Vilniaus universitetas
Tarptautinis žinių ekonomikos ir žinių vadybos centras

Ingrida Kriščiūnaitė
Informacijos sistemų vadybos studentė

VEIKLOS TĘSTINUMO IR ATKŪRIMO PO NENUMATYTO ATVEJO INFORMACINĖSE SISTEMOSE PLANAS

MAGISTRO DARBAS

Vadovas: asist. I. Aleliūnas

Vilnius, 2007

Ingridos Kriščiūnaitės_____magistro darbas

(magistranto (-ės) vardas, pavardė)

tema

Veiklos tęstinumo ir atkūrimo po nenumatyto atvejo informacinėse sistemose planas____

parengtas gynimui.

_____

(data) (vadovo parašas)

Darbas įregistruotas_____centre

_____

(data) (administratorės parašas)

Magistro darbą ginti leidžiu

_____(centro Direktoriaus parašas)_____

(data)

Recenzentu skiriu

_____

_____

(data) (Direktoriaus parašas)

Darbą recenzavimui gavau

_____

(data) (recenzento parašas)

Kriščiūnaitė Ingrida

Kr277

Veiklos tęstinumo ir atkūrimo po nenumatyto atvejo informacinėse sistemose planas: magistro darbas / Ingrida Kriščiūnaitė; mokslinis vadovas asist. I. Aleliūnas; Vilniaus universitetas.

Tarptautinis žinių ekonomikos ir žinių vadybos centras. Vilnius 2007.

71 lap. Mašinr., Santr.angl.: p. 70-71, Bibliog.: p.69 (15 pavad.)

UDK 658:004

Veiklos tęstinumo ir atkūrimo po nenumatyto atvejo informacinėse sistemose planas

Tyrimo objektas - Veiklos tęstinumo ir atkūrimo po nenumatyto atvejo informacinėse sistemose planavimas ir palaikymas. Darbo tikslai: išanalizuoti veiklos tęstinumo ir atkūrimo politiką ir plano žingsnius. Darbo uždaviniai: išsiaiškinti informacinių sistemų sampratą, nustatyti grėsmes ir pažeidžiamumus galinčius pakenkti organizacijos veiklai, išnagrinėti veiklos tęstinumo, atkūrimo valdymo etapus, pateikti, išanalizuoti ir palyginti su šia tema susijusius kelis pagrindinius tarptautinius standartus, sudaryti planą, kaip užkirsti kelią pažeidžiamumams bei grėsmėms ir užtikrinti veiklos tęstinumą organizacijoje atsitikus nenumatytam atvejui.

Informacinių technologijų svarba organizacijos veikloje labai išaugo. Jos yra viena iš pagrindinių valdymo dalių organizacijoje. Informacinė sistema – tai prasmingą informaciją asmenims ir organizacijoms pateikianti ir kartu veikiančios aparatūros ir programinės įrangos, žmonių, procedūrų ir duomenų visuma. Šiuo metu vis daugiau informacijos yra automatizuojama, panaudojant kompiuterizuotas informacines sistemas.

Informacinės sistemos komponentai yra organizacijos turtas, kurį sudaro fizinis, informacinis, nematerialusis turtas, paslaugos, personalas ir programinė įranga.

Turtas yra įvairių rūšies grėsmių taikinys. Kad padaryti turtui žalą, grėsmė atsiranda silpniausioje, mažiausiai tikėtinoje situacijoje. Grėsmių sukėlėjai yra žmonės, žmonių grupės, gamtos reiškiniai, politiniai, ekonominiai ir socialiniai reiškiniai, galintys kelti grėsmę informacinių sistemų saugumui. Norint apsaugoti organizaciją nuo grėsmių, išvengti pagrindinių pasekmių bei rizikos bet kurioje srityje, būtina gerai žinoti informacijos saugumo valdymo sistemą.

Informacijos saugumo valdymo sistema – programinių, techninių, organizacinių priemonių visuma, kuri kuriama atsižvelgiant į teisines normas reglamentuojančias informacijos apsaugą. Informacijos saugos pagrindas – patikima informacijos saugumo valdymo sistema, apimanti tiek organizacinę, tiek technologinę dalį. Tačiau informacijos saugumo valdymo sistemos nepakanka užtikrinti organizacijos veiklos pilną saugumą ir gerą valdymą. Tam reikalingas nuoseklus procesų planas, kuris būtų naudojamas nuo veiklos ciklo gyvavimo pradžios iki pabaigos. Norint užtikrinti veiklos ciklus ir vykdymą, reikia susidaryti veiklos tęstinumo ir atkūrimo planą. Šis planas susideda iš veiklos tęstinumo ir atkūrimo valdymo procesų.

Veiklos tęstinumo ir atkūrimo valdymas reikalingas, kad organizacija tęstų veiklą duomenų praradimo, kritinių sistemų gedimo bei kitų informacinių technologijų veiklą nutraukiančių nelaimingų atvejų metu. Reikalinga dokumentuota ir pagrindžiama informacija apie tai, kiek įmonės veiklos funkcijos yra priklausomos nuo informacinių sistemų ir kokios informacinės sistemos yra labiausiai kritiškos, kurios mažiau kritiškos. Tai veiklos vadovams leis efektyviau panaudoti ir pagrįsti investicijas, skiriant daugiau lėšų kritiškoms sistemoms.

Darbo aktualumas: suformavus veiklos tęstinumo ir atkūrimo po nenumatyto atvejo informacinėse sistemose planą, galima įmonėje sutaupyti laiko, o tuo pačiu ir finansinių išteklių. Reikia atsižvelgti į organizacijos veiklos sritį, įmonės saugumui kylančius pavojus. Be šio plano organizacija rizikuoja, kad įvykus nenumatytam atvejui organizacijos veikla gali sutrikti ir būti neatkurta reikiamu laiku. Susistemintas veiklos tęstinumo ir atkūrimo valdymo planas palengvins vadovams nenutrūkstamai valdyti organizacijos veiklą. Numatant būsimas grėsmes darbuotojai imsis prevencinių veiksmų, o įvykus nelaimingam atsitikimui atkurs veiklą iki buvusios situacijos.

Magistro darbas gali būti naudingas organizacijos vadovams, darbuotojams, auditoriams.

TURINYS

ĮVADAS

Šiandien pasaulis – nuolat besikeičiantis, besivystantis, lankstus: sparčiai kinta technika, technologija, ūkinės veiklos, darbo organizavimas bei valdymas. Tai kelia naujus reikalavimus aktyviam ir lemiamam bet kurios organizacijos struktūros objektui, pavyzdžiui: darbuotojams, jų kompetencijai, pačiai organizacijai, rinkodarai. Nepaisant visų pastangų, kurias organizacijos skiria aplinkos bei vidaus problemoms nustatyti ir spręsti, jos nuolat susiduria su vis netikėtai iškylančiais išorės ar vidaus veiksniais. Smulkiausias neapdairus atvejis, sukeliantis riziką organizacijos veiklai, grasina jos reputacijai, gali sugriauti valdymo struktūras, sukelti didelių finansinių sunkumų ar netgi pavojų įmonės gyvavimui.

Tyrimo objektas - Veiklos tęstinumo ir atkūrimo po nenumatyto atvejo informacinėse sistemose planavimas ir palaikymas.

Darbo aktualumas: suformavus veiklos tęstinumo ir atkūrimo po nenumatyto atvejo informacinėse sistemose planą, galima įmonėje sutaupyti laiko, o tuo pačiu ir finansinių išteklių. Reikia atsižvelgti į organizacijos veiklos sritį, įmonės saugumui kylančius pavojus. Be šio plano organizacija rizikuoja, kad įvykus nenumatytam atvejui organizacijos veikla gali sutrikti ir būti neatkurta reikiamu laiku. Susistemintas veiklos tęstinumo ir atkūrimo valdymo planas palengvins vadovams nenutrūkstamai valdyti organizacijos veiklą. Numatant būsimas grėsmes darbuotojai imsis prevencinių veiksmų, o įvykus nelaimingam atsitikimui atkurs veiklą iki buvusios situacijos.

Darbo tikslai: išanalizuoti veiklos tęstinumo ir atkūrimo politiką ir plano žingsnius.

Darbo uždaviniai:

Išsiaiškinti informacinių sistemų sampratą;

Nustatyti grėsmes ir pažeidžiamumus galinčius pakenkti organizacijos veiklai;

Išnagrinėti veiklos tęstinumo ir atkūrimo valdymo etapus;

Pateikti, išanalizuoti ir palyginti su šia tema susijusius kelis pagrindinius tarptautinius standartus;

Išanalizuoti plano žingsnius, kaip užkirsti kelią pažeidžiamumams bei grėsmėms ir užtikrinti veiklos tęstinumą organizacijoje atsitikus nenumatytam atvejui.

Darbe naudota 2000-2007 metų literatūra: žiniatinklio informacija, projektuojant veiklos tęstinumo ir atkūrimo po nenumatyto atvejo planą, remtasi tarptautiniais saugumo standartais ir seminarų medžiaga.

Apžvelgiant literatūrą darbe naudojami struktūrinės analizės, sintezės, indukcijos, dedukcijos metodai. Aprašant ir analizuojant tarptautinius standartus taikyti aprašymo ir aiškinimo metodai. Taip pat naudojami vaizdiniai metodai lentelėms ir schemoms braižyti.

Darbas susideda iš šešių dalių.

Pirmoje dalyje pateikiama informacinių sistemų samprata. Čia kalbama kokią svarbią vietą jos užima organizacijoje. Atskleidžiama kokios pagrindinės dalys sudaro informacines sistemas, nes visi pateikti informacinių sistemų komponentai yra organizacijos turtas, kurį reikia saugoti.

Antroje dalyje – aptariami kokie egzistuoja nenumatyti atvejai, galintys pakenkti organizacijos veiklai. Pateikiama keletas pavyzdžių, kokie pagrindiniai veiksniai daro organizacijai žalą.

Trečioje dalyje – remiantis informacijos šaltiniais, ir išanalizavus informacijos saugumo valdymą pateikiama informacijos saugumo valdymo sistemos analizė.

Ketvirtoje dalyje apžvelgiami veiklos tęstinumo ir atkūrimo etapai.

Penktoje dalyje pateikiami su šia tema susiję pagrindiniai tarptautiniai standartai. Sudaryta šių standartų panašumų ir skirtumų lentelė.

Šeštoje dalyje pateikiamas susistemintas veiklos tęstinumo ir atkūrimo po nenumatyto atvejo informacinėse sistemose planas.

Magistro darbas gali būti naudingas organizacijos vadovams, darbuotojams, auditoriams.

1. INFORMACINĖS SISTEMOS SAMPRATA

Pastaraisiais metais labai išaugo informacinių technologijų svarba organizacijos veikloje. Todėl informacinės technologijos bei informacinės sistemos yra viena pagrindinių valdymo dalių organizacijoje. Reikia pastebėti, kad organizacijos informacinių sistemų problemos atsiranda tose vietose kur mažiausiai apsaugota informacinių sistemų infrastruktūra.

Informacinė sistema – tai prasmingą informaciją asmenims ir organizacijoms pateikianti ir kartu veikiančios aparatūros ir programinės įrangos, žmonių, procedūrų ir duomenų visuma. Šiuo metu vis daugiau informacijos yra automatizuojama, panaudojant kompiuterizuotas informacines sistemas.

Plačiąja prasme informacinės sistemos priima, saugo ir apdoroja duomenis, o rezultatus pateikia informacijos pavidalu. Informacinės sistemos atlieka keturias pagrindines funkcijas:

įvestis

Duomenų įvedimui dažniausiai naudojama klaviatūra ir pelė. Pats įvedimo procesas stebimas monitoriuje. Naudojama programinė įranga priklauso nuo organizacijos poreikių.

saugojimas

Informacinė sistema saugo ir atnaujina duomenis, informaciją ir programas. Žmonių dalyvavimas šioje fazėje yra minimalus. Jie nustato, kaip dažnai reikia daryti esamų duomenų kopijas, kada galima pašalinti senus duomenis iš sistemos.

apdorojimas

Apdorojimo fazės metu duomenys paverčiami informacija. Pagrindinį darbą atlieka kompiuteris, o žmogus tik koordinuoja jo veiklą, nurodydamas, kokias procedūras reikia atlikti. Dažniausiai naudojama techninė įranga yra centrinis procesorius ir pagrindinė atmintis.

išvestis (atgalinis ryšys)

Išvedimo procedūros pateikia vartotojui visą norimą informaciją, kuri gali būti skirta tiesioginiam panaudojimui arba tolimesniam saugojimui informacinėje sistemoje. Informacijos pateikimo forma priklauso nuo poreikių. Ji gali būti pateikta popieriuje, kompiuterio ekrane.

Informacinė sistema sudaroma kompiuterinės sistemos pagrindu. Todėl informacinę sistemą sudaro penki komponentai:

- kompiuterinė sistema;
- žmonės;
- procedūros;
- duomenys ir informacija;
- ryšio priemonės.

Kompiuterinė sistema – bet kuri įranga arba tarpusavyje sujungtų ar susijusių įrenginių grupė, kur vienas ar daugiau įrenginių atlieka automatinį duomenų apdorojimą pagal programą. Ši sistema, susideda bent iš pagrindinio procesoriaus, pagrindinės plokštės, standžiojo disko, maitinimo šaltinio ir korpuso,

Žmonės - tai svarbiausioji informacinės sistemos dalis. Nors šis faktas turėtų būti akivaizdus, tačiau jis dažnai nepakankamai vertinamas.

Žmonės kompiuterines sistemas valdo šiais būdais:

- kompiuterių profesionalai kuria techninę ir programinę kompiuterių įrangą;
- profesionalūs kompiuterių administratoriai prižiūri ir valdo kompiuterinių sistemų veiklą;
- kompiuterių vartotojai kiekvieną dieną įveda didžiulius kiekius duomenų, kurie vėliau bus apdorojami ir paverčiami informacija;
- vartotojai kuria savo specializuotą programinę įrangą;
- vartotojai analizuoja informaciją, gautą kompiuteriu, kad galėtų priimti efektyvius veiklos sprendimus;
- vartotojai ir kompiuterių profesionalai priima sprendimus, naudoja ir valdo kompiuterines sistemas, kurios gali turėti įtaką saugumui ir sėkmingam gyvenimui.

Procedūros - Informacinėje sistemoje yra vykdomos keturios pagrindinės procedūros:

- duomenų įvedimas;
- duomenų apdorojimas;
- informacijos išvedimas;
- informacijos saugojimas.

Įvesdami duomenis žmonės atlieka tokius veiksmus:

- surenka duomenis;
- nurodo kompiuteriui, kad jis pradėtų įvedimą;
- įveda duomenis į kompiuterį, kuris juos konvertuoja į jam tinkamą formą;
- prižiūri duomenų surinkimo ir įvedimo procesą.

Neautomatizuotas žmonių atliekamas procedūras dalinai "prižiūri" kompiuteris. Jis nurodo, ką, kada ir kaip daryti. Visi dokumentai, iš kurių vyko įvedimas, turi būti saugomi, kad būtų galima patikrinti, ar visi duomenys yra įvesti. Kompiuterizuotos procedūros yra reikalingos, norint:

- koordinuoti duomenų įvedimą ir apdorojimą sistemoje;
- tikrinti įvedamų duomenų teisingumą;
- saugoti duomenis kompiuterine forma;
- formuoti įvestų duomenų kontrolines ataskaitas.

Duomenys - tėra "žali", neįvertinti faktai. Kiekvieną dieną gaunami dideli kiekiai duomenų.

Informacija - gaunama surinkus duomenis ir juos prasmingai apdorojus. Kompiuteriai yra puiki priemonė duomenų įsisavinimui, rūšiavimui ir naudingos informacijos pateikimui. Kompiuterių skaičius pasaulyje sparčiai didėja. Kartu auga jų galimybės. Sunku net įsivaizduoti, kokių naujų programų bus sukurta netolimoje ateityje. [1]

Ryšio priemonės - Informacinėje visuomenėje strateginis resursas yra informacija. Informacijai perduoti kompleksiškai naudojama kompiuteriai ir kitos ryšio priemonės.

Visi išvardinti informacinės sistemos komponentai yra organizacijos turtas, kurį reikia saugoti.

Todėl informacinių sistemų tikslas – užtikrinti efektyvų informacijos panaudojimą organizacijoje, aprūpinti ją tikslia ir pilna informacija, užtikrinančia įmonės reikmes, priimant valdymo sprendimus. Galima išskirti keletą informacinių sistemų tipų.

1. Informacinė valdymo sistema;
2. Duomenų apdorojimo sistema.

Atsižvelgiant į tai, kad informacinė sistema yra neatsiejama nuo įmonės veiklos rezultatų ir informacinės sistemos dalys susijusios kaip vientisa masė, vienos dalies nebuvimas gali sugriauti visą sistemą. Todėl būtina imtis saugumo priemonių.

Saugumo priemonės – tai veiksmai, procedūros ar mechanizmai, kurie gali apsaugoti nuo grėsmių, sumažinti pažeidžiamumus, apriboti nepageidaujamų incidentų poveikį, aptikti nepageidaujamus incidentus ir palengvinti veiklos atkuriamą jiems įvykus. Efektyvus saugumas paprastai reikalauja derinti įvairias apsaugos priemones, kad būtų garantuota organizacijos turto apsauga.

Tinkamas turto valdymas yra labai svarbus organizacijos sėkmei.

Organizacijos turtą sudaro:

Fizinis turtas - kompiuterių įrengimai (procesoriai, monitoriai, nešiojami kompiuteriai, spausdintuvai, kopijavimo aparatai), ryšio įrengimai (maršrutizatoriai, fakso aparatai, auto atsakikliai, modemai, mobilūs telefonai), magnetinės ir optinės media priemonės (juostos, diskai, CD, DVD), kiti techniniai įrengimai (energijos tiekimo šaltiniai, oro kondicionieriai), baldai, patalpos;

Informacinis turtas - duomenų bazės ir duomenų failai, sutartys ir susitarimai, sistemų dokumentai, tyrimų informacija, naudotojų vadovai, apmokymų medžiaga, eksploatacijos ar pagalbinės procedūros, atsarginiai pasirengimai, archyvuota informacija;

Nematerialusis turtas – įvaizdis, reputacija;

Paslaugos - skaičiavimų ir ryšio paslaugos, bendrosios paslaugos, pvz. šildymas, apšvietimas, energija, oro kondicionavimas;

---

[1] Informatika. [interaktyvus]. Kaunas: KTU – [žiūrėta 2007m. kovo 15d] Prieiga per internetą <http://distance.ktu.lt/kursai/informatika1/1/teorija5.html>

Personalas (žmogiškieji ištekliai) –darbuotojai, jų kvalifikacijos, sugebėjimai ir patyrimas;

Programinės įrangos turtas - taikomoji programinė įranga, sisteminė programinė įranga, plėtros priemonės ir paslaugų programos.

Daugumai šio turto gali būti reikalinga tam tikra apsauga. Jei turtas nėra pakankamai apsaugotas / būtina įvertinti rizikos laipsnį.

Saugumo požiūriu neįmanoma įdiegti ir palaikyti sėkmingą saugumo programą, jei organizacijoje nėra nustatytas turtas. Daugelyje atveju turto nustatymo procesas gali pareikalauti daug laiko reikalaujančios analizės. Šios analizės detalumo laipsnis reiškiamas reikalingo laiko ir lėšų dydžiais, atsižvelgiant į turto reikšmingumą. Kiekvienu atveju detalumo laipsnis turi būti nustatomas saugumo tikslų pagrindu, tam reikia turtą grupuoti.

Turto apsaugą įtakoja ir jo pažeidžiamumas atskiru grėsmės atveju. Jei šie aspektai greitai pastebimi, juos reikia fiksuoti pirmiausiai.

Turtas yra įvairių rūšių grėsmių taikinys. Kad padaryti turtui žalą, grėsmė atsiranda silpniausioje, mažiausiai tikėtinoje situacijoje.

2. NENUMATYTI ATVEJAI

2.1. Grėsmės

Grėsmių sukėlėjai yra žmonės, žmonių grupės, gamtos reiškiniai, politiniai, ekonominiai ir socialiniai reiškiniai, galintys kelti grėsmę informacinių sistemų saugumui. Grėsmėje slypi galimybė sukelti nepageidaujamą incidentą, kuris gali padaryti žalą sistemai ar organizacijai bei jos turtui. Dažnai žala įvyksta dėl tiesioginės ar netiesioginės atakos informacinėse sistemose funkcionuojančios informacijos ar paslaugos atžvilgiu. Pavyzdžiui nelegalus informacijos sunaikinimas, atskleidimas, modifikavimas, sugadinimas, neprieinamumas ar praradimas.

Grėsmės šaltinis gali būti žmogus ar gamta, ji gali būti atsitiktinė arba sąmoninga. Tiek atsitiktinei tiek sąmoningai grėsmei turi būti nustatytas ir įvertintas jos rizikos laipsnis bei tikimybę. Nuo to priklausys kokio dydžio gali būti grėsmės sukelta žala.

Grėsmes galima suskirstyti pagal jas sukeliančius gamtos, technologinius, infrastruktūrinius ir žmogiškuosius veiksnius. Pagal grėsmių charakteristikas galima nusakyti apie pačią grėsmę ir nustatyti kokią žalą patirs organizacija. Kiekvienu atveju grėsmės sukelta žala gali būti įvairi. Tam įtakos turi,organizacijos reakcija. Kraštutiniais atvejais, kai kurios grėsmės yra nežalingos ir atvirkščiai gali sukelti katastrofą. Būtina atsižvelgti į išorinės, vidinės aplinkos bei kultūros faktorius.

Grėsmių tipai

1 lentelė

<table>
<tr><td>Loginės grėsmės</td><td colspan="2">Nesankcionuota prieiga prie informacinių sistemų;
Pavojingas programinės įrangos diegimas;
Apsimetimas kitu vartotoju.</td></tr>
<tr><td rowspan="2">Žmonių sukeltos grėsmės</td><td>Tyčinės</td><td>Atsitiktinės</td></tr>
<tr><td>Slaptas klausymasis
Informacijos pakeitimas
Įsilaužimas į sistemą
Piktavalė programa</td><td>Vartotojų klaidos
Programuotojų klaidos
Operatorių klaidos
Failų ištrynimas
Klaidingas kelias</td></tr>
<tr><td>Fizinės grėsmės</td><td colspan="2">Vagystė
Sukeltas gaisras
Stichinė nelaimė</td></tr>
</table>

1 lentelės tęsinys

Išorinės grėsmės	Netinkamai sudarytos sutartys su įrangos ar paslaugų tiekėjais Nesąžiningi įrangos ar paslaugų tiekėjų bei informacinių sistemų kūrėjų veiksmai Įsibrovimas iš išorės, pasinaudojus neapsaugotu bendrų resursų vartotojo vardu Fizinis priėjimas prie įrangos Virusai, loginės bombos Įsilaužimas per ryšį su globaliu tinklu (Internetu)
Gamtos sukeltos grėsmės	Žemės drebėjimas Žaibas Potvynis Ugnis
Techninės grėsmės	Įrangos techninis gedimas Infrastruktūrinis gedimas (elektros tiekimas, oro kondicionavimas) Išorės poveikių ir aplinkos veiksnių įtaka įrangos darbui Nesaugi įranga
Komunikacijos grėsmės	Įsiskverbimas į ryšio sesiją Ryšio sesijų perėmimas Ryšio sesijų nutraukimas

Visos įvykusios grėsmės sukelia vienokių ar kitokių nuostolių. Komercinėse organizacijose grėsmes dažniausiai sukelia tiesioginius trumpalaikius finansinius nuostolius arba netiesioginius ilgalaikius finansinius nuostoliu.

