ISO/IEC 27001:2005

Information Security Management Systems

Information technology - Security techniques - Information security management systems - Requirements

Překlad a interpretace pro české prostředí

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 technických komisí zřízených příslušnou organizací k tomu, aby se zabývaly určitou oblastí technické činnosti. V oblastech společného zájmu technické komise ISO a IEC spolupracují. Práce se zúčastňují i jiné mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informačních technologií zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou zpracovány v souladu s pravidly uvedenými v části 2 Směrnic ISO/IEC.

Hlavním úkolem společné technické komise je připravovat mezinárodní normy. Návrhy mezinárodních norem přijaté společnou technickou komisí se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Pozornost je třeba věnovat možnosti, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nenesou odpovědnost za identifikaci všech patentových práv nebo kteréhokoliv z nich.

Mezinárodní norma ISO/IEC 27001 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Information technology*, subkomise SC 27, *IT Security techniques*.

0 Úvod

1.1 Všeobecně

Tato mezinárodní norma byla připravena proto, aby poskytla podporu pro ustavení, zavedení, provozování, monitorování, udržování a zlepšování systému řízení bezpečnosti informací (Information Security Management Systems nebo ISMS). Přijetí ISMS by mělo být strategickým rozhodnutím organizace. Návrh a zavedení ISMS v organizaci je podmíněno potřebami a cíli činností (business) organizace a z toho vyplývajících požadavků na bezpečnost, dále pak používanými procesy a velikostí a strukturou organizace. Všechny tyto a jejich podpůrné systémy podléhají změnám v čase. Předpokládá se, že jednoduché situace vyžadují jednoduchá řešení ISMS.

Tuto normu mohou využívat interní i externí subjekty, včetně certifikačních orgánů, k hodnocení schopnosti organizace splnit vlastní požadavky, stejně jako požadavky dané zákonem nebo požadavky zákazníků.

1.2 Procesní přístup

Tato mezinárodní norma prosazuje přijetí procesního přístupu pro ustavení, zavedení, provozování, monitorování, udržování a zlepšování efektivnosti ISMS v organizaci.

Aby organizace fungovala efektivně, musí pojmenovat a řídit mnoho vzájemně propojených činností. Činnost, která využívá zdroje a je řízena za účelem přeměny vstupů na výstupy, může být považována za proces. Výstup z jednoho procesu často přímo tvoří vstup pro následující proces.

Aplikace systému procesů v organizaci, spolu s identifikací těchto procesů, jejich vzájemným působením a řízením může být označováno jako "procesní přístup".

Při použití procesního přístupu tak, jak je prezentován v této normě, je kladen důraz na:

a) pochopení požadavků na bezpečnost informací a potřebu stanovení politiky a cílů bezpečnosti informací;

b) zavedení a provádění kontrol v kontextu s řízením celkových rizik činností organizace;

c) monitorování a přezkoumání funkčnosti a efektivnosti ISMS;

d) neustálé zlepšování založené na objektivním měření.

Model známý jako "Plánuj-Dělej-Kontroluj-Jednej" (Plan-Do-Check-Act nebo PDCA) může být aplikován na všechny procesy ISMS tak, jak jsou zavedeny touto normou. Obrázek 1 znázorňuje, jak ISMS přijímá požadavky bezpečnosti informací a očekávání zainteresovaných stran jako vstup, a jak pomocí nezbytných činností a procesů vytváří výstupy bezpečnosti informací (např. řízenou bezpečnost informací), které splňují tyto požadavky a očekávání.

Obrázek 1 také znázorňuje propojení procesů uvedených v kapitolách 4, 5, 6, 7 a 8.

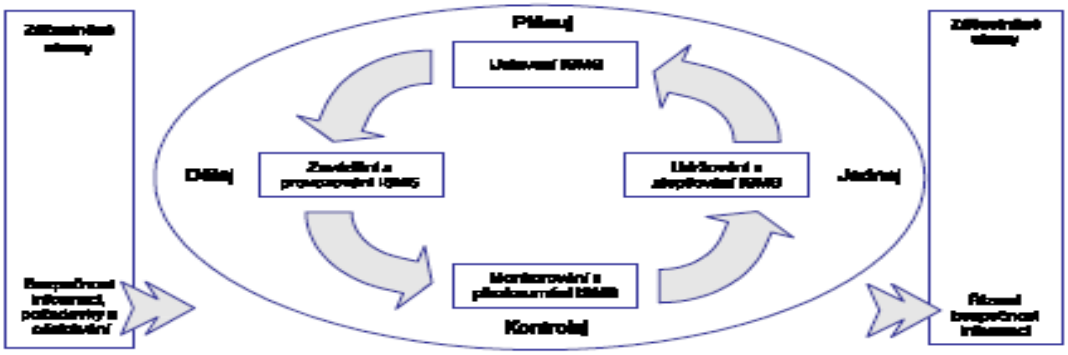
Zavedení modelu PDCA bude také odrážet principy, které jsou definovány ve směrnici OECD (2002)1 pro řízení bezpečnosti informačních systémů a sítí. Norma ISO/IEC 27001 poskytuje celistvý model pro zavedení principů definovaných v této směrnici, které upravují hodnocení rizik, návrh a zavedení bezpečnosti, řízení bezpečnosti a opětovné hodnocení bezpečnosti.

PŘÍKLAD 1

Může být například požadováno, aby v případě narušení bezpečnosti nebyly způsobeny organizaci vážné finanční škody ani jiné těžkosti (např. ztráta image).

PŘÍKLAD 2

Vyskytne-li se závažný incident, například napadení (hacking) eBusiness systému organizace (web site) očekává se, že pro minimalizaci dopadů incidentu budou k dispozici dostatečně vyškolení zaměstnanci.



Obrázek 1- PDCA model aplikovaný na procesy ISMS

Plánuj (ustavení ISMS)	Ustavení politiky ISMS, cílů, procesů a postupů souvisejících s řízením rizik a zlepšováním bezpečnosti informací tak, aby poskytovaly výsledky v souladu s celkovou politikou a cíli organizace.
Dělej (zavádění a provozování ISMS)	Zavedení a využívání politiky ISMS, opatření, procesů a postupů.
Kontroluj (monitorování a přezkoumání ISMS)	Posouzení, kde je to možné i měření výkonu procesu (resp. jeho funkčnosti a efektivnosti) vůči politice ISMS, cílům a praktickým zkušenostem a hlášení výsledků vedení organizace k přezkoumání.
Jednej (udržování a zlepšování ISMS)	Provedení opatření k nápravě a preventivních opatření, založených na výsledcích interního auditu ISMS a přezkoumání systému řízení ze strany vedení organizace tak, aby bylo dosaženo neustálého zlepšování ISMS.

1.3 Kompatibilita s jinými systémy řízení

Tato mezinárodní norma je propojena s normami ISO 9001:2000 a ISO 14001:2004 tak, aby bylo podpořeno jejich konzistentní a jednotné zavedení a provoz. Jeden vhodně navržený systém řízení tak může naplnit požadavky všech tří norem. Tabulka C.1 znázorňuje vztah mezi kapitolami ISO 27001:2005, ISO 9001:2000 a ISO 14001:2004.

Tato norma je navržena tak, aby organizaci umožnila propojit nebo integrovat ISMS s odpovídajícími požadavky systémů řízení.

Informační technologie – Bezpečnostní techniky – Sytém řízení bezpečnosti informací – Požadavky

Důležité upozornění

Tato publikace nemůže obsáhnout všechna opatření z oblasti jejího určení. Uživatelé jsou sami odpovědni za její správné použití. Shoda s normou sama o sobě nezbavuje organizaci odpovědnosti za splnění závazků vyplývajících ze zákona.

1 Působnost

1.1 Všeobecně

Tato mezinárodní norma je použitelná pro všechny typy organizací (např. komerční organizace, státní organizace a úřady, neziskové organizace). Norma specifikuje požadavky na ustavení, zavedení, provoz, monitorování, přezkoumání, udržování a zlepšování dokumentovaného ISMS v kontextu celkových rizik činností organizace. Specifikuje požadavky na zavedení bezpečnostních opatření, upravených podle potřeb jednotlivých organizací nebo jejich částí. ISMS je navržen tak, aby zajistil odpovídající a přiměřená bezpečnostní opatření, adekvátně chránící informační aktiva a poskytující odpovídající jistotu klientům a dalším zainteresovaným stranám2.

POZNÁMKA 1

Slovo „business" je v textu normy překládáno jako „činnost organizace", v kontextu celé normy jsou činnostmi organizace myšleny veškeré aktivity, které jsou důležité pro existenci organizace a naplňování jejích cílů.

POZNÁMKA 2

ISO/IEC 17799 poskytuje doporučení, která mohou být použita při návrhu a realizaci jednotlivých opatření.

1.2 Použití

Požadavky této normy jsou obecně použitelné a jsou aplikovatelné ve všech organizacích bez ohledu na jejich typ, velikost a povahu činností. **Vyřazení jakýchkoli požadavků specifikovaných v odstavcích 4, 5, 6, 7 a 8 je v případě, že chce organizace dosáhnout souladu s touto normou, nepřijatelné.**

Jakékoliv vyřazení opatření, která byla identifikována jako nezbytná pro snížení rizik na akceptovatelnou úroveň3, musí být opodstatněno a musí být doloženo, že rizika s tím spojená byla akceptována odpovědnými osobami. Tam, kde se tato vyřazení provedou, lze akceptovat nároky na soulad s touto normou, jedině pokud tato vyřazení neovlivní schopnost a/nebo odpovědnost organizace zajistit bezpečnost informací v souladu s bezpečnostními požadavky stanovenými analýzou rizik a odpovídajícími zákonnými a regulatorními požadavky.

POZNÁMKA

V případech, kdy má organizace již zaveden systém řízení (např. podle ISO 9001 nebo ISO 14001), je ve většině případů vhodné implementovat požadavky této normy v rámci existujícího

systému.

2 Normativní odkazy

Pro použití tohoto dokumentu jsou nezbytné odkazy na následující dokumenty. U datovaných odkazů připadají v úvahu pouze uvedená vydání. U nedatovaných odkazů je myšleno jejich poslední vydání.

