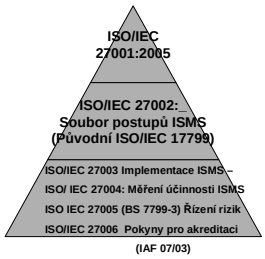
ČSN ISO/IEC 27001

Informační technologie - Bezpečnostní techniky – Systémy managementu bezpečnosti informací - Požadavky

Představení normy ISO/IEC 27001 a norem souvisejících - Současný stav

Stav norem v ČR současný stav

Prognóza dalšího vývoje souboru norem ISO/IEC 27000

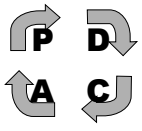


Struktura normy ISO 27001

- 1. Předmět normy
- 2. Normativní odkazy
- 3. Termíny a definice
- 4. Systém managementu bezpečnosti informací
- 5. Odpovědnost managementu
- 6. Interní audity ISMS
- 7. Přezkoumání ISMS vedením organizace
- 8. Zlepšování ISMS
- *Příloha A (Normativní) Cíle a opatření A5 – A15*

ISO/IEC 27001 Principy

P - Plan …….. Plánuj
D - Do …….. Dělej
C - Check …….. Kontroluj
A - Act …….. Jednej



Tento princip byl zaveden již do normy BS 7799:2002 (Převratná novela, která se podobala novele ISO 9001:2000

Termíny a definice 1

- aktivum = cokoliv, co má pro organizaci hodnotu
- bezpečnost informací = důvěrnost + integrita + dostupnost
- událost v ISMS = identifikovaný výskyt narušení, chyby zabezpečení nebo neznámé situace, mající vliv na ISMS
- incident v ISMS = jedna nebo více událostí v ISMS, která s významnou pravděpodobností může poškodit organizaci

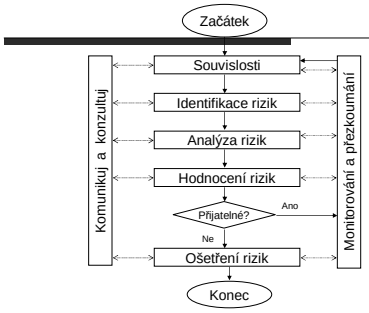
Termíny a definice 2

- integrita = zajištění správnosti a úplnosti informací
- analýza rizik = systematický odhad míry rizika a určení jeho zdrojů
- posuzování rizik (assessment) = analýza a hodnocení rizik
- vyhodnocení rizik (evaluation) = porovnání odhadu rizika vůči daným kriteriím

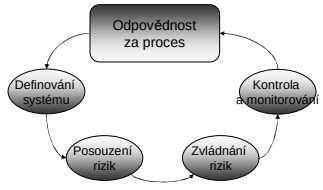
Termíny a definice 3

- akceptace rizika = rozhodnutí přijmout riziko
- zvládání rizik = výběr a přijímání opatření pro zmenšení rizik
- prohlášení o aplikovatelnosti = dokument popisující cíle a opatření, která jsou relevantní a aplikovatelná na ISMS v závislosti na vyhodnocení a zvládání rizik

Proces managementu rizik podle připravované ISO 31000



Proces managementu rizik

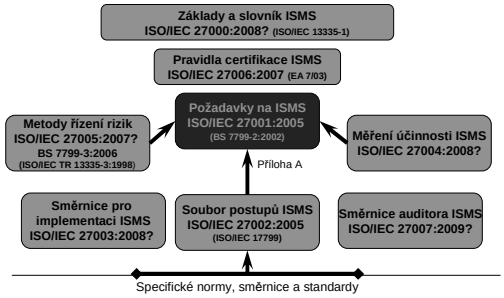


Politika v managementu rizik

1. Stanovuje principy (proč je důležitý management rizik) a demonstruje zapojení vrcholového managementu
2. Popisuje významná rizika organizace v kontextu příležitostí a faktorů úspěšnosti
3. Stanovuje cíle (co?) pro management rizik a určuje zdroje (kdo?)
4. Definuje rozsah managementu rizik (strategický, operativní, Subdodávky, el. pošta, produkty, procesy)
5. Ukazuje metodologie vyhodnocování rizik a kdy jsou aplikovány (ze shora dolů, ze zdola nahoru)
6. Vyjadřuje míru odpovědnosti vlastníků rizik a managerů rizik včetně externí podpory
7. Stanovuje, jak bude organizace monitorovat a řídit rizika a jak je struktura systému managementu propojena s dalšími firemními nástroji managementu jako ke plánování, controlling, zajištění jakosti a vnitřní kontrola