Galimų nuostolių pavyzdžiai:

- tiesioginis pinigų praradimas;
- tiesioginis aktų sulaužymas;
- reputacijos praradimas;
- pavojaus sukėlimas darbuotojams arba klientams
- pasitikėjimo praradimas;
- veiklos galimybių praradimas;
- veiklos rodiklių pablogėjimas;
- veiklos sutrikimas.

Siekiant sumažinti grėsmes reikia skirti dėmesį pažeidžiamumų minimizavimui.

2.2. Pažeidžiamumai

Pažeidžiamumas – tai organizacijos turto silpnosios vietos. Pažeidžiamumas yra informacinės vertybės netinkama apsauga nuo konkrečios grėsmės, tai grėsmės galimybė padaryti žalą. Kai jos sukėlėjas išnaudoja informacinės sistemos pažeidžiamumą, informacinei sistemai padaroma žala. Ji gali būti tiek materiali (sugadinamas turtas), tiek nemateriali (įvaizdžio praradimas, laiko praradimas).

Pažeidžiamumų nustatymo metu turi būti išaiškintos silpnosios vietos susijusios su:

- turto fizine aplinka;
- personalu, valdymo ir administracinėmis procedūromis bei kontrolės priemonėmis;
- technine, programine bei ryšių įranga ir infrastruktūra.

Pažeidžiamumus galima suskirstyti į grupes, pagal juos išnaudojančius sukėlėjus: gamtos, infrastruktūrinius, technologinius ir žmogiškuosius veiksnius.

Pažeidžiamumų pavyzdžiai:

- vartotojų žinių trūkumas;
- saugumo funkcionalumo trūkumas;
- slaptažodžių silpnumas;
- neišbandytos technologijos;
- duomenų perdavimas nesaugiais kanalais.

2.3. Poveikis

Poveikis yra nepageidaujamo incidento, sukelto tyčia ar atsitiktinai, nepageidaujama įtaka turtui. Tai gali būti kai kurio turto sunaikinimas, informacinės sistemos pažeidimas, slaptumo, vientisumo, prieinamumo, atsakingumo, tapatumo ar patikimumo praradimas. Galimi netiesioginiai poveikiai apima finansinius nuostolius, rinkos ar kompanijos įvaizdžio praradimą. Poveikio įvertinimas leidžia priimti tinkamus sprendimus kaip elgtis su nepageidaujamais ir tikėtinais, pasikartojančiais kelis kartus incidentais. Reikia atsižvelgti į nepageidaujamo incidento pasikartojimo dažnumą. Tai labai svarbu kai pavienio incidento žala yra nedidelė, bet per ilgą laikotarpį bendras efektas gali būti žalingas ir skaudus organizacijai. Poveikio įvertinimas yra svarbus rizikos įvertinimo ir apsaugos priemonių parinkimo elementas.

2.4. Rizika

Rizika yra galimybė, kad tam tikra grėsmė pasinaudos pažeidžiamumu tam, kad sunaikintų ar padarytų žalos turtui ir grupei turto, ir tiesiogiai arba netiesiogiai net pačiai organizacijai. Greitas aplinkos ar sistemos pokyčių pastebėjimas arba sužinojimas apie juos padidina tinkamų riziką mažinančių veiksmų galimybę.

Rizika lydi kiekvieną veiklos sritį ir gali padaryti tam tikros žalos. Iš tikrųjų rizikas sukeliančios grėsmės yra ir bus. Jos gali būti realios, arba tikimybė, kad tai įvyks, gali būti labai maža. Bet kuriuo atveju jos turės įtakos organizacijos veiklai ir nepriklausys nuo buvimo vietos, aplinkos.

Vis daugėja nusikaltėlių ir jie tobulėja, todėl organizacijoje labai svarbu yra rizikos, grėsmės, pažeidžiamumo nustatymas ir jų įvertinimas. Todėl būtina turėti pakankamai žinių ar bent supratimą apie galimas pasekmes bei poveikį organizacijos veiklai. Numatant incidentus, kurie gali sutrikdyti technologinius ir kitokius veiklos procesus, padaryti žalos įmonės turtui, darbuotojams, reikalinga iš anksto priimti reikiamus sprendimus. Pavojingiausius įvykius galim numatyti. Sudėtinga nuspėti kada atsitiks incidentas, gal apskritai tai neįvyks.

Tačiau kai kurių grėsmių neįmanoma net tik apibrėžti, bet ir nujausti, o grėsmės, kurios yra kaip dominuojančios, gali būti ir nerealios. Sunku atskirti pakankamai rimtas grėsmes nuo grėsmių, kylančių dėl augančio nusikalstamumo ar išorinių ir vidinių rizikos šaltinių.

Apsaugos specialistas turėtų padėti organizacijos vadovams numatyti saugos politiką ir ją įgyvendinti. Šiuo metu daugelio įmonių vadovai samdo ar perka saugos paslaugas net gerai nežinodami, ką ir nuo ko nori saugoti, kaip kas nors galėtų pakenkti įmonei, kada tai galėtų įvykti.

Norint, tai išsiaiškinti reikia suprasti šiuos etapus:

1. numatyti saugos politiką;
2. užtikrinti saugos kontrolę;
3. išanalizuoti ir įvertinti riziką;
4. suprojektuoti apsaugos sistemą (planą);
5. įdiegi sukurtą sistemą, planą;
6. kontroliuoti sistemos plano veikimą ir nuolat atnaujinti.

Šis procesas turi būti nuolatinis apimantis visą įmonę, o ne atskiras jos dalis.

Pirmiausia įmonių vadovai turi kartu išsiaiškinti, kurios grėsmės, pavojai, įvykiai padarytų daugiausia nuostolių. Visų atsakingų asmenų tikslas – žinoti, per kiek laiko galima būtų atnaujinti sutrikusią veiklą, ką reikia daryti, kokių priemonių imtis, kiek laiko užtruktų ir kiek tai kainuotų.

Dauguma įstaigų vadovų neturi supratimo kokių apsaugos priemonių reikia pakankamam saugumui užtikrinti. Daugelis sutrinka kai visos saugos bendrovės siūlo savo paslaugas, tvirtindamos, jog išspręs visas problemas. Vieni vadovai didesnį saugumą skiria vienai sričiai, kiti kitai. Tačiau tinkamam problemos sprendimui priimti reikalinga tiek vadovo, tiek savo paslaugas siūlančios organizacijos tarpusavio sutarimas ir su atitinkamos rašytinės procedūros.

Nustačius procedūras ar susidarius planą, prevencijai prieš nenumatytus atvejus, jų laikymasis gali užtikrinti organizacijos saugumą. Daug problemų gali būti išsprendžiama organizacinėmis priemonėmis – jas taikant galima išvengti darbuotojų klaidų, vagysčių, sukčiavimų ar piktnaudžiavimo įrenginiais.

Norint apsaugoti organizaciją nuo grėsmių, išvengti nepageidaujamų pasekmių bei rizikos bet kurioje srityje, būtina gerai žinoti informacijos saugumo valdymo sistemą.

3. INFORMACIJOS SAUGUMO VALDYMO SISTEMA

Informacijos saugumo valdymo sistema – programinių, techninių, organizacinių, etinių ir moralinių priemonių visuma, kuri kuriama atsižvelgiant į teisines normas reglamentuojančias informacijos apsaugą. Pagrindinis informacijos saugumo valdymo sistemos kūrimo tikslas – saugoti informaciją, kuria disponuoja organizacija, kiek įmanoma sumažinti riziką prarasti šią informaciją ir dėl to atsirasiančius nuostolius.

Įmonių informacijos saugos pagrindas – patikima informacijos saugumo valdymo sistema, apimanti tiek organizacinę (saugumo dokumentus, politiką, procedūras, tvarką), tiek technologinę (programines priemones ir įrangą, kuria realizuojami sprendimai) dalį. Šiai sistemai prižiūrėti būtina pasitelkti geriausius savo srities profesionalus, nes tik tada sistema garantuos visus svarbiausius įmonės informacijos saugumo aspektus – konfidencialumą, prieinamumą ir vientisumą.

Pasaulyje įprasta praktika, kad įmonių informacijos saugumo valdymo sistemas prižiūri trys specialistai: už informacinių technologijų saugos organizavimą atsakingas vadovas, saugos administratorius ir informacinių technologijų saugos auditorius. Šias funkcijas su mūsų specialistų pagalba gali atlikti patys įmonės darbuotojai arba profesionalai, turintys ilgametę informacinių technologijų saugumo priežiūros (ugniasienių administravimas, pranešimų žurnalų stebėjimas, incidentų fiksavimas), informacinių technologijų audito bei informacijos saugą reglamentuojančių dokumentų rengimo ir koordinavimo patirtį.

Norint sukurti gerą informacijos saugumo valdymo sistemą, būtina gerai žinoti galimas grėsmių sukeliamas rizikas ir iš to spręsti kokiomis priemonėmis bus saugomasi.

Informacijos saugumo valdymo sistema yra priemonė, kurios pagalba aukštesnioji administracija tikrina ir valdo saugumą, minimizuodama veiklos riziką ir užtikrina, kad saugumas ir toliau vykdys įmonės, kliento ir teisinius reikalavimus.

Pagrindiniai informacijos saugumo valdymo sistemos komponentai yra PLANUOK – DARYK- TIKRINK – VEIK (1 schema). Darbai nuolat sukasi ratu tai atspindi Deming‘o ciklas[2].

1 schema. Informacijos saugumo valdymo sistema

Planuok. Pakeitimų planavimas. Analizuojami ir numatomi rezultatai. Šis etapas apima veiklos apimtį, saugumo politiką, rizikos įvertinimą, rizikos valdymo planus, tinkamumo patvirtinimą.

Daryk. Planų vykdymas, kontroliuojant aplinkybes. Šiame etape įvardijama kontrolės priemonės, personalo mokymų ir išteklių valdymo svarba.

Tikrink. Rezultatų tikrinimas. Dažniausiai tikrinimus atlieka vidiniai auditoriai arba vadovybė.

Veik. Veiksmų procesų tobulinimui arba standartizavimui. Tai informacijos saugumo valdymo tobulinimas, prevenciniai veiksmai, koregavimo veiksmai, incidentų aptikimas ir reagavimas į juos.

Šis modelis naudojamas tada kai:

- norima gerinti veiklos procesus, sekti nenutrūkstamos veiklos procesus;
- pradedami naujo tobulinimo, vystymo projektai;
- kai planuojami nauji arba tobulinami esamus procesai, produktų ir paslaugų planai;
- nustatomi pasikartojantys darbo procesai;
- planuojamas duomenų kaupimas, analizuojamos problemos bei priežastys;
- įgyvendinami įvairūs pakeitimai.

[2] Project Planning and Implementing Tools. [interaktyvus], [žiūrėta 2007m. kovo 15d] Prieiga per internetą <http://www.asq.org/learn-about-quality/project-planning-tools/overview/pdca-cycle.html>

Deming‘ o rato etapai nuosekliai eina vienas paskui kitą, tai pastoviai pasikartojantys veiksmai. Pateikiamas išsamesnis Deming‘o ratas (2 schema).[3]

2 schema. Išsamesnė informacijos saugumo valdymo sistema

Planuok

Planavimo procese personalas įsigilina į galimybių ir plano pasikeitimus. Reikia nustatyti organizacijos tikslus ir užduotis bei nustatyti metodus ir kaip tuos tikslus įgyvendinti. Tam reikalinga išsianalizuoti visus šios dalies veiksmus:

1. Apimtis

Pirmas žingsnis yra nustatyti informacijos saugumo valdymo sistemos apimtį. Ji gali apimti visą organizaciją arba tam tikrą vietą bei tam tikrą paslaugą – pavyzdžiui, Internetinę bankininkystę.

2. Informacijos saugumo valdymo sistemos politika

Kodėl yra svarbus informacijos saugumas?

Ar yra konkreti grėsmė ar kiti rūpesčiai, keliantys nerimą?

Ar yra kokių apribojimų, tokių kaip įstatymai ir taisyklės, ar tam tikri būdai, kuriais norima tvarkyti reikalus?

Reikia dokumentuoti visus atsakymus politikos dokumente. Tai turėtų būti santykinai trumpas dokumentas (1-3 puslapiai) ir pasirašytas vadovaujančio darbuotojo. Saugumas, kaip ir visos kitos vidinės kontrolės priemonės tvirtinamos aukščiausiame organizacijos lygmenyje.

3. Rizikos įvertinimas

---

[3] PDCA - the deming cycle. [interaktyvus], [žiūrėta 2007m. kovo 15d] Prieiga per internetą <http://www.ifm.eng.cam.ac.uk/dstools/process/pdca.html>

Kada žinoma, ką reikia apsaugoti ir koks yra priimtinas rizikos lygis, kokia yra faktinė rizika pasirenkamas organizacijai tinkamas metodas ir informacijos saugos valdymo sistemos apimtis. Kokia yra rizika? Tai nustatoma įvertinant poveikius, kurie galėtų kilti, jei kažkokia grėsme pasinaudotų gynybos silpnybėmis, ir pastatytų į pavojų turto saugumą, bei kiek tikėtina, kad tai gali įvykti.

Planuojant poveikio kilimo tikimybę palyginti su poveikio reikšmingumu, reikėtų įvertinti, kad yra tokios rizikos, dėl kurių nereikia labai jaudintis, nes:

- net jei ji turėtų didelį poveikį - yra ypatingai neįtikėtina,
- arba, jei ji kiltų nuolat - turėtų nereikšmingą poveikį.

4. Rizikos valdymas

Užbaigus rizikos įvertinimą, saugumo standartai siūlo, kad būtų nuspręsta, kaip tą riziką valdyti. Nauja tarptautinio saugumo standarto ISO 17799 versija (ISO 27000), kalba apie elgesį su rizika. Ar tiesiog priimti riziką ir pasikliauti savo sugebėjimu greitai nustatyti ir reaguoti į saugumo incidentus? Ar vengti rizikos, perkelti ją trečiajai pusei (pvz., per draudimą), ar taikyti atitinkamus valdymo svertus? Tai yra elgesio su rizika planas.

5. Tinkamumo Patvirtinimas

Reikia nustatyti visas pasirinktas saugumo kontrolės priemones ir pagrįsti, kodėl jos yra tinkamos, ir parodyti kodėl valdymo priemonės, kurios nebuvo pasirinktos, yra nesvarbios. Reikia susieti valdymo priemonių pasirinkimą su rizikos įvertinimu. Praktiškai, galima susieti valdymo priemonių pasirinkimą su informacijos saugumo valdymo sistemos politikos pareiškimais.

Daryk

Tikrinami pokyčiai. Kaupiami tyrinėjimų rezultatai. Personalo švietimas ir apmokymas.

Daryk ciklo dalis reikalauja, kad būtų įdiegta reikiami priežiūros metodai. Tam reikia procedūros, kuri užtikrintų greitą incidentų aptikimą ir reagavimą į juos. Reikia užtikrinti, kad visi darbuotojai, suprastų saugumą ir būtų tinkamai apmokyti ir kompetentingi įgyvendinti atliekamas saugumo užduotis.

Tikrink

Tikrinimo procese atliekamas testavimas, rezultatų analizė, nustatoma ką personalas išmoko.

Tikrink fazės paskirtis yra užtikrinti, kad būtų kontrolės metodai ir būtų pasiekiami tikslai. Yra daug įvairių galimų tikrinimo veiksmų, tačiau tik vidinė informacijos saugumo valdymo sistema ir vadovybės patikrinimai yra privalomieji ir laisvai pasirenkami reikalavimai:

- įsibrovimo nustatymas;
- incidentų valdymas;
- einamieji patikrinimai;
- savikontrolės procedūros;
- mokymasis iš kitų;

- vidinis informacijos saugumo valdymo sistemos auditas;
- valdymo patikrinimas.

Veik

Reikia imtis veiksmų remiantis tuo ką išmokai „tikrink“ etapo metu. Jei tikslai nepasiekti reikia kartoti ciklą iš naujo naudojant kitą planą. Jei viskas buvo sėkminga panaudoti tai kas išmokta ankščiau didesniuose pokyčiuose. Naudoti tai kas išmokta planuojamuose naujuose patobulinimuose pradedant ciklą iš naujo.

Veik procese yra tikrink veiklos rezultatas. Yra trys veiksmų rūšys:

- koregavimo veiksmai,
- krevencinei veiksmai,
- tobulinimas.

Organizacijoje naudojančioje Deming‘o rato privalumai:

- atskirų žmonių ir grupių kasdieninis valdymas;
- problemų spendimų procesai;
- projektų valdymas;
- nenutrūkstamas valdymas;
- projektavimas;
- žmogiškųjų išteklių plėtimas;
- naujų projektų diegimas;
- procesų išbandymas.

Tačiau informacijos saugumo valdymo sistemos nepakanka užtikrinti organizacijos veiklos pilną saugumą ir gerą valdymą. Vis dažniau sutinkamos įvairios nenumatytos situacijos informacinių technologijų sferoje. Tam reikalingas nuoseklus procesų planas, kuris būtų naudojamas nuo veiklos gyvavimo pradžios iki pabaigos. Norint užtikrinti veiklos ciklus ir vykdymą, reikia susidaryti veiklos tęstinumo ir atkūrimo planą.

Daug organizacijų vadovų nežino, jog jiems reikalingas planas, kuris užtikrins organizacijos valdymą ir išgyvenimą. Nemažai gyvuoja organizacijų, kurių vadovai nenori investuoti į veiklos ciklo analizės planus manydami, kad nelaimė aplenks jų organizaciją. Kol kas veiklos tęstinumo ir atkūrimo planas organizacijose mažai naudojamas, tačiau jis yra labai svarbus veiklos valdymui. Veiklos tęstinumo valdymas bei veiklos procesų atkūrimas yra būtinas, kad organizacija išgyventų. Be to veiklos tęstinumo ir atkūrimo planas jau nebe prabanga, bet esminis organizacijos rizikos valdymo programos elementas, nes netikėtos situacijos informacinėse sistemose nėra išimtys, jos sutinkamos vis dažniau.

4. VEIKLOS TĘSTINUMO IR ATKŪRIMO PO NENUMATYTO ATVEJO VALDYMAS

4.1. Veiklos tęstinumo svarba

Kodėl organizacijos vadovai nesirengia blogiausiam scenarijui? Galbūt, organizacijos vadovai dažnai tiki, kad bet kokia bėda juos aplenks. Jei organizacija pakankamai didelė, vadinasi ji ir „stipri“, su kliūtimis susidoros, juk tai visada pavyksta. Yra manoma, kad smulkūs pažeidimai didelės kompanijos nepaveikia, kam saugotis nuo to, kas neįvyks. Kompanijos vadovai nesidomi teroristais, o dar lengviau vadovauti žinant, kad visus nuostolius padengs draudimas. Tačiau nereikėtų tuo pasikliauti. Geriau jau nuo įmonės įkūrimo pradžios būti užtikrintu įmonės veiklos tęstinumu.

Veiklos tęstinumo vadyba reikalinga, kad organizacija tęstų veiklą duomenų praradimo, kritinių sistemų gedimo bei kitų informacinių technologijų veiklą nutraukiančių nelaimingų atvejų metu.

Veiklos tęstinumo vadyba – tai rizikos valdymo proceso dalis, skirta užtikrinti, kad bet kokiomis aplinkybėmis organizacija sugebės vykdyti veiklą bent jau nustatytu minimumu. Vykstant pokyčiams kiekviename veiklos tęstinumo procese turi būti numatyti, identifikuoti, sukontroliuoti, sumažinti ar net pašalinti rizikingi ar kritiniai veiklos atvejai.

Į besiplečiančių ir bręstančių organizacijų sėkmės veiksmų sąrašą galima įrašyti ir veiklos tęstinumo rizikos valdymo sistemą. Galbūt šiandieną įvairios įmonės turi vienokias ar kitokias veiklos tęstinumo rizikos valdymo sistemos apsaugos dalis, įdiegtas apsaugos priemones, bet jos mažai suderintos tarpusavyje, todėl gali patirti nenumatytų nesėkmių.

Veiklos tęstinumo rizikos valdymas tiesiogiai veikia organizacijos turtą. Organizacijų veiklos rezultatai priklauso nuo turto naudojimo ir valdymo metodų bei įrankių.

Pažeidus turto slaptumą, vientisumą, tapatumą, pajuntama žala organizacijos veiklai ir jos rezultatams. Kiekvienam vadovui svarbu apsaugoti turtą ir garantuoti, kad organizacija veiktų esant priimtam rizikos lygiui.

Veiklos tęstinumo rizikos valdymą sudaro šie elementai:

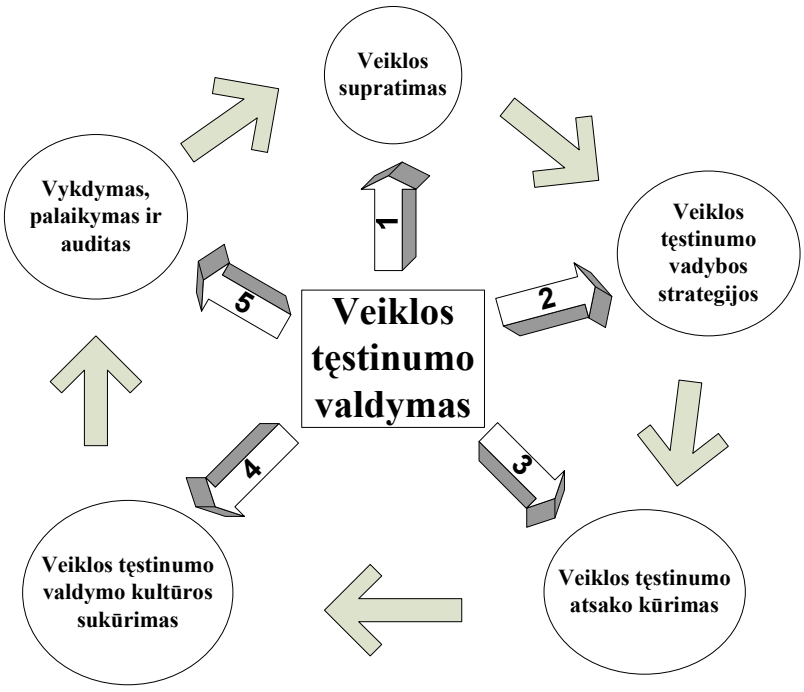
- turtas ir jo reikšmė organizacijai (turtas ir žala jo netekus);
- grėsmė (potenciali nepageidaujamų įvykių, galinčių padaryti žalą organizacijai, galimybė);
- pažeidžiamumas (silpnosios turto pusės, kuriomis gali pasinaudoti grėsmė);
- rizika (potenciali galimybė, kad konkreti grėsmė pasinaudos turto grupės pažeidžiamumu ir sunaikins ar sugadins turtą);
- apsaugos priemonės (praktinės priemonės, procedūros ar mechanizmai mažinantys riziką).

