# Návrh doplnenia štandardov ISVS:

(Pojmy do §2, ak existujú –napr. audit- nahradiť týmito pojmami):

**Audit** - Nezávislé formálne preskúmanie reálneho stavu systému (organizácie) oproti želanému stavu, definovanému napr. zákonom, štandardom, bezpečnostnou politikou alebo nejakým interným dokumentom organizácie.

Bezpečnostný audit je zameraný na posúdenie adekvátnosti bezpečnostných opatrení, na zistenie súladu s ustanovenými politikami a prevádzkovými postupmi a overenie skutočného stavu systému oproti želanému stavu. Výsledkom bezpečnostného auditu je vyjadrenie miery zhody so želaným stavom a odporúčania nevyhnutných zmien opatrení, politík a procedúr s cieľom vyhodnotiť a zlepšiť účinnosť a efektívnosť riadenia rizík a riadiacich a kontrolných procesov. 2. Vytváranie záznamov o bezpečnostne relevantných činnostiach v systéme

**Bezpečnostný audit** - proces nezávislého formálneho preskúmania záznamov a činností, procesov a systémov. Slúži na posúdenie adekvátnosti riadiacich a kontrolných prvkov systému, na kontrolu súladu s platnými politikami a prevádzkovými postupmi a na overenie zhody s bezpečnostnými požiadavkami. Môže obsahovať odporúčania nevyhnutných zmien

riadiacich a kontrolných prvkov, politík a procedúr s cieľom zlepšiť účinnosť a efektívnosť riadenia rizík a riadiacich a kontrolných procesov pri zaisťovaní dôvernosti, integrity a dostupnosti.

(Audit event? Audit logging? Audit record?)

**Autentizácia, autentifikácia** - proces overovania proklamovanej identity nejakej entity (používateľa počítačového systému, druhej strany v komunikácií, elektronického dokumentu, správy prijatej z počítačovej siete, a podobne).

**Bezpečný manažment konfigurácie** - množina procedúr vhodných na riadenie zmien hardvérovej a softvérovej konfigurácie systému, ktorej použitie zaisťuje, že zmeny konfigurácie nepovedú k narušeniu bezpečnostnej politiky systému

**Dostupnosť** - bezpečnostná požiadavka na to, aby údaje a zdroje systému boli dostupné oprávnenej osobe vždy, keď o to požiada.

**dôvernosť údajov** - bezpečnostná požiadavka na ochranu údajov, ktorej splnenie znamená, že k informácii obsiahnutej v údajoch nemajú prístup nepovolané osoby/entity

**Integrita údajov** - 1. bezpečnostná požiadavka na ochranu údajov, ktorej splnenie znamená, že údaje nemôžu byt’ modifikované bez toho, aby to ich oprávnený používateľ nebol schopný

zistiť, 2. atribút (údajov) ktorý majú údaje získané zo zdroja informácií vtedy, ak neboli náhodne alebo zámerne modifikované, poškodené alebo zničené

**Havária, katastrofa** - náhla, nepredvídaná katastrofická udalosť, ktorej dôsledkom je závažné poškodenie alebo strata kapacít/zdrojov, čo sťažuje až znemožňuje organizácii plniť niektoré jej funkcie alebo poskytovať služby, ktoré závisia na systémoch postihnutých touto udalosťou.

**Plán obnovy po havárii** - dokumentácia obsahujúca postupy, procesy a procedúry upravujúce spôsob, ako reagovať na havarijnú situáciu, zálohovať zdroje a informácie a ako obnoviť činnosť po havárii v prípade, že organizácia prekoná čiastočný alebo úplný výpadok svojej technologickej infraštruktúry alebo fyzickej lokality po prírodnej katastrofe alebo havárii spôsobenej ľudským činiteľom. Primárnym cieľom plánu obnovy po havárii je poskytnúť rozumnú záruku, že sa technologickú infraštruktúru po takýchto incidentoch podarí obnoviť v dostatočnej miere na to, aby mohla pokračovať v spracovaní životne dôležitých procesov v degradovanom režime (t.j. podporovať minimálne kritické procesy) a v prijateľnom čase obnoviť normálnu prevádzku.

**Bezpečnostný profil** - detailný popis fyzickej štruktúry, komponentov zariadenia, umiestnenia, vzťahov a všeobecného prevádzkového prostredia informačného systému z hľadiska bezpečnosti.