ISO/IEC 17799:2005, Information technology – Security techniques – Code of practice for information security management

(Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací.)

3 Termíny a definice

Pro účely tohoto dokumentu jsou platné následující definice.

3.1

aktivum (asset)

cokoliv, co má pro organizaci nějakou hodnotu

[ISO/IEC 13335-1:2004]

3.2

dostupnost (availability)

zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby

[ISO/IEC 13335-1:2004]

3.3

důvěrnost (confidentiality)

zajištění, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni

[ISO/IEC 13335-1:2004]

3.4

bezpečnost informací (information security)

zachování důvěrnosti, integrity a dostupnosti informací a s nimi spojené priority např. autentičnost, odpovědnost, nepopiratelnost a hodnověrnost

[ISO/IEC 17799:2005]

3.5

bezpečnostní událost (information security event)

bezpečnostní událost je identifikovaný stav systému, služby nebo sítě, ukazující na možné porušení bezpečnostní politiky, nebo selhání bezpečnostních opatření. Může se také jednat o jinou předtím nenastalou situaci, která může být důležitá z pohledu bezpečnosti informací

[ISO/IEC TR 18044:2004]

3.6

bezpečnostní incident (information security incident)

bezpečnostní incident je jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činností organizace a ohrožení bezpečnosti informací

3.7

systém řízení bezpečnosti informací ISMS (information security management system)

část celkového systému řízení organizace, založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustavení, zavádění, provoz, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací

POZNÁMKA

Systém řízení zahrnuje organizační strukturu, politiky, plánovací činnosti, odpovědnosti, praktiky, postupy, procesy a zdroje.

3.8

integrita (integrity)

zajištění správnosti a úplnosti informací

[ISO/IEC 13335-1:2004]

3.9

zbytkové riziko (residual risk)

riziko, které zůstane po implementaci bezpečnostních opatření

[ISO/IEC Guide 73:2002]

3.10

akceptace rizika (risk acceptance)

rozhodnutí přijmout riziko

[ISO/IEC Guide 73:2002]

3.11

analýza rizik (risk analysis)

systematické používání informací k odhadu rizika a k určení jeho zdrojů

[ISO/IEC Guide 73:2002]

3.12

hodnocení rizik (risk assessment)

celkový proces analýzy a vyhodnocení rizik

[ISO/IEC Guide 73:2002]

3.13

vyhodnocení rizik (risk evaluation)

proces porovnávání odhadnutého rizika vůči daným kritériím pro určení jeho významu

[ISO/IEC Guide 73:2002]

3.14

řízení rizik (risk management)

koordinované činnosti sloužící k řízení a kontrole organizace s ohledem na rizika

[ISO/IEC Guide 73:2002]

POZNÁMKA

Řízení rizik zpravidla zahrnuje hodnocení rizik, zvládání rizik, akceptaci a seznámení s rizikem

3.15

zvládání rizik (risk treatment)
proces výběru a přijímání opatření pro změnu rizika
[ISO/IEC Guide 73:2002]

3.16

prohlášení o aplikovatelnosti (statement of applicability)
dokumentované prohlášení popisující cíle opatření a jednotlivá bezpečnostní opatření, která jsou relevantní a aplikovatelná v rámci ISMS organizace

POZNÁMKA

Cíle opatření a jednotlivá bezpečnostní opatření jsou založena na výsledcích a závěrech procesů hodnocení a zvládání rizik, legislativních a regulatorních požadavcích, smluvních závazcích a požadavcích organizace na bezpečnost informací.

4 Systém řízení bezpečnosti informací

4.1 Všeobecné požadavky

Organizace musí ustavit, zavést, provozovat, monitorovat, přezkoumávat, udržovat a soustavně zlepšovat dokumentovaný ISMS organizace, a to v kontextu všech činností a rizik. Použitý proces je, pro účely této normy, založen na modelu PDCA znázorněném na obrázku č.1.

4.2 Ustavení a řízení ISMS

4.2.1 Ustavení ISMS

Organizace musí provést následující.

a) Definovat rozsah a hranice ISMS na základě posouzení specifických rysů činností organizace, jejího uspořádání, struktury, umístění (lokality), aktiv a technologií, včetně důvodů pro vyjmutí z rozsahu ISMS (viz 1.2).

b) Definovat politiku ISMS na základě posouzení specifických rysů činností organizace, její struktury, umístění aktiv a technologií, která:

1. zahrnuje rámec pro stanovení jejích cílů a ustavuje celkový směr řízení a rámec zásad činností týkající se bezpečnosti informací;
2. bere v úvahu požadavky vyplývající z činností organizace a legislativní nebo regulatorní požadavky a smluvní bezpečnostní závazky;
3. pro vybudování a údržbu ISMS vytváří potřebné vazby na prostředí, tedy na strategii organizace, její organizační strukturu a proces řízení rizik;
4. stanovuje kritéria, kterými bude hodnoceno riziko [viz 4.2.1 c)];
5. byla schválena vedením.

POZNÁMKA

Pro účely této normy je politika ISMS považována za nadřazenou bezpečnostní politice organizace. Obě politiky mohou být součástí jednoho dokumentu.

c) Definovat systematický přístup k hodnocení rizik.

1. Určit metodiku hodnocení rizik, která vyhovuje ISMS a stanovené bezpečnosti informací, legislativním a regulatorním požadavkům.
2. Určit kritéria pro akceptaci rizik a pro definování jejich akceptační úrovně [viz 5.1 f)].

Vybraná metodika hodnocení rizik musí zajistit, že jsou výsledky hodnocení rizik porovnatelné a reprodukovatelné.

POZNÁMKA

Pro hodnocení rizik existuje řada různých metodik. Příklady metodik pro hodnocení rizik lze nalézt v normě ISO/IEC TR 13335-34, *Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security*.

d) Identifikovat rizika.

1. Identifikovat aktiva v rámci rozsahu ISMS a jejich vlastníky5.
2. Identifikovat hrozby pro tato aktiva.
3. Identifikovat zranitelnosti, které by mohly být hrozbami využity.
4. Identifikovat, jaké dopady na aktiva by mohla mít ztráta důvěrnosti, integrity a dostupnosti.

e) Analyzovat a vyhodnocovat rizika.

1. Ohodnotit dopady na činnost organizace, které by mohly vyplynout ze selhání bezpečnosti s tím, že vezme v úvahu případné následky ztráty důvěrnosti, integrity nebo dostupnosti aktiv.
2. Ohodnotit reálnou pravděpodobnost selhání bezpečnosti, které by se mohlo vyskytnout působením existujících hrozeb a zranitelností a dopady na konkrétní aktiva s přihlédnutím k aktuálně zavedeným opatřením.
3. Odhadnout úrovně rizik.
4. Určit, zda je riziko akceptovatelné nebo vyžaduje zvládání podle kritérií stanovených v 4.2.1c)2).

f) Identifikovat a vyhodnotit varianty pro zvládání rizik.

Možné činnosti zahrnují:

1. aplikování vhodných opatření;
2. vědomé a objektivní akceptování rizik za předpokladu, že naplňují politiku organizace a kritéria pro akceptaci rizik [viz 4.2.1c)2)];
3. vyhnutí se rizikům;
4. přenesení rizik spojených s činností organizace na třetí strany, např. na pojišťovny, dodavatele.

g) Vybrat cíle opatření a jednotlivá bezpečnostní opatření pro zvládání rizik.

Z přílohy A této normy musí být vybrány a implementovány vhodné cíle opatření a jednotlivá bezpečnostní opatření a tento výběr musí být zdůvodněn na základě výsledků procesů hodnocení a zvládání rizik. Při výběru musí být zohledněna kritéria pro akceptaci rizik [viz 4.2.1c)], stejně tak jako legislativní, regulatorní a smluvní požadavky.

Cíle opatření a jednotlivá bezpečnostní opatření uvedená v příloze A nejsou vyčerpávající, mohou tedy být vybrány i další cíle opatření a jednotlivá opatření.

POZNÁMKA

Příloha A obsahuje ucelený seznam cílů opatření a jednotlivých bezpečnostních opatření, které byly shledány jako obecně použitelné pro všechny typy organizací. Seznam poskytuje uživatelům důležité vodítko pro zajištění toho, aby nebyla opomenuta nebo přehlédnuta žádná z důležitých opatření.

h) Získat souhlas vedení organizace s navrhovanými zbytkovými riziky.

i) Získat povolení ze strany vedení organizace k zavedení a provozu ISMS.

j) Připravit Prohlášení o aplikovatelnosti.

Prohlášení o aplikovatelnosti musí obsahovat následující:

1. cíle opatření a jednotlivá bezpečnostní opatření vybrané v 4.2.1g) a důvody pro jejich výběr;
2. cíle opatření a jednotlivá bezpečnostní opatření, která jsou již v organizaci implementována [viz 4.2.1e)2)];
3. vyřazené cíle opatření a jednotlivá vyřazená bezpečnostní opatření uvedená v příloze A, včetně zdůvodnění pro jejich vyřazení.

POZNÁMKA

Prohlášení o aplikovatelnosti poskytuje souhrn rozhodnutí jakým způsobem bude naloženo s identifikovanými riziky. Zdůvodnění pro vyřazení cílů a jednotlivých opatření poskytuje zpětnou kontrolu zda nebyly vyřazeny omylem.

4.2.2 Zavádění a provozování ISMS

Organizace musí provést následující:

a) Formulovat plán zvládání rizik, který vymezí odpovídající řídící činnosti, zdroje, odpovědnosti a priority pro řízení rizik bezpečnosti informací (viz kapitola 5).

b) Zavést plán zvládání rizik tak, aby dosáhla určených cílů opatření, přičemž vezme v úvahu finanční a lidské zdroje a přiřazení rolí a odpovědností.

c) Zavést bezpečnostní opatření vybraná v 4.2.1 g) pro dosažení (naplnění) cílů těchto opatření.

d) Určit jakým způsobem bude měřit účinnost vybraných opatření nebo skupin opatření a stanovit jakým způsobem budou tato měření použita k vyhodnocení účinnosti opatření tak, aby závěry hodnocení byly porovnatelné a opakovatelné [viz 4.2.3c)].