Veiklos tęstinumo rizikos valdymo sistemos įgyvendinimas apima šias sritis:

- organizacijos saugumo tikslų, strategijos ir politikos nustatymas;
- organizacijos saugumo reikalavimų nustatymas turtui;
- grėsmių turto saugumui organizacijos viduje nustatymas ir analizė;
- rizikos nustatymas ir analizė;
- atitinkamų apsaugos priemonių pritaikymas;
- priemonių, efektyviai apsaugančių turtą organizacijos viduje, įdiegimo ir naudojimo priežiūra;
- saugumo įsisąmoninimo programos plėtra ir diegimas;
- incidentų atskleidimas ir reakcija į juos.

4.1.1. Veiklos tęstinumo rizikos valdymo sistemos modelis

Veiklos tęstinumas organizacijoje priklauso nuo daug faktorių, kuriuos atskleidžia rizikos valdymo gyvavimo ciklo sistema (3 schema).



3 schema. Veiklos tęstinumo valdymo gyvavimo ciklas[4]

Schemoje matoma, kad veiklos tęstinumo valdymo gyvavimo ciklas apima penkis etapus:

[4] Procesų valdymo sistemos. [interaktyvus]. Vilnius: Entering Lithuanian market - 2007. [žiūrėta 2007m. gegužės 5 d] Prieiga per internetą <http:/www.elm.lt/lt/vadybos_konultacijos/rizikos_valdymo_p.php>

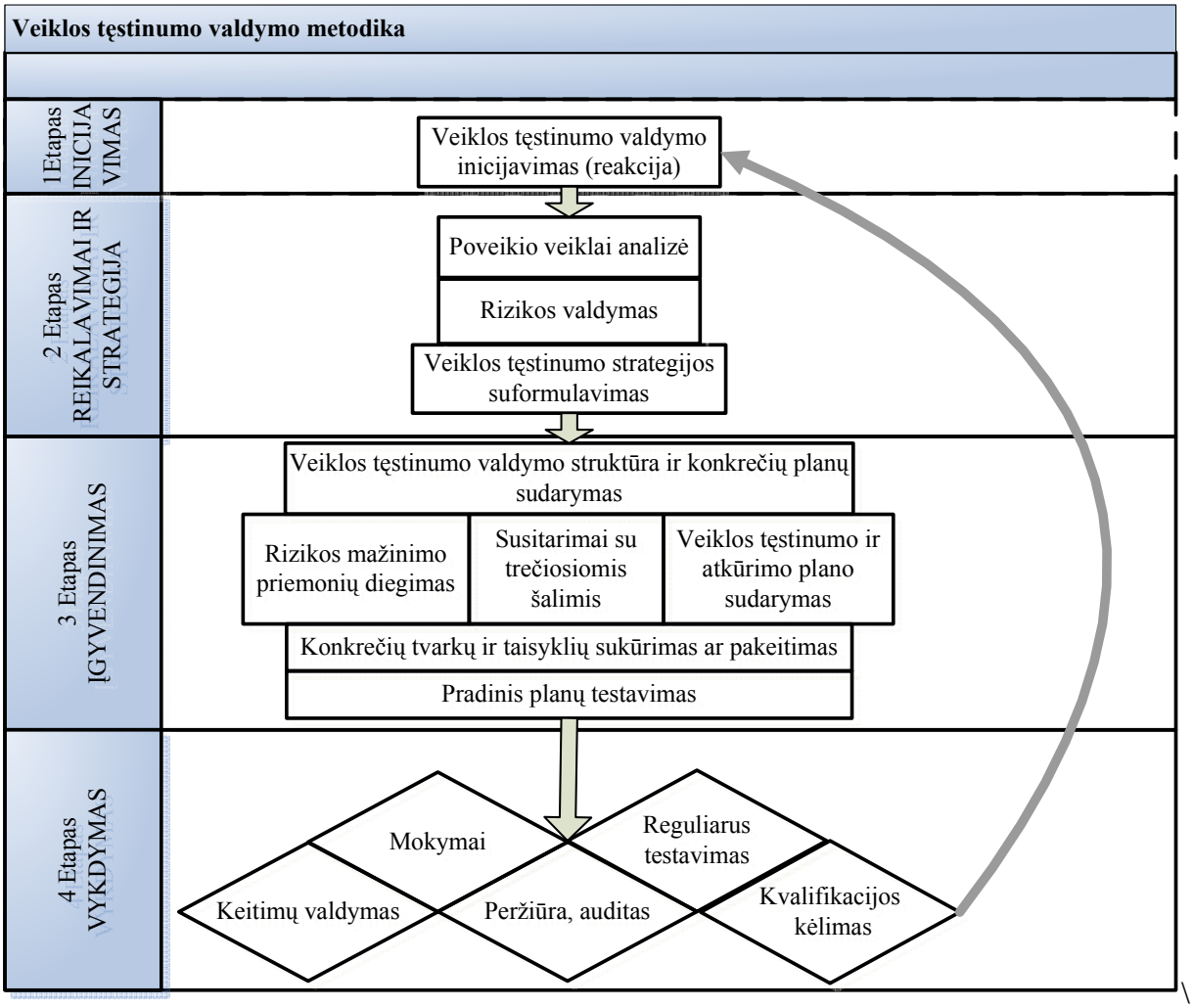
1. Veiklos supratimas - organizacinė strategija, veiklos poveikio analizė, rizikos įvertinimas ir kontrolė.
2. Veiklos tęstinumo vadybos strategijos - organizacijos veiklos tęstinumo plano strategija, išteklių atkūrimo veiklos tęstinumo plano strategija.
3. Veiklos tęstinumo atsako kūrimas - krizių valdymas, viešieji ryšiai, visuomenės informavimo priemonės, veiklos tęstinumo planai, veiklos planai, incidentų atsakas.
4. Veiklos tęstinumo valdymo kultūros sukūrimas - įvertinimas, projektavimas ir įvykdymas, rezultatų įvertinimas.
5. Vykdymas, palaikymas ir auditas - vykdyti veiklos tęstinumo planus, jų testavimas ir palaikymas, auditas.

4.1.2. Veiklos tęstinumo rizikos valdymo sistemos nauda

Veiklos tęstinumo rizikos valdymo sistemos įgyvendinimas gali padėti:

- užtikrinti suinteresuotų šalių lūkesčius įgyvendinant strateginius tikslus;
- identifikuoti turtą ir jo reikšmę organizacijoje;
- nustatyti veiklos tęstinumui gresiančias rizikas, organizacijos trūkumus ir jų reikšmingumo laipsnį (įvertinant grėsmes, pažeidžiamumus);
- užsibrėžti norimą ir nustatyti turimą apsaugos priemonių lygį;
- racionaliai panaudoti apsaugos priemonėms skirtus išteklius;
- padidinti darbuotojų saugumą ir pasitenkinimą;
- operatyviai reaguoti į incidentus garantuojant veiklos tęstinumą;
- greičiau prisitaikyti prie greitai besikeičiančios aplinkos, turinčios įtaką veiklos tęstinumui.

Veiklos tęstinumo valdymo gyvavimo ciklas organizacijoje atsispindi veiklos tęstinumo veiklos metodikos etapuose (4 schema).



4 schema. Veiklos tęstinumo metodikos etapai

1 Etapas. Inicijavimas

Pirmiausia reikia gauti vadovybės įsipareigojimą.

Šiame etape turi dalyvauti vadovybė, jos parama ir dalyvavimas labai svarbus. Vadovybė privalo:

- užtikrinti, kad nebūtų neatitikimo tarp veiklos ir informacinių technologijų strategijų;
- užtikrinti reikiamus įgaliojimus ir finansavimus;
- užtikrinti bendradarbiavimą tarp padalinių;
- didinti visų darbuotojų suvokimą apie veiklos tęstinumo ir atkūrimo svarbą.

Antra, surinkti medžiagą planui pagrįsti.

Surinkti visi istoriniai dokumentai padeda įtikinti vadovus pritarti veiklos tęstinumo plėtojimui. Visi informaciniai leidiniai, naujienos padės suvokti ir aptarti veiklos tęstinumo planus ir kaip kompanija veikia jei ji neturi tokio plano. Turint informaciją galima problemą iliustruoti, vadovams

grafiškai parodyti koks laukia rezultatas nesėkmės atveju. Toks paaiškinimas padės vadovams suprasti kylančią problemą ir parems veiklos tęstinumo palaikymą.

Trečia, nustatyti tikslus bei siekius.

Veiklos tęstinumo reikalavimai susideda iš šių dalių:

- sumažinti veiklos kliūtis;
- imtis svarbiausių procesų (veiksmų plano);
- sumažinti per numatytą laiką finansinius nuostolius;
- išlaikyti teigiamą įvaizdį krizės metu ir po jos.

Ketvirta, paskirti asmenį atsakingą už veiklos tęstinumo planą.

Kol kuriama ar renkama žmonių grupė veiklos tęstinumo plano procesams vykdyti, reikalingas vienas žmogus, kuris tuo metu bus atsakingas už procesų vykdymą. Šis asmuo vadinamas veiklos tęstinumo plano vadovas. Vadovas atsakingas už šiuos uždavinius:

- nustato tikslus, politiką ir kritinius sėkmės faktorius;
- derina, organizuoja, ir prižiūri veiklos tęstinumo plano projektą;
- supažindina vadovus bei personalą, su projektu;
- apskaičiuoja ir pateikia planą kiek kiekvienam užduoties etapui reikia skirti finansų;
- apibūdina ir rekomenduoja projekto struktūrą ir valdymą;
- valdo procesą;
- kontroliuoja plano įgyvendinimą;
- planuoja, apmoko kaip įgyvendinti planą;
- periodiškai prižiūri, tikrina plano procesus.

Penkta, sudaryti veiklos tęstinumo plano darbo grupes.

Kuriant veiklos tęstinumo planą verta sudaryti veiksmų planą ir veiklos tęstinumo darbo grupes siekiant koordinuoti veiklas susijusias su plano kūrimu. Visos susijusios organizacijos sritys turi būti atstovaujamos žmogaus išmanančio tos srities veiklos procesą.

Veiklos tęstinumo plano vadovas paskirsto personalą į grupes, kurios atsakingos už tam tikrų užduočių vykdymą. Tipinės grupės ir pareigos gali būti šios:

- tęstinumo plano koordinatorius – valdo procesus ir derina su įvairiomis grupėmis;
- vyresniųjų vadovų grupė – tvirtina planus, paskirsto biudžetą, nustato lūkesčius;
- žmogiškųjų išteklių grupė – nusamdo laikiną personalą jei reikalinga verslui palaikyti;
- visuomenės informavimo priemonių, žiniasklaidos ryšių grupė – bendrauja su žiniasklaida dėl nelaimės poveikio.
- juridinė grupė – tvarko teisinius ir draudiminius klausimus ir pasekmes iškilusias dėl nelaimės.

- informacinių technologijų saugumo grupė – ši grupė atsakinga už visą informacinių technologijų saugumą prieš, per ir po nelaimingo atvejo. Ši grupė sutelkta užtikrinti saugų duomenų slaptumą, duomenų vientisumą, duomenų naudingumą ir palaikymą visuose procesuose;
- fizinio saugumo grupė – atsakinga už fizinio turto saugumą, bendrauja su avarinių tarnybų personalu nelaimės metu.
- pastatų valdymo grupė – atsakinga už pastatų darbą ir priežiūra, krizės metu.
- avarijos likvidavimo grupė – reaguoja į nelaimę, įgyvendindami tęstinumo ir atkūrimo po nenumatyto atvejo planus.
- gedimų, žalos įvertinimo grupė – atsakinga už nelaimės sukelto nuostolio įvertinimą.
- išorinės saugyklos grupė – saugo, palaiko organizacijos dokumentus, el. įrašus.
- pakaitinės vietos grupė – atsakinga už būtinos kompiuterinės ir programinės įrangos atstatymą.
- veiklos atkūrimo grupė – atsakinga už nelaimės metu sugadintų sistemų taisymą.

Šešta - kainodara

Veiklos tęstinumo ir atkūrimo planavimas yra kaip draudimas, jis yra būtinas, bet tikimasi, kad nereikės juo pasinaudoti. Kainodara yra sudedamoji plano dalis. Veiklos tęstinumo ir atkūrimo planas gali būti, bet daug kur ir yra labai brangus sukurti ir brangus palaikyti. Dėl to reikia įvertinti ir pradinius ir einamuosius kaštus.

2 Etapas. Reikalavimai ir strategija

Šiame etape analizuojama poveikio veiklai analizė, rizikos valdymas ir veiklos tęstinumo strategijos suformulavimas.

Poveikio veiklai analizė

Poveikio veiklai analizė leidžia įvertinti, kiek organizacijos veikla yra priklausoma nuo informaciją apdorojančių sistemų, taip pat kurios iš šių sistemų yra svarbiausios, o kurios mažiau svarbios.

1. Projekto planavimas.

Reikia gauti aukščiausio lygio vadovo palaikymą, surinkti projekto komandą, nustatyti tikslus kartu su aukštesniąją vadovybe, nustatyti įvykdymo grafiką ir pristatyti projektą dalyviams.

2. Duomenų rinkimas.

Reikia pasirinkti duomenų surinkimo metodus ar tai klausimynai, ar interviu, ar grupiniai susitikimai. Nustatyti surinkimo kriterijus, surinkti informaciją, ją įvertinti, patikrinti. Ir sutikrinti informaciją su grupės dalyviais. Visą informaciją reikia surašyti.

3. Duomenų analizė.

Kai duomenys yra surinkti juos reikia peržiūrėti ir analizuoti. Tikslas – įvertinti poveikį

kaštams ir kitus poveikius to kad nebus atliekamos tam tikrą laiką tam tikros funkcijos; nustatyti kritines funkcijas ir nuo kokių duomenų bei programų jos priklauso; nustatyti skirtingas sistemas ir sukurti atstatymo laiko tikslą kiekvienai kritinei funkcijai.

4. Išvadų surašymas (įforminimas).

Reikia sukurti santrauką aukščiausiai vadovybei atkūrimo prioritetų rekomendacijas, grafikus brėžinius ir kitas vizualines priemones.

5. Išvadų pateikimas.

Pristatyti raštu ir žodžiu išvadas, ataskaitas vyresniajai vadovybei. Reikia būti pasiruošus apginti veiklos poveikio analizės procesą bei rekomendacijas kokios pasirinktos, nurodant žingsnius planavimo procese. Tada vadovybė šią informaciją panaudos prioritizuojant saugotinus išteklius ir nukreips nepakankamus resursus efektyviausiu būdu.

Rezultatai

Reikalinga dokumentuota ir pagrindžiama informacija apie tai, kiek įmonės veiklos funkcijos yra priklausomos nuo informacinių sistemų. Dokumentuojama, kokios informacinės sistemos yra labiausiai kritiškos.

Veiklos vadovams ši informacija leis efektyviau panaudoti ir pagrįsti investicijas, skiriant daugiau lėšų kritiškoms sistemoms.

Poveikio veiklai analizė padeda išversti techninę informacinių sistemų poreikių kalbą į veiklos vadovų kalbą, kuri daugiau orientuota į veiklos procesus ir jų rizikas. Tai leidžia pagrįsti informacinių sistemų poreikius, nustatyti ir patvirtinti sistemų reikšmingumo lygius.

Įgyvendinimas

Informacija surenkama interviu su informacinių sistemų naudotojais metu. Jais gali būti veiklos padalinių vadovai arba kiti patyrę darbuotojai.

Visa interviu metu surinkta medžiaga dokumentuojama naudojant patikrintą ir efektyvią metodiką, kuri leidžia lengvai atnaujinti analizės rezultatus kitais metais.

Remiantis poveikio veiklai analizės rezultatais, priimami sprendimai, kokioms sistemoms reikalinga detali rizikos analizė, kokie informacijos saugumo aspektai yra labiausiai kritiški tam tikrai sistemai.

Parengiama ataskaita, kurioje pateikiami informacinių sistemų svarbumo įvertinimai, interviu metu surinkti duomenys, svarbiausių rezultatų santrauka.[5]

[5] Rizikos vertinimas. [interaktyvus]. Vilnius: UAB Informacijos saugos sprendimai. [žiūrėta balandžio 3d.] Prieiga per internetą <http://www.isec.lt/pdf/riziku_vertinimas.pdf>

Rizikos valdymas

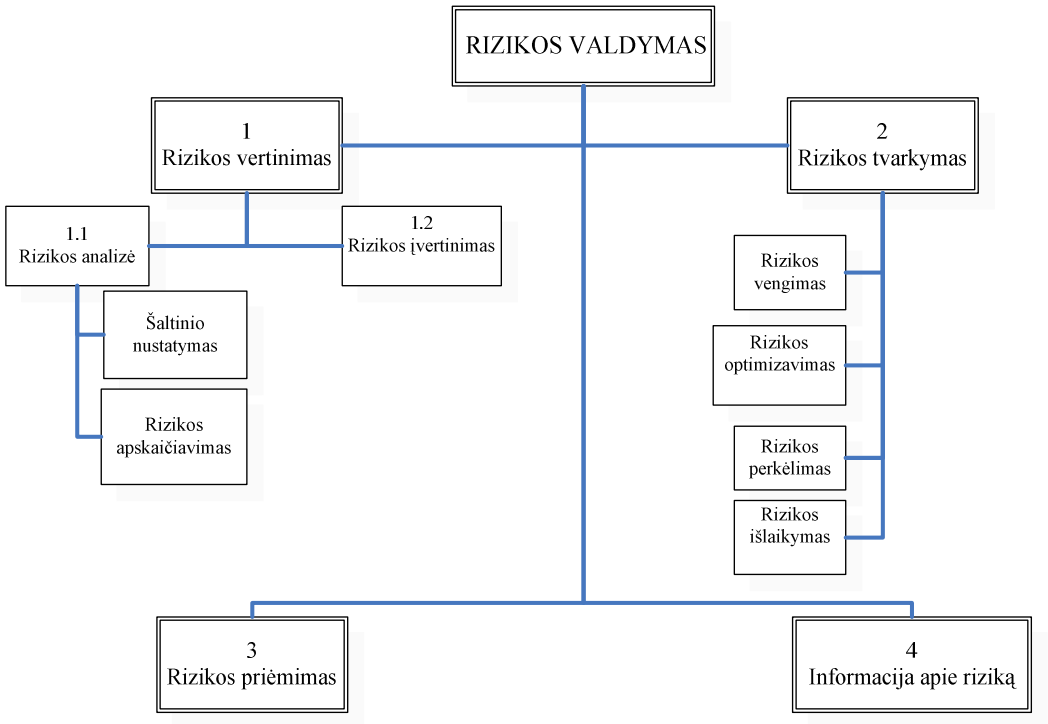
Rizika – tai galinčio įvykti nelaimingo atsitikimo tikimybė ir jos galimas poveikis organizacijai.

Rizikos valdymo veiksmai būna efektyviausi, jeigu jie atliekami per visą sistemos gyvavimą. Rizikos valdymo procesas pats savaime yra didelis veiksmų ciklas (5 schema).

Reikia pastebėti, kad apsaugos priemonės taip pat gali turėti pažeidžiamumų ir dėl to gali atsirasti naujų rizikų. Todėl pasirenkant atitinkamas apsaugos priemones reikia rūpintis ne tik rizikos sumažinimo, bet taip pat tuo, kad neatsirastų potencialios naujos rizikos.

Rizikos valdymo ir rizikos analizės procesai gali atrodyti identiški, tačiau būtina suprasti jų skirtumus ir bendrumus.

Rizikos valdymo tikslas sumažinti riziką iki priimtino lygio, tuo tarpu rizikos analizė atliekama tam, kad jos rezultatai būtų panaudoti ir jų veiksmingumui įvertinti.



5 schema. Rizikos valdymas

Rizikos valdymas – koordinuoti veiksmai, kuriais siekiama valdyti ir kontroliuoti organizacijos rizikas.

Rizikos valdymo tikslas yra gerinti projekto veikimą, sistemiškai identifikuojant, vertinant ir valdant su projektu susijusią riziką. Kadangi rizikos valdymas nėra tik neigiamų padarinių vengimo procesas, rizikos valdymą reikia traktuoti kaip projekto planavimo proceso dalį, nes esminiai aspektai gali būti stipriai įtakojami.

Rizikos valdymas apima:

- rizikos vertinimą;
- rizikos tvarkymą;
- rizikos priėmimą;
- informavimą apie riziką.

Kaip organizacijose vertinama informacinių sistemų rizika?

Rizika pagal pasirinktą metodiką turėtų būti vertinama periodiškai. Ji turėtų apimti:

- informacinių sistemų turto įvertinimą, informacinių sistemų pažeidžiamumų nustatymą ir informacinių sistemų grėsmių bei jų tikimybės įvertinimą,
- galimos grėsmės poveikio nustatymą,
- kontrolės nustatymą, siekiant apsisaugoti nuo įvardintų grėsmių poveikio,
- rizikos vertinimą ir apsidraudimą nuo jos.

Rizikos vertinimas – tai bendras rizikos analizės ir rizikos įvertinimo procesas.

Rizikos vertinimo apimtis ir gylis skirtingose organizacijose skiriasi. Tai priklauso nuo organizacijos veiklos, informacinių vertybių, patirties informacijos saugos organizavimo srityje bei finansinių galimybių. Norint pasiekti optimalių rezultatų, reikia atsižvelgti į konkrečios organizacijos poreikius ir situaciją.

Be vadovybės paramos ir palaikymo, rizikos valdymas nebus veiksmingas. Organizacija gali įvertinti riziką remdamasi jos reikšmingumu veiklai.

Proceso sėkmingumui esminę reikšmę turi aiškus vaidmenų ir atsakomybės apibrėžimas. Veiklos procesų valdytojai atsako už rizikos poveikio nustatymą. Kiti svarbiausi sėkmės veiksniai yra:

- tinkamai sudarytas rizikos valdymo subjektų sąrašas;
- rizikos valdymo organizacijos brandumas;
- atviro bendravimo atmosfera;
- komandinio darbo dvasia;
- kompleksinis organizacijos požiūris į rizikos valdymą;
- rizikos valdymo grupės autoritetas. [6]

Pirmas žingsnis kuriant patikimą apsaugos sistemą – atlikti rizikos analizę. Tik geras išankstinis pasiruošimas padeda riziką minimaliai sumažinti ir išvengti nepageidaujamų pasekmių.

[6] Rizikos analizės vadovas. [interaktyvus]. Vilnius: Vidaus reikalų ministerija - 2006. [žiūrėta balandžio 3d.] Prieiga per internetą <http://www.vrm.lt/fileadmin/Padaliniu_failai/Informacines_politikos_dep/IT_sauga/Rizikos_analize.pdf, (23psl.)>

Rizikos analizė (rizikos vertinimas) – nuoseklus rizikos objektų ir jų poveikių identifikavimas ir įvertinimas.

Atliekant rizikos analizę, turi būti išnagrinėti rizikos objektai, pavojingi veiksniai ir pažeidžiami objektai bei įvertinta nelaimingo atsitikimo, susijusio su šiais veiksniais, tikimybė ir pasekmės organizacijai.

