Vilniaus universiteto
Komunikacijos fakulteto
Informacijos ir komunikacijos katedra

Dainius Neverbickas
Informacijos sistemų vadybos
magistratūros studijų programos studentas

INFORMACIJOS SAUGUMO RIZIKOS ANALIZĖS METODAS INFORMACINĖS SISTEMOS KŪRIMO PROCESE

magistro darbas

Vadovas dr. I. Aleliūnas

Vilnius
2008

MAGISTRO DARBO LYDRAŠTIS

Pildo bakalauro/ magistro baigiamojo darbo autorius

DAINIUS NEVERBICKAS

(bakalauro/ magistro baigiamojo darbo autoriaus vardas, pavardė)

INFORMACIJOS SAUGUMO RIZIKOS ANALIZĖS METODAS INFORMACINĖS SISTEMOS KŪRIMO PROCESE

(bakalauro/ magistro baigiamojo darbo pavadinimas lietuvių kalba)

INFORMATION SECURITY RISK ANALYSIS METHOD IN PROCESS OF DEVELOPING INFORMATION SYSTEM

(bakalauro/ magistro baigiamojo darbo pavadinimas anglų kalba)

Patvirtinu, kad bakalauro/ magistro baigiamasis darbas parašytas savarankiškai, nepažeidžiant kitiems asmenims priklausančių autorių teisių, visas baigiamasis bakalauro/ magistro darbas ar jo dalis nebuvo panaudotas kitose aukštosiose mokyklose.

_____

(bakalauro/ magistro baigiamojo darbo autoriaus parašas)

Sutinku, kad bakalauro/ magistro baigiamasis darbas būtų naudojamas neatlygintinai 5 metus Vilniaus universiteto Komunikacijos fakulteto studijų procese.

_____

(bakalauro/ magistro baigiamojo darbo autoriaus parašas)

Pildo bakalauro/ magistro baigiamojo darbo vadovas

Bakalauro/ magistro baigiamąjį darbą ginti _____

(įrašyti – leidžiu arba neleidžiu)

_____ _____

(data) (bakalauro/ magistro baigiamojo darbo vadovo parašas)

Pildo instituto/ katedros, kuruojančios studijų programą, reikalų tvarkytoja

Bakalauro/ magistro baigiamasis darbas įregistruotas

_____

(instituto/ katedros, kuruojančios studijų programą, pavadinimas)

_____ _____

(data) (instituto/ katedros reikalų tvarkytojos parašas)

Pildo instituto/ katedros, kuruojančios studijų programą, vadovas

Recenzentu skiriu _____

(recenzento vardas, pavardė)

_____ _____

(data) (instituto/ katedros vadovo parašas)

Pildo recenzentas

Darbą recenzuoti gavau. _____ _____

(data) (recenzento parašas)

REFERATO LAPAS

Neverbickas, Dainius

Ne206 Informacijos saugumo rizikos analizės metodas informacinės sistemos kūrimo procese: magistro darbas / Neverbickas Dainius; mokslinis vadovas Alelūnas Irmantas; Vilniaus universitetas. Komunikacijos fakultetas. Informacijos ir komunikacijos katedra. – Vilnius, 2008. – 88 lap.: lent. – Mašinr. – Santr. angl. – Bibliogr.: p. 80–83 (28 pavad.).

UDK 65.012(075.8)

Raktiniai žodžiai: *Informacijos saugumas, rizikos valdymas, rizikos analizė, rizikos valdymo metodai, rizikos valdymo įrankiai, rizikos analizės metodai, Informacinės sistemos saugumas, Informacinės sistemos rizikos analizė.*

Magistro *darbo objekt*as – informacinės sistemos saugumas. *Darbo tikslas* – sukurti informacijos saugumo rizikos analizės metodą, kuris būtų tikslingai pritaikytas naudoti informacinės sistemos kūrimo procese bei padėtų padidinti jos saugumo lygį. *Darbo uždaviniai*: nustatyti pagrindinius rizikos valdymo principus bei palyginti populiariausias metodikas ir įrankius; įvertinti plačiai paplitusius rizikos analizės metodus; apibrėžti kuriamo rizikos analizės metodo etapus remiantis geriausiomis egzistuojančių metodų savybėmis; eksperimentu įvertinti sukurto metodo efektyvumą.

Naudojantis literatūros šaltinių analizės, lyginamuoju, ekstrapoliacijos ir eksperimento metodais, darbe pateikti pagrindiniai informacijos saugumo rizikos valdymo ir analizės principai, palyginti populiariausi rizikos valdymo bei vertimo metodai ir įrankiai, sukurtas naujasis RAISKP rizikos analizės metodas bei įvertintas jo efektyvumas.

Nustačius pagrindinius rizikos valdymo principus, paaiškėjo, jog norint efektyviai valdyti rizikas, būtina pastoviai vykdyti tokius etapus kaip: rizikos apimties apibrėžimas, rizikos vertinimas, rizikos tvarkymas, informavimas apie riziką, rizikos stebėjimas ir peržiūrėjimas. Rizikos valdymas padidina organizacijos stabilumą, nes kiekviena galima grėsmė yra numatoma ir jai pritaikomos apsisaugojimo priemonės. Lyginant populiariausius rizikos valdymo metodus, išryškėjo jų skirtumai ir panašumai. Metodai išsiskiria savo būdais pasiekti tikslą, pritaikomumu organizacine

pagal jos dydį, reikalingų žinių lygių norint taikyti metodą bei suderinamumu su tarptautiniais saugumo standartais. Metodai panašūs savo taikymo filosofija, vykdomom procedūromis, iškeltais

reikalavimais bei užsibrėžtais tikslais. Lyginant populiariausius rizikos valdymo ir vertinimo įrankius paaiškėjo, kad dauguma jų automatizuoja ataskaitų ruošimo ar rizikos apskaičiavimo procesus, sukauptomis žynių bazėmis padeda nustatyti organizacijai kylančias grėsmes bei parinkti geriausias kontrpriemones, nustato arba padeda pasiekti atitikimą tarptautiniams saugumo standartams. Įrankiai išsiskiria naudojamais rizikos valdymo ir vertinimo metodais, funkcionalumu bei kaina. Vertinant rizikos analizės metodus, nustatyta, jog analizę galima atlikti pritaikius kiekybinį ar kokybinį metodą. Kiekybiniai metodai yra labiau tinkami tais atvejais, kai saugos sprendimai daro įtaka finansiniams sprendimams, o kokybinė rizikos analizė turėtų būti pasirinkta tuomet, kai priimami sprendimai yra susiję su baziniu saugos sukūrimu. Egzistuojančių rizikos analizės metodų tyrimas leido išskirti geriausias jų savybes. Metodų tyrimo metu buvo identifikuoti greičiausi ir lengviausiai atliekami etapai, kurie su nedideliais pakeitimas buvo pritaikyti naujame RAISKP metode. Praktinis RAISKP metodo pritaikymo tyrimas leido įvertinti jo efektyvumą ir teikiamą naudą IS kūrimo procesui. Tyrimo metu buvo įsitikinta, kad informacinės sistemos kūrimo grupei naujasis rizikos analizės metodas leidžia įvertinti vystomo produkto galimas saugumo grėsmes projektavimo etape bei padeda sukurti saugesnę sistemą.

Darbas gali būti naudingas informacijos saugumo specialistams, informacinių sistemų kūrėjams ar informacinius sistemų studijų studentams.

TURINYS

SANTRUMPŲ IR TERMINŲ SĄRAŠAS

SANTRUMPOS:

- **IS** – informacinė sistema;
- **IT** – informacinės technologijos;
- **DB** – duomenų bazė;
- **RA** – rizikos analizė;
- **RV** – rizikos valdymas;
- **B2B** (*business to business*) – verslas verslui;
- **RAISKP** – rizikos analizė informacinės sistemos kūrimo procese;
- **ISMS** (*Information Security Management system*) – informacijos saugos valdymo sistema;
- **KURAP** – kuruojamos rizikos analizės procesas;
- **30MM** – 30 minučių metodas;
- **10ŽM** – dešimties žingsnių metodas;
- **3ŽM** – Trijų žingsnių metodas;
- **ISO** (*International Organization for Standardization*) – tarptautinė standartizavimo organizacija;
- **PSĮ** – preliminarus saugos įvertinimas;
- **TMN** – tikėtinas metinis nuostolis;
- **PV –** pažeidžiamumo veiksnys ;
- **MDR –** metinis dažnumo rodiklis;
- **TVN** - tikėtinas vienkartinis nuostolis;
- **CCTA** (*Central Communication and Telecommunication Agency*) - centrinė komunikacijos ir telekomunikacijos agentūra;
- **CRAMM** (*CCTA Risk Analysis and Management Methodology*) – CCTA rizikos analizė ir valdymo Metodologija;
- **EBIOS** (*Expression des Besoins et Identification des Objectifs de Sécurité*) - poreikių nustatymas ir saugumo tikslų identifikavimas;
- **ISF** (*Information Security Forum*) - informacijos saugumo forumas;
- **FIRM** (*Fundamental Information Risk Management*) - fundamentalus Informacijos Rizikos valdymas;
- **IRAM** (*Information Risk Analysis Methodologies*) - informacijos rizikos analizės metodologija;

- **SARA**(*Simple to Apply Risk Analysis*) - paprastas rizikos analizės pritaikymas;
- **SPRINT** (*Simplified Process for Risk Identification*) - Supaprastintas procesas rizikos identifikavimui;
- **OCTAVE** (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) - operatyvus kritiškų grėsmių, turto ir pažeidžiamumų įvertinimas;
- **COBIT** (*Control Objectives for Information and related Technology*) - informacijos kontrolės tikslai ir susietos technologijos;

TERMINAI [1]:

- **Informacijos sistemų turtas (vertybės)** – informacija , programinė įranga, fizinė įranga ir paslaugos;
- **Įvykis** – konkrečių aplinkybių derinys;
- **Pasekmė** – įvykio rezultatas;
- **Rizika** – įvykio tikimybė ir jo pasekmių derinys;
- **Informavimas apie riziką** – apsikeitimas arba pasidalinimas informacija apie riziką tarp asmens, priimančios spendimus, ir rizikos subjektų;
- **Rizikos analizė** – sistemingas informacijos panaudojimas, siekiant nustatyti šaltinius ir įvertinti riziką;
- **Rizikos vertinimas** – procesas, kurio metu rizikos tikimybė ir pasekmės išreškiamos konkrečia verte;
- **Rizikos išlaikymas** – susitaikymas su konkrečios rizikos sąlygojamais nuostoliais arba nauda;
- **Rizikos vengimas** – sprendimas nedalyvauti ar pasitraukti iš rizikingos situacijos;
- **Rizikos įvertinimas** – procesas, kurio metu apskaičiuota rizika įvertinama pagal rizikos kriterijus, siekiant nustatyti rizikos reikšmingumą;
- **Rizikos kriterijai** – veiksniai, įvertinantys rizikos reikšmingumą;
- **Rizikos optimizacija** – su rizikos kontrole susijęs procesas, kuriuo siekiama sumažinti neigiamų pasekmių tikimybę ir padidinti teigiamų pasekmių atsiradimo tikimybę;
- **Rizikos perdavimas** – konkrečios rizikos sąlygojamų nuostatų naštos arba naudos pasidalijimas su kita šalimi;
- **Rizikos priėmimas** – sprendimas prisiimti riziką;
- **Rizikos tvarkymas** – procesas, kurio metu pasirenkamos ir įdiegiamos priemonės, keičiančios rizikos tikimybę;
- **Rizikos valdymas** – koordinuoti veiksmai, kuriais siekiama valdyti ir kontroliuoti organizacijos rizikas;
- **Rizikos vertinimas** – bendras rizikos analizės ir rizikos įvertinimo procesas;

ĮVADAS

Informacija tampa vis brangesnė ir vertingesnė prekė, todėl natūralu, kad informacijos saugumas tampa vis aktualesnė problema. Šiuolaikinės kompanijos, kurios tiesiogiai yra priklausomos nuo informacinių sistemų, neišvengiamai susiduria su kompleksiškomis informacijos konfidencialumo, vientisumo ir prieinamumo problemomis. Efektyviausias būdas apsisaugoti nuo kylančių grėsmių – informacijos saugumo valdymo sistemos įdiegimas. Vienas svarbiausių informacijos saugumo valdymo sistemos etapų yra rizikos valdymas ir analizė. Pagrindiniai rizikos valdymo ir analizės uždaviniai yra identifikuoti esančias rizikas, įvertinti jų poveikį organizacijai bei parinkti efektyviausias saugumo priemones mažinančias riziką.

Yra sukurta daug metodinių nurodymų bei įrankių, kurie padeda organizacijai vykdyti informacijos saugumo rizikos valdymo ir analizės procesą. Plačiai paplitę rizikos valdymo ar analizės metodai (tokie kaip CRAMM, EBIOS, ISO/IEC 13335-2, 10ŽM, KURAP) nurodo įmonei grėsmių nustatymo, rizikos vertinimo bei rizikos tvarkymo būdus, kurie gali padidinti informacinių sistemų saugumo lygį.

Šiame darbe yra analizuojamas informacinės sistemos saugumo rizikos analizės atlikimas jos kūrimo stadijoje naudojantis IS kūrimo grupės žmogiškaisiais resursais. Dažnai pasitaiko, kad IS yra kuriama ne pačios bendrovės, bet užsakoma IT įmonės, kuris specializuojasi tokioje srityje. Norint IT įmonei atlikti rizikos analizę kuriamai sistemai, yra sunku pritaikyti vieną iš populiariųjų metodų, kadangi jų analizės ribos yra platesnes organizacijos infrastruktūros mastu bei analizės rezultatai įtakoja bendrą jos saugumo politiką, o ne vien tik tiriama informacinę sistemą. Įvertinus tokią situaciją, apibrėžta šio darbo *problema* – trūksta rizikos analizės metodo, kuris tikslingai būtų pritaikytas naudoti informacinės sistemos kūrimo procese. Norint išspęsti iškilusią problemą, apsibrėžtas darbo objektas, tikslas bei uždaviniai tikslui pasiekti.

*Darbo objekt*as – informacinės sistemos saugumas.

Darbo tikslas – sukurti informacijos saugumo rizikos analizės metodą, kuris būtų tikslingai pritaikytas naudoti informacinės sistemos kūrimo procese bei padėtų padidinti jos saugumo lygį.

Darbo uždaviniai:

1. Nustatyti pagrindinius rizikos valdymo principus bei palyginti populiariausias metodikas ir įrankius;
2. Įvertinti plačiai paplitusius rizikos analizės metodus;

3. Apibrėžti kuriamo rizikos analizės metodo etapus remiantis geriausiomis egzistuojančių metodų savybėmis;
4. Eksperimentu įvertinti sukurto metodo efektyvumą.

Atliekant sukurto metodo panaudojimo eksperimentą, bus bandoma įrodyti *hipotezę* - informacinės sistemos kūrimo grupei naujasis rizikos analizės metodas leis įvertinti vystomo produkto galimas saugumo grėsmes projektavimo etape bei padės sukurti saugesnę sistemą.

Naudojantis *literatūros šaltinių analizės, lyginamuoju, ekstrapoliacijos ir eksperimento metodais,* darbe pateikti pagrindiniai informacijos saugumo rizikos valdymo ir analizės principai, palyginti populiariausi rizikos valdymo bei vertimo metodai ir įrankiai, sukurtas naujasis RAISKP rizikos analizės metodas bei įvertintas jo efektyvumas.

Šis darbas yra *metodologinio* pobūdžio. *Darbo struktūrą* sudaro 6 dalys.

Pirmojoje darbo dalyje nustatomi rizikos valdymo principai, tiriami jo etapai bei sąveiką su informacijos saugumo valdymo sistema.

Antrojoje dalyje nustatomos populiariausios rizikos valdymo ir vertinimo metodologijos, analizuojamos jų savybės bei pateikiamas palyginimas pagal apibrėžtus kriterijus.

Trečiojoje dalyje, tokiu pat principu kaip ir antrojoje, analizuojami ir lyginami populiariausi rizikos valdymo ir vertinimo įrankiai (programinė įranga).

Ketvirtojoje dalyje tiriami kokybiniai ir kiekybiniai rizikos analizės metodai bei pateikiami jų privalumai ir trūkumai.

Penktojoje dalyje yra apibrėžiami naujojo RAISKP metodo etapai, kurie yra sukurti remiantis ištirtomis populiariausiomis rizikos valdymo ir analizės metodologijomis.

Šeštojoje dalyje yra atliekamas RAISKP metodo panaudojimo eksperimentas, aprašoma tiriama informacinė sistema, įvertinami metodo vykdymo etapai bei pateikiami rezultatai.

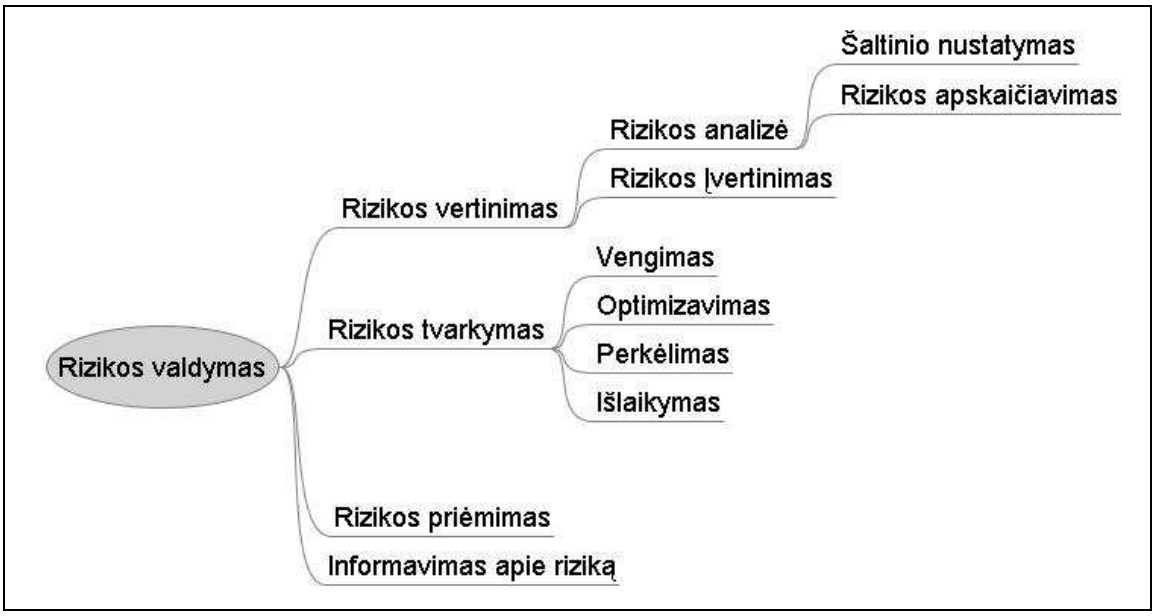
Darbe daugiausiai naudotasi Europos tinklų ir informacijos saugumo agentūros duomenimis, ISO standartų dokumentacija, rizikos valdymo ir analizės metodų internetinių svetainių duomenimis bei rizikos analizės vadovu.

Darbas gali būti naudingas informacijos saugumo specialistams, informacinių sistemų kūrėjams ar informacinius sistemų studijų studentams.

1. RIZIKOS VALDYMAS

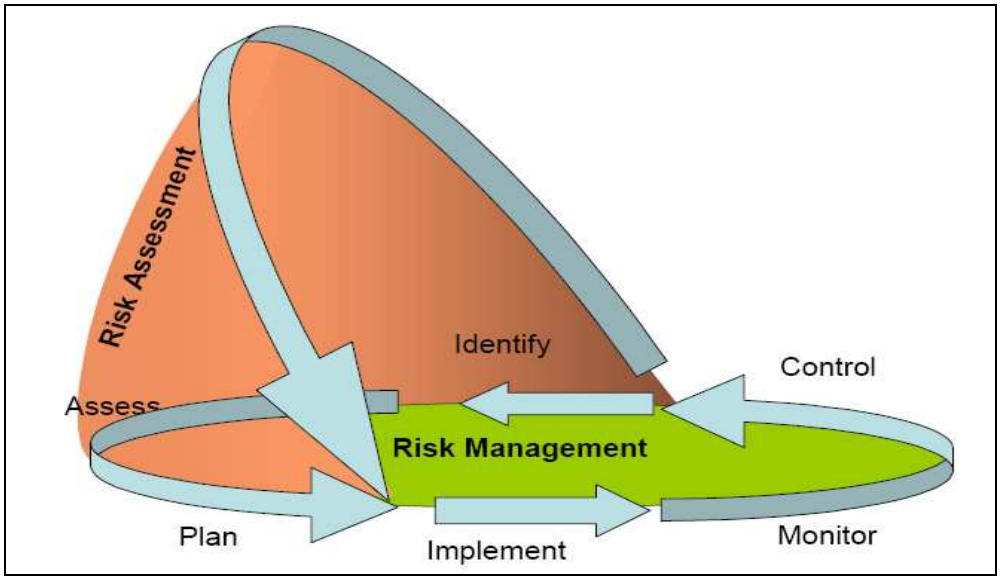
Rizikos valdymas tai koordinuoti veiksmai, kuriais siekiama valdyti ir kontroliuoti organizacijos rizikas. Rizikos valdymo ir analizės procesai gali pasirodyti identiški, bet reikėtų suprasti jų skirtumus ir bendrumus. Rizikos valdymo proceso tikslas yra sumažinti riziką iki priimtino lygio, tuo tarpu rizikos analizė atliekama tam, kad jos rezultatai būtų panaudoti kaip pagrindas rizikos mažinimo procesams įgyvendinti ir veiksmingumui įvertinti [3]. RV sąvokų sąsajos pavaizduotos 1.1 schemoje.

1.1 schema. Rizikos valdymo sąvokų sąsajos (pagal ISO 72 vadovą)



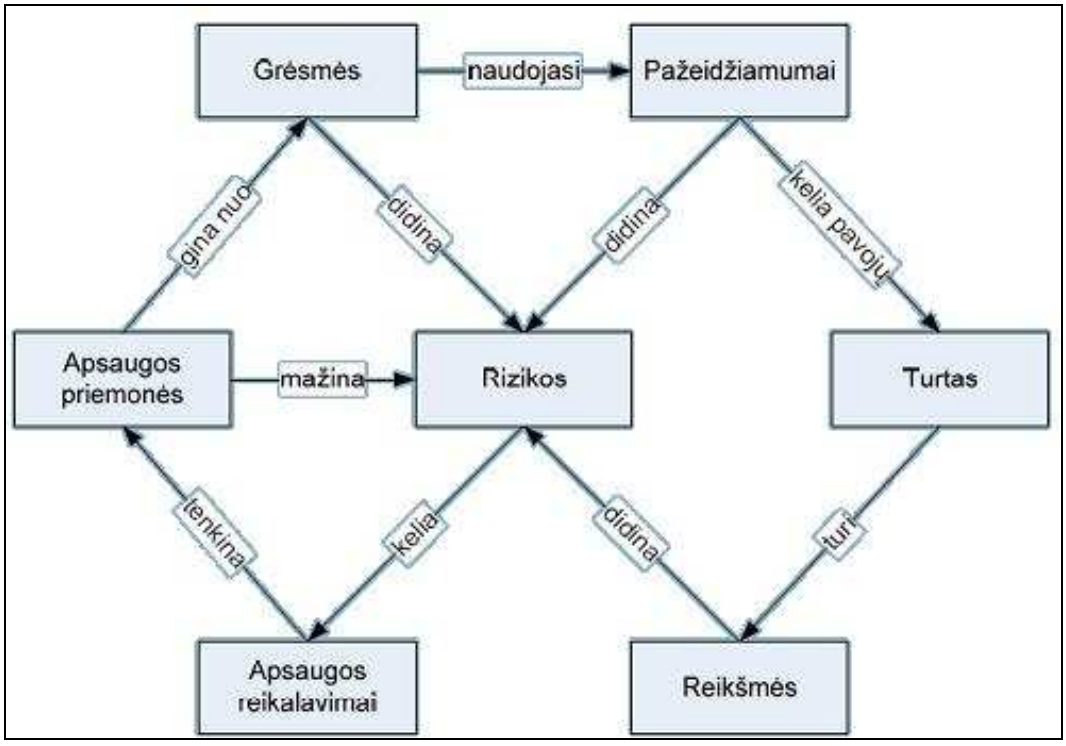
Rizikos valdymas yra pasikartojanti veikla (ciklas), kuri yra įtakojama saugumo politikos ir susideda iš vertinimo, planavimo, įgyvendinimo, kontrolės ir įdiegtų priemonių stebėjimo (žr. 1.2 schemą).

1.2 schema. Rizikos valdymo ciklas ir sąveika su rizikos vertinimo procesu[4]



Norint tinkamai valdyti rizikas organizacijoje, būtina žinoti RV elementų sąsajas (žr. 1.3 schemą). Suvokiant rizikos valdymo elementų tarpusavio ryšius, galima tiksliau apsibrėžti kylančias grėsmes, nustatyti pažeidžiamumus bei pasirinkti saugumo priemones.

1.3 schema. Rizikos valdymo elementų tarpusavio sąsajos[5]



1.1. Rizikos valdymo ir vertinimo sąveika su ISMS

ISMS pagrindinė paskirtis - įdiegti būtinas priemones, kad eliminuoti ar sumažinti įvairių su sauga susijusių grėsmių ar pažeidžiamumų poveikį organizacijai. Taip pat, ISMS suteikia galimybę užtikrinti efektyvią informacijos apsauga, nustatyti esamą saugos lygį, išryškinti grėsmes ir jų poveikį veiklos procesams bei efektyviai investuoti į saugos priemones. Kad ISMS sėkmingai funkcionuotų, ji turi tenkinti tokius faktorius [4]:

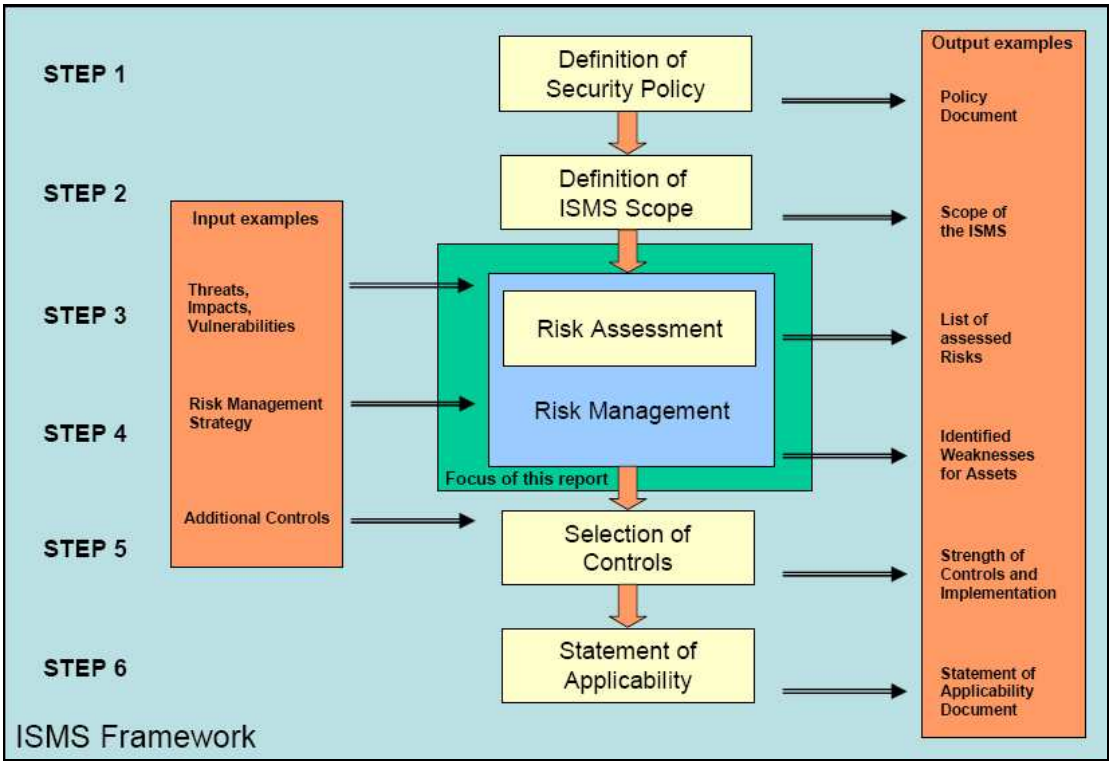
- Turi turėti aukščiausios vadovybės palaikymą;
- Valdoma centralizuotai ir paremta bendra organizacijos strategija ir politika;
- Saugos siekiai ir veikla turi būti paremti verslo tikslais bei reikalavimais;
- Apimti tik reikalingiausius veiklos procesus ir vengti visapusiškos kontrolės;
- Laikytis bendros organizacijos filosofijos;
- Būti nesibaigiančių procesu.

Informacijos saugumo valdymo sistema susideda iš(žr. 1.4 schemą):

1. Saugumo politikos apibrėžimo;
2. ISMS apimties apibrėžimo;
3. Rizikos vertinimo (rizikos valdymo dalis);
4. Rizikos valdymo;
5. Kontrolės būdo pasirinkimo;
6. Kontrolės būdo tinkamumo patvirtinimo.

Rizikos valdymo ir vertinimo procesas (3 ir 4 žingsniai) yra tarsi ISMS širdis. Šie procesai iš vienos pusės „transformuoja“ saugumo politikos gaires ir tikslus, o iš kitos pusės ISMS siekius į specifinius kontrolės įgyvendinimo planus ir mechanizmus, kurie sumažina grėsmes ir pažeidžiamumus. Kontrolės būdo pasirinkimo ir tinkamumo patvirtinimo etapai yra skirti vykdymo veiksmams, kurie reikalauja saugumo techninio įgyvendinimo, palaikymo ir kontrolės nustatymo. Pirmasis ir antrasis ISMS žingsniai yra vykdomi ilgesnį laiko tarpą, kadangi įsteigimas saugumo politikos ir ISMS apimties apibrėžimas yra tvarkomi ir svarstomi organizacijos mastu. Galiausiai reikėtų paminėti, kad ISMS yra rekursinis procesas.

