ARABCO 2019

Analýza rizík a aktualizácia katalógu aktív a Plánovanie kontinuity činností - BCM

I. Analýza rizík a aktualizácia katalógu aktív

Cieľom projektu je :

1. Vytvorenie dokumentu Analýza rizík, ktorý bude obsahovať identifikované bezpečnostné riziká, ktoré sú závislé od aktív systému, ich zraniteľností, vplyvov prostredia (hrozby) a potenciálneho negatívneho dopadu (dopadov) na ministerstvo. Súčasťou dokumentu analýza rizík je:

- Analýza rizík - podrobná správa, ktorá obsahuje identifikáciu:
    - aktíva a ich vlastníkov - zoznam aktív je špecifikovaný na úroveň jednotlivých technických komponentov, údajových štruktúr, lokácií, miestností a pod., úložísk,
    - rizík, ktoré majú dopad na aktíva - návrh sa riadenie rizík, pričom spôsob realizácie nemusí byť predikovateľný (t. j. nemusí byť určené, či správa rizika bude realizovaná organizačným alebo technickým opatrením, či prenos rizika bude znamenať poistenie alebo outsourcing a pod.),
    - hrozieb využívajúce zraniteľnosti aktív, ohodnotenie pravdepodobnosti naplnenia hrozieb, pričom stupnica hodnotenia je delená do minimálneho počtu úrovní tak, že stupne hodnotenia musia umožniť účelne rozlíšiť rozdiely v sile hrozby (pri hodnotení pravdepodobnosti naplnenia hrozby s použitou stupnicou by nemalo dôjsť k váhaniu pri výbere medzi viac ako 2 stupňami hodnotenia),
    - existujúcich opatrení,
    - zraniteľnosti zvyšujúcich bezpečnostné riziká - určenie zraniteľností aktív, pričom stupnica hodnotenie je delená do minimálneho počtu úrovní tak, že stupne hodnotenia musia umožniť účelne rozlíšiť rozdiely v úrovni zraniteľnosti (pri hodnotení zraniteľnosti by nemalo dôjsť k váhaniu pri výbere medzi viac ako 2 stupňami hodnotenia),
    - následkov dopadu jednotlivých hrozieb na aktívum – detailný popis možných dopadov na organizáciu v dôsledku narušenia dôvernosti, integrity alebo dostupnosti údajov a komponentov systému,
- návrh na ošetrenie rizík obsahuje:

- podrobný popis postupov na ošetrenie jednotlivých rizík bude so zreteľom na povahu a rozsah rizík,
- návrh na primerané technické a organizačné opatrenia
- návrh stratégie riešenia havarijných stavov vrátane identifikácie kontaktného miesta pre dozorný orgán, mechanizmu nahlasovania incidentov a hrozieb, poskytovania poradenstva prevádzkovateľovi.

- Katalóg aktív, identifikované aktíva rozdelené do skupín umožňujúce analyzovať jednotlivé subsystémy z rôznych pohľadov v závislosti na hodnotených skupinách aktív.

- Manažérske zhrnutie výsledkov – hodnotenie, odporúčania a návrh opatrení.

2. Nástroj na manažment rizík a evidenciu aktív

   Obsahom nástroja na zvládanie rizík a evidenciu aktív budú spracovateľné dáta obsahujúce:

   - Katalóg aktív z pohľadu jednotlivých :
     i. Aktív
     ii. Procesov
     iii. Závislosti jednotlivých aktív navzájom, identifikovaných v dokumente Analýza rizík podľa bodu 1.

   - Katalóg rizík a súbory pripravené na zaznamenávanie a vyhodnotenie zmien v rizikách
   - Metriky a pripravené súbory na hodnotenie metrík
   - Šablóny na vytvorené reportov zo spracovaných informácii
   - Vytvorené reporty zo spracovaných informácii.

3. Zaškolenie zamestnanca/ov Ministerstva financií Slovenskej republiky zodpovedných za informačnú bezpečnosť na Ministerstve financií Slovenskej republiky do vyššie uvedených procesov a vykonávania analýzy rizík. Pomôcky a dokumenty použité pri procesoch riadenia rizík budú po zaškolení odovzdané manažérovi bezpečnosti ministerstva, čím sa vytvorí nástroj na systém manažmentu rizík.

