Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Systém manažérstva (riadenia) informačnej bezpečnosti
–
Information security management system (ISMS)

Michal Bubák

Máj 2013

KPMG
cutting through complexity™

Agenda

- Význam, história, vzťahy
- Systém manažérstva informačnej bezpečnosti - Procesy
- Požiadavky na dokumentáciu
- Zodpovednosť manažmentu
- Interné audity
- Manažérske preskúmanie
- Zlepšovanie ISMS
- Príloha A - Ciele riadenia a opatrenia
- Záver

Význam ISMS

- Každá organizácia má systém riadenia informačnej bezpečnosti s rôznym stupňom formálnosti a dokumentácie.
- Štandard poskytuje model pre systematický prístup k riadeniu informačnej bezpečnosti.
- Certifikácia systému manažérstva informačnej bezpečnosti podľa štandardu.

Štandard a jeho historický vývoj

- Pôvodný štandard BS 7799:1998
  - Časť 1 Pravidlá dobrej praxe manažérstva informačnej bezpečnosti
  - Časť 2 Systémy manažérstva informačnej bezpečnosti

- Časť jedna prevzatá ako ISO/IEC 17799:2000, neskôr vydaná ako **ISO/IEC 27002**:2005
- Časť dva prevzatá ako **ISO/IEC 27001**:2005
- Ďalšie štandardy zo skupiny ISO/IEC 27000

- **STN ISO/IEC 27001**:2006 Informačné technológie. Zabezpečovacie techniky. Systémy manažérstva informačnej bezpečnosti. Požiadavky
- **STN ISO/IEC 27002**:2006 Informačné technológie. Zabezpečovacie techniky. Pravidlá dobrej praxe manažérstva informačnej bezpečnosti

Vzťah k iným systémom riadenia

Iné systémy riadenia:

- ISO 9001:2000 Systém manažérstva kvality
- ISO 14001:2004 Systém environmentálneho manažérstva

Kompatibilita systémov riadenia

- Uvedené systémy riadenia sú konzistentné, kompatibilné a implementovateľné ako jeden integrovaný systém riadenia
- Príloha C obsahuje mapovanie medzi požiadavkami jednotlivých systémov

Model PDCA aplikovaný na procesy ISMS

Plánovať (zavedenie ISMS) – **PLAN**

- Navrhnúť bezpečnostnú politiku, ciele, procesy a procedúry relevantné pre manažment rizika a zlepšovanie informačnej bezpečnosti, s cieľom priniesť výsledky v súlade s celkovou politikou a cieľmi organizácie.

Vykonávať (implementovať a prevádzkovať ISMS) – **DO**

- Implementovať a prevádzkovať bezpečnostnú politiku, opatrenia, procesy a procedúry.

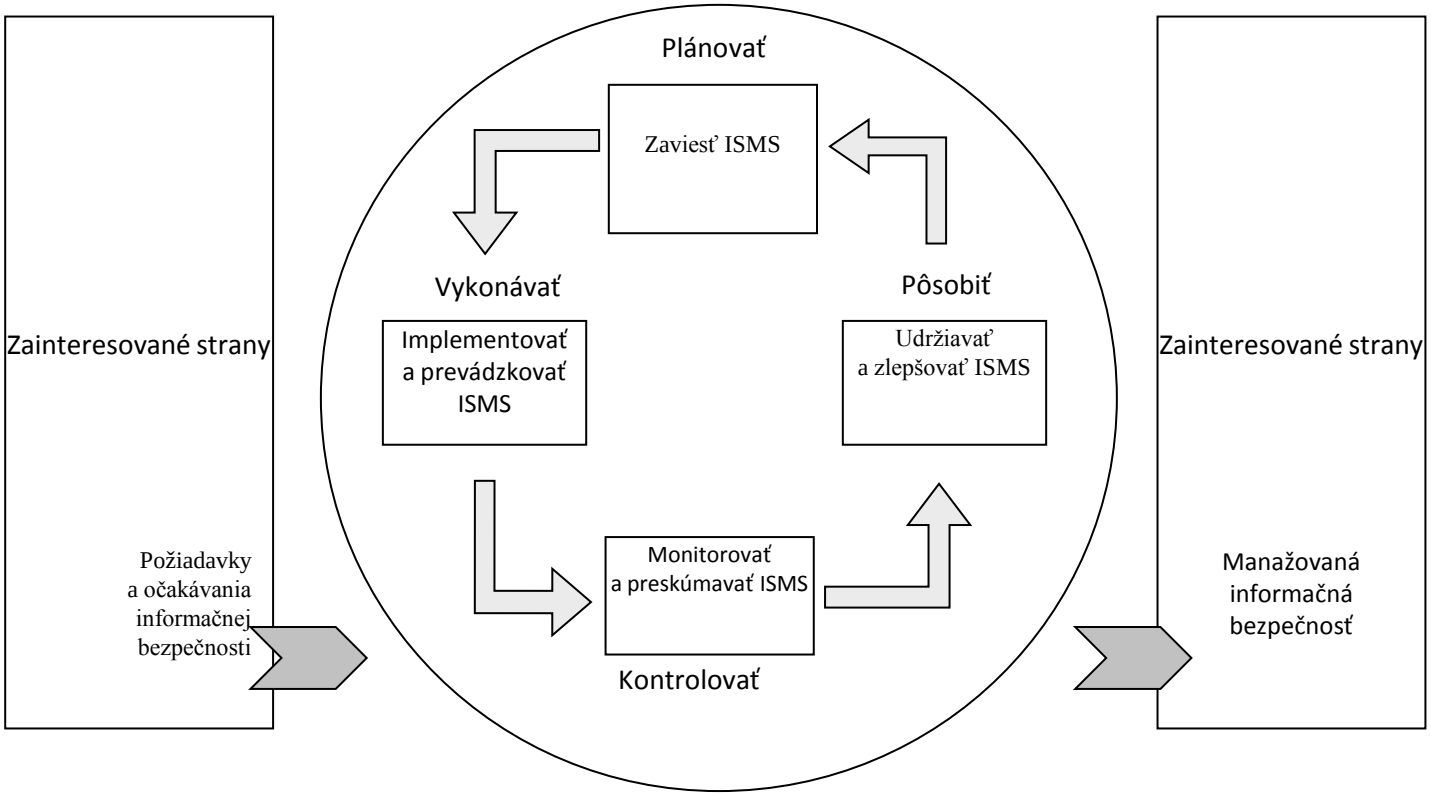
Kontrolovať (monitorovať a preskúmavať ISMS) – **CHECK**