POZNÁMKA

Měření účinnosti opatření poskytuje vedení organizace a zaměstnancům informaci o tom, jak jednotlivá opatření naplňují plánované cíle.

e) Zavést programy školení a programy zvyšování bezpečnostního povědomí (viz 5.2.2).

f) Řídit provoz ISMS.

g) Řídit zdroje ISMS (viz 5.2).

h) Zavést postupy a další opatření pro rychlou detekci a reakci na bezpečnostní události a postupy reakce na bezpečnostní incidenty [viz 4.2.3a)].

4.2.3 Monitorování a přezkoumání ISMS

Organizace musí provést následující:

a) Monitorovat, přezkoumávat a zavést další opatření:

1. pro včasnou detekci chyb zpracování;
2. pro včasnou detekci úspěšných i neúspěšných pokusů o narušení bezpečnosti a detekci bezpečnostních incidentů;
3. umožňující vedení organizace určit, zda bezpečnostní aktivity, prováděné pověřenými osobami nebo pro které byly implementovány technologie, fungují dle očekávání;
4. umožňující detekci bezpečnostních událostí a zabránění tak vzniku bezpečnostních incidentů;
5. umožňující vyhodnocení účinnosti činností podniknutých při narušení bezpečnosti.

b) Pravidelně přehodnocovat účinnost ISMS (včetně splnění politiky ISMS, cílů a analýzy bezpečnostních opatření) s ohledem na výsledky bezpečnostních auditů, incidentů, výsledků měření účinnosti opatření, návrhů a podnětů všech zainteresovaných stran.

c) Měřit účinnost zavedených opatření pro ověření toho, zda byly naplněny požadavky na bezpečnost.

d) V plánovaných intervalech provádět přezkoumání hodnocení rizik a přehodnocování úrovně zbytkového a akceptovatelného rizika s ohledem na změny:

1. organizace;
2. technologií;
3. cílů činností organizace a procesů;
4. identifikovaných hrozeb;
5. účinnosti zavedených opatření;
6. regulatorního a právního prostředí, změny vyplývající ze smluvních závazků, změny sociálního klima.

e) Provádět interní audity ISMS v plánovaných intervalech (viz kapitola 6).

POZNÁMKA

Interní audity jsou prováděny přímo organizací nebo externími auditory. Jejich cílem může být například prověření systému řízení před samotným certifikačním auditem.

f) Na úrovni vedení organizace pravidelně přehodnocovat ISMS, aby se zajistilo, že jeho rozsah je i nadále odpovídající, a že se daří nacházet možnosti zlepšení (viz 7.1).

g) Aktualizovat bezpečnostní plány s ohledem na nálezy zjištěné v rámci monitorování a přezkoumání.

h) Zaznamenávat všechny činnosti a události, které by mohly mít dopad na účinnost nebo výkon ISMS (viz 4.3.3).

4.2.4 Udržování a zlepšování ISMS

Organizace musí pravidelně provádět následující:
a) Zavádět identifikované možnosti vylepšení ISMS.
b) Provádět odpovídající nápravné a preventivní činnosti v souladu s 8.2 a 8.3 s využitím jak vlastních zkušeností v oblasti bezpečnosti, tak i zkušeností jiných organizací.
c) Projednávat činnosti a návrhy na zlepšení na požadované úrovni detailu se všemi zainteresovanými stranami a domluvit další postup.
d) Zaručit, že zlepšení dosáhnou předpokládaných cílů.

4.3 Požadavky na dokumentaci

4.3.1 Všeobecně

Dokumentace musí obsahovat záznamy o rozhodnutích učiněných vedením organizace. Veškeré činnosti musí být zpětně identifikovatelné v politikách a dohledatelné záznamech o rozhodnutí vedením. Veškeré činnosti musí být zaznamenány, aby se zajistila jejich opakovatelnost.
Je důležité mít zdokumentován, a na požádání doložit, vztah mezi vybranými opatřeními a závěry z procesů hodnocení a zvládání rizik a následně vazbu zpět na politiku a cíle ISMS.
Dokumentace ISMS musí obsahovat následující:
a) dokumentovaná prohlášení politiky a cílů ISMS [viz 4.2.1 b)];
b) rozsah ISMS [viz 4.2.1 a)];
c) postupy a opatření podporující ISMS;
d) popis použitých metodik hodnocení rizik [viz 4.2.1c)];
e) zprávu o hodnocení rizik [viz 4.2.1 c) až 4.2.1 g)];
f) plán zvládání rizik [viz 4.2.2 b)];
g) dokumentované postupy nezbytné pro zajištění efektivního plánování, provozu a řízení procesů bezpečnosti informací organizace a popis toho jakým způsobem je měřena účinnost zavedených opatření [viz 4.2.3c)];
h) záznamy vyžadované touto normou (viz 4.3.3);
i) prohlášení o aplikovatelnosti.

POZNÁMKA 1

Termín "dokumentovaný postup" v této normě znamená, že je tento postup vytvořen, dokumentován, zaveden a udržován.

POZNÁMKA 2

Rozsah dokumentace ISMS se může pro jednotlivé organizace lišit, závisí na:
- velikosti organizace a typu její činnosti;
- rozsahu a složitost systému jenž je řízen a požadavcích na bezpečnost.

POZNÁMKA 3

Dokumenty a záznamy mohou být v jakékoliv formě a na jakémkoliv nosiči.

4.3.2 Řízení dokumentů

Dokumenty požadované ISMS musí být chráněny a řízeny. Musí být vytvořen dokumentovaný postup tak, aby vymezil řídící činnosti potřebné k:
a) schvalování obsahu dokumentů před jejich vydáním;
b) přezkoumání dokumentů, popřípadě jejich aktualizaci a opakovanému schvalování;
c) zajištění identifikace změn dokumentů a aktuálního stavu revize dokumentů;
d) zajištění dostupnosti příslušných verzí aplikovatelných dokumentů v místech jejich používání;
e) zajištění čitelnosti a snadné identifikovatelnosti dokumentů;
f) zajištění dostupnosti dokumentů pro všechny, kteří je potřebují, zajištění přenášení, ukládání a likvidace dokumentů v souladu s postupy odpovídající jejich klasifikaci;
g) zajištění identifikace dokumentů externího původu;
h) zajištění řízené distribuce dokumentů;
i) zabránění neúmyslného použití zastaralých dokumentů;
j) aplikování jejich vhodné identifikace pro případ dalšího použití.

4.3.3 Řízení záznamů

Záznamy musí být vytvořeny a udržovány tak, aby poskytovaly důkaz o shodě s požadavky a o efektivním fungování ISMS. Záznamy musí být chráněny a řízeny. ISMS musí zohlednit všechny příslušné právní nebo regulatorní požadavky a smluvní závazky. Záznamy musí zůstat čitelné, snadno identifikovatelné a musí být možné je snadno vyhledat. Opatření potřebná k identifikaci, uložení, ochraně, vyhledání, době platnosti a uspořádání záznamů musí být dokumentována.
Musí být udržovány záznamy o fungování a efektivnosti procesu budování a řízení ISMS, jak je popsáno v kapitole 4.2. Dále musí být udržovány záznamy o všech výskytech bezpečnostních incidentů, vztahujících se k ISMS.

PŘÍKLAD

Příklady záznamů jsou návštěvní kniha, záznamy z auditu a záznam o autorizaci přístupu.

5 Odpovědnost vedení

5.1 Závazek vedení

Vedení organizace musí deklarovat svoji vůli k ustavení, zavedení, provozu, monitorování, přezkoumání, udržování a zlepšování ISMS tak, že:
a) ustanoví politiku ISMS;
b) zajistí stanovení cílů ISMS a plánu jejich dosažení;
c) stanoví role, povinnosti a odpovědnosti v oblasti bezpečnosti informací;
d) propaguje v rámci organizace význam plnění cílů bezpečnosti informací, jejich souladu s politikou bezpečnosti informací, plnění povinností vyplývajících ze zákona a potřebu soustavného zlepšování;
e) zajistí dostatečné zdroje pro ustavení, zavedení, provoz, monitorování, přezkoumání, údržbu a zlepšování ISMS (viz 5.2.1);
f) stanoví svým rozhodnutím akceptovatelnou úroveň rizika;
g) zajistí provádění interních auditů ISMS (viz kapitola 6);
h) provede přezkoumání ISMS (viz kapitola 7).

5.2 Řízení zdrojů

5.2.1 Zajištění zdrojů

Organizace musí určit a zajistit zdroje potřebné pro:
a) ustavení, zavedení, provoz, monitorování, přezkoumání, udržování a zlepšování ISMS;
b) zajištění podpory cílů činností organizace postupy bezpečnosti informací;
c) určení a věnování náležité pozornosti zákonným a regulatorním požadavkům a smluvním bezpečnostním závazkům;
d) udržování odpovídající úrovně bezpečnosti správnou aplikací všech zavedených opatření;
e) provedení přezkoumání podle potřeby a zajištění odpovídajících reakcí na jejich výsledky;
f) zlepšení efektivnosti ISMS podle potřeby.

5.2.2 Školení, vědomí závažnosti a odborná způsobilost

Organizace musí zajistit, aby zaměstnanci, kterých se týkají povinnosti určené v ISMS, byli kompetentní k výkonu požadovaných úkolů. Zajišťuje to pomocí:
a) určení nezbytných kompetencí personálu vykonávajícího práci ovlivňující ISMS;
b) zajištění odpovídajícího školení nebo podniknutí jiných kroků (např. zaměstnání kvalifikovaného personálu);
c) vyhodnocení efektivnosti zajištěného školení a provedených činností;
d) udržování záznamů o vzdělávání, školení, dovednostech, zkušenostech a kvalifikačních předpokladech (viz 4.3.3).
Organizace musí také zajistit, aby si byl veškerý příslušný personál vědom závažnosti a významu svých činností v rámci bezpečnosti informací a svého přínosu k dosažení cílů ISMS.