1.4 schema. ISMS konstrukcija (paremta ISO 17799 standartu)[4]



1.2. Rizikos valdymo procesas

Rizikos valdymo efektyvumas priklauso nuo jo pasisekimo tapti organizacijos filosofijos, praktikos, kultūros ir verslo procesų dalimi. Rizikos valdymas yra kiekvieno organizacijos nario pareiga. Šio procesų įgyvendinimo dizainas organizacijoje visuomet priklauso nuo[4]:

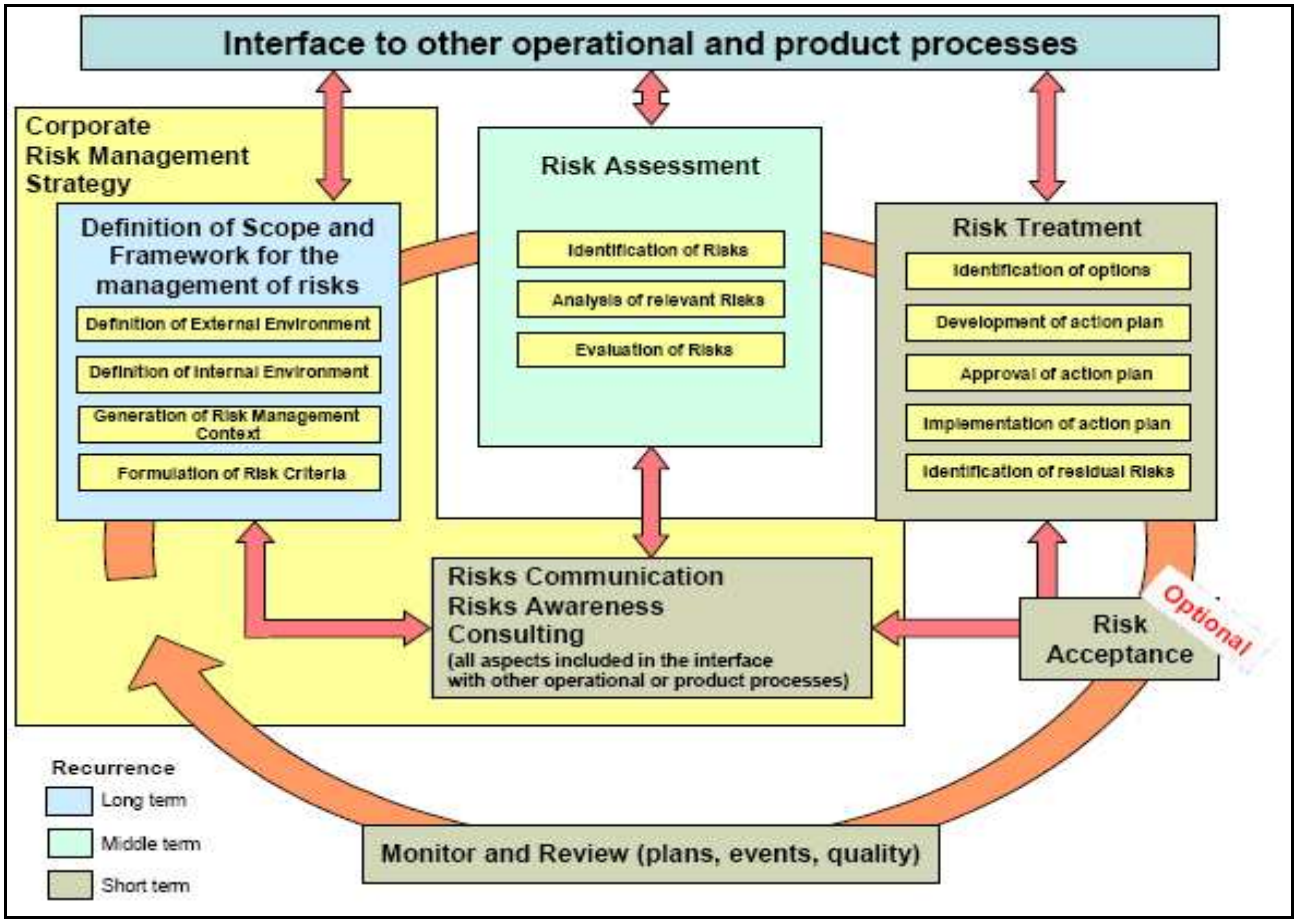
- Organizacijos misijos ir siekių;
- Produktų ir paslaugų;
- Valdymo ir operacinių procesų;
- Specifinio darbo pobūdžio;
- Fizinių, aplinkos ir kontrolės sąlygų.

Rizikos valdymas susideda iš penkių pagrindinių procesų (žr. 1.5 schemą):

1. Rizikos valdymo nuostatos ir apimties apibrėžimo;
2. Rizikos Vertinimo;
3. Rizikos tvarkymo;
4. Rizikos komunikacijos;
5. Rizikos Stebėjimo ir peržiūrėjimo.

Panašūs etapai yra apibrėžti ir ISO 27001 rizikos valdymo sistemoje.

1.5 schema.Detalus rizikos valdymo proceso ciklas[4]



1.2.1. Rizikos valdymo nuostatos ir apimties apibrėžimas

Nuostatų ir apimties apibrėžimo etapas nustato globalius kriterijus rizikos valdymui organizacijoje. Yra įvertinami vidiniai (organizacijos stiprios vietos, silpnos vietos, galimybės, grėsmės, struktūra, kultūra, resursai ...) ir išoriniai (įstatymai, kultūra, rinka, konkurencingumas, socialinė, finansinė ir politinė aplinka ...) faktoriai. Šiame etape reikia:

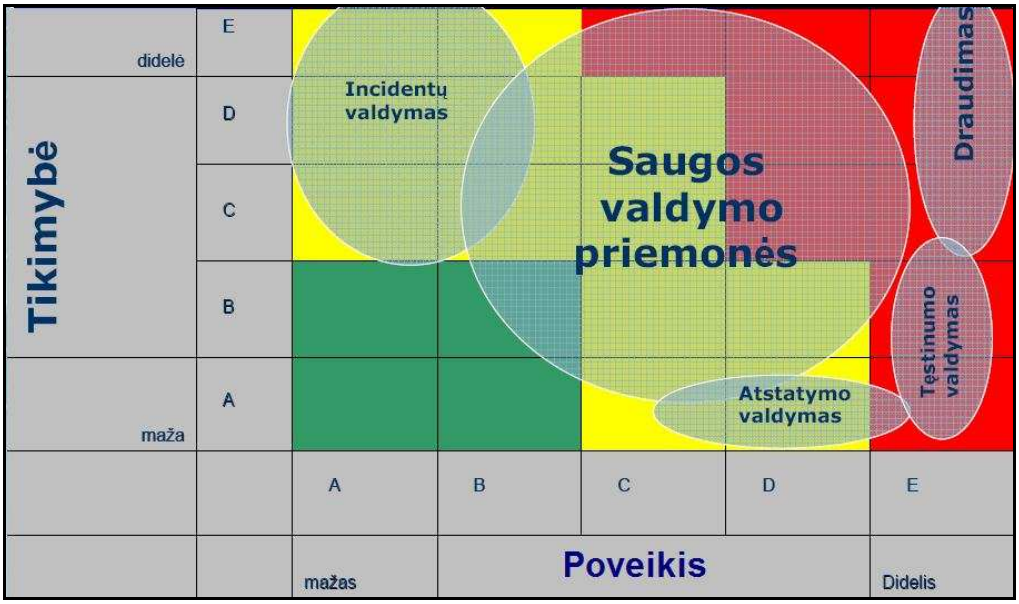
- Išsiaiškinti pagrindinius organizacijos siekius;
- Nustatyti organizacijos aplinką;
- Apibrėžti rizikos valdymo tikslus, apribojimus ar sąlygas, pageidaujamus rezultatus;
- Nustatyti eilę kriterijų, pagal kuriuos bus matuojama rizika;
- Apibrėžti rinkinį pagrindinių elementų, pagal kuriuos bus atliekama rizikos atpažinimo ir vertinimo procesas.

Rizikos valdymas suteikia balansą tarp kainos, naudos ir galimybių, todėl yra būtina teisingai nustatyti apimtis ir ribas. Nustatant rizikos valdymo kontekstą, turi būti aprėžta:

- Organizacijos procesai, projektai ar veikla bei pagrindiniai jų siekiai;

- Projektų, veiklos ar funkcijų trukmė;
- Rizikos valdymo veiklos pilna apimtis, kuri apibrėžia kas bus įtraukta o kas ne;
- Rizikos vertinimo metodo įvardijimas bei vykdymo dažnumas;
- Įvairių organizacijos dalių vaidmenys ir atsakomybės dalyvaujant rizikos valdymo procese (kas atsakingas už rizikos analizės vykdymą; sprendimus, susijusius su nepriimtinos rizikos tvarkymu; nepriimtinų rizikos valdymo plano paruošimą ir įgyvendinimą.);
- Projektų ar veiklų tarpusavio priklausomybės.
- Priimtinas rizikos lygis, kuris gali būti įvertintas nuostolių matricos pagalba (žr. 1.6. schemą).

1.6 schema. Rizikos valdymo nuostolių matrica[5]



1.2.2. Rizikos vertinimas

Šis etapas yra vykdomas remiantis rizikos valdymo nuostatais. Rizikos vertinimas yra mokslu ir technologijomis paremtas procesas, kuris susideda iš rizikos nustatymo, analizės ir įvertinimo. Šie trys etapai yra vienintelis būdas suprasti ir pamatuoti rizikos poveikį bei imtis atitinkamu priemonių ir kontrolės valdant rizikas. Apžvelgsime kiekviena iš rizikos vertinimo etapų:

1. **Rizikos identifikavimas –** fazė, kurioje grėsmės, pažeidžiamumai ir su jais susijusi rizika yra nustatoma. Šis procesas yra sistemingas ir visapusiškas, kad užtikrintų, jog nei viena rizika nebus nesąmoningai nepastebėta.
2. **Rizikos analizė –** fazė, kurioje rizikos lygis ir jos prigimtis yra įvertinama ir suprantama. Analizės rezultatai yra pirmieji duomenys, pagal kuriuos galima: vertinti

riziką; spęsti ar reikia riziką tvarkyti (mažinti) ar ne; nustatyti labiausiai tinkamus apsisaugojimo metodus (plačiau rizikos analizės metodai ir principai bus aptarti 4 dalyje).

3. **Rizikos įvertinimas –** fazė, kurioje turi būti atliekamas sprendimas, kuriai rizikai reikalingas tvarkymas ir kuriai ne, bei nustatomi tvarkymo prioritetai. Sprendimas priimamas atsižvelgiant į rizikos lygį, kuris buvo nustatytas rizikos analizės proceso metu, bei rizikos kriterijų, kuris buvo įvardintas rizikos apimties apibrėžimo stadijoje.

1.2.3. Rizikos tvarkymas

Rizikos tvarkymas yra procesas, kurio tikslas yra pasirinkti ir realizuoti saugumo priemones, kad sumažinti riziką. Šis procesas įtraukia rinkos vengimo, optimizavimo, perkėlimo ir išlaikymo tvarkymo būdus. Rizikos tvarkymo procesas susideda iš tokių etapų:

1. *Tvarkymo priemonės pasirinkimo nustatymas***.** Identifikuojami atitinkami tvarkymo būdai nepriimtinoms rizikoms. Vykdoma remiantis rizikos vertinimu. Kiekvienai nepriimtinai rizikai yra išnagrinėjamos rizikos tvarkymo galimybės ir atliekama išlaidų/naudos analizė. Sudaromas nepriimtinų rizikos rūšių ir jų tvarkymo priemonių sąvadas.
2. *Veiksmų plano kūrimas*. Šis planas reikalingas tam, kad apibrėžti kaip bus atliekamas pasirinktos kontrpriemonės diegimas. Jame yra inicijuojami rizikos valdymo priemonės įgyvendinimo projektas(ai) bei nustatomi rizikos valdymo priemonės efektyvumo matavimo rodikliai.
3. *Plano patvirtinimas***.** Vadovybės plano patvirtinimas, kad kontrpriemonės diegimo procesas būtų efektyvus.
4. *Veiksmų plano diegimas.*
5. *Likutinės rizikos nustatymas*. Koks rizikos lygis liko po kontrpriemonės įdiegimo.

1.2.4. Rizikos priėmimas

Rizikos priėmimas – tai sprendimas priimti riziką organizacijos valdymo atsakomybėje. Rizikos priėmimas yra nebūtinas procesas, nes jis gali būti pakeistas rizikos tvarkymu. Sprendimą priima organizacijos vadovai remiantis: veiklos strategija, misija ir vizija; resursų pakankamumu ar stoka; ankstesniais rizikos valdymo priemonių efektyvumo matavimais ir istorija. Šis sprendimas

yra palankiausias, kai rizikos lygis yra priimtinas, arba kiti sprendimai perdaug sudėtingi (neįmanomi) ar jų kaštai didesni už tikėtinus nuostolius.

1.2.5. Rizikos komunikacija, supratimas ir konsultavimas

Rizikos komunikacija – procesas, kuris skirtas keistis ar dalintis informaciją apie riziką tarp sprendimus atliekančių asmenų ir suinteresuotų asmenų. Rizikos valdymas turi tapti organizacijos kultūros dalimi, todėl bendravimas ir supratimo kūrimas tarp organizacijos narių apie problemas, susijusias su RV procesu, yra labai svarbus. Efektyvus rizikos valdymas priklauso nuo kiekvieno organizacijos suinteresuoto asmens. Kai žmonės nėra supažindinami ar sudominami RV procesais, tai jie linkę ignoruoti valdymo procedūras ir jos tampa neefektyvios. Reikia diskutuoti ir konsultuoti, kad visi turėtu vienodą supratimą apie RV ir nevertintų jų pagal subjektyvų nusistatymą. Taip pat, yra naudingos išorinių ekspertų konsultacijos, nes jos suteikia naujų žinių, kurios padeda geriau spręsti iškilusias RV problemas.

1.2.6. Rizikos Stebėjimas ir peržiūra

Rizikos stebėjimas ir priežiūra – procesas, kuris skirtas vertinti rizikos valdymo veiksmingumą ir efektyvumą. Šis etapas užtikrina, kad apibrėžtas rizikos valdymo veiksmų planas išliks tinkamas ir atnaujintas. Taip pat, šiame procese yra vykdoma kontrolės veikla, kuri numato RV apimties pervertinimus.

Nuolatinis verslo aplinkos kitimas įtakoja rizikos kitimą, todėl svarbu nuolat kartoti rizikos valdymo ciklą. Kad RV taptų organizacijos kultūros ir filosofijos dalimi, būtina rinkti ir dokumentuoti įgytą patirtį bei žinias, kurios gaunamos per stebėjimo ir peržiūrėjimo veiklą, tvarkymo planus ir rezultatus. Kiekviena rizikos valdymo pakopa turi būti tinkamai aprašinėjama ir dokumentuojama.

Rizikos valdymas yra nenutrūkstantis procesas ir kiekvienas iš jo etapų turi būti kruopščia atlikti, kad būtų užtikrintas rezultatų veiksmingumas ir efektyvumas. Į rizikos valdymo procesą turi būti įtraukti visi suinteresuoti asmenys, nes šios veiklos procedūrų ignoravimas ar nesupratimas gali užkirsti kelia geriems jos įgyvendinimo rezultatams. Taip pat, rizikos valdymo procesai turi būti pritaikyti prie organizacijos kultūros ir jos brandumo lygio saugumo atžvilgiu, nes kitaip reikalingos procedūros gali būti per sudėtingos ir nesuprantamos.

2. RIZIKOS VALDYMO IR VERTINIMO METODIKOS

Yra sukurta nemažai metodų/standartų, kuriuose aprašoma kaip įgyvendinti rizikos valdymą organizacijoje. Visi metodai yra panašūs tuo, kad juose yra apžvelgiami rizikos valdymo etapai ar bent dalis jų, o skirtumus galima įžvelgti rizikos valdymo principuose, strategijose bei kiekvieno iš rizikos valdymo etapų aprašymo detalumo lygio. Reikia pastebėti, kad daugumoje metodų/standartų yra aprašoma ne vien rizikos valdymo procesai, bet ir kiti informacijos saugumo aspektai, tačiau šiame darbe metodai/standartai bus vertinami ir analizuojami tik iš rizikos valdymo pusės.

2.1. CRAMM

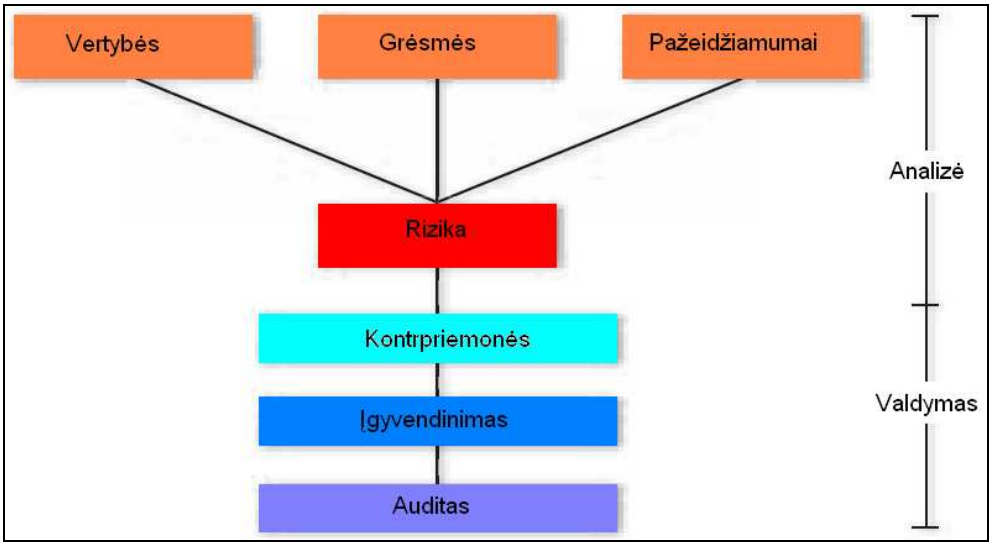
CRAMM - D. Britanijos vyriausybės užsakymu sukurta ir visame pasaulyje taikoma informacijos apsaugos rizikos analizės ir valdymo metodika. *CRAMM* metodika yra nuolat tobulinama jau beveik 20 metų ir yra nepakeičiama priemonė saugumo vadovams ir analitikams. Ji buvo sukurta britų valstybinės organizacijos CCTA. Šį metodą yra sunku taikyti be įrankio pagalbos, kuris taip pat vadinasi *CRAMM*. Pirmoji versija metodo ir įrankio buvo paremta geriausiom britų valstybinių organizacijų praktikom. *CRAMM* buvo išskirtinai naudojama Jungtinės Karalystės valdžios, tačiau taikymas paplito ir kitose šalyse. Šis metodika yra pritaikyta didelėms organizacijoms, tokioms kaip valstybiniai organai ar pramonė [4].

CRAMM yra plačiausiai taikomas informacijos saugumo ir valdymo metodika Europos sąjungos šalyse. Ją naudoja virš 500 organizacijų daugiau nei 23 pasaulio šalyse. Vidaus reikalų ministerija šią metodologiją yra parekomendavusi naudoti visose Lietuvos Respublikos ministerijose.

CRAMM – tai laipsniškas ir metodiškas būdas analizuoti ir valdyti tiek techninius (pavyzdžiui, IT techninę ir programinę įrangą), tiek netechninius (pavyzdžiui, fizinius ir žmoniškuosius) informacijos apsaugos aspektus. Norint juos įvertinti, metodikoje naudojami trys etapai (žr. 2.1 schemą) [10]:

1. Vertybių identifikacija ir įvertinimas;
2. Grėsmių ir pažeidžiamumų įvertinimas;
3. Kontrolės priemonių parinkimas ir rekomendacijos.

2.1 schema. CRAMM metodologijos etapai[11]



Vertybių identifikacijos ir įvertinimo etape yra identifikuojamos fizinės (pavyzdžiui, techninė įranga), programinės (pavyzdžiui, taikomoji programinė įranga), duomenų (pavyzdžiui, informacija, esanti informacinėse sistemose) vertybės bei lokacijos, kuriose yra informacinės sistemos. Fizinės vertybės yra vertinamos pagal jų pakeitimo kaštus. Duomenų ir programinės vertybės yra vertinamos pagal jų sukeliamą poveikį organizacijos veiklai jeigu informacija bus neprieinama, sunaikinta, nesankcionuotai atskleista ar pakeista.

Žinant saugumo incidentų poveikį ir problemas, kurias jie gali sukelti, *grėsmių ir pažeidžiamumų įvertinimo etape* yra nustatoma grėsmių atsiradimo tikimybę. *CRAMM* apima pilną tyčinių ir atsitiktinių grėsmių, galinčių paveikti informacijos saugumą, spektrą, įskaitant:

- Įsilaužimus;
- Virusus;
- Techninės ir programinės įrangos veikimo sutrikimus;
- Tyčinę žalą arba terorizmą;
- Žmonių klaidas ir t.t.

Užbaigus šį etapą, yra gaunamas rizikos lygio įvertinimas.

CRAMM metodikoje yra sukaupta labai didelė kontrolės priemonių biblioteka, kurią sudaro virš 3000 kontrolės priemonių, suskirstytų į 70 loginių grupių. *Kontrolės priemonių parinkimo ir rekomendacijų* etape *CRAMM* programiniai įrankiai įgalina lyginti praeitame žingsnyje gautus rizikos lygius su kontrolės priemonių apsaugos lygiais, siekiant nustatyti, ar rizika yra pakankamai didelė, kad būtų pateisintas tam tikros kontrolės priemonės diegimas.

Egzistuoja keletas skirtingų *CRAMM* metodikos versijų, skirtų konkrečioms geografinėms rinkoms ir valstybinėms institucijoms:

- *CRAMM Standard Profile* - tai plačiausiai taikomas versija, kuri yra prieinama tiek valstybinėms institucijoms, tiek komerciniams vartotojams visame pasaulyje.
- *CRAMM NATO Profile (CRAMM (NATO) Toolkit)* - speciali *CRAMM* versija, skirta NATO ir šalių karinėms organizacijoms, kuri apima specifines grėsmes ir kontrolės priemones. Ji taip pat nustato situacijas, kurioms esant, yra laikoma, kad minimalios NATO rizikos ribos yra peržengtos. *CRAMM NATO Profile* taip pat gali naudoti organizacijos, kurios siekia prisijungti prie NATO sistemos ar tinklo, arba teikiančios tokias paslaugas. Ši *CRAMM* versija yra prieinama tik pagal specialų susitarimą su NATO saugumo tarnyba.
- *CRAMM Standard Consultancy Profile* - suteikia teisę įsigijusiai organizacijai taikyti metodiką ne tik savo reikmėms, bet ir teikti paslaugas klientams.

Pabrėžiant *CRAMM* metodo populiarumą, pateiksime kelėta žinomiausių jos vartotojų. Lietuvoje informacijos apsaugos rizikos analizės ir valdymo metodiką *CRAMM* turi įsigiję šie klientai[10]:

- *CRAMM Standard profilį:*
  - AB „Lietuvos energija“;
  - AB „Lietuvos geležinkeliai“;
  - Lietuvos Respublikos finansų ministerija;
  - Lietuvos Respublikos vidaus reikalų ministerija;
  - Valstybinė mokesčių inspekcija prie Lietuvos Respublikos finansų ministerijos.
- *CRAMM NATO profilį:*
  - Krašto apsaugos ministerija (Ryšių ir informacinių sistemų tarnyba).
- *CRAMM Standard Consultancy profilį:*
  - UAB „Compservis“;
  - UAB „Alna Intelligence“.

Kitų valstybių žinomiausi vartotojai yra[11]:

- AE Systems Electronic;
- DEFRA;
- English Heritage;
- GEC-Marconi Secure Systems;
- General Motors AC;
- IBM;

- Royal Air Force;
- Serious Fraud Office;
- Swiss Bank Corporation;
- T Mobile;
- Thames Valley Police;
- The Council for the European Union;
- WS Atkins Consultants.

2.2. EBIOS

EBIOS yra išsamus rinkinys nurodymų, skirtų informacijos sistemų rizikos valdymui. Šiai metodikai taip pat yra sukurtas nemokamas įrankis, palengvintais jos realizavimą. *EBIOS* buvo sukurtas Prancūzijos vyriausybės ir dabar yra palaikomas grupelės įvairių ekspertų, kurie veiklą vykdo rizikos valdymo forumo pagalba. Toks metodo palaikymo būdas suteikia galimybę taikyti geriausią praktiką bei pateikti taikomosios programos dokumentaciją įvairiame kontekste. *EBIOS* yra plačiai naudojama viešajame ir privačiame sektoriuje, Prancūzijoje ir kitose valstybėse. Metodas yra suderinamas su pagrindiniais IT saugos standartais.

EBIOS padeda įgyti globalią ir aiškią viziją, kuri yra naudinga aukštesniems vadovams priimant spendimą globaliuose projektuose (verslo tęstinumo plano, pagrindinio saugumo plano, saugumo politikos), ar specifinėse sistemose. *EBIOS* suteikia aiškesnį bendravimą tarp projekto savininko ir projekto vadovo saugumo klausymais. Toks būdas palengvina bendradarbiavimą tarp saugumu specialistų ir niekuo saugume nenusimanančiųjų [17].

EBIOS metodo vykdymas paremtas ciklo principu, kuris susideda iš penkių etapų:

- Pirmajame etape yra nagrinėjamas rizikos valdymo kontekstas globaliame verslo procese, kuris yra susijęs su informacinėmis sistemomis (prisidėjimas prie globalių grėsmių, tikslus ribų apibrėžimas, tiesiogiai susijusios informacijos srautų ir funkcijų skaidymas);
- Antrame etape yra atliekama saugumo reikalavimų analizė;
- Trečiame etape yra atliekama grėsmių analizė;
- Ketvirtame ir penktame etape yra nustatomos būtinos ir pakankamos saugumo priemonės bei tolimesni saugumo reikalavimai. Taip pat yra aiškiai įvardijama likutinė riziką.

EBIOS yra lankstus įrankis. Į ši įrankį lengvai galima įkelti *IT Grundschutz* standarto žinių bazes (atakų metodus,vientisumo, pažeidžiamumo) ir geriausios praktikos katalogus iš *ISO/IEC IS 17799* standarto. Ši metodologija išsamiai apžvelgia rizikos valdymo ir rizikos analizės etapus, ją galima taikyti įvairaus dydžio organizacijose ir pakanka standartinių žinių.

2.3. ISF metodai (FIRM, IRAM, SARA, SPRINT)

ISF yra tarptautinė organizacija, kurią vienija 296 korporacijos ir privataus sektoriaus organizacijos. *ISF* yra pateikusi rinkinį rizikos vertinimo ir valdymo metodų. Jie gali būti panaudoti organizacijoje įvairiais būdais gerinant saugumo lygį. *ISF* metodai yra suskirstyti penkiais skirtingais aspektais, kurių kiekvienas skirtas tam tikrai aplinkai [4]:

- Saugumo valdymas (įmonės rėmuose);
- Kritinės verslo taikomosios programos;
- Kompiuterio diegimai;
- Tinklas;
- Sistemų plėtojimas.

FIRM - vienas iš *ISF* metodologijų, skirtų informacijos rizikos stebėjimui ir kontrolei įmonės lygyje. Šis metodas buvo sukurtas efektyviam informacijos saugumo stebėjimui. Jis įgalino informacijos riziką valdyti sistemingai visos įmonės mastu. Į *FIRM* yra įtraukti išsamūs įgyvendinimo nurodymai, kurie paaiškina kaip įgyti saugumo palaikymą bei kaip priversti saugumo sistemą tinkamai veikti. Šiame metode yra naudojamos formos, kurios padeda surinkti daugybė svarbių detalių apie tam tikrą informacijos resursą. Yra renkami tokie duomenys kaip: sistemos savininko vardas, grėsmės lygis, poveikis verslui, pažeidžiamumai ir t.t.

IRAM yra rizikos analizės metodologija, paremta dešimties metų tyrimų. Ji susideda iš trijų etapų:

- Įtakos verslui įvertinimo;
- Grėsmių ir pažeidžiamumų įvertinimo;
- Kontrolės pasirinkimo.

SARA - metodas, skirtas informacijos rizikos analizei kritinėse informacijos sistemose. Jis susideda iš keturių etapų:

- Planavimas;
- Verslo reikalavimų identifikavimas saugumui;
- Pažeidžiamumų įvertinimas ir kontrolės reikalavimai;
- Ataskaitos.

SPRINT yra santykinai greita ir lengvai naudojama metodologija, skirta įvertinti poveikį verslui ir analizuoti informacijos rizikas svarbiose, bet ne kritinėse informacinėse sistemose. Šis metodas pirmiausia padeda įvertinti rizikos, susietos su sistema, lygį. Kitame žingsnyje *SPRINT* padeda nustatyti kaip elgtis su iškilusia rizika. Ir paskutiniame etape yra sudaromas veiksmų planas, kad išlaikyti rizikos lygį tenkinančiame lygyje. *SPRINT* gali padėti:

- Nustatyti sistemos pažeidžiamumus ir kontrpriemones;
- Apibrėžti sistemos, esančios kūrimo stadijoje, saugumo reikalavimus bei kontrolės priemones, padedančias tų reikalavimų laikytis.