- Ohodnocovať a tam, kde je to vhodné, merať výkonnosť procesov voči politike ISMS, cieľom a praktickým skúsenostiam a oznamovať výsledky manažmentu na preskúmanie.

Pôsobiť (udržiavať a zlepšovať ISMS) – **ACT**

- Vykonávať nápravné a preventívne činnosti, založené na výsledkoch interných auditov ISMS, preskúmania manažmentom alebo iných relevantných informácií s cieľom dosiahnuť kontinuálne zlepšovanie ISMS.

Model PDCA aplikovaný na procesy ISMS



4.2.1 Zavedenie ISMS

V rámci zavedenia ISMS podľa štandardu musí organizácia vykonať nasledovné:

1. definovať rozsah a hranice ISMS
2. definovať politiku ISMS
   - Určenie cieľov a celkové chápanie smerovania a zásad konania vzhľadom na informačnú bezpečnosť
3. definovať systematický prístup na ohodnotenie rizík
   - metóda ohodnotenia rizika
   - kritériá na akceptovanie rizík
   - prijateľné úrovne rizika
4. identifikovať riziká
   - identifikovať aktíva a ich vlastníkov
   - identifikovať hrozby pre tieto aktíva
   - identifikovať zraniteľnosti, ktoré by mohli byť zneužité hrozbami
   - Identifikovať dopady na aktíva pri strate dôvernosti, integrity a dostupnosti

4.2.1 Zavedenie ISMS

V rámci zavedenia ISMS podľa štandardu musí organizácia vykonať nasledovné :

5. analyzovať a ohodnotiť riziká
   - určiť podnikateľské dopady na organizáciu
   - určiť realistickú pravdepodobnosť výskytu zlyhania bezpečnosti
   - odhadnúť úroveň rizík
   - určiť, či je riziko akceptovateľné, resp. či si vyžaduje ošetrenie
6. identifikovať a ohodnotiť možnosti ošetrenia rizík
   - aplikovanie vhodných opatrení
   - vedomé a objektívne akceptovanie rizík
   - vyhnutie sa rizikám
   - prenesenie súvisiacich podnikateľských rizík na iné strany

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

4.2.1 Zavedenie ISMS

V rámci zavedenia ISMS podľa štandardu musí organizácia vykonať nasledovné :

7. vybrať ciele riadenia a opatrenia na ošetrenie rizík
   - Ciele riadenia a opatrenia musia byť zvolené a implementované tak, aby spĺňali požiadavky identifikované v procese ohodnotenia a ošetrenia rizík
   - Ciele riadenia a opatrenia uvedené v **prílohe A** nie sú vyčerpávajúce, a teda môžu byť zvolené aj iné
8. získať schválenie manažmentu o navrhovaných zostatkových rizikách
9. získať autorizáciu manažmentu pre implementáciu a prevádzku ISMS
10. pripraviť vyhlásenie o aplikovateľnosti (Statement of Applicability)
    - zvolené ciele riadenia a opatrenia a dôvody ich zvolenia
    - ciele riadenia a opatrenia, ktoré sú v súčasnosti implementované
    - výluku z prílohy A a zdôvodnenie tejto výluky

