Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Manažment informačnej bezpečnosti

Doc. Ing. Ladislav Hudec, CSc., CISA

Pripravené pre vzdelávanie GR dňa 29.5.2014

KPMG
cutting through complexity™

Úvod

- Informačná bezpečnosť je **dosiahnutá zavedením vhodnej sady opatrení**, vrátane politiky, procesov, procedúr, organizačných štruktúr a softvérových a hardvérových funkcií. Je potrebné tieto opatrenia stanoviť, realizovať, monitorovať, preskúmať a zlepšiť, kde je to potrebné, aby sa zabezpečilo, že **sú splnené špecifické bezpečnostné ciele a poslanie organizácie**.
- STN ISO/IEC 27002:2013 Informačné technológie. Bezpečnostné techniky. Kódex uplatňovania opatrení v informačnej bezpečnosti.
- Dnes sa budeme zaoberať týmito oblasťami informačnej bezpečnosti:
  - Bezpečnostná politika IS
  - Organizácia informačnej bezpečnosti
  - Manažment aktív
  - Bezpečnosť ľudských zdrojov
  - Fyzická a objektová bezpečnosť
  - Komunikačný a prevádzkový manažment

Bezpečnostná politika – politika informačnej bezpečnosti

- Cieľom tejto časti je zistiť, či manažment organizácie **orientuje a podporuje** informačnú bezpečnosť v súlade s požiadavkami na činnosť organizácie, relevantnými zákonmi a reguláciami.
- Manažment organizácie by mal **zaviesť jasnú orientáciu politiky** v súlade s cieľmi činnosti organizácie a **demonštrovať podporu** pre, a záväzok voči, informačnej bezpečnosti **prostredníctvom vydania a údržby** politiky informačnej bezpečnosti a to naprieč celou organizáciou.
- **Dokument politiky informačnej bezpečnosti** - Opatrenie
  - Dokument politiky informačnej bezpečnosti by mal byť schválený manažmentom organizácie, prístupný a oznámený všetkým zamestnancom organizácie a dôležitým spolupracujúcim organizáciam.
- **Dokument politiky informačnej bezpečnosti** - Návod na implementáciu
  - Dokument politiky informačnej bezpečnosti by mal obsahovať **vyhlásenie záväzku manažmentu organizácie na zavedenie prístupu k manažmentu informačnej bezpečnosti** naprieč celou organizáciou. Dokument politiky informačnej bezpečnosti by mal obsahovať stanoviská týkajúce sa:
    - Definícii informačnej bezpečnosti, jej **celkový účel a rozsah**, jej dôležitosť ako mechanizmu umožňujúceho spoločné používanie informácií
    - **Prehlásenie úmyslu manažmentu** podporovať ciele a princípy informačnej bezpečnosti v súlade s obchodnou stratégiou a cieľmi
    - Stanovenie rámca **cieľov riadenia informačnej bezpečnosti** a opatrení, vrátane **štruktúry ohodnotenia rizík a manažmentu rizík**

Bezpečnostná politika – politika informačnej bezpečnosti

- **Stručný výklad** bezpečnostných pravidiel, princípov, štandardov a požiadaviek súladu, ktoré sú pre organizáciu zvlášť dôležité (vrátane súladu s legislatívou, nariadeniami regulátorov a zmluvnými požiadavkami, bezpečnostného vzdelávania, školenia a bezpečnostného povedomia, manažmentu kontinuity obchodných činností, dôsledkov pri porušení bezpečnostnej politiky)
- Definovanie všeobecných a špecifických **povinností za manažment informačnej bezpečnosti**, vrátane oznamovania bezpečnostných incidentov
- **Referencie na dokumenty podporujúce politiku**, napríklad detailné bezpečnostné politiky a procedúry pre špecifické informačné systémy alebo bezpečnostné pravidlá, ktoré by mali používatelia dodržiavať

- Táto politika informačnej bezpečnosti by mala byť oznámená **v celej organizácii používateľom** takou formou, že je relevantná, dostupná a zrozumiteľná zamýšľanému čitateľovi.

Bezpečnostná politika – politika informačnej bezpečnosti

- **Posudzovanie politiky informačnej bezpečnosti** – opatrenie
  - Politika informačnej bezpečnosti by mala byť **preskúmaná v plánovaných intervaloch alebo v prípade výskytu významných zmien** tak, aby sa zabezpečilo jej sústavnej vhodnosti, primeranosti a efektívnosti.
- **Posudzovanie politiky informačnej bezpečnosti** – Návod na implementáciu
  - Politika informačnej bezpečnosti **by mala mať vlastníka schváleného manažmentom** a ktorého povinnosťou je vytvorenie, preskúmanie a hodnotenie bezpečnostnej politiky. Preskúmanie by malo zahrňovať posudzovanie možností na **vylepšenie politiky** informačnej bezpečnosti organizácie a prístup na spravovanie informačnej bezpečnosti v reakcii na zmeny v prostredí organizácie, obchodných podmienok, právnych podmienok alebo technického prostredia.
  - Preskúmanie politiky informačnej bezpečnosti by malo brať do úvahy výsledky **manažérskeho preskúmania**. Mali by byť definované procedúry manažérskeho preskúmania, vrátane plánu alebo periódy preskúmania.
  - Vstupy do manažérskeho preskúmania by mali zahrňovať informácie o:
    - Spätnej väzbe od zúčastnených strán
    - **Výsledkoch nezávislých previerok**
    - Stave preventívnych a opravných akcií
    - **Výsledkoch predchádzajúcich manažérskych previerok**
    - Súladu výkonnosti procesu a politiky informačnej bezpečnosti
    - Zmenách, ktoré môžu ovplyvniť prístup manažmentu informačnej bezpečnosti naprieč celou organizáciou, zmeny prostredia organizácie, podnikateľské okolnosti, dostupnosť zdrojov, zmluvné, regulačné a právne podmienky, technické prostredie
    - Trendoch súvisiacich s hrozbami a zraniteľnosťami
    - **Oznámených bezpečnostných incidentoch**
    - **Odporúčaniach poskytnutých relevantnými autoritami**

Bezpečnostná politika – politika informačnej bezpečnosti

- Výstupy manažérskeho preskúmania by mali zahrňovať všetky rozhodnutia a akcie majúce súvis s:
  - **Zlepšením** prístupu spravovania informačnej bezpečnosti naprieč celou organizáciou a jeho procesu
  - **Zlepšením** cieľov riadenia a opatrenia
  - **Zlepšením** v alokácii zdrojov a/alebo zodpovedností
- Záznam z manažérskeho preskúmania **by mal byť založený**.
- **Revidovaný dokument politiky informačnej bezpečnosti by mal byť schválený manažmentom organizácie**.