**Riziko** - potenciálna možnosť, že dôjde k naplneniu hrozby voči aktívu, čo bude mat’ negatívne dôsledky voči aktívu a organizácii, ktorej aktívum patrí. Miera, alebo hodnota rizika sa vyjadruje ako stredná hodnota dopadu hrozby, t.j. súčin pravdepodobnosti toho, že sa hrozba naplní a

dopadu hrozby na konkrétne aktívum.

**Akceptovateľné riziko** - riziko, ktoré je organizácia ochotná tolerovať bez toho, aby na jeho elimináciu alebo zníženie prijala dodatočné opatrenia

**Akceptovanie rizika -** rozhodnutie o akceptovaní konkrétneho rizika (t.j. rozhodnutie, že organizácia nebude prijímať opatrenia na zníženie alebo elimináciu daného rizika), založené na poznaní hodnoty rizika a dôsledkov, ktoré jeho akceptovanie pre systém resp. inštitúciu

prináša

**Analýza rizík -** proces, ktorý systematicky (a) identifikuje aktíva systému, hrozby voči týmto aktívam, zraniteľnosti aktív a existujúce bezpečnostné opatrenia na ochranu aktív (b) na základe možných dopadov hrozieb a pravdepodobnosti ich naplnenia odhadne potenciálne straty a (c) (nepovinne) odporúča, ako využiť dostupné zdroje na protiopatrenia na minimalizáciu celkového ohrozenia. Postup pri analýze rizík špecifikuje norma ISO/IEC 27005.

**Odhad rizika** - priradenie hodnôt pravdepodobnosti hrozby a dopadu hrozby na aktívum, na základe ktorého sa potom vyjadrí hodnota rizika. Ak má organizácia 10 PC v hodnote 1000 Euro za PC a pravdepodobnosť krádeže je 0.01, tak riziko krádeže PC dosahuje pre danú organizáciu 100 Euro. Predchádzajúci príklad ilustroval kvantitatívny odhad rizika.

Keďže aj pravdepodobnosť aj dopad hrozby je niekedy ťažké presne vyčísliť (napríklad poškodenie dobrého mena organizácie, pravdepodobnosť ochorenia kľúčového IT špecialistu) na odhad rizika je možné použiť kvalitatívny prístup, založený na klasifikácii pravdepodobností a dopadu na škále (nulový (0) nízky (N), stredný(S), vysoký(V)). Riziko je možné určiť napr. pomocou tabuľky:

D/P 0 N S V

0 0 0 0 0

N 0 N N S

S 0 N S V

V 0 S V V

Pozri tiež: ISO/IEC 27005

**Vyhodnotenie rizika** - proces porovnávania a tiež výsledok porovnania odhadovaného rizika oproti stanoveným kritériám (organizácie) s cieľom určiť závažnosť rizika. Základným cieľom vyhodnotenia rizika je určenie tých rizík, ktorých hodnota prekračuje úroveň akceptovateľného rizika.

**Manažment rizík** - proces identifikácie, ohodnocovania a riadenia (zmierňovania) rizík v informačných a komunikačných systémoch alebo organizáciách, ktorého cieľom je redukovať riziká na úroveň primeranú hodnote aktív, ktoré je potrebné chrániť.

**Redukcia rizika** - Kroky podniknuté na zníženie pravdepodobnosti naplnenie hrozby a/alebo jej dopadu na aktívum, napr. odstránením zraniteľností, ktoré daná hrozba využíva

**Ošetrenie rizika** - výber a implementácia opatrení na zmiernenie, elimináciu, prenesenie rizika alebo spôsob spravovanie rizika

**Bezpečnostné opatrenia** - 1. riadiace, prevádzkové a technické riešenia a postupy (napríklad ochrana a obrana) stanovené pre informačný systém na ochranu dôvernosti, integrity a dostupnosti systému a informácií 2. Techniky a metódy na zabezpečenie toho, aby len oprávnení používatelia majú prístup k informačným systémom a ich zdrojom

**Administratívne opatrenia** - činnosti alebo opatrenia na zaistenie efektívnosti a bezpečnosti

prevádzky systémov (a organizácie), založené na účinnosti a dodržiavaní predpisov a bezpečnostných politík

**Aktívum -** čokoľvek, čo má pre organizáciu alebo vlastníka nejakú cenu. Medzi aktíva súvisiace s IKT patria informačné aktíva (databázy, súbory, kontrakty a dohody, dokumentácia systémov, výsledky výskumu, používateľské manuály, tréningové materiály, operačné a podporné procedúry, plány kontinuity, archívne údaje;)

• softvérové aktíva (systémový softvér, aplikačný softvér, vývojové nástroje)

• fyzické aktíva (počítače, komunikačné zariadenia, prenosné pamäťové médiá a iné zariadenia)

• služby (výpočtové a komunikačné služby, kúrenie, osvetlenie, klimatizácia, zdroje energie, vody a i.)

