VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS

INFORMACINIŲ TECHNOLOGIJŲ KATEDRA

Aleksandras Spiridenkovas

INFORMACIJOS APSAUGOS STANDARTŲ PRITAIKYMAS

ADAPTATION OF INFORMATION SECURITY STANDARTS

Baigiamasis magistro darbas

Inžinerinės informatikos studijų programa, valstybinis kodas 62407T104
Duomenų gavybos technologijų specializacija
Informatikos inžinerijos mokslo kryptis

Vilnius, 2009

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS
FUNDAMENTINIŲ MOKSLŲ FAKULTETAS
INFORMACINIŲ TECHNOLOGIJŲ KATEDRA

TVIRTINU
Katedros vedėjas
_____
(Parašas)
_____
(Vardas, pavardė)
_____
(Data)

Aleksandras Spiridenkovas

INFORMACIJOS APSAUGOS STANDARTŲ PRITAIKYMAS

ADAPTATION OF INFORMATION SECURITY STANDARTS

Baigiamasis magistro darbas

Informacinių technologijų studijų programa, valstybinis kodas 62407T104
Duomenų gavybos technologijų specializacija
Informatikos inžinerijos mokslo kryptis

Vadovas_____ _____ _____
(Moksl. laipsnis, vardas, pavardė) (Parašas) (Data)

Konsultantas_____ _____ _____
(Moksl. laipsnis, vardas, pavardė) (Parašas) (Data)

Konsultantas_____ _____ _____
(Moksl. laipsnis, vardas, pavardė) (Parašas) (Data)

Vilnius, 2009

Vilniaus Gedimino technikos universitetas
Fundamentinių fakultetas
Informacinių technologijų katedra

ISBN ISSN
Egz. sk. 2
Data 09-06-12

Duomenų gavybos technologijų studijų programos baigiamasis magistro darbas
Pavadinimas **Informacijos saugumo standartų pritaikymas.**
Autorius **Aleksandras Spiridenkovas** Vadovas . habil. dr. **Genadijus Kulvietis**

Kalba

X	lietuvių
	užsienio

Anotacija

Baigiamojo darbo analitinėje dalyje nagrinėjamos informacijos apsaugos problemos ir jų sprendimo būdai, pagrindinės saugumo sąvokos ir rekomendacijos. Pateikiama aktualios grėsmes įmonėms, kokie galimi nuostoliai. Išanalizuoti ISO/IEC 17799:2005 ir CobiT 4.1 standartai.

Praktinėje darbo dalyje, naudojant ISO ir COBIT standartus, atlikta informacijos saugumo analizė. Pagrindinis šio darbo tikslas – telekomunikacinės įmonės informacijos saugumo valdymo atitikimas tarptautiniams standartams.

Darba sudaro 6 dalys: įvadas, informacijos apsaugos problemų analizė, saugumo standartai ir metodologijos, standartų pritaikymas, išvados, literatūros sąrašas.

Prasminiai žodžiai: ISO, COBIT, saugumas, konfidencialumas, rizika, kibernetiniai nusikaltimai.

Vilnius Gediminas Technical University

Fundamental Sciences faculty
Information Technologies department

ISBN ISSN
Copies No. 2
Date 09-06-12

Data mining technologies study program master thesis.
Title: **Addaptation of information security standarts**
Author **Aleksandras Spiridenkovas** Academic supervisor Prof. Dr. Habil. **Genadijus Kulvietis**

Thesis language

[X] Lithuanian

[ ] Foreign (English)

Annotation

In the analytical part of my final work we are assessing information security issues and possible solutions. We start by describing main concepts of information security and delve into current security recommendations. We describe the actual threats that current security recommendations try to address and what are the possible consequences for companies that fail to adopt security recommendations. We focus on ISO/IEC 17799:2005 and CobiT 4.1 standards.

In the practical part of my final work we study a particular security policy designed using ISO and COBIT standards. The security policy under consideration was designed for use in an actual telecommunications company and our goal is to quantify the compliance of such policy to international standards.

The work consists of six parts: introduction, analysis of information security issues, security standards and methodologies, application of security standards, conclusion, and related work section.

Keywords: ISO, CobiT, security, cyber crime, risk, confidentiality

Paveikslėlių sąrašas

Lentelių sąrašas

Turinys

1. Įvadas

Temos aktualumas. Kiekviena organizacija norėdama būti pirmaujančia rinkoje turi įrodyti, kad yra patikima ir stipri. Šiuolaikiniame pasaulyje yra sunku pelnyti klientų pasitikėjimą, o galiausiai jį išlaikyti. Kad organizacija būtų patikima, ji turi užtikrinti savo ir klientų informacijos saugumą. Svarbu suprasti, kas yra informacijos saugumas ir kokios galimos rizikos, nes informacinių sistemų saugumas yra vienas iš aktualiausių ir svarbiausių klausimų, kurį turi išspręsti šiuolaikinė informacinių technologijų įmonė. Kompetentingi duomenų ir technikos saugumo sprendimai garantuoja verslo stabilumą, padeda išvengti nuostolių ir suteikia naujų veiklos galimybių. Klaidingai manoma, kad norint išspręsti saugumo problemas, užtenka tik techninių priemonių. Planuodama tobulinti saugą bendrovė turi atidžiai įvertinti savo informacinių sistemų pažeidžiamumą, grėsmes ir riziką, kylančią jos turimai informacijai ir kompiuterinėms sistemoms, paruošti atitinkamas procedūras, skirtas informacijos valdymui. Tai yra labai aktualu, nes kritiniu atveju, jei kažkas atsitiktų, galimi dideli nuostoliai ar net bankrotas.

Mokslinis naujumas. Šiuo metu egzistuoja daugybė įvairių standartų, dauguma jų yra bendriniai, o įmonės kurioms jie taikomi - specifinės, todėl atsiranda nemažai problemų, išsirenkant reikiamą standartą specifinei įmonei ir jį pritaikant. Atsiranda poreikis vertinimo metrikų atsiradimui.

Šiame darbe aptariami populiariausi saugumo standartai, išskiriami du priimtiniausi ir aktualiausi telekomunikacinėms įmonėms, taip pat sukurtos metrikos, kurių pagalba įvertinama saugumo standartų atitiktis, pasirinktos vertinimui įmonės saugumo reikalavimams. Atliekama ne tik įmonės atitikties saugumo standartams analizė, bet ir ISO standarto atitikties įmonės saugumo poreikiams analizė.

Praktinė nauda. Gauti rezultatai bus panaudoti įmonės veikloje.

Tyrimo tikslas. Darbo tikslas – tarptautinių informacijos saugumo standartų pritaikymo įvertinimas įmonėje. Darbo analizei pasirinkta viena didžiausių telekomunikacijos įmonių Lietuvoje.

Uždaviniai. Tikslui pasiekti buvo iškelti ir atlikti šie uždaviniai:

- Pateikti tarptautinių informacijos saugumo ISO ir COBIT standartų analizę.
- Atlikti informacijos apsaugos pagrindinių problemų analizę.
- Atlikti ISO ir COBIT standartų panašumų ir skirtumų analizę.

Darbo struktūra. Darbas susidedaiš penkių dalių. Įžangos, trijų dėstymo dalių (*antroji*, *trečioji ir ketvirtoji*) ir išvadų. Kiekviena dalis suskirstyta į skyrius, pagal nagrinėjamų klausimų pobūdį.