Organizácia informačnej bezpečnosti – interná organizácia

- Cieľom tejto časti je zistiť ako sa manažuje informačná bezpečnosť **vo vnútri organizácie**.
- Vo vnútri organizácie by mal byť **zriadený manažérsky rámec na inicializáciu a riadenie implementácie informačnej bezpečnosti.**
- **Manažment by mal schváliť politiku informačnej bezpečnosti, prideliť bezpečnostné roly a koordinovať a posudzovať implementáciu bezpečnosti naprieč celou organizáciou**.
- Pokiaľ je to nevyhnutné, vo vnútri organizácie by mal byť zriadený a dostupný zdroj na poradenstvo špecialistov na informačnú bezpečnosť. Mal by byť **vytvorený a udržiavaný kontakt s externými bezpečnostnými špecialistami alebo skupinami**, vrátane relevantných inštitúcií, na monitorovanie štandardov a vyhodnocovacích metód a zabezpečenie vhodných kontaktných bodov pre prípad narábania s bezpečnostnými incidentmi.
- K informačnej bezpečnosti by mal byť podporovaný **multidisciplinárny prístup**.

Organizácia informačnej bezpečnosti – interná organizácia

- **Záväzok manažmentu pre informačnú bezpečnosť** – Opatrenie
  - **Manažment by mal aktívne podporovať bezpečnosť v organizácii** prostredníctvom jasného smerovania, preukázaného záväzku, explicitného pridelenia a potvrdenia povinností v informačnej bezpečnosti.
- **Záväzok manažmentu pre informačnú bezpečnosť** - Návod na implementáciu
  - Manažment organizácie by mal:
    - Zabezpečiť, že **ciele informačnej bezpečnosti sú identifikované**, **odpovedajú požiadavkám** organizácie a **sú integrované** do relevantných procesov organizácie
    - **Formulovať, posudzovať a schvaľovať politiku informačnej bezpečnosti**
    - **Posudzovať efektívnosť implementácie** politiky informačnej bezpečnosti
    - Poskytovať jasnú orientáciu a **viditeľnú manažérsku podporu pre bezpečnostné iniciatívy**
    - **Poskytovať potrebné zdroje** pre informačnú bezpečnosť
    - **Schvaľovať pridelenie špecifických rolí** a povinností v informačnej bezpečnosti naprieč celou organizáciou
    - **Iniciovať plány a programy na udržiavanie povedomia** v informačnej bezpečnosti
    - Zabezpečovať, že implementácia opatrení informačnej bezpečnosti je koordinovaná naprieč celou organizáciou
  - Manažment by mal identifikovať potreby na interné alebo externé poradenstvo špecialistov na informačnú bezpečnosť a posudzovať a koordinovať výsledky poradenstvo v rámci celej organizácie.
  - V závislosti na veľkosti organizácie by tieto povinnosti mali byť vykonávané vyhradeným manažérskym fórom alebo existujúce riadiacim orgánom, ako je vedenie organizácie.

Organizácia informačnej bezpečnosti – interná organizácia

- **Koordinácia informačnej bezpečnosti** – Opatrenie
  - Aktivity v oblasti informačnej bezpečnosti by mali **byť koordinované zástupcami z rôznych častí organizácie s príslušnými rolami a pracovných funkciami**.
- **Koordinácia informačnej bezpečnosti** - Návod na implementáciu
  - Koordinácia aktivít v oblasti informačnej bezpečnosti zahrňuje spoluprácu **manažérov, používateľov, administrátorov, vývojárov aplikácií, audítorov a bezpečnostného personálu a špecialistov v oblasti poistenia, právnych otázok, ľudských zdrojov, IT a manažmentu rizík**. Tieto aktivity by mali:
    - Zabezpečiť, že aktivity v informačnej bezpečnosti **sú vykonávané v zhode s politikou informačnej bezpečnosti**
    - Stanoviť **ako postupovať v prípade nezhody**
    - **Schvaľovať metodológie a procesy v informačnej bezpečnosti, napríklad ohodnotenie rizík, klasifikácia informácií**
    - **Identifikovať významné zmeny v hrozbách** a vystavenie informácií a zariadení na spracovanie informácií týmto hrozbám
    - **Vyhodnocovať adekvátnosť a koordináciu implementácií opatrení** informačnej bezpečnosti
    - Efektívne **podporovať vzdelávanie** v informačnej bezpečnosti, školenie a povedomie a to naprieč celou organizáciou
    - **Vyhodnocovať informácie získané z monitorovania a posudzovania incidentov** v informačnej bezpečnosti a odporúčať vhodné akcie ako odpoveď na identifikované bezpečnostné incidenty
  - Ak organizácia nepoužíva **samostatnú prierezovú funkčnú skupinu** napríklad preto, že taká skupina nie je vhodná z pohľadu veľkosti organizácie, by vyššie opísané aktivity mal vykonávať **ďalší vhodný riadiaci orgán** organizácie alebo individuálny manažér..