2.4. IT Grundschutz/IT Baseline Protection Manual

IT-Grundschutz/IT Baseline Protection Manual pateikia organizacijai metodus, padedančius įsteigti ISMS. Jis susideda iš bendrų IT saugumo rekomendacijų, skirtų įgyvendinti tinkamą IT saugumo procesą, ir detalių techninių rekomendacijų, skirtų pasiekti būtiną IT saugumo lygį specifinėse srityse (rizikos valdymo ir analizės etapai yra aprašyti *IT-Grundschutz* 6 skyriuje – „Handling threats“). *IT-Grundschutz* siūlomas IT saugumo procesas susideda iš tokių žingsnių [23]:

- Procesų nustatymas:
    - Apibrėžimas IT saugumo tikslų ir verslo aplinkos;
    - Organizacijos IT saugumo struktūros įsteigimas;
    - Reikalingų resursų aprūpinimas.
- IT saugumo koncepcijos kūrimas:
    - IT struktūros analizė;
    - Apsaugos reikalavimų įvertinimas;
    - Modeliavimas;
    - IT saugumo patikrinimas;
    - Papildoma saugumo analizė.
- Įgyvendinimo planavimas ir vykdymas;
- *IT-Grundschutz* sertifikavimas (neprivalomas).

IT-Grundschutz moduliuose yra pateiktas sąrašas susijusių grėsmių ir reikalingų kontrpriemonių grėsmei sumažinti. Priklausomai nuo organizacijos reikmių, sąrašas gali būti išplėstas ar papildytas. Šis metodas yra skirtas įvairaus dydžio organizacijoms bei jo taikymui pakanka standartinių žinių. *IT-Grundschutz* pagrindinis tikslas yra pateikti IT saugumo valdymo sistemos gaires (*framework*).

2.5. Austrijos IT saugumo vadovas

Austrijos IT saugumo vadovas susideda iš dviejų dalių. Pirmoje dalyje pateiktas detalus IT saugumo valdymo procesų aprašymas, kuriame yra įtrauktas saugumo politikos rengimas, rizikos analizė, saugumo koncepcijos modelis, saugumo plano įgyvendinimas ir tęstinumo veikla. Antra dalis susideda iš 230 pradinių saugumo kontrpriemonių kolekcijos. Yra prieinamas įrankis(prototipo stadijoje), kuris palaiko metodo įgyvendinimą [4].

Pradžioje šis vadovas buvo sukurtas tik valstybinėms organizacijoms, bet dabar prieinamas visų rūšių verslui. Austrijos IT saugumo vadovas yra suderinamas su *„IT Grundschutz“* metodu bei *ISO/IEC IS 13335* ir dalinai su *ISO/IEC IS 17799* standartais. Šiame vadove yra nagrinėjamos rizikos valdymo ir analizės temos, bet deja nėra apibrėžtas joks specifinis rizikos analizės metodas. Austrijos IT saugumo vadovą galima taikyti įvairaus dydžio organizacijose ir pakanka standartinių žinių, tačiau jis prieinamas tik vokiečių kalba.

2.6. Olandų A&K Analizė

Metodo A&K (*Afhankelijkheids- en Kwetsbaarheidsanalyse)* pirminė versija buvo sukurta visuomeninės Olandijos kompanijos RCC, o 1996 metais šis metodas buvo užbaigtas kurti Olandijos vidaus reikalų ministerijos, kuri taip pat ir išleido vadovą, apibrėžiantį A&K analizę. Šis metodas nebuvo atnaujintas nuo to laiko. *A&K analizė* yra unikalus ir plačiai naudojamas Olandijos valstybiniuose organuose nuo 1994 metų. Taip pat ši analizė yra dažnai naudojama ir Olandijos kompanijų.

A&K analizės metode yra nagrinėjami rizikos identifikavimo, analizės ir įvertinimo etapai. Metodas yra suderinamas su *ISO/IEC IS 17799* standartu*. A&K analizės* taikymui pakanka elementarių žinių ir jis yra pritaikytas įvairaus dydžio organizacijoms. Deja šis metodas prieinamas tik olandų kalba [4].

2.7. ISO/IEC 13335-2

ISO/IEC IS 1335-2 yra ISO standartas, kuris aprašo pilną informacijos saugumo rizikos valdymo procesą bendruoju atveju. Standarto priede yra pateikti rizikos vertinimo būdų pavyzdžiai, sąrašas galimų grėsmių, pažeidžiamumų ir kontrpriemonių. *ISO/IEC IS 1335-2* galima įvardinti kaip baziniu informacijos rizikos valdymo standartu tarptautiniame lygyje, kuris apibrėžia rizikos valdymo proceso gaires. Šiame standarte bendruoju atveju yra apžvelgiami rizikos identifikavimo, analizės ir įvertinimo etapai, o kiek išsamiau rizikos tvarkymo, priėmimo bei komunikacijos etapai [4].

2.8. ISO/IEC IS 17799:2005

ISO/IEC IS 17799:2005 standartas yra kilęs iš Jungtinės Karalystės, tačiau buvo pritaikytas tarptautinės reikmėms. Dokumentas parodo, kas yra gera praktika informacijos saugumo procesuose. Šis standartas nėra nei metodas nei vadovas rizikos valdymui, tik trumpai viename skyriuje yra apžvelgta rizikos identifikavimo ir rizikos grėsmių temos. Standartas yra skirtas aprašyti įvairius veiksmus, kurių reikia imtis, kad tinkamai tvarkyti informacinę sistemą [4].

2.9. ISO/IEC 27001

ISO/IEC 27001 standartas yra skirtas sertifikavimo procesui aprašyti. Jis įgalina lyginti informacijos saugumo valdymą per eilę kontrolės priemonių. Šiame standarte yra aprašomi bendri reikalavimai rizikos identifikavimui, vertinimui, tvarkymui ir priėmimui. *ISO/IEC 27001* yra kilęs iš Jungtinės Karalystės, o ISO, pridėjus kai kuriuos pakeitimus, pritaikė platesnei auditorijai. Sertifikatas yra suteikiamas, jeigu organizacija atitinka visus jame apibrėžtus informacijos saugumo valdymo reikalavimus ir kontrolės priemones [4].

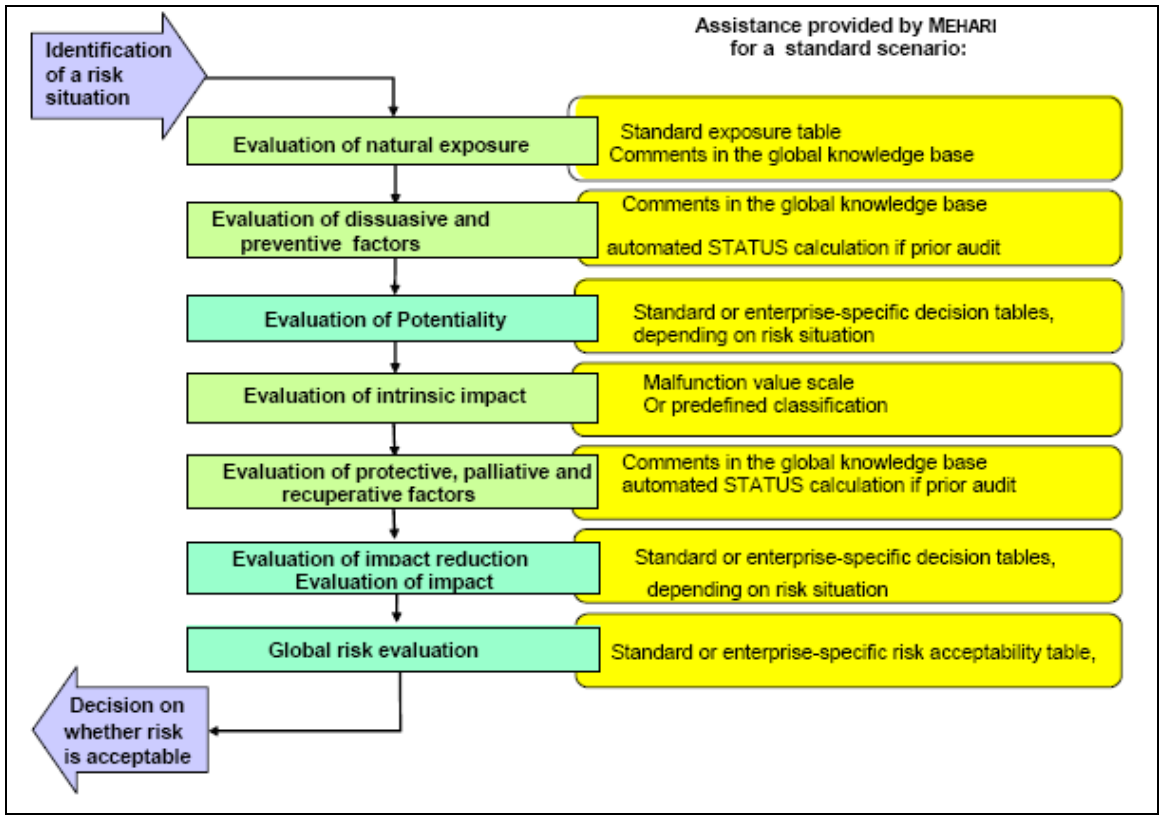
2.10. Marion ir Mehari

MARION (Méthodologie d'Analyse des Risques Informatiques etd'Optimisation par Niveau) rizikos analizės metodologija sukurta CLUSIF saugumo ekspertų. Jos paskutinis atnaujinimas buvo 1998 metais. *MARION* yra paremtas audito metodologijomis, kurios leidžia apytiksliai apskaičiuoti organizacijos IT saugumo rizikos lygį. Rizikos lygio nustatymo procesas yra atliekamas iš užpildytų

formų ir apskaičiuojamas pagal 27 pateiktus indikatorius, suskirstytus į 6 didelius objektus, kurių kiekvienas turi reikšmę nuo 0 iki 4. Šio metodo analizės pabaigoje yra atliekama detalesnė rizikos analizė, kuri nustato, kokios grėsmės ir pažeidžiamumai gresia kompanijai. Šiuo metu *MARION* daugiau nebėra palaikomas CLUSIF, jis yra pakeistas nauju metodu *MEHARI*, tačiau *MARION* ir toliau yra naudojamas įvairiose kompanijose [4].

MEHARI (Méthode Harmonisée d'Analyse de Risques Informatiques) rizikos analizės metodas pateikia rizikos mažinimo priemones, pritaikytas organizacijos objektams. Šis metodas padidina galimybę surasti pažeidžiamumus audito pagalba bei padeda analizuoti įvairias rizikos situacijas. Taip pat *MEHARI* pateikia būdus, kurie palengvina grėsmių identifikavimą ir charakterizavimą, bei optimizuoja teisingų veiksmų pasirinkimą [21]. MEHARI rizikos analizės procesas pavaizduotas 2.2 schemoje.

2.2 schema. MEHARI metodo rizikos analizės procesas [21]



2.11. Octave

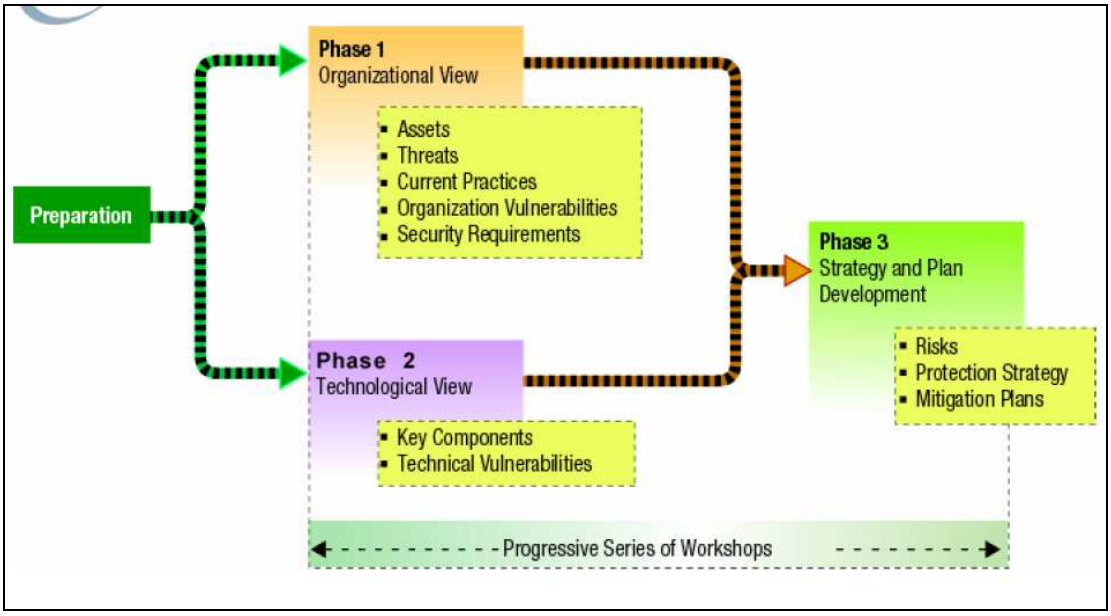
OCTAVE metodologija yra naudojama apibrėžti rizikos vertinimo strategiją ir saugumo planavimo metodus. *OCTAVE* yra skirtas įgyvendinti saugumo strategijas organizacijos žmogiškųjų resursų jėgomis. *OCTAVE-S* yra paprastesnė metodo versija, kuri yra pritaikyta nedidelėms

kompanijoms (iki 100 žmonių). *OCTAVE-S* metodas vykdomas nedidelėje (nuo 3 iki 5 žmonių) komandoje iš organizacijos personalo, kurie renka ir analizuoja informaciją, kuria apsaugos strategiją ir rizikos sušvelninimo planus, paremtus unikalia organizacijos struktūra. Grupės nariai turi gerai išmanyti organizacijos verslo ir saugumo procesus, kad efektyviai išnaudoti OCTAVE-S galimybes [20].

Octave metodas susideda iš trijų etapų (žr. 2.3 schemą):

1. Vertybėmis paremtas grėsmių nustatymas;
2. Infrastruktūros pažeidžiamumų identifikavimas;
3. Saugumo strategijos ir plano rengimas.

2.3 schema. Octave metodo etapai[20]



2.12. Metodikų palyginimas

Ištyrus rizikos valdymo ir vertinimo metodikas, palyginsime jų savybes pagal tokius kriterijus (žr. 2.1 lentelę):

1. Rizikos identifikavimo, analizės, įvertinimo, vertinimo, tvarkymo, priėmimo ir komunikacijos aprašymo detalumo lygis;
2. Metodikų/Standartų įkainiai;
3. Kokio tipo organizacijoms skirtas metodas;
4. Reikalingų įgūdžių lygis, norit pritaikyti metodą organizacijoje;
5. Metodikos licencijavimas;
6. Ar suteikia metodika sertifikatą;

7. Kokie programiniai įrankiai yra sukurti, kad palengvinti metodikos realizavimą organizacijoje;
8. Su kokiais standartais yra suderinamas metodas.

2.1 lentelė. Rizikos valdymo/vertinimo metodų palyginimas

Atributai / Metodas	Rizikos vertinimas			Rizikos valdymas				Metodo kaina	Skirta organizacijos	Reikalingos žinios	Licencijavimas	Sertifikavimas	Skirti įrankiai	Suderinama su IT standartais
	Rizikos identifikavimas	Rizikos analizė	Rizikos įvertinimas	Rizikos vertinimas	Rizikos tvarkymas	Rizikos priėmimas	Rizikos komunikacija							
Austrijos IT saugumo vadovas	••	•	•	•••	•••	•••	•••	Nemok.	Visoms	**	Ne	Ne	Prototipas	ISO/IEC IS 13335-1,-2; ISO/IEC IS 17799 (iš dalies)
CRAMM	•••	•••	•••					Mok.	Val, Did	***	Ne	Ne	CRAMM expres, CRAMM expert	ISO/IEC IS 17799
Olandų A&K analizė	•••	•••	•••					Nemok.	Visoms	*	Ne	Ne		ISO/IEC IS 17799
EBIOS	•••	•••	•••	•••	•••	•••	•••	Nemok.	Visoms	**	Taip	Ne	EBIOS v2 (atviro kodo)	ISO/IEC IS 27001, 15408, 17799, 13335, 21827
ISF metodai	•••	•••	•••	•••	•••	•••	•••	Nemok.	Visoms, išskyrus MV	* iki ***	Ne	Ne	Įvairūs ISF įrankiai (nariams)	ISO/IEC IS 17799
ISO/IEC IS 13335-2	••	••	••	••	•••	•••	•••	100 €	Visoms	**	Ne	Ne	Ebios	ISO/IEC IS 13335-1, 17799, 27001
ISO/IEC IS 17799	•				•			130 €	Visoms	**	Ne	Taip	Daug	ISO/IEC IS 13335
ISO/IEC IS 27001					•	•		80 €	Val, Did	**	Taip	Taip	Daug	ISO/IEC IS 17799
IT-Grundschulz	•••	•••	•••	•••	•••	•••	•••	Nemok.	Visoms	**	Taip	Taip	Daug	ISO/IEC IS 17799, 27001
MARION	•••	•••	•••					Mok.	Did	*	Ne	Ne		
MEHARI	•••	•••	•••					100-150€	Visoms	**	Ne	Ne	RISICARE	ISO/IEC IS 17799, 13335
OCTAVE	••	••	••	••	••	••	••	Nemok	MV	**	Ne	Ne	Octave	

Aprašymo detalumo lygis. („“ - jokio „•“ - mažas„••“ - vidutinis „•••“ - detalus).
Reikalingų įgūdžių lygis („*“ - bazinis, „**“- standartinis, „***“ - specialisto)
Organizacijos („MV“ – mažos ir vidutinės, „Val“ – valstybinės, „Did“ – didelės, nuo 250 žmonių)

Kiekviena aukščiau aprašyta metodika daugiau ar mažiau apžvelgia rizikos valdymo ir analizės etapus. Organizacijai, prieš pradedant taikyti vieną iš paminėtų metodikų, reikėtų įvertinti: kokie jai rizikos valdymo etapai yra aktualiausi, ar atitinkamas metodas tinka organizacijos politikai, ar įmonė bus pajėgi realizuoti vieną ar kitą metodą, ar metodas tinka organizacijos dydžiui bei kokius sertifikatus gali padėti įgyti pasirinka metodika.

Ištirtus populiariausius rizikos valdymo ir vertimo metodikas, pastebėta, kad jos nėra tikslingai pritaikytos naudoti informacinės sistemos kūrimo procese, kadangi analizuotų metodų keliami tikslai ir uždaviniai yra plačiau apbrėžti už IS rėmus. Tokie rezultatai patvirtina šio darbo iškelta problemą, kad trūksta rizikos analizės metodo, tikslingai pritaikyto naudoti IS kūrimo procese.

3. RIZIKOS VALDYMO IR VERTINIMO ĮRANKIAI

Pagrindinė įrankių paskirtis yra automatizuoti rizikos valdymo ir vertinimo procesą, kad analitikai daugiau lako galėtų skirti sudėtingiems ir intelekto reikalaujantiems tyrimams. Beveik visų įrankių veikimo metodai yra paremti tam tikru saugumo standartu ar metodologija. Daugumoje jų yra įdiegta grėsmių ar kontrpriemonių žinių bazė, automatinis ataskaitų ar dokumentų rengimas, moduliai, kurie palengvina duomenų surinkimą, ir kitos būtinosios rizikos valdymo funkcijos. Be rizikos valdymo funkcionalumo, nemažai įrankių turi modulius, padedančius organizacijai įvertinti, pasiekti ar valdyti atitikimą saugumo standartų keliamiems reikalavimams. Sukurtų įrankių tikslai yra pakankamai panašus, bet taikomi metodai ir funkcionalumas kiekvieno įrankio skiriasi. Šiame skyriuje bus tiriami ir lyginami populiariausi įrankiai, skirti rizikos valdymo ir vertinimo procesų automatizuoti.

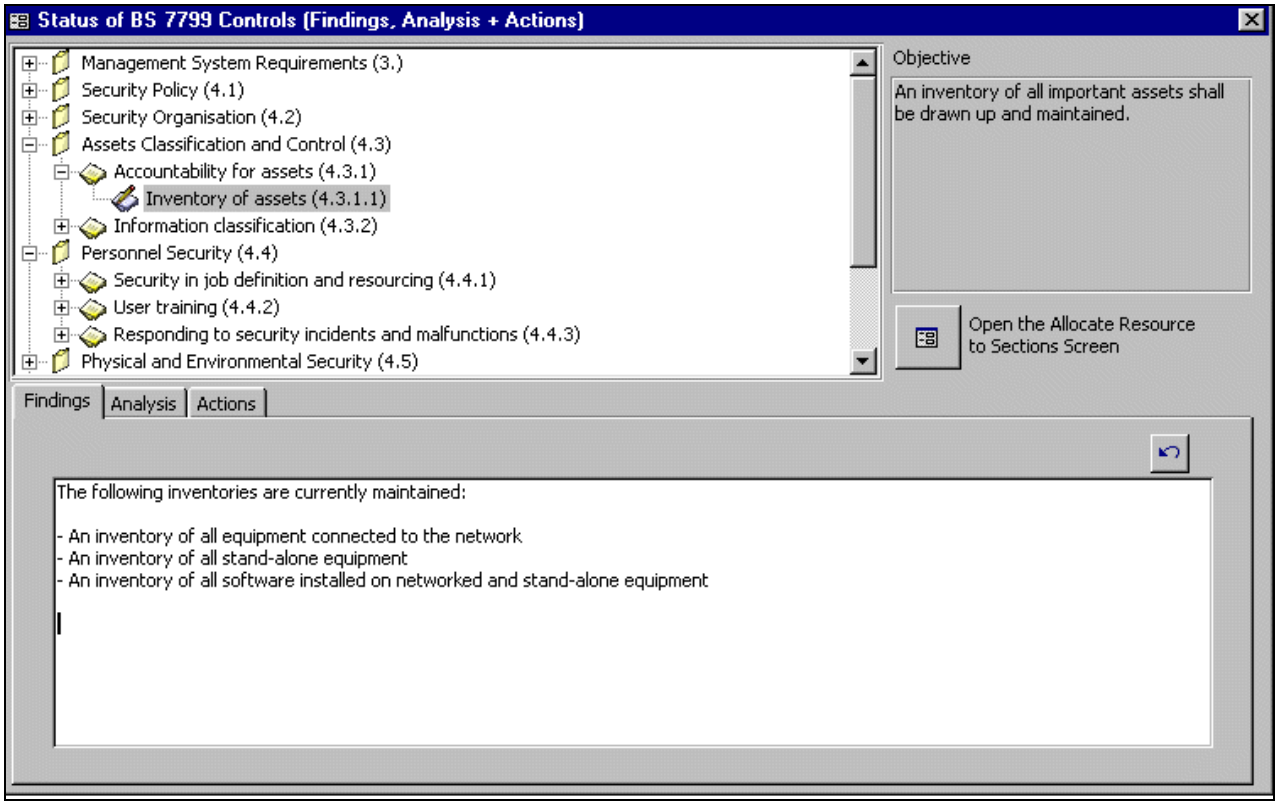
3.1. CRAMM

CRAMM įrankis skirtas palengvinti CRAMM rizikos valdymo metodo vykdymą (plačiau aprašyta 2.1. skyriuje). Visi trys *CRAMM* metodo etapai yra pilnai palaikomi šios programos. Įrankis turi 3500 apsaugos kontrolės priemonių sąrašą, apibrėžtus rizikos vertinimus bei išsamias pagalbines rizikos valdymo priemones, skirtas apsaugos gerinimo planavimui ir apsaugos biudžeto sudarymui. Yra įdiegtos tokios funkcijos kaip: grafinės kontrpriemonių ataskaitos, ataskaitų eksportavimas į MS word/Excel/Graph, apsaugos resursų katalogas, kopijavimo ir palyginimo priemonės, leidžiančios kopijuoti informaciją iš vieno vertinimo į kitą bei atlikti palyginimus.

CRAMM įrankis padeda organizacijoms įvertinti atitikimą *BS 7799* standarto reikalavimams, suplanuoti ir įgyvendinti veiksmus, būtinus atitikimą pasiekti (šis modulis pavaizduotas 3.1 paveiksle). *CRAMM* atitikimo *BS 7799* analizės priemonės apima šiuos aspektus [10]:

- ISMS apimties nustatymas;
- ISMS valdymo gairių (*Management Framework*) nustatymas;
- Neatitikimų (*GAP*) analizės atlikimas;
- Informacijos apsaugos gerinimo programos kūrimas;
- Tinkamumo pareiškimo (*Statement of Applicability*) parengimas;
- Informacinių vertybių registro sukūrimas;
- *BS 7799* standarto reikalavimus atitinkančios rizikų analizės atlikimas.

3.1 paveikslas. CRAMM atitikimo BS7799 modulis[11]



CRAMM kontrolės priemonių duomenų bazė pati savaime yra labai vertingas resursas. Ji apima visas informacijos apsaugos sritis, įskaitant techninius, fizinius, personalo apsaugos aspektus, dokumentacijos ir procedūrines priemones. Kontrolės priemonės yra parengtos pagal informaciją, gautą iš daugybės patikimų šaltinių ir pripažintų standartų (BS 7799, ITSEC, UK Government Security Authorities) bei įvairių informacijos apsaugos konsultantų. Kiekviena kontrolės priemonė charakterizuojama pagal[10]:

- Vertybę, kuriai ji yra taikoma;
- Tipą (paskirtį) (pavyzdžiui, ar ji sumažina apsaugos pažeidimo grėsmę, ar pažeidžiamumą, ar pažeidimo poveikį, leidžia aptikti sutrikimus ar palengvina atstatymą);
- Rizikas, kurioms ji tinkama;
- Efektyvumą;
- Kaštus;
- *BS 7799* standarto kontrolės tikslus, kuriuos padeda pasiekti.

Vartotojai gali naršyti po kontrolės priemonių duomenų bazę bei nurodyti kontrolės priemones, kurios gali būti svarbios jų veiklai bei informacinėms sistemoms. *CRAMM* rizikos vertinimo priemonės leidžia nustatyti ar kontrolės priemonės yra reikalingos ir ar jų diegimas yra

pagrįstas. Kontrolės priemonių duomenų bazė ir nuolat atnaujinama, atsižvelgiant į informacijos apsaugos procesų, standartų ir technologijų naujoves.

CRAMM įrankyje yra nemažas skaičius pro-forma dokumentų ir vedlių (*Wizards*), kurie yra puiki pagalbos priemonė organizacijoms, kuriančioms visapusišką informacijos apsaugos dokumentaciją, įskaitant[10]:

- Informacijos apsaugos politiką;
- ISMS apimtį (pagal *BS 7799* standarto reikalavimus);
- ISMS valdymo gaires (*Management Framework*);
- Rizikų analizės ataskaitą;
- Rizikų valdymo ataskaitą;
- Informacinių sistemų apsaugos politiką;
- Duomenų mainų sutartį.

CRAMM įrankis yra platinamas *Expert* ir *Express* versijomis. *CRAMM Expert* versija yra profesionalus informacijos saugumo įrankis, skirtas detaliai rizikos analizei, o *CRAMM Express* versija yra skirta bazinio lygio rizikos vertinimui kai pilnas rizikos vertinimas nėra reikalaujamas. *CRAMM Express* puikiai tinka kai informacijos saugumo rizikos vertinimą reikia perdotuoti įgyvendinti IT projektų vadovams, sistemos vadovams ar operacijų vadovams, kurie neturi pakankamos patirties rizikos analizėje. Be to, norint naudotis *CRAMM Expert* įrankiu, būtina turėti *CRAMM* metodo žinių, o *CRAMM Express* gali naudotis vartotojas, kuris prieš tai nėra nieko girdėjas apie *CRAMM* [11].

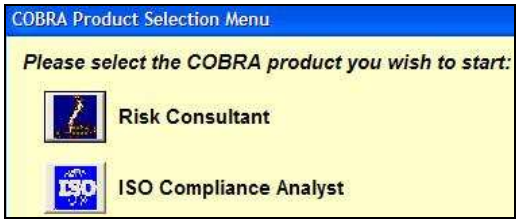
CRAMM įrankis palaiko identifikavimo, analizės, įvertinimo, vertinimo ir tvarkymo rizikos valdymo etapus. Nėra tik nagrinėjami rizikos priėmimo ir komunikacijos etapai, tačiau papildomai yra vertybių identifikavimo ir įvertinimo galimybė. *CRAMM Expert* kaina yra 2950£ + 875£ metinė licencija, o *CRAMM Express* 1500£ + 250£ metinė licenzija [4].

3.2. Cobra

Cobra - rizikos valdymo programa, kuri gali būti naudojama grėsmių identifikavimui ir atitinkamų kontrpriemonių nustatymui. Ji gali išmatuoti rizikos lygį kiekvienai sričiai ir nurodyti jos poveikį verslui. Produktas pasiūlo detalų sprendimą ir rekomendacijas kaip sumažinti riziką. Paruošia tiek verslui tiek technikams skirtas ataskaitas. Šis įrankis yra skirtas smulkioms ir vidutinėms įmonėms, kad jos galėtų pačios atlikti rizikos analizę be išorinių specialistų pagalbos.

Cobra įrankis susideda iš dviejų dalių: rizikos konsultanto ir ISO atitikimo analitiko (žr. 3.2 paveikslą).

3.2 paveikslas. Cobra produktai[25]



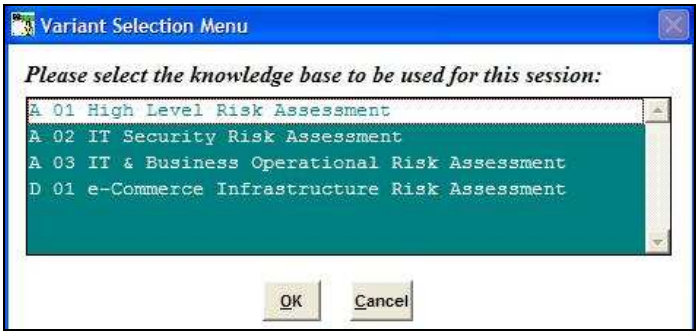
Risk Consultant buvo pradėtas kurti 1990 metais. Šis įrankis yra skirtas Windows platformai, kuris naudoja ekspertinės sistemos principus ir rinkinį žinių bazių. *Cobra Risk Consultant* gali[14]:

- Identifikuoti sistemos grėsmes ir pažeidžiamumus;
- Išmatuoti esančios grėsmės laipsnį kiekvienai sistemos sričiai ar aspektui, bei nurodyti kokį poveikį tai turi verslui;
- Pasiūlyti detalų sprendimą ar rekomendaciją, kad būtų sumažinta rizika;
- Suformuoti ataskaitas, skirtas tiek verslo, tiek techniniam personalui.