Rizikos analizės struktūra, jos pagrindiniai elementai pateikiami 2 lentelėje:

Rizikos analizės struktūra

2 lentelė

Objektas	Operacija	Pavojingas veiksnys	Nelaimingo atsitikimo pobūdis	Pažeidžiami objektai	Pasekmės pažeidžiamiems objektams	Reikšmingumas			Nelaimingo atsitikimo greitis	Nelaimingo atsitikimo tikimybė	Svarba (rizikos laipsnis)	Prevencinės priemonės	Pastabos
						darbuotojams	organizacijai	nuosavybei					
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Rizikos aptikimas				Rizikos nustatymas		Rizikos klasifikavimas				Rizikos įvertinimas			
__1___2___3_a*___4				5_b*___6___		7___8____9____10				11___12___13__14			

a* - baigti čia, jei pavojingi veiksniai menki.

b* - baigti čia, jeigu nėra atitinkamų pažeidžiamų objektų.

Pirmoje grafoje pateikiami analizuojami atskiri rizikos objektai, kuriuose yra rizikos šaltiniai.

Antroje grafoje nurodoma, kokios operacijos bus vykdomos objekte.

Trečioje grafoje nurodomi pavojingi veiksniai.

Ketvirtoje grafoje analizuojama, kokio pobūdžio nelaimingus atsitikimus gali sukelti pavojingi veiksniai pavieniui ir kartu su kitais pavojingais veiksniais. Ties kiekvienu pavojingu veiksniu išvardijami nelaimingi atsitikimai, kuriuos tas veiksnys gali sukelti.

Penktoje grafoje nurodomi objektai, kurie yra rizikos zonoje.

Jei esami pavojingi veiksniai nekelia grėsmės darbuotojams ar organizacijos turtui, tai tokie rizikos objektai toliau nebenagrinėjami.

Šeštoje grafoje nurodomos nelaimingo atsitikimo pasekmės pažeidžiamiems objektams, išreikštos kokybiškai.

Septintoje grafoje analizuojamos pasekmės darbuotojams, išreikštos kiekybiškai.

Aštuntoje grafoje analizuojamos pasekmės organizacijai, išreikštos kiekybiškai.

Devintoje grafoje analizuojamos pasekmės organizacijos turtui, išreiktos kiekybiškai;

Dešimtoje grafoje nurodomas nelaimingo atsitikimo greitis ir poveikio trukmė.

Vienuoliktoje grafoje prognozuojama, kokia yra įvykių tikimybė

Dvyliktoje grafoje nurodoma, kurie rizikos šaltiniai objekte yra svarbesni.

Tryliktoje grafoje pateikiamos priemonės nelaimingiems atsitikimams išvengti bei pasekmėms likviduoti.

Keturioliktoje grafoje galima pateikti prognozuojamus žalos apskaičiavimo duomenis, nurodyti galimą nelaimingą atsitikimą su blogiausiomis pasekmėmis. [7]

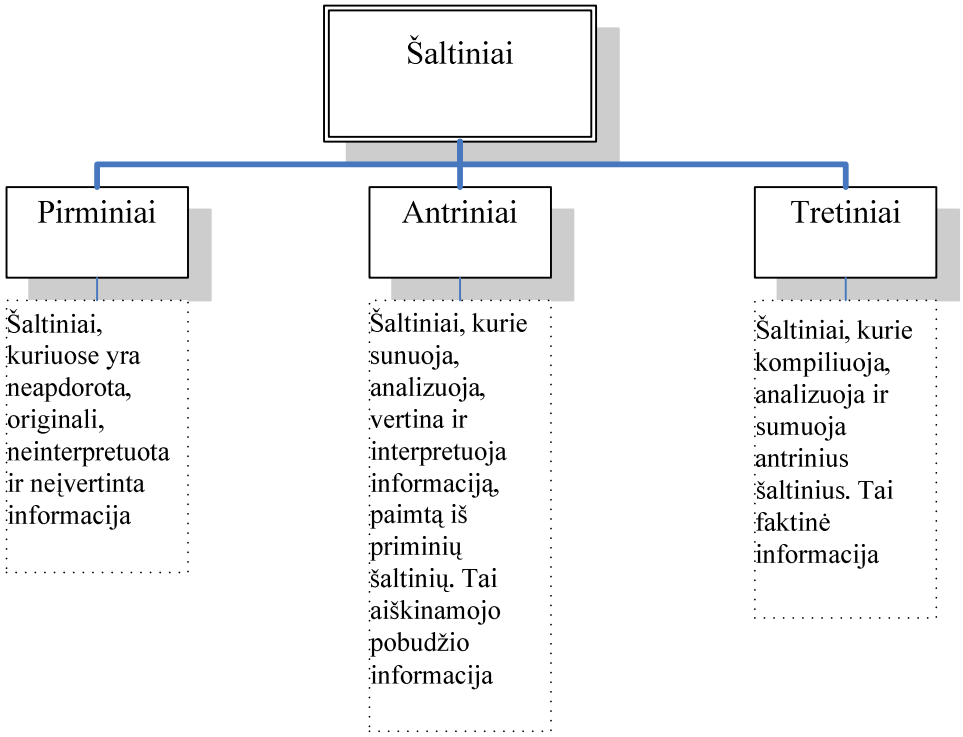
Informacijos šaltiniai. [8]

Rizikos analizės metu, būtina labai gerai suvokti pagrindinius informacijos šaltinius, jų privalumus ir trūkumus. Nustatyti informacijos gavimo būdus ir jos parametrus. Informacijos šaltiniai vertinami pagal tikslumą, tinkamumą ir patikimumą.

Informacijos tikslumas reiškia pirminio reiškinio atspindėjimo laipsnį.

Tinkamumas parodo, kaip informacija susijusi su analizės objektu.

Patikimumas išreiškia tikimumą, kad atlikus pakartotinį tikrinimą, bus gauti tokie patys rezultatai. Pagal informacijos tikslumą, tinkamumą ir patikimumą informacijos šaltiniai skirstomi į pirminius antrinius ir tretinius (6 schema).



6 schema. Informacijos šaltiniai

Rizikos apskaičiavimas.

Pačią rizikos analizę galima įvardinti kaip nuostolių, atsiradusių grėsmei pasitvirtinus,

[7] LR aplinkos ministro Įsakymas“ Dėl planuojamos ūkinės veiklos galimų avarijų rizikos vertinimo rekomendacijų R41-02 patvirtinimo 2007.07.16 Nr. 367, Vilnius

[8] Rizikos analizės vadovas. [interaktyvus]. Vilnius: Vidaus reikalų ministerija - 2006. [žiūrėta balandžio 3d.] Prieiga per internetą <http://www.vrm.lt/fileadmin/Padaliniu_failai/Informacines_politikos_dep/IT_sauga/Rizikos_analize.pdf>

paskaičiavimą. Rizika apskaičiuojama remiantis turto vienetų vertėmis ir įvertintais tarpusavyje susijusiais reikalavimų lygiais.

Nustačius rizikos elementus jie apjungiami, siekiant pamatyti bendrą rizikos vaizdą. Dažniausiai naudojamas rizikos elementų apjungimo metodas yra:

Bendra rizika = Poveikis X Grėsmės tikimybė

Grėsmės tikimybė dažniausiai nustatoma atsižvelgiant į praeities faktus arba į vadovo nuomonę.

Šie veiksniai gali būti susieti skirtingais būdais. Pavyzdžiui rizikos reikšmės apskaičiuojamos pagal turto vienetams, pažeidžiamumams ir grėsmėms bei teisiniams ir veiklos reikalavimams priskirtų verčių sumą.

Svarbu pastebėti, kad nėra „teisingų“ ir „neteisingų“ rizikos apskaičiavimo būdų. Organizacija gali pasirinkti tą rizikos vertinimo metodiką, kuri geriausiai atitinką veiklos ir jos saugos reikalavimus. Šio apskaičiavimo rezultatas turėtų būti apskaičiuotų rizikų sąrašas, susijęs su kiekvienu informacijos atskleidimo, modifikacijos arba neprieinamumo atveju, arba turto vieneto sunaikinimu, neperžengiant informacijos saugumo valdymo sistemos ribų.[9]

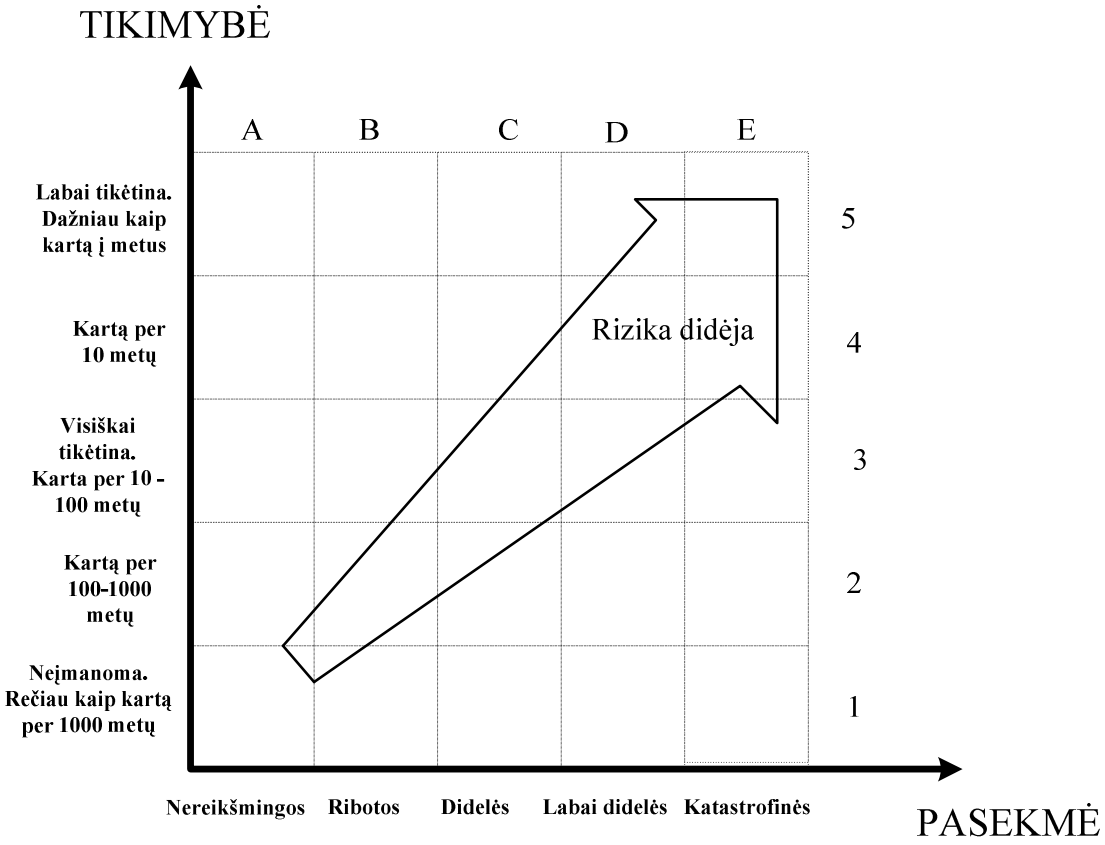
Kiekvienos analizės metu įvertinamos kylančios grėsmės, sistemos dalių pažeidžiamumas ir galimos kontrpriemonės nelaimės atveju. Paprastai rizikos įvertinimas prasideda nuo galimų grėsmių numatymo ir sistemos pažeidžiamų vietų aprašymo.

Rizikos įvertinimo stadijoje atsakinga grupė turėtų identifikuoti esančius ir galimus pavojus, įvertinti saugos spragas, kurios gali būti išnaudotos grėsmių realizacijai bei parodyti:

- rizikos objektus, kuriuose gali įvykti nelaimingas atsitikimas;
- rizikos šaltinius rizikos objektuose;
- nelaimingų atsitikimų pobūdį;
- galimus pažeidžiamus objektus;
- nelaimingo atsitikimo pasekmes;
- nelaimingo atsitikimo tikimybę.

[9] Rizikos analizės vadovas. [interaktyvus]. Vilnius: Vidaus reikalų ministerija - 2006. [žiūrėta balandžio 3d.] Prieiga per internetą <http://www.vrm.lt/fileadmin/Padaliniu_failai/Informacines_politikos_dep/IT_sauga/Rizikos_analize.pdf>

Rizikos objekto ir jo dalies rizikos laipsnis pagal nustatytas galimo nelaimingo atsitikimo juose tikimybes ir pasekmes gali būti įvertinamas remiantis matrica (7 schema).



7 schema. Galimo nelaimingo atsitikimo pasekmių vertinimas

E stulpelyje pateikiami rizikos objektai ir operacijos, kuriuose įvykus incidentui, pasekmės organizacijai būtų katastrofinės. Taip pat nurodomos situacijos, kuriose gelbėjimo darbai būtų sudėtingi ir labai brangūs.

D stulpelyje pateikiami rizikos objektai ir operacijos, kuriuose įvykus incidentui, pasekmės būtų labai didelės. Gelbėjimo darbai būtų sunkūs, bet pasitelkus esamas gebėjimo tarnybų pajėgas bei ūkio objektų personalą bei priemones, įmanoma likviduoti avariją.

C stulpelyje pateikiami rizikos objektai ir operacijos, kiuriuose, įvykus incidentui, pasekmės būtų didelės. Avarijos pasekmes galima likviduoti esamomis gelbėjimo tarnybų pajėgomis ir turimomis priemonėmis.

B stulpelyje pateikiami rizikos objektai ir operacijos, kiuriuose, įvykus incidentui, pasekmės būtų ribotos.

A stulpelyje pateikiami rizikos objektai ir operacijos, kiuriuose, įvykus incidentui, pasekmės būtų nereikšmingos.

Rizikos įvertinimo grupės nariai sudaro išsamų grėsmių ir pavojų sąrašą. Atsižvelgiant į įvairių įvykių kilimo tikimybę, privaloma atlikti rizikos įvertinimą, taip pat įvertinti galimą įvykių poveikį vertybėms. Tačiau, kad atlikti įvertinimą, kiekvienas grupės narys turi gerai suprasti šias sąvokas: rizika, įvykio tikimybė, pasekmė (žala).

Tai atlikdama grupė užpildo atitinkamą 3 lentelę:[10]

Rizikos vertinimas

3 lentelė

		Pasekmė (žala)				
		Nereikšminga	Ribota	Didelė	Labai didelė	Katastrofiška
Tikimybė	Labai tikėtina					5
	Karta per 10 m.				4	
	Visiškai tikėtina			3		
	Kartą per 100-1000 m.		2			
	Neįmanoma	1				

Atlikus rizikos analizę galutiniai rezultatai turi atspindėti:

- kritinės reikšmės vertybių finansinį įvertinimą;
- detalų svarbiausių grėsmių sąrašą;
- kiekvienos grėsmės tikimybę ir galimą jos iškilimo dažnumą;
- grėsmės sąlygojamus potencialius nuostolius – finansinį poveikį, kuris gali grėsti vertybei;
- rekomenduojamus sprendimus ir saugos priemones arba kontrpriemones.

Sekantis žingsnis rizikos valdymo procese yra rizikos tvarkymas.

Rizikos tvarkymas – tai veiklos, susijusios su rizika administravimas, inventorizavimas, vertinimas, tikrinimas, draudimas. Tai procesas, kurio metu pasirenkamas ir įdiegiamos priemonės, keičiančios rizikos tikimybę.

Vadinasi reikia nustatyti tinkamiausias rizikos valdymo priemones. Tam reikia atsižvelgti į konkrečius turto vienetus ir su jais susijusius rizikos poveikius. Kiekvienos konkrečios rizikos atveju būtina įvertinti visas galimybes, kad būtų galima pasirinkti tinkamiausią sprendimą.

Rizikos tvarkymo etape aptariami tokie pasirinkimai įvertinus situaciją. Šiuos sprendimus galima taikyti po vieną arba kombinuojant tarpusavy.

Rizikos vengimas. Jis apibūdina bet kokį atvejį, kai turtas iškeliamas iš rizikos zonų.

[10] LR aplinkos ministro Įsakymas“ Dėl planuojamos ūkinės veiklos galimų avarijų rizikos vertinimo rekomendacijų R41-02 patvirtinimo 2007.07.16 Nr. 367, Vilnius

Svarstant šią galimybę būtina subalansuoti veiklos ir finansinius poreikius.

Rizikos optimizavimas. Tai su rizikos kontrole susijęs procesas, kuriuo siekiama sumažinti neigiamų pasekmių tikimybę ir padidinti teigiamų pasekmių atsiradimo tikimybė

Rizikos perkėlimas gali būti geriausia alternatyva, jeigu tai leidžia išvengti rizikos arba rizikos mažinimo priemonės yra labai sudėtingos ar brangios. Tai gali būti potencialių kaštų arba nuostolių perkėlimas kitai šaliai (pavyzdžiui draudimo bendrovei).

Rizikos išlaikymas. Šiuo procesu organizacija susitaiko su konkrečios rizikos sąlygojamais nuostoliais ir nauda.

Trečiasis rizikos valdymo etapas – rizikos priėmimas.

Priimant riziką reikia pasirinkti „rizikos mažinimo“ variantą, bei priemones, kad sumažintų riziką iki nustatyto priimtino lygio. Norint nustatyti tinkamiausias kontrolės priemones, naudinga įvertinti su kiekviena rizika susijusius saugos reikalavimus.

Kontrolės priemonių rizikos mažinimo būdai:

- sumažinti grėsmės tikimybę ar riziką sukeliantį pažeidžiamumą;
- užtikrinti teisinių ar sutartinių reikalavimų laikymąsi;
- sumažinti galimą iškilusios rizikos poveikį;
- aptikti pageidautinus įvykius, reaguojant į juos ir pašalinti jų pasekmes.

Būdas, kurį pasirinks organizacija, siekdama apsaugoti savo turtą, yra sprendimas, kuris priklauso nuo veiklos aplinkos, kurioje dirba organizacija. Svarbu, kad kontrolės priemonės atitiktų specifinius organizacijos poreikius, taip pat svarbu, kad jų pasirinkimas būtų pagrįstas. Nustačius kontrolės priemones, kurios leistų sumažinti riziką iki priimtino lygio, būtina įvertinti kiek minėtų priemonių įdiegimas sumažins riziką vadinamą liekamąja rizika. Liekamoji rizika – tai likęs rizikos lygis, kuris išlieka įdiegus kontrolės priemones. Liekamąją riziką vadovai gali naudoti tam, kad nustatytų tas sritis, kurioms reikia papildomos kontrolės. Vadovybė nusistato sau priimtiną liekamosios rizikos dydį, įvertinant išlaidas kontrolei. Dažniausiai organizacijos draudžiasi nuo liekamosios rizikos.

Įvertinti liekamąją riziką visuomet sunku, bet būtina įvertinti bent tai, kiek kontrolės priemonės sumažina rizikos vertę.

Jei paaiškėja, kad liekamoji rizika tebėra nepriimtina, būtinas sprendimas, kaip ją kontroliuoti. Viena galimybė yra įdiegti papildomas kontrolės priemones, kurios galutinai sumažintų riziką iki priimtino lygio. Tačiau kartais gera praktika atsisakyti toleruoti nepriimtiną riziką. Kartais riziką mažinti iki priimtino lygio būna neįmanoma arba finansiškai nepriimtina.

Netgi įdiegus pasirinktas kontrolės priemones, tam tikra rizika visuomet lieka. Taip yra todėl, kad organizacijos informacinių sistemų neįmanoma visiškai apsaugoti.

Ketvirtasis etapas informacija apie riziką. Dažniausia tai naudojama informacijos pasikeitimui

ar perdavimui. Bendravimo procesas turi du tikslus: informuoti arba įgalioti.

Eksperto tikslas perduoti informaciją, publika ją gali priimti arba ne informuoti (kai yra poreikis veiksmui ir bendravimui).

Kodėl grupės turi informuoti apie riziką?

1. Kad personalo bendras supratimas išaugtų. Perspėjimai apie nežinomą riziką, pranešimai apie jau išnykusią riziką.
2. Vadovo pranešimas kartais gali būti naudingas, kai kiti darbuotojai neturi pakankamai žinių patys įvertinti riziką. Vadovo informacijos pateikimui keliami dideli reikalavimai.
3. Informacija siunčiama, norint turėti grįžtamąjį tikslą (žvalgomasis tyrimas apie ateities planus) tam, kad struktūrizuoti procesą, kai priimami keli tarpiniai sprendimai.
4. Informacija siunčiama, kad grįžtamojo ryšio pagrindu priimti sprendimą.

   Informacija apie riziką interpretuojama labai įvairiai, ir tai priklauso nuo daugelio faktų:

   - laiko parinkimas;
   - siuntėjo statusas;
   - informacijos pateikimo stilius;
   - teigiami pranešimai iššaukia teigiamą reakciją, neigiami- neigiamą;
   - žmonių išankstinės nuostatos rizikos atžvilgiu.

Jei rizikos elementai yra nelabai suprantami arba sukelia neigiamą įspūdį, reakciją gali būti neadekvačiai aktyvi.

Rizikos valdymas yra procesas, kuriame gali dalyvauti daug skirtingų pareigybių ir skirtingų sričių specialistų. Norint, kad rizikos valdymas padidintų organizacijos saugumo lygį ir šis lygis laikui bėgant išliktų, būtina aiškiai apibrėžti paties proceso tobulinimo mechanizmus, numatomų periodinių įvykių tvarkaraštį, kas dalyvauja organizacijos rizikos valdymo procese ir kokia dalyvių atsakomybė.

Veiklos tęstinumo strategijos suformulavimas

Suformuota veiklos tęstinumo strategija, sudaryti valdymo procesai turi būti dokumentuoti, patvirtinti vadovybės. Šie dokumentai turi būti naudojami ir bandomi. Būtina sudaryti procesus, kurie bus reikalingi jei organizaciją ištiks katastrofa. Tam reikalingas veiklos atkūrimo planas.

4.2. Veiklos atkūrimo po nenumatyto atvejo svarba

Tikriausiai ne vienas kompiuterio vartotojas ar specialistas, susidūręs su duomenų praradimo problema, galvoja, kad atkurti prarastus duomenis - neįmanoma, o jų turima informacija apie duomenų atkūrimą - netiksli ir nenuosekli. Todėl nenuostabu, kad sąvokos "duomenų praradimas" ir "duomenų atkūrimas" - vienos painiausiai ir klaidingiausiai suprantamų vartotojams.

Pirminės duomenų praradimo priežastys - gana įvairios.