Antroji darbo dalis. Antrojoje darbo dalyje aptariamos informacijos apsaugos problemos, saugos aktualumas. Pateikiama išsami grėsmių prigimtis ir kokios galimos ateities rizikos. Įvardinami pagrindiniai saugumo kriterijai ir metodai, kuriais remiantis sumažinama grėsmė. Pagrindinis dėmesys skiriamas pagrindinių saugumo kriterijų užtikrinimui skirtų metodų analizei.

Trečiojis darbo dalis. Trečiojoje darbo dalyje pateikiami pagrindiniai saugumo standartai, išskiriami du aktualiausi telekomunikacijnių įmonių saugumui, atliekama jų analizė.

Ketvirtoji darbo dalis. Ketvirtojoje dalyje pagrindinis dėmesys skiriamas saugumo standartų ISO 17799:2005 ir CobiT 4.1 atitikties pasirinktai įmonei analizei. Analizei atlikti buvo kuriamos anketos pagal TARPTAUTINIS STANDARTAS ISO/IEC 17799 ir COBIT 4.1 leidinio metodologiją. Anketos buvo kuriamos kiekvienam standartų skyriui. Anketos buvo išsiųstos atitinkamų skyrių darbuotojams. Pagal gautus atsakymus į anketas buvo sudaroma atitikčių lentelė. Taip pat sudaryta lentelė, kurioje pateikiama ISO standarto atitikitis įmonės tinklo ir technologijų saugumo reikalavimams. Ketvirtos darbo dalies pabaigoje pateikiamos atitikties išvados..

Aprobacija. Informacijos apsaugos standartų pritaikymo tematika yra parašytas mokslinis straipsnis „Informacijos saugumo standartų pritakymas“, kuris buvo pristatytas jaunųjų mokslininkų konferencijoje „Informacinės technologijos“ 2009 m. balandžio 9 dieną. Darbo rezultatai pristatyti įmonės veiklos saugumo ir operacijų tęstinumo komiteto posėdžio metu.

2. Informacijos apsaugos problemų analizė

2.1. Įvadas

Visame pasaulyje yra skiriamas didelis dėmesys informacijos konfidencialumui ir saugumui. Informacinės technologijos ir telekomunikacijos nuolat traukia naujas investicijas, o tai lemia šios srities pelningumą. Todėl techninė įranga, sistemos nuolat plėtojamos ir tobulinamos, taikomi patys naujausi technologiniai elektronikos bei informatikos laimėjimai. Įmonių IT infrastruktūros darosi vis sudėtingesnes, reikalaujančios nemažai resursų jų priežiūrai, taipogi keliami didesni reikalavimai saugumui, kadangi kompiuterizuojant daugelį veiklos procesų atsiranda daugiau grėsmių ir informacijos vientisumui, bei saugumui, tačiau ne tik skaitmeninė informacija turi būti apsaugota, daugelis organizacijų paslapčių ar vidiniam naudojimui skirtų dokumentų saugomi popieriniu pavidalu ir ne ką mažiau turi būti apsaugoti. Prieš bandant išsiaiškinti, kaip galima efektyviai užtikrinti informacijos saugumą, reikėtų suprasti, kas yra informacijos apsauga ir kodėl ji reikalinga, kokios yra ir iš kur atsiranda informacijos grėsmės ir į ką reikia atsižvelgti norint jas sumažinti. Darbe aptariamos saugumo problemos ir rekomendacijos yra aktualios visoms organizacijoms, kurios pasiryžusios užtikrinti informacijos apsaugą, vienoms turėtų būti taikomos griežčiau kitoms atlaidžiau, priklausomai nuo organizacijos pobūdžio. Pavyzdžiui, kai kurie industrijos sektoriai turi politikas, procedūras, standartus ir direktyvas, kurių reikia laikytis – mokėjimo kortelių industrija (MKI), duomenų saugumo standartai. Visa ir MasterCard vienas iš tokių pavyzdžių.[3]

2.2. Informacijos apsaugos pagrindiniai kriterijai

Informacijos apsauga reiškia informacijos ir informacinių sistemų apsaugą nuo neleistino pasiekimo, panaudojimo, atskleidimo, sugadinimo ar pradanginimo. Informacijos apsauga, kompiuterių apsauga ir informacijos patikimumas tai neatsiejamos sritys, jas sieja tie patys tikslai, konfidencialumo užtikrinimas, vientisumas ir informacijos naudingumas, tačiau tarp jų yra tam tikrų neryškių skirtumų. Šie skirtumas atsiranda dėl skirtingos metodologijos naudojimo ir srities, į kurią gilinamasi. Informacijos apsauga susijusi su konfidencialumu, vientisumu ir duomenų prieinamumu nepriklausomai nuo jų formos: elektroninės, spausdintinės ar kitos. Įvairios institucijos ir organizacijos sukaupia didelius kiekius konfidencialios informacijos apie savo darbuotojus, klientus, produktus, tyrimus ir finansinį statusą. Daugiausia šios informacijos renkama, apdorojama ir saugoma kompiuteriuose elektroniniu formatu ir perduodama kitiems tinklo kompiuteriams. Informacijos saugumo spragos, tokios kaip galimybė, kad konfidenciali informacija apie verslo klientus ar finansus ar naują produktų liniją pateks į konkurentų rankas, gali lemti verslo praradimą, teisines pasekmes ar net bankrotą. Saugoti konfidencialią informaciją – verslo, ir daugeliu atvejų, etiniai ir teisiniai reikalavimai. Fiziniam asmeniui informacijos saugumas irgi yra svarbus norint užsitikrinti privatumą.

Jau daugelį metų laikoma, kad konfidencialumas, vientisumas ir prieinamumas žinomi kaip KVP triada (*angl. CIA triad*) yra pagrindiniai informacijos apsaugos principai.[4]

Konfidencialumas - tai teisė neleisti informacijos atskleidimo neleistiniems asmenims arba sistemoms ir garantija, kad niekas be informacijos savininko ar valdytojo žinios jos nepanaudos.[4] Faktiškai neįmanoma gauti vairuotojo pažymėjimo, išsinuomoti būsto, gauti medicininę pagalbą ar paimti paskolą neatskleidžiant asmeninių duomenų, tokių kaip vardas, adresas, telefono numeris, gimimo data, socialinio draudimo pažymėjimo numeris, šeimyninė padėtis, pajamos, darbovietė, medicinos kortelės duomenys ir pan. Visa tai labai asmeninė ir privati informacija, kurią dažnai reikia pateikti tvarkant verslo reikalus. Mes paprastai tikimės, kad asmuo, verslo įmonė ar organizacija, kuriai atskleidžiame tokią asmeninę informaciją imasi priemonių, kad užtikrintų tokių duomenų saugumą nuo neleistino tiek tyčinio, tiek netyčinio jų atskleidimo, ir kad tokia informacija bus dalinamasi tik su tomis įmonėmis ar institucijomis, kurios turi teisę prie jos prieiti ir joms tikrai to reikia. Konfidenciali informacija turi būti pasiekiama, naudojama, kopijuojama ar atskleidžiama asmenų, kurie turi teisę tai daryti ir tik tada, kai yra pagrįstas poreikis ir duotas informacijos savininko sutikimas. Konfidencialumas yra būtinas (bet nepakankamas) išsaugant privatumą žmonių, kurių duomenis turi organizacija.