Viena iš gerųjų *Risk Consultant* savybių yra ta, kad jis pats atlieka analitiko darbą, todėl nereikia išsamių saugumo žinių ar patirties naudojant rizikos valdymo įrankį. Kitas įrankio privalumas yra išsamios žinių bazės, kurios gali būti pakeistos ar papildytos kad prisitaikytų prie organizacijos aplinkos ar specifinių užduočių. Taip pat galima atlikti „*Kas jeigu*“ testavimą, kuris suteikia galimybę dinamiškai nustatyti papildomų kontrolės priemonių įtaką rizikos lygiui.

Risk Consultant turi keturias žinių bazes (žr. 3.3 paveikslą), kurios atlieka skirtingas funkcijas. Pirmoji yra skirta atlikti aukšto lygio rizikos vertinimą visos verslo sistemos mastu. Atroji ir trečioji suteikia galimybę visapusiškai ir detaliai atlikti rizikos vertinimą atitinkamoje srityje. Paskutinioji žinių bazė yra specialiai sukonstruota modernioms tinklinėms sistemoms vertinti.

3.3 paveikslas. Risk Consultant žinių bazės[25]

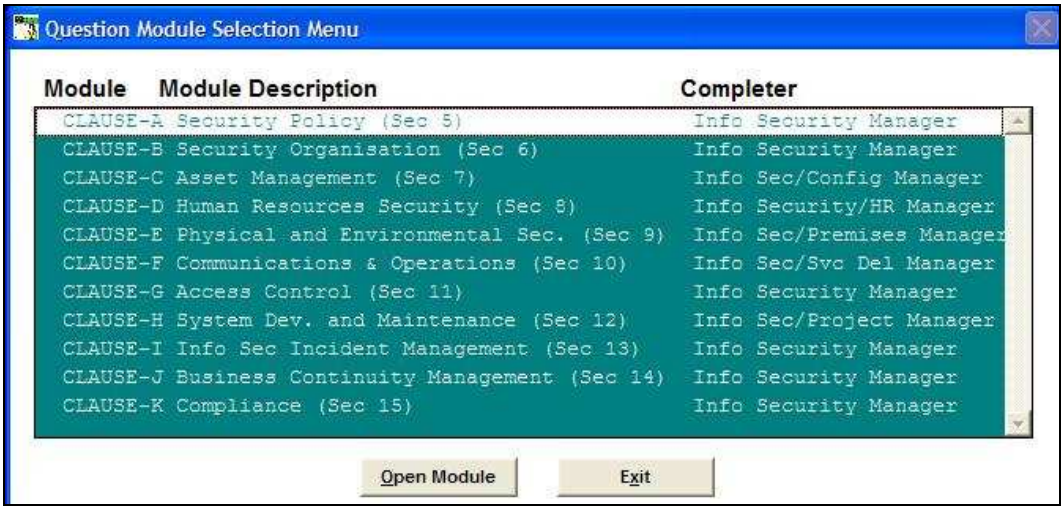


Risk Consultant žinių bazės apžvelgia saugumo grėsmes visapusiškai. Kiekviena potencialios rizikos sritis yra pilnai išanalizuojama, dažniausiai per specifinius klausimų/žinių modulius. Kaip pavyzdį pateiksime sritis, kurios yra įkeltos į IT saugumo žinių bazę[14]:

- Loginis priėjimas; plėtojimas(*development*);
- Sistemos auditas; tinklas, personalas; fizinis priėjimas;
- Pakeitimų kontrolė; sistemos prieinamumas; atsitiktinumai;
- Saugumo valdymas; saugumo supratimas; saugumo administravimas;
- Sistemų programavimas; funkcinis kontroliavimas.

ISO Compliance Analyst modulis yra skirtas įvertinti organizacijos atitikimą *ISO 17799* standartui bei padėti pasiekti atitikimą standartui. *ISO 17799* yra saugumo etalonas organizacijai, kuris susideda iš eilės geriausios praktikos kontrolės priemonių informacijos saugumui. Standartas susideda iš dešimties skirtingų sekcijų, kurios ir yra nagrinėjamos *ISO Compliance Analyst* (žr. 3.4 paveikslą).

3.4 paveikslas. ISO Compliance Analyst pagrindinis meniu[25]



ISO Compliance Analyst yra žinių baze paremtas produktas, kuris, kaip vedlys, padės atlikti užduotis. Jis atidžiai apžvelgs ir nustatys organizacijos situaciją ir atitikimą *ISO 17799* standartui, bei pateiks reikiamas rekomendacijas. Šis įrankis, klausimų su galimų atsakymų pagalba, apžvelgs visas dešimt *ISO 17799* sričių ir atliks[25]:

- Kiekvienos standarto kategorijos atitikimo lygio nustatymą;
- Papildomų kontrolės priemonių nustatymą, kad padidinti atitikimą standartui ir sustiprinti organizacijos saugumą;
- Išsamių ir profesionalių ataskaitų parengimą verslo formatu.

Cobra pilnas paketas kainuoja 1995$. Jeigu reikalingas tik *ISO Compliance Analyst*, tai jo kaina yra 895$ [4]. Taip pat galima atsisiųsti bandomąją *Cobra* versiją, kad išmėginti galimybes.

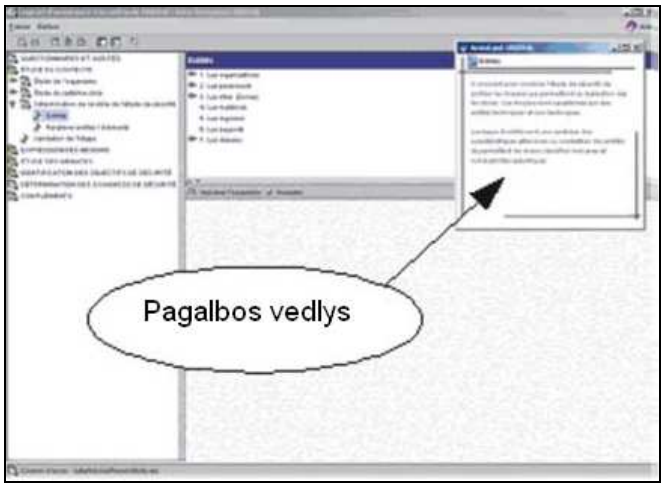
3.3. EBIOS

EBIOS yra *Central Information Systems Security Division* (Prancuzija) sukurtas įrankis, kuris skirtas padėti realizuoti *EBIOS* metodą. Įrankis padeda atlikti visus rizikos analizės ir valdymo žingsnius, remiantis penkiais *EBIOS* metodo etapais(žr. 2.2 skyrių). Taip pat, programa įgalina užfiksuoti visus tyrimo rezultatus bei suformuoti reikalingus dokumentus. *EBIOS* įrankis yra suderinamas su *ISO 13335*, *ISO 15408*, *ISO 17799* standartais. Į programos žinių bazes yra įdiegtos *ISO 15408* ir *ISO 17799* standartų geriausios praktikos. Be to, vartotojas gali lengvai prieiti prie žinių bazių ir jas adaptuoti prie specifinio konteksto. *EBIOS* įrankis padeda[17]:

- Tirti grėsmių šaltinius;
- Identifikuoti saugumo objektus;
- Tirti pažeidžiamumus;
- Formalizuoti grėsmes;
- Identifikuoti sistemos taikinius, pagrindinę informaciją, naudojimo kontekstą, nustatyti vientisumą;
- Apskaičiuoti riziką, apibrėžti rizikos kriterijus;
- Apibrėžti saugumo reikalavimus;
- Išvesti likutinę riziką;
- Sugeneruoti ataskaitas kiekvienam *EBIOS* metodo žingsniui.

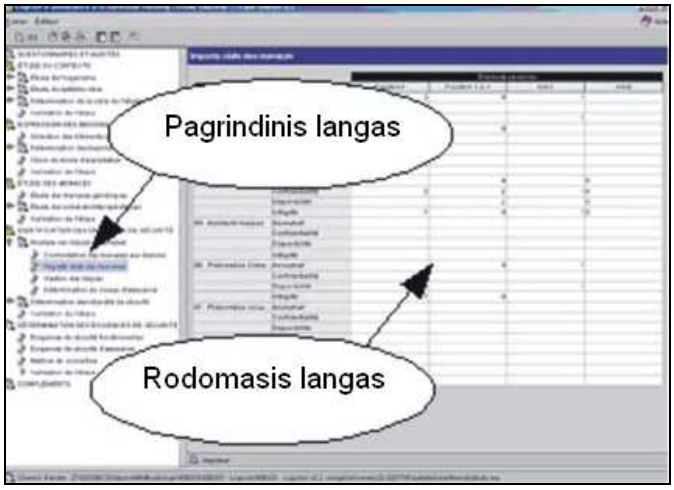
EBIOS programos naudojimąsi palengvina įdiegti pagalbos vedlių(*tutorial*) moduliai su praktiniais pavyzdžiais, kurie palengvina vartotojui vykdyti tyrimus bei atskleidžia įrankio galimybes (žr. 3.5 paveikslą).

3.5 paveikslas. EBIOS įrankio pagalbos vedlys[16]



Įrankis yra paremta *EBIOS* metodo filosofija. Pavyzdžiui žinių bazių ir tyrimų struktūra yra tokia pati kaip ir metodo vadove (tyrimo modulis pavaizduotas 3.6 paveiksle). Tokia struktūra žymiai palengvina įrankio naudojimąsi gerai žinant *EBIOS* metodiką. Iš kitos pusės žvelgiant, įrankių sunku naudotis prieš tai nesusipažinus su *EBIOS* metodika.

3.6 paveikslas. EBIOS tyrimų modulis[16]



Reikia paminėti, kad *EBIOS* įrankis yra atviro kodo, nemokamas ir gali būti įdiegtas į Windows, Linux ar Solaris aplinkas. Programa gali būti lengvai performuota ar papildoma organizacijos poreikiams, nes programiniai kodai yra atviri, yra techninė programos dokumentacija bei specialūs įrankiai programai tobulinti.

3.4. RA2 art of risk

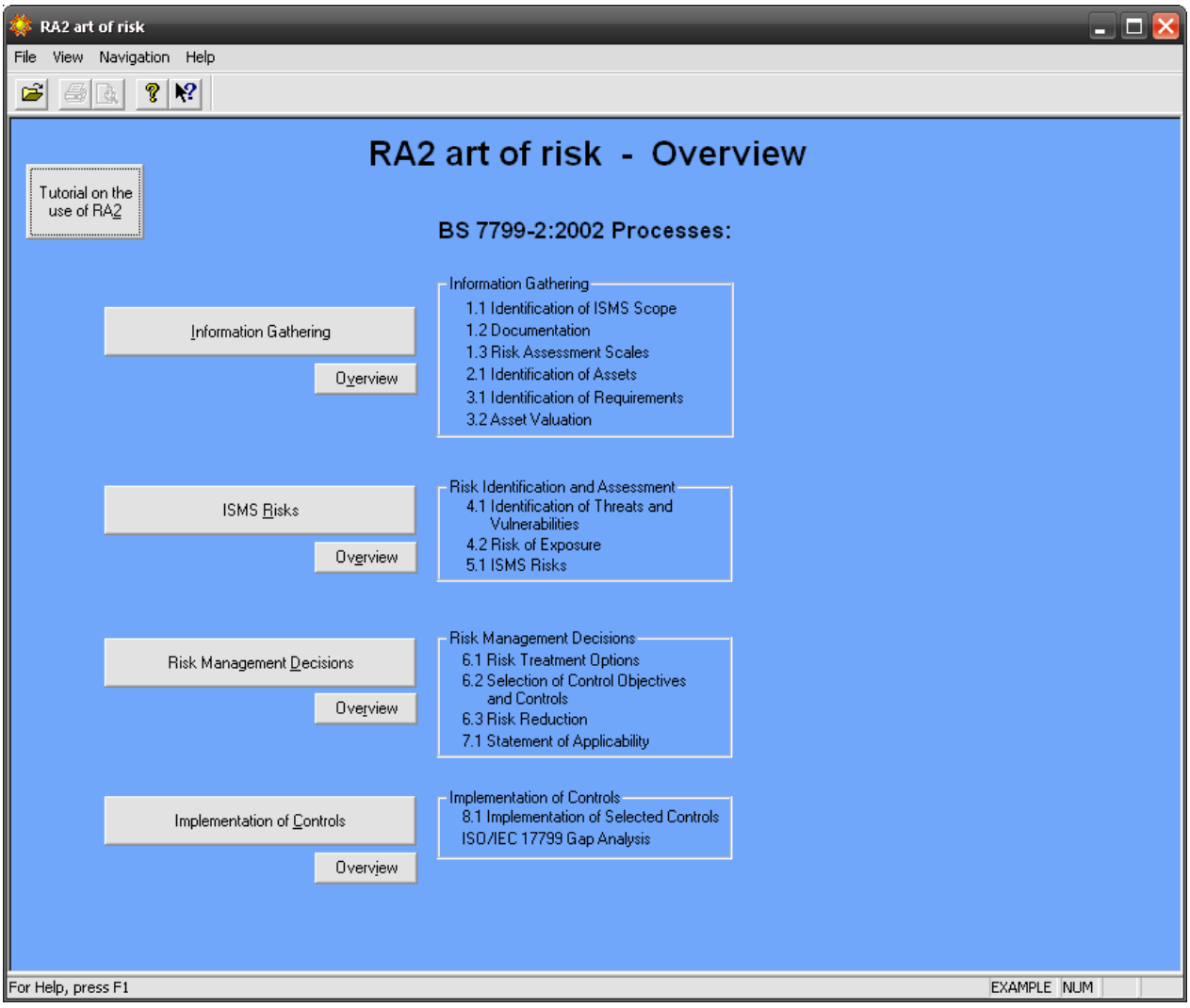
RA2 art of risk yra rizikos valdymo įrankis, paremtas *ISO 17799* ir *ISO 27001* standartais. Programa netik atlieka rizikos vertinimo funkcija, bet ir apžvelgia saugumo procesus kad padėtų organizacijai suprojektuoti ir įdiegti ISMS (įrankio funkcijos pavaizduotos 3.7 paveiksle). Kad padėti organizacijai suprojektuoti ir įdiegti ISMS, kuri atitiktų *ISO 17799* ir *ISO 27001* standartų reikalavimus, yra įkeltos tokios galimybės [12]:

- Verslo reikalavimų ir apimties apibrėžimas, ISMS politika ir objektai;
- ISMS turto inventorizacija;
- ISMS rizikos vertinimas;
- Sprendimo proceso palengvinimas, svarstant tinkamas rizikos mažinimo tvarkymo savybes;
- Kontrolės priemonių pasirinkimas;

- Dokumentavimo palengvinimas ruošiant ISMS dokumentus.

RA2 art of risk įranku yra nesunku naudotis ir lengva įsisavinti „žingsnis po žingsnio“ veikimo principu. Programoje yra įdiegtas „*kas tai*“ pagalbininkas, kuris padeda suprasti vieną ar kitą funkciją. Papildomi patikrinimo klausimai užtikrina, kad niekas nebūtų pamiršta atlikti. Įrankiu galima naudotis per pateiktus pavyzdžius, kurie iliustruoja rizikos vertinimo ir tvarkymo procesą.

3.7 paveikslas. RA2 art of risk įrankio pagrindinis langas[26]



RA2 art of risk gali būti pilnai pritaikytas organizacijos keliamiems reikalavimams, į kuriuos įeina turto įvertinimas, organizacijoje egzistuojančios grėsmės ir pažeidžiamumai ar papildomos kontrolės priemonės, kurios nėra pateiktos su *ISO 17799* vertinimo aprašymu.

Norint sėkmingai vykdyti rizikos vertinimą ir valdymą, būtina surinkti informaciją iš skirtingų šaltinių visos organizacijos mastu. *RA2 art of risk* programa turi papildomą informacijos rinkimo įrankį (*RA2 Information Collection Device*), kuris sugeba surinkti reikiamą medžiagą rizikos vertinimo procesui. Šis įrankis gali būti įdiegtas atskirai nuo *RA2 art of risk* bet kurioje organizacijos vietoje.

Yra išleista naujausia *Ra2 art of risk v1.1* versija, kurios pagrindinis skirtumas yra tas, kad ji palaiko ir senesnį *ISO 17799:2000* ir naujesnį *ISO 17799:2005* standartą bei suteikia galimybę vartotojui lengvai migruoti iš seno prie naujesnio standarto. *RA2 art of risk* kaina yra 1100£, o programos atnaujinimas iki 1.1 versijos dar papildomai kainuoja 200£ [4].

3.5. GStool

GStool įrankis yra sukurtas BSI (*Federal Office for Information Security*) ir yra skirtas padėti vartotojams pasiruošti, administruoti bei atnaujinti IT saugumo koncepciją, kuri yra paremta *IT-Grundschutz* metodikos (plačiau 2.4 skyriuje) reikalavimais.

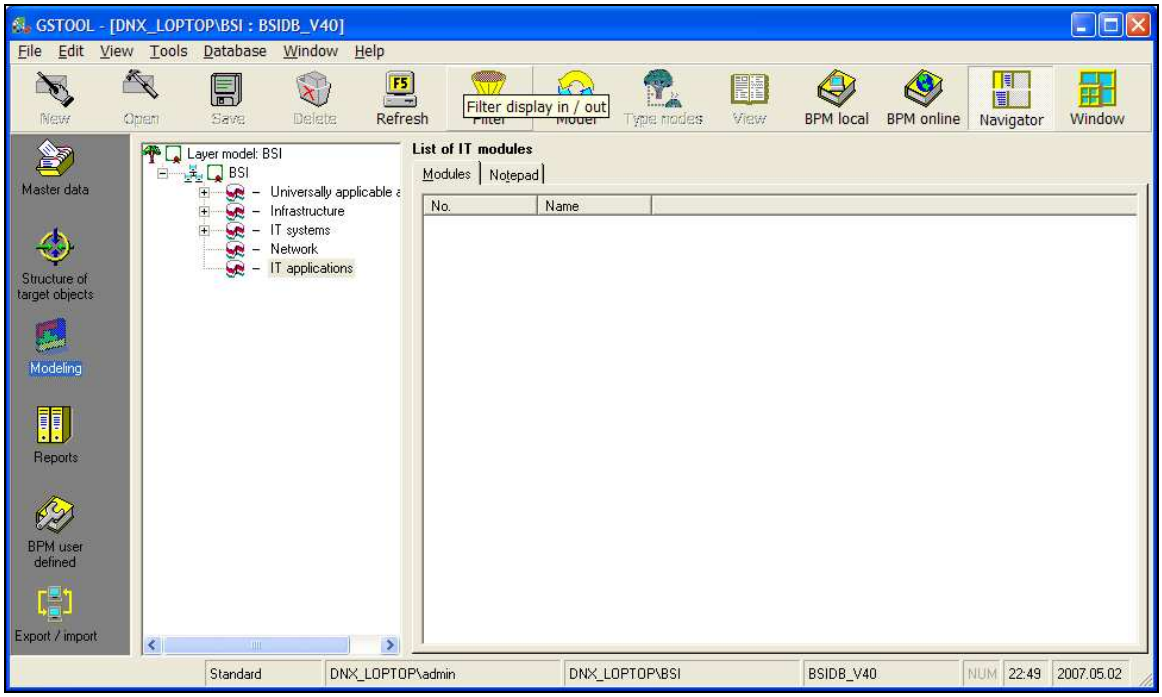
Su *GStool* galima atlikti tokias užduotis (įrankio pagrindinis langas pavaizduotas 3.8 paveiksle) [18]:

- Modeliavimas ir modelių sluoksniavimas pagal atitikimą *IT-Grundschutz*;
- IT sistemų registracija / struktūrinė analizė;
- Taikomųjų programų registracija;
- Saugumo priemonių realizavimas;
- Kainos ir naudos analizė;
- Likutinės rizikos įvertinimas;
- Apsisaugojimo reikalavimų apibrėžimas;
- Ataskaitos;
- Papildomas peržiūrėjimas;
- Bazinio saugumo patikrinimas;
- *IT-Grundschutz* sertifikavimas.

GStool įrankis taip pat turi tokias technines savybes:

- Kelių saugumo koncepcijų administravimas;
- Tinklo palaikymas;
- Dvikalbė aplinka (Vokiečių/Anglų);
- Specifinių duomenų šifravimas juos eksportuojant;
- Istorijos registravimas;
- Patogus dizainas;
- Duomenų bazės lengvai atnaujinamos per elektroninį paštą ar Internetą.

3.8 paveikslas. GStool pagrindinis langas[27]



GStool įrankis naudoja *Microsoft MSDE* ar *Microsoft SQL-Server* duomenų bazės vartotojo duomenims saugoti. Įrankio kaina 887 € [4].

3.6. Callio Secura 17799

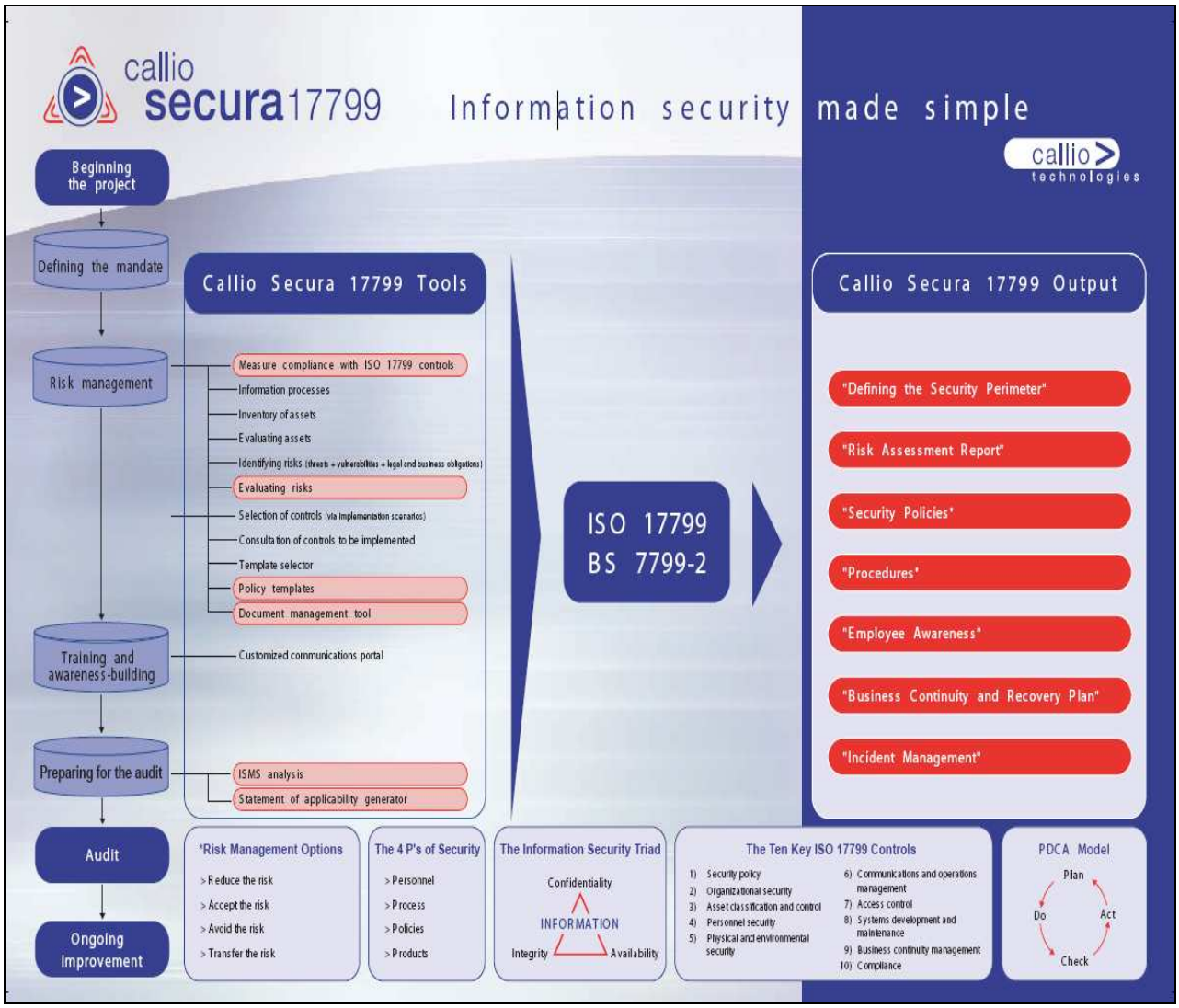
Callio Secura 17799 produktas yra sukurtas *Callio technologies* kompanijos. Programa yra realizuota internetinės svetainės technologija (*web based*) su duomenų bazės palaikymu, kuri suteikia vartotojui galimybę įgyvendinti ir sertifikuoti informacijos saugumo valdymo sistemą. Šis įrankis palaiko *ISO 17799* ir *ISO 27001* standartus bei gali sugeneruoti dokumentus, kurie reikalingi sertifikavimuisi. Taip pat, įmanoma atlikti kitų standartų auditą (pvz. *COBIT* ar *Garbanes&Oxley*) importuojant savo paruoštas apklausos anketas.

Callio Secura 17799 palaikomas funkcionalumas [13]:

- Pažeidžiamumų ir grėsmių identifikavimas, kuris susietas su vertybėmis;
- Siūlomas grėsmių sąrašas;
- Rizikos įvertinimas ir rizikos paskaičiavimas;
- Vertybių inventorizacija ir įvertinimas (yra nemažai praradimo ar pažeidimo įvertinimo pavyzdžių, kurie yra sugrupuotų į kategorijas);
- *ISO 17799* siūlomų kontrolės priemonių sąrašas, kuris padeda sukurti ir įvertinti skirtingus scenarijus;

- Dokumentacijos valdymas;
- *ISO 17799* standarto atitikimo diagnostika (saugumo būklės nustatymas);
- Politikos valdymas (sukuria saugumo politiką naudojant pateikiamus nurodymus ir strategiją);
- Informacijos saugumo terminų žodynas;
- Galimybė išplatinti saugumo dokumentus suinteresuotiems asmenims.

3.9 paveikslas. Callio Secura 17799 veikimo schema[13]



Su *Callio Secura 17799* įrankių galimą (įrankio veikimo schema pavaizduota 3.9 paveiksle):

- Patikrinti atitikimo *ISO 17799* standartui lygį;
- Apibrėžti ISMS struktūrą ir procesus;
- Sumažinti riziką kiekvienai vertybei;
- Apibrėžti kontrolės įgyvendinimo scenarijus;
- Paruošti saugumo politiką (virš 50 pavyzdžių);

- Valdyti politikos dokumentus;
- Patvirtinti ar atšaukti dokumentus, kurie laukia patvirtinimo;
- Kurti, importuoti ar eksportuoti anketas.

Norint naudotis *Callio Secura 17799* įrankiu, reikia turėti tarnybinę stotį, kurioje būtų įdiegta *Windows* operacine sistema, *SQL Server 2000* ar *MySQL* duomenų bazė, *Apache web* serveris bei *Blue Dragon JX* serveris. Naudotojo kompiuteryje tereikia turėti Interneto naršyklę. Šio įrankio 2 vartotojų licenzijos kaina yra 4495 € [4].

3.7. Octave Automated Tool

Octave Automated Tool buvo sukurtas ATI (*Advanced Technology Institute*), kad būtų galima lengviau įgyvendinti *Octave* ir *Octave-S* metodus (plačiau 2.12. skyriuje). Šis įrankis padeda rizikos analitikų komandai surinkti reikalingus duomenis, tvarkyti surinką informaciją, sugeneruoti tyrimų ataskaitas (kurios gali būti eksportuojamos į *MS word*, *Excel* ar *Oracle* duomenų bazę), bei lengviau vykdyti *Octave* metodu paremta rizikos vertinimo procesą. Sukaupti vertinimo duomenys į *Octave Automated Tool* duomenų bazę suteikia analitikų komandai galimybę daugiau laiko skirti intelektinei analizei ar užduočių planavimui, o ne rankiniam duomenų rinkimui ar apdorojimui. Ankstesni rizikos vertinimo duomenys gali būti lengvai panaudoti kaip pagrindas sekantiems rizikos vertinimams , nes surinkti duomenys yra saugomi lankčiai keičiamam formate. Kiekviename programos žinginyje yra nuorodos į pagalbą, kad rizikos vertinimo procesas vyktų sklandžiai ir būtų atsakyta į visus su *Octave Automated Tool* funkcionalumu iškilusius klausimus [20].

Octave Automated Tool programa naudojasi virš 200 pramonės ir valstybės organizacijų visame pasaulyje. Įrankio kainą yra 1500 $ [4].