• ľudia, ich kvalifikácia, skúsenosti a zručnosti,

• nehmotné aktíva, ako reputácia a imidž organizácie

**Hodnota aktíva** - dá sa merať’ výškou ujmy, ktorú by organizácia utrpela stratou alebo zničením aktíva. V prípade hmotných aktív sa dá vyjadriť kvantitatívne, napr. hodnota systému organizácie pozostáva z ceny za obnovu systému, výšky strát ktoré organizácia utrpela v dôsledku nefunkčnosti systému a prípadnej kompromitácie údajov, ktoré systém obsahoval; v prípade nehmotných aktív (know-how, dobré meno organizácie) je vhodnejšie kvalitatívne ohodnotenie. Hodnota aktív sa využíva pri výpočte hodnoty rizík.

**Bezpečnostná klasifikácia informácie**

1. Bezpečnostná klasifikácia informácie je rozdelenie informácie do tried podľa potrieb ochrany. V jednej triede sú informácie (typy informácií) s rovnakými potrebami na úroveň ochrany.
2. Potreba úrovne ochrany informácie sa stanovuje postačujúcou[[1]](#footnote-1) úrovňou ochrany pred narušením jej dôvernosti, integrity, autentickosti a dostupnosti.
3. postačujúca úroveň ochrany informácie je v prípade integrity, dostupnosti a autentickosti vyjadrená na trojstupňovej škále – vysoká, stredná a nízka; v prípade dôvernosti na štvorstupňovej škále vysoká, stredná, nízka a žiadna alebo nulová[[2]](#footnote-2)
4. vysoká úroveň ochrany dôvernosti informácie je potrebná vtedy, ak by narušenie dôvernosti spôsobilo
   1. poškodenie dobrého mena SR, organizácie
   2. smrť alebo vážne poškodenie zdravia ľudí,
   3. finančné straty ohrozujúce existenciu organizácie
   4. dlhodobú stratu schopnosti organizácie plniť jej základné funkcie.
5. nízka úroveň ochrany dôvernosti informácie je postačujúca vtedy, ak by narušenie dôvernosti informácie spôsobilo
   1. malé finančné straty
   2. krátkodobé výpadky v poskytovaní, alebo zníženie dostupnosti služieb, ale neovplyvniko hlavné činnosti organizácie
6. stredná úroveň ochrany dôvernosti je potrebná vtedy, ak nepostačuje nízka úroveň, ale nie je potrebná vysoká úroveň ochrany dôvernosti
7. verejne dostupná informácia si nevyžaduje ochranu z hľadiska dôvernosti, úroveň ochrany dôvernosti zverejnenej informácie je nulová.
8. úroveň ochrany z hľadiska integrity, dostupnosti a autentickosti informácie sa stanovuje analogicky ako v od. 4) – 6).
9. výsledok bezpečnostnej klasifikácie informácie má podobu idTypuInformácie [dôvernosť: C; integrita: I; dostupnosť: Av, autentickosť: Au], kde
   1. idTypuInformácie je identifikátor označujúci druh informácie z hľadiska obsahu, alebo účelu (administratívna, osobné údaje, utajované skutočnosti, zdravotné údaje, mzdy, a.i.)
   2. C je potrebná úroveň ochrany dôvernosti; C ∈{nulová, nízka, stredná, vysoká}
   3. I je potrebná úroveň ochrany integrity; I ∈{ nízka, stredná, vysoká}
   4. Av je potrebná úroveň ochrany dostupnosti; Av ∈{ nízka, stredná, vysoká}
   5. Au je potrebná úroveň ochrany autentickosti; Au ∈{ nízka, stredná, vysoká}

**Administratívne/organizačné zabezpečenie** - organizačné postupy, politiky a procedúry na riadenie výberu, vývoja, implementácie a údržby bezpečnostných opatrení a na riadenie pracovníkov zúčastňujúcich sa týchto procesov

**Odhaľovanie anomálií** - technika detekcie narušenia systému na základe aktivít, ktoré sa líšia

od normálneho správania systémových entít a systémových zdrojov

**Bezpečnostné povedomie** - poznanie potreby ochrany informácií a IKT systémov a tiež vlastnej účasti na ich ochraňovaní. Budovanie bezpečnostného povedomia sa orientuje na vytvorenie základnej predstavy laických používateľov IKT systémov o tom, čo a prečo treba robiť, resp. čo a prečo sa robiť nemá a ako bezpečne používať konkrétne IKT systémy.