Představení normy ISO/IEC 27001 a norem souvisejících - Současný stav

Budoucí uspořádání řady norem ISO/IEC 27000



ISO/IEC 17799:2005

Soubor postupů pro řízení bezpečnosti informací

- Ucelená a vyvážená soustava opatření pro ochranu informačních aktiv
- Mezinárodně respektovaná soustava doporučení
- 11 oblastí bezpečnosti
- 39 cílů opatření
- 133 opatření
- Opatření obsahují popis způsobu implementace

ISO/IEC 17799:2005 (ČSN ISO/IEC 17799:2006)

Soubor postupů pro řízení bezpečnosti informací, který se v normě ISO/IEC 27001 promítá do Přílohy A, která je nedílnou součástí normy

- Ucelená a vyvážená soustava opatření pro ochranu informačních aktiv
- Mezinárodně respektovaná soustava doporučení
- 11 oblastí bezpečnosti
- 39 cílů opatření
- 133 opatření
- Opatření obsahují popis způsobu implementace

Opatření se týkají (ale nejsou omezena jen na) bezpečnosti dodávání externích služeb a poskytování outsourcingu, současná ohrožení, jako management patchů, lépe strukturované požadavky na personalistiku, větší důraz na práci s riziky a incidenty, přenosná zařízení, distribuce a zpracování informací

ČSN ISO/IEC 17799

Opatření

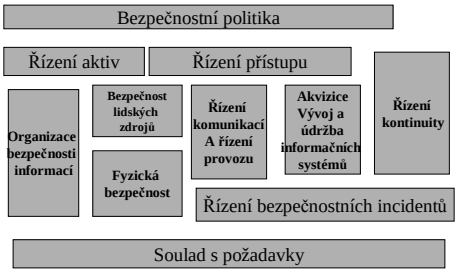
- **Návod na implementaci**

poskytuje detailní popis opatření s uvedením příkladů. Uvedený návod se nemusí nutně hodit na všechny možné případy a připouští se i jiná řešení

- **Další informace**

poskytuje detailní popis pro implementování opatření, včetně popisu faktorů, které musí být vzaty v úvahu (např. legislativa) při zavádění opatření

ČSN ISO/IEC 17799:2006 Oblasti bezpečnosti informací



ISO/IEC 2005
(ČSN ISO/IEC 2006)

- **Bezpečnostní politika**
- **Organizování bezpečnosti informací**
- **Management aktiv**
- **Bezpečnost lidských zdrojů**
- **Fyzická bezpečnost a bezpečnost prostředí**
- **Management komunikace a management provozu**
- **Management přístupu**
- **Nabídka, vývoj a udržování informačních systémů**
- **Management incidentů informační bezpečnosti**
- **Management kontinuity činnosti organizace**
- **Soulad s požadavky**

ISO/IEC 17799: 2000 a 2005
Může tato norma sloužit pro certifikaci?

- Norma není určena pro certifikaci, ale je komplementární s přílohou A normy ISO/IEC 27001, která je povinnou součástí normy.
- Norma ISO/IEC 27001 je určena pro certifikaci.