Organizácia informačnej bezpečnosti – interná organizácia

- **Pridelenie zodpovednosti za informačnú bezpečnosť** – Opatrenie
  - **Všetky povinnosti v oblasti informačnej bezpčnosti by mali byť jasne definované**.
- **Pridelenie zodpovednosti za informačnú bezpečnosť** - Návod na implementáciu
  - **Pridelenie povinností** za informačnú bezpečnosť by malo byť **stanovené v súlade s politikou informačnej bezpečnosti**. Povinnosti ochrany jednotlivých aktív a vykonávanie špecifických bezpečnostných procesov by mali byť jasne identifikované.
  - **Jednotlivci s pridelenými povinnosťami** za informačnú bezpečnosť **môžu delegovať** bezpečnostné úlohy na iných. Aj napriek tomu **zostávajú zodpovední** a mali by stanoviť, že všetky delegované úlohy boli správne vykonané.
  - Oblasti, v ktorých je **jednotlivec zodpovedný za ochranu zvereného aktíva, by mali byť jasne definované**. Konkrétne by malo byť zavedené, že
    - **Aktíva a bezpečnostné procesy súvisiace s každým jednotlivým systémom by mali byť identifikované a jasne definované**
    - Mala by byť **určená entita zodpovedná za každé aktívum alebo bezpečnostný proces** a detaily tejto zodpovednosti by mali byť dokumentované
    - **Úroveň autorizácie by mala byť jasne definovaná a dokumentovaná**

Organizácia informačnej bezpečnosti – interná organizácia

- **Autorizačný proces pre prostriedky spracovania informácií** – Opatrenie
  - Pre **nové zariadenia** na spracovanie informácií by mal byť **zriadený a implementovaný manažérsky autorizačný proces**.
- **Autorizačný proces pre prostriedky spracovania informácií** - Návod na implementáciu
  - Pre autorizačný proces by mali byť vzaté do úvahy tieto odporúčania:
    - **Nové zariadenia by mali mať vhodnú manažérsku autorizáciu od používateľov**, ktorá by autorizovala účel a použitie. Autorizácia by mala byť získaná tiež **od manažéra zodpovedného za prevádzku bezpečnostného prostredia informačného systému**, aby sa zaistilo, ža budú splnené všetky relevantné bezpečnostné politiky a požiadavky.
    - Kde je to potrebné, mal by byť skontrolovaný hardvér a softvér, aby sa zabezpečilo, že je kompatibilný s ostatnými komponentmi systému
    - **Používanie osobných alebo privátne vlastnených zariadení** na spracovanie informácií, napríklad laptopy, počítače z domu, mobilné zariadenia, na spracovanie obchodných informácií **môže zaviesť nové zraniteľnosti** a je potrebné identifikovať a implementovať nevyhnutné opatrenia

Organizácia informačnej bezpečnosti – interná organizácia

- **Zmluva o dôvernosti** – Opatrenie
  - **Požiadavky na dôvernosť alebo dohody o nezverejňovaní** odrážajúce potreby organizácie na ochranu informácií by mali byť **identifikované a pravidelne preskúmavané**.
- **Zmluva o dôvernosti** - Návod na implementáciu
  - Zmluva o dôvernosti alebo nezverejňovaní musí vyjadriť požiadavky na ochranu dôverných informácií vo **forme právne vymožiteľných požiadaviek**. Na identifikovanie požiadaviek pre dôvernosť alebo dohody o nezverejňovaní by mali byť vzaté do úvahy tieto elementy:
    - **Definícia chránenej informácie (dôverná informácia)**
    - Očakávaná **doba trvania zmluvy** vrátane prípadov, keď dôvernosť informácie je potrebné zachovať bez časového obmedzenia
    - Požadované **aktivity pri ukončení dohody**
    - **Povinnosti a akcie zmluvných strán** na zamedzenie neautorizovanému zverejneniu informácie (ako napríklad „potreba vedieť“)
    - Vlastníctvo informácie, obchodné tajomstvo a duševné vlastníctvo, a aký majú vzťah k ochrane dôvernej informácii
    - **Dovolené používanie dôvernej informácii**, práva zmluvného partnera na použitie informácie
    - **Právo na auditovanie a monitorovanie aktivít** zahrňujúcich dôvernú informáciu
    - **Proces notifikácie a oznamovania v prípade neautorizovaného zverejnenia** alebo porušenia dôvernosti informácie
    - **Podmienky na navrátenie informácie alebo jej zničenia** v prípade ukončenia zmluvy
    - **Očakávané akcie, ktoré nastanú v prípade porušenia tejto zmluvy**

Organizácia informačnej bezpečnosti – interná organizácia

- **Zmluva o dôvernosti** - Návod na implementáciu
  - V závislosti na bezpečnostných podmienkach organizácie môžu byť v dohodách o dôvernosti a nezverejňovaní potrebné aj ďalšie elementy.
  - **Požiadavky na dôvernosť a dohody o nezverejňovaní** by mali byť **pravidelne posudzované** a keď sa vyskytnú zmeny, mala by byť **dohoda doplnená**.

Organizácia informačnej bezpečnosti – interná organizácia

- **Kontakt s oficiálnymi inštitúciami** – Opatrenie
  - Organizácia by mala mať zriadené vhodné kontakty s **relevantnými oficiálnymi inštitúciami**.
- **Kontakt s oficiálnymi inštitúciami** - Návod na implementáciu
  - Organizácia by mala mať **zriadené procedúry špecifikujúce kedy a ktorú oficiálnu inštitúciu** (polícia, hasičský zbor, inštitúcie vykonávajúce dohľad atď.) **kontakovať** a **ako** by mali byť **identifikované incidenty informačnej bezpečnosti oznámené** a oznámené včas v prípade, že je podozrenie na porušenie zákona.
  - Organizácia vystavená útoku z internetu môže potrebovať externú tretiu stranu (poskytovateľ internetových služieb alebo telekomunikačný operátora), ktorá vykoná akcie proti zdroju útoku.

Organizácia informačnej bezpečnosti – interná organizácia

- **Kontakt so špeciálnymi záujmovými skupinami** – Opatrenie
  - Organizácia by mala udržiavať vhodné kontakty so **špeciálnymi záujmovými skupinami alebo inými fórami bezpečnostných špecialistov a profesijnými organizáciami**.
- **Kontakt so špeciálnymi záujmovými skupinami** - Návod na implementáciu
  - **Členstvo v špeciálnych záujmových skupinách alebo fórach** by mal byť vzatý do úvahy **ako prostriedok na**:
    - **Zlepšenie znalostí** o najlepších praktikách a ako zdroj aktuálnych informácií o bezpečnosti
    - **Zaistenie, že vedomosti** o prostredí informačnej bezpečnosti **sú aktuálne a úplné**
    - **Získanie včasného varovania o ostražitosti, doporučeniach a záplatách** týkajúcich sa útokov a zraniteľností
    - **Získanie prístupu k doporučeniam** špecialistov na informačnú bezpečnosť
    - **Zdieľanie a výmeny informácií** o nových technológiách, produktoch, hrozbách alebo zraniteľnostiach
    - **Zabezpečenie vhodných styčných bodov pri narábaní s incidentmi** informačnej bezpečnosti
  - V prípade **členstva organizácie alebo jej zamestnancov** v špeciálnych záujmových skupinách by mala byť **zaistená ochrana citlivých informácií organizácie**.