Použitá metodika - minimálne v rozsahu - Metodika kvalitatívnej analýza rizík podľa ISO/IEC 27005 a STN ISO/IEC 27002

4. Dodávateľ v rámci predmetu zákazky dodá:
   a) metodiku na vykonanie analýzy rizík,

b) dokument Analýza rizík, ktorý obsahuje identifikované bezpečnostné riziká, ktoré sú závislé od aktív systému, ich zraniteľností, vplyvov prostredia (hrozby) a potenciálneho negatívneho dopadu (dopadov) na ministerstvo. podľa bodu 1

c) katalóg aktív, identifikované aktíva rozdelené do skupín umožňujúce analyzovať jednotlivé subsystémy z rôznych pohľadov v závislosti na hodnotených skupinách aktív, identifikovaných v dokumente Analýza rizík podľa bodu 1.

d) nástroj na manažment rizík a evidenciu aktív

5. vypracuje a zrealizuje:

a) školenia k metodike na vykonanie analýzy rizík, a nástroju na zvládanie rizík a evidenciu aktív

II. Plánovanie kontinuity činností - BCM

1. Analýza dopadov
2. BC a DR plány
3. Testovanie

1. Analýza dopadov

1. Popis

Analýza dopadov je základným nástrojom Business Continuity Management na identifikáciu požiadaviek organizácie na kontinuitu prevádzky procesov, aktivít a zdrojov. Na základe analýzy dopadov, výstupov analýzy rizík a finančných možnosti stanoví organizácia svoju stratégiu k zaisteniu kontinuity činností nasledovne:

- Analýza dopadov stanoví požiadavky na kontinuitu,
- Analýza rizík stanoví riziká, ktoré môžu znamenať výpadok pracovných procesov,
- Finančné možnosti stanovia opatrenia, ktoré je možné aplikovať na zaistenie kontinuity činností.

Na základe schválených stratégii môže organizácia:

- realizovať projekty na zlepšenie odolnosti obchodných procesov voči identifikovaným rizikám,
- naplánovať obnovu kontinuity v prípade výpadku pracovných procesov.

2. Ciel a Výstup projektu

Cieľom analýzy dopadov je:

a) identifikácia procesov organizácie,

b) identifikácia závislostí a vzťahov identifikovaných procesov organizácie:

1. s ostanými súvisiacimi procesmi,
    (a) Ľudských zdrojov
    (b) Lokalít / budov
    (c) Technológií / IT systémov
    (d) a pod.
2. s tretími stranami,
3. v oblasti právnych predpisov, štandardov, noriem, metodík a pod., ktorými sa organizácia pri výkone činností riadi.

c) identifikácia informácií pre každý identifikovaný proces:
    1. identifikácia aktív nevyhnutných na zabezpečenie kontinuity procesov (bezproblémové vykonávanie procesov),
    2. informácie o maximálne tolerovateľnej nedostupnosti procesov (maximálne prípustná doba nevykonávania činností (MTD)),
    3. cieľ obnovy aktivity / procesu (RTO)
    4. cieľ obnovy dát (RPO)
    5. minimálna akceptovateľná úroveň služby
    6. identifikácia závislostí (právne, regulačné, zmluvné a pod.),
    7. zoznam dopadov v prípade úplného prerušenia vykonávania činností.

Výstupom z analýzy dopadov je dokumenty obsahujúci najmä:

a) zoznam kritických procesov organizácie a ich kategorizácia vzhľadom na
    1. prioritu obnovy (na základe identifikovaných maximálne tolerovateľných dôb nedostupnosti),
    2. stanovenie lehoty (doby) obnovy na základe zistených maximálne tolerovateľných dôb nedostupnosti,
b) zoznam dopadov,
c) zoznam závislostí vo vzťahu ku kritickým procesom,
d) zoznam aktív nevyhnutných na zabezpečenie kontinuity kritického procesu (bezproblémové vykonávanie činností procesu),
e) zoznam tretích strán so vzťahom ku kritickým procesom,
f) stratégia obnovy pre jednotlivé typy zdrojov a kritické zdroje minimálne v rozsahu :
    1. Stratégia obnovy pre ľudské zdroje Opatrenia v rámci stratégie obnovy pre personál:
        (a) Dokumentácia pracovných postupov
        (b) Prekrývajúce sa pracovné pozície
        (c) Zastupiteľnosť / Plánovanie nástupníctva
        (d) Rotácia zamestnancov
        (e) Použitie tretích strán
    2. Opatrenia v rámci stratégie obnovy pre priestory:
        (a) Alternatívne priestory v rámci organizácie
        (b) Alternatívne priestory poskytnuté treťou stranou (recipročné alebo komerčné dohody)
    3. Opatrenia v rámci stratégie obnovy pre dodávateľov :

(a) *Zvýšenie počtu dodávateľov*
(b) *Identifikácia vhodných alternatívnych dodávateľov*
(c) *Požiadavky na preukázateľné a overiteľné zabezpečenie BCM na strane dodávateľa*
(d) *Dohody o úrovni poskytovaných služieb (SLA)*

g) celková stratégia obnovy pre základné business procesy.

2. BC a DR plány

- **Plány kontinuity činnosti - BCP**
- **Havarijné plány - DRP**

BCM plány budú vytvorené pre vybrané aktíva v rozsahu 3 IS podľa výberu objednávateľa.