3.8. Proteus

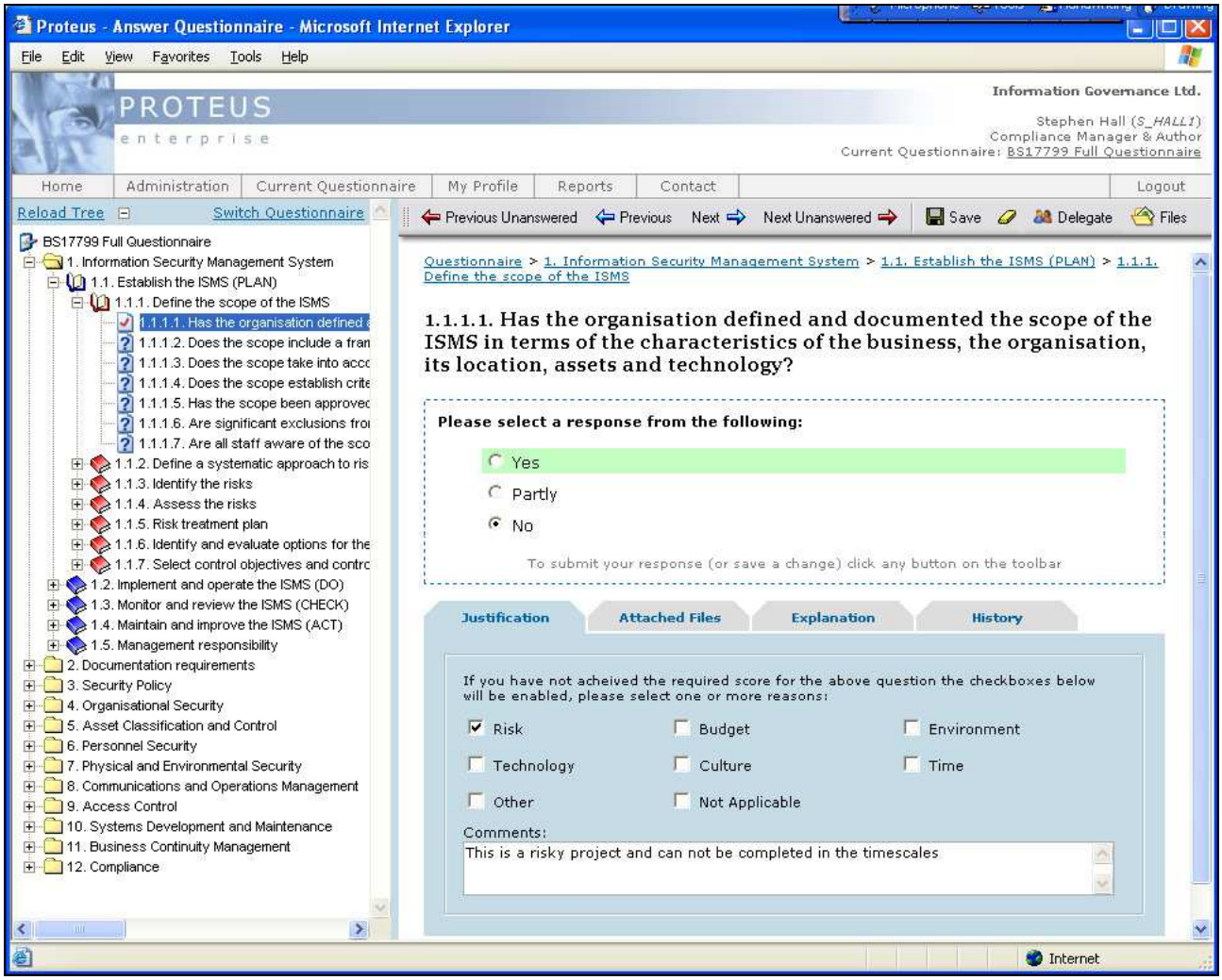
Proteus yra „de facto“ įrankis norint analizuoti, valdyti ar nustatyti atitikimą viešam, pramoniniam ar bendram standartui ar reglamentui (ISO/IEC 17799, BS ISO/IEC 27001, BS 25999, SOX, CobiT, PCI DSS, NIST,, FISMA, ISF SoGP , ISF HC, DPA, CCA, FOI, Basel II, …) [22].

Proteus yra galingas saugumo valdymo įrankis, kuris turi daugybę galimybių bei tvirtus ryšius tarp kiekvieno saugumo valdymo proceso (įrankio langas pavaizduotas 3.10 paveiksle). Pavyzdžiui, bet koks incidentas ar sistemos pakeitimas automatiškai bus fiksuojamas incidentų valdymo, veiksmo planų ar kituose susijusiuose moduliuose.

Pateiksime keletą *Proteus* galimybių:

- Neatitikimų analizė;
- Vertybių inventorizacija ir įvertinimas;
- Vertybių rizikos vertinimas, kuris nukreiptas į saugumo kontrolę;
- Centralizuotas politikos ir procedūrų valdymas su pilna pakeitimų kontrolę;
- Incidentų valdymas ir apsisaugojimas.
- Poveikio verslui ir kritinės infrastruktūros identifikavimas;
- Lankstus ataskaitų valdymas;
- Veiklos tęstinumo valdymas;
- Rizikos analizė;
- Veiksmų planai;
- Dokumentų kontrolė;
- Nuotolinis auditas;
- Automatinis incidentų praneršimo valdymas (trumpąja žinute ar elektroniniu paštu).

3.10 paveikslas. Proteus enterprice įrankio langas[28]



Proteus rizikos valdymo ir vertinimo palaikomas funkcionalumas yra[4]:

- **Rizikos identifikavimas.** Kiekybinis ir kokybinis rizikos vertinimo metodai palaikomi. Abu metodai pilnai integruoti į vertybių valdymą, grėsmes, kontrpriemones, rizikos tvarkymo planus ir incidentų valdymą;
- **Rizikos analizė.** Gali būti naudojamas santykinis ir tiesioginis rizikos vertinimas, kad prisitaikyti prie bendro „rizikos apetito“;
- **Rizikos įvertinimas.** Fizinės, informacinės, aptarnavimo, taikomų programų ar jų kombinacijų vertybės yra palaikomos. Grėsmės gali būti automatiškai paveldėtos per vertybių tarpusavio sąryšius, vietą ar vertybių savybes.
- **Rizikos tvarkymas.** Veikimo planai yra pilnai integruoti į rizikos vertinimą, poveikio verslui analizę, veiklos tęstinumo ir incidentų valdymą.
- **Rizikos priėmimas.** Pilnas sistemos auditas atseka bet kokius jos pasikeitimus. Kiekvienas procesas yra automatiškai fiksuojamas kas tam tikra laiką. Yra palaikomas rizikos priėmimas arba nepriėmimas per elektroninį paštą ar kitas tinklines sistemas.
- **Rizikos komunikacija.** Kiekvienas sistemos aspektas gali būti praneštas arba peržiūrėtas. Su *Proteus RiskView* pagalba galima valdyti informaciją per grafinius „prietaisų skydus“.

Proteus yra internetinės svetainės technologija (*web based*) paremta sistema, kurios tarnybinėje stotyje turi būti įdiegta *Linux* operacinė sistema, *Web serveris*, *PHP*, *MySql* duomenų bazė. Vartoto kompiuteryje reikalinga tik Interneto naršyklė. Įrankių naudojasi daugiau negu 600 vartotojų iš 40 pasaulio šalių. Yra prieinamos trys *Proteus* versijos: *Proteus Solo* (licencijos kainą 600£ per metus), *Proteus Professional* (6000£ per metus), *Proteus Enterprise* (kaina sutartinė) [4].

3.9. Įrankių palyginimas

Ištyrus rizikos valdymo ir vertinimo įrankius, palyginsime jų savybes pagal tokius kriterijus (žr. 3.1 lentelę):

- Ar yra galimybė vykdyti rizikos identifikavimo, analizės, įvertinimo, vertinimo, tvarkymo, priėmimo ir komunikacijos etapus;
- Įrankių versijos ir kainos eurais;
- Ar yra galimybė išbandyti programa nemokamai;
- Kokiomis kalbomis yra pateikiamas įrankis;
- Įrankio vartotojų paplitimas;
- Pagrindinė įrankio paskirtis;

- Su kokiais standartais ar metodikom yra suderinamas įrankis.

3.1 lentelė. Rizikos valdymo/vertinimo įrankių palyginimas

Atributai / Programa	Rizikos vertinimas			Rizikos valdymas				Įrankio kaina eurais	Demonstracinė versija	Palaikomos kalbos	Naudotojų paplitimas	Įrankio pagrindinė paskirtis	Suderinama su IT standartais (metodikom)
	Identifikavimas	Analizė	Įvertinimas	Vertinimas	Tvarkymas	Priėmimas	Komunikacija						
Cramm	X	X	X	X	X			Expert 4321+1282/met. Express 2197+366/met.	X	EN, NL, CZ	Virš 500 vartotojų 23 šalyse	Padėti lengviau įgyvendinti CRAMM rizikos valdymo metodą	CRAMM, ISO 27001 (BS7799)
Cobra	X		X	X	X		X	Pilna versija - 1464 Cobra for ISO17799 - 657	X	EN		Įrankis susideda iš 2 produktų: • *Risk Consultant* -užpildytų anketų duomenimis pats atlieka rizikos analitiko darbą • *ISO Compliance Analyst* – padeda įvertinti ir pasiekti atitikimą ISO 17799 standartui	ISO17799
Ebios	X	X	X	X	X		X	Nemokamas		FR, EN, ES, DE	Virš 1000 vartotojų	Padėti lengviau įgyvendinti EBIOS metodą	ISO17799, ISO13335, ISO15408, EBIOS
Ra2 art of risk	X	X		X	X		X	1611		EN	FR, DE, UK, AU, BR, SE, CA, JP	Padėti suprojektuoti ir įdiegti ISMS, kuri atitiktų ISO 17799 ir ISO 27001 standartų reikalavimus	ISO17799, ISO27001
GStool	X	X	X	X	X	X	X	887	X	EN, DE		Skirtas padėti vartotojams pasiruošti, administruoti bei atnaujinti IT saugumo koncepciją, kuri yra paremta IT-Grundschutz metodikos	IT-Grundschutz
Callio Secura 17799	X		X	X	X		X	2200	X	FR, EN, ES	EU, CA, MX, TW ...	Įdiegti, plėtoti, valdyti bei sertifikuoti ISMS, paremta ISO 17799 / BS 7799-2 standartais	ISO17799 / BS7799-2
Octave Automated Tool	X	X	X	X	X	X		1100	X	EN	Virš 200 vartotojų	Padėti lengviau įgyvendinti OCTAVE ir OCTAVE-S metodus	OCTAVE, OCTAVE-S
Proteus	X	X	X	X	X	X	X	Solo - 880/met. Profesional-8791/met. Enterprise – sutartinė	X	EN	Virš 600 vartotojų 40 šalių	„de facto“ įrankis norit analizuoti, valdyti ar nustatyti atitikimą viešam, pramoniniam ar bendram standartui ar reglamentui	ISO17799, ISO27001, BS 25999, SOX, CobiT, PCI DSS, NIST, FISMA, ISF SoGP , ISF HC, DPA, CCA, FOI, Basel II

Yra ganėtinai platus rizikos valdymo ir analizės įrankių pasirinkimas. Kiekvieno įrankio funkcionalumas dažniausiai yra paremtas vienu ar kitu rizikos valdymo metodu, todėl, prieš pasirenkant organizacijai naudoti vieną iš paminėtų įrankių, ypatingą dėmesį reikėtų atkreipti į įrankio naudojamą metodologiją. Kai kurie įrankiai yra net specialiai sukurti atitinkamo metodo realizavimo palengvinimui ir automatizavimui. Taip pat, reikėtų įvertinti: įrankio kainą, kokius rizikos valdymo ar analizės etapus programa padeda atlikti, kokiomis kalbomis prieinamas įrankis bei su kokiais standartais yra suderinamas.

Ištirtus populiariausius rizikos valdymo ir vertimo įrankius, pastebėta, kad jie nėra tikslingai skirti taikyti informacinės sistemos kūrimo procese (kaip ir tirti rizikos valdymo ir vertinimo metodai), o tai dar kartą patvirtina specifinio rizikos analizes metodo poreikį.

4. RIZIKOS ANALIZĖS METODAI

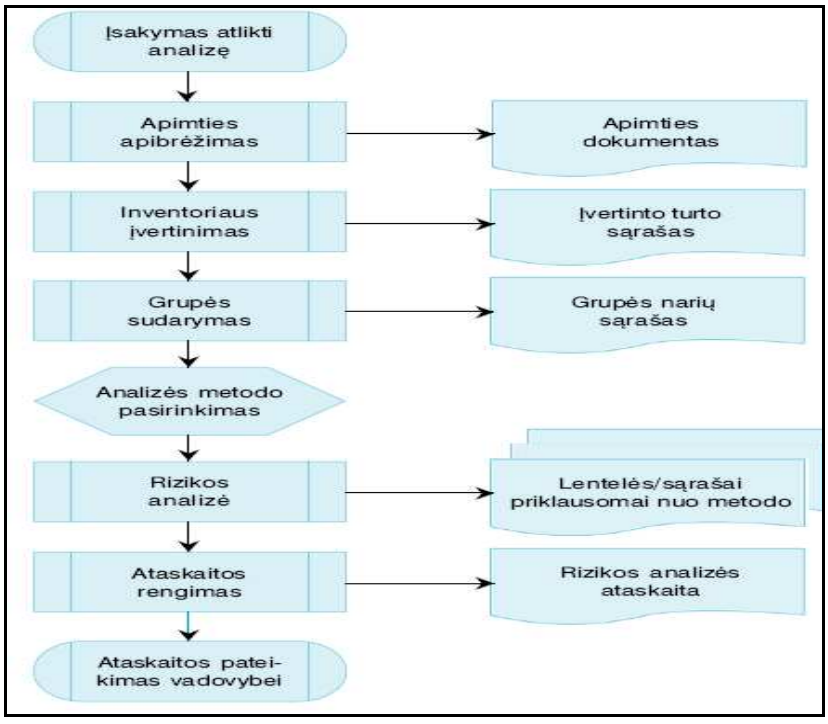
Rizikos analizės metodai skirstomi į dvi pagrindines grupes: kiekybinė rizikos analizė ir kokybinė rizikos analizė. Analizės metodas turi būti pasirinktas atsižvelgiant į analizės tikslą, apimtį, išteklius ir laiką. Kiekybė rizikos analizė labiausiai tinka tais atvejais, kai saugos spendimai daro įtaką finansiniams sprendimams(pvz., biudžetui ar kaštams), tačiau, ji reikalauja didesnių lėšų, laiko bei ekspertų pagalbos. Kokybinė analizė yra paprastesnė už kiekybinę, yra greičiau atliekama, nereikalauja didelių finansinių išteklių bei specialistų pagalbos. Kokybinė rizikos analizė turėtų būti pasirinkta tuo atveju, jeigu priimami spendimai yra susiję su bazinių saugos sukūrimu. Vienas iš rizikos analizės metodo pasirinkimo būdų yra pateiktas 4.1 lentelėje.

4.1 lentelė. Metodo pasirinkimo matrica[3]

	Siauros apimties analizė	**Plačios apimties analizė**
Sprendimai dėl finansavimo / biudžeto lėšų skirstymo	• Atakos medžio metodas (kombinuotas metod.) • TMN (kiekybinis metod.)	• TMN • KURAP
Prioritetų nustatymas / procedūriniai sprendimai	• BS 7799 (kokybinis metod.) • KURAP (kokybinis metod.) • Atakos medžio metodas	• BS 7799 • 3ŽM/10ŽM • KURAP

Nesvarbu kokį rizikos analizės metodą bepasirinktumėte, visi jie turi bendrą procedūrą (žr. 4.1. schemą).

4.1 schema. Bendra rizikos analizės procedūra[3]



4.1. Kiekybinė rizikos analizė

Kiekybinė analizė labiausiai tinkama kai vertinama viena sistema ar viena vertė ir tam turime pakankamai duomenų bei ekspertizės išvadų leidžiančių apskaičiuoti tikimybę ir galimą poveikį. Kiekybinės analizės rezultatas yra finansinė išraiška, kuri parodo tikėtinus nuostolius jeigu nebus imtasi kontrpriemonių konkrečiai grėsmei sumažinti. Jeigu suklasifikuojami ir įvertinami visi elementai (turto vienetų vertė, poveikis, grėsmės dažnumas, saugos priemonių efektyvumas, jų kaštai, grėsmės dažnumas, abejotinas ir tikimybė), ir jiems priskiriamos vertės, tai rizikos analizės metodas ir yra laikomas kiekybinių [3].

Kiekybinės rizikos analizės procesas – tai didelis projektas, kuris reikalauja nemažai pastangų ir laiko, todėl jam reikalingas projekto ar programos vadovas, kuris koordinuotų pagrindinius analizės etapus. Prieš pradedant kiekybinė rizikos analizę, paprastai atliekamas preliminarus saugos įvertinimas, kuris padeda pasirengti ir susikoncentruoti ties kiekybinę rizikos analizę. Šio etapo metu turi būti identifikuota turto vertė, organizacijai kylančių iš aplinkos ir iš personalo grėsmių sąrašas, bei egzistuojančių saugos priemonių dokumentacija.

Vienas paprasčiausių kiekybinės analizės metodu – apskaičiavimas tikėtino metinio nuostolio. Taip pat yra ir sudėtingesnių metodų, kurie pagrįsti aukštomis teorijomis (statistika, kombinatorika, žaidimų teorija, chaoso teorija ir pan.) ar dirbtinio intelekto sistemomis ar neuroniniais tinklais. Sudėtingesnius metodus daugiausiai naudoja draudimo įmonės ar investicinės bendrovės.

TMN metodo atveju kiekybinę rizikos analizę galima suskirstyti į tokius etapus:

1. Analizuojamos vertybės įvertinimas piniginę išraiška;
2. Potencialių grėsmių nustatymas;
3. TMN apskaičiavimas kiekvienai grėsmei;
4. Saugos priemonių parinkimas;
5. Analizės rezultatų paruošimas;
6. Sprendimo pasirinkimas.

4.1.1. Analizuojamos vertybės įvertinimas pinigine išraiška

Vertybės nustatymas piniginę išraiška yra vienas pirmųjų ir vienas svarbiausių analizės etapų, nes visi kiti analizės rodikliai yra tiesiogiai susiję su šia reikšme. Visi gaunami skaičiai, pagal kuriuos yra vertinamos grėsmės ir priimami sprendimai, yra apskaičiuojami iš analizuojamos turto vertės. Turto vertė paprastai išreiškiama atsižvelgiant į tai, kokį tikėtiną poveikį veiklai gali turėti nepageidaujami įvykiai, tokie kaip informacijos atskleidimas, modifikacija, neprieinamumas ar sunaikinimas. Šių įvykių galimas padarinys: finansiniai nuostoliai, rinkos dalies praradimas ar organizacijos įvaizdžio pakenkimas. Vertinamas turtas turėtų būti susietas su:

- įsigijimo ir priežiūros kaštais;
- neigiamu finansiniu poveikiu, kuri organizacijai gali turėti dėl informacijos atskleidimo, jos vientisumo pažeidimo arba neprieinamumo.

4.1.2. Potencialių grėsmių nustatymas

Prieš nustatant finansinę žalą, kuri gali būti įtakota vieno ar kito pažeidžiamumo, reikia identifikuoti įmanomas grėsmės tiriamai vertybei. Kad galėtume nustatyti grėsmes, reikia suprasti vertybės pažeidžiamumus. Šiame etape turi būti įvertintos visų pabudžiu grėsmės, nepriklausomai nuo to, ar jos atrodo tikėtinos, ar ne. Taip pat reikėtų įvertinti kaip dažnai jos gali kartotis. Kai kurios organizacijos gali pateikti jų veikloje iškylančių grėsmių statistiką.

Nustatant grėsmių sąrašą, yra naudinga jas sugrupuoti pagal tipus, šaltinius ar pagal jų numanoma mastą. Pateiksime vieną iš grupavimo pavyzdžių[3]:

- **Duomenų klasifikacija** – duomenų rinkimas arba koncentravimas, kuris gali sudaryti sąlygas neteisingam duomenų interpretavimui, slaptam manipuliavimui kanalais, piktybinio kodo panaudojimui.
- **Informacinis karas** – technologinis terorizmas, piktybinis kodas ar įsiskverbimas karinio ar pramoninio šnipinėjimo tikslu;
- **Personalas** – neteisėtas arba nekontroliuojamas prisijungimas prie sistemų, įgaliotų vartotojų piktnaudžiavimas technologija, nepatenkintų darbuotojų kenkėjiški veiksmai arba suklastotų informacijos duomenų įvestys;
- **Programinė įranga/veikimas –** programa, sąlygojanti procedūrines klaidas arba neteisingas duomenų įvestis;
- **Kriminaliniai atvejai –** vertybės ar informacijos fizinis sunaikinimas ar vagystė, ginkluotas apiplėšimas, fizinė žala personalui;

- **Aplinka –** stichinės nelaimės, paslaugų neteikimas, infrastruktūros gedimai;
- **Kompiuterinė infrastruktūra –** Techninės įrangos gedimai, programinės įrangos veikimo sutrikimai, ryšių sistemos gedimai.
- **Pavėluotas apdorojimas –** sumažėjęs produktyvumas arba pavėluotai gautos lėšos, lemiančios pajamų mažėjimą, išlaidų augimą ar delspinigius.

4.1.3. Tikėtino metinio nuotolio skaičiavimas

Tikėtinas metinis nuostolis – tai nuostolis, kurį gali patirti organizacija dėl vienokios ar kitokios grėsmės per metus. TMN yra skaičiuojamas kiekvienai grėsmei. Šis rodiklis yra išreikštas piniginę suma, todėl jis padeda pasirinkti kokias saugos priemones apsimoka diegti, o kuriais ne. Tai pat, TMN yra pagrindinis rodiklis priimant sprendimą dėl apsisaugojimo nuo grėsmės būdo. Pavyzdžiui, jeigu grėsmės sukeliami metiniai nuostoliai yra mažesni negu tam tikros saugos priemonės įdiegimas ir eksploatacija, tai gal geriau apsidrausti nuo grėsmės, o jeigu TMN mažesnis ir už draudimą, tai gal iš vis nesiimti jokiu saugos priemonių nuo jos.

Norint apskaičiuoti TMN, pirmiausia reikia įvertinti kitus rodiklius, iš kurių ir išvedamas tikėtinas metinis nuostolis. Taigi, pirmiausia reikia sužinoti tokias reikšmes, kaip:

- **Vertybė (V) –** Analizuojamos vertybės piniginė išraiška.
- **Pažeidžiamumo veiksnys (PV)** – žalos procentinė išraiška, kurią patirtų konkrečios vertybės grėsmės realizavimo atveju. PV procentinė vertė gali būti labai maža, pvz., 1% dėl 3 val. sistemos prastovos sąlygotas nuostolis, arba labai didelė, pvz., 100% dėl gaisro;
- **Tikėtinas vienkartinis nuostolis (TVN)** – piniginė vertė, priskiriama vienam saugos įvykiui. Ji išreiškia nuostolį, kurį organizacija gali patirti dėl vienos grėsmės. Pvz., jeigu turto vertė yra 10 000 Lt, o PV yra 10%, tai TVN = 100 Lt;
- **Metinis dažnumo rodiklis (MDR)** – tai skaičius, kuris reškia grėsmės iškilimo dažnumą per metus. Objektyviai šį rodiklį apskaičiuoti yra labai sunku, paprastai jis nustatomas remiantis įvykio tikimybę. Ši reikšmė gali būti labai maža, pvz., kad Lietuvoje įvyktų žemės drebėjimas MDR yra 0,001. Tuo tarpu, kad 100 darbuotojų suves į sistemą neteisingus duomenys gali pasitaikyti dešimt kartų per metus kiekvienam darbuotojui. Tuomet MDR bus lygus 1000.

Kuomet yra nustatytos aukščiau išvardintas reikšmes, tai tuomet galima apskaičiuoti tikėtina metinį nuostolį tokiomis formulėmis:

$$TMN = MDR * TVN$$
$$TVN = V * PV$$

Pateiksime paprasta TMN apskaičiavimo pavyzdį (žr. 4.2 lentelę).

4.2 lentelė. TMN apskaičiavimo pavyzdys.

Gaisras tarnybinių stočių patalpose
V = 100 000 Lt *PV (dėl gaisro) = 100% (visiškas serverių sunaikinimas)* *TVN = 100 000 * 100% = 100 000 Lt* *MDR (gaisro) = 1%* *TMN = 100 000 * 1% = 1 000 Lt*
Į rizikos mažinimo priemones ar draudimą reikėtų investuoti ne daugiau kaip 1000 LT

4.1.4. Saugos priemonių parinkimas

Kai nustatytos visos grėsmės ir apskaičiuotos kiekvienos grėsmės TMN, kitas žingsnis yra saugos priemonių apžvalga ir įvertinimas. Rekomenduojamos saugos priemonės turi būti pateiktos rizikos analizės ataskaitoje. Yra keletas saugos priemonių pasirinkimo principų, kurie garantuoja tinkamą grėsmės prevenciją ir kontrolę. Norint pasirinkti veiksmingiausia kontrpriemonę, reikėtų įvertinti tokius kriterijus:

- **Kontrpriemonės kaštai**. Saugumo priemonės įsigijimo bei eksploatacijos kaštai neturėtų būti didesni už grėsmės tikėtina metinį nuostolį. Jeigu kaštai didesni už TMN, tai gal geresnis sprendimas būtų draudimas nuo grėsmės arba susitaikymas su galimais nuostoliais. Gali būti, kad viena kontrpriemonė sumažins kelių grėsmių riziką, tuomet reikėtų įvertinti tų grėsmių TMN sumą ir saugos priemonės kaštus.
- **Darbo sąnaudos.** Kiekviena sistema reikalauja priežiūros, todėl reikėtų įvertinti kokios reikalingos darbo sąnaudos saugos priemones eksploatavimui. Taip pat dėl žmogiškųjų klaidų atsiranda papildomų pažeidžiamumų, todėl geriausia, kad kontrpriemonė kuo labiau būtų automatizuota, nes tuomet procesas yra nuoseklesnis ir patikimesnis. Be to, saugos priemonė turi būti lengvai valdoma.
- **Sąveika su įprastiniais procesais.** Saugumo priemonė neturi trukdyti įprastiniems procesams, nes jeigu įdiegta saugumo priemonė sukels nepatogumų ir reikalaus didesnio laiko atlikti įprastinius darbu organizacijoje, tai ji gali sulaukti nepritarimo iš aptarnaujančio personalo, o tai gali įtakoti vadovybės nepakankamo palaikymo kontrpriemonės atžvilgiu.
- **Atskaitomybė ir auditavimas**. Saugumo priemonė turi leisti atlikti auditavimo ir atskaitomybės funkcijas. Auditoriai turi būti suteikta galimybė tikrinti saugos priemonę.

Taip pat turi būti leidžiama stebėti kiekvieną asmenį, kuris prisijungia prie kontrpriemonių ar jų nustatymų.

- **Santykiai su tiekėjais**. Turi būti patikrintas saugos priemonės tiekėjo patikimumas bei jo darbas praeityje. Turi būti žinomas programinės įrangos atviras kodas, kad būtų galima atlikti reikalingas modifikacijas ir kad nebūtų paslėptas kenkėjiškas kodas. Be to, reikėtų atkreipti dėmesį į sistemos palaikymo sąlygas.

Iš išvardintų kriterijų bene vienas svarbiausių būtų kontrpriemonės kaštų įvertinimas. Vienas iš šio kriterijaus apskaičiavimo būdų yra kaštų-naudos analizė. Norint nustatyti bendruosius saugos kaštus, reikia įvertinti:

- Saugos priemonės įsigijimo, sukūrimo ir/arba licencijos kaštus;
- Fizinio įdiegimo kaštus įskaitant ir procesų sutrikimo kaštus kontrpriemonės diegimo ir testavimo metu;
- Eksploatacines išlaidas

Apskaičiuoti saugos priemonės naudą galima pagal formulė:

(TMN prieš saugos priemonės įdiegimą) – (TMN po saugos priemonės įdiegimo) – (metiniai saugos priemonės eksploatavimo kaštai) = saugos priemonės naudingumas

4.1.5. Analizės rezultatai

Atlikus visus skaičiavimus ir vertinimus, vienas paskutinių kiekybinės rizikos analizės etapų yra atliktų vertinimų ataskaitos paruošimas vadovybei. Analizės rezultatuose tūrėtų būti pateikta:

- Vertybių finansinis įvertinimas;
- Detalus svarbiausių vertybių sąrašas;
- Grėsmių tikimybės ir tikėtinas dažnumas;
- Apskaičiuotas kiekvienos grėsmės galimas finansinis nuostolis vertybei.

4.1.6. Sprendimai

Galutinai baigus kiekybinės rizikos analizę, vadovybė, pagal pateiktas išvadas, turi priimti labiausiai priimtina apsisaugojimo nuo grėsmės sprendimą. Pasirinkimo sprendimas labiausiai priklauso nuo to, kas labiausiai sumažina riziką bei užtikrina mažiausius eksploatavimo kaštus. Tai gi, po kiekybinės rizikos analizes gali būti priimti tokie sprendimai:

- **Rizikos mažinimas**. Priemonės, mažinančios rizikos lygį ir jos poveikį. Jeigu kontrpriemonės įsigijimo ir eksploatavimo kaštai yra mažesni už tikėtinus nuostolius, bei

jeigu yra pakankamai kompetentingų žmogiškųjų resursų, kurie užtikrintų sklandų saugumo priemonės darbą, tai šis sprendimas yra tinkamiausias;

- **Rizikos perkėlimas**. Potencialių kaštų perkėlimas trečiajai šaliai (pvz. draudimo bendrovei). Kartais draudimas gali pareikalauti mažesnių kaštų negu riziką mažinančių priemokų diegimas ir eksploatacija. Taip pat šis sprendimas priimamas tuomet, kai kontrpriemonės sumažina rizikos lygį nežymiai ir jis nėra priimtinas organizacijai. Be to, kartais yra neįmanoma įdiegti jokių mažinančių riziką saugumo priemonių;
- **Rizikos priėmimas.** Šis sprendimas yra palankiausias, kai rizikos lygis yra priimtinas, arba kiti sprendimai perdaug sudėtingi (neįmanomi) ir jų kaštai didesni už tikėtinus nuostolius.