Organizácia informačnej bezpečnosti – interná organizácia

- **Nezávislé posúdenie informačnej bezpečnosti** – Opatrenie
  - **Prístup organizácie** k spravovaniu informačnej bezpečnosti a jej implementácii (napríklad ciele opatrení, opatrenia, politiky, procesy a procedúry informačnej bezpečnosti) by mali byť **nezávisle preskúmavané v plánovaných intervaloch alebo v prípade výskytu podstatnej zmeny v implementácii bezpečnosti**.
- **Nezávislé posúdenie informačnej bezpečnosti** - Návod na implementáciu
  - Nezávislé preskúmanie stavu informačnej bezpečnosti by malo byť **iniciované manažmentom**.
  - Nezávislé preskúmanie stavu informačnej bezpečnosti zabezpečí **zaistenie pokračujúcej vhodnosti, účinnosti prístupu organizácie na manažment informačnej bezpečnosti**. Preskúmanie by malo tiež zahrnúť **vyhodnotenie možností na vylepšenie** a potrebu zmien prístupu k bezpečnosti vrátane politiky a cieľov opatrení.
  - Preskúmanie v organizácii by malo byť vykonané **jednotlivcami nezávislými na posudzovanej oblasti**, t.j. zamestnanec útvaru interného auditu, **nezávislý manažér organizácie** alebo **spoločnosť tretej strany špecializujúca sa na takúto činnosť**. Osoby vykonávajúcu nezávislé posúdenia stavu informačnej bezpečnosti by mali mať primerané zručnosti a skúsenosti.
  - **Výsledky nezávislého posúdenia stavu** informačnej bezpečnosti by mali byť **zaznamenané a oznámené manažmentu**, ktorý nezávislé posúdenie inicioval. Záznamy by mali byť archivované.
  - **Ak nezávislé posúdenia stavu informačnej bezpečnosti indikuje**, že prístup organizácie a implementácia manažmentu informačnej bezpečnosti **nie sú adekvátne** alebo nie sú v súlade s orientáciou informačnej bezpečnosti stanovenej v dokumente politiky informačnej bezpečnosti, **iniciuje následne manažment korektívne akcie na odstránenie zistených nedostatkov**.

Organizácia informačnej bezpečnosti – externé strany

- Cieľom tejto časti je zistiť **ako je zaistená bezpečnosť informácií organizácie a zariadení** na spracovanie informácií organizácie, v prípade, že **tieto informácie a zariadenia sú pristupované, spracovávané, komunikované alebo manažované externými stranami**.
- Bezpečnosť informácií organizácie a zariadení na spracovanie informácií organizácii **by nemala byť znížená začlenením produktov alebo služieb externých strán**.
- **Každý prístup externej strany** k zariadeniu spracovávajúceho informácie organizácie a k spracovaniu a ku komunikácii informácií **by mal byť riadený**.
- Pokiaľ existujú obchodné potreby pre spoluprácu s externými stranami a tieto potreby vyžadujú prístup k informáciam organizácie a k prostriedkom spracovania informácií organizácie alebo potreba získania alebo zabezpečenia produktu alebo služby z/do externej strany, malo by sa **vykonať ohodnotenie rizík na stanovenie bezpečnostných dopadov a požiadavky na opatrenia**. **Opatrenia** by mali byť odsúhlasené a stanovené **v dohode s externou stranou**.
- Opatrenia:
  - **Identifikácia rizika vo vzťahu k externým stranám – Riziká pre prostriedky spracovania informácií organizácie** z obchodných procesov **zahrňujúcich externé strany by mali byť identifikované a príslušné opatrenia implementované pred poskytnutím prístupu**.
  - **Zaistenie bezpečnosti pri kontakte so zákazníkmi – Všetky bezpečnostné požiadavky by mali byť identifikované predtým** ako organizácia dá prístup zákazníkovi k informáciám a aktívam organizácie.

Organizácia informačnej bezpečnosti – externé strany

- **Zaistenie bezpečnosti v zmluvách s tretími stranami** – **Zmluvy s tretími stranami** zahrňujúce pristupovanie, spracovanie, komunikovanie alebo spravovanie informácií organizácie alebo prostriedky spracovania informácie, alebo pridanie produktu alebo služby do prostriedkov spracovania informácie, **by mali pokrývať všetky relevantné bezpečnostné požiadavky**.

Manažment aktív – zodpovednosť za aktíva

- Cieľom tejto časti je zistiť ako sa dosahuje a udržuje primeraná ochrana aktív organizácie.
- **Všetky aktíva organizácie by mali byť evidované a mali by mať stanoveného vlastníka**.
- **Vlastník** by mal byť identifikovaný pre každé aktívum a **mala by byť stanovená jeho zodpovednosť za prevádzku vhodných opatrení**. Pokiaľ je to potrebné, **vlastník môže delegovať implementáciu špecifických opatrení**, **ale vlastník zostáva zodpovedný** za primeranú ochranu aktív.
- Opatrenia:
  - **Inventárny zoznam aktív** - Všetky aktíva organizácie by mali byť jasne identifikované a mal by byť **vytvorený inventárny zoznam** všetkých dôležitých aktív a **tento zoznam pravidelne udržiavaný.**
  - **Vlastníctvo aktív** - **Všetky informácie a aktíva** súvisiace s prostriedkami spracovania informácií by mali byť **vlastnené stanoveným útvarom organizácie**.
  - **Akceptovateľné použitie aktív** - V organizácii by mali byť identifikované, dokumentované a implementované **pravidlá akceptovateľného použitia** informácií a aktív zviazaných s prostriedkami spracovania informácií.