Žmogiškosios klaidos sudaro net 32 proc. visų atvejų, kai prarandami duomenys. Šis faktas atskleidžia, kokie pažeidžiami ir nesaugūs yra duomenys. Kitos priežastys, sukeliančios duomenų praradimą, yra:

- kompiuterių gedimai (35%),
- kompiuteriniai virusai (7%),
- kompiuterinės įrangos sabotažas (2%),
- programinės įrangos sabotažas (5%),
- aptarnavimo/ eksploatacijos klaidos (7%),
- stichinės nelaimės (gaisras, potvynis)(4%),
- programinės įrangos klaidos (4%),
- kita (4%).[11]

Pasaulinėje incidentų, nelaimingų atvejų įvaldymo praktikoje, katastrofa yra laikomas aukščiausio lygmens nelaimingas įvykis. Pateikiamas sąrašas, kuris yra geras orientyras, kaip suprati nelaimingo atvejo etapus ir kokių reikia imtis laipsniškų veiksmų:

1. Pasirengimas
    a. tinkamos apsaugos politikos sukūrimas;
    b. gero veiklos tęstinumo ir po nelaimingo atvejo atkūrimo plano nustatymas;
    c. nelaimingų įvykių prevencijos procedūrų diegimas.
2. Nustatymas
    a. pasirodžius nelaimingo atvejo požymiams, reikia paskirti atsakingą asmenį;
    b. poreikis apibūdinti ar tai iš tiesų nelaimingas atsitikimas (katastrofa);
    c. derinimas su kitais darbuotojais;
    d. tinkamų institucijų, vadovų informavimas;
3. Situacijos valdymas, suvaržymas
    a. teritorijos apsauga katastrofos metu;

[11]Duomenų atstatymas [interaktyvus]. Vilnius: IBM [žiūrėta 2007m. kovo 25d.]. Prieiga per internetą <http://www-05.ibm.com/lt/services/da.html>

b. sprendimas, kurios operacijos tęsiamos, o kurias reikia nutraukti.

4. Sunaikinimas
    a. nustatoma katastrofos priežastis;
    b. analizuojama kaip būtų galima ateityje išvengti panašios nelaimės;
    c. jei reikia partvarkoma sistema, arba vengti tu pačių problemų.
5. Atnaujinimas
    a. reikia išsiaiškinti ar po nelaimingo atsitikimo saugu grįžti;
    b. atkuriama pradinė veiklos būsena;
    c. nuodugniai kontroliuojama atnaujinta sistema.
6. Mokymasis iš klaidų
    a. reikia parašyti įgyvendinimo ataskaitą komandai ir jos vadovui;
    b. tikrinama išvada su komanda;
    c. nustatoma ar pasimokyta, ir kokias sritis reikia tobulinti;
    d. atnaujinant dokumentus naudojama ir peržiūrima paruošta informacija.

Veiklos atkūrimas daugiau naudojamas procesuose susijusiuose su informacinėmis technologijomis.

Jei organizacija nesiims saugumo priemonių, tai gali ištikti blogiausia. Remiantis statistiniais duomenimis:

80% veiklos atkūrimo nesuplanavusių ir katastrofą patyrusių kompanijų žlunga per dvylika mėnesių.

90% informacinių technologijų duomenis praradusių verslų žlunga per du metus.

Pusė kompanijų, nesugebėjusių atstatyti kompiuterinių sistemų per dešimt dienų, neatsigauna.

Vienas iš penkių šimtų duomenų centrų patiria rimtą katastrofą kartą per metus.

Veiklos atkūrimo procesai reikalingi tuomet kai organizaciją ištiks krizė.[12]

4.2.1. Šiuolaikinės krizės samprata

Krizių vadybos požiūriu, krizė – tai proceso sutrikimas, ir nenumatytas atvejis, keliantis grėsmę organizacijai, ūmus netikėtas įvykis, svarbus atsitikimas, potencialiai galintis pakenkti ar net sugriauti organizacijos reputaciją.

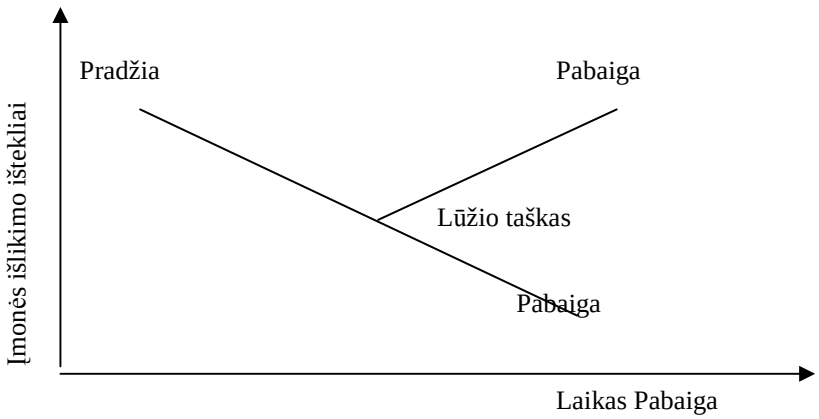
Viešieji ryšiai įgalina įmonę sumažinti žalą jos įvaizdžiui ir patikimumui. Krizinių situacijų neišspręsite tylėdami, nes informacijos stoka tik dar labiau sustiprins klaidingą nuomonę ir skatins išankstinį nusistatymą.

Įmonės krizė šiuolaikinėje ekonomikos literatūroje apima įvairius įmonės gyvavimo fenomenus – nuo paprastų įmonės funkcionavimo trukdžių, esant įvairiems konfliktams, iki įmonės likvidavimo. Įmonės krizę galima traktuoti kaip neplanuota ir nepageidaujamą, apribotą laiku procesą, kuris gali

[12] Informacijos centro vadovas, Londonas, Prekybos ir pramonės rūmai - 2003

sutrukdyti įmonės funkcionavimą arba nutraukti jos veiklos tęstinumą. Taigi krizė – tai bet kuri nestandartinė įmonės situacija, kurioje kyla rizikos grėsmė.

Įmonės krizė – tai nuoseklios procesų ir įvykių eigos lūžio momentas. Šiai situacijai būdingi du variantai: įmonės likvidavimas arba sėkmingas krizės įveikimas (8 schema).



8 schema. Įmonės krizės raida

Organizacijos valdymo metu išskiriamos trys krizių grupės:

Netikėtos krizės – tokios krizės, kurių neįmanoma numatyti ir planuoti jų prevencijos. Tokioms krizėms priskiriami įvairūs techniniai gedimai, nelaimingi atsitikimai, lėktuvų katastrofos, gaisrai, organizacijos vadovo žūtis ir pan. Į tokias krizes galima tik reaguoti ir rekomenduotina, kuo greičiau. Pastarosioms krizėms turi būti iš anksto parengtas krizės valdymo planas, darbuotojai turi žinoti, kas sudaro krizės valdymo komandą, kam tenka atsakomybė, kas bendrauja su žiniasklaida ir pan., kad neįvyktų nesusipratimų, ir kad krizė kuo greičiau būtų išspręsta.

Išaugančios krizės - tai ilgainiui besiformuojančios krizės, kurių požymius galima numatyti iš anksto, taigi šiuo atveju pagrindinis veiksmų planavimo ir vadybos tikslas yra tinkamai įvertinti augančią krizę ir ją suvaldyti taip, kad neįvyktų kritinės situacijos. Šiai grupei dažniausiai yra priskiriamos tos krizės, kurių pamatas yra socialinės problemos, neramumai ar konfliktai, kurie nevaldomi gali iškilti į agresyvius priešiškus veiksmus, kas jau reiškia krizę.

Nuolatinės krizės - tai krizės, kurios gali trukti mėnesius ar metus, nepaisant pastangų jas suvaldyti. Tokio pobūdžio krizėms yra priskiriami gandai.[13]

Krizė - tai ne tik sprogimas gamykloje ar lėktuvo katastrofa, bet ir kompanijos vadovų atsistatydinimas, pateikti teisminiai ieškiniai, dideli gaminamos produkcijos defektai, konfliktai su nevyriausybinėmis organizacijomis ir kiti panašūs incidentai. Jei laiku nesiimama reikiamų veiksmų,

[13] Informacijos vadyba, [Interaktyvus][žiūrėta 2007 m. balandžio 9 d.]. Prieiga per Internetą: http://www.infovi.vu.lt/ivs/biblioteka/temos/infovadyba.htm#_Toc486382749

jie gali labai pakenkti kompanijos įvaizdžiui ar finansiniams rezultatams.

Kodėl atsiranda krizės, dėl kokių priežasčių jų negalima išvengti? Gal todėl, kad gyvenime nėra idealumo, kur galima vykdyti, bet kokią užgaidą ir nuo to niekas nenukentėtų. Skaudžiausia būna tada, kai netikėtos ir nelauktos situacijos aplanko netinkamiausiu laiku. Dažniausiai tai pasitaiko dėl:

- žmogiškojo faktoriaus;
- technologinių sutrikimų;
- stichinių nelaimių.

Kaip reikia elgtis, norint užkirsti kelią krizėms? Kuom rizikuoti ir kaip kontroliuoti situacija, kad jokia organizacija nepatirtų nesėkmės?

Pirmiausia reikalinga :

- situacijos analizė;
- pasirengimas galimoms krizinėms situacijoms;
- krizinės situacijos sušvelninimo plano parengimas;
- operatyvus reagavimas ir spaudos analizė, iškilus netikėtai krizinei situacijai;
- po krizinė komunikacija.

4.2.2. Veiklos valdymas krizės metu

Kiekviena komercinė struktūra rinkos sąlygomis siekia gauti pelną. Tačiau pelną įmonė gauna nuolatos rizikuodama, konkuruodama su kitais veiklos subjektais. Rizika yra neatskiriamas bet kurios žmogaus ūkinės veiklos elementas. Rinkos ekonomikoje rizika yra neišvengiama - tai, kas šiandien yra stabilu, rytoj gali pasikeisti. Paklausos ir pasiūlos pokyčiai, konkurencija ir infliacija, daugelis kitų analogiškų veiksnių nuolat keičia veiklos aplinką. Dėl šios kintančios aplinkos verslą pastoviai lydi neapibrėžtumas, prognozuojamų rezultatų neužtikrintinumas, rizikingi sprendimai. Neapibrėžta rinkos situacija yra objektyvus rizikingų sprendimų pamatas. Tokie sprendimai gali slypėti tiek organizuojant verslą, tiek formuojant įmonės strategiją, tiek pačių vadybininkų veikloje. Todėl neretai įmonės nesugeba išsilaikyti ir žlunga.

Kiekviena įmonė sprendžia daugelį ūkinės veiklos uždavinių:

- klientų poreikių patenkinimas;
- nuolatinis produktų ar paslaugų tobulinimas;
- geros finansinės būklės užtikrinimas;
- įmonės ateities vystymosi numatymas ir tikslų formulavimas.

Nesugebėjimas atlikti bent vieno iš uždavinių ar nekokybiškas jų atlikimas stumia įmonę prie krizinės situacijos.

Krizinė situacija susidaro, kai pažeidžiamas įmonės funkcionavimas ir plėtotė, tačiau kritinis momentas gali būti įveikiamas, pasitelkus vidinį įmonės potencialą. Krizinė situacija laikinai paveikia tik pavienes veiklos sritis, negatyvus poveikis nėra perduodamas į kitas ūkinio subjekto veiklas.

Bankrotas yra paskutinė krizinės situacijos stadija, reiškianti sistemos žlugimą.

Krizių vadybos uždavinys - ne tik užfiksuoti esamą situaciją, konstatuoti iškilusias problemas. - svarbu numatyti ir galimus situacijos keitimo variantus, geriausiai atitinkančius laukiamus ateities pokyčius. Todėl svarbu laiku pastebėti krizę, kad kuo ilgesnis būtų laiko tarpas nuo pradžios iki lūžio taško (8 schema) arba pasiekti, kad krizė plistų kuo lėčiau, o proceso trukmė būtų kuo ilgesnė.

Ką reikia daryti, norint išvengti krizinės situacijos?

Krizių valdymas skirstomas etapais. Jie susideda iš

1. pasiruošimo;
2. identifikavimo;
3. plitimo sustabdymo;
4. pasekmių pašalinimo;
5. veiklos atstatymo.

Pasiruošimas

Daugumą krizių būtų galima išvengti, jei joms būtų pasiruošta.

Pasiruošimas - tai pagrindinis ir pirmas etapas apsisaugoti nuo krizės atakos. Ypatingai organizacijoje reikia išsiaiškinti, kurie vadovai gali būti krizių valdymo komandos dalis. Nustatyti, kurie yra geri oratoriai ir patikrinti ar jie apmokyti.

Kadangi vadovas –žmogus, atsakantis už darbų apimtį. Jis turi mokėti prisitaikyti prie įvairių aplinkos reikalavimų. Taip pat žinoma, jog vadovui pavaldūs kiti darbuotojai, padedantys pasiekti numatytų rezultatų. Todėl paruošiamas palaikymo personalas.

„Labai svarbu suburti krizių valdymo komandą, iš anksto žinant jos poziciją. Tokia komanda turi reguliariai susitikti ir aptarti potencialių krizių atsiradimą bei veikimo planą prieš jas“[14].

Krizių valdymo plano eiga turi remtis įmonių apsauga, komunikacija bei žalos mažinimu. Sukūrus tokį planą, visi jo dalyviai turi būti betarpiškai informuojami, o planas nuolatos peržiūrimas.

Neslėpti slaptų krizių planų nuo išrinktos valdymo grupės. Visas personalas turi žinoti veiksmus krizės metu, ar tai yra esminė nelaimė, ar masinės informacijos priemonių apsiaustis.

Identifikavimas

Iškilus krizės grėsmei, būtina sutelkti netradiciškai mąstančius įmonės novatorius, sudaryti krizinių situacijų valdymo ir strateginės plėtros komandas. Jos kartu su įvairių lygių vadovais turėtų parengti ir įgyvendinti krizinės situacijos likvidavimo ir finansinio pajėgumo stabilizavimo strategiją.

Tačiau pirmiausia būtina:

- kruopščiai išanalizuoti ir įvertinti informaciją apie visus išorės aplinkos veiksnius ir procesus;

[14] Ką ir kaip veikia vadovai. [interaktyvus],[žiūrėta 2007 m. vasario mėn. 5 d.]. Prieiga per internetą: <http://verslas.banga.lt/lt/leidinys.full/3fd5e5ab4e3e7>

- sudaryti jų įtakos prognozes;
- išsiaiškinti, ar darbuotojai atitinka naujausios dalykinės kompetencijos lygį;
- ar galimas svarbios ir slaptos informacijos „nutekėjimas“;
- kokia yra debitorinio ir kreditorinio įsiskolinimo kokybė;
- koks beviltiškų skolų dydis;
- kokia įmonės veiklos priklausomybė nuo licencijų;
- kiek prarasta grynųjų pajamų dėl neprofesionalių sprendimų ir prasto darbo organizavimo.

Plitimo sustabdymas

Plitimo sustabdymas – organizacijos praktikoje, iškilus krizinėms situacijoms, dažniausiai yra kreipiamasi į ryšių su visuomene tarnybas. Ji parengia krizių prevencijos programą, krizės pobūdžio identifikavimą, operatyvius veiksmus iškilus krizei, krizės padarinių likvidavimą, reabilituojant organizacijos reputaciją.

Norint efektyviai kontroliuoti krizę, ryšių su visuomene tarnyba turi operatyviai sudaryti krizių valdymo komandą: finansų, teisės, personalo valdymo ekspertų, atstovų žiniasklaidai, nuolat komunikuojančių su komandos vidinėmis ir išorinėmis auditorijomis. Kai krizių valdymo komandos elementai yra kompleksiškai suderinti, krizinė situacija - valdoma efektyviai.

Krizės pasekmių pašalinimas

Priemonės krizei pašalinti skirstomos į:

Operatyvines – trumpalaikes priemones, kuriomis siekiama pagerinti įmonės likvidumą.

Vidutinio laikotarpio priemonės, kuriomis siekiama konsoliduoti įmonę baudomis, limitais, sumažinti iš esmės kaštus, įvesti vienetinį darbo užmokestį ir siekti padidinti darbuotojų darbo efektyvumą.

Ilgalaikes priemones, kuriomis siekiama iš esmės pakeisti įmonės struktūrą plečiant naujus veiklos laukus, pakeičiant teisinę įmonės formą, išsidėstymą erdvėje, sujungiant atskiras veiklos sritis, diegiant naujas gamybos technologijas, naujus gaminius, įeinant į naujas rinkas.

Motyvacija - tai procesas, skatinantis imtis veiklos, kuri padėtų pasiekti organizacijos tikslus.

Kad organizacija įgyvendintų tikslą, vadovas privalo koordinuoti darbus ir priversti darbuotojus juos atlikti laiku.

Veiklos atkūrimas

Dominuoja dvi krizės suvokimo koncepcijos:

Siekis išlikti

Šiuo atveju krizė suvokiama kaip grėsmė, išlikimo problema, žlugimo prielaida. Toks neigiamas krizės akcentas formuoja atitinkamas priemones atkurti įmonės iki krizinę būklę.

Siekis atsinaujinti

Šiuo atveju krizė suvokiama kaip būtinybė atsinaujinti, pertvarkyti įmonės strategiją, eliminuoti neracionalius fragmentus, pagrįsti tikslus ir jų įgyvendinimo veiksmus. Todėl priemonės pakeisti krizinę situaciją yra traktuojamos ne kaip kova su krize, o kaip teigiami įmonės strategijos pokyčiai.

Atstačius organizacijos pradinę būsena reikalingas ir veiklos tęstinumo valdymas.

1. Sudaromas veiklos tęstinumo planas:
    a. rizikos ir poveikio analizė;
    b. plano rengimas;
    c. veiksmų aprašymas.
2. Plano sudarymas.
3. Priežiūra, kontrolė ir atnaujinimas.

Išanalizavus ir įgyvendinus šiuos žingsnius galima lengviau nuspėti, kuriose vietose organizaciją gali ištikti nesėkmė. Kad tai neatsitiktų reikia susidaryti preliminarų planą, kurį sudarytų bent paprasčiausi etapai:

- įvertinti veiklos poreikius;
- nustatyti galimas rizikas veiklai, jas vertinti, valdyti bei stebėti;
- suplanuoti kas bus daroma įvykus tam tikram įvykiui, laiku atnaujinti tikrinti šiuos planus testuoti bei nepamiršti pasitvirtinti su aukščiausia vadovybę.

Apsaugant įmonės turtą nuo praradimo būtina turėti veiklos atkūrimo po nenumatyto atvejo planą.

Įvykių numatymo plane pateikiama informacija, kaip tęsti veiklą, kai palaikantys procesai, taip pat ir informacinės sistemos, yra pažeisti arba jais negalima naudotis. Šiuose planuose turi būti numatyta daugelis galimų scenarijų, apimančių:

- įvairios trukmės pertrūkius;
- įvairių rūšių įrenginių praradimą;
- visišką fizinio ryšio su objektais praradimą;
- būtinumą atkurti padėtį, kuri būtų, jei pertrūkis nebūtų įvykęs.

Žalos padarinių atkūrimo planuose aprašoma, kaip atkurti sistemų, paveiktų nepageidaujamo įvykio, veiklą.

Žalos padarinių atkūrimo planai apima:

- kriterijus pagal kuriuos nusakoma žala;
- pareigas, susijusias su žalos padarinių atkūrimo planų vykdymo pradžia;
- pareigas, susijusias su įvairia žalos padarinių atkūrimo veikla;
- žalos padarinių atkūrimo veiklos aprašus.

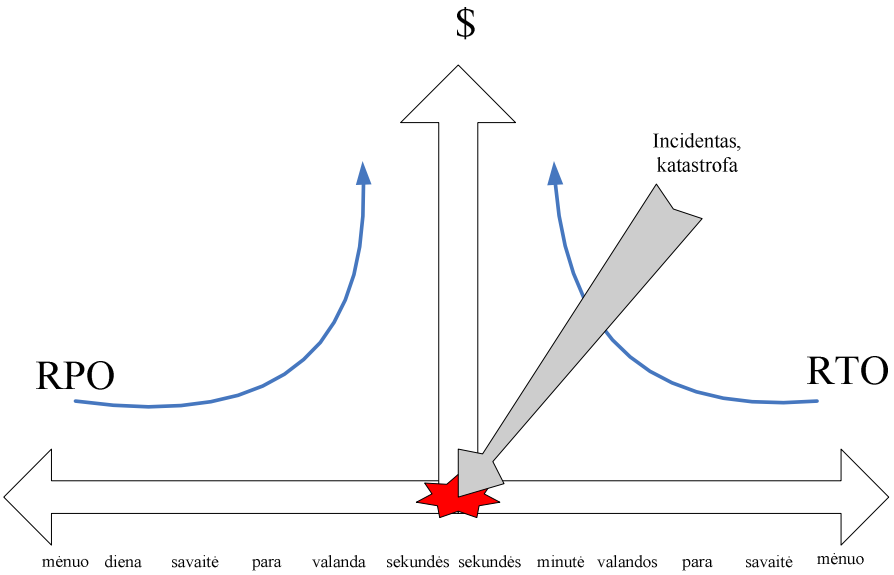
Toks veiklos atkūrimo planas gali būti naudojamas bet kurios veiklos organizacijoje.

Kai kurių nenumatytų situacijų negalima kontroliuoti ar išvengti. Tokiais atvejais veiklos tęstinumo planas turi padėti atkurti informacines sistemas per tokį laiką, kad išvengti rimtų nuostolių verslui.

Atkūrimo kontrolės, leidžia atstatyti sistemas įvykus nenumatytam atvejui.

Visų pirma reikia įvertinti atstatymo laiko (RTO) apibrėžimus bei atstatymo taškus (RPO) įvairioms sistemoms, kurioms skirtas planas.

RTO ir RPO turi būti suderinti su veiklos poreikiais (9 schema).



9 schema. Katastrofos galimybė organizacijoje.

RTO didžiausias leistinas laikas per kurį sistema turi būti paleista po nenumatyto atvejo.

RPO apibrėžia kokio amžiaus duomenys turi būti atstatyti pagal planą.

Turi būti tikrinama ar veiklos tęstinumo planas yra pastoviai atnaujinamas ar teisingai atspindi informacinių technologijų aplinką.

Kitas svarbus aspektas kurį reikia vertinti yra veiklos tęstinumo plano ir atstatymo po nenumatyto atvejo plano testavimo reikalavimai. Jie turi būti numatyti atlikti periodiškai įvairių tipų nenumatytiems atvejams.

3 Etapas. Veiklos tęstinumo valdymo struktūra ir konkretus planų sudarymas.

1. Nustatyti atnaujinimo strategijas.

Yra keletas būdų atkurti informacines sistemas. Tipinės atkūrimo strategijos yra:

- karšta vieta (angl. hot site) – yra pilnai sukonfigūruota vieta, kurioje yra turima kompiuterinė ir programinė įranga paruošta pilnai perimti veiklą, neveikiant pagrindinei sistemai. Turint karštą vietą, sistemą galima atstatyti per kelias valandas.
- šiltos vietos (angl. worm sites) – šilta vieta yra panaši į karštą vietą, bet joje nėra kompiuterinės įrangos. Kompiuterinė įranga pristatoma tada kai reikia, bet tai sulėtina sistemos atkūrimą ir paleidimą.