Vientisumas informacijos apsaugoje reiškia tai, kad duomenys negali būti sukurti, pakeisti ar ištrinti be įgaliojimo (tai ne tas pats, kas referentinis vientisumas duomenų bazėje).[4] Tai taip pat reiškia tai, kad vienoje duomenų bazės sistemos dalyje saugomi duomenys sutampa su kitais susijusiais duomenimis, saugomais kitoje duomenų bazės sistemos vietoje (ar kitoje sistemoje). Vientisumo praradimas atsiranda kai asmuo turintis prieigas prie informacijos netyčia ar turėdamas piktų kėslų, ištrina svarbias duomenų bylas, ar kai į kompiuterį patenka virusas. Taipogi vientisumo praradimas gali atsirasti ir dėl sisteminių klaidų.

Prieinamumo sąvoka reiškia, kad informacija, jos apdorojimui naudojama kompiuterinė sistema ir apsaugos priemonės yra prieinami ir veikia korektiškai.[4] Aukšto prieinamumo sistemos turi būti prieinamos bet kuriuo metu, apsaugotos nuo paslaugų žlugimo dėl prastovos, techninės įrangos klaidų bei sistemos pakilimų. Prieinamumo užtikrinimas taip pat apima apsaugą nuo paslaugų paneigimo atakų.

2002 m. buvo pasiūlyta alternatyva klasikinei KVP triadai, kurią pateikė P. Donnas Parkeris.

Jo alternatyvus modelis apėmė konfidencialumą, valdymą arba kontrolę, vientisumą, autentiškumą, prieinamumą ir naudingumą ir vadinamas šešiais atominiais informacijos elementais.

Autentiškumas - naudojantis kompiuteriu elektroniniam verslui ir informacijos saugumui būtina užtikrinti, kad duomenys, komunikacijos ar dokumentai (elektroniniai ar fiziniai) būtų tikri (pvz., nebuvo suklastoti ar išgalvoti).

Neatsisakymas - teisėje neatsisakymas įgalina atlikti sutarties prievoles. Tai taip pat reiškia, kad viena sandorio šalis negali neigti, kad gavo sandorį, o kita šalis negali paneigti, kad jį siuntė. Elektroninėje

komercijoje, norint nustatyti autentiškumą ir neatsisakymą, naudojamos tokios technologijos kaip skaitmeninis parašas ir kodavimas.[4]

2.3 Grėsmių informacijos saugumui prigimtis

Informacija – kiekvienos šiuolaikinės kompanijos pagrindas. Jos prieinamumas, vientisumas ir konfidencialumas svarbiausi 21 amžiaus kompanijų ilgalaikiam gyvavimui. Jei kompanija nesiima visapusiškos ir nuoseklios informacijos prieinamumo, vientisumo ir konfidencialumo politikos, ji yra neapsaugota nuo įvairių grėsmių. Tai gresia interneto kompanijoms, internetinei prekybai, įvairias technologijas naudojančioms kompanijoms arba kompanijoms, turinčios slaptos ar konfidencialios informacijos, visoms organizacijoms, visose ekonomikos srityse, tiek privačiose, tiek ir viešose. Gresiantis pavojus ir strateginė atsakomybė turi užtikrinti, kad visos organizacijos tinkamai saugotų savo informacijos bazes. 75 procentai Didžiosios Britanijos vadybininkų mano, kad informacijos saugumui turi būt teikiama pirmenybė. Šiandien jau imamasi konkrečių veiksmų. Vidutinė Didžiosios Britanijos kompanija 4-5 procentus informacinių technologijų biudžeto skiria informacijos apsaugai, panašus skaičius ir didesnių Lietuvos kompanijų. Tačiau dauguma apklausoje dalyvavusiu saugumo specialistu mano, kad išlaidos informacijos saugumui atitinka tik 77% organizacijos veiklos poreikius. Beveik visos naudojasi užsienio patirtimi ir išvadomis, kad padidintų savo saugumą.

Išaugusios investicijos stabilizuoja padėtį. Nors sumažėjo kompanijų, patiriančių informacijos nutekėjimą, tokių atvejų skaičius vienai kompanijai ženkliai padidėjo. Šitokia padėtis rodo, kad organizacijoms atsirado gyvybiškai svarbi būtinybė taikyti geriausią tarptautinę informacijos saugumo patirtį. Padėtis prastėja kiekvienais metais. Atsitiktiniai, ne trečiųjų šalių, išprovokuoti išpuoliai prieš organizacijų informacines sistemas yra tokie pat pavojingi, kaip ir tyčiniai veiksmai. Vidinės grėsmės yra taip pat rimtos. Galima numatyti, koks išpuolis, kada ir kaip gali būti įvykdytas, tačiau greitis, kuriuo vystosi išpuolių metodai, sumenkina veiksmus, kurių imamasi prieš specifines, identifikuotas grėsmes. Tik nuoseklus ir sisteminis požiūris į šitą problemą gali garantuoti tokį informacijos apsaugos lygį, kuris reikalingas kiekvienai kompanijai. Reikia suvokti, kaip rizikuoja organizacija, neturinti šiuolaikinės informacijos apsaugos sistemos. Rizikos gali būt trijų tipų:

- Proceso sutrikdymas.
- Žala reputacijai.
- Teisinė žala.

Visų trijų kategorijų žala gali būti matuojama poveikiu organizacijos trumpalaikių ir ilgalaikių siekių įgyvendinimui. Kol kas nėra vieningos, nuoseklios, pasaulinės informacijos rizikos ir grėsmių studijos, kuria remtųsi visos šalys. Turime daugybę įvairių apžvalgų, ataskaitų ir tyrinėjimų, atliktų įvairiose valstybėse, dažnai turint šiek tiek skirtingų tikslų, kurie atskleidžia informacijos saugumo rizikos ir

grėsmių prigimtį, mastą, kompleksiškumą ir reikšmę. O taip pat ir organizacijų pažeidžiamumą dėl savo paties neapdairumo ar savo sistemų pažeidžiamumo. [3]

Grėsmių informacijos saugumui paplitimas

DB Prekybos ir ekonomikos departamento atlikta aštuntoji metinė „Saugumo spragų apžvalga“(ISBS 2006), vadovaujant „PricewaterhouseCoopers“, apžvelgė informacijos saugumo būklę įvairiose Jungtinės Karalystės organizacijose. Iš visų organizacijų 58 procentai pripažino, turintys labai konfidencialios informacijos. Tarp stambesnių organizacijų šitas skaičius pakilo iki 77 procentų ir daugiau. Iš tikrųjų, jei smulkesnės organizacijos geriau suprastų savo turimos informacijos vertę, pastarasis skaičius, ko gero, būtų atspindėtas visose grupėse. Šitą apžvalgą galima rasti adresu www.security-survei.gov.uk/ .

Jos svarbiausi punktai:

- 97 procentai Jungtinės Karalystės verslų turi internetinį ryšį.
- 80 procentų savo kompiuteriuose laiko labai svarbių ir konfidencialių įrašų.
- 74 procentai patirtų žymių nuostolių, jei šita informacija būtų sugadinta ar nutekinta.

Internetinės šiukšlės tampa nuolat didėjančia problema (ko gero, dabar jos sudaro 80 procentų visų elektroninių laiškų).