A5 Bezpečnostní politika

- **Dokument sdělující bezpečnostní politiku musí pojednávat o důležitých problémech:**
- **Jak se bezpečnost týká zaměstnanců**
- **Důraz na bezpečnost fyzickou a bezpečnost prostředí**
- **Míra bezpečnosti elektronické pošty**
- **Bezpečnost elektronických kancelářských systémů**
- **Politika přístupu k informacím**
- **Mobilní výpočetní prostředky a práce na dálku**
- **Politika o použití kryptografických nástrojů řízení**

A5 Bezpečnostní politika

- **Dokument sdělující politiku musí být schválen vedením a musí být vydán. Každoroční přezkoumání včetně schválení je důležité. Dokument musí být komunikován všem zaměstnancům.**
- **Dokument musí být pravidelně přezkoumáván**

A6 Organizace bezpečnosti informací
A 6.1 Interní organizace

- **Závazek vedení k bezpečnosti informací**
- **Koordinace bezpečnosti informací**
- **Přidělení odpovědností v oblasti bezpečnosti informací**
- **Proces autorizace u zařízení zpracovávajících informace**
- **Ujednání o důvěrnosti**
- **Kontakt s orgány veřejné správy**
- **Kontakty se specializovanými zainteresovanými skupinami**
- **Nezávislá přezkoumání bezpečnosti informací**

A6 Organizace bezpečnosti informací
A 6.2 Externí organizace

- **Identifikace rizik plynoucích z přístupu externích subjektů**
- **Bezpečnostní požadavky pro přístup klientů**
- **Bezpečnostní požadavky v dohodách se třetí stranou**

A.7 Řízení aktiv

A 7.1 Odpovědnost za aktiva
A 7.2 Klasifikace informací

- **Evidence aktiv**
- **Vlastnictví aktiv**
- **Přípustné použití aktiv**

- **Směrnice pro klasifikaci**
- **Označování a nakládání s informacemi**

A.8 Personální bezpečnost
A.8.1 Před zahájením pracovního poměru

- **Role a odpovědnosti**
- **Prověřování pracovníků**
- **Podmínky výkonu pracovní činnosti**

A.8 Personální bezpečnost
A.8.2 Během pracovního vztahu
A 8.3 Ukončení nebo změna pracovního vztahu

- **Odpovědnost vedoucích zaměstnanců**
- **Informovanost, vzdělávání a školení v oblasti bezpečnosti informací**
- **Disciplinární řízení**

- **Odpovědnosti při ukončení pracovního vztahu**
- **Navrácení aktiv**
- **Odebrání přístupových práv**

A.9 Fyzická bezpečnost a bezpečnost prostředí
A.9.1 Zabezpečené oblasti

- **Fyzický bezpečnostní perimetr**
- **Řízení fyzického přístupu osob**
- **Zabezpečení kanceláří, místností a zařízení**
- **Ochrana před hrozbami z vnějšku na prostředí**
- **Práce v zabezpečených prostorách**
- **Veřejně přístupné prostory, prostory příjmu zboží a nakládky**

A.9 Fyzická bezpečnost a bezpečnost prostředí
A.9.2 Bezpečnost zařízení

- **Umístění zařízení a jeho ochrana**
- **Podpůrná zařízení**
- **Bezpečnost kabeláže**
- **Údržba zařízení**
- **Bezpečnost zařízení mimo objekt**
- **Bezpečná likvidace nebo opakované použití zařízení**
- **Přemístění majetku**

A.10 Řízení komunikací a řízení provozu
A.10.1 Provozní postupy a odpovědnosti
A.10.2 Řízení dodávek služeb třetí strany

- **Dokumentované provozní postupy**
- **Řízení změn**
- **Oddělení povinností**
- **Oddělení vývojových, testovacích a provozních zařízení**

- **Dodávka služeb**
- **Monitorování a přezkoumání služeb třetí strany**
- **Řízení změn ve službách třetí strany**

A.10 Řízení komunikací a řízení provozu
A.10.3 Plánování a přejímání systémů
A.10.4 Ochrana proti škodlivým programům a mobilním kódům

A.10.5 Zálohování
A.10.6 Řízení bezpečnosti sítě

- **Kapacitní plánování**
- **Akceptace systému**
- **Nástroje řízení proti škodlivým programům**
- **Nástroje proti mobilním kódům**
- **Zálohování informací**
- **Síťová opatření**
- **Bezpečnost síťových služeb**