- šaltos vietos (angl. cold sites) – šaltos vietos paprastai patalpa su kondicionuojamu oru, elektros įvadas, be jokios kompiuterinės programinės įrangos. Atkūrimui reikėtų pristatyti visą reikiamą įrangą, tik atstatymas gali užtrukti. Trūkumas – brangus testavimas.
- vidinės paskirstytos sistemos ir tinklai – nurodomos kitos vidinės informacinės sistemos, paprastai nenaudojamos atstatymui po nenumatyto atvejo, kurios bus naudojamos kaip pakaitinės sistemos atkūrimui po nenumatyto atvejo.
- abipusiai susitarimai – abipusiu susitarimu dvi ar daugiau kompanijų susitaria naudoti viena kitos infrastruktūrą. Tam reikia, kad kompiuterinė ir programinė įranga būtų panašios. Privalumas yra maži kaštai. Taip pat yra daug spręstinu klausimų tokių kaip, vienodos kompiuterinės ir programinės įrangos palaikymas abiejuose vietose, jų koordinavimas. Svarbu, kad priimanti kompanija gali lėtai reaguoti ir yra klausimas dėl informacijos saugumo.
- du duomenų centrai – kai kurios organizacijos turi kelis duomenų centrus, kurie sureguliuoti perimti darbą kito centro neveikimo atveju. Tai panašu į abipusį susitariama su ta pačia kompanija.
- pardavėjo tiekiama įranga – kai kurie pardavėjai gali teikti įrangą kai jos reikia nelaimės metu. Šios strategijos problema, tokia kad pardavėjas ne visada galės patenkinti įrangos poreikį.
- visų išvardintų dalių kombinacijos.

2. Parengti ir kontroliuoti nenumatytų atvejų kontaktinį sąrašą.

Nelaimingo atvejo metu, ne laikas planuoti, kas už ką yra atsakingas. Tuo metu turi veikti visas personalas iš anksto pasiskirstęs pareigas. Nenumatytų atvejų sąrašas turi būti visiems prieinamas bet kuriuo metu, nuolat pildomas ir atnaujinamas. Už šį sąrašą atsakingi:

- paskirtas valdymo personalas;
- informacinių technologijų kritikinis personalas;
- medicinos ir psichinės pagalbos paslaugų sektorius;
- pardavėjai;
- valstybės pareigūnai;
- bendravimas su žiniasklaida (TV, radijas).

3. Surinkti ir kontroliuoti daiktų aprašą (inventorizacinį sąrašą).

Šis sąrašas turi būti laikomas saugioje patalpoje ir prieinamas tik veiklos tęstinumo plano vadovui.

Į šį sąrašą įtraukti:

- bendravimo įrenginių surašymas;
- dokumentų surašymas;
- kompiuterių kietųjų diskų ir programinės įrangos surašymas;

- įrengimų (išskyrus IT) surašymas;
- atsarginių patalpų surašymas;
- programinės įrangos ir duomenų failų atsarginių kopijų surašymas;
- laikinos vietos duomenys (adresas, telefono numeris).

4. Susitikti, diskutuoti ir pritarti įmonės tiekėjų planams.

Susitarimas su pardavėjais turi būti susitartas iš anksto. priklausomai nuo atstatymo laiko poreikio, kad veikla gautų reikiamas atsargas ir paslaugas nenumatyto atvejo metu.

5. Tyrinėti alternatyvius tiekimo šaltinius.

Kai kuriais atvejais, rekomenduojama turėti papildomus tiekimo šaltinius tokiems atvejams, jei paprasti tiekėjai nepasiekiami ar nenori tiekti reikalingų produktų ar paslaugų.

Testavimas

Kai tobulinamas veiklos tęstinumo planas reikalaujama daug pastangų. Vadovas mano, kad darbas yra pabaigtas. Tačiau taip nėra, kai planas bus baigtas reikia patikrinti visas veiklos sritis, kuriose reikalinga atlikti atnaujinimą, ištaisyti visus trūkumus, kad organizacija vadovaudamasi veiklos tęstinumo planu neturėtų netikėtų spragų ar neatrastų klaidų.

1. Apibūdinti išbandymo tikslus;

Testavimo plane pirmas žingsnis yra apsibrėžti testuojamus objektus. Testuojamo plano tikslas susideda iš:

- įrodyti, kad planas tikrai veikia;
- patikrinti ar alternatyvi infrastruktūra atitinka veiklos tęstinumo plano poreikius;
- patikrinti komandos procedūrų adekvatumą;
- nustatyti plano privalumus ir trūkumus;
- apmokyti dalyvaujančius asmenis;
- plano atnaujinimas.

2. Nustatyti reikiamą įrangą ir išteklius;

Priklausomai nuo testavimo metodologijos gali reikėti tam tikros įrangos ir išteklių. reikia užtikrinti, kad vadovybė pritaria įrangos pirkimui. Problemos: kur saugoma įranga kai nenaudojama ji turi būti lengvai prieinama. Nustatyti kas gali prie jos prieiti ir ar galima naudoti kitiems tikslams, rezervuota tik atkūrimo tikslams, įrangos perkėlimas į veiklos atkūrimo vietą, per kiek laiko galima perkelti įrangą į reikiamą vietą ir kas tai atliks.

3. Nustatyti reikiamą personalą;

Vykdant testavimo scenarijų nereikės viso personalo, reikia nustatyti kokios komandos dalyvaus ir kas už ką atsakingas.

4. Dokumentuoti testavimo grafiką, tvarką ir vietas;

Priklausomai nuo testavimo metodologijos yra patariama sukurti testavimo grafiką, kuris

nepertrauks normalios veiklos. Testavimas gali vykti savaitgaliais ar atostogų metu. Priklausomai nuo testo sudėtingumo reikalinga, kad išorinis personalas būtų pasiekiamas. Jei organizacija turi keletą testavimų vietų reikia nustatyti kurios bus testuojamos pirmos.

5. Nustatyti testavimo metodologiją;

Struktūrinė metodologija. Šis testavimas yra kai skirtingos testavimo komandos kartu detaliai peržiūri planą. Peržiūrimas kiekvienas žingsnis paeiliui tai užtikrina kad planuojamos veiklos yra gerai aprašytos plane. Šis scenarijus yra minimalus, ir leidžia komandoms susipažinti ir bendrauti.

Tikrinimų sąrašo testas. Šis metodas įgyvendinamas pateikiant plano kopijas visoms grupėms. Kiekviena grupė peržiūri planą ir pasižymi vietas, kurios susijusios su jų veikla.

Imitavimo testas. Plano veiklos ir palaikymo funkcijos išbandomos praktiškai. Kadangi tai imitacija šis testas yra vykdomas iki vietos kur reikėtų persikelti į kitą vietą ar pakeisti įrangą, kur reikėtų kito žingsnio.

Lygiagretus testas. Šis testas patvirtina plano pasirengimą veiksmui. Testo metu kritinės sistemos paleidžiamos alternatyvioje vietoje ir patikrinama ar viskas veikia kaip planuota. Visi nukrypimai nuo numatytos veikimo yra aprašomi ir taisomi.

Pilno pertraukimo testas. Šio testo metu veikla yra pilnai stabdoma. Visi veiksmai atliekami alternatyvioje vietoje, naudojant medžiagas kurios yra saugomos kitoje vietoje. Naudojamas personalas kuris yra priskirtas atstatymo komandoms.

6. Nustatyti numanomus testavimo rezultatus;

Norint įvertinti tęstinumo plano efektyvumą, testavimo rezultatus reikia lyginti su iš anksto nustatytais rezultatais. Taip galima įvertinti ar testas iš tikrųjų pasiekė norimus rezultatus.

7. Pratybos;

Parašyti veiklos tęstinumo tęstavimo planą. Jame turi būti nurodyti tikslūs žingsniai kaip įvykdyti testą, kokie žmonės ar departamentai dalyvaus ir tikėtini rezultatai.

8. Koordinuoti ir vykdyti testavimo planą;

Testo administratorius yra atsakingas už testavimo procedūrų koordinavimą bei testavimo rezultatų fiksavimą.

9. Rezultatų dokumentavimas;

Testavimo administratorius turi surinkti visus rezultatus ir paruošti galutinę ataskaitą. Tai bus naudojama vertinant ar testas veikia. Pastebėjimai bus naudojami planui koreguoti.

10. Rezultatų įvertinimas;

Ar rezultatai tokie kaip tikėtasi? Jei ne tai ką galima daryti kad jie tokie būtų. Ar tai priklauso nuo testavimo būdo?

11. Pristatyti rezultatus vadovybei;

Ataskaitą paruoštai taip kad vadovybei būtų lengvai suprantama, patartina pateikti grafikus,

lenteles, schemas.

12. Atnaujinti planą atsižvelgiant į rezultatus ir vadovo rekomendacijas;

Planas turi būti atnaujinamas ir peržiūrimas priklausomai nuo testavimo rezultatų ir vadovybės rekomendacijų. Testavimo rezultatai naudojami gerinant planą.

13. Koordinuoti plano palaikymą;

Nustatyti kaip dažnai reikia peržiūrėti, testuoti ir atnaujinti planą. Gera praktika planą peržiūrėti ir atnaujinti kas metus, nebent yra didelių pokyčių informacinėse sistemose.

14. Sukurti veiklos plano mokymo programą;

Turėti veiklos tęstinumo planą yra gerai, bet nepakankama jei darbuotojai nebus apmokyti kaip tuo planu naudotis atsitikus nelaimei. Reikia mokyti periodiškai, jei ir daromi dideli pakeitimai organizacijoje.

Plano tobulinimas ir atnaujinimas

Veiklos tęstinumo ir atkūrimo planą reikia atnaujinti pagal veiklos ar personalo pokyčius ir rastus neatitikimus tęstinumo metu.

Gera praktika yra atnaujinti planą kas metus. Yra situacijų kada planą reikia atnaujinti dažniau:

- kaip pasikeičia pagrindinė sistema, technologijos arba verslo procesai;
- kai padidėja priklausomumas nuo esamos ar naujos technologijos;
- organizacijos pertvarkymas, veiklos iškėlimas, personalo kaita, srities keitimas;
- jei klientai, priežiūros tarnybos, investitoriai, draudikai ar kreditoriai domisi tęstinumo planavimu;
- finansinės netektys, ankstesni įvykiai nulėmę finansinius nuostolius;
- prastovos, ankstesni įvykiai nulėmę sistemos prastovas;
- padidėję veiksniai (padidėjusi tikimybė ar poveikis);
- planas nebuvo atnaujintas ir testuotas per praeitus metus.

1. Pagal testavimo rezultatus nustatoma kokių reikia pakeitimų ar patobulinimų.

Testavimas turėtų nurodyti kokie yra plano trūkumai ar kas jame praleista. Ši informacija naudojama peržiūrint planą.

2. Planą atnaujinti reikia jei pakito kompiuterinės įrangos komponentai.

Planas atnaujinamas, kad būtų atsižvelgta į naujus organizacijos kompiuterinės ar programinės įrangos komponentus. Kai kuriais atvejais reikalingas ne planas pakeitimui, o jo testavimas.

3. Planą reikia atnaujinti jei pasikeitė ar atsirado naujos veiklos sistemos.

Kai organizacijoje pakeičiamas ar pašalinamas ar sukuriamas naujas kritinis veiklos procesas pagal tai keičiami planai.

4 etapas. Plano patvirtinimas ir įgyvendinimas

Kai planas yra sukurtas ir ištestuotas jį peržiūri ir patvirtina vadovybė. Tai užtikrina, kad planas

atitinka vadovybės veiklos tikslus. Kai planas yra patvirtintas jį reikia įgyvendinti organizacijoje.

1. Plano adekvatumo įvertinimas;

Vadovybė turi užtikrinti, kad planas atitinka organizacijos veiklos poreikius.

Tuo tikslu vadovybė nustato politikas, procedūras ir veiklos tęstinumo atsakomybes. Jei organizacija pasikliauja išorinėmis paslaugomis vadovybė taip pat turėtų įvertinti išorinių organizacijų veiklos tęstinumo planus bei suderinti jų atitikimą organizacijos reikmėms.

2. Vadovybės patvirtinimas bei plano pasirašymas;

Vadovybė turi patvirtinti bei pasirašyti veiklos tęstinumo ir atkūrimo planus. Ji turi juos peržiūrėti, palyginti gautus testavimo rezultatus su numatytais rezultatais tam, kad įsitikinti jog planai atitinka organizacijos tikslus bei lūkesčius.

3. Apmokyti darbuotojus pagal plano turinį ir tikslą;

Reikia nustatyti gyvenimiškus scenarijus siekiant ištestuoti plano dalis.. Testavimo atveju turėtų būti įvairių lygių tokių kaip padalinio ar visos organizacijos .

4. Peržiūrėti apmokymus;

Surengti bendrą susitikima su dalyviais, peržiūrėti kas veikia o kas ne. Pagal susitikimo rezultatus sudaryti veiksmų planą. Numatyti kada kas bus išspręsta.

5. Plano auditas

Periodiškai (patartina kas metus) peržiūrėti planą ir audituoti organizaciją siekiant užtikrinti, kad planas yra įgyvendintas:

- darbuotojų apmokymas yra tinkamas;
- nauji darbuotojai yra apmokyti;
- pagrindiniai darbuotojai turi pakeičiamumą.;
- pagrindinės prielaidos ir planą iššaukiantys įvykiai vis dar tokie kokie numatyti;
- peržiūrėtos ir atnaujintos grėsmės pažeidžiamumai;
- plano įgyvendinimo veiksmai kaip rezervinis kopijavimas atsargų pirkimas įrangos priežiūros yra vykdomi;
- vadovybė informuota apie atnaujinimus.

Kiekviena organizacija turi turėti veiklos tęstinumo planą, kuris turi užtikrinti, kad organizacijos informacinės sistemos yra pasiekiamos ir veikia kai reikalinga verslui ir jo plėtrai. Nežiūrint į visus įspėjimus ir atsargumo priemones, nenumatyti atvejai gali nutikti.

4.2.2. Pagrindinės veiklos tęstinumo plano klaidos

Organizacijų vadovams sunku patikėti, kad ir kaip gerai sukurtas planas darbuotojai elgdamiesi neapsieina be klaidų, dažniausios klaidos pasitaiko tokios:

Neapgalvotas pasitikėjimas veikos tęstinumo planu- daugelis organizacijų tiki, kad pakanka vien turėti veiklos tęstinumo planą ir to užteks idealiems veiklos procesams. Tačiau veiklos tęstinumo

planas yra tik minimaliai naudingas atitinkamai jo neatnaujinant, netestuojant ir nerengiant.

Ribotinos galimybės – veiklos tęstinumo plane ne viskas atsispindi ko reikia organizacijos atnaujinimui. Veiklos tęstinumo planas veiklos procesams reikalingas tik kaip priemonė kaip atlikti procesus, sistemos atnaujinimą, grąžinti veiklos funkcijas.

Prioritetų trūkumas – reikalinga nusistatyti pagrindinius veiklos procesus prioriteto tvarka. Nuo mažiausios rizikos iki didžiausios labiausiai lemiančios veiklos išlikimą.

Trūkumai atnaujinat planus – veiklos tęstinumo planas turi būti atnaujinamas periodiškai, ypatingai tada kai sistemų ir veiklos procesų esminiai pasikeitimai.

Bendravimo trūkumai – reikalingas švarus ir tikslus bendravimas su darbuotojais, prekiautojais, veiklos partneriais ir klientais.

Saugumo kontrolės trūkumai - per atkūrimo procesą apsaugos kontrolė gali būti ignoruojama, taip atsiranda didelė rizika.

Neišvengus kai kurių klaidų organizacijoje neapsieinama ir be nesėkmių, nenumatytų situacijų, grėsmių. Ką daryti kad taip nenutiktų? Reikalingas nuoseklus planas, kuris padeda susidaryti tarptautiniai standartai.

4.2.3. Kokią įtaka veiklai daro veiklos tęstinumo ir atkūrimo po nenumatyto atvejo planas?

Teikia naudą plėtojant ir vystant organizacijos valdymą.

Kokią įtaką verslui daro šis planas?

Leidžiama organizacijai išvengti tam tikrų rizikų arba mažinti neišvengiamus grėsmių poveikius:

- mažinant potencialias išlaidas;
- mažinant potencialius nuostolius;
- slopinti tikėtinus atvejus;
- pagerinti kompetenciją atnaujinant veiklos procesus.

Leidžia mažinti žlugimo tikimybę kritinėmis funkcijomis – procesas atnaujina greitai ir sėkmingai krizinėse situacijose. Taip slopinamas procesų žlugimas, užtikrinamas organizacijos stabilumas.

Tačiau nereikia tikėtis, kad turint susidarius veiksmų planą užteks lengvai valdyti organizacijos procesus ir funkcijas. Reikia apsisaugoti ir nuo kylančių pavojų dėl neapdairios veiklos tęstinumo plano klaidos.

Taigi, reikia susidaryti preliminarų planą, kurį sudarytų verslo poreikių įvertinimas, valdyti galimas rizikas, suplanuoti kas bus daroma įvykus tam tikram įvykiui, laiku atnaujinti tikrinti šiuos planus testuoti bei nepamiršti pasitvirtinti su aukščiausia vadovybę. Tam kad nuosekliai atlikti šiuos procesus reikia remtis tarptautiniu mastu pripažintais standartais, geromis praktikomis. Pagrindiniai jų yra CobIT metodika, tarptautinių rekomendacinių informacijos saugumo standartų grupė.

5.TARPTAUTINIAI SAUGUMO STANDARTAI

5.1. CobIT metodika

CobIT (Control objectives for information and related technologies) – Informacinių technologijų uždavinių, valdymo ir kontrolės gebėjimų organizacinis ugdymas strateginiame lygyje (toliau CobIT) orientuojasi į organizacijos veiklą, jos procesus, funkcijas. Metodikoje pateikiamos išsamios gairės skirtos ne tik vadovams bet taip pat darbuotojams, auditoriams, ir kitiems informacinių technologijų veiklos procesų savininkams. Vis daugiau organizavimo praktikoje įmonių savininkai įgauna pilną atsakomybę už visus veiklos procesus. Iš esmės tai apima tinkamos kontrolės užtikrinimą.

CobIT struktūra įmonės savininkui suteikia įrankį, kuris nurodo atsakomybių pasidalijimą, pareigų pasiskirstymą.

CobIT turi brandos lygio matavimo modelius naudojamus informacinių technologijų procesų matavimui, kad vadovybė galėtų nustatyti, kur organizacija yra šiandien, kokia jos pozicija lyginant su geriausiais rinkoje bei geriausiais standartais, ir kur organizacija nori būti rytoj. Kritinės sėkmės faktoriai (CSFs) nurodo svarbiausias įgyvendinimo gaires vadovybei, siekiant kontroliuoti informacinių technologijų procesus. Pagrindiniai tikslo indikatoriai (KGIs) teikia galimybę vadovams pasitikrinti ar informacinių technologijų procesas įvykdė veiklos reikalavimus.

CobIT pateikia kokios veiklos ir kokios funkcijos atliekamos įvertinant ir valdant informacinių technologijų rizikas. vieni atsakingi už savo veiklą, kiti atlieka tik informavimo arba aiškinimo funkcijas. Tačiau visa informacija labai naudinga analizuojant organizacijos veiklą ir saugant ją nuo netikėtų pavojų.

Norint teisingai diegti arba naudoti CobIT standarto modelį reikalinga nusistatyti kokia organizacijos dabartinė situacija, tam pateiksiu CobIT‘e esama brandos modelį.[15]

5.1.1. Brandos modelis

Prieš pradedant rizikos analizę, būtina įvertinti pačios organizacijos brandumą.

Organizacijos brandumas tai įgūdžių visuma, leidžianti efektyviai įgyvendinti procesus. Organizacijos brandumo modelio tikslas nustatyti organizacijos pajėgumą įgyvendinti procesus, planuoti tų procesų tobulumo būdus ir taikyti procesų įgyvendinimo priemones, atitinkančias jos brandumo lygį. Brandumo modelis patogus tuo, kad jį gali nusistatyti pati įmonė. Brandumo modelis apima penkis lygius.

0 neegzistuojantysis

Visiškas bet kokių procesų nebuvimas. Organizacija net nesuvokia, kad egzistuoja problema, kurią reikia spręsti. Politika(arba procesai) nėra parašyti, ir ankščiau organizacija nesuvokė veiklos

[15] Cobit 4.0 IT governance institute USA

rizikos, susijusios su tokiu rizikos valdymu. Todėl problema nebuvo svarstoma. Procesų ir veiklos sprendimų rizikos analizė neatliekama. Organizacija neįvertino saugos pažeidimų rizikų poveikio veiklai. Rizikos valdymas nebuvo identifikuotas kaip informacinių technologijų sprendimų įsigijimo ir informacinių technologijų tiekimo sudėtinė dalis.

1. pradinis ad/hots(kai nutinka tada ir sprendžiama)

Organizacija pripažino, kad problema egzistuoja ir ją reikia spręsti. Tačiau nėra standartizuotų procesų, yra tik ad/hots (specialūs) sprendimai, taikomi tam tikriems asmenims arba tam tikrais atvejais. Bendras požiūris į rizikos valdymą dezorganizuotas. Akivaizdu, kad kai kurie organizacijos nariai jau pripažino rizikos valdymo naudą. tačiau rizikos valdymas atliekamas ad/hots būdu. Nėra nei formaliai aprašytos politikos, nei procesų, procesai įgyvendinami nenuosekliai. Apskritai rizikos valdymo projektai atrodo chaotiški ir nekoordinuojami, o rezultatai nei įvertinamu nei audituojami. Organizacija suvokia savo teisinius ir sutartinius įsipareigojimus, bet tvarko informacinių technologijų riziką ad/hots būdu, neturėdama įvardintos politikos ir procesų. Neformali projektų rizikos analizė atliekama kiekvienam projektui atskirai ir kiekvieną kartą savaip. Rizikos analizė nėra išskiriama projekto plane ir nėra pavedama konkretiems projekte dalyvaujantiems vadovams. Informacinių technologijų vadovybė nenurodo atsakomybės už rizikos valdymą pareiginiais nuostatais ir išsamiau neaiškina jos kitokiais būdais. Specifinė informacinių technologijų rizika, tokia, kaip slaptumas, prieinamumas ir vientisumas, kartais analizuojama kiekvieno konkretaus projekto atveju. Informacinių technologijų rizika, veikianti kasdien darbines operacijas, kartais aptariama vadovybės susirinkimuose, ten kur rizikos buvo pastebėtos ir svarstomos rizikos mažinimas yra nepakankamas. Kyla supratimas, kad informacinių technologijų rizikos yra svarbios ir turi būti svarstomos.

2. Kartojamas bet intuityvus.

Procesai išplėtoti tokiu lygiu, kad skirtingi žmonės, atliekantys identiškas užduotis, laikosi panašių procedūrų. Formalūs mokymai ir informavimas apie standartines procedūras nėra organizuojami, o atsakomybė paliekama kiekvienam asmeniui atskirai, kai kurių asmenų žiniomis labai pasitikima, todėl galimos klaidos. Rizikos valdymas suvokiamas visos organizacijos mastu. Rizikos valdymo procesas kartotinis, bet nebrandus. Procesas visiškai neaprašytas, tačiau veikla vykdoma reguliariai, ir organizacija siekia sukurti visapusį rizikos valdymo procesą, į kurį būtų įtraukta ir jos aukščiausioji vadovybė. Formalūs rizikos valdymo mokymai arba informavimas apie rizikos valdymo procesus nevykdomi, atsakomybė už jų įgyvendinimą paliekama tam tikriems darbuotojams. Didėja supratimas, kad informacinėse technologijose rizika yra svarbi ir kad į ją reikia atsižvelgti. Egzistuoja tam tikra rizikos analizė, tačiau procesas tebėra nebrandus – jis vis dar vystymosi stadijoje. Rizikos analizė paprastai atliekama aukščiausiu organizaciniu lygiu ir taikoma tik svarbiausiems projektams. Vykdomų operacijų analizė paprastai priklauso tik nuo to, ar informacinių technologijų vadovai pasistengia įtraukti šį klausimą į darbotvarkę, o jie tai daro dažniausiai tik iškilus

problemai. Bendrai informacinių technologijų vadovai nėra nustatę procedūrų ar pareiginių instrukcijų, formaliai sisteminančių rizikos valdymą.