Manažment aktív – klasifikácia informácií

- Cieľom tejto časti je zistiť ako je zabezpečené, že **informáciam sa dostáva primeraná úroveň ochrany**.
- Informácie by mali byť **klasifikované vo vzťahu k ich potrebnosti, priorite a očakávanému stupňu ochrany**, keď sa s nimi narába.
- Informácie majú **rôzny stupeň citlivosti a kritickosti**. Niektoré položky môžu vyžadovať dodatočnú úroveň ochrany alebo špeciálne zaobchádzanie. **Klasifikačná schéma** informácií by mala byť **použitá na stanovenie vhodnej množiny úrovní ochrany** a vyjadrenie potreby pre špeciálne opatrenia na narábanie s informáciou.
- Opatrenia:
  - **Smernice na klasifikáciu** - Informácie by mali byť **klasifikované v súvislosti s ich hodnotou**, **zákonnými požiadavkami, citlivosťou a kritickosťou pre organizáciu**.
  - **Označovanie informácií a narábanie s nimi** - V organizácii by mali byť vytvorené a implementované **vhodné procedúry na označovanie informácií a narábanie s nimi**, ktoré sú v súlade klasifikačnou schémou schválenou v organizácii.

Bezpečnosť ľudských zdrojov – pred zamestnaním

- Cieľom tejto časti je zistiť, či je zabezpečené, **že zamestnanci, zmluvní partneri a používatelia tretích strán chápu svoje povinnosti** a sú vhodní pre role, do ktorých sa s nimi uvažuje, a **na redukciu rizika krádeže, defraudácie a nesprávneho používania prostriedkov**.
- **Bezpečnostné povinnosti** by mali byť **oznámené kandidátovi pred nástupom do zamestnania** vo vhodnom opise pracovnej pozície a v pracovnej zmluve pri nástupe do zamestnania.
- Všetci kandidáti pre zamestnanie, zmluvní partneri a používatelia tretích strán by mali byť **vhodne preverení**, zvlášť pre citlivé pracovné pozície.
- Zamestnanci, zmluvní partneri a používatelia tretích strán prostriedkov spracovania informácií by mali **podpísať zmluvu o svojich bezpečnostných rolách a povinnostiach**.
- Opatrenia:
  - **Role a povinnosti** - **V organizácii by mali byť definované a dokumentované**, v súlade s politikou informačnej bezpečnosti organizácie**, bezpečnostné roly a povinnosti zamestnancov, zmluvných partnerov a používateľov tretej strany**.
  - **Previerka** - Mala by byť vykonaná **verifikačná kontrola profilu všetkých kandidátov na zamestnanie, zmluvných partnerov a používateľov tretích strán** v súlade s relevantnými zákonmi, reguláciami a etikou a proporcionálna obchodným podmienkam, klasifikácii pristupovaných informácií a vnímaného rizika.

Bezpečnosť ľudských zdrojov – pred zamestnaním

- **Pracovná zmluva** - **Súčasťou zmluvných záväzkov** zamestnancov, zmluvných partnerov a používateľov tretej strany **by mal byť súhlas a podpis všeobecných obchodných (pracovných) podmienok** ich zamestnaneckej zmluvy, ktorá by mala **stanoviť ich povinnosti a povinnosti organizácie v oblasti informačnej bezpečnosti**.

Bezpečnosť ľudských zdrojov – počas zamestnania

- Cieľom tejto časti je zistiť, či je zabezpečené, že **zamestnanci**, zmluvní partneri a používatelia tretích strán **sú si vedomí hrozieb a obáv informačnej bezpečnosti**, **svojich povinností a zodpovedností**, a či sú vybavení podporovať politiku informačnej bezpečnosti **v súvislosti ich normálnou pracovnou činnosťou** a redukovať riziko ľudských chýb.
- Mal by byť definovaný manažment povinností, aby sa zaistilo, že bezpečnosť je realizovaná prostredníctvom individuálneho zamestnaneckého pomeru v rámci organizácie.
- Na minimalizáciu možných bezpečnostných rizík by mali byť poskytnuté všetkým zamestnancom, zmluvným partnerom a používateľom tretích strán **primeraná úroveň povedomia, vzdelania a školenie** v bezpečnostných procedúrach a v správnom používaní prostriedkov spracovania informácií. Mal by byť zavedený formálny **disciplinárny proces** na zaoberanie sa s bezpečnostnými priestupkami.
- Opatrenia:
  - **Povinnosti manažmentu** - Manažment organizácie by **mal vyžadovať od zamestnancov**, zmluvných partnerov a používateľov tretích strán **aplikovať bezpečnosť** v súlade so zavedenými politikami a procedúrami organizácie.
  - **Povedomie v informačnej bezpečnosti, vzdelávanie a školenie** - Všetci zamestnanci organizácie, a kde je to relevantné, zmluvní partneri a používatelia tretej strany by mali **dostať primerané školenie povedomia a pravidelné aktualizácie** v politikách a procedúrach organizácie ako dôležitú funkciu ich pracovnej pozície.
  - **Disciplinárny proces** - V organizácii by mal byť zavedený formálny **disciplinárny proces** so zamestnancami, **ktorí spáchali bezpečnostný priestupok**.

Bezpečnosť ľudských zdrojov – ukončenie alebo zmena zamestnania

- Cieľom tejto časti je zistiť, či je zabezpečené, že zamestnanci, zmluvní partneri a používatelia tretích strán **ukončujú zamestnanie v organizácii alebo menia** zamestnanie v organizácii **riadnym spôsobom**.
- Mali by byť zavedené povinnosti, ktoré zabezpečujú, že **ukončenie práce v organizácii** pre zamestnancov, zmluvných partnerov a používateľov zmluvných strán **je manažovaný a že sú navrátené všetky zariadenia a odstránené všetky prístupové práva**.
- **Zmena povinností a zamestnaneckého pomeru** v organizácii by mala byť **manažovaná ako ukončenie odpovedajúcej povinnosti** alebo zamestnania v súlade s touto časťou a každý nový zamestnanecký pomer (zmena pomeru) by mal byť manažovaná ako nový zamestnanecký pomer.
- Opatrenia:
  - **Ukončenie povinností** - **Povinnosti na vykonanie ukončenia** zamestnaneckého pomeru alebo **zmenu** pracovnej pozície by mali byť **jasne definované a pridelené**.
  - **Navrátenie aktív** - Všetci zamestnanci, zmluvní partneri a používatelia tretej strany by mali **vrátiť všetky aktíva organizácie**, ktoré mali v držaní, pri ukončení zamestnaneckého pomeru, zmluvy alebo dohody.
  - **Odstránenie prístupových práv** - **Prístupové práva** všetkých zamestnancov, zmluvných partnerov a používateľov tretích strán k informáciám a prostriedkom spracovania informácií **by mali byť odstránené pri ukončení** zamestnaneckého pomeru, zmluvy alebo dohody alebo nastavené podľa zmeny.