A.10 Řízení komunikací a řízení provozu
A.10.7 Bezpečnost při nakládání s médii
A.10.8 Výměna informací

- **Správa počítačových výměnných médií**
- **Likvidace médií**
- **Postupy pro nakládání s informacemi**
- **Bezpečnost systémové dokumentace**

- **Politika a postupy pro výměnu informací**
- **Dohody o výměně informací a programů**
- **Bezpečnost médií při přepravě**
- **Elektronické posílání zpráv**
- **Informační systémy organizace**

A.10 Řízení komunikací a řízení provozu
A.10.9 Služby elektronického obchodování
A.10.10 Monitorování

- **Elektronický obchod**
- **Online transakce**
- **Veřejně dostupné informace**

- **Auditní záznamy**
- **Monitorování používání systému**
- **Ochrana vytvořených záznamů**
- **Administrátorský a operátorský deník**
- **Záznam selhání**
- **Synchronizace hodin**

A 11 Řízení přístupu
A 11.1 Požadavky na řízení přístupu

Cíl: Řídit přístup k informacím.

Přístup k informacím a podnikovým (obchodním) postupům musí být řízen na základě požadavků politiky zabezpečení informací a celkové strategie a politiky podniku. Přitom musí být vzaty v úvahu všechny existující technické a technologické prostředky pro šíření a autorizaci informací.

A 11.2 Řízení přístupu uživatelů

Registrace uživatele
Řízení privilegovaného přístupu
Správa uživatelských hesel
Přezkoumání přístupových práv uživatelů

A 11.3 Odpovědnosti uživatelů

Cíl: Předcházet neoprávněnému přístupu uživatelů.

Pro účinné zabezpečení je důležitá kooperace oprávněných uživatelů. Uživatelé musí být obeznámeni s jejich odpovědnostmi za dodržování účinných kontrol přístupu, zvláště týkajících se použití hesel a zabezpečení zařízení uživatelů.

Informace a zařízení na zpracování informací musí být chráněny proti zneužití, úpravě nebo krádeži neoprávněnými osobami a pro minimalizování ztrát nebo poškození musí být použity odpovídající zabezpečovací mechanismy. (Např. „Prázdný stůl, čistá obrazovka“).

A 11.4 Řízení přístupu k sítím

Cíl: Ochránit síťové služby před neautorizovaným přístupem

Přístup jak k interním, tak externím síťovým službám musí být řízen a kontrolován. Kontrola je nutná také proto, aby uživatelé, kteří mají přístup k sítím a síťovým službám, neprozrazovali zabezpečení těchto síťových služeb. To lze zajistit např.:

a) užitím vhodných rozhraní mezi sítí organizace a sítěmi vlastněnými jinými organizacemi, nebo veřejnými sítěmi

b) užitím vhodných opravňujících mechanismů pro uživatele a zařízení

c) kontrolami přístupu uživatelů k informačním službám.

A 11.5 Řízení přístupu k operačnímu systému

Cíl: Předcházet neoprávněnému přístupu k operačním systémům počítače.

Pro zamezení přístupu k počítačovým prostředkům musí být použita bezpečnostní opatření na úrovni operačního systému. Tato zařízení musí být schopna následujících činností:

- identifikace a ověření identity uživatelů
- evidování úspěšných a neúspěšných přístupů k systému
- poskytování odpovídajících prostředků pro ověřování; pokud je použitý systém kontroly heslem, musí zajistit správu hesel
- tam, kde je to vhodné, realizovat omezení doby připojení uživatelů.

A 11.6 Řízení přístupu k informacím a k aplikacím

Cíl: Předcházet neoprávněnému přístupu k informacím, uloženým v informačních systémech.

Pro omezení přístupu do aplikačních systémů musí být použita zabezpečovací opatření. Přístup k softwaru a informacím musí být omezen pouze na oprávněné uživatele.