**Havarijný plán** - plán činnosti v núdzovej situácii, na zaistenie záložných operácií a na obnovenie činnosti po katastrofe v systéme. Havarijný plán predstavuje úplný a ucelený prehľad všetkých činností, ktoré je potrebné vykonávať pred, počas a po katastrofe, spolu so zdokumentovanými a otestovanými procedúrami, ktorý v prípade, že sa podľa neho bude postupovať, zaistí dostupnosť kritických zdrojov a uľahčí zachovanie kontinuity operácií v núdzovej situácii.

**Kontinuita** - nepretržitá dostupnosť zdrojov potrebných k efektívnemu priebehu procesov v organizácii

**Plán kontinuity činností** 1. formálne zdokumentovaný a testovaný plán činností, ktoré sa majú vykonávať v prípade bezpečnostného incidentu alebo havárie, aby sa zaistilo nepretržité poskytovanie služieb a dodávanie produktov 2. súbor dokumentovaných postupov a informácií, ktoré tvoria, zdokonaľujú a udržujú pripravenosť organizácie v čase incidentu a umožnia organizácii kontinuálne realizovať jej kritické procesy na preddefinovanej akceptovateľnej úrovni.

**Plánovanie kontinuity činnosti**- proces zameraný na zabezpečenie toho, aby v prípade výskytu neočakávanej alebo nežiadúcej udalosti, ktorá spôsobí narušenie funkčnosti infraštruktúry, systému alebo organizácie, bola prevádzka narušenej infraštruktúry, systému alebo organizácie v požadovanom čase obnovená. Plánovanie kontinuity činnosti pozostáva z piatich základných fáz: analýzy, návrhu riešení (vypracovania plánov kontinuity činnosti), implementácie riešení, testovania a napokon údržby plánov kontinuity činnosti.

**Analýza dopadov na činnosť** - analýza ktorá odhadne dopady výpadku (straty, poškodenia) jednotlivých zdrojov organizácie, odhadne narastanie strát v čase, identifikuje minimum zdrojov potrebných na obnovu a stanoví priority pri obnove procesov a podporných systémov

**Intrusion prevention system (IPS) systém na prevenciu narušenia** - proces alebo podsystém detegujúci pokusy o narušenie alebo príznaky narušenia počítačového systému alebo siete, ktorý sa zároveň pokúša zabrániť aktivitám vedúcim k narušeniu počítačového systému alebo siete (v ideálnom prípade ešte pred dokonaním narušenia).

**Škodlivý kód** - program, ktorý je zvyčajne tajne vložený do systému so zámerom narušiť dôvernosť, integritu alebo dostupnosť údajov, aplikácií, operačného systému alebo iných zdrojov cieľového systému, alebo nejakým iným spôsobom obťažovať alebo poškodzovať

obeť. Motívom vytvárania a šírenia škodlivého kódu je najčastejšie zisk.

**Penetračné testovanie** - testovanie bezpečnosti systému, pri ktorom sa testujúci snažia na základe znalosti návrhu a implementácie informačného systému obísť jeho bezpečnostné funkcie (a preniknúť do systému)

**Sociálne inžinierstvo** - netechnické metódy prieniku do systémov (ale aj pokusy o podvod), založené na interakcii s inými ľuďmi, ktorých sa útočník snaží nejakým spôsobom oklamať a priviesť k tomu, aby porušili normálne bezpečnostné procedúry. Napríklad, podvodník sa môže pokúsiť získať dôveru oprávnenej osoby, tým, že sa vydáva za bezpečnostného experta, ktorý rieši akútny problém v informačnom systéme a požiada oprávnenú osobu, aby mu prezradila prístupové heslo, alebo umožnila prístup do systému. Podvodníci využívajú skutočnosť, že ľudia si väčšinou neuvedomujú hodnotu informácií, ktoré vlastnia ani potrebu ich ochrany; zneužívajú márnivosť, ochotu ľudí pomáhať, bezradnosť pri riešení neočakávaných situácií, rešpekt pred autoritami a iné prirodzené ľudské vlastnosti. Mnohé z útokov na informačné systémy prostredníctvom ich oprávnených používateľov využívajú metódy sociálneho inžinierstva.