3. Apibrėžtas

Rizikos vertinimas ir valdymas yra standartinės procedūros. Jos aprašytos, o darbuotojai supažindinami su jomis mokymų metu. Tačiau šių procedūrų laikymasis paliktas darbuotojų nuožiūrai, ir nukrypimų fiksavimas mažai tikėtinas. Pačios procedūros nėra išplėtotos, jos tiesiog formalizuoja esančią praktiką. organizacija priėmusi formalų sprendimą imtis rizikos valdymo ir įgyvendinti savo informacijos saugos programą. Pamatiniai procesai sukurti, jie turi aiškiai apibrėžtus tikslus, taip pat apima procedūras, leidžiančias juos pasiekti ir įvertinti procesų sėkmingumą. Be to, tam tikri rudimentiniai rizikos valdymo mokymai rengiami visam personalui. Pagaliau organizacija aktyviai įgyvendina formaliai aprašytus rizikos valdymo procesus. Rizikos valdymo politika, taikoma visai organizacijai, nustato, kada ir kaip reikia atlikti rizikos analizę. Rizikos analizė vykdoma, laikantis nustatytų procedūrų, kurios yra aprašytos ir su kuriomis darbuotojai buvo supažindinti mokymų metu. Sprendimą dėl procedūrinių reikalavimų laikymosi ir dalyvavimo mokymuose priima kiekvienas darbuotojas savo nuožiūra. Metodologija yra darni ir veiksminga, užtikrinanti, kad pagrindiniai veiklos rizikos tipai bus nustatyti. Procedūrinių reikalavimų laikymasis paliktas atskiro informacinių technologijų vadovo nuožiūrai, nėra procedūros, užtikrinančios, kad rizikos analizė bus atliekama kiekvieno projekto atveju, ir kad jau vykdomos operacijos bus reguliariai įvertinamos rizikos požiūriu.

4. Valdomas ir matuojamas

Galima prižiūrėti ir kontroliuoti procedūrų laikymąsi, taip pat imtis veiksmų, paaiškėjus, kad procesas nėra pakankamai efektyvus. Procesai nuolat tobulinami, atsižvelgiant į pasiteisinusią praktiką. Automatizacija ir techninės priemonės naudojami ribotai arba fragmentiškai, Visuose organizacijos lygiuose egzistuoja išsamus rizikos valdymo supratimas. Rizikos valdymo procedūros sukurtos, procesas yra aiškiai apibrėžtas, plačiai skatinamas sąmoningumas, rengiami privalomi mokymai, taip pat egzistuoja kai kurios pradinės priemonės, leidžiančios įvertinti sėkmingumą. Rizikos valdymo programai skirti pakankami ištekliai. Daugelis organizacijos padalinių jau patyrė jos naudingumą, o saugos rizikos valdymo grupė pajėgi nuolat tobulinti procesus ir priemones. Naudojamos kai kurios technologinės rizikos valdymo priemonės, tačiau dauguma, jei ne visos rizikos analizės, kontrolės, identifikavimo ir kaštų-naudos analizės procedūros atliekamos rankiniu būdu. Rizikos analizė yra standartinė procedūra, ir jos nesilaikymo atvejus gali pastebėti informacinių technologijų vadovai. Tikėtina, kad informacinėse technologijose rizikos valdymas yra formalizuota aukščiausio lygio vadovybės funkcija. Procesas išplėtotas, rizika analizuojama tiek tam tikro projekto lygiu, tiek reguliariai visos informacinės sistemos požiūriu. Vadovybė informuojama apie informacinių technologijų aplinkos pokyčius, galinčius iš esmės paveikti rizikos scenarijus, tokius kaip padidintas duomenų tinklo pavojus arba techniniai sprendimai, darantys įtaka informacinių sistemų strategijos

vidinei logikai. vadovybė pajėgi prižiūrėti rizikos situaciją ir priimti pagrįstus sprendimus dėl rizikos lygio priimtinumo. Aukščiausioji vadovybė ir informacinių technologijų vadovai yra nusistatę organizacijos toleruojama rizikos lygį ir turi standartines priemones rizikos ir rezultatų santykiui įvertinti. Vadovybė skiria biudžetinių lėšų operacinės rizikos analizės projektams, kurie leidžia reguliariai pervertinti riziką. Yra sukurta rizikos valdymo duomenų bazė.

5. Optimizuotas

Procesai ištobulinti iki geriausios praktikos lygio, remiantis nuolatinio tobulinimo rezultatais ir brandumo modeliavimu kartu su kitomis organizacijomis. Informacinės technologijos nuosekliai naudojamos darbui automatizuoti, jos teikia kokybės ir efektyvumo gerinimo priemones ir leidžia įmonei greitai prie jų prisitaikyti. Organizacija saugos rizikos valdymui skiria pakankamai lėšų, o darbuotojai siekia užtikrinti, kad problemos ir jų sprendimai būtų numatomi prieš kelis mėnesius ir metus. Rizikos valdymo procesas gerai įsimintinas ir maksimaliai automatizuotas, pasitelkus atitinkamas priemones. Nustatoma kiekvieno saugos įvykio pirminė priežastis ir imamasi tinkamų veiksmų, leidžiančių išvengti jo pasikartojimo. Darbuotojams rengiami įvairūs kvalifikacinio lygio mokymai. Rizikos analizė išplėtota tokiu lygiu, kad visos organizacijos mastu yra įgyvendinamas struktūrinis, reguliariai prižiūrimas ir gerai valdomas procesas. Pasitelkus specialistus, kolektyvinis rizikos svarstymas ir pirminių priežasčių analizė atliekami visoje organizacijoje. Rizikos valdymo duomenų fiksavimas, analizavimas ir pranešimas gerai automatizuotas. Specialistai parengę instrukcijas, o informacinių technologijų organizacija dalyvauja patirties keitimosi grupių darbe. Rizikos valdymas realiai integruotas į visą organizacijos veiklą ir informacinių technologijų operacijas, jį pripažįsta ir jame plačiai dalyvauja informacinių technologijų paslaugų vartotojai.

Brandumo lygį lemia trys pagrindiniai veiksniai – žmonių kompetencija, organizacija ir taikomos technologijos. Tik nustačius brandumo lygį, galima identifikuoti tinkamus rizikos analizės metodus. Kuo žemesnis brandumo lygis, tuo paprastesni rizikos analizės metodai turėtų būti taikomi.[16]

5.1.2. Aukščiausias lygis - objektų kontrolė

Norint pasiekti užsibrėžtų uždavinių, organizacijoje privaloma atlikti stebėjimą kaip vyksta procesai. Tam reikalinga dalinė arba pilna kontrolė, tai priklauso nuo situacijos.

Šiuo atveju nagrinėjama situacija ko galima tikėtis organizacijos veikloje jei staiga užklups netikėti atvejai. Kadangi tikimasi išvengti nepageidaujamų situacijų, pirmiausia reikia apžvelgti ką siūlo CobIT metodika, kad taip neatsitiktų.

Pirmiausia reikia

Įvertinti – valdyti IT rizikas.

Reikalinga sukurti ir palaikyti rizikos struktūrą. Jos dokumentas - tai bendrai priimtinas

[16] Rizikos analizės vadovas. [interaktyvus]. Vilnius: Vidaus reikalų ministerija - 2006. [žiūrėta balandžio 3d.] Prieiga per internetą <http://www.vrm.lt/fileadmin/Padaliniu_failai/Informacines_politikos_dep/IT_sauga/Rizikos_analize.pdf, (16-21 psl.)

informacinių technologijų rizikos lygis, rizikų mažinimo strategijos priimtos pagal liekamąsias rizikas (tai su verslu susitartos kokios priimtinos liekamosios rizikos).

Bet koks potencialus poveikis organizacijos tikslams, sukeltas nenumatyto įvykio, turi būti identifikuotas, išanalizuotas ir įvertintas.

Rizikos mažinimo strategijos turi būti pritaikytos sumažinti liekamąją riziką iki priimtino lygio. Įvertinimo rezultatas turi būti suprantamas akcininkams ir išreikštas finansiškai, kad akcininkai galėtų nustatyti rizikoms tinkamą toleranciją (pakantumas).

Antra informacinių technologijų procesų kontrolė

Tai tenkina veiklos reikalavimus informacinių technologijų srityje, analizuojant ir komunikuojant informacinių technologijų rizikas ir jų galimą poveikį veiklos procesams ir tikslams.

Tai susitelkiama į rizikos valdymo struktūros kūrimą, kuris integruotas į verslą ir darbinės rizikos valdymo struktūrą, rizikos vertinimą, rizikos sumažinimo ir komunikavimo liekamąją riziką.

Tai pasiekiama naudojantis tokiais uždaviniais:

- užtikrinti, kad rizikos valdymas yra pilnai įgyvendintas valdymo procesuose;
- įgyvendinti rizikos įvertinimus;
- siūlyti veiksmų planą kaip aplenkti rizikas.

Ir rizikos procesų vertinimas pagal:

- procentas nuo visų kritinių objektų, kurie įvertinti rizikos vertinimu;
- procentas nuo visų identifikuotų kritinių informacinių technologijų rizikų su sukurtais veiksmų planais;
- procentas nuo visų rizikos valdymo veiksmų planų patvirtintų įgyvendinimu.

5.1.3. Informacinių technologijų ir veiklos rizikos valdymo reguliavimas.

Integruoti informacinių technologijų valdymą, rizikos valdymo struktūra su organizacijos valdymo struktūra. Tai yra reguliavimas organizacijos rizikos apetitas ir rizikos tolerancijos lygis.

- rizikos situacijos nustatymas;
- įvykių identifikavimas;
- rizikos įvertinimo metodika;
- rizikos atsakymas;
- palaikymo ir tikrinimo rizikos veiksmų planas.

5.1.4. Pakeitimų valdymas

1. Pakeitimų inicijavimas ir valdymas Pakeitimai turi būti valdomi. Vadinasi, jie turi būti visiems žinomi ir matomi. Reikalinga vieninga procedūra, kaip jie atliekami;
2. Poveikio įvertinimas;
3. Pakeitimai turi būti suderinti su konfigūracijos valdymu;
4. Skubūs pakeitimai – sąlygos procedūros;

5. Dokumentacija ir procedūros;
6. Pakeitimų valdymą reikia stebėti / tikrinti;
7. Išleidimo tvarka;
8. Pakeitimų išplatinimas.

5.1.5. Veiklos tęstinumo užtikrinimas

1. Tęstinumo modelio sudarymas
2. Tęstinumo planas
3. Plano struktūra
    a. plano vykdytojai
    b. reakcijos ir atsakymo procedūros
    c. bendravimo procedūros
4. Informacinių technologijų veiklos tęstinumo reikalavimų minimizavimas
5. Informacinių technologijų veiklos tęstinumo plano palaikymas
6. Tęstinumo plano testavimas
7. Tęstinumo plano mokymai
8. Plano platinimas
9. Kritinių resursų identifikavimas

Bendram supratimui kas, kokias veiklas ir kokias funkcijas atlieka įvertinant ir valdant informacinių technologijų rizikas, pateikiama 4 lentelėje.

Veiklos ir funkcijos atliekamos įvertinant ir valdant informacinių technologijų rizikų matrica

4 lentelė

Veiklos /funkcijos	CEO Aukščiausias vadovas	CFO Finansų vadovas	Veiklos vadovas	CIO Aukščiausias informacijos vadovas	Veiklos vyresnysis vadybininkas	Procesų vadovas	Informacinių technologijų administravimo vadovas	Auditas
Nulemia rizikos valdymo reguliavimą	Aiškina	Atsako ir aiškina	Konsultuoja	Konsultuoja	Atsako ir aiškina	Informuoja		Informuoja
Svarbiausių strateginio veiklos objektų supratimas		Konsultuoja	Konsultuoja		Konsultuoja	Konsultuoja		Informuoja
Svarbiausių veiklos procesų objektų supratimas				Konsultuoja				Informuoja
Įvertinti rizikas susijusias su įvykiais			Aiškina	Konsultuoja	Atsako	Atsako		Konsultuoja
Įvertinti rizikos atsakomybę	Informuoja	Aiškina	Aiškina	Aiškina	Atsako	Atsako		Konsultuoja
Pateikti pagal svarbą ir planą kontroliuojamas veiklas	Konsultuoja	Aiškina	Aiškina	Informuoja	Informuoja	Informuoja		Informuoja
Palaikymo ir tikrinimo rizikos veiksmų planas	Aiškina	Konsultuoja		Atsako	Atsako	Konsultuoja	Konsultuoja	Atsako

5.2. Informacijos saugos standartų grupė ISO 27000

5.2.1. Veiklos tęstinumo valdymo informacijos saugumo aspektai

Tikslas: neutralizuoti veiklos pertrūkius ir apsaugoti svarbiausius veiklos procesus nuo didesnių informacijos sistemų gedimų arba nelaimių padarinių bei užtikrinti savalaikį veiklos atnaujinimą.

1. Informacijos saugumo įtraukimas į veiklos tęstinumo procesą

Turi būti numatytos ir išlaikytos visos organizacijos atžvilgiu taikomos veiklos tęstinumo procedūros, atsižvelgiant į informacijos saugumo reikalavimus organizacijos veiklos tęstinumui.

2. Veiklos tęstinumas ir rizikos vertinimas

Privaloma nustatyti įvykius, kurie gali lemti veiklos pertrūkius, įvertinti šių įvykių galimybę ir poveikį bei padarinius informacijos saugumui.

3. Tęstinių planų, apimančių informacijos saugumą, sudarymas ir įgyvendinimas

Siekiant išlaikyti arba atkurti vykdomas operacijas ir užtikrinti reikiamo lygio ir per numatytą laiko tarpą teikiamos informacijos parengtumą, svarbios veiklos pertrūkio arba klaidos atveju, turi būti parengti ir įgyvendinti tęstiniai planai.

4. Veiklos tęstinumo planavimo struktūra

Siekiant užtikrinti visų planų suderinamumą, nuoseklų informacijos saugumo reikalavimų taikymą ir identifikuoti testavimo bei priežiūros prioritetus, turi būti išlaikoma vieninga veiklos tęstinumo planavimo struktūra.

5. Komercinės veiklos tęstinumo planų testavimas, priežiūra ir koregavimas

Siekiant užtikrinti, kad veiklos tęstinumo planai būtų efektyvūs ir atitiktų esamą padėtį, jie turi būti periodiškai testuojami ir atnaujinami.

5.2.2. Informacijos saugumo incidentų valdymas ir tobulinimas

Tikslas: užtikrinti, kad apie informacijos sistemomis susijusius informacijos saugumo įvykius ir silpnąsias vietas būtų pranešta laiku ir būtų galima imtis atsakomųjų veiksmų.

1. Pranešimai apie informacijos saugumo įvykius

Apie informacijos saugumo įvykius turi būti pranešta kiek įmanomai greičiau, pasitelkus tinkamus valdymo kanalus.

2. Pranešimai apie saugumo silpnąsias vietas

Reikalaujama, kad visi darbuotojai, rangovai ir trečiosios šalies atstovai, besinaudojantys informacijos sistemomis ir paslaugomis, Atkreiptų dėmesį į visas esamas ar galimas sistemos arba paslaugos saugumo silpnąsias vietas ir apie jas praneštų vadovams.

3. Atsakomybės ir procedūros

Siekiant užtikrinti greita, efektyvų ir deramą atsaką į informacijos saugumo incidentus, turi būti numatytos valdymo atsakomybės ir procedūros.

4. Mokymasis iš informacijos saugumo incidentų

Turi būti taikomi mechanizmai, užtikrinantys, kad informacijos saugumo incidentų tipai, dydžiai ir susijusios išlaidos yra apskaičiuojami ir stebimi.

5. Įrodymų rinkimas

Tais atvejais, kai informacijos saugumo incidentas asmens ar organizacijos atžvilgiu gali turėti teisinių pasekmių, turi būti renkami ir išsaugomi įrodymai bei pateikiami atitinkamos žinyboms pagal visas atitinkamas jurisdikcijos numatytas taisykles.

5.2.3. Tarptautinis rekomendacinis informacijos saugumo standartas ISO 17799

Tikslas: neutralizuoti veiklos trukdymus bei apsaugoti svarbiausius veiklos procesus nuo didesnių nesėkmių ar nelaimių.

Veiklos tęstinumo valdymo procesas turėtų būti įdiegtas siekiant sumažinti veiklos žlugimą sukeliančius veiksnius, kaip netikėtos nelaimės, nelaimingi įvykiai, įrengimų gedimai bei tyčiniai kenkimai iki priimtino lygmens panaudojant prevencinio ir atkuriamojo reguliavimo derinį.

Reikia analizuoti nelaimių, saugos sutrikimų padarinius ir aptarnavimo nuostolius. Reikia sukurti nenumatytų trikdžių planus ir juos įdiegti, kad veiklos procesus būtų galima atstatyti per reikiamą, tinkamą laiką. Toks planas turėtų būti naudiojamas ir palaikomas nuolat, kad taptų visų kitų valdymo procesų neatsiejama dalimi.

Į veiklos tęstinumo valdymą reikia įtraukti reguliatorius, kurie gali nustatyti ir sumažinti riziką, apriboti žalą sukeliančių avarijų padarinius ir užtikrintų savalaikį pagrindinių veikimo procesų atnaujinimą.

5.2.4. Veiklos tęstinumo valdymo procesas

Reikia parengti valdomą procesą, kad būtų palaikomas veiklos tęstinumas visoje organizacijoje. Turi būti apjungiami tokie pagrindiniai, svarbiausieji elementai:

- rizikos, su kuria gali susidurti organizacija, suvokimas ir supratimas atsižvelgiant į tokių veiksnių galimumą ir poveikį, įskaitant ir kritinių veiklos procesų nustatymą bei prioritetų išskyrimą;
- supratimą, kokie trikdžiai gali turėti didžiausią poveikį verslui (svarbu surasti sprendimus, pažabojančius smulkesnes avarijas, nelaimingus atsitikimus, taip pat rimtus avarinius gedimus, rimtas grėsmes organizacijos pagrindinei veiklai), nustatyti veiklos tikslus informacijos tvarkymo priemonėms;
- apsvarstyti tinkamo draudimo pirkimą, kuris gali suformuoti veiklos tęstinumo proceso dalį;
- formuoti ir dokumentuoti veiklos tęstinumo strategiją atitinkančią sutartus veiklos tikslus ir prioritetus;
- formuluoti ir dokumentuoti veiklos tęstinumo planus pagal sutartą strategiją;
- diegti reguliarų planų ir procesų tikrinimą, testavimą ir atnaujinimą;

- užtikrinti, kad veiklos tęstinumo valdymas būtų įtrauktas į organizacijos procesus ir struktūrą. Atsakomybė už veiklos tęstinumo valdymo proceso koordinavimą turi būti priskirta atitinkamu organizacijos vidaus lygiu, t.y. informacijos saugos forume.

5.2.5. Veiklos tęstinumas ir poveikio (veiksnių įtakos) analizė

Veiklos tęstinumą privaloma pradėti nuo įvykių, galinčių sukelti sutrikimus veiklos procesams nustatymo, t.y. įrengimų sutrikimai, gedimai, potvynis ar ugnis. Toliau reikia įvertinti riziką ir apibrėžti tokių sutrikimų poveikį (tiek atsižvelgiant į žalos dydį apimtį tiek ir į atstatymo (atkūrimo) laiką). Abu šios veiklos etapai turi būti vykdomi naudojant veiklos savininkų išteklius ir procesus. Šis įvertinimas turi apimti visus veiklos procesus ir neapsiriboti informacijos tvarkymo priemonėmis.

Priklausomai nuo rizikos įvertinimo rezultatų, turi būti parengtas strategijos planas, atspindintis bendrą veiklos tęstinumo metodą. Kai tik toks planas yra sukuriamas, jį reikia pagrįsti valdymu.

5.2.6. Veiklos tęstinumas ir rizikos valdymas

Kai nustatomi įvykiai, galintys lemti veiklos pertrūkius, įvertinamą šių įvykių galimybė ir poveikis bei jų padariniai informacijos saugumui.

Įgyvendinimo rekomendacijos

Veiklos tęstinumo informacijos saugumo aspektai turėtų būti grindžiami įvykių ar jų sekos, galinčių sukelti organizacijos veiklos pertrūkius, nustatymu, pavyzdžiui gali būti įrangos gedimas, žmogiškosios klaidos, vagystė, gaisras, gamtos nelaimės ar teroristiniai išpuoliai. Be to, siekiant nustatyti tokių pertrūkių galimybę bei poveikį sugaišto laiko, padarytos žalos ir atkūrimo trukmės atžvilgiu, turėtų būti atliekas rizikos vertinimas.

Atliekant veiklos tęstinumo rizikos vertinimus turėtų dalyvauti visi veiklos išteklių ir procesų valdytojai. Vertinant turėtų būti atsižvelgiama į visus veiklos procesus ir nederėtų apsiriboti vien informacijos apdorojimo priemonių vertinimu, tačiau reikėtų atsižvelgti ir į visus su informacijos saugumu susijusius aspektus. Siekiant pilnutinai nustatyti organizacijos veiklos tęstinumo reikalavimus, svarbu įvertinti skirtingų rizikos aspektų tarpusavio ryšius. Atliekant vertinimą, rizikos turėtų būti nustatytos, apskaičiuotos bei išdėstytos pagal grėsmių lygį ir tai turėtų būti daroma atsižvelgiant į organizacijos specifiką atitinkančius kriterijus bei tikslus, kaip svarbiausius išteklius, pertrūkio poveikį, didžiausią galimą prastovos trukmę ir atkūrimo prioritetus.

5.2.7. Tęstinumo planų rašymas ir įdiegimas

Planai turi būti kuriami tam, kad būtų palaikomos arba atstatomos veiklos operacijos, per reikalaujamą laiką, atsiradus svarbiausių veiklos procesų trikdžiams ar gedimams. Planuojant veiklos tęstinumo procesus turi būti atsižvelgta į:

- nustatymą ir darną (suderinimą) visų atsakomybių ir avarinių procedūrų;
- nustatytas priimtinas informacijos ar paslaugų praradimo lygis;
- įgyvendintos nepaprastosios padėties procedūros, kad būtų užtikrintas atkūrimas ir atstatymas

procesų per reikiamą laikotarpį. Ypatingas dėmesys turi būti kreipiamas į išorinių veiklos priklausomybės veiksnių įvertinimą ir sutarčių būvimą;

- numatytos operacinės procedūros, kurių reikia laikytis kol bus visiškai atlikti atkūrimo darbai;
- sutartų procedūrų ir procesų dokumentavimą;
- tinkamą personalo parengimą, apmokymą pagal sutartą avarinių procedūrų ir procesų planą bei krizių valdymą;
- planų testavimą ir atnaujinimą.