6 Interní audity ISMS

Organizace musí provádět interní audity ISMS v naplánovaných intervalech, aby zjistila, zda cíle opatření, jednotlivá bezpečnostní opatření, procesy a postupy ISMS:
a) vyhovují požadavkům této normy a odpovídající legislativě nebo regulatorním požadavkům;
b) vyhovují stanoveným požadavkům na bezpečnost informací;
c) jsou zavedeny a udržovány efektivně;
d) fungují tak, jak se očekává.
Program auditu musí být naplánován s ohledem na stav a význam auditovaných procesů a oblastí a s ohledem na výsledky předchozích auditů. Musí být definována kritéria auditů, jejich rozsah, četnost a metody. Výběr auditorů a vlastní provedení auditů musí zajistit objektivitu a nestrannost procesu auditu. Auditoři nesmí prověřovat svou vlastní práci.
Odpovědnosti a požadavky na plánování a provedení auditů, na hlášení výsledků a udržování záznamů (viz 4.3.3) musí být určeny dokumentovaným postupem.
Vedoucí zaměstnanci odpovědní za oblast, která je předmětem auditu musí zajistit, že kroky na odstranění zjištěných nedostatků jsou prováděny bez zbytečného odkladu. Tyto kroky musí obsahovat zpětnou kontrolu a hlášení o výsledcích této kontroly (viz kapitola 8).

POZNÁMKA

Norma ISO 190011:20026, *Guidelines for duality and/or environmental management systems auditing*, může být dobrým zdrojem doporučení jak provádět interní audity ISMS.

7 Přezkoumání ISMS vedením organizace

7.1 Všeobecně

Vedení organizace musí provádět přezkoumání ISMS organizace v naplánovaných intervalech (alespoň jednou za rok), aby zajistilo jeho permanentní účelnost, adekvátnost a efektivnost. Tato přezkoumání musí také hodnotit možnosti zlepšení a potřebu změn v ISMS, včetně bezpečnostní politiky a cílů bezpečnosti. Výsledky přezkoumání musí být jasně zdokumentovány a musí být o nich udržovány záznamy (viz 4.3.3).

7.2 Vstup pro přezkoumání

Vstupy pro přezkoumání vedením organizace musí zahrnovat informace o:
a) výsledcích auditů a přezkoumání ISMS;
b) zpětné vazbě od zainteresovaných stran;
c) technikách, produktech nebo postupech, které by mohly být použity v organizaci ke zlepšení výkonu a efektivnosti ISMS;
d) stavu preventivních opatření a stavu opatření k nápravě;
e) slabinách nebo hrozbách, jimž nebyla v rámci předchozích přezkoumání rizik věnována náležitá pozornost;
f) závěrech měření účinnosti zavedených opatření;
g) činnostech, které následovaly po předchozích přezkoumání vedením organizace (tj. vyplývaly z jeho závěrů);
h) změnách, které by mohly ovlivnit ISMS;
i) doporučeních pro zlepšování.

7.3 Výstup z přezkoumání

Výstupy přezkoumání prováděného vedením organizace musí zahrnovat jakákoli rozhodnutí a činnosti vztahující se k:
a) zvyšování efektivnosti ISMS;
b) aktualizaci hodnocení rizik a plánu zvládání rizik;
c) nezbytným změnám postupů bezpečnosti informací, v reakci na vnitřní nebo vnější události, které by mohly mít vliv na ISMS. Změny se mohou týkat:
1) požadavků spojených s činností organizace;
2) bezpečnostních požadavků;
3) procesů organizace ovlivňujících existující požadavky spojené s činností organizace;
4) regulatorních nebo zákonných požadavků;
5) smluvních závazků;
6) úrovní rizika a/nebo úrovní akceptovatelnosti rizika.
d) potřebě zdrojů;

e) zlepšování postupů měření účinnosti opatření.

8 Zlepšování ISMS

8.1 Soustavné zlepšování

Organizace musí neustále zvyšovat efektivnost ISMS s využitím politiky bezpečnosti informací, cílů bezpečnosti, výsledků auditu, analýz monitorovaných událostí, nápravných a preventivních akcí a přezkoumání prováděných vedením organizace (viz kapitola 7).

8.2 Opatření k nápravě

Organizace musí provést příslušné činnosti pro odstranění nedostatků spojených s implementací a provozem ISMS, aby zabránila jejich opětovnému výskytu. Zdokumentované postupy nápravných činností musí určit požadavky na:

a) identifikaci neshod v zavedení a/nebo provozu ISMS;
b) určení příčin neshod;
c) vyhodnocení potřeby opatření, kterým se zajistí, že se neshody znovu nevyskytnou;
d) určení a zavedení potřebných opatření k nápravě;
e) zaznamenání výsledků zavedených opatření (viz 4.3.3);
f) přezkoumání provedených nápravných opatření.

8.3 Preventivní opatření

Organizace musí určit opatření, která zabrání opakovanému výskytu neshod. Preventivní opatření musí být přiměřená závažnosti možných problémů. Zdokumentovaný postup aplikace preventivních činností musí definovat požadavky na:

a) identifikaci potenciálních neshod a jejich příčin;
b) vyhodnocení potřeby provedení činností k zamezení opětovnému výskytu neshod;
c) určení a zavedení potřebných preventivních opatření;
d) zaznamenání výsledků podniknutých opatření (viz 4.3.3);
e) přezkoumání provedených preventivních opatření;

Organizace musí identifikovat změny rizik a určit požadavky na nápravná opatření, zejména pak u těch rizik jejichž změna byla významná.

Priorita preventivních opatření bude určena na základě výsledků hodnocení rizik.

POZNÁMKA

Opatření pro prevenci vzniku neshod jsou většinou finančně méně náročná než opatření nápravná.

Příloha A

(normativní)

Cíle opatření a jednotlivá bezpečnostní opatření

Cíle opatření a jednotlivá bezpečnostní opatření v tabulce A.1 jsou přímo odvozeny a propojeny s těmi, které jsou uvedeny v ISO/IEC 17799:2005 kapitola 5 až 15. Seznam opatření uvedených v tabulce A.1 není vyčerpávající a organizace může považovat za potřebné přidat dodatečné cíle opatření a jednotlivá opatření. Cíle opatření a jednotlivá opatření z těchto tabulek musí být vybrány v rámci procesu zavádění ISMS, specifikovaném v kapitole 4.2.1.

ISO/IEC 17799:2005 kapitoly 5 až 15 poskytují doporučení a návod pro zavedení nejlepších praktik pro podporu opatření uvedených v A.5 až A.15.

Tabulka A.1 – Cíle opatření a jednotlivá bezpečnostní opatření

A.5 Bezpečnostní politika

A.5.1 Bezpečnostní politika informací

Cíl: Definovat směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky organice, příslušnými zákony a regulatorními požadavky.

A.5.1.1 Dokument bezpečnostní politiky informací

Opatření

Dokument bezpečnostní politiky informací by měl být schválen vedením organizace, vydán a být dán na vědomí všem zaměstnancům a relevantním třetím stranám.

A.5.1.2 Přezkoumání a aktualizace bezpečnostní politiky informací

Opatření

Pro zajištění její neustálé použitelnosti, přiměřenosti a účinnosti by bezpečnostní politika informací měla být přezkoumávána v plánovaných intervalech a vždy když nastane významná změna.

A.6 Organizace bezpečnosti

A.6.1 Interní organizace

Cíl: Řídit bezpečnost informací v organizaci.

A.6.1.1 Závazek vedení *Opatření*

Vedení organizace by mělo stanovit jasný směr a aktivně podporovat bezpečnost v rámci organizace. Mělo by demonstrovat svůj závazek a jednoznačně přiřadit a vymezit role v oblasti bezpečnosti informací.

A.6.1.2 Koordinace bezpečnosti informací

A.6.1.3 Přidělení odpovědností v oblasti bezpečnosti informací

Opatření

Činnosti v oblasti bezpečnosti informací by měly být koordinovány prostřednictvím zástupců různých útvarů z celé organizace.

Opatření

Měly by být jednoznačně určeny odpovědnosti v oblasti bezpečnosti informací.

A.6.1.4 Schvalovací proces zařízení pro zpracování informací

A.6.1.5 Dohody o ochraně důvěrných informací

A.6.1.6 Kontakt s orgány veřejné správy

A.6.1.7 Kontakt se zájmovými skupinami

A.6.1.8 Nezávislá přezkoumání bezpečnosti informací

A.6.2 Externí subjekty

Opatření

Měl by být ustaven a zaveden postup schvalování (vedoucími zaměstnanci) nových zařízení pro zpracování informací.

Opatření

Měly by být určeny a v pravidelných intervalech přezkoumávány dohody obsahující požadavky na ochranu důvěrnosti nebo povinnost zachovávat mlčenlivost, reflektující potřeby organizace na ochranu informací.

Opatření

Měly by být udržovány přiměřené vztahy s orgány veřejné správy.

Opatření

Měly by být udržovány přiměřené vztahy se zájmovými skupinami nebo speciálními fóry na bezpečnost a profesními sdruženími.

Opatření

Přístup organizace k řízení a implementaci bezpečnosti informací (tj. cíle opatření, jednotlivá opatření, politiky, směrnice a postupy) by měly být v pravidelných intervalech (a nebo v případě jakékoliv významné změny ve vztahu k bezpečnosti) nezávisle přezkoumávány.

Cíl: Zachovat bezpečnost informací organizace a zařízení pro zpracování informací, které jsou přístupné, zpracovávané, sdělované nebo spravované externími subjekty.

A.6.2.1 Identifikace rizik plynoucích z přístupu externích subjektů

A.6.2.2 Bezpečnostní požadavky pro přístup klientů

A.6.2.3 Bezpečnostní požadavky v dohodách se třetí stranou

Opatření

Předtím, než je externím subjektům povolen přístup k informacím organizace a zařízením pro zpracování informací, by měla být identifikována rizika a implementována vhodná opatření na jejich pokrytí.

Opatření

Předtím, než je klientům umožněn přístup k informací a aktivům organizace by měly být zjištěny veškeré požadavky na bezpečnost.

Opatření

Dohody, uzavřené s třetími stranami zahrnující přístup, zpracování, šíření nebo správu informací organizace nebo správu zařízení pro zpracování informací (případně dodávku produktů nebo služeb k zařízení pro zpracování informací), by měly pokrývat veškeré relevantní bezpečnostní požadavky.