1. Popis

Stratégie obnovy sú rozpracované do plánov obnovy „top-down“ prístupom. Posledným krokom je otestovanie plánov na základe vypracovanej metodiky a plánu. Používaný je prístup „bottom-up“, t.j. v prvom slede sa otestujú plány obnovy zdrojov a až následne sa vykonávajú testy komplexnejších plánov obnovy aktivít a procesov. Testovanie plánov je taktiež realizované od jednoduchších testov (napr. desk check) k zložitejším.

2. Ciel a Výstup

- Individuálne akčné plány – Plány kontinuity činností a havarijné plány špecifikujúce alternatívne procedúry pre kritické procesy a techniky obnovy pre kritické zdroje
- Vyškolený personál schopný používať akčné plány
- Dokument Politika kontinuity činností - BCM Policy

- **Plány kontinuity činnosti - BCP**

a) Metodika tvorby plánov kontinuity činností a vzorové šablóny pre tvorbu plánov nižšej úrovne
b) Vypracované BC plány v minimálne štruktúre:
    1. Popis procesu
        (a) Popis procesu z analýzy dopadov
        (b) Vlastník procesu a jeho zástupcovia
        (c) Parametre procesu – MTO, RTO, RPO
        (d) Zdroje využívané procesom
            (i) Aplikácie

(ii) Infraštruktúra
(iii) Údaje (vo fyzickej aj logickej podobe)
(iv) Ľudské zdroje
(v) Lokality
(vi) Dodávatelia

2. Popis minimálne týchto typov BC plánov
   (a) Nedostupnosť aplikácie
   (b) Obmedzenie funkčnosti aplikácie
   (c) Nedostupnosť budovy
   (d) Výpadok podporných služieb (elektrina, voda, kúrenie)
   (e) Výpadok služieb dodávateľa
   (f) Nedostupnosť ľudských zdrojov
3. Obmedzenia/predpoklady
4. Kontaktné údaje všetkých osôb uvedených v pláne

c) Vypracované BC plány na úrovni:
1. Strategický plán
2. Taktické plány pre jednotlivé procesy, základné business procesy a skupiny zdrojov
3. Prevádzkové plány pre jednotlivé zdroje

Štruktúra pre každý BC plán

(a) Prípravné úlohy
(b) Identifikácia problému
(c) Fáza reakcie
(d) Alternatívny proces
(e) Obnovovacie postupy
(f) Kontrolné úlohy

d) Metodika cvičení plánov kontinuity činností
e) Plán cvičení plánov
f) Záznamy z cvičení a testov realizovaných podľa plánu

- ## Havarijné plány - DRP

a) Metodika tvorby plánov kontinuity činností a vzorové šablóny pre tvorbu plánov nižšej úrovne
b) Vypracované DR plány v minimálne štruktúre
1. Popis zdroja (systému)
   (a) Popis zdroja
   (b) Vlastník/IT gestor zdroja a ich zástupcovia
   (c) Zoznam podporovaných procesov
   (d) Požiadavky na obnovu (MTO, RTO, RPO)

(e) Stratégia obnovy

2. Popis minimálne týchto typov DR plánov
   (a) Obnova údajov zo zálohy
   (b) Obnova konfigurácie aplikácie/databázy/operačného systému
   (c) Opätovná inštalácia aplikácie/ databázy/ operačného systému
   (d) Výmena hardvérového komponentu
   (e) Opätovná inštalácia celého hardvéru

   Štruktúra pre každý DR plán

   (i) Prípravné úlohy
   (ii) Identifikácia problému
   (iii) Fáza reakcie
   (iv) Obnovovacie postupy
   (v) Kontrolné úlohy
3. Obmedzenia/predpoklady
4. Kontaktné údaje všetkých osôb uvedených v pláne

3. Testovanie

1. Popis

Zistenia z testovania plánov sú zosumarizované s ostatnými zisteniami z procesu zavádzania BCM (napr. zistené body zlyhania – single point of failure, úpravy v metodike analýzy rizík atď.) a vytvorené odporúčania na ich odstránenie.

2. Ciel a Výstup

- Výsledky testovania akčných plánov
- Výsledky previerky BCM funkcie
- Identifikované nedostatky a odporúčania na zlepšenie
- Aktualizované BCM procesy a akčné plány

Použitá metodika minimálne v rozsahu podľa

- ISO/IEC ISO 22301:2012 Ochrana spoločnosti. Systémy manažérstva plynulého podnikania
- BSI-Standard 100-4 - Business Continuity Management

Ďalšie štandardy:
SANS Institute - Introduction to Business Continuity Planning

NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems - NIST SP-800-34

NFPA® 1600 - Standard on Disaster/Emergency Management and Business Continuity Programs