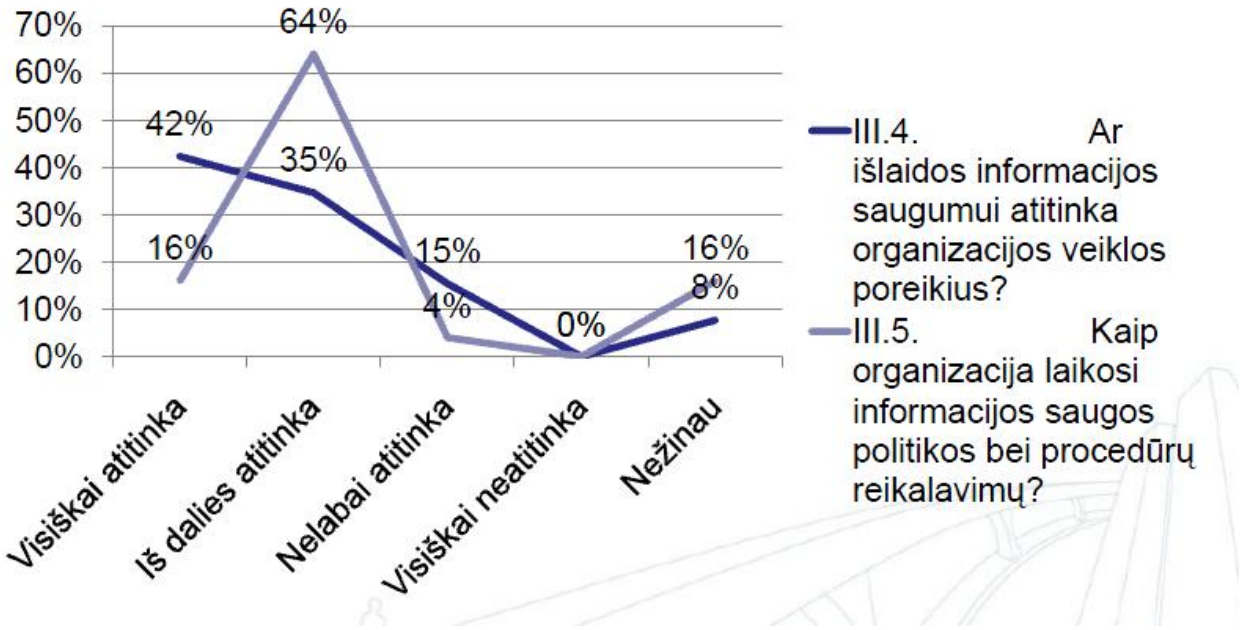
Tik ketvirtadalis visų Jungtinės Karalystės verslų pastaraisiais metais tikrino savo gelbėjimo planus, norėdami įsitikinti, ar jie pasitvirtins praktikoje.

62 procentai Jungtinės Karalystės kompanijų pastaraisiais metais turėjo incidentų dėl saugumo.

Vidutiniškai per metus patiriami aštuoni tokie incidentai. Didesnėse kompanijose - net devyniolika per metus. Saugumo spragos jau dabar Jungtinės Karalystės pramonei kainuoja 10 milijardų svarų per metus. Per dvejus pastaruosius metus šita suma išaugo 50 procentų.

Organizacijos vis pesimistiškiau vertina ateities informacijos saugumą, manydamos, kad incidentų vis daugės ir juos bus sunkiau aptikti. Naujosios technologijos kelia ypatingą grėsmę informacijos saugumui. ISBS 2006 sako, kad Jungtinės Karalystės kompanijos nekuria kovos su į technologijas orientuotų informacijos vagių strategijos. Daroma išvada, kad be integruoto, rizikos mastais pagrįsto požiūrio į informacijos saugumą, turint omeny vis naujesnes technologijas, Jungtinės Karalystės kompanijos bus vis mažiau apsaugotos. Įsilaužėliai (hakeriai, krakeriai), virusų kūrėjai, brukalų siuntėjai (*angl. spamers*), apgavikai ir visi kiti kibernetiniai nusikaltėliai vis tobuliau išnaudoja informacijos saugumo spragas. Jie buriasi į grupes, kad galėtų vykdyti integruotas atakas prieš verslą visame pasaulyje. Štai kodėl didėja efektyvios apsaugos būtinybė. Tačiau kol kas neužtektinai suprantama ir įsisąmoninama, ką galima padaryti, kad būtų pasipriešinta svarbiausioms grėsmėms, ypatingai toms, kurias sukelia žmogaus veiksmai, ir toms, kurių kyla, verčiantis elektroniniais verslais. Tik viena kompanija iš aštuonių turi kvalifikuotų informacijos apsaugos darbuotojų ir tik viena iš aštuonių moko savo darbuotojus atsakingai saugoti informaciją. Dažnai, bet ne visada, informacijos saugumas yra laikomas informacinių technologijų skyriaus reikalu, nors aišku, kad taip nėra. Tinkamas informacijos saugumo valdymas

reiškia, kad organizacija supranta riziką ir grėsmes, su kuriomis susiduria jų kompiuterinis procesas, ir jo pažeidžiamumą. Tai reiškia, kad vykdomos tam tikros procedūros, įgalinančios sumažinti riziką, darbuotojams aiškinama jų atsakomybė. Svarbiausia – užtikrinti, kad informacijos saugumo valdymo politika – vyresniojo personalo pareiga. Tik tada, kai bus atkreiptas dėmesys į šitas procedūrines ir valdymo problemas, organizacija gali spręsti, kokių saugumo technologijų jai reikia. Apytikriais duomenimis, dvi penktosios kompanijų iki šiol informacijos saugumui skiria mažiau negu vieną procentą informacinėms technologijoms skirto biudžeto. Vidutinė kompanija skiria 4-5 procentus, nors išlaidos saugumui turėtų būti artimesnės 10 procentų. Kol į informacijos saugumą nebus žiūrima rimtai, padėtis gali tik blogėti. [3]



1 pav. Išlaidų informacijos saugumui atitikimas organizacijos veiklai – apklausa (atlikta UAB BlueBridge)

Grėsmių informacijos saugumui poveikis

Didžiojo penketuko konsultacinės kompanijos „KPMG“ 2000 – ųjų metų informacijos saugumo apžvalga, nurodanti atspirties tašką, nuo kurio reikėtų žvelgti į šiuolaikinės informacijos saugumo būklę, padarė išvadą, kad informacijos saugumo spragų daugėja. Virusų atvejų padaugėjo nuo 20 procentų iki 73, vagysčių – nuo 23 iki 46, įsilaužimų į elektroninį paštą – nuo 2 procentų iki 29 procentų. 78 procentai apklaustųjų nurodė nepakankamą saugumą, kaip pagrindinę internetinės prekybos atsisakymo priežastį. 55 procentuose organizacijų informacijos saugumas buvo paliktas informacinių technologijų skyrių žiniai, ir kompanijų vadovybė, greičiausiai, negalėjo užtikrinti, kad būtų imamasi reikiamų priemonių.

2001 Jungtinės Karalystės Prekybos ir pramonės departamento atlikta studija nurodo, kad informacijos saugumo spragos atsiėjo nuo 5,7 procentų iki 7 procentų metinių 2000 –ųjų metų pajamų. Teigiama, kad tais metais vien Europos verslas prarado per 4,3 milijardų svarų dėl su internetu susijusių nusikaltimų.