Planavimo procesas turi būti kreipiamas į reikiamus veiklos tikslus, t.y. į konkrečių paslaugų klientams atkūrimą per priimtiną laiką. Turi būti apsvarstytos pastangos ir šaltiniai, kurie galėtų sąlygoti atkūrimą, įskaitant personalo atranką, ne informacijos tvarkymo išteklius, o taip pat gedimų neutralizavimo (atsarginio varianto) pasiruošimas informacijos tvarkymo priemonėms.

5.2.8. Veiklos tęstinumo planavimo struktūra

Turi būti palaikoma vieninga veiklos tęstinumo planų struktūra, siekiant užtikrinti, kad visi planai būtų nuoseklūs, suderinti bei nustatyti testavimo ir priežiūros prioritetus. Kiekvienas veiklos tęstinumo planas turi aiškiai įvardyti jo aktyvavimo sąlygas, o taip pat asmenis atsakingus už kiekvieno plano elemento vykdymą. Nustatant naujus reikalavimus, reikia atitinkamai pakeisti ir suderinti avarijos procedūras, t.y. evakuacijos planus ar pasirengimus gedimų neutralizavimui.

Veiklos tęstinumo planavimo struktūroje reikia atsižvelgti į:

- planų, apibūdinančių kokių reikia imtis veiksmų aktyvavimo sąlygas (kaip įvertinti situaciją, kas yra įtrauktas, kt.) prieš aktyvuojant kiekvieną planą;
- avarijos procedūras, apibūdinančias, kokių reikia imtis veiksmų įvykiui pažaboti, kuris kelia grėsmę veiklos operacijoms arba žmonių gyvybei. Tai apima pasiruošimą viešiesiems ryšiams valdyti ir efektyvius ryšius su valstybinėmis institucijomis, t.y. policija, ugniagesiais ir vietos valdžios pareigūnais;
- gedimų neutralizavimo procedūras (tvarką), nustatančias kokių reikia imtis veiksmų perkelti svarbiausius veiklos veikimo procesus arba palaikyti tarnybas bei perkelti į laikinas vietas, bei atnaujinti veiklos operacijas per tinkamiausią laiką;
- atnaujinimo procedūras, kurios nustato kokių reikia imtis veiksmų grįžtant į normalų veiklos operacijų ritmą.
- palaikymo grafiką, nustatantį kaip ir kada planas bus tikrinamas, testuojamas ir plano palaikymo procesas;
- informuotumą ir švietimo veiklą, skirtą sukurti veiklos tęstinumo procesų sampratai bei užtikrinti, kad procesai būtų efektyvūs;
- individų atsakomybę, apibūdinančią, kas konkrečiai yra atsakingas už plano dalių vykdymą. Turėtų būti išvardytos ir alternatyvos kaip reikalaujama;

- svarbiausias turtas ir ištekliai, kurių reikia siekiant pritaikyti avarines, atsarginių priemonių ar atkūrimo procedūrų;
- supratimo, švietimo ir mokymo veikla skirta veiklos tęstinumo supratimui ir jo veiksmingumui užtikrinti.

Kiekvienas planas turėtų turėti atskirą savininką (valdytoją). Avarijų procedūros (avarijų įveikimo tvarka), rankų darbo gedimų neutralizavimo planai ir procesų atnaujinimo planai turi būti priskirti valdytojų atsakomybei iš atitinkamų veiklos išteklių ar susijusių procesų. Gedimų įveikimo pasirengimai kaip alternatyvi techninė priežiūra, kaip informacijos tvarkymas ir komunikacijų įrengimai, turi būti priskirti paslaugų teikėjų atsakomybei.

5.2.9. Veiklos tęstinumo planų testavimas, priežiūra ir įvertinimo atnaujinimas

Planų testavimas

Veiklos tęstinumo planų testavimas gali nepavykti, dažnai dėl neteisingų prielaidų, apsirikimų, įrengimų ar personalo kaitos. Todėl jie turi būti nuolat testuojami, kad būtų užtikrintas jų atnaujinimas ir efektyvumas. Tokie testai taip pat turėtų užtikrinti, kad visi atnaujinimo komandos nariai ir kitas susijęs personalas žinotų apie planus.

Veiklos tęstinumo plano testavimo grafikas turi parodyti kaip ir kada kiekvienas plano elementas turi būti testuojamas. Rekomenduojama dažnai testuoti atskiras jo dalis. Tam tikslui taikoma įvairi metodika, testavimo būdai siekiant įsitikinti, kad jie praktiškai bus įgyvendinami ir veiks. Tai turi apimti pristatytus įvairius scenarijus; išgalvotus pavyzdžius; techninio atkūrimo testavimas; atkūrimo testavimas alternatyvioje vietoje; testavimas tiekimo priemonių ir paslaugų; atlikti repeticijas.

Šiuos metodus gali naudoti bet kokia organizacija ir jie turi atspindėti konkretaus atstatymo plano pobūdį.

Planų kontroliavimas priežiūra ir persvarstymas

Veiklos tęstinumo planai turi būti peržiūrimi nuolat, ir atnaujinami, siekiant, kad jie būtų veiksmingi. Į organizacijos keitimo valdymo programą reikia įtraukti procedūras, užtikrinant kad veiklos tęstinumo reikalais bus tinkamai rūpinamasi.

Kiekvieno veiklos tęstinumo plano atsakomybė turi būti paskirstyta nuolatiniams patikrinimams, apžvalgoms. Keitimo nustatymas veiklos pertvarkymuose dar neįtrauktas į veiklos tęstinumo planus turi būti įgyvendintas atitinkamai planą atnaujinus. Šis formalus keitimas kontrolės procese turėtų užtikrinti kad atnaujinti planai būtų paskirstyti paskleisti ir pastiprinti nuolat vykstančiomis viso plano apžvalgomis.

Turėtų būti taikoma daugelis metodų, diegiant įsitikinti, kad planas bus realiai įvykdytas. Turėtų būti numatyta:

1. neformalus įvairių scenarijų tikrinimas (veiklos atkūrimo veiksmų aptarimas, pasitelkiant

pertrūkių pavyzdžius);

2. imitavimas (ypač mokant žmones, kaip elgtis įvykus incidentui ar krizei);

3. techninio atkūrimo tikrinimas įsitikinant, kad informacijos sistemos gali būti veiksmingai atkurtos;

4. atkūrimo tikrinimas alternatyviojoje darbo vietoje (vykdant veiklą ir atkuriant vykdytas operacijas ne pagrindinėje darbo vietoje);

5. tiekėjo įrangos ir priemonių tikrinimas (įsitikinant, kad iš išorės teikiamos paslaugos ir produktai atitinka sutarties įsipareigojimus);

6. nuodugnus pasirengimas (tikrinimas siekiant nustatyti, ar organizacija, personalas, įranga, priemonės ir procedūros gali susidoroti su pertrūkiais).

Šiuos metodus gali pasitelkti bet kuri organizacija. Jie turėtų būti taikomi atsižvelgiant į konkrečių atkūrimo planų specifiką. Tikrinimo rezultatai turėtų būti registruojami ir, esant reikalui, turėtų būti imtasi atitinkamų veiksmų planams pagerinti.

Kiekvieną veiklos tęstinumo planą nuolat turėtų peržiūrėti paskirtas atsakingas asmuo. Jei nustatomi veiklos pokyčiai, į kuriuos veiklos tęstinumo planuose nėra atsižvelgta, šie planai turėtų būti atitinkamai atnaujinami. Oficialios pakyčių valdymo procedūros turėtų užtikrinti, kad atnaujinti planai būtų išplatinami ir nuolat tobulinami atsižvelgiant į bendrojo plano peržiūrų rezultatus

Situacijų pavyzdžiai, planų atnaujinimas, skatinamas kai nauji įrenginiai įsigyjami arba patobulinamos veikiančios sistemos ir įvyksta pasikeitimai:

- personalo;
- adresų ar telefonų numerių;
- veiklos strategijos;
- įrengimų ir išteklių vietos;
- įstatymų leidybos;
- rangovų, tiekėjų ir pagrindinių klientų;
- procesuose, arba atsiranda nauji/ atšaukiami seni;
- rizikos (operacijų ir finansinės).[17]

[17] International Standard ISO/IEC 17799, ISO copyrigt office Switzerland, 2000

5.3. Tarptautinis IT paslaugų standartas ISO 20000

Paslaugų tęstinumas ir pasiekiamumo valdymas.

Tikslas: Užtikrinti kad sutarti paslaugų tęstinumo ir pasiekiamumo įsipareigojimai klientams būtų vykdomi įvairiomis aplinkybėmis.

Esmė: paslaugų tęstinumo ir paslaugų reikalavimai turi būti nustatyti klientų paslaugos prioritetais, aptarnavimo lygio susitarimais ir įvertinta rizika. Paslaugų tiekėjas turi prižiūrėti pakankamą paslaugų pajėgumą, kartu su veikiančiais planais sukurtais taip, kad užtikrinti sutartus reikalavimus esant bet kokioms aplinkybėms apimančioms nuo normalaus lygio iki visiško paslaugos žlugimo. Paslaugų tiekėjas turi planuoti žinomus duomenų naudojimo kiekio padidėjimus ar sumažėjimus, tikėtinus trūkius ar pertrūkius darbų krūvyje ar kitokius žinomus ateities pokyčius. Reikalavimuose turi būti pasiekiamumo teisės, reagavimo reakcijos laikai, taip pat sistemos komponentų pasiekiamumas. Paslaugų prieinamumo ir paslaugų tęstinumo planai turi veikti informacines technologijas kartu taip, kad užtikrinti sutartus paslaugų lygius. Šie reikalavimai turi įtakoti veiksmus, pastangas ir resursus skirtus atitikti paslaugų pasiekiamumui. Procesai skirti užtikrinti tinkamą pasiekiamumą yra palaikomi ir turi turėti šiuos paslaugų teikimo elementus, kurie yra valdomi kliento ar kito paslaugų tiekėjo.[18]

[18] International Standard ISO/IEC 20000, ISO copyrigt office Switzerland, 2005

5.4. CobIT ir tarptautinių saugumo standartų grupių panašumai ir skirtumai

Analizei pateikiu palyginti ką siūlo daryti CobIT metodika ir tarptautinių saugumo standartų grupė, kai atsitinka nenumatytas atvejis, kokius reikėtų organizacijai priimti sprendimus, kad ištaisyti esamas klaidas arba užkirsti kelią būsimai krizei

Tarptautinių saugumo standartų panašumai ir skirtumai

5 lentelė

CobIT metodika	Tarptautinių saugumo standartų grupė
Veiklos rizikos įvertinimas	
Rizikos vertinimo požiūris	Informacijos apsaugos politika Informacijos pasaugos infrastruktūra
Rizikos atpažinimas	Apsaugos priėjimas Informacijos klasifikavimas Saugumo etapai Įrenginių sauga Vartotojų priėjimo valdymas Tinklo priėjimo kontrolė Šifruoto rašto kontrolė
Rizikos nustatymas	
Rizikos veiksmų planas	Sistemos įrenginių sauga
Rizikos pripažinimas	
Saugumo pasirinkimas	Saugumo priėjimas
Įvertinimo perdavimas	Informacijos apsaugos politika

Iš pateiktos lentelės matome, kad tarptautiniai standartai siūlo skirtingus etapus vienas daugiau pataria atlikti funkcijų, kiti mažiau, tačiau jie siekia to pačio tikslo užkirsti kelia nenumatytiems atvejams, kurie gali sutrukdyti arba net sugriauti organizacijos veiklą.

6. VEIKLOS TĘSTINUMO IR ATKŪRIMO PO NENUMATYTO ATVEJO INFORMACINĖSE SISTEMOSE PLANAS

Išsiaiškinus veiklos tęstinumo ir veiklos atkūrimo valdymo etapus, išanalizavus keletą tarptautinių saugumo standartų, galima sudaryti bendrą planą veiklos tęstinumo ir atkūrimo valdymui. Šis planas orientuotas užkirsti veiklos trūkius, sumažinti riziką iki priimtino lygio ir užtikrinti organizacijos funkcijų ir paslaugų teikimą sutartu lygiu.

Pateikiamas veiklos tęstinumo procesų kūrimo planas.

1. PATEIKTI PROJEKTĄ (INICIJUOTI)

Taikomos naujos ar pagerintos funkcijos. Šiame procese reikia vykdyti šiuos nurodymus:

   a. Gauti vadovybės įsipareigojimą;
   b. Surinkti medžiagą organizacijos plano pagrindimui;
   c. Nustatyti tikslus ir siekius;
   d. Nustatyti asmenį ar grupę atsakingą už veiklos tęstinumo planą;
   e. Skirti finansavimą.

2. ATLIKTI VEIKLOS POVEIKIO ĮVERTINIMĄ

Reikia nustatyti atnaujinimo prioritetus. Šio proceso etapai:

   a. Projekto planavimas;
   b. Duomenų rinkimas;
   c. Duomenų analizė;
   d. Išvadų surašymas;
   e. Išvadų pateikimas.

3. ATLIKTI RIZIKOS VALDYMĄ

Nustatyti organizacijos silpnąsias puses pažeidžiamumus. Šio proceso etapai šie:

   a. Nustatyti pagrindines veiklos rizikos sritis veiklos procese;
   b. Suprasti tikimybinę funkciją ir rizikos mažinimą organizacijoje;
   c. Nustatyti pažeidžiamas sritis, grėsmes, silpnąsias vietas;
   d. Nustatyti patikimus informacijos šaltinius;
   e. Susitikti su vadovybe ir apsibrėžti priimtinus rizikos lygmenis;
   f. Nustatyti procesų ir veiksmų prioritetus;
   g. Įvertinti nenumatytų atvejų priemonių pajėgumus;
   h. Suformuoti tęstinumo veiklos ataskaitas ir pateikti vadovybei.

4. PLANO SUDARYMAS

Sukurti paringti strategijas, parašyti planą. Šio procesas atliekamas taip:

   a. Nustatyti atnaujinimo strategijas;

b. Parengti ir kontroliuoti nenumatytų atvejų kontaktinį sąrašą;
c. Atlikti inventorizaciją;
d. Planuoti susirinkimus.

5. TESTAVIMAS

Atliekami praktiniai veiksmai, pratybos / padarinių apžvalga. Tam reikia atlikti šiuos etapus:

a. Apibūdinti išbandymo tikslus;
b. Nustatyti reikiamą įranga;
c. Nustatyti reikiamą personalą;
d. Sužymėti bandymo grafiką, tvarką ir vietas;
e. Nustatyti testavimo metodus;
f. Apsibrėžti numatomus rezultatus;
g. Atlikti pratybas;
h. Derinti plano priežiūrą, palaikymą;
i. Sukurti veiklos tęstinumo plano mokymo programą.

6. ĮGYVENDINIMAS

Gauti pritarimą ir įgyvendinti planą. Šis procesas atliekamas taip:

a. Įvertinti plano adekvatumą;
b. Gauti raštu vadovybės pritarimą ir patvirtinimą planui;
c. Apmokinti darbuotojus pagal plano turinį ir tikslą;
d. Analizuoti apmokymus;
e. Atlikti plano tikrinimą.

IŠVADOS

1. Pirmas žingsnis kuriant veiklos tęstinumo ir atkūrimo planą – atlikti rizikos analizę. Geras išankstinis pasiruošimas padeda riziką minimaliai sumažinti ir išvengti nepageidaujamų pasekmių. Norint apsisaugoti nuo šių grėsmių ir išvengti pagrindinių pasekmių organizacijoje, pravartu gerai susipažinti su informacijos saugumo valdymo sistema. Jos tikslas – saugoti informaciją, kuria disponuoja organizacija, kiek įmanoma sumažinti riziką prarasti šią informaciją ir dėl to atsirasiančius nuostolius.

2. Verslo tęstinumo valdymo procesas turėtų būti įdiegtas siekiant sumažinti veiklos žlugimą sukeliančius veiksnius, kaip netikėtos nelaimės, nelaimingi įvykiai, įrengimų gedimai bei tyčiniai, piktybiniai veiksmai iki priimtino lygmens panaudojant prevencinio ir atkuriamojo reguliavimo derinį.

3. Nuosekliam rizikos valdymo, veiklos atstatymo ir tęstinumo planavimo procesų valdymui tikslinga vadovautis tarptautiniu mastu pripažintais standartais, geromis praktikomis pagrindiniai jų yra CobIT metodika, tarptautinių saugumo standartų grupės ISO 27000 ir ISO20000.

4. CobIT metodika yra orientuota į veiklos valdymą, strateginių sprendimų priėmimą. Tai puikus įrankis įmonės vadovybei, kuriant informacinių sistemų strategiją. Tuo tarpu tarptautinių saugumo standartai grupės ISO 27000 ir ISO 20000 gerokai detaliau aprašo veiklas, funkcijas ir leidžia geriau suprasti bei planuoti veiksmus ir priklausomybes. Šie standartai vienas kitam neprieštarauja, o vienas kitą papildo. Naudojant šiuos standartus įmonės veiklos tęstinumo ir atkūrimo planavime, galima pasiekti norimų rezultatų.

5. Suformavus veiklos tęstinumo ir atkūrimo po nenumatyto atvejo informacinėse sistemose planą, galima įmonėje sutaupyti laiko, o tuo pačiu ir finansinių išteklių. Reikia atsižvelgti į organizacijos veiklos pobūdį, įmonės saugumui kylančius pavojus. Neturint šio plano, organizacija rizikuoja, kad įvykus nenumatytam atvejui organizacijos veikla gali sutrikti ir būti neatkurta reikiamu laiku. Susistemintas veiklos tęstinumo ir atkūrimo valdymo planas palengvins vadovams nenutrūkstamai valdyti organizacijos veiklą. Numatant būsimas grėsmes darbuotojai imsis prevencinių veiksmų, o įvykus nelaimingam atsitikimui atkurs veiklą iki buvusios situacijos.

BIBLIOGRAFINIŲ NUORODŲ SĄRAŠAS

1. Informatika. [interaktyvus]. Kaunas: KTU – [žiūrėta 2007m. kovo 15d] Prieiga per internetą <http://distance.ktu.lt/kursai/informatika1/1/teorija5.html>
2. Project Planning and Implementing Tools. [interaktyvus], [žiūrėta 2007m. kovo 15d] Prieiga per internetą <http://www.asq.org/learn-about-quality/project-planning-tools/overview/pdca-cycle.html>
3. pdca - the deming cycle. [interaktyvus], [žiūrėta 2007m. Kovo 15d] Prieiga per internetą <http://www.ifm.eng.cam.ac.uk/dstools/process/pdca.html>
4. Procesų valdymo sistemos. [interaktyvus]. Vilnius: Entering Lithuanian market - 2007. [žiūrėta 2007m. gegužės 5 d] Prieiga per internetą <http:/www.elm.lt/lt/vadybos_konultacijos/rizikos_valdymo_p.php>
5. Rizikos vertinimas. [interaktyvus]. Vilnius: UAB Informacijos saugos sprendimai. [žiūrėta balandžio 3d.] Prieiga per internetą <http://www.isec.lt/pdf/riziku_vertinimas.pdf>
6. [1] Rizikos analizės vadovas. [interaktyvus]. Vilnius: Vidaus reikalų ministerija - 2006. [žiūrėta balandžio 3d.] Prieiga per internetą <http://www.vrm.lt/fileadmin/Padaliniu_failai/Informacines_politikos_dep/IT_sauga/Rizikos_analize.pdf>
7. LR aplinkos ministro Įsakymas“ Dėl planuojamos ūkinės veiklos galimų avarijų rizikos vertinimo rekomendacijų R41-02 patvirtinimo 2007.07.16 Nr. 367, Vilnius
8. Rizikos analizės vadovas. [interaktyvus]. Vilnius: Vidaus reikalų ministerija - 2006. [žiūrėta balandžio 3d.] Prieiga per internetą <http://www.vrm.lt/fileadmin/Padaliniu_failai/Informacines_politikos_dep/IT_sauga/Rizikos_analize.pdf>
9. Duomenų atstatymas [interaktyvus]. Vilnius: IBM [žiūrėta 2007m. kovo 25d.]. Prieiga per internetą <http://www-05.ibm.com/lt/services/da.html>
10. Informacijos centro vadovas, Londonas, Prekybos ir pramonės rūmai - 2003
11. Informacijos vadyba, [Interaktyvus][žiūrėta 2007 m. balandžio 9 d.]. Prieiga per Internetą: <http://www.infovi.vu.lt/ivs/biblioteka/temos/infovadyba.htm#_Toc486382749>
12. Ką ir kaip veikia vadovai. [interaktyvus],[žiūrėta 2007 m. vasario mėn. 5 d.]. Prieiga per internetą: <http://verslas.banga.lt/lt/leidinys.full/3fd5e5ab4e3e7>
13. Cobit 4.0 IT governance institute USA
14. International Standard ISO/IEC 17799, ISO copyrigt office Switzerland, 2000
15. International Standard ISO/IEC 20000, ISO copyrigt office Switzerland, 2005

Business Continuity and Disaster Recovery of Information Systems

Ingrida Kriščiūnaitė

SUMMARY

Research object – Planning and maintenance of business continuity and disaster recovery in information systems. The goals of the research: to analyze business continuity and recovery policy and develop business continuity and recovery main steps. The tasks of research: to investigate the concept of information systems, identify threats, vulnerabilities which might undermine the activity of the organisation, as well as investigate business continuity, recovery management phases, present, examine and compare relevant to the topic basic international standards, develop the plan concerning the prevention of threats and business continuity ensurance in organisation in case of emergency.

Of late, the importance of information technologies in organisation has increased considerably. This accounts for the information technologies being a major segment of management in an organisation. Information system – is considered as an integrity of people, hardware and software, procedures and data operating together in providing meaninful information to individuals and organisations. Currently more and more information have been automated by using computerised information systems.

Information systems are composed of organisation facilities, including tangible property, information sources, intagibles, services, staff, software property.

Property becomes a target for threats. The threat arises in the bottleneck, least probable situation to cause damage. Threats are posing people, groups of people, natural phenomenon, political, economical and societal phenomenon due to which threats may occur to security of information systems. In order to ensure the prevention of threats to organisation, evade the major consequences and risk in any area it is necessary to know information security management system.

Information security management system – entirety of program, technical, organizational measures, developed pursuant to the legal regulations establishing the information security. The information security basis is a reliable information security management system, comprising organisational and technological segments. However the information security management system is not adequate to ensure total security for organisation activity and the proper management. For this to achieve it is needed a consistent plan of processes which is to be followed from beginning to the end of its activity. In order to ensure business continuity and performance, it is necessary to draw up a business continuity and recovery plan. The plan consists of business continuity and recovery management processes.

The management of business continuity and recovery is needed for the organisation to continue its activity in cases of lost data, critical deterioration of the systems and any interruption in information technologies functions in case of disaster. Documented and well grounded information on dependency of the activity of the enterprise regarding which information systems are least critical, most critical. This will enable business leaders to effectively use and justify the investments, allocate assignations appropriate to critical systems, and to noncritical accordingly.

The relevancy of the research: Upon developing the plan of business continuity and disaster recover in case of emergency in information systems, it is beneficial for the organisation, enterprise in terms of time saving and cost saving. It is important to consider the business area of the organisation, the threats and danger to security of the enterprise. Without such plan the organisation risks to have the interrupted or discontinued activity and not being timely recovered. The constructive business continuity management plan will facilitate the leaders to continually run the business. For the foreseen threats the employees will take up established preventive measures, therefore in case of disaster the business status will be recovered.