4.1.7. Kiekybinės analizės privalumai ir trūkumai

Kiekybinė rizikos analizė yra pakankamai ilgas ir sudėtingas procesas. Organizacija, prieš apsispręsdama naudoti šį metodą, turėtų įvertinti visus jos privalumus ir trukumus [3].

Kiekybinės analizės privalumai:

- Objektyvus rezultatai;
- Nuostoliai išreikšti piniginę verte, todėl labiau suprantami;
- Patikima kaštų-naudos analizė, todėl sukuriamas pagrindas saugos finansavimui;
- Rizikos kaštų efektyvumas gali būti nustatytas ir įvertintas;
- Rizika geriau suprantama vadovybei;
- Prioritetai pagal piniginę išraiška;
- Daug pastangų skiriama turto vertei nustatyti ir rizikai mažinti;
- Sukuriamos tikslesnės DB vėlesniems analizės.

Kiekybinės analizės trūkumai:

- Sudėtingi apskaičiavimai;
- Be automatizavimo priemonių sunku atlikti;
- Būtina surinkti daug duomenų apie informacines vertybes;
- Naudojamos rizikos DB yra neobjektyvios ir priklauso nuo gamintojo;
- Analize atlieka ekspertai, todėl dalyvius sunku sudominti proceso metu;
- Sunku keisti analizės kryptį;
- Bendriems sutarimams ir rezultatams reikia daug laiko;
- Rezultatai tik piniginę išraiška.

4.2. Kokybinė rizikos analizė

Kokybinės analizė yra ne tokia sudėtinga kaip kiekybinė. Jos procesas nereikalauja didelių piniginių išlaidų, jis įvykdomas greičiau bei galima apsieiti be ekspertų pagalbos. Kokybinės analizės metu nėra suteikiama vertybėms ir nuostoliams piniginės išraiškos. Taikant šį metodą, yra suteikiamos nematerialios verčių išraiškos, tokios kaip duomenų praradimas, paviešinimas, pakeitimas ar neprieinamumas. Yra orientuojamasi į kitus veiksnius, užuot naudojant pinigines išraiškas.

4.2.1. Dešimties žingsnių metodas

Dešimties žingsnių metodas apima kokybinės rizikos analizės procesą nuo planavimo stadijos iki galutinės ataskaitos. Kiekvieno ankstesnio žingsnio rezultatai yra naudojami kaip duomenys kitam etapui. Trumpai aptarsime kiekvieną iš šio metodo etapų[3]:

1. **Rizikos analizės apimties nustatymas.** Šiame etape turi būti apibrėžta kas turi būti atlikta. Reikia įvardinti kokie yra analizės tikslai, kokia turėtų būti darbų apimtis bei kokių rezultatų tikimasi. Turi būti apibrėžti pagrindiniai analizės uždaviniai – galimų nuostolių dėl informacijos vientisumo, konfidencialumo ar prieinamumo keliamų grėsmių įvertinimas. Taip pat turi būti apibrėžtos analizės ribos, nes kitaip analizės procesas gali išsivystyti iki milžiniškų apimčių ir niekada nebus baigtas. Darbų apimtį paprastai nustato sistemos valdytojas (asmuo, atsakingas už sistemos saugą).
2. **Kompetentingos grupės suformavimas.** Kad analizės procesas vyktų sklandžiai ir veiksmingai, į rizikos analizės grupę turi būti įtraukti visų organizacijos padalinių atstovai, kuriems analizuojama sistema daro įtaką jų darbo procesams. Be to, surinktos grupės nariai turį būti savo srities žinovai kad galėtų aiškiai ir argumentuotai reikšti mintis iš savo profesinės prizmės. Tai yra labai svarbu, nes vienos profesijos specialistas sunkiai gali įvertinti grėsmes iš visiškai jam nežinomos srities. Grupė turėtų būti sudaryta iš funkcinių vertybių valdytojų, sistemos vartotojų, sistemos analizės padalinio atstovų, duomenų bazių administratorių, fizinės saugos atstovų, ryšių padalinio žmonių, saugos padalinio žmonių, sistemos programuotojų, duomenų valdymo ir apdorojimo atstovų bei jeigu reikia teisininkų ir auditorių.
3. **Rizikos nustatymas.** Šiame žingsnyje suburtos analizės grupės nariai turi sudaryti sąrašą rizikos rūšių, kylančių analizuojamam objektui. Ši procesą galima įgyvendinti keliais metodais. Vienas iš metodų – atrinkimas aktualių rizikos rūšių iš pateikto sąrašo. Bet toks

metodas turi trūkumų, nes dažniausiai rizikos yra imamos iš sąrašo ir nėra ieškoma naujų idėjų. Kitas metodas būtų „idėjų vėtra“ (brainstorming) – visi grupės nariai sugalvoja savo idėjas, o vėliau jos atrenkamos ir suklasifikuojamos.

4. **Rizikos klasifikacija.** Kai yra nustatytos rizikos, reikia kiekvienai rizikos tikimybei priskirti skaitines reikšmes. Pvz., maža-1 , tarp mažos ir vidutinės- 2, vidutinė-3 , tarp vidutinės ir didelės -4, didelė - 5. Po to, kiekvienai rizikai yra priskiriama skaitinė tikimybės reikšmė pagal suderintus visų narių įvertinimus.
5. **Rizikos įvertinimas.** Šiame žingsnyje yra įvertinama žalą vertybei, kurią gali sukelti kiekviena rizika. Kiekvienai rizikos galimai žalai yra priskiriama skaitinė reikšmė (panašiai kaip 4 žingsnyje).
6. **Bendros rizikos sąlygojamos žalos apskaičiavimas.** Kai jau žinome rizikos tikimybės ir galimos žalos įvertinimus, paskaičiuojame rizikos veiksnį, kuris yra 4 ir 5 žingsnyje gautų skaičių suma. Kadangi 4 ir 5 žingsnyje didžiausia reikšmė yra 5, tai veiksnys gali būti tarp 2 ir 10.

Atlikus 3, 4 ,5 ir 6 žingsnus, yra sudaroma lentelė, kurioje atsispindi visi įvertinimai (pavyzdys pateiktas 4.3 lentelėje).

4.3 lentelė. Rizikos veiksniai

Analizuojamos vertybės pavadinimas			
Rizika (3 žingsnis)	**Rizikos tikimybė** (4 žingsnis)	**Rizikos žala** (5 žingsnis)	**Veiksnys** (6 žingsnis)
Gaisras	3	5	8
Užliejimas vandeniu	4	3	7
Vagystė	2	3	5
Uraganas	2	5	7

Kai rizikos veiksnių lentelė paruošta, tai tuomet yra atrenkamos rizikos rūšys, kurių veiksnys didesnis už 6 ir mažėjimo tvarka perrašomos į saugos priemonių identifikavimo lentelę (žr. 4.4 lentelę). Toliau analizuojamos grėsmės veiksnio dydis priklauso nuo organizacijoje priimtino rizikos lygio.

7. **Saugos priemonių nustatymas**. Šiame etape yra analizuojami nustatyti pažeidžiamumai ir ieškoma techniniu, administracinių ar fizinių priemonių, kurios užtikrintų priimtiną vertybės saugumo lygį. Saugumo priemonės gali būti:
   - ***Rizikos išvengimo*** –iš anksto suplanuotos kontrpriemonės (pvz., šifravimas ir tapatybės nustatymas, politika ir standartai, saugus ryšių planavimas, viešojo rakto infrastruktūra)

- ***Papildomos kontrpriemonės*** – didina esamų priemonių saugumą(pvz., auditas, saugos spragų skanavimas)
- ***Susekimo*** – saugumo spragų susekimas, blokavimas ir reagavimas į jas (pvz., įsiskverbimo aptikimas).
- ***Atkūrimo*** – atkuria saugumą ir informaciją po pažeidimo (pvz., veiklos tęstinumo planavimas, krizių valdymo planas).

Šio etapo rezultatas yra sąrašas labiausiai tinkamų kontrpriemonių.

8. **Kaštų- naudos analizė**. Šis žingsnis turi būti kruopščiai atliekamas, nes jis labiausiai įtakoja saugumo priemonės pasirinkimą (plačiau šis metodas aprašytas 4.1.4 skyriuje). Šiame etape turi būti nustatytos veiksmingiausios ir pigiausios saugos priemonės.

Kai yra atliktas 7 ir 8 punktas, tuomet yra atmetamos visos netinkamos saugumo priemonės ir sudaroma priemonių identifikavimo lentelę (žr. 4.4 lentelę).

4.4 lentelė. Saugos priemonių nustatymas

Analizuojamos vertybės pavadinimas			
Rizika	**Rizikos veiksnys**	**Galimos saugos priemonės** (7 žingsnis)	**Veiksnys** (8 žingsnis)
Gaisras	8	Priešgaisrinė sistema	15 000 Lt
Uraganas	7	Veiklos tęstinumo planavimas	75 000 Lt
Užliejimas vandeniu	7	Veiklos tęstinumo planavimas	75 000 Lt

9. **Saugos priemonių klasifikacija.** Saugumo priemonės yra suklasifikuojamos pagal diegimo pirmumą, atsižvelgiant į tokius kriterijus kaip: kiek rizikos rūšių apsaugos kontrpriemonė; diegimo kaštai; poveikis organizacijai; žmogiškieji ištekliai priemonės diegimui ar eksploatacijai.
10. **Rizikos analizės ataskaita.** Baigus rizikos analizę, vadovybei turi būti pateikti jos rezultatai ataskaitos forma. Atskaitoje turi būti pateikta: įvadas, analizės pagrindimas, apimties apibrėžimas, metodų išaiškinimas, bendra analizės proceso apžvalga, rizikos ir jos veiksnių nustatymas, saugos priemonių nustatymas, kaštų-naudos analizė, rekomendacijos, įvairūs priedai.

Kadangi kokybinės analizės rezultatai yra subjektyvus, tai šio metodo rezultatų kokybė labai priklauso nuo surinktos analizės grupės kompetencijos. Jeigu grupė tikrai profesionali, tai šis metodas gali prilygti kiekybinės rizikos analizei, kuri reikalauja daug darbo ir laiko.

4.2.2. Trijų žingsnių metodas

Trijų žingsniu metodas yra panašus į dešimties žingsnių, pagrindinis skirtumas tas, kad šis metodas yra skirtas vertinti mažiau apčiuopiamas rizikos rūšis, tokias kaip reputacija, klientų pasitikėjimas ar pozityvus žiniasklaidos požiūris. Kaip ir kituose analizės metoduose, pirmiausia yra nustatomas vertybių valdytojas ir sudaroma analizės grupė. Trijų žingsnių metodo etapai yra[3]:

1. **Vertybių įvertinimas**. Šio etapo užduotis yra įvertinti žalą, kurią organizacija patirtų, jeigu būtų pažeista vertybė. Analizės grupė turi vertinti vertybės iš paruoštų lentelių, kurios yra parengiamos aptariant su visų padalinių darbuotojais. Lentelėse turi būti pateikti skaitiniai žalos įvertinimai susiję su informacijos paviešinimu, pakeitimu, praradimu, neprieinamumu ar teisinėmis pasekmėmis. Pvz., veiklos sutrikdymas, kuris gali būti paskelbtas žiniasklaidoje – 7 balai, dėl konkurencijos patirtas nuostolis 100 000 Lt – 4 balai, teisinės pasekmės 50 000 Lt – 4 balai. Kai yra paruostos vertinimo lentelės, grupės narai įvertina kokia finalinė, teisinė, konkurencingumo ir veiklos sutrikdymo žala yra vertybės paskelbimui, pakeitimui, neprieinamumui ir praradimui.
2. **Rizikos įvertinimas**. Sudaromas galimų grėsmių ir pavojų sąrašas ir įvertinama jų rizika pagal rizikos vertinimo matrica. (žr. 4.5 lentelę).

4.5 lentelė Rizikos vertinio matrica[3]

		Žala		
		Didelė	**Vidutinė**	**Maža**
Tikimybė	**Didelė**	3	6	9
	Vidutinė	2	5	8
	Maža	1	4	7

3. **Rizikos valdymas.** Analizės grupės narai, naudodamiesi 1 etapo rezultatais, nustato vertybių reikšmę, o 2 etapo rezultatų pagalba įvertinta nepriimtina rizika. Taip pat, reikia apžvelgti kokios saugumo priemonės yra įdiegtos. Visiems pavojams, kuriems nėra įdiegta prevencinės priemonės, turi būti parengtos rekomendacijos, kokias priemones taikyti. Turi būti atsižvelgta į tai ar kontrpriemonė sumažins rizika iki priimtino lygio, ar jų kaštai priimtini. Priemonės gali veikti riziką tokiais būdais:
    - Mažinti rizikos tikimybę;
    - Mažinti rizikos poveikį;

- Nustatyti iškilusią riziką;
- Švelninti rizikos padarinius.

Baigus 3 žingsnių rizikos analizę, yra paruošiama ataskaita, kurioje pateikiamos rekomendacijos vadovybei. Yra nurodomos efektyviausios saugos priemonės ir kokias rizikos grupes jos mažina, įvardijami atsakingi asmenys už priemonių diegimą bei pateikiamas diegimo grafikas.

4.2.3. 30 minučių metodas

Šis metodas yra skirtas organizacijoms, kurios turi mažai patirties informacijos saugumo rizikos analizės srityje. 30MM skirtas nustatyti saugos reikalavimus kuriant veiksmų planus, analizuojant kaštus ir paskirstant atsakomybę. Analizę vykdo kuratorius, kuris įtraukia į 30MM procesą sistemos vartotojus, kurie padeda sudaryti rizikos bei kontrpriemonių sąrašą ir jų vertinimą. Patartina, kad kuratorius nebūtų nagrinėjamos srities specialistas, nes pagrindinė jo funkcija yra nuomonių klausymasis.

Uždaviniai

Nustatyti tyčines ir netyčines rizikos rūšis, kurios susijusios su vertybes vientisumu, konfidencialumu bei prieinamumu ir pasirinkti mažinančias rizikos lygį saugumo priemones.

Procesas

30MM susideda iš tokių etapų [3]:

1. Pirmas žingsnis yra su tiriama vertybę susijusių darbuotojų subūrimas apklausai.
2. Darbuotojų apklausa vykdoma .„idėjos vėtros“ principu. Yra sudaroma matrica , kuri nustato darbuotojų nuomonę dėl tyčinių ir netyčinių rizikos rūšių veiksnių, sąlygojančių vertybės vientisumą, konfidencialumą bei prieinamumą (pvz. žr. 4.6 lentelėje).

4.6. lentelė. Tyčinės ir netyčinės grėsmės

	Vientisumas	**Konfidencialumas**	**Prieinamumas**
Nesąmoningi veiksniai	• Neteisingų duomenų įvedimas. •	• Baigus darbą, neišeinama iš sistemos •	• Atsitiktinis duomenų sunaikinimas • .....
Sąmoningi veiksniai	• Neteisingų duomenų įvedimas •	• Neteisėtas prisijungimas •	• Sabotažas • .....

3. Apklausiant darbuotojus sudaroma tokia pat matrica kaip ir antrame punkte, tik vietoj rizikos rūšių yra surašomi siūlomi sprendimai.
4. Išrenkami naudingiausi saugos sprendimai organizacijai. Dažnai vienas sprendimas sumažina keletą rizikos rūšių ir atvirkščiai. Sprendimas turi būti pagristas kaštų-naudos analize, tačiau nereikia vertinti rizikos piniginę išraiška, užtenka įvertinti kaštus.
5. Parengiami dokumentai, atspindintis rizikos analizės rezultatus. Turi būti aprašyta analizės procedūra, sistemos saugotinos dalys, kokios priemonės turėtų būti taikomos bei nekontroliuojami procesai (kai reikia priimti riziką ar neįmanoma pritaikyti kontrpriemonių).

Šis metodas padeda organizacijai įvertinti matomus ir slaptus pavojus, kylančius jos vertybėms, bei priimti saugos sprendimus jeigu nėra pakankamai žmogiškųjų resursų ar patirties rizikos analizei.

4.2.4. Kuruojamos rizikos analizės procesas

KURAP buvo sukurtas tam, kad rizikos analizę galėtų atlikti patys organizacijos vadovai pasitelkdami savo turimus specialistų išteklius. Kai dar nebuvo šio metodo, organizacija laikydavo rizikos analizę labai sudėtingu procesu ir, neįvertindama savu specialistų, samdydavo konsultantus iš šalies, kurie dažnai parikdavo nepriimtinus sprendimus organizacijos veiklos procesams. KURAP trunka kelias dienas, o ne kelias savaites, kaip daugelis analizes metodų. KURAP vadovauja kuratorius, kuris turi turėti vadovavimo, klausymosi, valdymo įgūdžių. Šį rizikos analizės procesą vykdo surinkta grupė iš susijusių su sistema žmonių. Kaip ir kituose kokybinės rizikos nustatymo metoduose, vienas pagrindinių grupės savybių turi būti kompetentingumas. KURAP rezultatas yra dokumentas, nustatantis grėsmes, grėsmių priimtinumą bei siūlomus sprendimus joms švelninti. KURAP yra labai panašus į „30 minučių“ metodą, tik skirtumas tas, kad KURAP parenkami bendri saugos sprendimai (pvz., atsarginė kopija, mokymai, fizinė apsauga, prieigos kontrolė ir t.t.) iš pateikto sąrašo.

KURAP yra suskirstytas į 3 pagrindinius etapus [3]:

1. **Parengiamasis posėdis**. Šis posėdis trunka apie valandą, per kuri turi būti parengta:
   - *Apimties apibrėžimas*. Suformuluojama, kas tiksliai turi būti nagrinėjama.
   - *Vizualinė schema.* Atvaizduojama analizuojamo proceso schema, kurioje turi būti matoma proceso pradžia ir pabaiga.

- *Grupės narių sąrašas*. Nuo 7 iki 15 žmonių. Į grupę turi būti įtraukta kuo daugiau su sistema susijusių skirtingų sričių žmonių. Pagrindinis grupės sudarymo kriterijus yra kompetencijos lygis.
- *Susirinkimo tvarka*. Sutvarkomi organizaciniai klausimai dėl posėdžių. Turi būti pasirūpinta patalpomis ir reikiamomis priemonėmis bei suderintas tvarkaraštis.
- *Sąvokos*. Susitariama dėl sąvokų. Turi būti apibrėžtos tokios sąvokos kaip vientisumas, konfidencialumas, prieinamumas, rizika, saugos priemonė, poveikis, pažeidžiamumas.

2. **KURAP sesija**. Trunka apie 4 valandas. Posėdžio metu yra paskirti dalyvių vaidmenys: valdytojas, projekto vadovas, kuratorius, sekretorius, grupės narys. Dalyviai yra supažindinami su parengiamojo posėdžio parengta medžiaga. Šio etapo metu turi būti parengti dokumentai:
   - *Rizikos nustatymas*. Idėjų vėtros proceso pagalba yra nustatomas grėsmių, susijusių su vientisumo, konfidencialumo bei prieinamumo pažeidimais, sąrašas. Besidubliuojantys elementai yra pašalinami.
   - *Suskirstytos rizikos pagal svarbą.* Kai jau visos grėsmes yra nustatytos, jas reikia suskirstyti pagal svarbą, nustatant grėsmės keliama žalą, tikimybę bei įtaką. Skirtingi vertinimai tarp narių yra aptariami ir rezultate priimamas vieningas įvertinimas. Galima naudotis tokiais kriterijais: A –korekciniai veiksmai reikalingi, B – korekciniai veiksmai pageidaujami, C – būtina stebėti, D – nereikia imtis jokių veiksmų. Taip pat galima pateikti prioritetų matrica (žr. 4.7. lentelę).

4.7 lentelė. Prioritetų matrica[3]

		Poveikis veiklai		
		Didelis	**Vidutinis**	**Mažas**
Pažeidžiamumas	**Didelis**	A	B	C
	Vidutinis	B	B	C
	Mažas	C	C	D

- *Siūlomos saugos priemonės*. Grupės narai iš saugos priemonių lentelės, kuri buvo kruopščiai parengta per keletą metų, parenka labiausiai tinkamas kontrpriemones kiekvienai grėsmei. Pvz., priemonės gali būti: 1-atsarginė kopija, 2- fizinė apsauga, 3 – techninė priežiūra ir t.t. Baigus KURAP sesija turi būti parengta rezultatų lentelė (pvz. 4.8 lentelėje).

4.8 lentelė. KURAP sesijos rezultatai

Nr	Grėsmė	Tipas (vient., konf., priein.)	Prioritetas	Saugos priemonė
1	Personalas neteisėtai gauna prieiga prie informacijos	Vient.	B	3,5,6,11
2	Nepranešama apie vientisumo pažeidimus	Vient.	A	7,11,12
...	...	...	...	...

3. **Baigiamasis etapas**. Trunka apie 10 dienų ir šiame etape yra parengiama galutinė ataskaita iš 1 ir 2 žingsnio rezultatų. Šis etapas yra sudarytas iš trijų elementų:
   - *Kryžminių nuorodų lentelės sudarymas*. Šiame etape iš gautų pagrindinės sesijos rezultatų (žr. 4.8.lentelę) yra sudaroma lentelė, kurioje yra sugrupuojami duomenys pagal saugumo priemonę. Lentelėje turi matytis kokia saugumo priemonė apsaugo nuo kokių grėsmių.
   - *Egzistuojančių saugos priemonių nustatymas.* Nustatoma kokios jau saugos priemonės yra įdiegtos. Dažnai būna, kad net 80% išnagrinėtų grėsmių jau yra taikomos saugumo priemonės. Jeigu saugos priemonės nėra, tai yra paskiriama diegimo data bei vykdytojas.
   - *Saugos priemonių parinkimas nustatytoms rizikos grupėms arba rizikos prisiėmimas.* Vadovai priima sprendimą dėl saugos priemonės taikymo. Yra atsižvelgiama į kontrpriemonės kaštus ir jos veiksmingumą. Jeigu rizika priimtina, tai tuomet jei nėra taikomos saugos priemonės.

Kuruojamos analizės procesas yra šiandien plačiai taikomas kokybinės analizės metodas. Pagrindiniai jos privalumai yra tai, kad nereikalauja daug laiko ir analizę galima atlikti pasitelkus organizacijoje esamus specialistus.

4.2.5. BS 7799 rizikos vertinimo procesas

BS 7799 standarte yra pateiktas rizikos vertinimo procesas taikant kokybinės analizės metodą. Šis metodas išsiskiria tuo, kad yra vertinama ne konkreti vertinė, o jų visuma ISMS rėmuose. Šis rizikos vertinimo procesas susideda iš tokių etapų:

1. **Vertybių nustatymas.** Turi būti nustatytos visos vertybės ISMS rėmuose. Šio etapo rezultatas yra vertybių sąrašas su nurodyta vieta ir turėtoju. Vertybes galima suskirstyti į tokias grupes kaip:
   - *informacinis turtas* (duomenų bazės, duomenų bylos, sistemų dokumentacija, ...);
   - *Popierinė dokumentacija* (sutartys, rekomendacijos, rezultatų dokumentai, ...);

- *Programinė įranga* (taikomosios programos, sisteminės programos, ...);
- *Fizinis turtas* (kompiuteriai, ryšio įranga, baldai, patalpos, ...);
- *Žmonės* (personalas, klientai, abonentai, ...);
- *Paslaugos* (ryšių paslaugos, apšvietimas, šildymas, kondicionavimas, ...).

2. **Vertybių Įvertinimas.** Šiame etape turi būti įvertintas turtas atsižvelgiant į tai, kokius finansinius nuostolius ar įvaizdžio pakenkimą gali patirti organizacija dėl informacijos atskleidimo, modifikacijos, neprieinamumo ar sunaikinimo. Kiekviena vertybė turi būti įvertinta konfidencialumo prieinamumo ir vientisumo atžvilgiu priskiriant jiems vertes pagal finansinę ar kokia kitą žalą organizacijai (pvz., .maža – 1, vidutinė – 3 ir t.t.). Priklausomai nuo organizacijos didžio, įvertinimo skalė yra skirtinga. Pavyzdžiui didėlės organizacijos maža – 1 įtaka gali būti nuo 50 000 Lt iki 100 000 Lt. Šio etapo rezultatas yra sąrašas vertybių su vientisumo, konfidencialumo bei prieinamumo sąlygojančios žalos įvertinimais.
3. **Saugos reikalavimų nustatymas.** Šiame etape yra nustatoma vertybės grėsmės, pažeidamumai bei teisiniai, sutartiniai ar veiklos saugos reikalavimai (pvz., dėl duomenų apsaugos įstatymo) taikytini vertybei.
4. **Saugos reikalavimų įvertinimas.** Šiame žingsnyje yra įvertinamos grėsmės, pažeidžiamumai ir teisiniai, sutartiniai ar veiklos reikalavimai. Vertinama yra kaip ir pirmajame punkte: maža -1, vidutinė -3 ir t.t.
5. **Saugos rizikos apskaičiavimas .** Saugos rizika yra apskaičiuojama remiantis turto verte ir įvertintais tarpusavyje saugumo lygių reikalavimais. Šio etapo rezultatas yra vertybės įvertinta informacijos atskleidimo rizika, modifikacijos rizika, neprieinamumo rizika, sunaikinimo rizika.
6. **Rizikos valdymo priemonių pasirinkimas.** Nustatoma, koks rizikos valdymo būdas bus pasirinktas kiekvienai rizikai. Šiame etape turi būti aiškiai apibrėžtas priimtinas rizikos lygis. Rizikos valdymo būdai gali būti:
   - *Mažinimas* - įdiegiamos kontrolės priemonės;
   - *Priėmimas* - rizika lygis yra priimtinas ir atitinka keliamus reikalavimus;
   - *Vengimas* – turtas iškeliamas iš rizikos zonos (fizinių ar veiklos procesų). Pvz., nenaudoti Interneto tam tikroms operacijoms;
   - *Perkelti kitoms šalims* – geriausias sprendimas kai kitos priemonės pernelyg sudėtingos arba jų įdiegimo kaštai per dideli. Pvz., draudimas.
7. **Saugos kontrolės priemonių pasirinkimas.** Pasirinkti konkrečia priemonę kad ji sumažintų rizika iki priimtino lygio.

4.2.6. Kokybinės analizės privalumai ir trūkumai

Kokybinė rizikos analizė yra greičiau ir lengviau atliekama nei kiekybinė. Tačiau nereikėtų pulti daryti kokybinės analizės ir visiškai ignoruoti kiekybinę analizę dėl jos sudėtingumo. Pirmiausia reikia įvertinti visus kokybinės analizės privalumus ir trukumus.

Kokybinės analizės privalumai:

- Skaičiavimai paprasti, lengvi ir suprantami;
- Nereikia nustatyti piniginės informacijos vertės;
- Nustatomos svarbiausios rizikos grupės;
- Proceso lakstumas;
- Vizualiai pateikiama rizikos klasifikacija;
- Lengviau pasiekti bendrą susitarimą;
- Į procesą lengviau įtraukti žmones, kurie nėra saugos ekspertai.

Kokybinės analizės trūkumai:

- Rezultatai subjektyvūs;
- Nėra įvertinama objektyvi piniginė turto vertė, todėl galimos paklaidos vertinant rizikos nuostolius;
- Nesukuriama kaštų-naudos DB;
- Objektyviai neįvertinamas priemonių efektyvumas;
- Rezultatai priklauso nuo grupės kompetencijos;
- Neaiškūs skirtumai tarp rizikos rūšių.

Kiekvienas rizikos analizės metodas turi savu privalumų ir trūkumų. Organizacijai, prieš pradedant vykdyti rizikos analizę, reikėtų rinktis tą metodą, kuris yra labiausiai tinkamas jos struktūroje ir kultūroje. Reikėtų atsižvelgti į tokius kriterijus kaip: analizės tikslas, analizės apimtys, prieinami organizacijos ištekliai, finansavimo dydis analizės procesui bei skiriamas laikas analizei.

5. NAUJAS RIZIKOS ANALIZĖS METODAS - RAISKP

Ištyrus populiariausius rizikos valdymo ir vertinimo metodikas bei įrankius (2 ir 3 skyriuje), rizikos analizės kiekybinius ir kokybinius metodus (4 skyriuje), pastebėta, kad trūksta RA metodo, kuris būtų tikslingai pritaikytas tirti informacinę sistemą jos kūrimo stadijoje. Plačiai paplitę rizikos valdymo ar analizės metodai yra skirti spęsti globalesnes organizacijai kylančiais grėsmes bei rizikas, kurių siūlomi spendimai neapribojami vienos sistemos rėmais. Jie labiau pritaikyti tirti sistemas, kurios yra eksploatacijos stadijoje. Susidūrus su tokia problema, nuspręsta sukurti naują rizikos analizės metodą, kuris tikslingai būtų pritaikytas tirti IS jos kūrimo procese.

Naujasis RA metodas pavadintas RAISKP (*rizikos analizė informacinės sistemos kūrimo procese*) . RAISKP etapai yra paremti geriausiomis ir tinkamiausiomis išnagrinėtų populiariųjų rizikos analizės metodų procedūromis ir savybėmis. Kai kurie žingsniai yra naujai suformuluoti, kad metodą labiau pritaikyti prie analizuojamos srities.

RAISKP metodas yra kokybinės analizės tipo. Kokybinė rizikos analizė pasirinkta todėl, kad ji greičiau, pigiau ir paprasčiau atliekama bei jos rezultatų tikslumas tenkina IS baziniam saugumui užtikrinti. Metodo pagrindiniai žingsniai, uždaviniai ir formalizavimo būdai yra sukurti pagrinde remiantis 10ŽM, 30MM ir KURAP kokybinės analizės metodais, atsižvelgiant į:

- Pagrindinius analizės etapus;
- Grėsmių nustatymo tvarką;
- Rizikos įvertinimo būdus;
- Saugumo priemonių parinkimo būdus;
- Saugumo priemonių pasirinkimo kriterijus;
- Ataskaitos paruošimo būdus.