Padėtis tik blogėja. Jungtinės Karalystės Nacionalinis aukštųjų technologijų nusikaltimų padalinys, jau įtrauktas į Organizuoto nusikalstamumo agentūrą, 2005 metų ataskaitoje pažymėjo:

1. 2005 metais 89 procentai Jungtinės Karalystės kompanijų patyrė vieną ir daugiau incidentų, susijusių su kompiuteriniais nusikaltimais.

2. Šitų nusikaltimų padaryta žala siekė 2,5 milijardus svarų.[3]

Kompanija „Ernst and Young“ jau nuo 1993 metų kiekvienais metais spausdina informacijos saugumo apžvalgą. 2004 metų apžvalga leido padaryti porą išvadų:

Nuo pirmos mūsų išleistos apžvalgos 1993 metais, kompanija „Ernst ant Young“ išstudijavo įvairių informacijos saugumo priemonių, taikomų pasaulinių organizacijų, svarbą. Ironiška, bet šių metų apžvalga tarsi atkartoja ankstesnių metų apžvalgas, nes kompanijos mieliau pasikliauja sėkme, negu informacijos apsaugos priemonėmis. Nuostabu, kaip mažai pasikeitė požiūris, praktika ir veiksmai nuo 1993 metų, nors grėsmės ir rizika padidėjo labai ženkliai. Du faktoriai leidžia manyti, kad reikalai pablogėjo.

Pirmas: grėsmės turi daug skaudesnių pasekmių, negu 1993 metais. Kompanijos menkai suvokia, kad tai, ko jos nežino, kenkia joms pačioms. Kol panikieriai kausto visuomenės dėmesį ties išoriniais pavojais, abejotinai skaičiuodami žalą, organizacijos susiduria su didesne žala, daroma viduje, neteisingai elgiantis, dėl apsileidimo, neapsižiūrėjimo arba organizacinių klaidų, kurios pažeidžia egzistavusias prieš tai politikas ir procedūras.

Antras: pastebimos nedidelės permainos saugumo srityje. 1994 respondentas mums pasakė: „Kol šita kompanija imsis priemonių, ko gero, turės būt padaryta didelė žala dėl aplaidžios apsaugos sistemos.“ Po dešimties metų šitas sakinys tebėra akivaizdus ir charakterizuoja organizacijų nenorą imtis priemonių, kad būtų imtasi visiem priimtinų kontrolės būdų ir kad nebūtų padaryta didelė žala.

UAB „BlueBridge“ atliktos apklausos, kurioje dalyvavo, didžiausių Lietuvos įmonių, saugumo specialistai, rezultatai rodo, kad didžiausią procentą žalos sudaro incidentai sukelti tinklo įrangos gedimais 62%, esami darbuotojai 54%, hakeriai 46% procentus.

Kibernetiniai nusikaltimai

Žurnalas „Informacijos saugumas“ apklausė 2545 informacijos saugumo priemonių vartotojų internetu, įtraukdami tiek valstybines, tiek privačias organizacijas Šiaurės Amerikoje, Europoje ir Tolimuosiuose Rytuose. Nors šitas tyrimas vyko 2001 metų lieps ir rugpjūčio mėnesiais, jo metu gauti duomenys tebėra aktualūs ir svarbūs šiandien.

Virusai, kirminai, Trojos arkliai ir kiti „blogiukai“ padarė žalos 90 procentų organizacijų, nors jų 80 procentų turėjo antivirusines programas.

Nuo 2000 iki 2001 metų organizacijų, kurios buvo puolamos per žiniatinklio serverius, padvigubėjo. Vidaus saugumo incidentų pasitaikydavo dažniau, negu išorės, tačiau saugumo specialistai labiau rūpinosi apsaugoti išorinį organizacijos perimetrą, negu imtis priemonių viduje.

Vidiniai saugumo incidentai: neleistinų programų įdiegimas (78 procentai tyrime dalyvavusių organizacijų), kompanijos kompiuterinių išteklių naudojimas nelegaliai ar nusikalstamai veiklai (naršymas po porno svetaines arba persekiojimas elektroniniu būdu), kompanijos kompiuterinių išteklių naudojimas, siekiant asmeninės naudos (lošimas, „šiukšlinimas“, asmeninė internetinė prekyba) ir taip toliau. Iš tiesų, daugelis šitų informacijos saugumo incidentų yra nusikaltimai. Jungtinės Karalystės piktnaudžiavimo kompiuteriais aktas 1990 (netaisytas) buvo pripažinęs priėjimą prie kompiuterio, kompiuterio turinio keitimą be leidimo arba šios veiklos leidimą nusikaltimu. Už šitokius veiksmus buvo numatytos sankcijos, įskaitant baudas ir laisvės atėmimą. Kitos šalys irgi ėmėsi panašių veiksmų pripažinti tai nusižengimu, už kurį įstatymo vykdymą garantuojančios institucijos turi bausti. Vis dažniau šitokia neteisėta veikla vadinama kibernetiniais nusikaltimais. Europos kibernetinių nusikaltimų konvencija, pirmasis daugiašalis susitarimas, turintis atkreipti dėmesį į problemas, kylančias dėl besiplečiančios nusikalstamos veiklos kompiuteriniuose tinkluose, buvo pasirašytas 2001 metų lapkričio mėnesį. Jungtinės Valstijos galiausiai ratifikavo šitą konvenciją 2006 metais ir nuo 2007 sausio 1 dienos pradėjo ją vykdyti. Kibernetinių nusikaltimų konvencija buvo sukurta tam, kad apsaugotų piliečius nuo kompiuterinių įsilaužėlių ir internetinių apgavikų, kad internetiniai įrodymai, įskaitant vaikų seksualinį išnaudojimą, organizuotą nusikalstamumą ir terorizmą, būtų pripažinti teismuose. Kuriami įstatymai, padėsiantys kovoti su kibernetiniais nusikaltimais. Interpolas, Europos policijos agentūra, pastebėjo: „Visuomenei tampant vis labiau priklausoma nuo technologijų, organizuotas nusikalstamumas suranda vis naujų galimybių nusikalsti ir išnaudoti žmonijos silpnybes, užpuolant neužtektinai apsaugotas informacines sistemas.“ Taip ir atsitinka. Kibernusikaltimai yra tokie pat dažni, kaip ir tradiciniai. 2006 metais finansinių sukčiavimų atvejų internete padvigubėjo. Kompiuterių saugumo institutas (CSI) drauge su San Francisko federalinių tyrimų biuro Kompiuterinių nusikaltimų būrio specialistais atliko 11 metinių informacijos saugumo patikrinimų tose kompanijose, kurios yra CSI narės. Galima daryt išvadą, kad kompanijų – narių informacijos saugumo suvokimas ir priemonės, kurių imamasi, yra aukštesni lygio, negu eilinės kompanijos. Tačiau patikrinimo metu nustatyta, kad ir tarp kompanijų – narių auga nenoras pranešti valdžiai apie kinernusikaltimus, nes neišvengiamai plinta neigiama viešoji nuomonė. 2006 metų ataskaita nurodo, kad vidutinė metinė pripažinta žala sudarė 168.000 dolerių. Pagrindinės keturios finansinių nuostolių priežastys buvo virusų atakos, neleistinas priėjimas prie tinklų, pamesti arba pavogti nešiojamieji kompiuteriai arba mobili įranga ir konfidencialios informacijos vagystės.[3] Aišku viena, kad pusė dalyvavusiųjų tyrime negalėjo, nes neturėjo būdų susekti, arba nenorėjo, nes gali nukentėti reputacija, pateikti patirtų finansinių nuostolių skaičiais. Galima drąsiai teigti, kad kibernusikaltėliai lygiomis dalimis puolė kompiuterines sistemas tiek iš išorės, tiek iš vidaus.