KPMG
cutting through complexity™

4.2.2 Implementácia a prevádzka ISMS

V rámci implementácie a prevádzky ISMS podľa štandardu musí organizácia vykonať nasledovné:

1. formulovať plán ošetrovania rizík - kroky, zdroje, zodpovednosti a priority manažmentu rizík
2. implementovať plán ošetrovania rizík - financovanie a rozdelenia rôl a zodpovedností
3. definovať spôsob, akým sa musí merať efektivita zvolených opatrení

4.2.2 Implementácia a prevádzka ISMS

V rámci implementácie a prevádzky ISMS podľa štandardu musí organizácia vykonať nasledovné:

4. implementovať programy školení a budovania povedomia
5. manažovať prevádzku ISMS
6. manažovať zdroje ISMS
7. implementovať procedúry a iné opatrenia schopné umožniť rýchlu detekciu bezpečnostných udalostí a reagovanie na bezpečnostné incidenty

4.2.3 Monitorovanie a preskúmavanie ISMS

V rámci monitorovania a preskúmavania ISMS podľa štandardu musí organizácia vykonávať nasledovné:

1. realizovať procedúry monitorovania a preskúmania a iné opatrenia na:
   - rýchle zistenie chýb vo výsledkoch spracovania
   - rýchle identifikovanie zlyhaných a úspešných prienikov bezpečnosti a incidentov
   - určenie, či sa bezpečnostné aktivity vykonávajú podľa očakávania
   - napomáhať pri odhaľovaní bezpečnostných udalostí a tým predchádzať bezpečnostným incidentom
   - určenie, či podniknuté kroky, smerujúce k vysporiadaniu sa s porušením bezpečnosti, boli efektívne
2. vykonávať pravidelné preskúmanie efektivity ISMS
3. merať efektivitu opatrení s cieľom overiť, či boli splnené bezpečnostné požiadavky
4. preskúmavať ohodnotenie rizík v plánovaných intervaloch a preskúmavať úroveň zvyškového rizika a prijateľného rizika, berúc do úvahy relevantné zmeny

4.2.3 Monitorovanie a preskúmavanie ISMS

V rámci monitorovania a preskúmavania ISMS podľa štandardu musí organizácia vykonávať nasledovné:

5. vykonávať interné audity ISMS v plánovaných intervaloch
6. vykonávať preskúmanie ISMS manažmentom
7. aktualizovať bezpečnostné plány tak, aby brali do úvahy zistenia vyplývajúce z procesu monitorovania a preskúmania
8. zaznamenávať úkony a udalosti, ktoré by mohli mať vplyv na efektivitu alebo výkonnosť ISMS

4.2.4 Údržba a zlepšovanie ISMS

V rámci udržiavania a zlepšovania ISMS podľa štandardu musí organizácia vykonávať nasledovné:

1. implementovať identifikované zlepšenia v ISMS
2. vykonávať vhodné nápravné a preventívne činnosti
3. oznamovať úkony a vylepšenia zainteresovaným stranám v primeranej miere
4. zaisťovať, aby zlepšenia dosahovali zamýšľané ciele

4.3 Požiadavky na dokumentáciu

Dokumentáciu tvoria **dokumenty** a **záznamy**.

Dokumentácia musí obsahovať záznamy o rozhodnutiach manažmentu a zabezpečí, že činnosti sú spätne sledovateľné k rozhodnutiam manažmentu a politikám.

Je dôležité, aby bolo možné preukázať spojitosti od zvolených opatrení spätne k výsledkom ohodnotenia a ošetrenia rizík a následne spätne k politike a cieľom ISMS.

4.3 Požiadavky na dokumentáciu

Dokumentácia ISMS musí obsahovať:

- dokumentované formulácie politiky ISMS
- rozsah ISMS
- procedúry a opatrenia podporujúce ISMS
- opis metodológie na ohodnocovanie rizík
- správu (správy) o ohodnotení rizík
- plán ošetrovania rizík
- dokumentované procedúry potrebné na zaistenie efektívneho plánovania, prevádzky a manažmentu svojich procesov informačnej bezpečnosti a na opísanie spôsobu, akým sa musí merať efektivita opatrení
- záznamy požadované štandardom
- vyhlásenie o aplikovateľnosti

4.3.2 Riadenie dokumentov

Dokumenty, ktoré sú nevyhnutné pre ISMS musia byť chránené a riadené.