Aplikační systémy:

a) musí kontrolovat přístup uživatele k informacím a k funkcím aplikace v souladu s definovaným postupem řízení přístupu

b) musí zajišťovat ochranu proti neoprávněnému přístupu pro jakýkoli obslužný program, který je schopný překlenout kontroly systému a aplikace

c) nesmí narušit bezpečnost ostatních systémů, se kterými jsou sdíleny zdroje informací

d) musí být schopny zajistit přístup k informacím pouze vlastníkovi a oprávněným osobám nebo skupinám uživatelů.

A 11.7 Mobilní výpočetní prostředky a práce na dálku

Cíl: Zajistit zabezpečení informací při použití přenosných počítačových zařízení a zařízení pro zaměstnání na dálku.

Požadovaná ochrana musí být přiměřená rizikům těchto specifických způsobů práce. Při použití přenosných počítačových zařízení musí být rizika práce v nechráněném prostředí zvážena a musí být aplikována odpovídající ochrana. Při použití zařízení pro zaměstnání na dálku musí organizace aplikovat ochranu v místě vzdáleného zaměstnání a zajistit vhodné dohody pro tento způsob práce.

A 12 Sběr dat, vývoj a údržba systému
A 12. 1 Požadavky na bezpečnost informačních systémů

Cíl: Zajistit, aby bylo zabezpečení proti případným incidentům bylo nedílnou součástí informačních systémů.

To zahrnuje infrastrukturu, podnikové aplikace a uživatelem vyvinuté aplikace. Požadavky na zabezpečení musí být určeny a odsouhlaseny před vývojem informačních systémů.

Všechny požadavky na zabezpečení, včetně pravidel pro zálohování, musí být určeny ve fázi požadavků projektu a odůvodněny, odsouhlaseny a dokumentovány jako součást projektu informačního systému.

A 12.2 Správný postup v aplikacích

Cíl: Předcházet ztrátě, úpravám nebo zneužití uživatelských dat v aplikačních systémech.

Do aplikačních systémů, včetně uživatelem psaných aplikací, musí být navrženy vhodné kontroly a kontrolní záznamy. Ty musí zahrnovat ověřování vstupních dat, postupů vnitřního zpracování a výstupních dat. Další opatření mohou být nutná pro systémy, které zpracovávají nebo mají dopad na tajné, cenné nebo rozhodující informace. Taková opatření musí být stanovena na základě požadavků na zabezpečení a analýzy rizik.

A 12.3 Kryptografické kontroly

Cíl: Chránit důvěrnost, autentičnost a integritu informací.

Kryptografické systémy a metody se používají pro ochranu informací, které se považují za informace, které jsou ohroženy a pro které jiné kontroly neposkytují adekvátní ochranu. Použití kryptografických kontrol, šifrování, digitální podpisy, průkazní služby, správa klíčů a další normy, postupy a metody musí být řízeny a dokumentovány v souladu s informační politikou podniku.

A 12.4 Bezpečnost systémových souborů

Cíl: Zajistit bezpečnost systémových souborů

Přístup k systémovým souborům musí být řízen. Za udržování integrity systémů musí být stanoveni odpovědní pracovníci nebo vývojové skupiny, kterým aplikační systém nebo software patří.

A 12.5 Bezpečnost procesů vývoje a podpory

Cíl: Udržovat bezpečnost aplikačních programů a informací.

Projektová a podpůrná prostředí musí být přísně kontrolována. Vedoucí odpovědní za aplikační systémy musí být odpovědní také za zabezpečení projektových a podpůrných prostředí. Musí zajišťovat, že všechny navrhované změny systémů jsou řízeny, že nepoškozují zabezpečení ani systému ani operačního prostředí.

A 12.6 Management technické zranitelnosti (nové)

Cíl: Redukovat rizika pramenící z využívání publikovaných technických zranitelností

Musí se vyžadovat a získávat aktuální informace o technických zranitelnostech informačních systémů, vyhodnocovat náchylnost k těmto zranitelnostem a přijímat vhodná opatření k k minimalizaci rizik.

