

# Rizikų vertinimas

**UAB „Informacijos saugos sprendimai“**  
www.isec.lt

2007 metų balandis



## Turinys

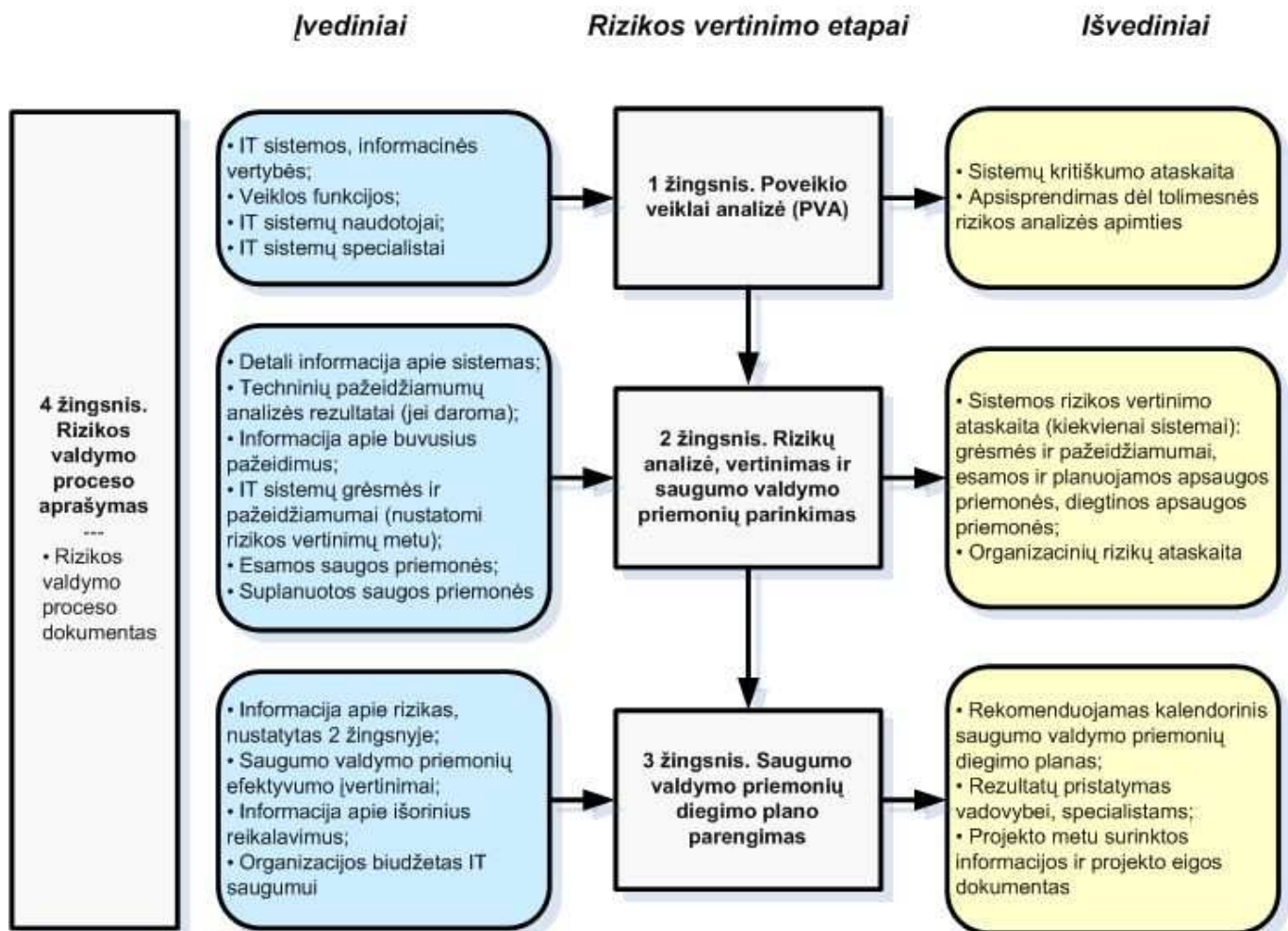
1. Rizikų vertinimas .....	3
2. Poveikio veiklai analizė .....	3
3. Rizikų analizė, vertinimas ir saugumo valdymo priemonių parinkimas.....	4
4. Saugumo valdymo priemonių diegimo plano parengimas.....	5
5. Rizikos valdymo proceso dokumentas.....	5
6. Apie mus .....	5
7. Kontaktai .....	6