A.7 Klasifikace a řízení aktiv

A.7.1 Odpovědnost za aktiva

Cíl: Udržovat přiměřenou ochranu aktiv organizace.

A.7.1.1 Evidence aktiv *Opatření*

Měla by být identifikována všechna aktiva organizace, všechna důležitá aktiva by měla být evidována a seznam udržován aktuální.

A.7.1.2 Vlastnictví aktiv *Opatření*

Veškeré informace a aktiva související se zařízením pro zpracování informací by měly mít určeného vlastníka7.

A.7.1.3 Přípustné použití aktiv *Opatření*

Měla by být ustavena, zdokumentována a do praxe zavedena pravidla pro přípustné použití informací a aktiv souvisejících se zařízením pro zpracování informací.

A.7.2 Klasifikace informací

Cíl: Zajištění přiměřenosti ochrany informačních aktiv.

A.7.2.1 Doporučení pro klasifikaci *Opatření*

Informace by měly být klasifikovány a to ohledem na jejich hodnotu, právní požadavky, citlivost a kritičnost.

A.7.2.2 Označování a nakládání s informacemi

Opatření

Pro značení informací a zacházení s nimi by měly být vytvořeny a do praxe zavedeny postupy, které jsou v souladu s klasifikačním schématem přijatým organizací.

A.8 Bezpečnost lidských zdrojů

A.8.1 Před vznikem pracovního vztahu8

Cíl: Zajistit, aby zaměstnanci, smluvní a třetí strany byli srozuměni se svými povinnostmi, aby pro jednotlivé role byli vybráni vhodní kandidáti a snížit riziko lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace.

A.8.1.1 Role a odpovědnosti *Opatření*

Role a odpovědnosti zaměstnanců, smluvních a třetích stran v oblasti bezpečnosti informací by měly být stanoveny a zdokumentovány v souladu s bezpečnostní politikou organizace.

A.8.1.2 Prověrka *Opatření*

Všichni uchazeči o zaměstnání, smluvní a třetí strany by měly být prověřeni dle platných zákonů, předpisů a v souladu s etikou. Prověření by měla být prováděna na základě požadavků stanovených organizací, dále s ohledem na klasifikaci informací, ke kterým by měli získat přístup, ale také z hlediska jejich spolehlivosti9 a potenciálních rizik.

7 Pojmem „vlastník" je myšlen jedinec nebo entita, který má vedením organizace přidělenou odpovědnost za výrobu, vývoj, údržbu, použití a bezpečnost aktiv. Pojmem „vlastník" není myšleno skutečné vlastnictví aktiva.

8 Pracovním vztahem je myšleno: zaměstnání lidí (pracovní poměr na dobu určitou nebo neurčitou), přidělení pracovní role, změna pracovní role, dohoda o pracovní činnosti, dohoda o provedení práce a nebo ukončení jakéhokoliv z těchto vazeb.

9 V případech, které se týkají ochrany utajovaných skutečností, tj. v případech stanovených zákonem, musí mít odpovídající prověrku.

A.8.1.3 Podmínky výkonu pracovní činnosti

A.8.2 Během pracovního vztahu

Opatření

Pracovní smlouvy uzavřené se zaměstnanci, smluvními a třetími stranami by měly obsahovat ustanovení o jejich odpovědnostech za bezpečnost informací.

Cíl: Zajistit, aby si zaměstnanci, smluvní a třetí strany byli vědomi bezpečnostních hrozeb a problémů s nimi spjatých, svých odpovědností a povinností a byli připraveni podílet se na dodržování politiky bezpečnosti informací během své běžné práce a na snižování rizika lidské chyby.

A.8.2.1 Odpovědnosti vedoucích zaměstnanců

A.8.2.2 Povědomí, vzdělávání a školení v oblasti bezpečnosti informací

Opatření

Vedoucí zaměstnanci by měly po uživatelích, smluvních a třetích stranách, požadovat dodržování bezpečnosti v souladu se zavedenými politikami a směrnicemi.

Opatření

Všichni zaměstnanci organizace, a je-li to důležité i pracovníci smluvních a třetích stran, by měli s ohledem na svoji pracovní náplň, projít odpovídajícím a pravidelně se opakujícím školením v oblasti bezpečnosti informací, bezpečnostní politiky a směrnicím organizace.

A.8.2.3 Disciplinární řízení *Opatření*

Mělo by existovat formalizované disciplinární řízení vůči zaměstnancům, kteří se dopustili narušení bezpečnosti.

A.8.3 Ukončení nebo změna pracovního vztahu

Cíl: Zajistit, aby ukončení nebo změna pracovního vztahu zaměstnanců, smluvních a třetích stran proběhla řádným způsobem.

A.8.3.1 Odpovědnosti za ukončení pracovního vztahu

A.8.3.2 Navrácení zapůjčených předmětů

Opatření

Měly by být jasně definovány a přiděleny odpovědnosti pro případ ukončení nebo změny pracovního vztahu.

Opatření

Při ukončení pracovního vztahu by měli zaměstnanci, pracovníci smluvních a třetích stran odevzdat veškeré jim svěřené předměty, které jsou majetkem organizace.

A.8.3.3 Odebrání přístupových práv *Opatření*

Při ukončení pracovního vztahu by měla být uživatelům, smluvním a třetím stranám odejmuta nebo pozměněna

přístupová práva k informacím a zařízení pro zpracování informací.

A.9 Fyzická bezpečnost a bezpečnost prostředí

A.9.1 Zabezpečené oblasti

Cíl: Předcházet neautorizovanému přístupu do vymezených prostor, předcházet poškození a zásahům do provozních budov a informací organizace.

A.9.1.1 Fyzický bezpečnostní perimetr

Opatření

Při ochraně prostor ve kterých se nachází informace nebo zařízení pro zpracování informací by měly být používány bezpečnostní perimetry (bariéry jako například zdi, vstupní turniket na karty nebo recepce).

A.9.1.2 Kontroly vstupu osob *Opatření*

Aby bylo zajištěno, že je přístup do zabezpečených oblastí povolen pouze oprávněným osobám, měly by být tyto oblasti chráněny vhodným systémem kontrol vstupu.

A.9.1.3 Zabezpečení kanceláří, místností a zařízení

A.9.1.4 Ochrana před hrozbami vnějšího prostředí

A.9.1.5 Práce v zabezpečených oblastech

A.9.1.6 Veřejný přístup, prostory pro nakládku a vykládku

A.9.2 Bezpečnost zařízení

Opatření

Mělo by být navrženo a aplikováno fyzické zabezpečení kanceláří, místností a zařízení.

Opatření

Na ochranu proti škodám způsobeným požárem, povodní, zemětřesením, výbuchem, civilními nepokoji a jinými přírodními nebo lidmi zapříčiněnými katastrofami by měly být navrženy a aplikovány prvky fyzické ochrany.

Opatření

Pro práci v zabezpečených oblastech by měly být navrženy a aplikovány prvky fyzické ochrany.

Opatření

Prostory pro nakládku a vykládku a další místa, kudy se mohou neoprávněné osoby dostat do prostor organizace, by měla být kontrolována a pokud možno by měla být izolována od zařízení pro zpracování informací tak, aby se zabránilo neoprávněnému přístupu.

Cíl: Předcházet ztrátě, poškození nebo kompromitaci aktiv a přerušení činnosti organizace.

A.9.2.1 Umístění zařízení a jeho ochrana

Opatření

Zařízení by měla být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup.

A.9.2.2 Podpůrná zařízení *Opatření*

Zařízení by mělo být chráněno před selháním napájení a před dalšími výpadky způsobenými selháním podpůrných služeb.

A.9.2.3 Bezpečnost kabelových rozvodů

Opatření

Silové a telekomunikační kabelové rozvody, které jsou určeny pro přenos dat a podporu informačních služeb, by měly být chráněny před poškozením či odposlechem.

A.9.2.4 Údržba zařízení *Opatření*

Zařízení by mělo být správně udržováno pro zajištění jeho stálé dostupnosti a integrity.

A.9.2.5 Bezpečnost zařízení mimo prostory organizace

A.9.2.6 Bezpečná likvidace nebo opakované použití zařízení

Opatření

Zařízení používané mimo prostory organizace by mělo být zabezpečeno s přihlédnutím k různým rizikům vyplývajících z jejich použití mimo organizaci.

Opatření

Všechna zařízení obsahující paměťová média by měla být kontrolována tak, aby bylo možné zajistit, že před jejich likvidací nebo opakovaným použitím budou citlivá data a licencované programové vybavení odstraněna

nebo přepsána.
A.9.2.7 Přemístění majetku *Opatření*
Zařízení, informace nebo programové vybavení by bez schválení nemělo být přemisťováno.

A.10 Řízení komunikací a řízení provozu

A.10.1 Provozní postupy a odpovědnosti

Cíl: Zajistit správný a bezpečný provoz zařízení pro zpracování informací.

A.10.1.1 Dokumentace provozních postupů
Opatření
Provozní postupy by měly být zdokumentovány a udržovány a měly by být dostupné všem uživatelům dle potřeby.

A.10.1.2 Řízení změn *Opatření*
Změny ve vybavení a zařízení pro zpracování informací by měly být řízeny.

A.10.1.3 Oddělení povinností *Opatření*
Pro snížení příležitostí k neoprávněné modifikaci nebo zneužití aktiv organizace by mělo být zváženo oddělení jednotlivých povinností a odpovědností.

A.10.1.4 Oddělení vývoje, testování a provozu

A.10.2 Řízení dodávek třetích stran

Opatření
Pro snížení rizika neoprávněného přístupu k provoznímu systému a nebo jeho změn by mělo být zváženo oddělení procesů vývoje, testování a provozu.

Cíl: Zavést a udržovat přiměřenou úroveň bezpečnosti informací a úroveň dodávky služeb ve shodě s uzavřenými dohodami.

A.10.2.1 Dodávky služeb *Opatření*
Zajistit, aby úroveň služeb týkajících se bezpečnosti informací poskytovaných třetí stranou byla v souladu se smluvními podmínkami.