A 13 Řízení incidentů v oblasti bezpečnosti informací
A 13.1 Hlášení událostí a slabých míst

Cíl: Zajistit, aby byly včas komunikovány mimořádné události v rámci ISMS a slabá místa způsobem, umožňujícím přijmout včas opatření k nápravě

Události, ovlivňující zabezpečení informací musí být hlášeny prostřednictvím vhodných řídicích kanálů co nejrychleji. Všichni zaměstnanci a smluvní strany musí být uvědoměni o postupech hlášení různých typů událostí (porušení, ohrožení, oslabení nebo nesprávná činnost zabezpečení informací), které mohou mít dopad na zabezpečení organizačních majetků. Všechny podezřelé události musí být hlášeny co nejrychleji do určeného styčného bodu.

A 13.2 Správa informačních incidentů a zlepšení (nové)

Cíl: Zajistit, aby byl aplikován konzistentní a efektivní přístup k managementu bezpečnostních incidentů

Musí být stanoveny odpovědnosti a postupy pro zajištění rychlé a systematické odezvy na informaci o incidentu. Tam, kde dochází k následné akci proti osobám nebo organizaci po incidentu, jenž souvisí s porušením právních předpisů, musí být shromážděny a uchovány důkazy.

A 14 Řízení kontinuity činností
A 14.1 Aspekty řízení kontinuity činností organizace 1

Cíl: Bránit přerušení podnikových činností a chránit rozhodující podnikové procesy před následky závažných chyb, nebo havárií a zajistit jejich včasné navrácení do původního stavu.

Proces řízení kontinuity podniku musí být zaveden za účelem redukce narušení podnikových činností způsobeného haváriemi a poruchami zabezpečení (které mohou být výsledkem např. přírodních katastrof, neštěstí, poruch zařízení a úmyslných jednání) na akceptovatelné úrovni pomocí kombinace preventivních a regeneračních opatření.

A 14.1 Aspekty řízení kontinuity činností organizace 2

Následky havárií, poruch zabezpečení a ztrát služeb musí být analyzovány. Musí být vypracovány a zavedeny havarijní plány, které zajistí obnovení podnikových procesů v požadované době. Tyto plány musí být udržovány, testovány a zdokonalovány, aby se staly nedílnou součástí všech dalších řídicích procesů. Řízení kontinuity podniku musí zahrnovat kontroly pro určení a snížení rizik, omezení následků poškozujících událostí a zajištění včasného obnovení důležitých operací.

A 15 Soulad s požadavky
A 15.1 Soulad s právními požadavky

Cíl: Vyvarovat se porušení jakýchkoliv norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků.

Konstrukce, provoz, použití a správa informačních systémů mohou podléhat statutárním, regulačním a smluvním bezpečnostním požadavkům. Pro specifické právní požadavky je účelné využít poradenství u právních poradců. Legislativní požadavky se mohou v různých státech lišit a také se mohou lišit pro informace vytvořené v jedné zemi, které jsou převáděny do druhé země. Nejčastějším takovým požadavkem je ochrana autorských práv, ochrana osobních dat, kvalita, přípustnost a kompletnost důkazů.

A 15.2 Posouzení shody s bezpečnostními politikami a normami

Cíl: Zajistit shodu systémů s bezpečnostní politikou a normami organizačního zabezpečení.

Zabezpečení informačních systémů musí být pravidelně kontrolováno a revidováno. Tyto revize musí být prováděny v souladu s příslušnou politikou zabezpečení. Technické platformy a informační systémy musí být spravovány tak, aby byla zajištěna shoda s normami implementace zabezpečení.

A 15.3 Aspekty auditu informačních systémů

Cíl: Maximalizovat účinnost procesu auditu systému a minimalizovat zásahy do něho nebo z něho.

Pro zabezpečení provozních systémů a prostředků během auditu ochrany informací musí být stanovena odpovídající opatření. Je rovněž nezbytné zabezpečit neporušenost informačních zdrojů a zamezit zneužití prostředků auditu.