V rámci riadenia dokumentov musí byť zabezpečené nasledovné:

- schválenie dokumentov na príslušnej úrovni riadenia pred ich vydaním;
- preskúmavanie a aktualizácia dokumentov podľa potreby a ich opätovné schválenie;
- aby zmeny a stav aktuálnych verzií dokumentov boli identifikované;
- aby najaktuálnejšie verzie relevantných dokumentov boli k dispozícii na miestach ich použitia;
- aby dokumenty boli čitateľné a ľahko identifikovateľné;
- aby dokumenty boli dostupné pre tých, ktorí ich potrebujú a aby boli presúvané, uchovávané a nakoniec vyradené v súlade s príslušnými procedúrami vzhľadom na ich klasifikačný stupeň;
- aby dokumenty externého pôvodu boli identifikované;
- aby distribúcia dokumentov bola riadená;
- predchádzanie neúmyselnému používaniu zastaraných dokumentov

4.3.3 Riadenie záznamov

- Záznamy musia byť vytvárané a udržiavané tak, aby poskytovali dôkaz o súlade s požiadavkami a o efektívnom fungovaní ISMS.
- Záznamy musia byť chránené, riadené, čitateľné, ľahko identifikovateľné a dohľadateľné.
- Opatrenia potrebné na identifikáciu, uloženie, ochranu, vyhľadanie, stanovenie času uchovávania a používania záznamov musia byť zdokumentované a implementované.

Príklady záznamov:

- kniha návštev
- auditné záznamy
- vyplnené formuláre autorizácie prístupu
- zápisy zo stretnutí

5. Zodpovednosť manažmentu

Záväzok manažmentu

- Zavedenie a schválenie dokumentov
- Stanovenie cieľov a plánov
- Pridelenie rôl a zodpovedností
- Stanovenie kritérií na akceptovanie rizík a prijateľnej úrovne rizika
- Zaistenia realizácie interných auditov ISMS
- Manažérske preskúmanie ISMS

Poskytovanie zdrojov

- Finančné zdroje
- Ľudské zdroje

Školenie, povedomie a kompetentnosť

6. Interné audity ISMS

Spoločnosť musí v plánovaných intervaloch vykonávať interné audity ISMS s cieľom určiť, či ciele riadenia, opatrenia, procesy a procedúry ISMS spĺňajú nasledovné:

- vyhovujú požiadavkám normy a relevantnej legislatívy alebo predpisov;
- vyhovujú identifikovaným požiadavkám informačnej bezpečnosti;
- sú efektívne implementované a udržiavané; a
- sú vykonávané podľa očakávania.

Program auditu musí byť plánovaný, brať do úvahy stav a **dôležitosť procesov a oblastí**, ktoré majú byť auditované, rovnako ako výsledky predošlých auditov.

Musia byť definované kritériá, pôsobnosť, frekvencia a metódy auditov. Plánovanie a vykonávanie auditov, oznamovanie výsledkov a udržiavanie záznamov musí byť definované v **dokumentovanej procedúre**.

Výber audítorov a výkon auditov musia zaisťovať **objektivitu** a **nestrannosť** procesu auditu.

7. Preskúmanie ISMS manažmentom

Manažment musí preskúmavať ISMS organizácie v plánovaných intervaloch (minimálne 1 krát ročne).

Cieľ je zaistiť jeho kontinuálnu primeranosť, vhodnosť a efektívnosť.

Výsledky preskúmania musia byť jasne dokumentované a musia sa o nich udržiavať záznamy.

7. Preskúmanie ISMS manažmentom

Vstupy do preskúmaní vykonávaných manažmentom musia obsahovať informácie o:

- výsledkoch auditov a preskúmaní ISMS;
- spätnej väzbe zainteresovaných strán;
- technikách alebo procedúrach, ktoré by mohli byť v organizácii použité na zlepšenie výkonnosti a efektivity ISMS;
- stave preventívnych a nápravných činností;
- zraniteľnostiach alebo hrozbách, ktorými sa predošlé ohodnotenie rizík primerane nezaoberalo;
- výsledkoch meraní efektivity;
- následných činnostiach po predošlých preskúmaniach manažmentom;
- všetkých zmenách, ktoré by mohli ovplyvniť ISMS; a
- odporúčaniach na zlepšenia.

7. Preskúmanie ISMS manažmentom

Výstupy z preskúmaní vykonávaných manažmentom musia obsahovať všetky rozhodnutia a činnosti týkajúce sa:

- zlepšenia efektivity ISMS
- aktualizácie ohodnotenia rizík a plánu ošetrovania rizík
- modifikácie procedúr a opatrení, ktoré ovplyvňujú informačnú bezpečnosť
- potreby zdrojov
- zlepšenia v spôsobe, akým sa meria efektivita opatrení

8. Zlepšovanie ISMS

Kontinuálne zlepšovanie

Spoločnosť musí kontinuálne zlepšovať efektivitu ISMS prostredníctvom používania politiky informačnej bezpečnosti, cieľov informačnej bezpečnosti, výsledkov auditov, analýz monitorovaných udalostí, nápravných a preventívnych činností a manažérskych preskúmaní.