**Hrozba** - objektívne existujúca možnosť, ktorej naplnenie je schopné spôsobiť škodu na informáciách, IKT systéme, technickej infraštruktúre, dobrom mene alebo iných aktívach organizácie.

**Analýza hrozieb** - identifikovanie relevantných hrozieb voči systému (organizácii) a tiež identifikácia aktív, na ktoré sú tieto hrozby zamerané

**Odhad hrozby** - formálne popísanie druhu a charakteru hrozby a vyhodnotenie úrovne hrozby voči aktívu

**Monitorovanie hrozieb** - analýza záznamov monitorovania, prípadne aj iných údajov, zhromažďovaných s cieľom identifikovať udalosti v systéme, ktoré by mohli predstavovať porušenie, alebo pokus o porušenie bezpečnosti údajov alebo systému

**Topológia** - geometrické usporiadanie systému alebo siete. Fyzická topológia popisuje kadiaľ vedú komunikačné linky spájajúce jednotlivé komponenty systému alebo siete a logická topológia popisuje tok údajov medzi komponentami systému alebo siete.

**Zodpovednosť používateľa od začiatku do konca** - vlastnosť systému, ktorá umožňuje jednoznačne zistiť, aké činnosti daná entita vykonávala v systéme od vstupu do systému až po jeho opustenie (odhlásenie sa zo systému)

**Zraniteľnosť** - slabé miesto informačného systému, šifrovacieho systému, alebo komponentov, ktoré môže byt’ využité pre vedenie útoku.

**Analýza zraniteľnosti** - systematické overovanie informačného systému alebo produktu s cieľom určiť adekvátnosť bezpečnostných opatrení, identifikovať bezpečnostné nedostatky, získať údaje na predikciu účinnosti navrhovaných bezpečnostných opatrení a potvrdiť adekvátnosť takýchto opatrení po ich implementácií.

**Posúdenie/hodnotenie zraniteľností** - formálne popísanie a hodnotenie zraniteľností, ktoré zahŕňa citlivosť určitého systému na špecifický útok

**Služby**:

1. **služby verejnej správy** - výkon právomocí, práv a povinností orgánov riadenia, ktorých rozsah a spôsob výkonu ustanovujú osobitné predpisy,
2. **elektronické služby verejnej správy** - elektronická forma komunikácie s orgánmi riadenia pri vybavovaní podaní, oznámení, prístupe k informáciám a ich poskytovaní, alebo účasti verejnosti na správe verejných vecí,
3. **služby vo verejnom záujme** - výkon právomocí, práv a povinností orgánov riadenia, ktorých rozsah ustanovuje osobitný predpis, pričom spôsob ich výkonu osobitný predpis neustanovuje,

**Kritický proces** – činnosti povinnej osoby z hľadiska ich závislosti na ISVS bez ktorých povinná osoba nie je schopná vykonávať služby.

Do politiky (vložiť za č.14 písmena a) v §29)

1. určí bezpečnostné opatrenia na úrovni procesnej, organizačnej a technickej, v nadväznosti na rozhodnutia o spôsobe riadenia rizika, a určí opatrenia na ochranu dôvernosti, dostupnosti a integrity informácií, vrátane ochrany osobných údajov v zmysle osobitných predpisov[[3]](#footnote-3),
2. vyčlení zdroje na zabezpečenie implementácie a riadneho fungovania bezpečnostných opatrení,
3. určí prostriedky kontroly uplatňovania bezpečnostných opatrení,
4. určí postupy riešenia bezpečnostných incidentov v prípade narušenia definovaných bezpečnostných cieľov, a to aj v nadväznosti na mechanizmy riešenia bezpečnostných incidentov
5. určí minimálny rozsah vyhodnocovania stavu bezpečnosti informačných technológií verejnej správy najmenej raz ročne vo forme správy schvaľovanej na najvyššej úrovni povinnej osoby. Minimálne vstupy pre vyhodnotenie stavu sú:
   1. výsledky v oblasti kontrolných mechanizmov podľa § 32 vrátane správy z bezpečnostného auditu, prijatých opatrení na odstránenie prípadných zistených nedostatkov a hodnotenie účinnosti týchto opatrení
   2. akceptácia zvyškových rizík zistených pri analýze rizík
   3. vyhodnotenie účinnosti opatrení prijatých na ošetrenie rizík
   4. vyhodnotenie dostatočnosti zdrojov potrebných pre účinnú realizáciu bezpečnostných opatrení
   5. vyhodnotenie dostupnosti a výpadkov služieb vplyvom bezpečnostných incidentov
   6. vyhodnotenie dopadov bezpečnostných incidentov vrátane sankcií z dôvodu narušenia súkromia podľa osobitného predpisu (udelených štátom alebo vyplatených dotknutým osobám)
   7. vyhodnotenie účinnosti testovania BCM

