také na způsobu, jakým se opatření vzájemně ovlivňují, aby poskytovaly hloubkovou ochranu.

Organizace může navrhnout opatření podle potřeby nebo je identifikovat z libovolného zdroje. Při specifikaci
takových opatření má organizace zvážit zdroje a investice potřebné k zavedení a provozování opatření v porovnání s realizovanou hodnotou ve vztahu k činnosti organizace. Viz ISO/IEC TR 27016 pro pokyny k rozhodování
o investicích do ISMS a ekonomické důsledky těchto rozhodnutí s ohledem na konkurenční požadavky na zdroje.

Má existovat rovnováha mezi prostředky vynaloženými na zavedení opatření a potenciálním dopadem na činnosti organizace v důsledku bezpečnostních incidentů při absenci těchto opatření. Výsledky posouzení rizik mají pomoci směrovat a určit vhodné kroky vedení, priority pro management rizik informační bezpečnosti a pro zavedení opatření určených jako nezbytné k ochraně před těmito riziky.

Některá z opatření v tomto dokumentu mohou být považována za hlavní zásady pro management informační bezpečnosti a za použitelné pro většinu organizací. Více informací o určování opatření a dalších možnostech ošetření rizik lze nalézt v ISO/IEC 27005.

0.5 Vypracování směrnic specifických pro organizaci

Tento dokument může být považován za výchozí bod pro vypracování směrnic specifických pro danou organizaci. Ne všechna opatření a pokyny uvedené v tomto dokumentu mohou být použitelné pro všechny organizace. K řešení specifických potřeb organizace a identifikovaných rizik mohou být zapotřebí i další opatření a směrnice, které nejsou v tomto dokumentu zahrnuty. Pokud jsou vypracovány dokumenty obsahující další směrnice nebo opatření, může být pro budoucí použití užitečné zahrnout křížové odkazy na články v tomto dokumentu.

0.6 Zohlednění životního cyklu

Informace má svůj životní cyklus, od vytvoření až po likvidaci. Hodnota informací a rizika pro ně se mohou v průběhu tohoto životního cyklu měnit (např. neoprávněné vyzrazení nebo odcizení finančních účtů společnosti není po jejich zveřejnění významné, ale integrita zůstává kritická), proto zůstává informační bezpečnost do určité míry důležitá ve všech fázích.

Informační systémy a další aktiva související s informační bezpečností mají životní cykly, v jejichž rámci jsou koncipovány, specifikovány, navrhovány, vyvíjeny, testovány, zaváděny, používány, udržovány a nakonec vyřazovány z provozu a likvidovány. Informační bezpečnost má být zohledněna v každé fázi. Projekty vývoje nových systémů a změny stávajících systémů poskytují příležitosti ke zlepšení opatření bezpečnosti a zároveň zohledňují rizika organizace a zkušenosti získané
z incidentů.

0.7 Související mezinárodní normy

Zatímco tento dokument nabízí pokyny k široké škále opatření informační bezpečnosti, které se běžně používají v mnoha různých organizacích, další dokumenty z řady ISO/IEC 27000 poskytují

doplňující rady nebo požadavky týkající se dalších aspektů celkového procesu managementu informační bezpečnosti.

Obecný úvod k ISMS a řadě dokumentů naleznete v ISO/IEC 27000. ISO/IEC 27000 obsahuje slovník, který definuje většinu termínů používaných v celé řadě dokumentů ISO/IEC 27000, a popisuje rozsah a cíle každého člena této řady.

Existují normy specifické pro odvětví, které obsahují další opatření zaměřené na konkrétní oblasti (např. ISO/IEC 27017 pro cloudové služby, ISO/IEC 27701 pro ochranu soukromí, ISO/IEC 27019 pro energetiku, ISO/IEC 27011 pro telekomunikační organizace a ISO 27799 pro zdravotnictví). Tyto normy jsou zahrnuty v bibliografii a na některé z nich se odkazuje v oddílech s pokyny a dalšími informacemi v kapitolách 5 až 8.

1 Předmět normy

Tento dokument poskytuje referenční soubor obecných opatření informační bezpečnosti včetně pokynů k implementaci. Tento dokument je určen k použití organizacemi:

a) v rámci systému managementu informační bezpečnosti (ISMS) založeném na ISO/IEC 27001;

b) pro zavádění opatření informační bezpečnosti založených na mezinárodně uznávaných osvědčených postupech;

c) pro vypracování směrnic pro management informační bezpečnosti specifických pro organizaci.