Nápravné činnosti

Spoločnosť musí vykonávať činnosti na eliminovanie príčin nezhôd voči požiadavkám ISMS s cieľom predísť ich opätovnému výskytu.

Preventívne činnosti

Spoločnosť musí určovať činnosti na eliminovanie príčin potenciálnych nezhôd voči požiadavkám ISMS, s cieľom predísť ich výskytu.

Dokumentovaná procedúra pre nápravné činnosti a preventívne činnosti.

Príloha A - Ciele riadenia a opatrenia

A.5 - Bezpečnostná politika

A.5.1 - Politika informačnej bezpečnosti

Cieľ riadenia: Poskytnúť usmernenie manažmentu a podporu informačnej bezpečnosti v súlade s obchodnými požiadavkami a relevantnými zákonmi a vyhláškami.

- A.5.1.1 - Dokument politiky informačnej bezpečnosti
- A.5.1.2 - Preskúmanie politiky informačnej bezpečnosti

A.6 - Organizácia informačnej bezpečnosti

A.6.1 - Interná organizácia

Cieľ riadenia: Riadiť informačnú bezpečnosť v organizácii.

- A.6.1.1 - Záväzok manažmentu smerom k informačnej bezpečnosti
- A.6.1.2 - Koordinácia informačnej bezpečnosti
- A.6.1.3 - Pridelenie zodpovedností za informačnú bezpečnosť
- A.6.1.4 - Autorizačný proces pre prostriedky spracúvajúce informácie
- A.6.1.5 - Dohody o zachovaní dôvernosti
- A.6.1.6 - Kontakt so štátnou mocou
- A.6.1.7 - Kontakt so špecifickými záujmovými skupinami
- A.6.1.8 - Nezávislé preskúmanie informačnej bezpečnosti

A.6 - Organizácia informačnej bezpečnosti

A.6.2 - Externé subjekty

Cieľ riadenia: Udržiavanie bezpečnosti informácií a prostriedkov organizácie na ich spracovanie, ktoré sú sprístupnené, spracúvané, oznamované alebo spravované externými subjektmi.

- A.6.2.1 - Identifikácia rizík spojených s externými subjektmi
- A.6.2.2 - Riešenie bezpečnosti pri styku so zákazníkmi
- A.6.2.3 - Riešenie bezpečnosti v zmluvách s tretími stranami

A.7 - Riadenie aktív

A.7.1 - Zodpovednosť za aktíva

Cieľ riadenia: Dosiahnuť a udržiavať primeranú ochranu aktív organizácie.

- A.7.1.1 - Inventárny zoznam aktív
- A.7.1.2 - Vlastníctvo aktív
- A.7.1.3 - Prijateľné použitie aktív

A.7.2 - Klasifikácia informácií

Cieľ riadenia: Zabezpečiť, že informácie získajú vhodnú úroveň ochrany.

- A.7.2.1 - Klasifikačné smernice
- A.7.2.2 - Označovanie informácií a nakladanie s nimi

A.8 - Bezpečnosť ľudských zdrojov

A.8.1 - Pred nástupom do zamestnania

Cieľ riadenia: Zabezpečiť, že zamestnanci, zmluvní partneri a používatelia v pozícií tretích strán rozumejú svojim zodpovednostiam a že sú vhodní na výkon rôl, ktoré im boli pridelené a že sa tak zníži riziko krádeže, podvodu alebo zneužitia zariadení.

- A.8.1.1 - Roly a zodpovednosť
- A.8.1.2 - Proces preverovania
- A.8.1.3 - Pracovná náplň a podmienky zamestnania

A.8 - Bezpečnosť ľudských zdrojov

A.8.2 - Počas zamestnania

Cieľ riadenia: Zabezpečiť, že zamestnanci, zmluvní partneri a používatelia v pozícii tretích strán sú si vedomí hrozieb týkajúcich sa informačnej bezpečnosti, ich zodpovednosti a záväzkov a že sú pripravení podporovať politiku informačnej bezpečnosti organizácie v priebehu ich každodennej činnosti, ako aj znižovať riziká ľudskej chyby.

- A.8.2.1 - Manažérske zodpovednosti
- A.8.2.2 - Povedomie o informačnej bezpečnosti, vzdelávanie a školiaca činnosť
- A.8.2.3 - Disciplinárny proces

A.8 - Bezpečnosť ľudských zdrojov

A.8.3 - Ukončenie alebo zmena pracovnoprávneho vzťahu

Cieľ riadenia: Zabezpečiť, že zamestnanci, zmluvní partneri a používatelia v pozícii tretích strán opustia organizáciu alebo zmenia podmienky svojho vzťahu primeraným spôsobom.