A.10.2.2 Monitorování a přezkoumávání služeb třetích stran

A.10.2.3 Řízení změn služeb poskytovaných třetími stranami
Opatření
Služby, zprávy a záznamy poskytované třetí stranou by měly být monitorovány a pravidelně přezkoumávány, audity by měly být opakovány v pravidelných intervalech.
Opatření
Změny v poskytování služeb, včetně udržování a zlepšování existujících bezpečnostních politik, směrnic a bezpečnostních opatření, by měly být řízeny s ohledem na kritičnost systémů a procesů organizace, které jsou součástí opakovaného hodnocení rizik.

A.10.3 Plánování a přejímání informačních systémů

Cíl: Minimalizovat riziko selhání informačních systémů.

A.10.3.1 Řízení kapacit *Opatření*
Pro zajištění požadovaného výkonu informačního systému, s ohledem na budoucí kapacitní požadavky, by mělo být monitorováno, nastaveno a projektováno využití zdrojů.

A.10.3.2 Přejímání systémů *Opatření*
Měla by být určena kritéria pro přejímání nových informačních systémů, jejich aktualizaci a zavádění nových verzí a vhodný způsob testování systému v průběhu vývoje a před zavedením do ostrého provozu.

A.10.4 Ochrana proti škodlivým programům a mobilním kódům

Cíl: Chránit integritu programů a dat.

A.10.4.1 Opatření na ochranu proti škodlivým programům

A.10.4.2 Opatření na ochranu proti mobilním kódům

A.10.5 Zálohování

Opatření
Na ochranu proti škodlivým programům a nepovoleným mobilním kódům by měla být implementována opatření na jejich detekci, prevenci a nápravu a zvyšováno odpovídající bezpečnostní povědomí uživatelů.
Opatření
Použití povolených mobilních kódů by mělo být nastaveno v souladu s bezpečnostní politikou, mělo by být zabráněno spuštění nepovolených mobilních kódů.

Cíl: Udržovat integritu a dostupnost informací a zařízení pro jejich zpracování.

A.10.5.1 Zálohování informací *Opatření*
Záložní kopie důležitých informací a programového vybavení organizace by měly být pořizovány a testovány v pravidelných intervalech.

A.10.6 Správa sítě

Cíl: Zajistit ochranu informací v počítačových sítích a ochranu jejich infrastruktury.

A.10.6.1 Síťová opatření *Opatření*
Pro zajištění ochrany před možnými hrozbami, pro zaručení bezpečnosti systémů a aplikací využívajících sítí a pro zajištění bezpečnosti informací při přenosu by počítačové sítě měly být vhodným způsobem spravovány a kontrolovány.

A.10.6.2 Bezpečnost síťových služeb *Opatření*
Měly by být identifikovány a do dohod o poskytování síťových služeb zahrnuty bezpečnostní prvky, úroveň poskytovaných služeb a požadavky na správu všech síťových služeb a to jak v případech, kdy jsou tyto služby zajišťovány interně, tak i v případech, kdy jsou zajišťovány cestou outsourcingu.

A.10.7 Bezpečnost při zacházení s médii

Cíl: Předcházet neoprávněnému prozrazení, modifikaci, ztrátě nebo poškození aktiv a přerušení činnosti organizace.

A.10.7.1 Správa vyměnitelných počítačových médií
Opatření
Měly by být vytvořeny postupy pro správu vyměnitelných počítačových médií.

A.10.7.2 Likvidace médií *Opatření*
Jestliže jsou média dále provozně neupotřebitelná, měla by být bezpečně a spolehlivě zlikvidována.

A.10.7.3 Postupy pro manipulaci s informacemi
Opatření
Pro zabránění neautorizovanému přístupu nebo zneužití informací by měla být stanovena pravidla pro manipulaci s nimi a pro jejich ukládání.

A.10.7.4 Bezpečnost systémové dokumentace
Opatření
Systémová dokumentace by měla být chráněna proti neoprávněnému přístupu.

A.10.8 Výměny informací

Cíl: Zajistit bezpečnost informací a programů při jejich výměně v rámci organizace a při jejich výměně s externími subjekty.

A.10.8.1 Postupy při výměně informací a programů

A.10.8.2 Dohody o výměně informací a programů

A.10.8.3 Bezpečnost médií při přepravě
Opatření
Měly by být ustaveny a do praxe zavedeny formální postupy, politiky a opatření na ochranu informací při jejich výměně pro všechny typy používaných komunikačních zařízení.
Opatření
Výměna informací a programů by měla být založena na dohodách uzavřených mezi organizací a externími subjekty.
Opatření
Média obsahující informace by měla být během přepravy mimo organizaci chráněna proti neoprávněného přístupu, zneužití nebo narušení.

A.10.8.4 Elektronické zasílání zpráv *Opatření*
Elektronicky přenášené informace by měly být vhodným způsobem chráněny.

A.10.8.5 Podnikové informační systémy
Opatření
Na ochranu informací v propojených podnikových informačních systémech by měla být vytvořena a do praxe zavedena politika a odpovídající směrnice.

A.10.9 Služby elektronického obchodu

Cíl: Zajistit bezpečnost služeb elektronického obchodu a jejich bezpečné použití.

A.10.9.1 Elektronický obchod *Opatření*
Informace přenášené ve veřejných sítích v rámci elektronického obchodování by měly být chráněny před podvodnými aktivitami, před zpochybňováním smluv, prozrazením či modifikací.

A.10.9.2 On-line transakce *Opatření*
Měla by být zajištěna ochrana informací přenášených při on-line transakcích tak, aby byl zajištěn úplný přenos informací a zamezilo se špatnému směrování, neoprávněné změně zpráv, neoprávněnému prozrazení, neoprávněné duplikaci nebo opakování zpráv.
A.10.9.3 Veřejně přístupné informace *Opatření*
Informace publikované na veřejně přístupných systémech by měly být chráněny proti neoprávněné modifikaci.

A.10.10 Monitorování

Cíl: Detekovat neoprávněné zpracování informací.
A.10.10.1 Zaznamenávání událostí *Opatření*
Auditní záznamy, obsahující chybová hlášení a jiné bezpečnostně významné události, byměly být pořizovány a uchovány po stanovené období tak, aby byly se daly použít pro budoucí vyšetřování a pro účely monitorování řízení přístupu.
A.10.10.2 Monitorování používání systému
A.10.10.3 Ochrana vytvořených záznamů
A.10.10.4 Administrátorský a operátorský deník
Opatření
Měla by být stanovena pravidla pro monitorování použití zařízení pro zpracování informací, výsledky těchto monitorování by měly být pravidelně přezkoumávány.
Opatření
Zařízení pro zaznamenávání informací a vytvořené záznamy by měly být vhodným způsobem chráněny proti neoprávněnému přístupu a zfalšování.
Opatření
Aktivity správce systému a systémového operátora by měly být zaznamenávány.
A.10.10.5 Záznam selhání *Opatření*
Měly by být zaznamenány a analyzovány chyby a provedena opatření k nápravě.
A.10.10.6 Synchronizace času *Opatření*
Hodiny všech důležitých systémů pro zpracování informací by měly být v rámci organizace nebo domény synchronizovány se schváleným zdrojem přesného času.

A.11 Řízení přístupu

A.11.1 Požadavky na řízení přístupu

Cíl: Řídit přístup k informacím.
A.11.1.1 Politika řízení přístupu *Opatření*
Měla by být vytvořena, dokumentována a v závislosti na aktuálních bezpečnostních požadavcích přezkoumávána politika řízení přístupu.

A.11.2 Řízení přístupu uživatelů

Cíl: Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k informačním systémům.
A.11.2.1 Registrace uživatele *Opatření*
Měl by existovat postup pro formální registraci uživatele včetně jejího zrušení, který zajistí autorizovaný přístup ke všem víceuživatelským informačním systémům a službám.
A.11.2.2 Řízení privilegovaného přístupu
Opatření
Přidělování a používání privilegií by mělo být omezeno a řízeno.
A.11.2.3 Správa uživatelských hesel *Opatření*
Přidělování hesel by mělo být řízeno formálním procesem.
A.11.2.4 Přezkoumání přístupových práv uživatelů
Opatření
Vedení organizace by mělo v pravidelných intervalech provádět formální přezkoumání přístupových práv uživatelů.

A.11.3 Odpovědnosti uživatelů

Cíl: Předcházet neoprávněnému uživatelskému přístupu, prozrazení nebo krádeži informací a zařízení pro zpracování informací.
A.11.3.1 Používání hesel *Opatření*
Při výběru a používání hesel by mělo být po uživatelích požadováno, aby dodržovali stanovené bezpečnostní postupy.
A.11.3.2 Neobsluhovaná uživatelská