**Zmeniť názov § 31 (už dnes je tam priplácnuté BCM a to nedostatočne) na**

**§ 31 Manažment rizík pre oblasť informačnej bezpečnosti a riadenie kontinuity**

**Odsek 1**

**Bezpečnostná klasifikácia informácie**

Štandardom pre bezpečnostnú klasifikáciu informácie je rozdelenie informácií v ISVS do tried podľa potrieb ochrany v súlade s potrebou úrovňou ochrany s minimálnym výsledkom bezpečnostnej klasifikácie informácie idTypuInformácie [dôvernosť: C; integrita: I; dostupnosť: Av, autentickosť: Au], kde

* 1. idTypuInformácie je identifikátor označujúci druh informácie z hľadiska obsahu, alebo účelu (administratívna, osobné údaje, utajované skutočnosti, zdravotné údaje, mzdy, a.i.)
  2. C je potrebná úroveň ochrany dôvernosti; C ∈{nulová, nízka, stredná, vysoká}
  3. I je potrebná úroveň ochrany integrity; I ∈{ nízka, stredná, vysoká}
  4. Av je potrebná úroveň ochrany dostupnosti; Av ∈{ nízka, stredná, vysoká}
  5. Au je potrebná úroveň ochrany autentickosti; Au ∈{ nízka, stredná, vysoká}

**Existujúce a)-e) dať ako odsek 2.**

**Bod f) presunúť do ods.3 a)**

**V odseku 2 pokračovať pri štandardoch pre analýzu rizík:**

f) V nadväznosti na klasifikáciu informácií v ISVS a bezpečný manažment konfigurácií je nutné aby povinná osoba zohľadnila analýze dopadov všetky aktíva súvisiace s ISVS vrátane závislosti služieb povinnej osoby na ISVS pri podpore kritických procesov.

g) výsledkom analýzy rizík je minimálne: určenie hladiny akceptovateľného rizika, odhad rizika, redukcia rizika a ošetrenie rizika. Zoznam identifikovaných rizík ako aj riziká nad hladinou akceptovateľného rizika musí správca predložiť najvyššiemu vedeniu povinnej osoby na  určenie potrebných opatrení a zabezpečenie zdrojov pre vykonanie potrebných opatrení.

Odsek 3. Riadenie kontinuity služieb povinnej osoby

Štandardom pre riadenie kontinuity služieb povinnej osoby je:

1. vypracovanie plánov kontinuity povinnej osoby na zabezpečenie všetkých činností potrebných pre fungovanie služieb povinnej osoby
2. vypracovanie analýzy dopadov výpadkov ISVS na kritické procesy pre fungovanie služieb povinnej osoby vrátane:
   1. identifikácie kritických procesov
   2. závislostí kritických procesov na ISVS
   3. vypracovanie požiadaviek na obnovu ISVS z pohľadu prípustnej doby výpadku a doby, počas ktorej je nutné obnoviť funkčnosť ISVS
3. vypracovanie plánov na obnovu činnosti nefunkčných, poškodených alebo zničených kritických informačných systémov verejnej správy zodpovedajúcich stanoveným požiadavkám na obnovu
4. Vypracovanie plánov obnovy ISVS správcom v nadväznosti na vypracovanie plánov kontinuity služieb povinnej osoby
5. zabezpečenie testovania v nadväznosti na identifikované riziká, pričom overovanie musí pokrývať všetky ISVS a ich prvky, ktorých výpadok by mal vplyv na kritické procesy povinnej osoby a služieb
6. c)zabezpečenie vykonania testu obnovy informačného systému verejnej správy najmenej raz za jeden rok a vyhodnotenie testu vzhľadom k schopnosti zabezpečenia kontinuity ISVS (presunúť z §39 d)
7. d) aktualizácia plánov na zabezpečenie kontinuity na základe výsledkov testovania BCM