- A.8.3.1 - Zodpovednosti v súvislosti s ukončením pracovnoprávneho vzťahu
- A.8.3.2 - Vrátenie aktív
- A.8.3.3 - Odňatie prístupových práv

A.9 - Fyzická bezpečnosť a bezpečnosť prostredia

A.9.1 - Zabezpečené oblasti

Cieľ riadenia: Zabrániť neautorizovanému fyzickému prístupu, poškodeniu a ohrozovaniu priestorov a informácií spoločnosti.

- A.9.1.1 - Perimeter fyzickej bezpečnosti
- A.9.1.2 - Opatrenia pre fyzický prístup
- A.9.1.3 - Zabezpečenie kancelárií, miestností a prostriedkov
- A.9.1.4 - Ochrana pred vonkajšími hrozbami a hrozbami prostredia
- A.9.1.5 - Práca v zabezpečených oblastiach
- A.9.1.6 - Verejne prístupné priestory, zásobovacie a expedičné oblasti

A.9 - Fyzická bezpečnosť a bezpečnosť prostredia

A.9.2 - Bezpečnosť zariadení

Cieľ riadenia: Predísť strate, poškodeniu alebo kompromitácii aktív a prerušeniu podnikových aktivít.

- A.9.2.1 - Umiestnenie a ochrana zariadení
- A.9.2.2 - Podporné služby
- A.9.2.3 - Bezpečnosť kabeláže
- A.9.2.4 - Údržba zariadení
- A.9.2.5 - Bezpečnosť zariadení mimo priestorov organizácie
- A.9.2.6 - Bezpečná likvidácia alebo opätovné použitie zariadení
- A.9.2.7 - Premiestňovanie majetku

A.10 - Riadenie komunikácie a prevádzky

A.10.1 - Prevádzkové postupy a zodpovednosti

Cieľ riadenia: Zabezpečiť správnu a bezpečnú prevádzku prostriedkov spracúvajúcich informácie.

- A.10.1.1 - Dokumentované prevádzkové postupy
- A.10.1.2 - Riadenie zmien
- A.10.1.3 - Oddeľovanie povinností
- A.10.1.4 - Separácia prostriedkov vývoja, testovania a prevádzky

A.10 - Riadenie komunikácie a prevádzky

A.10.2 - Riadenie dodávky služieb poskytovaných tretími stranami

Cieľ riadenia: Implementovať a udržiavať primeranú úroveň informačnej bezpečnosti a dodávky služieb v súlade so znením dohôd o dodávke služieb tretími stranami.

- A.10.2.1 - Dodávka služieb
- A.10.2.2 - Monitorovanie a preskúmanie služieb poskytovaných tretími stranami
- A.10.2.3 - Riadenie zmien týkajúcich sa služieb poskytovaných tretími stranami

A.10.3 - Plánovanie a akceptácia systému

Cieľ riadenia: Minimalizovať riziko zlyhania systému.

- A.10.3.1 - Riadenie kapacít
- A.10.3.2 - Akceptácia systému

A.10 - Riadenie komunikácie a prevádzky

A.10.4 - Ochrana proti škodlivému softvéru

Cieľ riadenia: Chrániť integritu softvéru a informácií.

- A.10.4.1 - Opatrenia proti škodlivému kódu
- A.10.4.2 - Opatrenia ochrany proti mobilnému kódu

A.10.5 – Zálohovanie

Cieľ riadenia: Udržovať integritu a dostupnosť informácií a prostriedkov na ich spracovanie.

- A.10.5.1 - Zálohovanie informácií

A.10 - Riadenie komunikácie a prevádzky

A.10.6 - Riadenie sietí

Cieľ riadenia: Zaistiť ochranu informácií v sieťach a ochranu podpornej infraštruktúry.

- A.10.6.1 - Sieťové opatrenia
- A.10.6.2 - Bezpečnosť sieťových služieb

A.10 - Riadenie komunikácie a prevádzky

A.10.7 - Manipulácia s médiami

Cieľ riadenia: Zabrániť neautorizovanému prezradeniu, modifikácii, odstráneniu alebo zničeniu aktív alebo prerušeniu obchodných aktivít.

- A.10.7.1 - Riadenie prenosných počítačových médií
- A.10.7.2 - Likvidácia médií
- A.10.7.3 - Postupy manipulácie s informáciami
- A.10.7.4 - Bezpečnosť systémovej dokumentácie

A.10 - Riadenie komunikácie a prevádzky

A.10.8 - Výmeny informácií a softvéru

Cieľ riadenia: Zachovať bezpečnosť informácií a softvéru vymieňaných medzi organizáciou a externým subjektom.

- A.10.8.1 - Politiky a postupy o výmene informácií
- A.10.8.2 - Dohody o výmene
- A.10.8.3 - Fyzické média počas prenosu
- A.10.8.4 - Výmena elektronických správ
- A.10.8.5 - Informačné systémy organizácie (prepojené systémy)

A.10 - Riadenie komunikácie a prevádzky

A.10.9 - Služby elektronického obchodu

Cieľ riadenia: Zaistenie bezpečnosti služieb elektronického obchodu a ich bezpečného použitia.