zařízení
A.11.3.3 Zásada prázdného stolu a prázdné obrazovky monitoru
A.11.4 Řízení přístupu k síti
Opatření
Uživatelé by měli zajistit přiměřenou ochranu neobsluhovaných zařízení.
Opatření
Měla by být přijata zásada prázdného stolu ve vztahu k dokumentům a vyměnitelným médiím a zásada prázdné obrazovky monitoru u zařízení pro zpracování informací.
Cíl: Předcházet neautorizovanému přístupu k síťovým službám.
A.11.4.1 Politika užívání síťových služeb
A.11.4.2 Autentizace uživatele externího připojení
Opatření
Uživatelé by měli mít přímý přístup pouze k těm síťovým službám, pro jejichž použití byli zvlášť oprávněni.
Opatření
Přístup vzdálených uživatelů měl být autentizován.
A.11.4.3 Identifikace zařízení v sítích *Opatření*
Pro autentizaci připojení z vybraných lokalit a přenosných zařízení by se měla zvážit automatická identifikace zařízení.
A.11.4.4 Ochrana portů pro vzdálenou diagnostiku a konfiguraci
Opatření
Fyzický i logický přístup k diagnostickým a konfiguračním portům by měl být bezpečně řízen.
A.11.4.5 Princip oddělení v sítích *Opatření*
Skupiny informačních služeb, uživatelů a informačních systémů by měly být v sítích odděleny.
A.11.4.6 Řízení síťových spojení *Opatření*
U sdílených sítí, zejména těch, které přesahují hranice organizace, by měly být omezeny možnosti připojení uživatelů. Omezení by měla být v souladu s politikou řízení přístupu a s požadavky aplikací (viz 11.1).
A.11.4.7 Řízení směrování sítě *Opatření*
Pro zajištění toho, aby počítačová spojení a informační toky nenarušovaly politiku řízení přístupu aplikací organizace, by mělo být zavedeno řízení směrování sítě.
A.11.5 Řízení přístupu k operačnímu systému
Cíl: Předcházet neautorizovanému přístupu k operačním systémům.
A.11.5.1 Bezpečné postupy přihlášení *Opatření*
Přístup k operačnímu systému by měl být řízen postupy bezpečného přihlášení.
A.11.5.2 Identifikace a autentizace uživatelů
Opatření
Všichni uživatelé by měli mít pro výhradní osobní použití jedinečný identifikátor (uživatelské ID), měl by být také zvolen vhodný způsob autentizace k ověření jejich identity.
A.11.5.3 Systém správy hesel *Opatření*
Systém správy hesel by měl být interaktivní a měl by zajišťovat použití kvalitních hesel.
A.11.5.4 Použití systémových nástrojů *Opatření*
Použití systémových nástrojů, které jsou schopné překonat systémové nebo aplikační kontroly by mělo být omezeno a přísně kontrolováno.
A.11.5.5 Časové omezení relace *Opatření*
Neaktivní relace by měly se po stanovené době nečinnosti ukončit.
A.11.5.6 Časové omezení spojení *Opatření*
U vysoce rizikových aplikací by pro zajištění dodatečné bezpečnosti mělo být zváženo použití omezení doby spojení.
A.11.6 Řízení přístupu k aplikacím a informacím
Cíl: Předcházet neoprávněnému přístupu k informacím uloženým v počítačových systémech.
A.11.6.1 Omezení přístupu k informacím
Opatření
Uživatelé aplikačních systémů, včetně pracovníků podpory, by měli mít přístup k informacím a funkcím aplikačních systémů omezen v souladu s definovanou politikou řízení přístupu.

A.11.6.2 Oddělení citlivých systémů *Opatření*
Citlivé aplikační systémy by měly mít oddělené (izolované) počítačové prostředí.

A.11.7 Mobilní výpočetní zařízení a práce na dálku

Cíl: Zajistit bezpečnost informací při použití mobilní výpočetní techniky a při využití zařízení pro práci na dálku.

A.11.7.1 Mobilní výpočetní zařízení a sdělovací technika *Opatření*
Měla by být ustavena formální pravidla a přijata opatření na ochranu proti rizikům použití mobilních výpočetních a komunikačních zařízení.

A.11.7.2 Práce na dálku *Opatření*
Organizace by měla vytvořit a do praxe zavést zásady, operativní plány a postupy pro práci na dálku.

A.12 Nákup, vývoj a údržba informačního systému

A.12.1 Bezpečnostní požadavky systémů

Cíl: Zajistit, aby se bezpečnost stala neodlučitelnou součástí informačních systémů.

A.12.1.1 Analýza a specifikace bezpečnostních požadavků *Opatření*
Požadavky organizace na nové informační systémy nebo na rozšíření existujících systémů by měly obsahovat také požadavky na bezpečnostní opatření.

A.12.2 Správné zpracování v aplikacích

Cíl: Předcházet chybám, ztrátě, modifikaci nebo zneužití uživatelských dat v aplikacích.

A.12.2.1 Kontrola vstupních dat *Opatření*
Vstupní data aplikací by měla být kontrolována z hlediska správnosti a adekvátnosti.

A.12.2.2 Kontrola vnitřního zpracování *Opatření*
Pro detekci jakéhokoliv poškození nebo modifikace informací vzniklého chybami při zpracování nebo úmyslnými zásahy, by mělo být zváženo začlenění kontroly platnosti dat.

A.12.2.3 Integrita zprávy *Opatření*
U jednotlivých aplikací by měly být stanoveny bezpečnostní požadavky na zajištění autentizace a integrity zpráv, dle potřeby určena, a zavedena vhodná opatření.

A.12.2.4 Kontrola výstupních dat *Opatření*
Pro zajištění toho, že zpracování uložených informací je bezchybné a odpovídající dané situaci, by mělo být provedeno ověření platnosti výstupních dat.

A.12.3 Kryptografická opatření

Cíl: Ochránit důvěrnost, autentičnost a integritu informací s pomocí kryptografických prostředků.

A.12.3.1 Politika pro použití kryptografických opatření *Opatření*
Měla by být vytvořena a zavedena pravidla pro používání kryptografických opatření na ochranu informací.

A.12.3.2 Správa klíčů *Opatření*
Na podporu používání kryptografických technik v organizaci by měl existovat systém jejich správy.

A.12.4 Bezpečnost systémových souborů

Cíl: Zajistit bezpečnost systémových souborů

A.12.4.1 Správa provozního programového vybavení *Opatření*
Měly by být zavedeny postupy kontroly instalace programového vybavení na provozních systémech.

A.12.4.2 Ochrana systémových testovacích údajů *Opatření*
Testovací data by měla být pečlivě vybrána, chráněna a kontrolována.

A.12.4.3 Řízení přístupu ke knihovně zdrojových kódů *Opatření*
Přístup ke knihovně zdrojových kódů by měl být omezen.

A.12.5 Bezpečnost procesů vývoje a podpory

Cíl: Udržovat bezpečnost programů a informací aplikačních systémů.

A.12.5.1 Postupy řízení změn *Opatření*
Měly by být zavedeny formální postupy řízení změn.

A.12.5.2 Technické přezkoumání aplikací po změnách operačního systému *Opatření*

V případě změny operačního systému by měly být přezkoumány a otestovány kritické aplikace, aby bylo zajištěno, že změny nemají nepříznivý dopad na provoz nebo bezpečnost organizace. A.12.5.3 Omezení změn programových balíků

Opatření

Modifikace programových balíků by měly být omezeny pouze na nezbytné změny, veškeré prováděné změny musí být řízeny.

A.12.5.4 Únik informací *Opatření*

Mělo by být zabráněno úniku informací.

A.12.5.5 Programové vybavení vyvíjené externím dodavatelem

A.12.6 Řízení technických zranitelností

Opatření

Vývoj programového vybavení externím dodavatelem by měl být organizací dohlížen a monitorován.

Cíl: Snížit rizika vyplývající ze zneužití veřejně publikovaných technických zranitelností.

A.12.6.1 Řízení, správa a kontrola technických zranitelností

Opatření

Mělo by být zajištěno včasné získání informace o existenci technické zranitelnosti v provozovaném informačním systému, vyhodnocena úroveň ohrožení organizace vůči této zranitelnosti a přijata příslušná opatření na pokrytí souvisejících rizik.

A.13 Zvládání bezpečnostních incidentů

A.13.1 Hlášení bezpečnostních událostí a slabin

Cíl: Zajistit nahlášení bezpečnostních událostí a slabin informačního systému způsobem, který umožní včasné zahájení kroků vedoucích k nápravě.

A.13.1.1 Hlášení bezpečnostních událostí

A.13.1.2 Hlášení bezpečnostních slabin

Opatření

Bezpečnostní události by měly být hlášeny příslušnými řídícími cestami tak rychle, jak je to jen možné.

Opatření

Všichni zaměstnanci, smluvní strany a další nespecifikovaní uživatelé informačního systému a služeb by měli být povinni zaznamenat a hlásit jakékoliv bezpečnostní slabiny nebo podezření na bezpečnostní slabiny v systémech nebo službách.

A.13.2 Zvládání bezpečnostních incidentů a kroky k nápravě

Cíl: Zajistit odpovídající a účinný přístup ke zvládání bezpečnostních incidentů.

A.13.2.1 Odpovědnosti a postupy *Opatření*

Pro zajištění rychlé, účinné a systematické reakce na bezpečnostní incidenty by měly být zavedeny odpovědnosti a postupy pro zvládání bezpečnostních incidentů.

A.13.2.2 Ponaučení z bezpečnostních incidentů

Opatření

Měly by existovat mechanizmy, které by umožňovaly kvantifikovat a monitorovat typy, rozsah a náklady bezpečnostních incidentů.

A.13.2.3 Shromažďování důkazů *Opatření*

V případech, kdy vyústění bezpečnostního incidentu směřuje k právnímu řízení (dle práva občanského nebo trestního) vůči osobě a nebo organizaci, by měly být sbírány, uchovávány a soudu předkládány důkazy v souladu s pravidly příslušné jurisdikce, kde se bude případ projednávat. **A.14 Řízení kontinuity činností organizace**

A.14.1 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací

Cíl: Bránit přerušení provozních činností a chránit kritické procesy organizace před následky závažných selhání informačních systémů nebo katastrof a zajistit jejich včasnou obnovu.

A.14.1.1 Zahrnutí bezpečnosti informací do procesu řízení kontinuity činností organizace

A.14.1.2 Kontinuita činností organizace a hodnocení rizik

A.14.1.3 Vytváření a implementace plánů kontinuity

A.14.1.4 Systém plánování kontinuity činností organizace

A.14.1.5 Testování, udržování a přezkoumání plánů

kontinuity
Opatření
V rámci organizace by měl existovat řízený proces pro rozvoj a udržování kontinuity činností organizace.
Opatření
Měly by být identifikovány možné příčiny přerušení činností organizace, včetně jejich pravděpodobnosti, velikosti dopadu a možných následků na bezpečnost informací.
Opatření
Pro udržení nebo obnovení provozních činností organizace po přerušení nebo selhání kritických procesů a pro zajištění dostupnosti informací v požadovaném čase a na požadovanou úroveň by měly být vytvořeny plány.
Opatření
Pro zajištění konzistentnosti plánů a pro určení priorit testování a údržby by měl být k dispozici jednotný systém plánů kontinuity činností organizace.
Opatření
Plány kontinuity činností by měly být pravidelně testovány a aktualizovány, aby se zajistila jejich aktuálnost a efektivnost.