Fyzická bezpečnosť a bezpečnosť prostredia – bezpečné priestory

- Cieľom tejto časti je zistiť **ako sa bráni neautorizovanému fyzickému prístupu, poškodeniu a narušovaniu priestorov organizácie a informácií**.
- **Prostriedky spracovania** kritických alebo citlivých informácií by mali byť **umiestnené v bezpečných priestoroch**, chránených definovanými bezpečnostnými perimetrami, s primeranými bezpečnostnými bariérami a opatreniami vstupu. Mali by byť **fyzicky oddelené od neautorizovaného vstupu**, poškodeniu a narušeniu.
- **Poskytnutá ochrana by mala byť zrovnateľná s identifikovanými rizikami**.
- Opatrenia:
  - **Perimeter fyzickej bezpečnosti** - **Bezpečnostné perimetre** (bariéry ako steny, zábrany, cez ktoré je riadený prechod kartami alebo obsluhované recepčné pulty) by sa **mali používať na ochranu priestorov** s informáciami a prostriedkov spracúvajúcimi informácie organizácie.
  - **Opatrenia pre fyzický vstup** - Zabezpečené priestory by mali byť **chránené pomocou vhodných opatrení** pre vstup, ktoré zaistia, **že iba autorizovaným osobám je vstup povolený**.
  - **Zabezpečenie kancelárií, miestností a zariadení** - Mal by byť navrhnutý a použitý spôsob zaistenia fyzickej bezpečnosti pre kancelárie, miestnosti a prostriedky.
  - **Ochrana pred vonkajšími hrozbami a hrozbami okolia** - Mala by byť navrhnutá a zavedená **fyzická ochrana proti poškodeniu ohňom, záplavami, zemetrasením, výbuchom, občianskym nepokojom** a ostatnou formou prírodných a človekom spôsobených havárií.

Fyzická bezpečnosť a bezpečnosť prostredia – bezpečné priestory

- **Práca v bezpečných priestoroch** - V organizácii by mala byť navrhnutá a zavedená **fyzická ochrana a pravidlá na prácu v bezpečných priestoroch**.
- **Verejný prístup, dodávky a nakladacie priestory** - **Prístupové miesta** ako sú dodávacie a nakladacie priestory a iné miesta, kam môžu vstúpiť neautorizované osoby do priestorov organizácie, **by mali byť riadené** a ak je to možné, **oddelené od prostriedkov** spracovania informácií, na zabránenie neoprávnenému prístupu.

Fyzická bezpečnosť a bezpečnosť prostredia – bezpečnosť zariadení

- Cieľom tejto časti je zistiť ako je **zabránené strate, poškodeniu, krádeži alebo kompromitácii aktív a prerušeniu aktivít organizácie**.
- Zariadenia by mali byť chránené pred fyzickými hrozbami a hrozbami prostredia.
- **Ochrana zariadení** (vrátane používaných mimo priestorov organizácie a vyradenia majetku) je nevyhnutná **na redukciu rizika neautorizovaného prístupu** k informáciám a na ochranu proti strate a poškodeniu. To sa týka aj umiestnenia zariadení a jeho odstránenia. Špeciálne opatrenia môžu byť vyžadované na ochranu proti fyzickým hrozbám a na zabezpečenie podporných vybavení ako je napríklad dodávka elektriky a rozvodná infraštruktúra.
- Opatrenia:
  - **Ochrana a umiestnenie zariadení** - Zariadenie by malo byť umiestnené alebo chránené tak, aby sa **redukovalo riziko hrozieb** a nebezpečnosti prostredia a možnosti neautorizovaného prístupu.
  - **Podporné služby** - Zariadenia by mali byť **chránené proti poruchám napájania** a ostatným prerušeniam činnosti spôsobených poruchami v podporných službách.
  - **Bezpečnosť rozvodov** - Silové a **telekomunikačné rozvody** nesúce údaje alebo podporujúce informačné služby by mali byť **chránené proti odpočúvaniu alebo poškodeniu**.
  - **Údržba zariadení** - Zariadenia by mali byť správne **udržiavané s cieľom zaistiť ich kontinuálnu dostupnosť a integritu**.

Fyzická bezpečnosť a bezpečnosť prostredia – bezpečnosť zariadení

- **Bezpečnosť zariadení mimo priestorov organizácie** - Bezpečnosť by mala byť aplikovaná **na zariadenia mimo priestorov organizácie** berúc do úvahy rôzne riziká práce mimo priestorov organizácie.
- **Bezpečné odstavenie alebo znovupoužitie zariadenia** - Všetky položky zariadenia obsahujúce pamäťové médiá by mali byť **skontrolované**, aby sa zaistilo, že **všetky citlivé údaje a licencovaný softvér bol odstránený** alebo bezpečne prepísaný pred odstavením zariadenia.
- **Vynesenie zariadenia** - Zariadenie, informácie alebo softvér by **nemal byť vynesený z priestorov organizácie bez predchádzajúcej autorizácie**.

Komunikačný a prevádzkový manažment – prevádzkové procedúry a povinnosti

- Cieľom tejto časti je zistiť ako je zaistená **správna a bezpečná prevádzka prostriedkov** spracovania informácie.
- Mali by byť **zavedené povinnosti a procedúry na manažment a prevádzku všetkých prostriedkov** spracovania informácií. Toto zahrňuje návrh vhodných prevádzkových procedúr.
- Malo by byť implementované, kde je to vhodné, **oddelenie povinností** na redukciu rizika zneužitia systému z nedbanlivosti alebo z úmyslu.
- Opatrenia:
  - **Dokumentované prevádzkové procedúry** - Prevádzkové procedúry by mali byť **dokumentované, udržiavané** a mali by byť **dostupné** všetkým používateľom, ktorí ich potrebujú.
  - **Manažment zmien** - **Zmeny v prostriedkoch** spracovania informácií a v systémoch by mali byť **riadené**.
  - **Oddelenie povinností** - **Úlohy a oblasť povinností by mali byť oddelené** tak, aby sa **redukovali možnosti na neautorizovanú alebo neúmyselnú modifikáciu** alebo zneužitie aktív organizácie.
  - **Oddelenie vývojových, testovacích a prevádzkových prostriedkov** - Vývojové, testovacie a prevádzkové prostriedky by mali byť oddelené, aby sa **redukovalo riziko neautorizovaného prístupu alebo zmien v prevádzkovom systéme**.