- A.10.9.1 - Elektronický obchod
- A.10.9.2 - On-line transakcie
- A.10.9.3 - Verejne dostupné informácie

A.10 - Riadenie komunikácie a prevádzky

A.10.10 - Monitoring

Cieľ riadenia: Zistiť neautorizované aktivity v súvislosti so spracovaním informácií.

- A.10.10.1 - Auditné log záznamy
- A.10.10.2 - Monitorovanie používania systému
- A.10.10.3 - Ochrana informácií obsiahnutých v log záznamoch
- A.10.10.4 - Log záznamy o činnosti operátorov a administrátorov
- A.10.10.5 - Log záznamy o chybách
- A.10.10.6 - Synchronizácia hodín

A.11 - Riadenie prístupu

A.11.1 - Požiadavky na riadenie prístupu

Cieľ riadenia: Riadiť prístup k informáciám.

- A.11.1.1 - Politika riadenia prístupu

A.11.2 - Riadenie prístupu používateľov

Cieľ riadenia: Zabezpečiť autorizovaný prístup používateľov a zabrániť neautorizovanému prístupu do informačných systémov.

- A.11.2.1 - Registrácia používateľov
- A.11.2.2 - Riadenie privilégií
- A.11.2.3 - Riadenie používateľských hesiel
- A.11.2.4 - Preskúmanie prístupových práv používateľov

A.11 - Riadenie prístupu

A.11.3 - Zodpovednosti používateľov

Cieľ riadenia: Predísť neautorizovanému prístupu používateľov a kompromitovaniu alebo krádeži informácií a informačných procesov.

- A.11.3.1 - Používanie hesiel
- A.11.3.2 - Nestrážené prostriedky
- A.11.3.3 - Politika čistého stola a čistej obrazovky

A.11 - Riadenie prístupu

A.11.4 - Riadenie prístupu k sieti

Cieľ riadenia: Predchádzať neautorizovanému prístupu k sieťovým službám.

- A.11.4.1 - Politika používania sieťových služieb
- A.11.4.2 - Autentizácia používateľov pre externé pripojenia
- A.11.4.3 - Identifikácia zariadenia v sieťovom prostredí
- A.11.4.4 - Ochrana diaľkových diagnostických a konfiguračných portov
- A.11.4.5 - Oddeľovanie sietí
- A.11.4.6 - Riadenie sieťovej konektivity
- A.11.4.7 - Riadenie smerovania v sieťach

A.11 - Riadenie prístupu

A.11.5 - Riadenie prístupu do operačného systému

Cieľ riadenia: Zabrániť neautorizovanému prístupu do operačných systémov.

- A.11.5.1 - Bezpečné prihlasovacie postupy
- A.11.5.2 - Identifikácia a autentizácia používateľov
- A.11.5.3 - Systém riadenia hesiel
- A.11.5.4 - Používanie systémových pomocných programov
- A.11.5.5 - Uplynutie času pripojenia terminálu
- A.11.5.6 - Obmedzenie času pripojenia

A.11 - Riadenie prístupu

A.11.6 - Riadenie prístupu k aplikáciám a informáciám

Cieľ riadenia: Predísť neautorizovanému prístupu k informáciám obsiahnutým v informačných systémoch.

- A.11.6.1 - Obmedzenie prístupu k informáciám
- A.11.6.2 - Izolácia citlivého systému

A.11.7 - Mobilné počítačové spracúvanie a práca na diaľku

Cieľ riadenia: Zaistiť informačnú bezpečnosť, keď sa používa mobilné počítačové spracovanie a práca na diaľku.

- A.11.7.1 - Mobilné spracúvanie
- A.11.7.2 - Práca na diaľku

A.12 - Akvizícia, vývoj a údržba informačných systémov

A.12.1 - Bezpečnostné požiadavky na informačné systémy

Cieľ riadenia: Zaistiť, aby bezpečnosť bola integrálnou súčasťou informačných systémov.

- A.12.1.1 - Analýza a špecifikácia bezpečnostných požiadaviek

A.12.2 - Bezchybné spracúvanie v aplikáciách

Cieľ riadenia: Zabrániť chybám, strate, neautorizovanej modifikácii alebo zneužitiu informácií v aplikáciách.

- A.12.2.1 - Validácia vstupných dát
- A.12.2.2 - Riadenie interného spracovania
- A.12.2.3 - Integrita správ
- A.12.2.4 - Validácia výstupných dát

A.12 - Akvizícia, vývoj a údržba informačných systémov

A.12.3 - Kryptografické opatrenia

Cieľ riadenia: Chrániť dôvernosť, autentickosť alebo integritu informácií kryptografickými prostriedkami.