A.15 Soulad s požadavky

A.15.1 Soulad s právními normami

Cíl: Vyvarovat se porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků.
A.15.1.1 Určení relevantní legislativy *Opatření*
Pro každý informační systém by měly být jednoznačně definovány, zdokumentovány a udržovány aktuální veškeré relevantní zákonné, podzákonné a smluvní požadavky a způsob jakým je organizace dodržuje.
A.15.1.2 Zákony na ochranu duševního vlastnictví
A.15.1.3 Ochrana záznamů organizace
A.15.1.4 Ochrana osobních údajů a soukromí
Opatření
Pro zajištění souladu se zákonnými, podzákonnými a smluvními požadavky na použití materiálů a aplikačního programového vybavení, které mohou být chráněny zákony na ochranu duševního vlastnictví by měly být zavedeny vhodné postupy.
Opatření
Důležité záznamy organizace by měly být chráněny proti ztrátě, zničení a padělání a to v souladu se zákonnými, podzákonnými a smluvními požadavky a požadavky organizace.
Opatření
Ochrana osobních údajů a soukromí by měla být zajištěna v souladu s odpovídající legislativou, předpisy, a pokud je to relevantní, se smlouvami. A.15.1.5 Prevence zneužití zařízení pro zpracování informací
A.15.1.6 Regulace kryptografických opatření
Opatření
Mělo by být zakázáno používat zařízení pro zpracování informací jiným než autorizovaným způsobem.
Opatření
Kryptografická opatření by měla být používána v souladu s příslušnými úmluvami, zákony a předpisy.

A.15.2 Soulad s bezpečnostními politikami, normami a technická shoda

Cíl: Zajistit shodu systémů s bezpečnostními politikami organizace a normami.
A.15.2.1 Shoda s bezpečnostními politikami a normami
Opatření
Vedoucí zaměstnanci by měli zajistit, aby všechny bezpečnostní postupy v rozsahu jejich odpovědnosti byly prováděny správně, v souladu s bezpečnostními politikami a normami.
A.15.2.2 Kontrola technické shody *Opatření*
Informační systémy by měly být pravidelně kontrolovány, zda jsou v souladu s bezpečnostními politikami a standardy.

A.15.3 Hlediska auditu informačních systémů

Cíl: Maximalizovat účinnost auditu a minimalizovat zásahy do informačních systémů.
A.15.3.1 Opatření k auditu informačních systémů

A.15.3.2 Ochrana nástrojů pro audit informačních systémů

Opatření

Požadavky auditu a činnosti zahrnující kontrolu provozních systémů by měly být pečlivě naplánovány a schváleny, aby se minimalizovalo riziko narušení činností organizace.

Opatření

Přístup k nástrojům určeným pro audit informačních systémů by měl být chráněn, aby se předešlo jejich možnému zneužití nebo ohrožení.

Příloha B

(informativní)

Principy směrnice OECD a normy BS ISO/IEC 27001

Principy dané směrnicí OECD pro bezpečnost informačních systémů a sítí se vztahují jak na úroveň politik, tak na provozní úroveň, která řídí bezpečnost informačních systémů a sítí. Tato norma poskytuje rámec systému řízení bezpečnosti informací pro zavedení některých z principů OECD využitím modelu PDCA a procesů popsaných v odstavcích **4, 5, 6, 7** a **8**, tak jak naznačuje tabulka B.1.

Tabulka B.1 – principy OECD a model PDCA

Principy OECD	Odpovídající procesu ISMS a fázi PDCA
Informovanost	Účastníci by měli být informováni o potřebě bezpečnosti informačních systémů a sítí, a o tom, co mohou udělat ke zvýšení bezpečnosti.
Odpovědnost	Všichni účastníci jsou odpovědní za bezpečnost informačních systémů a sítí.
Reakce	Účastníci by měli jednat včas a vzájemně spolupracovat při předcházení bezpečnostním incidentům, při reakci a jejich odhalování.
Hodnocení rizik	Účastníci by měli provádět hodnocení rizik.
Návrh a implementace bezpečnosti	Účastníci by měli bezpečnost zahrnout mezi základní prvky informačních systémů a sítí.
Řízení bezpečnosti	Účastníci by měli přijmout komplexní přístup k řízení bezpečnosti.
Opětovné hodnocení	Účastníci by měli přezkoumávat a opětovně hodnotit bezpečnost informačních systémů a sítí a provádět příslušné úpravy bezpečnostní politiky, praxe, opatření a postupů.
	Tato činnost je součástí fáze **Dělej** (viz 4.2.2 a 5.2.2).
	Tato činnost je součástí fáze **Dělej** (viz 4.2.2 a 5.1).
	Toto je část monitorovací fáze **Kontroluj** (viz 4.2.3 a 6 až 7.3) a činnosti reakční fáze **Jednej** (viz 4.2.4 a 8.1 to 8.3). Součástí mohou být některé aspekty fází **Plánuj** a **Kontroluj**.
	Tato činnost je součástí fáze **Plánuj** (viz 4.2.1) a opětovné hodnocení rizik je část fáze **Kontroluj** (viz 4.2.3 a 6.1 až 6.4).
	Jakmile je dokončeno hodnocení rizika, vyberou se opatření pro zvládání rizik jako součást fáze **Plánuj** (viz 4.2.1). Fáze **Dělej** (viz 4.2.2 a 5.2) potom pokrývá implementaci a provozní využití těchto opatření.
	Řízení rizik je proces, který zahrnuje prevenci, detekci a reakci na incidenty, probíhající údržbu, přezkoumání a audit. Všechny tyto aspekty jsou zahrnuty ve fázích **Plánuj**, **Dělej**, **Kontroluj** a **Jednej**.
	Opětovné hodnocení bezpečnosti informací je část fáze **Kontroluj** (viz 4.2.3 a 6 až 7.3), kde by měla být prováděna pravidelná přezkoumání za účelem kontroly efektivnosti systému řízení bezpečnosti informací a zlepšování bezpečnosti jako součást fáze **Jednej** (viz 4.2.4 a 8.1 až 8.3).

Příloha C

(informativní)

Vztah mezi ISO 9001:2000, ISO 14001:2004 a ISO 27001:2005

Tabulka C.1 ukazuje vztah mezi ISO 9001:2000, ISO 14001:2004 a ISO 27001:2005

Tabulka C.1 - vztah mezi ISO 9001:2000, ISO 14001:2004 a ISO 27001:2005

ISO 27001:2005	ISO 9001:2000	ISO 14001:2004
0 Úvod		

1.1 Všeobecně
1.2 Procesní přístup
1.3 Kompatibilita s jinými systémy řízení

1 Působnost

1.1 Všeobecně
1.2 Použití

0 Úvod

1.1 Všeobecně
1.2 Procesní přístup
1.3 Vztah k ISO 9004
1.4 Kompatibilita s jinými systémy managementu

1 Předmět normy

1.1 Všeobecně
1.2 Aplikace

0 Úvod

1 Předmět normy

2 Normativní odkazy 2 Normativní odkazy 2 Normativní odkazy

3 Termíny a definice 3 Termíny a definice 3 Definice

4 Systém řízení bezpečnosti informací

4.1 Všeobecné požadavky
4.2. Ustavení a řízení ISMS
4.2.1 Ustavení ISMS
4.2.2 Zavádění a provozování ISMS
4.2.3 Monitorování a přezkoumání ISMS
4.2.4 Udržování a zlepšování ISMS
4.3. Požadavky na dokumentaci
4.3.1 Všeobecně
4.3.2 Řízení dokumentů
4.3.3 Řízení záznamů

4 Systém managementu jakosti

4.1 Všeobecné požadavky
8.2.3 Monitorování a měření procesů
8.2.4 Monitorování a měření produktu
4.2 Požadavky na dokumentaci
4.2.1 Všeobecně
4.2.2 Příručka jakosti
4.2.3 Řízení dokumentů
4.2.4 Řízení záznamů

4 Požadavky na systém environmentálního managementu

4.1 Všeobecné požadavky
4.4 Zavedení a provoz
4.5.1 Monitorování a měření
4.4.5 Řízení dokumentů
4.5.4 Záznamy

ISO 27001:2005 ISO 9001:2000 ISO 14001:2004

5. Odpovědnost vedení

5.1 Závazek vedení
5.2 Řízení zdrojů
5.2.1 Zajištění zdrojů
5.2.2 Školení, vědomí závažnosti a odborná způsobilost

5 Odpovědnost managementu

5.1 Osobní angažovanost a aktivita managementu
5.2 Zaměření na zákazníka
5.3 Politika jakosti
5.4 Plánování
5.5 Odpovědnost, pravomoc a komunikace

6 Management zdrojů

6.1 Poskytování zdrojů
6.2 Lidské zdroje
6.2.2 Odborná způsobilost, vědomí závažnosti a výcvik
6.3 Infrastruktura
6.4 Pracovní prostředí
4.2 Environmentální politika
4.3 Plánování

4.4.2 Výcvik, povědomí a odborná způsobilost

6 Interní audity ISMS 8.2.2 Interní audit 4.5.4 Audit systému environmentálního managementu

7. Přezkoumání ISMS vedením organizace

7.1 Všeobecně

7.2 Vstup pro přezkoumání

7.3 Výstup z přezkoumání

5.6 Přezkoumání systému managementu

5.6.1 Všeobecně

5.6.2 Vstup pro přezkoumání

5.6.3 Výstup z přezkoumání

4.6 Přezkoumání vedením organizace

8 Zlepšování ISMS

8.1 Soustavné zlepšování

8.2 Opatření k nápravě

8.3 Preventivní opatření

Příloha A Cíle opatření a jednotlivá bezpečnostní opatření

Příloha B Principy směrnice OECD a normy BS ISO/IEC 27001

Příloha C Vztah mezi ISO 9001:2000, ISO 14001:2004 a ISO 27001:2005

8 Měření analýza a zlepšování

8.5.1 Neustálé zlepšování

8.5.2 Opatření k nápravě

8.5.3 Preventivní opatření

Příloha A Soulad mezi ISO 9001:2000 a 14001:1996

4.5.2 Neshoda, nápravná a preventivní opatření

Příloha A Návod k použití normy

Příloha B Souvislosti mezi ISO 14001:2004 a 9001:2000