Ateities rizikos

Yra daugybė tendencijų, kurios slypi už nuolat didėjančios grėsmės kompiuterizuotos informacijos saugumui. Turint tai omeny galima teigti, kad padėtis tik blogės ir jokiu būdu ne gerės.

1. Kompiuteriais naudojasi vis didesnė visuomenės dalis. Nuo centralizuotų informacijos centrų pereinama prie nešiojamų, mikro kompiuterių, dėl to tampa vis sunkiau apsaugoti informaciją.
2. Plinta mobiliųjų kompiuterių naudojimas. Nešiojamų kompiuterių, PDA, mobiliųjų telefonų, skaitmeninių kamerų, nešiojamų projektorių, MP3 grotuvų naudojimas leidžia dirbti namie arba keliaujant. Tai vėl gi silpnina informacijos duomenų apsaugą. Tai reiškia, kad dramatiškai išaugo nuotolinio priėjimo prie tinklų ir lengvai prieinamų prietaisų naudojimas. Tuo pačiu padidėjo galimybė įsilaužti į tinklus, vogti arba naikinti informaciją.
3. Internetas tapo pagrindine verslo bendravimo priemone. Bevielių, VoIP, broadband technologijų spartus vystymasis žada dar didesnių permainų. Internetas – efektyvus, spartus ir galingas būdas bendrauti įvairiomis temomis.
4. Neišvengiamai daugėja „susimaišiusių“ grėsmių, kurias galima nugalėti tik suderinus veiksmus ir technologijas.
5. Nuolat tobulėjančios technologijų apsaugos sistemos, ypatingai naudotojo atpažinimo ir įgaliojimų suteikimo, paspartins ir hakerių tobulėjimą.
6. Kompiuterinis raštingumas sparčiai plinta. Jei šiandien daugelis žmonių moka naudotis kompiuteriais, tai ateinančioms kartoms jie bus savaime suprantamu dalyku visose gyvenimo srityse. Dėl to kils dar daugiau grėsmių informacijos saugumui. Instant messaging – naujos technologijos pavyzdys. Jis tobulesnis ir greitesnis už elektroninį paštą, tačiau yra labiau pažeidžiamas. Ateityje mes sulauksime ir daugiau šitokių technologijų.
7. Bevielės technologijos informaciją ir internetą padaro prieinamus pigiau ir lengviau beveik iš bet kurio žemės taško. Tuo pačiu menksta suvokiama informacijos vertė ir svarba. Konfidenciali informacija tampa lengviau pažeidžiama ir prieinama.
8. Dėl krintančių kompiuterių kainų jie tampa prieinami visiems. Šiandien daugelis kompiuteriais besinaudojančių žmonių gali kelti grėsmę, jeigu tik jie sugalvotų pasinaudoti aukščiau išvardintomis galimybėmis.[3]

Statistika verčia susimąstyti ir sunerimti. Grėsmės akivaizdžios. Jokia kompanija ar organizacija neturėtų ignoruoti informacijos saugumo. Faktas, kad šitie pavojai taip plačiai paplitę, o grėsmės šaltiniai tokie įvairūs, akivaizdžiai įrodo, jog neužtenka paprasčiausios antivisurinės programos. Vienintelė išeitis – protingai ir nuodugniai įvertinti riziką, kuri gresia kompanijai, ir priimti protingą bei sisteminį požiūrį į informacijos saugumą, kad būtų užkirsti keliai kibernusikaltimamas.

2.4 Rizikos valdymas

Šiais laikais rizikos valdymas nuo informacijos apsaugos neatsiejamas ir labai svarbus procesas. Sunku įsivaizduoti efektyvu saugumo užtikrinimą be rizikų valdymo.

„Rizikos valdymas – tai pažeidžiamumų ir grėsmių informacijos resursams identifikavimo procesas naudojamas organizacijos siekiant verslo tikslų bei sprendimas, nurodantis, kokių atsakomųjų priemonių reikia imtis, kad būtų sumažinta rizika iki priimtino lygio, priklausomai nuo to, kokią reikšmę organizacijai turi informacijos resursai“ (CISA apžvalgos vadovas 2006 (angl. CISA Review Manual)) .

Norint geriau suprasti šį apibrėžimą būtina suprasti du dalykus.

Pirma – rizikos valdymo procesas turi būti vykdomas nuolatos. Tai turi būti kartojama neribotai sutartu periodiškumu, kadangi verslo aplinka yra pastoviai kintanti, todėl nuolat atsiranda naujų grėsmių ir pažeidžiamumų.

Antra – rizikos valdymui skirtų atsakomųjų priemonių pasirinkimas turi būti suderintas atsižvelgiant į verslo poreikius ir jų efektyvumą.[2]

Plačiąja prasme rizikos vertinimo procesas susideda iš:

- Turto identifikavimo ir jo vertės apskaičiavimo. Į tai įeina: žmonės, pastatai, techninė įranga, programinė įranga, duomenys (elektroniniai, spausdinti, kt.), atsargos;
- Grėsmių įvertinimo. Į tai įeina: gamtos poveikis, karo veiksmai, piktybiniai veiksmai nukreipti į organizacijos vidų arba iš išorės;
- Pažeidžiamumų vertinimo. Taip pat reikia įvertinti galimybę pasinaudoti kiekvienu pažeidžiamumu. Įvertinti politiką, procedūras, standartus, mokymus, fizinę apsaugą, kokybės kontrolę, techninį saugumą;
- Apskaičiuoti galimą kiekvienos grėsmės poveikį bet kuriam turtui. Naudoti kiekybinę arba kokybinę analizę;
- Identifikuoti, parinkti ir įdiegti atitinkamą kontrolę. Atitinkamai atsakyti. Apsvarstyti produktyvumą, kainų efektyvumą ir turto vertę;
- Įvertinti kontrolės priemonių efektyvumą. Užtikrinti, kad kontrolė teiktų reikalaujamą kainos ir kokybės santykį atitinkančią apsaugą neprarandant produktyvumo.

Kiekvienai rizikos vertinimo metu nustatytai rizikai reikia taikyti tam tikrą rizikos priežiūros sprendimą. Galimi tokie rizikos priežiūros būdai:

- tinkamų valdymo priemonių taikymas, siekiant sumažinti riziką;
- sąmoningas ir objektyvus rizikos prisiėmimas, užtikrinant, jog ji aiškiai atitinka organizacijų politiką ir rizikos prisiėmimo kriterijus;
- rizikos išvengimas, užkertant kelią veiksmams, dėl kurių galėtų kilti rizika;

- galimos rizikos perdavimas kitoms šalims, pavyzdžiui, draudikams ar tiekėjams.[4]

Sprendimas sušvelninti riziką, gali būti diegiamas nuo vieno iki trijų kontrolės būdų. Administracinės kontrolės priemonės (taip pat vadinamos procedūrinėmis) susideda iš patvirtintos rašytinės politikos, procedūrų, standartų ir direktyvų.