**Bezpečný manažment konfigurácie (zatiaľ len v §36?)**

**Bezpečnosť ISVS v rámci životného cyklu (vložiť do §36 Aktualizácia softvéru, premenovať ho na Bezpečnosť ISVS v rámci životného cyklu a aktualizácia softvéru)**

Štandardom pre riadenie životného cyklu ISVS je zabezpečenie činností od vytvárania, nadobúdania, prevádzky a vyraďovania ISVS:

1. Povinná osoba pri vytváraní alebo nadobúdaní informačného systému verejnej správy
2. zhodnotí riziká informačného systému verejnej správy a určí bezpečnostné požiadavky na tento systém v súlade s platnou legislatívou a štandardizačnými dokumentami platnými pre povinnú osobu,
3. určí bezpečnostné požiadavky na informačný systém verejnej správy, vrátane podmienok jeho vývoja, testovania a dodania, v podmienkach vytvorenia alebo dodania informačného systému verejnej správy,
4. poskytne dodávateľovi informačného systému verejnej správy anonymizované kópie údajov na testovanie informačného systému verejnej správy a jeho vývoj.
5. Povinná osoba zabezpečí formou písomnej zmluvy pred obstaraním, že dodávateľ informačného systému verejnej správy pre vývoj tohto systému
6. zabezpečí
   1. bezpečné vývojové prostredie,
   2. dokumentáciu vývoja, vrátane používateľskej a administrátorskej dokumentácie,
   3. v prípade použitia technických lebo programových prostriedkov tretích strán ich certifikáciu alebo ich minimálne testovanie,
7. je oprávnený zabezpečiť vytvorenie časti informačného systému verejnej správy treťou osobou len s predchádzajúcim písomným súhlasom správcu,
8. je povinný
9. dodržiavať mlčanlivosť o dodávanom informačnom systéme verejnej správy aj po ukončení dodania a zaviazať rovnakou povinnosť všetky osoby, ktoré sa na dodaní podieľali,
10. dodržiavať vhodné bezpečnostné mechanizmy a preukázať, že ich rozsah a úroveň zodpovedajú bezpečnostným požiadavkám podľa odseku 1 písm. b),
11. identifikovať bezpečnostné požiadavky na informačný systém verejnej správy podľa odseku 1 písm. b), ktoré nie sú pokryté týmto systémom a predložiť správcovi návrh bezpečnostných opatrení na naplnenie týchto bezpečnostných požiadaviek pre prostredie, v ktorom bude informačný systém verejnej správy prevádzkovaný,
12. upozorniť správcu na kritické alebo rizikové časti informačného systému verejnej správy, ktoré odhalí pri jeho dodaní a navrhnúť opatrenia na ich riešenie,
13. preukázateľne odstrániť alebo znemožniť používanie funkcie informačného systému verejnej správy, ktoré by jemu alebo tretej strane umožňovali získať neoprávnený prístup do tohto systému a k údajom, ktoré obsahuje.
14. Pri odovzdaní odovzdať správcovi všetky administrátorské prihlasovacie mená a heslá.
15. V rámci zabezpečenia riadenia služieb bezpečnosti prevádzky povinná osoba
16. zabezpečuje zavedenie informačného systému verejnej správy do prevádzky,
17. zabezpečuje prevádzku informačného systému verejnej správy,
18. zabezpečuje vyradenie informačného systému verejnej správy z prevádzky.
19. V rámci zabezpečenia zavedenia informačného systému verejnej správy do prevádzky povinná osoba
20. pred zavedením do prevádzky overí splnenie funkčných, výkonnostných a bezpečnostných požiadaviek,
21. nezavedie do prevádzky informačný systém verejnej správy, ktorý nespĺňa požiadavky podľa písmena a),
22. pri zavádzaní informačného systému verejnej správy do prevádzky dbá na to, aby nebol dodávateľovi umožnený prístup k  ostatným informačným systémom, ani údajom, ktoré sa v nich spracúvajú a ak to nie je možné, zabezpečí nepretržitú kontrolu dodávateľa počas celej doby, po ktorú je potrebný prístup k ostatným informačným systémom alebo údajom, ktoré sa v nich spracúvajú,
23. V rámci zabezpečenia prevádzky informačného systému verejnej správy povinná osoba
24. zabezpečí pre informačný systém verejnej správy
    1. určenie a pravidelné aktualizovanie bezpečnostných cieľov,
    2. naplnenie bezpečnostných cieľov a eliminovanie negatívnych vplyvov a udalostí na informačný systém verejnej správy pri jeho prevádzkovaní.
25. v závislosti od zaradenia informačného systému verejnej správy z pohľadu klasifikácie informácií a kategorizácie sietí a informačných systémov
26. vypracuje pre tento systém bezpečnostný projekt ako dokumentáciu bezpečnostného profilu,
27. zavedie jednotný systém riadenia informačnej bezpečnosti pre všetky informačné systémy, ktoré sú v jej správe,
28. zabezpečí bezpečný manažment konfigurácie informačného systému verejnej správy a jeho častí vrátane aktualizácie údajov,
29. určí bezpečnostne závažné operácie, ktorými sa rozumejú najmä správa prístupov a prístupových údajov, ukladanie záznamov o systémových udalostiach, realizácia bezpečného oddelenia vnútornej časti systému a siete od vonkajšej časti a zavedie dokumentovanie postupov pre tieto operácie,
30. zabezpečí nepretržitý monitoring informačného systému verejnej správy,
31. zabezpečí vykonanie bezpečnostného auditu informačného systému verejnej správy najmenej raz ročne a v prípade zistenia závažných bezpečnostných nedostatkov prepracuje bezpečnostný projekt a naň nadväzujúce dokumenty.
32. V rámci vyradenia informačného systému verejnej správy z prevádzky povinná osoba
33. vypracuje plán vyradenia informačného systému verejnej správy z prevádzky, ktorý obsahuje najmä
34. uchovanie kritických informácií vyraďovaného informačného systému verejnej správy, ktoré sú už nepotrebné pre funkčnosť iného informačného systému,
35. spoľahlivé odstránenie informácií z pamäťových médií vyraďovaného informačného systému verejnej správy
36. postup vyraďovania programových a technických častí informačného systému verejnej správy,
37. zabezpečí, aby nedošlo ku strate alebo úniku citlivých informácií a k narušeniu práv priemyselného a duševného vlastníctva.