Informacinės sistemos kūrimo procese dažnai yra pamirštama apžvelgti ir išanalizuoti saugumo rizikas, kurios gali kilti jos veikimo metu, arba galimos rizikos tik paviršutiniškai ištiriamos. IS kūrimo komanda būna labiau suinteresuota teisingu sistemos veikimu ir visų reikalingų funkcijų realizavimu nei jos saugumu. Toks elgesys yra natūralus, nes kam reikalinga IS, kuri yra saugi, bet neatlieka visų savo funkcijų. Nuodugni informacijos saugumo rizikos analizė dažniausiai yra atliekama tada, kai sistema yra jau įdiegta ir eksploatuojama. Toks veiksmų planas turi savų privalumų ir trūkumų. IS saugumo rizikos analizės atlikimas jos eksploatavimo metu leidžia tiksliau identifikuoti kylančias grėsmes ir esamus pažeidžiamumus, nes tyrimas yra atliekamas natūralioje jos veikimo aplinkoje, tačiau pažeidžiamumais gali būti jau pasinaudota, nes jie nebuvo ištaisyti laiku.

RAISKP metodo pagrindinis tikslas – išanalizuoti ir įvertinti rizikas bei parinkti saugumo priemones IS kūrimo stadijoje kad užkirsti kelia grėsmių realizavimui eksploatacijos metu. Šio metodo uždaviniai yra:

1. Padėti IS kūrimo komandai identifikuoti galimus sistemos pažeidžiamumus ir numatyti kontrpriemonių įdiegimą kaip vieną iš IS funkcionalumų;
2. Sumažinti galimas rizikas kol yra tik menama, o ne reali grėsmė;
3. Sumažinti IS korekcijos tikimybę, kuri yra susijusi su saugumo trūkumu;
4. Užtikrinti saugų sistemos veikimą jos eksploatacijos metu;
5. Integruotis į IS kūrimo procesą kaip vieną iš jo etapų;
6. Atlikti rizikos analizę greitai, paprastai ir be ekspertų pagalbos.

RAISKP metodas turi aiškiai apibrėžtas analizės ribas, į kurias nepatenka organizacijos IT ar kita infrastruktūra (nenagrinėjama fizinė sauga, tinklo sauga, organizacinės procedūros ir t.t.). Yra apsiribojama informacinės sistemos rėmuose esančios informacijos ir į ją patenkančių ir išeinančių duomenų saugumo rizikos analize. Toks apribojimas pasirinktas todėl, kad IS kūrimo grupei nepasidarytų rizikos analizė begalinis procesas. Organizacijos IT infrastruktūros saugumo rizikos analizė yra nemažos apimties darbas ir ją tikrai neturėtų atlikti IS kūrimo grupė, o ypač jeigu ji yra išorinė (ne organizacijos darbuotojai, o samdoma įmonė). RAISKP metodo privalumas - nuodugniau yra ištiriamos rizikos, kurios susietos būtent su nagrinėjama IS, o trūkumas - neįvertinamos rizikos, kurios gresia bendriems organizacijos procesams, kartu įskaitant ir tiriamą IS.

RAISKP metodo rizikos analizė turi būti atlikta tinkamiausiu laiku IS kūrimo procese. IS kūrimo procesas susideda iš dešimties pagrindinių etapų[24]:

1. Vartotojo reikalavimų analizė;
2. Vartotojo reikalavimų specifikavimas;
3. Reikalavimų programinei įrangai specifikavimas;
4. Sistemos architektūros projektavimas (dar vadinamas eskiziniu, arba loginiu, projektavimu);
5. Detalusis IS projektavimas (fizinis projektavimas);
6. IS realizavimas (kodavimas - taikomųjų programų kodo rašymas);
7. Programų testavimas: atskirų IS dalių testavimas;
8. Sistemos testavimas: visos IS testavimas;
9. IS eksploatavimas - diegimas organizacijoje;
10. IS funkcionalumo palaikymas.

RAISKP turi būti realizuota prieš 5 žingsnį (detalų IS projektavimą), kadangi esant šioje stadijoje yra įsivaizduojama IS struktūra ir tai padeda lengviau įvertinti kylančias rizikas. Be to,

kontrpriemones, kurios parenkamos po RAISKP analizės, galima aprašyti detalaus IS projektavimo etape kaip papildomas IS funkcionalumo savybes ir tuomet tolimesni kūrimo etapai liks nepakitę.

RAISKP metodas sudaro 7 rizikos analizės žingsniai:

1. Pasiruošiamieji darbai;
2. Rizikos analizės grupės sudarymas;
3. Grėsmių nustatymas;
4. Rizikos įvertinimas;
5. Saugos priemonių nustatymas;
6. Saugos priemonių parinkimas;
7. Dokumentavimas.

5.1. Pasiruošiamieji darbai

Pradinis RAISKP etapas turi lemiamos reikšmės analizės sėkmei, nes joje yra apibrėžiama pagrindinė informacija (tikslai, rezultatai, darbų apimtys) tolimesniems žingsniams įgyvendinti. Šiam etapui įgyvendinti reikalingi IS kūrimo komandos projektų vadovas, projektuotojas ir IS savininkas, kurio pagrindinė užduotis yra apibrėžti organizacijai priimtiną riziką. Šio etapo rezultatais turi būti:

1. Apibrėžtas RAISKP tikslas;
2. Nustatytos analizės ribos (kadangi šis metodas skirtas tirti riziką IS rėmuose, tai turi būti aiškiai nurodyti tie rėmai);
3. Apibrėžta priimtina rizika (tai tūrėtų atlikti IS savininkas);
4. Padarytas vizualinis IS modelis, kad lengviau būtų suprantama IS veikimo architektūra (pagrindinis šio darbo įnašas turėtų būti iš projektuotojo pusės);
5. Apibrėžtos pagrindinės sąvokos (rizika, saugos priemonė, poveikis, pažeidžiamumas,..).

5.2. Rizikos analizės grupės sudarymas

Kokybinės rizikos analizė yra atliekama remiantis subjektyvia nuomone, todėl labai svarbu parinkti kompetentingus asmenys jai atlikti. Grupė turėtų būti sudaryta iš vidinių IS kūrimo darbuotojų bei organizacijos (kurioje bus diegiama sistema) narių, kurie geriausiai žino vidinius procesus. Rekomenduojama, kad į rizikos analizės grupę būtų įtraukti šie asmenys:

1. Iš IS kūrimo grupės narių:
    - projektų vadovas;

- projektuotojas;
- programuotojas;
- verslo procesų analitikas;
- informacinės saugos specialistas (jeigu toks yra).

2. Iš organizacijos, kurioje diegiama sistema:
   - IS savininkas (žmogus atsakingas už IS vystymą, saugumą,..);
   - Informacinės saugos specialistas (jeigu tokio nėra organizacijoje, tai tuomet sistemų administratorius).

5.3. Grėsmių nustatymas

Kai jau yra suformuota saugumo rizikos analizės grupė, tai tuomet galima organizuoti susirinkimą ir atlikti grėsmių nustatymo etapą. Grėsmės turi būti nustatomos „idėjų vėtros“ principu, tačiau jei anksčiau buvo atliekamos panašios analizės, tai galima iškart aptarti ir seniau sudarytų grėsmių sąrašą. Panašiai kaip ir KURAP ar „10 žingsnių“ metode yra nustatomos sąmoningos ir nesąmoningos grėsmės informacijos vientisumui, konfidencialumui bei prieinamumui. Rizikos analizės grupė turi orientuotis į grėsmes, kurios patenka į apibrėžtas analizės ribas. Nenagrinėti grėsmių, kurios yra bendros organizacijos rėmuose (pvz. gaisras, fizinė vagystė). Visos sugalvotos grėsmės turi būti surašytos į lentelę (pavyzdys pateiktas 5.1 lentelėle).

5.1 lentelė. RAISKP grėsmių nustatymas

Nr	Grėsmė	Tipas	Kilmė
1	Neteisingų duomenų suvedimas	V	N
2	Neteisingų duomenų suvedimas	V	S
3	Neteisėtas prisijungimas	V, K	S

Grėsmė – grėsmės aprašymas
Tipas – grėsmė vientisumui(V), konfidencialumui(K) , prieinamumui (P)
Kilmė –grėsmės kilmė (S – sąmoninga, N - nesąmoninga)

5.4. Rizikos įvertinimas

Nustačius kylančias grėsmes ir surašius jas į lentelę, RAISKP grupė turi įvertinti rizikos tikimybę ir galimus nuostolius. Šis etapas yra vykdomas panašiai kaip 10ŽM metode. Grėsmės tikimybei ir galimiems nuostoliams yra priskiriama skaitinė vertė (1 – maža, 2 – maža-vidutinė,3 - vidutinė, 4 – vidutinė-didelė, 5 - didelė). Kai skaitinės reikšmės yra nustatytos, tuomet jos yra sudedamos. Grėsmės, kurių rizikos ir galimų nuostolių verčių suma mažiau už 6, yra pašalinamos iš grėsmių sąrašo kaip mažai įtakojančios organizacija. Tačiau, jeigu organizacija reikalauja didesnio

saugumo, tai tuomet svertinis vertinimas gali būti ne 6, o mažesnis. Priimtina rizika turi būti apibrėžta parengiamajame RAISKP etape IS savininko. Rizikos įvertinimo pavyzdys pateiktas 5.2 lentelėje.

5.2 lentelė. RAISKP rizikų įvertinimas

Nr	Grėsmė	Tipas	Kilmė	Tikimybė	Žala	Rizikos Veiksnys
1	Neteisingų duomenų suvedimas	V	N	5	2	7
2	Neteisingų duomenų suvedimas	V	S	4	4	8
3	Neteisėtas prisijungimas	V, K	S	2	5	6

5.5. Saugos priemonių nustatymas

Saugumo priemonių nustatymas yra sekantis etapas po rizikos įvertinimo. Saugumo priemonės yra parenkamos tik toms grėsmėms, kurių rizika yra nepriimtina organizacijai. RAISKP grupė turi siūlyti tokias kontrpriemones, kurios atitiktų kriterijus:

1. Saugos priemonė gali būti realizuota IS kūrimo procese (papildomas IS funkcionalumas, papildoma programinė įranga). Neturėtų būti analizuojamos tokios saugumo priemonės, kurios turi būti vykdomos visos organizacijos IT infrastruktūros mastu (pvz. fizinė apsauga).
2. Turi būti parinkta tinkamiausia saugumo priemonė rizikai sumažinti.
3. Atlikus preliminarią saugos priemonės „kaštų-naudos“ analizę , nesirinkti tokios kontrpriemonės, kurios nauda yra žymiai mažesnė nei kaštai (tai gali būti sudėtinga įvertinti, nes viena saugos priemonė gali padengti kelias grėsmes).

Saugumo priemonės, kaip ir grėsmės, yra parenkamos „idėjų vėtros“ principu, nors galima ir pasinaudoti iš anksto paruotu kontrpriemonių sąrašu. Turi būti analizuojamos įvairaus tipo kontrpriemonės (išvengimo, susekimo, atkūrimo, papildomos). Pritaikius grėsmei saugumo priemonę, reikia įvertinti likutinę riziką (koks rizikos lygis išliks kontrpriemonės įdiegimo atveju). Jeigu likutinė rizika yra priimtina, tai tuomet daugiau saugumo priemonių grėsmei nebeanalizuojama, o jeigu nepriimtina, tai bandoma ieškoti kitų kontrpriemonių. Gali būti toks atvejis, kad vienos saugumo priemonės neužtenka rizikai sumažinti iki priimtino lygio, tuomet bandoma kombinuoti kelias kontrpriemones ir įvertinti bendrą jų panaudojimo likutinę riziką. Saugumo priemonių parinkimo pavyzdys pateiktas 5.3 lentelėje.

5.3 lentelė. RAISKP saugumo priemonių nustatymas

Nr	Grėsmė	Tipas	Kilmė	Rizikos Veiksnys	Saugos priemonė	Likutinė rizika
1	Neteisingų duomenų suvedimas	V	N	7	Funkcijos, tikrinančios duomenų korektiškumą	2
2	Duomenų pakeitimas	V	S	8	Duomenų prieigos kontrolė	3
					Operacijų stebėjimas (ang. logging)	
3	Neteisėtas prisijungimas	V, K	S	6	Duomenų prieigos kontrolė	2

5.6. Saugos priemonių parinkimas

Saugumo priemonių parinkimo etape pagrindinis tikslas yra parinkti saugumo priemonės, kurios bus įdiegtos informacinėje sistemoje. Jeigu kai kurios kontrpriemonės bus nepriimtinos organizacijai, tai tuomet ji turės prisiimti rizikas, kurios nebus sumažintos iki priimtino lygio kontrpriemonės įdiegimo atveju. Taip pat turi būti pažymėtos kontrpriemonės, kurios jau yra įdiegtos organizacijoje.

Šiame etape yra pergrupuojamos grėsmės pagal saugumo priemonę (panašiai kaip KURAP ir „10 žingsnių“ metoduose). Yra įvertinami saugumo priemonės kaštai bei nustatoma ar ji bus diegiama ar ne (priimtinas kontrpriemones turėtų nustatyti IS savininkas). Kai kurios kontrpriemonės gali būti jau numatytos kaip IS funkcionalumo dalis, tai tuomet kaštai bus lygus 0. Jeigu kontrpriemonė bus įgyvendinta IS kūrimo grupės darbo jėgomis, tai kaštus galima įvertinti ne piniginę, o laiko išraiška. IS savininkas žino kiek kainuoja IS kūrimo grupės laikas ir gali lengvai tai konvertuoti į piniginę išraiška. Laiko ir pinigų sąryšis gali būti konfidenciali informacija ir jos atskleidimas gali būti nepageidaujamas kai kuriems rizikos analizės grupės nariams.

Galimas toks atvejis, kad neįmanoma pergrupuoti grėsmes pagal saugumo priemonę, nes riziką sumažina tik kelių saugumo priemonių panaudojimas. Tokiu atveju yra įrašoma į lentelę saugumo priemonių sąryšis (pvz. pateiktas 5.4 lentelėje). Jeigu iš jungtinės saugumo priemonės viena dalis nėra diegiama, tuomet yra perskaičiuojama likutinės rizikos vertė įvertinus vienos iš kontrpriemonės dalies nebuvimą.

5.4 lentelė. RAISKP saugumo priemonių parinkimas

Nr	Saugos priemonė	Kaštai	Diegti ?	Grėsmė	Tipas	Kilmė	Rizikos Veiksnys	Likutinė rizika
1	Funkcijos, tikrinančios duomenų korektiškumą	100 val.	Taip	Neteisingų duomenų suvedimas	V	N	7	2
2	Duomenų prieigos kontrolė	1000 Lt	Taip	Neteisėtas prisijungimas	V, K	S	6	2
3	2 saugumo priemonė	-	+	Duomenų pakeitimas	V	S	8	6
	Operacijų stebėjimas (ang. logging)	0	Ne					

5.7. Dokumentavimas

Dokumentavimas yra paskutinis žingsnis RAISKP analizėje. Šiame etape yra paruošiama ataskaita su RAISKP rezultatais bei prieš tai buvusių etapų rezultatų dokumentai kaip priedai. RAISKP dokumentacija yra pridedamas prie bendros IS dokumentacijos. Šį darbą turi atlikti IS kūrimo grupės projektų vadovas. Ataskaitoje turi būti nurodyta:

1. Analizuojamos sistemos pavadinimas;
2. RAISKP analizės data;
3. Grupės narių sąrašas;
4. Analizės tikslas;
5. Pasirinktų kontrpriemonių sąrašas (žr. 5.4 lentelę);
6. Nepasirinktų saugumo priemonių sąrašas ir kokias rizikas prisiima organizacija;
7. Kokių grėsmių rizika bus(nebus) sumažinta iki priimtino lygio;
8. Kokių grėsmių rizika yra priimtina be kontrpriemonės įdiegimo;
9. IS kūrimo grupės projektų vadovo ir IS savininko parašai.

Naujasis RAISKP rizikos analizės metodas sukurtas taip, kad ją greitai (per viena dieną) ir savo jėgomis galėtų atlikti informacinės sistemos kūrimo grupė produkto projektavimo stadijoje. Analizės rezultatai padės nustatyti IS galimas grėsmes bei parinkti geriausias kontrpriemones, kurios sumažins rizikas iki priimti lygio. Šio metodo pagalba informacinė sistema pasižymės didesniu saugumo lygiu savo eksploatacijos metu.

6. RAISKP METODO PANAUDOJIMO TYRIMAS

Norint įvertinti naujojo rizikos analizės metodo RAISKP panaudojimo efektyvumą, reikia atlikti tyrimą, kurio metu naujasis metodas bus praktiškai pritaikytas realioje aplinkoje, ir išanalizuoti gautus rezultatus. Tokiam tyrimui atlikti pasirinktas linijinio eksperimento metodas, nes RAISKP metodas nėra niekur taikomas ir tik tokiu būdų galima jį vertinti. Šiuo tyrimu bandysime įrodyti hipotezę: - *Informacinės sistemos kūrimo grupei naujasis rizikos analizės metodas leis įvertinti vystomo produkto galimas saugumo grėsmes projektavimo etape bei padės sukurti saugesnę sistemą.*

Tyrimo objektu pasirinktas realioje įmonėje kuriamos informacinė sistemos saugumas, nes realioje aplinkoje eksperimento rezultatai bus tikslesni. Analizuojama IS yra internetinis B2B portalas, skirtas elektroniniai prekybai tarp įmonių. Dėl konfidencialumo nei įmonės pavadinimas, nei realios kuriamos sistemos tikslus aprašymas nebus atskleistas. IS bus aprašoma tik bendrais bruožais.

Eksperimento tikslas yra įrodyti apsibrėžta hipotezę. Eksperimentui skiriamas terminas yra viena diena, o jo uždaviniai:

- Įvertinti RAISKP metodo etapų vykdymo sklandumą;
- Nustatyti grėsmių tikslumą;
- Įvertinti IS saugumo lygį prieš ir po galimo kontrpriemonių įdiegimo.

Šiame skyriuje bus aprašoma tiriamoji IS bei atliekamas eksperimentas, kurio metu bus vykdoma saugumo rizikos analizė RAISKP metodu.

6.1. Analizuojamos informacinės sistemos aprašymas

Analizuojama IS - Internetinė B2B sistema, kuri orientuota į didmeninę prekybą, kai vienas verslas parduoda kitam. Šios sistemos tikslas yra sukurti internetine svetainę – prekių katalogą, skirta vykdyti didmeninę prekybą Internetu tarp pramonės įmonės, užsiimančios tam tikros produkcijos gamyba, ir mažmeninių prekybininkų, ar tarp įmonės užsiimančios didmenine prekyba su mažmeninės prekybos įmonėmis.

6.1.1. Struktūra

Internetinę B2B sistemą sudaro:

- elektroninė parduotuvė, kurioje klientai peržiūri produktus, formuoja produktų krepšeli ir sudaro užsakymus;
- produktų administravimo sritis skirta informacijos apie produktus patalpinimui;
- užsakymų aptarnavimo (administravimo) sritis skirta vadybininkams klientų užsakymų apdorojimui;
- vartotojų administravimo dalis skirta sistemos vartotojų administravimui.

Sistema sudarys dvi pagrindinės dalys:

1. Publikuojamas prekių katalogas:
    - paieška pagal kriterijų;
    - autorizuotas prisijungimas;
    - prekių užsakymo sudarymas.
2. Katalogo administravimo dalis:
    - prekių administravimo modulis;
    - klientu administravimo modulis;
    - prekių užsakymų valdymo modulis;
    - administravimo dalies teisių ir naudotojų modulis.

6.1.2. Vartotojai

Internetinės B2B sistemos dalyviai skaidomi į 4 grupes:

1. **Klientas** – tai sistemos naudotojas, kuriam sutekti prisijungimo duomenys (prisijungimo vardas, slaptažodis) jungtis prie publikuojamo prekių katalogo. Jam galima naudotis visomis katalogo teikiamomis funkcijomis (peržiūri produktus, formuoja krepšeli, sudaro užsakymus).
2. **Vadybininkas** – tai sistemos naudotojas, kuris turi prisijungimo duomenis prie katalogo administravimo dalies, aptarnauja (tvirtina, sudaro, redaguoja, rezervuoja ir pan.) klientų užsakymus, tvarko informaciją apie produktus ir pagal jam suteiktas teises gali naudotis:
    - Prekių administravimo moduliu jam leistinomis funkcijomis,
    - Klientų administravimo moduliu jam leistinomis funkcijomis.

3. **Katalogo Administratorius** – tai sistemos naudotojas, kuris turi teisę naudotis administravimo dalies teisių ir naudotojų moduliu. Jis kuria vadybininkams skirtus prisijungimus ir suteikia jiems teises, kuriomis administravimo dalies funkcijomis jie galės naudotis (pvz., galės redaguoti prekes, bet negales kurti klientams prisijungimu ir pan.).
4. **Sistemos administratorius** - administruoja (kuria, redaguoja, suteikia teises) sistemos vartotojus.

6.1.3. Funkcionalumas

Internetinės B2B sistemos turi keturis pagrindinius modulius, ir kiekvienas jų turi skirtingą funkcionalumą:

1. Katalogo modulio funkcionalumas:
    - Norint peržiūrėti katalogą,reikia autorizuotis: prisijungti įvedus prisijungimo vardą ir slaptažodį.
    - Prekės kataloge pateikiamos sąrašu.
    - Prekių paieška atliekama pagal užduotus kriterijus, tai gali būti filtro parametrai, įvesti raktiniai žodžiai ar jų dalys:
        - prekės grupe – pasirinkimas iš sąrašo;
        - kodas – įvedamas visas arba fragmentas;
        - gamintojas – pasirenkamas iš sąrašo;
        - kaina – įvedamas skaičius (nuo - iki).
    - Prekės peržiūra.
    - „Akcijos prekių“ sąrašas.
    - Prekių „Naujiena“ sąrašas.
2. Prekių valdymo modulio funkcionalumas:
    - Informacijos apie prekę valdymas (suvedimas, redagavimas, šalinimas):
        - Bendros informacijos įvedimas, redagavimas: kodas, aprašymas, paveiksliukas;
        - Panaudojimo informacijos: gamintojo, pagal kainą priskyrimas;
        - Prekės šalinimas – gali būti pašalinama visai iš sistemos, arba uždedamas požymis, kad prekė nebeplatinama;
    - Prekių publikavimas – suvedus prekės informaciją, ji atsakingo žmogaus sutikrinama ir tik tada prekė publikuojama.
    - Prekių žymėjimas kaip „akcijos prekės“ ar naujos.

- Prekių grupių žinynas.
- Gamintojų žinynas.

3. Kliento valdymo modulio funkcionalumas:
   - Kliento registravimas, registracijos duomenų siuntimas elektroniniu paštu.
   - Prisijungimo duomenų suteikimas.
   - Prisijungimo uždraudimas ar pašalinimas.
   - Slaptažodžio keitimas, pakeisto siuntimas elektroniniu paštu.
4. Sistemos administravimo modulio funkcionalumas:
   - Vartotojo teisių koregavimas.
   - Statistinių duomenų stebėjimas.
   - Vartotojų informavimas elektroninių paštu.
   - Bendros informacijos turinio valdymo sistema.

6.2. Informacinės sistemos rizikos analizė vykdymas RAISKP metodu

Eksperimentui atlikti pasirinkta nedidelė įmonė, kurios pagrindinė veikla yra įvairūs internetiniai sprendimai. Analizuojama IS pasirikta Internetinė B2B sistema todėl, kad eksperimento metu ji buvo kuriama. Prieš pradedant tyrimą, IS projektų vadovas buvo supažindintas su RAISKP metodu (5.2 skyrius).

Šiame poskyryje aprašysime Internetinės B2B sistemos saugumo rizikos analizės eiga panaudojant RAISKP metodą. Pateiksime RAISKP analizės rezultatus, apžvelgsime metodo etapų procesą bei juos įvertinsime.

6.2.1. Pasiruošiamieji darbai ir grupės formavimas

IS kūrimo projektų vadovas, susipažinęs su RAISKP metodu, nesunkiai atliko primarį metodo etapą (pasiruošiamieji darbai). Pagal metodo reikalavimus, buvo apirėžta:

1. **Analizės tikslas** - Nustatyti sistemai gresiančias grėsmes ir parinkti kontrpriemones, kurios sumažintų rizika iki priimtino lygio.
2. **Analizės ribos** – Internetinė B2B sistema ir į ją įeinantys ir išeinantys duomenis;
3. **Priimtina rizika** – iki 5 (vertinimo skalė pateikta 4 priede). Deja IS savininkas negalėjo dalyvauti šiame tyrime, todėl priimtina rizika buvo nustatyta projektų vadovo.
4. **Pagrindinės sąvokos**:
   - Rizika – įvykio tikimybė ir jo pasekmių derinys;

- Rizikos vertinimas – procesas, kurio metu rizikos tikimybė ir pasekmės išreiškiamos konkrečia reikšme;
- Grėsmė – veiksnys, kuris gali sukelti nuostolius organizacijoje;
- Pažeidžiamumas – sistemos silpna vieta, kurią pasinaudojus gali būti realizuota grėsmė;
- Saugos priemonė – procesas ar funkcija, kuris sumažina riziką;
- Likutinė rizika – rizika, kuri lieka po saugumo priemonės įdiegimo.

Pagal RAISKP metodo reikalavimus, buvo padaryta vizualinė sistemos schema, kad analizės grupės nariai geriau galėtų identifikuoti grėsmes bei supratų IS ribas. Šiai užduočiai atlikti buvo pakviestas projektuotojas. Projektuotojui užduotis nepasirodė labai sudėtinga ir galinti užtrūkti daug laiko, nes eskizines schemas jis jau turėjo, tereikėjo jas truputi perdaryti, kad būtų labiau suprantamos analizės grupės nariams.

Kitas RAISKP metodo žingsnis yra analizės grupės suformavimas. Deja nepavyko pakviesti IS savininko ir Informacijos saugos specialisto ar sistemos administratoriaus iš organizacijos, kuriai buvo kuriama sistema, todėl RAISKP grupė buvo sudaryta iš vidinių resursų, kurią sudarė:

1. projektų vadovas;
2. projektuotojas;
3. programuotojas;
4. verslo procesų analitikas.

Vertinat pirmojo ir antrojo RAISKP metodo etapų procesą, galima būtų teikti, kad viskas vyko sklandžiai, neskaitant to, kad nepilna analizės grupė buvo sudaryta.

6.2.2. Grėsmių nustatymas ir vertinimas

Šiame etape rizikos analizės grupė turi nustatyti („idėjų vėtros“ principu) kylančias grėsmes analizuojamai sistemai, nustatyti grėsmių tipą (ar grėsmė kyla informacijos vientisumui, konfidencialumui ar prieinamumui), kilmę (ar grėsmė yra sąmoninga ar ne) bei įvertinti grėsmės tikimybę bei galima žalą sistemai (vertinimo lentelė pateikta 4 priede).

Šio proceso eiga iš pradžių vyko nelabai sklandžiai. Grupės nariams buvo sunku sugalvoti kylančias grėsmes, tačiau projektų vadovui pateiktus kelėta pavyzdžių, grėsmių generavimas įgavo pagreitį. Kartais grupės nariai siūlydavo grėsmes, kurios nepatekdavo į analizės ribas, todėl projektuotojui tekdavo priminti analizės rėmus. Žvelgiant į vertinimo lentelę, grėsmių tikimybė ir galimi nuostoliai buvo įvertinti nesunkiai (šio etapo rezultatas pateiktas 1 priede).

Vertinant grėsmių nustatymo ir vertinimo procesą, galimą būtų teikti, kad grėsmių generavimo etapas vyktų sklandžiau, jeigu būtų pateiktas sąrašas pavyzdinių grėsmių.

6.2.3. Saugumo priemonių nustatymas ir parinkimas

Saugumo priemonių nustatymo etape RAISKP grupė turi parinkti tinkamas kontrpriemones rizikai sumažinti bei įvertinti likutinę riziką. Jeigu vienos saugumo priemonės nepakanka rizikai sumažinti iki priimti lygio, tai tuomet yra parenkamos kelios. Nagrinėjamos tik tos grėsmės, kurios yra nepriimtinos rizikos lygio. Saugumo priemonių parinkimo etape yra nustatoma kokios kontrpriemonės bus diegiamos ir kokie jų kaštai. Taip pat yra pergrupuojamos grėsmės pagal saugumo priemones.

Stebint RAISKP metodo 5 ir 6 etapo vykdymą, buvo pastebėta, kad saugumo priemonių nustatymas vyko sklandžiau negu grėsmių. Likutinės rizikos nustatymas taip pat nesukėlė grupės nariams sunkumų. Kadangi rizikos analizėje nedalyvavo IS savininkas, tai priimtinas saugumo priemones nustatė visa grupė. Sunkiausiai sekėsi vertinti kontrpriemonės kaštus (saugumo priemonių nustatymo rezultatai pateikti 2 priede, o saugumo priemonių parinkimo rezultatai pateikti 3 priede).

Vertinant saugumo priemonių nustatymo ir parinkimo procesą, galimą būtų teikti, kad viskas vyko sklandžiai, gal tik reikėtų pateikti papildoma medžiagai apie kontrpriemonės kaštų vertinimą.

6.2.4. Baigiamieji darbai - dokumentavimas

Dokumentavimas yra paskutinis žingsnis RAISKP analizėje. Šiame etape yra paruošiama ataskaita su RAISKP rezultatais bei prieš tai buvusių etapų rezultatų dokumentai kaip priedai. RAISKP dokumentacija yra pridedama prie bendros IS dokumentacijos.

Pasibaigus visiems prieš tai buvusiems RAISKP etapams, projektų vadovas dokumentavo proceso eiga (1,2,3 priedai), bei padarė RAISKP ataskaitą (4 priedas). Šis etapas buvo lengvai atliktas pateikus dokumentavimo pavyzdį.