## 1. Rizikų vertinimas

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

Esame pasiruošę surinkti reikiamą informaciją ir parengti Jums tinkamiausią sprendimą.

Rizikų vertinimo procesą sudaro 4 pagrindiniai etapai



Toliau pateikiama informacija apie kiekvieną iš etapų.

## 2. Poveikio veiklai analizė

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

**Rezultatai:**

- Dokumentuota ir pagrindžiama informacija apie tai, kiek įmonės veiklos funkcijos yra priklausomos nuo informacinių sistemų. Dokumentuojama, kokios informacinės sistemos yra labiausiai kritiškos, kurios mažiau kritiškos.
- Veiklos vadovams ši informacija leis efektyviau panaudoti ir pagrįsti investicijas, skiriant daugiau lėšų kritiškos sistemoms, mažiau – nekritiškos.
- Poveikio veiklai analizė padeda išversti techninę informacinių sistemų poreikių kalbą į veiklos vadovų kalbą, kuri daugiau orientuota į veiklos procesus ir jų rizikas. Tai leidžia pagrįsti IT sistemų poreikius, nustatyti ir patvirtinti sistemų reikšmingumo lygius.
- 

**Įgyvendinimas**

- Informacija surenkama interviu su informacinių sistemų naudotojais metu. Jais gali būti veiklos padalinių vadovai arba kiti patyrę darbuotojai.
- Visa interviu metu surinkta medžiaga dokumentuojama naudojant patikrintą ir efektyvią metodiką, kuri leidžia lengvai atnaujinti analizės rezultatus kitais metais.
- Remiantis poveikio veiklai analizės rezultatais, priimami sprendimai, kokioms sistemoms reikalinga detali rizikos analizė, kokie informacijos saugumo aspektai yra labiausiai kritiški tam tikrai sistemai.
- Parengiama ataskaita, kurioje pateikiami informacinių sistemų svarbumo įvertinimai, interviu metu surinkti duomenys, svarbiausių rezultatų santrauka.

**3. Rizikų analizė, vertinimas ir saugumo valdymo priemonių parinkimas**

Šiame etape nustatomos ir įvertinamos organizacijos informacinių sistemų, jų fizinės apsaugos, saugumo valdymo sistemos grėsmės, pažeidžiamumai, rizikos, taip pat rekomenduojamos saugumo valdymo priemonės.

Priklausomai nuo organizacijos poreikių, gali būti atliekama gili tam tikrų sistemų arba viso tinklo technologinių pažeidžiamumų analizė, panaudojant metodus, analogiškus hakerių naudojamiems metodams.

**Rezultatai**

- Nustatytos, išanalizuotos ir dokumentuotos organizacijai būdingos informacijos saugumo rizikos.
- Tai leidžia atsakingai priimti sprendimą, kaip valdyti šias rizikas, pvz.: dalis šių rizikų yra priimtinos, nes apsaugos priemonių diegimas neatsipirks, kitas reikia mažinti.
- Jei nusprendžiama riziką sumažinti, yra parenkamos tinkamos saugumo valdymo priemonės. Jos gali būti techninės arba organizacinės.

**Įgyvendinimas**

- Analizuojant technines rizikas, atliekami interviu su informacinių technologijų specialistais, išmanančiais nagrinėjamas sistemas.
- Analizuojant organizacines rizikas, atliekami interviu su organizacijos atstovais, žinančiais esamas darbo tvarkas.
- Visa analizės metu surinkta medžiaga yra dokumentuojama. Dokumentavimo forma yra patogi atliekant pakartotines rizikos analizes.
- Parenkant saugumo valdymo priemones, remiamasi tarptautiniais standartais ISO/IEC 27001 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, ISO/IEC 17799:2005 „Informacijos technologija.