Administracinės kontrolės formuoja sistemą verslui ir valdomiems žmonėms. Tai informuoja žmones apie tai, kaip turi vykti verslas ir kaip turi būti vykdomos kasdienės operacijos. Valdžios organų sukurtos teisinės ir reguliavimo priemonės taip pat yra administracinės kontrolės tipai, nes jos informuoja verslą. Pavyzdžiui korporatyvinė saugumo politika, slaptažodžių politika, darbuotojų samdymo politika ir disciplinarinė politika. Administracinė kontrolė formuoja pagrindą parinkti ir įdiegti loginę ir fizinę kontrolę.

Loginė ir fizinė kontrolės yra administracinės kontrolės pasireiškimas. Administracinė kontrolė yra laikoma pirmaeilės svarbos priemone.

Loginė kontrolė (dar vadinama technine) naudoja programinę įrangą ir duomenis prieigai prie informacijos ir kompiuterinių sistemų kontroliuoti. Pavyzdžiui: slaptažodžiai, ugniasienės, įsibrovimų į tinklą aptikimo sistema, prieigos kontrolės sąrašai ir pasikėsinimas į duomenis yra loginės kontrolės dalykai. Loginė kontrolė yra diegiama mažiausiai privilegijuotojo principu. Mažiausiai privilegijuotojo principas reikalauja, kad individualiems, programiniams ar sisteminiams procesams nebūtų suteikta didesnė prieiga nei būtina atlikti užduotį.

Fizinė kontrolė apžvelgia ir kontroliuoja darbo vietos ir kompiuterinės infrastruktūros aplinką. Fizinės kontrolės priemonės taip pat apžvelgia ir kontroliuoja tokios infrastruktūros įeigą/išeigą. Pavyzdžiui: durys, spynos, šildymas ir vėdinimas, dūmų ir gaisro sistemos, gaisro gesinimo sistemos, kameros, barikados, tvoros, apsaugos darbuotojai ir pan. Tinklo ir darbo vietų skirstymas į funkcines sritis taip pat yra fizinė apsauga. Svarbi fizinės kontrolės dalis, kuri dažnai praleidžiama pro pirštus yra pasiskirstymas pareigomis**.** Pasiskirstymas pareigomis užtikrina, kad individas negalėtų pats atlikti kritinių uždavinių. Pavyzdžiui: programuotojas neturėtų būti ir serverio ar duomenų bazės administratoriumi – šie vaidmenys ir atsakomybės turėtų būti išskirtos.[4]

Dar vienas svarbus informacijos apsaugos ir rizikos valdymo aspektas yra informacijos vertės pripažinimas ir atitinkamų procedūrų informacijos saugumo reikalavimų aprašymas. Ne visa informacija yra vienoda ir ne visai informacijai reikia vienodo lygio apsaugos. Taigi reikalinga saugumo klasifikacija. Pirmasis informacijos klasifikavimo žingsnis – identifikuoti vyresniosios valdybos narį kaip tam tikros informacijos, kuri turi būti suklasifikuota, turėtoją. Toliau reikia išplėtoti klasifikavimo politiką. Kai kurie faktoriai darantys įtaką tam, kokia klasifikacija turi būti pasirinkta, priklauso nuo tos informacijos vertės organizacijai, kokio senumo ta informacija yra ir bet kuriuo atveju kai informacija yra pasenusi. Teisiniai

ir kiti reguliavimo reikalavimai taip pat svarbūs klasifikuojant informaciją. Pagrindinės informacijos apsaugos klasifikavimo žymės naudojamos verslo sektoriuje yra: vieša, vidinio naudojimo, konfidenciali ir slapta.[4]

Visi asmenys dalyvaujantys versle turi būti apmokyti pagal pagal įmonėje galiojančias informacijos klasifikacijos tvarkas. Įmonės informacijos klasifikacija turi būti periodiškai peržiūrima, kad būtų užtikrinta, kad klasifikacija yra. Turint tvarkinga ir veikianti klasifikacijos mechanizma galima žymiai lengviau vykdyti prieigų kontroles.

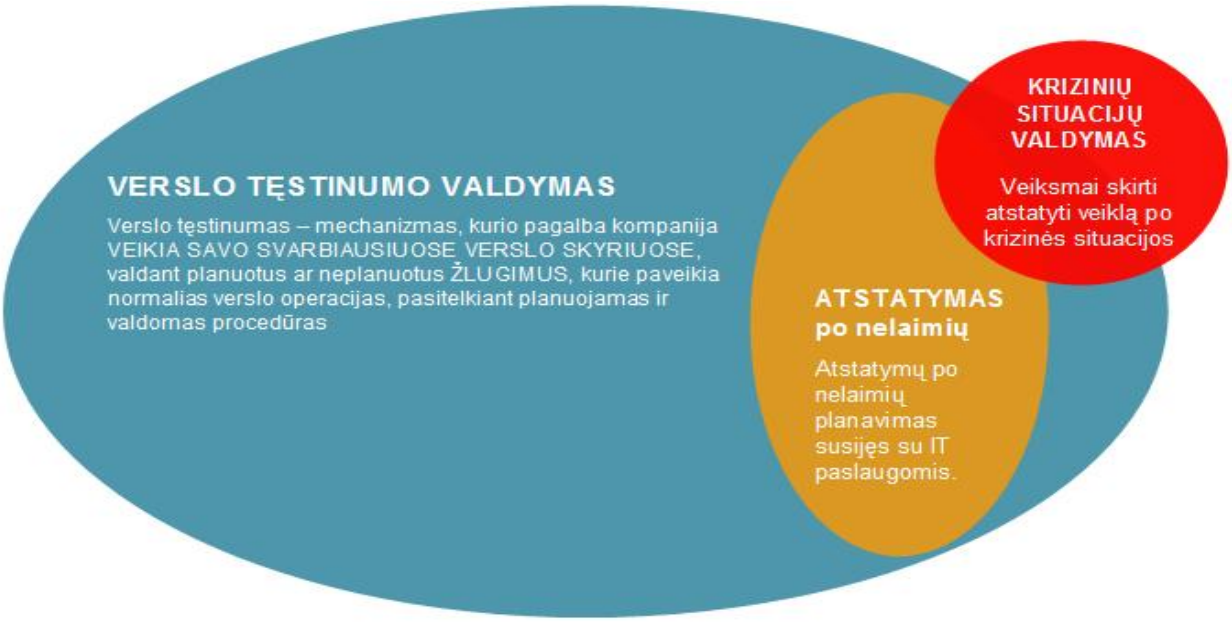
2.6 Verslo tęstinumo valdymas, atstatymas po nelaimių, krizių valdymas.

Verslo tęstinumas – mechanizmas, kurio pagalba kompanija veikia savo svarbiausiuose verslo skyriuose, valdant planuotus ar neplanuotus žlugimus, kurie paveikia normalias verslo operacijas, pasitelkiant planuojamas ir valdomas procedūras vadinamas verslo tęstinumu.[3]

Pagrindinis verslo tęstinumo tikslas neutralizuoti verslo veiklos pertrūkius ir apsaugoti svarbiausius verslo veiklos procesus nuo didesnių informacijos sistemų gedimų arba nelaimių padarinių bei užtikrinti savalaikį verslo veiklos atnaujinimą.