Komunikačný a prevádzkový manažment – manažment dodávky služieb tretej strany

- Cieľom tejto časti je zistiť, či **je implementovaná a udržiavaná primeraná úroveň informačnej bezpečnosti a dodávky služieb v súlade s dohodami** o dodávke služieb s tretími stranami.
- Organizácia by mala kontrolovať implementáciu dohody, monitorovať súlad s dohodami a manažovať zmeny, aby sa zaistilo, že dodávané služby splňujú všetky požiadavky dohodnuté s treťou stranou.
- Opatrenia:
  - **Dodávka služby** - Malo by byť zaistené, že **bezpečnostné opatrenia, definície a úrovne dodávky služieb zahrnuté do dohody o dodávke** s treťou stranou sú treťou stranou **implementované, prevádzkované a udržiavané**.
  - **Monitorovanie a hodnotenie služieb tretej strany** - **Služby, správy a záznamy** poskytnuté treťou stranou by mali byť **pravidelne monitorované a hodnotené a mali by byť pravidelne vykonávané audity**.
  - **Manažment zmien služieb tretej strany - Zmeny v zabezpečovaní služieb**, vrátane udržovania a zlepšovania existujúcich politík informačnej bezpečnosti, procedúr a opatrení by mali byť **manažované** a mal by sa brať zreteľ na **kritickosť dotknutých obchodných systémov a procesov a na opakované ohodnotenie rizík**.

Komunikačný a prevádzkový manažment – plánovanie a akceptácia systému

- Cieľom tejto časti je zistiť, či je **minimalizované riziko zlyhania systémov**.
- **Predbežné plánovanie** a príprava **sú nevyhnutné pre zabezpečenie dostupnosti** adekvátnej kapacity zdrojov na zabezpečenie **požadovaného výkonu systému**.
- Mali by byť dostupné **odhady budúcich požiadaviek na kapacitu**, aby sa znížilo riziko preťaženia systému.
- **Prevádzkové požiadavky nových systémov** by mali byť **stanovené, zdokumentované a testované** pred ich akceptáciou a použitím.
- Opatrenia:
  - **Manažment kapacity** - **Používanie zdrojov** by malo byť **monitorované, vyladené** a mal by byť **vykonaný odhad požiadaviek na budúce kapacity** tak, aby sa zaistila požadovaná výkonnosť systému.
  - **Akceptácia systému** - Mali by byť **stanovené akceptačné kritériá pre nové informačné systémy**, aktualizácie a nové verzie a mali by byť **vykonané vhodné testy systému počas vývoja ešte pred akceptáciou**.

Komunikačný a prevádzkový manažment – ochrana pred škodlivým a mobilným kódom

- Cieľom tejto časti je zistiť, či je **chránená integrita softvéru a informácií**.
- Sú **požadované preventívne opatrenia** na zábranu a detekciu zavedenia **škodlivého kódu a neautorizovaného mobilného kódu**.
- Softvér a prostriedky spracovania informácií sú zraniteľné na zavedenie škodlivého kódu ako sú počítačové vírusy, sieťové červy, Trójske kone a logické bomby. Používatelia by mali byť **vedomí nebezpečia škodlivého kódu**. Manažéri by mali, kde je to vhodné, **zaviesť opatrenia na prevenciu, detekciu a odstránenie škodlivého kódu** a na riadenie mobilného kódu.
- Opatrenia:
  - **Opatrenia proti škodlivému kódu** - Mali by byť implementované **opatrenia detekcie, prevencia a obnovenia na ochranu pred škodlivým kódom** a procedúry primeraného používateľského povedomia.
  - **Opatrenia proti mobilnému kódu** - Tam, kde je povolené použitie mobilného kódu, konfigurácia by mala zabezpečiť, aby sa **autorizovaný mobilný kód vykonával v súlade s jasne definovanou bezpečnostnou politikou**, a neautorizovanému mobilnému kódu by malo byť zabránené jeho vykonávaniu.

Komunikačný a prevádzkový manažment – zálohy

- Cieľom tejto časti je zistiť, či je **zachovaná integrita a dostupnosť prostriedkov** spracovania informácií.
- Mali by byť **zriadené rutinné procedúry** za účelom vykonávania dohodnutej politiky a stratégie **tvorby záložných kópií údajov a nacvičovanie včasného obnovenia údajov**.
- Opatrenie:
  - **Zálohy informácií** - **Záložné kópie** informácií a softvéru by mali byť **vytvorené a pravidelne testované** v súlade s dohodnutou politikou tvorby záloh.

Komunikačný a prevádzkový manažment – manažment sieťovej bezpečnosti

- Cieľom tejto časti je zistiť, či je **zabezpečená ochrana informácií v sieťach** a ochrana podpornej infraštruktúry.
- Bezpečný manažment sietí, ktoré môžu prekleňovať hranice organizácií, vyžaduje starostlivé uváženie toku údajov, právne dôsledky, monitorovanie a ochranu.
- **Dodatočné kontroly** môžu byť tiež potrebné k **ochrane citlivých informácií prechádzajúcich cez verejnú sieť**.
- Opatrenia:
  - **Sieťové opatrenia** - Siete by mali byť **adekvátnym spôsobom manažované a riadené, aby boli chránené pred hrozbami** a bola **zachovaná bezpečnosť systémov a aplikácií** používajúcich tieto siete, vrátane prenášaných informácií.
  - **Bezpečnosť sieťových služieb** - **Bezpečnostné funkcie, úrovne služieb a požiadavky na manažment všetkých sieťových služieb** by mali byť identifikované a **zahrnuté do každej dohody o sieťovej službe** (ak je to aplikovateľné), bez ohľadu na to či sú tieto služby poskytované interne alebo sú outsourcované.