Vertinant RAISKP dokumentacijos etapą, galimą būtų teikti, kad jis atliekamas nesunkiai, reikia tik pateikti pavyzdį.

6.3. Tyrimo rezultatai

Eksperimentu atlikus rizikos analizę RAISKP metodu galima teikti, kad metodas yra nesunkai atliekamas IS kūrimo grupės narių. Eksperimento dalyviai metodo pritaikymą įvertino kaip lengvai suprantamą, greitai atliekama ir teikiantį svarbių rezultatų, kurie bus panaudoti informacinės sistemos kūrime. RAISKP analizė užtruko nepilną darbo dieną ir leido IS kūrimo grupei nesudėtingai nustatyti rizikas, susijusias sus sistemos saugumų, bei pritaikyti tinkamiausias saugumo priemones rizikoms sumažinti iki priimtino lygio. Sklandų metodo taikymą truputi trikdė pavyzdžių trūkumas, todėl prie metodo aprašymo pageidautina būtų pateikti pavyzdinių grėsmių ir kontrpriemonių sąrašą.

Eksperimento metu nustatytos grėsmės ir kontrpriemonės tiriamai sistemai yra racionalios ir patenka į analizės apibrėžtus rėmus. Nors ir buvo siūlomos netinkamos grėsmės ir kontrpriemonės tiriamam objektui, bet jos buvo atmetamos kitų eksperimento dalyvių.

Apskaičiavus rizikos veiksnių vidurkį, kuriuos kėlė nustatytos grėsmės, bei apskaičiavus likutinės rizikos veiksniu vidurki po galimo kontrpriemonių įdiegimo, paaiškėjo, kad tiriamos informacinės sistemos saugumo lygis padidėtų 47% jeigu būtų įdiegtos saugumo priemonės, kurios buvo nustatytos RAISKP metodu.

Remiantis eksperimento rezultatais, laikoma, kad hipotezė yra įrodyta.

IŠVADOS

Nustačius pagrindinius rizikos valdymo principus, paaiškėjo, jog norint efektyviai valdyti rizikas, būtina pastoviai vykdyti tokius etapus kaip: rizikos apimties apibrėžimas, rizikos vertinimas, rizikos tvarkymas, informavimas apie riziką, rizikos stebėjimas ir peržiūrėjimas. RV yra privalomas procesas, jeigu organizacija nori nustatyti esamas rizikas, įvertini rizikos poveikį ir pasirinkti geriausias kontrpriemones, kurios sumažintu riziką. Šis procesas padeda sumažinti galimus nuostolius dėl kylančių organizacijai saugumo grėsmių. Rizikos valdymas padidina organizacijos stabilumą, nes kiekviena galima grėsmė yra numatoma ir jai pritaikomos apsisaugojimo priemonės. Sėkmingam RV įgyvendinimui būtina įmonės vadovybės parama ir palaikymas, saugos politika, uždaviniai ir veiksmai turi atspindėti organizacijos tikslus, proceso ribos turi būti aiškiai apibrėžtos.

Rizikos valdymo bei vertinimo metodikų analizė parodė, kad yra paltus jų pasirinkimas bei jie suteikia galimybę organizacijai tinkamai valdyti rizikas. Rizikos analitikai ir ekspertai, ilgais tyrimais ir praktika, yra numatę geriausius ir racionaliausius etapus bei funkcijas rizikos valdymo ir vertinimo procesuose.

Lyginant populiariausius RV metodus, išryškėjo jų skirtumai ir panašumai. Metodų skirtumai pastebimi valdymo etapų (rizikos identifikavimo, analizės, vertinimo, tvarkymo, priėmimo bei komunikacijos) metodinių nurodymų detalume. Vieni metodai nuodugniai nagrinėja tik tam tikrus RV etapus ir visiškai neaptariami kiti procesai (pvz. *MEHARI*), kiti apžvelgia visus etapus, tačiau tik bendrus reikalavimus (pvz. *OCTAVE*), treti detaliai nagrinėja visą rizikos valdymo procesą (pvz. *EBIOS*). Taip pat, metodai išsiskiria savo būdais pasiekti tikslą, pritaikomumu organizacine pagal jos dydį, reikalingų žinių lygių norint taikyti metodą bei suderinamumu su tarptautiniais saugumo standartais. Metodai panašūs savo taikymo filosofija, vykdomom procedūromis, iškeltais reikalavimais bei užsibrėžtais tikslais . Tinkamiausias metodas organizacijai turėtų būti tas, kuris labiausiai atitinka jos politiką, dydį bei turimus resursus rizikos valdymui vykdyti ir kontroliuoti.

Nagrinėjant rizikos valdymo ir vertinimo įrankius, pastebėta, kad kaip ir RV metodų, taip ir įrankių pasirinkimas yra platus. Visų įrankių funkcionalumas yra paremtas viena ar kita rizikos valdymo metodologija. Pagrindinis įrankių tikslas yra automatizuoti rizikos valdymo ir vertinimo procesus, kad analitikai daugiau lako galėtų skirti sudėtingiems ir intelekto reikalaujantiems tyrimams.

Lyginant populiariausius rizikos valdymo ir vertinimo įrankius paaiškėjo, kad dauguma jų automatizuoja ataskaitų ruošimo ar rizikos apskaičiavimo procesus, sukauptomis žynių bazėmis padeda nustatyti organizacijai kylančias grėsmes bei parinkti geriausias kontrpriemones, nustato

arba padeda pasiekti atitikimą tarptautiniams saugumo standartams. Įrankiai išsiskiria naudojamais rizikos valdymo ir vertinimo metodais, funkcionalumu bei kaina. Prieš renkantis rizikos valdymo įrankį, organizacija turėtų būti tvirtai apsisprendusi dėl naudojamo RV metodo tipo.

Vertinant rizikos analizės metodus, nustatyta, jog analizę galima atlikti pritaikius kiekybinį ar kokybinį metodą. Kiekybiniai metodai yra labiau tinkami tais atvejais, kai saugos sprendimai daro įtaka finansiniams sprendimams, o kokybinė rizikos analizė turėtų būti pasirinkta tuomet, kai priimami sprendimai yra susiję su baziniu saugos sukūrimu. Populiariausias kiekybinės analizės metodas yra TMN, o kokybinės 10ŽM, 3ŽM, 30MM bei KURAP. Kiekybinė analizė yra objektyvesnė bei geriau suprantama vadovybei dėl nuostolių įvertinimo pinigine verte, tačiau jos atlikimui reikia daugiau finansinių ir laiko resursų, nes būtina sukaupti daug informacijos bei atlikti sudėtingus skaičiavimus. Kokybinė analizė yra paprastesne, greičiau atliekama bei nereikalauja didelių resursų, tačiau jos rezultatai yra subjektyvus, todėl analizės grupė turi būti kompetentinga.

Egzistuojančių rizikos analizės metodų tyrimas leido išskirti geriausias jų savybes. Metodų tyrimo metu buvo identifikuoti greičiausi ir lengviausiai atliekami etapai, kurie su nedideliais pakeitimas buvo pritaikyti naujame RAISKP metode. Sukurtas metodas buvo orientuotas į siauresnę bet detalesnę analizę IS rėmuose, todėl taikant jį nėra nagrinėjamos bendros rizikos organizacijos mastu. Yra gilinamasi į smulkesnes informacines sistemos rizikas. Kontrpriemonės parenkamos tokios, kurios gali būti realizuotos IS kūrimo komandos. Vienas iš RAISKP metodo sukūrimo uždavinių buvo greitai ir lengvai atliki saugumo rizikos analizę, todėl jo etapai yra paprasti ir nereikalaujantys daug laiko.

Praktinis RAISKP metodo pritaikymo tyrimas leido įvertinti jo efektyvumą ir teikiamą naudą IS kūrimo procesui. Tyrimo metu buvo įsitikinta, kad metodo taikymas yra nesudėtingas ir neatimantis daug laiko. RAISKP metodo pateikti rezultatai suteikė daug naudingos informacijos IS kūrimo komandai, kuri aiškiai identifikavo saugumo rizikas ir pasirinko geriausiai tinkančias kontrpriemones. Eksperimento metu pasitvirtino iškelta hipotezė, kad informacinės sistemos kūrimo grupei naujasis rizikos analizės metodas leis įvertinti vystomo produkto galimas saugumo grėsmes projektavimo etape bei padės sukurti saugesnę sistemą.

SUMMARY

Information security risk analysis method in process of developing information system

Information is becoming a more valuable and a more expensive good, so there is no surprise that security of information has become a big issue as well. Modern companies directly deal and depend on information systems. These companies are facing with complex issues of integrity, privacy and accessibility of information. The most effective way to shade from arising threats is information security management system. One of the most important stages of information security management system is risk management and analysis. Main information risk management and analysis tasks is to identify existing risks, estimate the possible influence towards the organization and select most suitable preventive measures for minimizing risk level.

The object of the paper – security of the information systems. *The aim of the paper* – to create an information security risk analysis method, this could be applied in developing information system process and could increase security level. *The tasks of the paper* – are to determine the main risk management principles; compare the most popular methods and tools; evaluate widely spread methods of risk analysis; define main stages of new risk analysis method according to the best features of the existing methods; rate the efficiency of new method by the experiment.

According to the literature analysis; comparative; extrapolation and experimental methods in the paper are introduced the main principles of security risk management and analysis; compared the most popular tools and methods of risk management and evaluation; created and evaluated the new RAISKP method of risk analysis.

After determining the main risk management principles, it has been noticed that it is necessary permanently implement the below given stages for the effective risk management: risk volume description, risk evaluation, risk administration, informing about risks, risk monitoring and review. Risk management increases the stability of an organization, because each threat can be foreseen and security measures adjusted and applied.

After comparing the most popular risk management methods similarities and differences were noticed. Different methods are different in achieving goals, suitability for an organization depending on size of organization, compatibility with international standards, and required knowledge for applying the technique. But techniques are very similar in philosophy of practice, procedures, requirements and aims.

After comparing the most popular tools of risk management and evaluation it was noticed that most of them automates processes of reports and risk calculation; helps to foresee future threats according to accumulated knowledge base, and then helps to select most suitable preventive measures for it; determines or helps to conform suitability to international security standards. Tools are different in risk management and evaluation methods, functionality and price.

After evaluation risk analyses methods was noticed that analyses can be done using qualitative and quantitative methods. Quantitative methods are more suitable when security decision make influence on financial decisions, qualitative risk analyses should be chosen when made decisions are associated with basic security creation. The investigation of existing methods of risk analyses allowed segregate the best features of them. During the survey of methods were identified the fastest and easiest stages, which with small changes were adjusted for the new RAISKP method.

Practical RAISKP adjustability test allowed to evaluate method efficiency and benefits in the process of IS developing. During the test it was clear that the new risk analyses method allows foreseeing threat gaps already in the stage of projection, which helps to create a safer system.

This paper can be useful for information security specialists, for information system designers, and for information system discipline students.

Paper written by
Dainius Neverbickas

BIBLIOGRAFINIŲ NUORODŲ SĄRAŠAS

1. KARDELIS, Kęstutis. *Mokomųjų tyrimų metodologija ir metodai*: vadovėlis. 2-asis patais.ir papild. leid. Kaunas: Judex leidykla, 2002. 398 p. ISBN 9986-948-65-7.

2. ŠLEKIENĖ, Violeta. *Mokslinio tyrimo metodologija*: paskaitų konspektas [interaktyvus]. [S. l., s. a.] [žiūrėta 2007.11.05]. Prieiga per Internetą: <http://www.su.lt/article/articleview/1060/1/516/>.

3. VAGERIS, Robertas. *Rizikos Analizės Vadovas* [interaktyvus]. Vilnius: VAGA leidykla, 2005. 160p. ISBN 5-415-01827-1 [žiūrėta 2006.12.10]. Prieiga per Internetą: <http://www.vrm.lt/fileadmin/Padaliniu_failai/Informacines_politikos_dep/IT_sauga/Rizikos_analize.pdf >.

4. Technical Department of ENISA Section Risk Management. *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools*: Survey of existing Risk Management and Risk Assessments Methods [interaktyvus].Greese: ENISA, 2006. 168p. [žiūrėta 2007.01.04]. Prieiga per Internetą: <http://www.enisa.europa.eu/rmra/files/D1_Inventory_of_Methods_Risk_Management_Final.pdf>.

5. VAGERIS, Robertas. *Rizikos valdymas:* prezentacija [interaktyvus]. ISACA Lietuva 2006.04.27 [žiūrėta 2006.12.17]. Prieiga per Internetą: <http://www.ase.lt/Presentations/Rizikos%20valdymas%20200604.pdf>.

6. Lietuvos standartizacijos departamentas. *Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas (tapatus ISO/IEC 17799:2005)*: LST ISO/IEC 17799:2005 lt standartas. Vilnius: LSD, 2005.

7. ISO/IEC. *Information technology - Guidelines for the management of IT Security —Part 1: Concepts and models for IT Security:* ISO/IEC TR 13335-2:1997 standartas. Swizerlend: ISO, 1997.

8. ISO/IEC. *Information technology - Guidelines for the management of IT Security —Part 2: Managing and Planning IT Security:* ISO/IEC TR 13335-2:1996 standartas. Swizerlend: ISO, 1996.

9. Microsoft Corporation. *The Security Risk Management Guide v1.2* [interaktyvus]. San Francisco, California, USA: Microsoft Corporation, 2006. 126p. [žiūrėta 2006.12.17]. Prieiga per Internetą: <http://www.microsoft.com/downloads/details.aspx?familyid=C782B6D3-28C5-4DDA-A168-3E4422645459&displaylang=en>.

10. UAB „Compservis“ Informacijos apsaugos ir IT paslaugų valdymo skyrius. *CRAMM rizikų analizės ir valdymo metodika* [interaktyvus]. [S. l., s. a.] [žiūrėta 2007.04.04]. Prieiga per Internetą: <http://www.cramm.lt/>.

11. Siemens Enterprise Communications. *CRAMM tollkit* [interaktyvus]. [S. l., s. a.] [žiūrėta 2007.03.15]. Prieiga per Internetą: <http://www.cramm.com/>.

12. ÆXIS Security Consultants. *RA2 art of risk* [interaktyvus]. [S. l., s. a.] [žiūrėta 2007.03.13]. Prieiga per Internetą: <http://www.aexis.de/RA2ToolPage.htm>.

13. Callio. *Callio Secura 17799* [interaktyvus]. [S. l., s. a.] [žiūrėta 2007.04.14]. Prieiga per Internetą: <http://www.callio.com/>.

14. C&A Systems Security. *COBRA* [interaktyvus]. [S. l., s. a.] [žiūrėta 2007.02.13]. Prieiga per Internetą: <http://www.riskworld.net/>.

15. DCSSI Advisory Office. *EBIOS – Expression of Needs and Identification of Security Objectives* interaktyvus]. [S. l., s. a.] [žiūrėta 2007.04.04]. Prieiga per Internetą: <http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html>.

16. DCSSI Advisory Office *10 GOOD REASONS TO USE The EBIOS® application* [interaktyvus]. France, Paris: DCSSI, 2003. 2p. [žiūrėta 2007.03.16]. Prieiga per Internetą: <http://www.ssi.gouv.fr/en/confidence/documents/methods/ebiosv2-logiciel-plaquette-2003-06-30_en.pdf>.

17. DCSSI Advisory Office. „*EBIOS Inroduction*“. [interaktyvus]. France, Paris: DCSSI, 2004. 29p. [žiūrėta 2007.04.04]. Prieiga per Internetą: <http://www.ssi.gouv.fr/en/confidence/documents/methods/ebiosv2-section1-introduction-2004-02-05_en.pdf>.

18. Federal Office for Information Security (BSI). *IT-Grundschutz Tool* [interaktyvus]. [S. l., s. a.] [žiūrėta 2007.04.04]. Prieiga per Internetą: <http://www.bsi.bund.de/english/gstool/>.

19. Carnegie Mellon University. *OCTAVE® Overview:Operationally Critical Threat, Asset, and Vulnerability Evaluation* [interaktyvus]. [S. l.], 2003. 152p. [žiūrėta 2007.04.04]. Prieiga per Internetą: <http://www.cert.org/archive/pdf/octave_Alt_Exec_Session.pdf>.

20. ALBERTS, Christopher, *et al*. *Introduction to the OCTAVE® Approach* [interaktyvus]. [S. l.], 2003. 27p. [žiūrėta 2007.03.15]. Prieiga per Internetą <http://www.cert.org/octave/approach_intro.pdf>.

21. CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS. *MEHARI 2007Risk Analysis Guide* [interaktyvus]. France, Paris, 2007. 16p. [žiūrėta 2007.04.04]. Prieiga per Internetą: <http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2007-Risk_analysis_2007.pdf>.

22. Information Governance Ltd. *Proteus internetinė svetainė* [interaktyvus]. [S. l., s. a.] [žiūrėta 2007.02.13]. Prieiga per Internetą: <http://www.infogov.co.uk/>.

23. HELMBRECHT, Udo. *IT Baseline Security Manual (IT-Grundschutz) part 1*[interaktyvus]. [S. l], 2004. [žiūrėta 2007.01.17]. Prieiga per Internetą: <http://www.bsi.de/english/gshb/manual/download/modules.pdf>.

24. Bender RBT Inc. *Systems Development Lifecycle:Objectives and Requirements*. [S. l], 2003. 60p. [žiūrėta 2007.11.10]. Prieiga per Internetą: <http://www.benderrbt.com/Bender-SDLC.pdf>.

25. C&A Systems Security. *COBRA 3.1.8:* kompiuterinė programa [interaktyvus]. [S. l., s. a.] [žiūrėta 2007.02.13]. Prieiga per Internetą: < http://www.riskworld.net/evaluate.htm/>.

26. ÆXIS Security Consultants. *RA2 art of risk:* kompiuterinė programa [interaktyvus]. [S. l., s. a.] [žiūrėta 2007.03.13]. Prieiga per Internetą: <http://www.aexis.de/RA2_art_of_risk_%20Demo.zip >.

27. Bundesamt für Sicherheit in der Informationstechnik. *GSTOOL 4.1:* kompiuterinė programa [interaktyvus]. [S. l., s. a.] [žiūrėta 2007.03.13]. Prieiga per Internetą: <http://www.bsi.bund.de/gstool/down.htm>.

28. Proteus Enterprise. *Proteus:*rizikos valdymo įrankis [interaktyvus]. [S. l., s. a.] [žiūrėta 2007.03.13]. Prieiga per Internetą: <http://www.infogov.co.uk/proteus>.

PRIEDAI

1. Internetinės B2B sistemos rizikų įvertinimas RAISKP metodu

Nr	Grėsmė	Tipas	Kilmė	Tikimybė	Žala	Rizikos Veiksnys
1	Neteisingas duomenų įvedimas vartotojo registracijos metu	V	S	3	2	5
2	Neteisingas duomenų įvedimas vartotojo registracijos metu	V	N	3	2	5
3	Iš sistemos nėra atsijungiama baigus darbą	K,V,P	N	4	3	7
4	Vartotojas ištrina savo duomenys	V,P	N	1	3	4
5	Neteisėtas prisijungimas prie sistemos vartotojo vardu spėliojant slaptažodį	V,K,P	S	1	4	5
6	Neteisėtas sistemos prisijungimas administratoriaus teisėmis spėliojant slaptažodį	V,K,P	S	3	5	8
7	Neteisėtas priėjimas prie sistemos duomenų bazės pasinaudojant tarnybinėje stotyje esančiomis programinės įrangos spragomis	V,K,P	S	4	5	9
8	Sistemos duomenų praradimas, sunaikinimas	P	S,N	3	5	8
9	Neteisėtas sistemos duomenų pakeitimas	V	S	3	5	8
10	Sistemos veikimo sutrikdymas	P,V	N	3	4	7
11	Duomenų perėmimas ar pakeitimas tinkle	V,K	S	2	5	7
12	Vartotojas praranda ryši su sistema operacijos vykdymo metu	V	N	3	3	6
13	Netyčinis operacijos įvykdymas	V	N	3	2	5
14	Tyčinis sistemos veikimo trikdymas (DOS atakos,virusai)	P	S	4	4	8
15	Piktybinio kodo panaudojimas įvedant jį į sistemoje koreguojamus laukus	V,K,P	S	4	5	9
16	Įtartinai didelių užsakymų vykdymas	V	S	2	2	4
17	Vartotojas pateikia neteisingus duomenys apie produktus	V	S	2	2	4

2. Internetinės B2B sistemos saugumo priemonių nustatymas RAISKP metodu

Nr	Grėsmė	Tipas	Kilmė	Rizikos Veiksnys	Saugos priemonė	Likutinė rizika
1	Neteisingas duomenų įvedimas vartotojo registracijos metu	V	S	5	Duomenų patvirtinimas elektroniniu laišku	4
2	Neteisingas duomenų įvedimas vartotojo registracijos metu	V	N	5	Įvedamų laukų tikrinimo funkcijos	2
3	Iš sistemos nėra atsijungiama baigus darbą	K,V,P	N	7	Sistemos automatinis atsijungimas po tam tikro laiko	2
5	Neteisėtas prisijungimas prie sistemos vartotojo vardu spėliojant slaptažodį	V,K,P	S	5	Prisijungimo prie sistemos bandymų ribojimo funkcija Periodinio slaptažodžio keitimo funkcija	2
6	Neteisėtas sistemos prisijungimas administratoriaus teisėmis spėliojant slaptažodį	V,K,P	S	8	Slaptažodžio tvirtumo tikrinimas Prisijungimo vietos apribojimas Periodinio slaptažodžio keitimo funkcija	1
7	Neteisėtas priėjimas prie sistemos duomenų bazės pasinaudojant tarnybinėje stotyje esančiomis programinės įrangos spragomis	V,K,P	S	9	Antivirusinė programa Ugniasienė IDS (intrusion detection system)	2
8	Sistemos duomenų praradimas, sunaikinimas	P	S, N	8	Atsarginės kopijos periodinio darymo funkcija	2
9	Neteisėtas sistemos duomenų pakeitimas	V	S	8	Atsarginės kopijos periodinio darymo funkcija Operacijų stebėjimas (logging)	3
10	Sistemos veikimo sutrikdymas	V	N	7	Transakcijų funkcijos	3
11	Duomenų perėmimas ar pakeitimas tinkle	V,K	S	7	Duomenų šifravimas	2
12	Vartotojas praranda ryši su sistema operacijos vykdymo metu	V	N	6	Transakcijų funkcijos	3
13	Netyčinis operacijos įvykdymas	V	N	5	Operacijos atšaukimo funkcija	1
14	Tyčinis sistemos veikimo trikdymas (DOS atakos,virusai)	P	S	8	Ugniasienė IDS (intrusion detection system)	3
15	Piktybinio kodo panaudojimas įvedant jį į sistemoje koreguojamus laukus	V,K,P	S	9	Įvedamų duomenų filtravimo funkcijos	2

3. Internetinės B2B sistemos saugumo priemonių parinkimas RAISKP metodu

Nr	Saugos priemonė	Kaštai	Diegti?	Grėsmė	Tipas	Kilmė	Rizikos Veiksnys	Likutinė rizika
1	Duomenų patvirtinimas elektroniniu laišku	30 val	Taip	Neteisingas duomenų įvedimas vartotojo registracijos metu	V	S	5	4
2	Įvedamų laukų tikrinimo funkcijos	50 val	Taip	Neteisingas duomenų įvedimas vartotojo registracijos metu	V	N	5	2
3	Sistemos automatinis atsijungimas po tam tikro laiko	0	Taip	Iš sistemos nėra atsijungiama baigus darbą	K,V,P	N	7	2
4	Prisijungimo prie sistemos bandymų ribojimo funkcija	0	Taip	Neteisėtas prisijungimas prie sistemos vartotojo vardu spėliojant slaptažodį	V,K,P	S	5	2
5	Periodinio slaptažodžio keitimo funkcija	30 val	Taip					
6	Slaptažodžio tvirtumo tikrinimas	30 val	Taip	Neteisėtas sistemos prisijungimas administratoriaus teisėmis spėliojant slaptažodį	V,K,P	S	8	1
7	Prisijungimo vietos apribojimas	20 val	Taip					
	5 saugumo priemonė	0	+					
8	Antivirusinė programa	0	Yra	Neteisėtas priėjimas prie sistemos duomenų bazės pasinaudojant tarnybinėje stotyje esančiomis programinės įrangos spragomis	V,K,P	S	9	6
9	Ugniasienė	0	Yra					
10	IDS (intrusion detection system)	30 000 Lt	Ne					
11	Atsarginės kopijos periodinio darymo funkcija	30 val	Taip	Sistemos duomenų praradimas, sunaikinimas	P	S, N	8	2
	11 saugumo priemonė	0	+	Neteisėtas sistemos duomenų pakeitimas	V	S	8	3
12	Operacijų stebėjimas (logging)	40 val	Taip					
13	Transakcijų funkcijos	0	Taip	Sistemos veikimo sutrikdymas	V	N	7	3
				Vartotojas praranda ryši su sistema operacijos vykdymo metu	V	N	6	3
14	Duomenų šifravimas	0	Taip	Duomenų perėmimas ar pakeitimas tinkle	V,K	S	7	2
15	Operacijos atšaukimo funkcija	20 val	Taip	Netyčinis operacijos įvykdymas	V	N	5	1
	9 saugumo priemonė	0	Yra	Tyčinis sistemos veikimo trikdymas (DOS atakos,virusai)	P	S	8	6
	10 saugumo priemonė	30 000 LT	-					
16	Įvedamų duomenų filtravimo funkcijos	50 val	Taip	Piktybinio kodo panaudojimas įvedant jį į sistemoje koreguojamus laukus	V,K,P	S	9	2

4. Internetinės B2B sistemos RAISKP analizės ATASKAITA

Saugumo rizikos analizė RAISKP metodų ataskaita

Data: 2007.12.05

Sistema: Internetinė B2B sistema

Sistemos savininkas: Jonas Jonaitis

Analizės grupė:
Dainius Neverbickas, saugumo analitikas
Petras Petraitis, IS projektų vadovas
Juozas Juozaitis, IS projektuotojas
Giedrius Giedraidis, programuotojas

Analizės tikslas: Nustatyti sistemai gresiančias grėsmes ir parinkti kontrpriemones, kurios sumažintų rizika iki priimtino lygio.

Rizikos vertinimo kriterijai

Kaštai / Tikimybė	Maža	Maža-vidutinė	Vidutinė	Vidutinė-didelė	Didelė
Maža	2	3	4	5	6
Maža-vidutinė	3	4	5	6	7
Vidutinė	4	5	6	7	8
Vidutinė-didelė	5	6	7	8	9
Didelė	6	7	8	9	10

* Pilkai pažymėta rizika buvo nustatyta kaip priimtina

Saugumo priemonės, kurios buvo priimtos diegimui

NR	Saugumo priemonė	Kaštai
1	Duomenų patvirtinimas elektroniniu laišku	30 val
2	Įvedamų laukų tikrinimo funkcijos	50 val
3	Sistemos automatinis atsijungimas po tam tikro laiko	0
4	Prisijungimo prie sistemos bandymų ribojimo funkcija	0
5	Periodinio slaptažodžio keitimo funkcija	30 val
6	Slaptažodžio tvirtumo tikrinimas	30 val
7	Prisijungimo vietos apribojimas	20 val
8	Atsarginės kopijos periodinio darymo funkcija	30 val
9	Operacijų stebėjimas (logging)	40 val
10	Transakcijų funkcijos	0
11	Duomenų šifravimas	0
12	Operacijos atšaukimo funkcija	20 val
13	Įvedamų duomenų filtravimo funkcijos	50 val
	Viso:	**300 val**

Nepriimtinos saugumo priemonės

NR	Saugumo priemonė	Kaštai
1	IDS (intrusion detection system)	30 000 Lt

Esamos saugumo priemonės

NR	Saugumo priemonė
1	Antivirusinė programa
2	Ugniasienė

Grėsmės, kurios bus sumažintos iki priimtino lygio įdiegus saugumo priemones

NR	Grėsmė	Likutinė rizika
1	Neteisingas duomenų įvedimas vartotojo registracijos metu	4
2	Neteisingas duomenų įvedimas vartotojo registracijos metu	2
3	Iš sistemos nėra atsijungiama baigus darbą	2
4	Neteisėtas prisijungimas prie sistemos vartotojo vardu spėliojant slaptažodį	2
5	Neteisėtas sistemos prisijungimas administratoriaus teisėmis spėliojant slaptažodį	1
6	Sistemos duomenų praradimas, sunaikinimas	2
7	Neteisėtas sistemos duomenų pakeitimas	3
8	Sistemos veikimo sutrikdymas	3
9	Vartotojas praranda ryši su sistema operacijos vykdymo metu	3
10	Duomenų perėmimas ar pakeitimas tinkle	2
11	Netyčinis operacijos įvykdymas	1
12	Piktybinio kodo panaudojimas įvedant jį į sistemoje koreguojamus laukus	2

Grėsmės, kurias organizacija turi prisiimti savo atsakomybėn dėl nepriimtinų saugumo priemonių

NR	Grėsmė	Likutinė rizika
1	Neteisėtas priėjimas prie sistemos duomenų bazės pasinaudojant tarnybinėje stotyje esančiomis programinės įrangos spragomis	6
2	Tyčinis sistemos veikimo trikdymas (DOS atakos,virusai)	6

Grėsmės, kurios buvo priimtiname rizikos lygyje netaikant saugumo priemonių

NR	Grėsmė	Rizikos veiksnys
1	Vartotojas ištrina savo duomenys	4
2	Įtartinai didelių užsakymų vykdymas	4
3	Vartotojas pateikia neteisingus duomenys apie produktus	4

IS projektų vadovo vardas, pavardė ir parašas

_____

IS savininko vardas, pavardė ir parašas

_____