§32 Kontrolný mechanizmus doplniť

1. vykonávanie bezpečnostných auditov v súlade s frekvenciou určenou v bezpečnostnej politike povinnej osoby.
   * + 1. Bezpečnostný audit môže vykonať kvalifikovaná osoba na výkon auditu informačných systémov. Správa z auditu je povinnou súčasťou vstupov pre vyhodnocovania súladu podľa §14 , povinná osoba musí určiť opatrenia a zabezpečiť zdroje na odstránenie nedostatkov zistených bezpečnostným auditom.
       2. Fyzická osoba alebo právnická osoba je kvalifikovaná na výkon auditu bezpečnosti ISVS, ak

a) je držiteľkou platného medzinárodného alebo slovenského osvedčenia na výkon auditu informačných systémov,

b) má preukázateľnú odbornú prax v oblasti auditu informačných systémov nie kratšiu ako päť rokov,

c) je nezávislá od auditovaného subjektu,

d) zabezpečí, aby pri auditoch nedochádzalo ku konfliktu záujmov.

(3) Výkon auditu pozostáva z overenia

a) súladu so štandardami ISVS

b) vhodnosti a dostatočnosti opatrení a prostriedkov na zabezpečenie bezpečnostných požiadaviek vrátane súladu s podmienkami vnútorných predpisov v oblasti prevádzky ISVS, ktoré správca určil v súlade so všeobecne záväznými právnymi predpismi,

(4) Výkon auditu sa končí záverečnou správou, ktorá pozostáva z

a) výroku audítora a zo zhodnotenia súladu s požiadavkami v ods.3 alebo,

b) popisu zistení o nedostatkoch a nesúladu s požiadavkami,

c) odporúčaní na odstránenie zistených nedostatkov a lehôt na ich odstránenie.

**§ 33 ochrana voči škodlivému kódu**

**§ 34 Sieťová bezpečnosť (Vstup od CSIRT)**

Šifrová ochrana

**Detekcia anomálií**

**§36 Aktualizácia SW**

1. nie je potrebná vyššia úroveň [↑](#footnote-ref-1)
2. nie je potrebné zaisťovať dôvernosť informácie zverejňovanej na webe, ale je potrebné zaistiť jej integritu, dostupnosť a autentickosť [↑](#footnote-ref-2)
3. GDPR a zákon č. .../ Z.z. na ochranu osobných údajov [↑](#footnote-ref-3)