- A.12.3.1 - Politika používania kryptografických opatrení
- A.12.3.2 - Riadenie kľúčov

A.12.4 - Bezpečnosť systémových súborov

Cieľ riadenia: Zaistiť bezpečnosť systémových súborov.

- A.12.4.1 - Riadenie prevádzkovaného softvéru
- A.12.4.2 - Ochrana testovacích dát
- A.12.4.3 - Riadenie prístupu k zdrojovej knižnici programov

A.12 - Akvizícia, vývoj a údržba informačných systémov

A.12.5 - Bezpečnosť v procesoch vývoja a podpory

Cieľ riadenia: Udržovať bezpečnosť softvéru aplikačných systémov a informácií.

- A.12.5.1 - Postupy riadenia zmien
- A.12.5.2 - Technické preskúmanie aplikácií po zmene operačného systému
- A.12.5.3 - Obmedzenia zmien softvérových balíkov
- A.12.5.4 - Únik informácií
- A.12.5.5 - Vývoj softvéru prostredníctvom externých zdrojov

A.12 - Akvizícia, vývoj a údržba informačných systémov

A.12.6 - Riadenie technických zraniteľností

Cieľ riadenia: Znižovať riziká vyplývajúce zo zneužitia zverejnených technických zraniteľností.

- A.12.6.1 - Riadenie technických zraniteľností

A.13 - Riadenie incidentov informačnej bezpečnosti

A.13.1 - Oznamovanie incidentov informačnej bezpečnosti a slabiny

Cieľ riadenia: Zabezpečiť, aby boli udalosti a slabiny informačnej bezpečnosti spojené s informačnými systémami oznamované primeraným spôsobom, ktorý umožní včas podniknúť potrebné nápravné kroky.

- A.13.1.1 - Oznamovanie udalostí informačnej bezpečnosti
- A.13.1.2 - Oznamovanie bezpečnostných slabín

A.13 - Riadenie incidentov informačnej bezpečnosti

A.13.2 - Riadenie incidentov informačnej bezpečnosti a zlepšení

Cieľ riadenia: Zaručiť, že sa k manažmentu incidentov informačnej bezpečnosti pristupuje konzistentným a efektívnym spôsobom.

- A.13.2.1 - Zodpovednosti a postupy
- A.13.2.2 - Poučenie sa z incidentov informačnej bezpečnosti
- A.13.2.3 - Zber dôkazov

A.14 - Riadenie kontinuity činnosti

A.14.1 - Aspekty riadenia kontinuity činnosti

Cieľ riadenia: Zabrániť prerušeniam podnikových aktivít a chrániť kritické podnikové procesy pred vplyvmi závažných zlyhaní alebo havárií informačných systémov a zabezpečiť ich včasnú obnovu.

- A.14.1.1 - Zahrnutie informačnej bezpečnosti do procesu riadenia kontinuity činnosti
- A.14.1.2 - Kontinuita činnosti a preskúmanie rizík
- A.14.1.3 - Príprava a implementovanie plánov kontinuity činnosti vrátane informačnej bezpečnosti
- A.14.1.4 - Štruktúra plánovania kontinuity činnosti
- A.14.1.5 - Testovanie, údržba a prehodnocovanie plánov kontinuity činnosti

A.15 - Súlad

A.15.1 - Súlad so zákonnými požiadavkami

Cieľ riadenia: Vyhnúť sa porušeniam akýchkoľvek právnych, štatutárnych, regulačných alebo zmluvných záväzkov a akýchkoľvek bezpečnostných požiadaviek.

- A.15.1.1 - Identifikácia platnej legislatívy
- A.15.1.2 - Práva duševného vlastníctva
- A.15.1.3 - Zabezpečenie záznamov organizácie
- A.15.1.4 - Ochrana dát a ochrana osobných údajov
- A.15.1.5 - Predchádzanie zneužívaniu prostriedkov spracúvajúcich informácie
- A.15.1.6 - Regulácia kryptografických opatrení

A.15 - Súlad

A.15.2 - Súlad s bezpečnostnými politikami, normami a technický súlad

Cieľ riadenia: Zaistiť súlad systémov s bezpečnostnými politikami a normami organizácie.

- A.15.2.1 - Súlad s bezpečnostnými politikami a normami
- A.15.2.2 - Kontrolovanie technického súladu

A.15.3 - Hľadiská auditu informačného systému

Cieľ riadenia: Maximalizovať efektívnosť procesov auditu systému a minimalizovať ich negatívne vplyvy, podobne ako aj negatívne vplyvy na ne pôsobiace.

- A.15.3.1 - Opatrenia auditu informačného systému
- A.15.3.2 - Ochrana nástrojov auditu informačných systémov

Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Otázky a diskusia

Ďakujem za pozornosť

KPMG
cutting through complexity™