Informacijos saugumo valdymo praktikos kodeksas“, taip pat mūsų ekspertine patirtimi informacijos saugumo ir IT technologijų srityje.

#### 4. Saugumo valdymo priemonių diegimo plano parengimas

Rengiant parinktų saugumo valdymo priemonių diegimo planą, įvertinami šie aspektai:

- Koks yra tam tikros nagrinėjamos rizikos lygis?
- Ar yra sprendimų, kurie efektyviai mažina šią riziką? Kokios yra alternatyvos?
- Ar organizacija turi pakankamai lėšų, žmonių, žinių, laiko šių sprendimų diegimui ir priežiūrai?
- Ar yra teisinių reikalavimų, organizacijos standartų, kuriuos reikia atitikti?
- Taip pat gali būti ir kitų aplinkybių, į kurias reikia atsižvelgti, pvz., pirkimo procedūrų praktika.
- Įvertinus visas aplinkybes, parenkami optimaliausi sprendimai Jūsų organizacijai.

Rezultatai

- Parengiamas rekomenduojamas kalendorinis saugumo valdymo priemonių diegimo planas.
- Šis planas parengiamas remiantis projekto metu atlikta analize, todėl atitinkantis organizacijos poreikius, įvertinant organizacijos ypatumus, t.y. tiesiog bus tinkamas naudojimui.

Įgyvendinimas

- Bendraujant su suinteresuotais organizacijos vadovais ir specialistais bei remiantis anksčiau atliktomis analizėmis, išanalizavus visas aplinkybes, parengiamas saugumo valdymo priemonių diegimo planas.
- Esant pageidavimui, galima pristatyti projekto rezultatus ir patį planą organizacijos vadovams.

#### 5. Rizikos valdymo proceso dokumentas

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

Rezultatai

- Parengiamas dokumentas, kuriame aprašomas rizikos valdymo procesas.

Įgyvendinimas

- Rizikos valdymo procesas rengiamas atsižvelgiant į organizacijos ypatumus, esamas praktikas.

#### 6. Apie mus

UAB "Informacijos saugos sprendimai" - 2006 metais įkurta kompanija, kurios pagrindinė veikla yra konsultacijos, mokymai ir auditas, susiję su informacijos apsauga. Kompanija yra nepriklausoma ir neatstovauja nei vienam programinės ar techninės įrangos gamintojui, todėl visuomet išlieka nešališka.

Įmonėje dirba didelę patirtį turintys specialistai. Tai daug metų informacijos saugumu ir informacinėmis technologijomis besidomintys žmonės, konsultavę bei ruošę saugos politikas ir atlikę informacijos apsaugos auditus didžiosiose Lietuvos įmonėse. Kompanijos darbuotojai ne tik gerai išmano šiandien aktuales informacijos apsaugos standartus, hakerių metodus, bet turi patirties ruošiant su informacijos apsauga ir informacinių technologijų nusikaltimais susijusius įstatymus, kuriant incidentų valdymo tarnybą.

Kompanija laikosi savo etikos politikos - suteikti klientui tik aukščiausio lygio paslaugas.

Įmonė laikosi konfidencialumo principų net jei raštiškai nėra įsipareigojusi to daryti.

Kompanijai svarbu sukurti vertę, todėl ji savo darbą vertina pagal klientui suteiktą naudą.

## 7. Kontaktai

Marius Celskis

Mob. tel.: +370 685 52330

El. paštas: [marius@isec.lt](mailto:marius@isec.lt)

<http://www.isec.lt>

Audrius Lučiūnas

Mob. tel.: +370 615 20288

El. paštas: [audrius@isec.lt](mailto:audrius@isec.lt)

<http://www.isec.lt>