Komunikačný a prevádzkový manažment – narábanie s médiami

- Cieľom tejto časti je zistiť, či je **zabránené neoprávnenému zverejneniu, modifikácii, odstráneniu alebo zničeniu aktíva** a prerušeniu činnosti organizácie.
- **Médiá by mala byť riadené a fyzicky chránené**.
- Mali by byť **zavedené vhodné prevádzkové procedúry na ochranu** dokumentov, počítačových médií (napríklad pásky, disky), vstupných/výstupných údajov a systémovej dokumentácie **pred neautorizovaným zverejnením, modifikáciou, odstránením a zničením**.
- Opatrenia:
  - **Manažment vymeniteľných médií** - Mali by byť zavedené **procedúry na manažment vymeniteľných médií**.
  - **Likvidácia médií** - Médiá by mali byť **zlikvidované použitím formálnych procedúr bezpečne** a iste, ak už nie sú potrebné.
  - **Procedúry narábania s informáciami** - Mali by byť zriadené **procedúry na narábanie a ukladanie informácií** s cieľom ochrániť tieto informácie **pred neautorizovaným zverejnením alebo zneužitím**.
  - **Bezpečnosť systémovej dokumentácie** - Systémová dokumentácia by mala byť **chránená proti neautorizovanému prístupu**.

Komunikačný a prevádzkový manažment – výmena informácií

- Cieľom tejto časti je zistiť, či je **zachovaná bezpečnosť pri výmene informácií a softvéru v rámci organizácie a s externým subjektom**.
- Výmeny informácií a softvéru medzi organizáciami by mala byť založená **na formálnej politike výmeny**, ktoré sa vykonajú **v súlade s dohodami o výmene**, a ktoré by mali byť v súlade so všetkými relevantnými právnymi predpismi.
- Mali by byť stanovené procedúry a štandardy na **ochranu informácií a fyzických nosičov obsahujúcich informácie pri prenose**.
- Opatrenia:
  - **Politiky a procedúry na výmenu informácií** - Mali by byť zavedené **politiky formálnej výmeny**, procedúry a opatrenia na ochranu výmeny informácie **prostredníctvom všetkých typov komunikačných prostriedkov**.
  - **Dohody o výmene** - Pre výmenu informácií a softvéru medzi organizáciou a externou stranou by mali byť stanovené dohody.
  - **Prenos fyzických medií** - Médiá obsahujúce informácie by mali byť **chránené počas prepravy za fyzickými hranicami organizácie** pred neautorizovaným prístupom, zneužitím alebo poškodením.
  - **Elektronické posielanie správ** - Informácie obsiahnuté v elektronickej správe by mali byť **primerane chránené**.
  - **Obchodné informačné systémy** - Politiky a procedúry by mali byť vytvárané a vykonávané na ochranu informácií v súvislosti s prepojením obchodných informačných systémov.

Komunikačný a prevádzkový manažment – služby elektronického obchodu

- Cieľom tejto časti je zistiť, či je zaistená **bezpečnosť služieb elektronického obchodu a ich bezpečné používanie**.
- Mali by byť vzaté do úvahy **bezpečnostné dôsledky spojené s používaním služieb elektronického obchodu**, vrátane on-line transakcií a mali by byť vzaté do úvahy požiadavky na opatrenia. Tiež by mali byť vzaté do úvahy integrita a dostupnosť informácií elektronicky publikovaných prostredníctvom verejne dostupných systémov.
- Opatrenia:
  - **Elektronický obchod** - Informácie súvisiace s elektronickým obchodom a prechádzajúce cez verejné siete by mali byť **chránené pred podvodnou aktivitou, zmluvným sporom a neautorizovaným zverejnením a modifikáciou**.
  - **On-line transakcie** - Informácie obsiahnuté v on-line transakciách **by mali byť chránené, aby sa zabránilo** neúplnému prenosu, chybnému smerovaniu, neautorizovanej zmene správy, neautorizovanému zverejneniu, neautorizovanej duplikácii správy alebo znovuposlatiu správy.
  - **Verejne dostupné informácie** - **Integrita informácií**, ktoré sú dané k dispozícii na verejne prístupných systémoch **by mala byť chránená**, aby sa zabránilo jej neautorizovanej modifikácii.

Komunikačný a prevádzkový manažment – monitorovanie

- Cieľom tejto časti je zistiť, či sa **detekujú neautorizované aktivity spracovania informácií**.
- Systémy by mali byť monitorované a udalosti informačnej bezpečnosti by mali byť zaznamenané. Záznamy činnosti operátora a záznamy chýb by mali byť **použité na identifikáciu problémov informačného systému**.
- Organizácia by mala splňovať všetky príslušné **právne požiadavky** vzťahujúce sa na jej monitorovanie a zaznamenávanie činnosti.
- **Monitorovanie systému** by malo byť použité na **kontrolu účinnosti** prijatých opatrení a overenie zhody s modelom politiky prístupu.
- Opatrenia:
  - **Ukladanie auditných záznamov** - Auditný záznam zaznamenáva aktivity používateľov, výnimky a udalosti v informačnej bezpečnosti, a mal by byť **vytváraný a udržovaný po dohodnutú dobu** na pomoc pri **budúcich vyšetrovaniach a na monitorovanie riadenia prístupu**.
  - **Monitorovanie používania systému** - Procedúry na monitorovanie využitia prostriedkov spracovania informácií by mali byť zriadené a **výsledky monitorovacích aktivít pravidelne preskúmané**.
  - **Ochrana informácií v záznamoch** - Prostriedky záznamu a zaznamenané informácie by mali byť **chránené proti neoprávnenému zasahovaniu a neautorizovanému prístupu**.
  - **Záznamy administrátora a operátora** - Aktivity **administrátora systému a operátora systému** by sa mali **zaznamenať**.

Komunikačný a prevádzkový manažment – monitorovanie

- **Ukladanie chybových záznamov** - Chyby by mali byť zaznamenané, analyzované a mali by sa vykonať vhodné akcie.
- **Synchronizácia hodín** - Hodiny všetkých relevantných systémov spracovania informácií v rámci organizácie alebo bezpečnostnej domény by mali byť **synchronizované s dohodnutým zdrojom presného času**.