Ne taip, kaip daugelis galvoja, verslo tęstinumas nebūtinai yra IT sistema ar procesas. Šiandien nelaimės ar žlugimai yra realybė. Ar nelaimė gamtinė ar sukurta, ji paveikia normalų gyvenimą ir taip pat verslą. Tai kodėl planavimas toks svarbus? Leiskite mums drąsiai sutikti realybę, kad „kiekvienas verslas atsitaiso“ nepriklausomai nuo to, ar atsistatymas planuojamas ar ne, tiesiog dėl to, kad verslo tikslas – uždirbti pinigus tam, kad galima būtų išgyventi.

Planavimas padeda geriau tam pasiruošti, žinant, kad net geriausi planai gali žlugti. Planavimas gali sumažinti atstatymo kaštus, pridėtines operacines išlaidas ir svarbiausia, padėti išplaukti be didelių pastangų.



2 pav. Verslo tęstinumo planavimas

Kad verslui būtu sukuriami efektyvūs planai, rekomenduojama remtis keliais esminiais klausimais:

1. Kokia galima nelaimės rizika? Kokie esminiai pirmieji veiksmai, kuriuos reikia padaryti?
2. Kurią verslo dalį reikia atstatyti pirmiausiai?
3. Kaip greitai turiu nukreipti tam tikrus resursu, kad atstatyti svarbiausius verslo skyrius?
4. Ką reikia daryti, kad verslas būtų atstatytas?
5. Ar pasirūpinta visomis reikiamomis sąlygomis verslo atstatymui?
6. Kiek ilgai verslas gali veikti be pradinių vietų, sistemų, žmonių?
7. Ar numatyti VTP testavimo darbai?

Didžioji dauguma VTP žinovų rekomenduotų testuoti planą bent kartą per metus, peržiūrėti jo adekvatumą ir perrašyti ar atnaujinti kasmet, ar kai verslas pasikeičia.

Be pagrindinių VTP naudų, planavimas turi ir paslėptas naudas, pavyzdžiui žmonės kurie dalyvauja VTP plano paruošime turi gerą galimybę geriau suprasti kaip veikia verslas ir išskirti kritines vietas, kurių ankščiau nežinojo ir kurioms nebuvo skirta pakankamai dėmesio.

Ruošiant VTP reikėtu nepamiršti ir apie atstatymo po nelaimių (*angl. disaster recovery*) ir krizinių situacijų valdymo planus. Daugeliui gali pasirodyti keblu suprasti kas tai yra atsatymas po nelaimių planas ir lengvai galima ji sumaišyti su VTP, tokia situacija yra dėl to, kad istoriškai kol nebuvo VTP buvo kuriami atstatymo po nelaimių planai IT sistemoms, tačiau pastebėta, kad net IT įmonių verslas priklausiu ne tik nuo IT sistemų, todėl pradėti ruošti VTP planai skirti bendrai visam verslio, o atsatymo po nelaimių planas tapo šio proceso sudedamoji dalis fokusuojama į IT sistemų atsistatyma.

Krizinių situacijų valdymas taipogi yra VTP proceso dalis, apimanti veiksmus kuriuos reikia atlikti įvykus tokiai situacijai kuri sukelia krizę verslui ar organizacijos darbuotojams. Tai gali būti teroristu ataka (pvz. N.Y. Rugsėjo 11d. teraktai, pandemija) tai tokios situacijos paprastai verslo veikloje nenutinka, tačiau 21 amžiuje įsitikinome, kad grėsmės yra realios ir joms irgi reikia būti pasiruošus. Kriziniu situacijų valdymas labiau orientuotas į tam tikros valdymo komandos įkūrimą ir jų narių apmokymą kaip elgtis kritinėmis situacijomis. [4]

2.7 Išvados

Šioje dalyje aptartos pagrindinės informacijos apsaugos problemos, kurias būtina suprasti norint užtikrinti organizacijos saugumą. Susipažinę su pagrindiniais saugumo kriterijais, žinant juos, galima aiškiai iškelti tikslus, norint užtikrinti įmonės patikimumą.

Apžvelgėme, kokios aktualios šių dienų ir kokios galimos ateityje IT grėsmės. Iš pateiktų statistinių duomenų galima daryti išvadas, kad ateityje saugumas bus dar labiau aktualesnis nei šiandien, nes kibernetinių nusikaltimų skaičius nevaldomai didėja. Pavyzdžiui, daugeliui aktuali brukalų problema. Jei

ankščiau reikėdavo atkirti iš pašto srauto brukalus, tai šiandien reikia atrinkinėti pašto žinutes iš brukalų srauto.

Išnagrinėtas rizikų valdymo procesas, tai pirmas žingsnis kuris turi būti žengtas, norint užtikrinti organizacijos saugumą. Labai svarbu žinoti su kokiomis rizikomis, susiduria organizacija ir kaip galima jas valdyti. Susipažinta su verslo tęstinumo planavimu, į kokius klausimus reikėtų atsakyti norint paruošti efektyvų planą. Norėčiau pabrėžti, kad rizikų valdymo procedūros ir veiklos tęstinumo planavimas turėtų būti neatsiejama bet kokios organizacijos veiklos dalis, kuri turėtų neapsiriboti vien saugumo rizikomis, bet turėtų numatyti visas rizikas, kurios galėtų grėsti organizacijos veiklai.

Tik gerai supratę informacijos apsaugos problemas, galima pradėti tvarkyti įmonės procedūras, skirtas užtikrinti informacijos saugumą. Tam galima pasinaudoti saugumo standartais ir metodologijomis.

3 Saugumo standartai ir metodologijos.

3.1 Įvadas

Nepaisant to, kad egzistuoja daug informacijos saugumo standartų, dažniausiai jie yra tiesiog bendrosios gairės ar principai, kurie galbūt nėra pritaikomi tam tikroms organizacijoms. Jei organizacija siekia įgyvendinti saugumo kontroles, kurios yra susijusios su tam tikru standartu ar standartų kompleksu, turi būti išvystyti tam tikri procesai nuo aukščiausios vadovybės iki tiesioginio vartotojo. Diegiant standartizuotas praktikas ar gaires, proceso žinovai turi pasirūpinti, kad jos yra pritaikomos ir atitinkančios specifinę organizacijos kultūra ir verslo bei organizavimo praktikas. Organizacija turi įvykdyti trukumų analizę (angl. *gap anglysis),* kad identifikuotų esamas saugumo kontroles organizacijos viduje, galimas problemas, išlaidas, operacijų įtaką verslui, prieš pradedant bet kokio standarto taikymą. Saugumo politikų ir gairių sukūrimas turi atsirasti tik po trukumų analizės. Vadovybės palaikymas yra būtinas visuose lygmenyse. Taipogi turi būti atliktas vartotojų apmokymas, kad jie kuo geriau suprastų naudas ir galimus poveikius. Dažna problema, kuri atsiranda po standartizacijos, tai padidėjęs vartotojų nusiskundimų skaičius, dėl atsiradusiu naujų apribojimų. Sėkmingas saugumo standartų ar kontrolių pritaikymas turi būti balansas tarp saugumo reikalavimų, funkcinių reikalavimų ir vartotojų poreikių. [3]
Taipogi susiduriama su šiomis problemomis:

- Standartizacijos kaštai;
- Kompetencijos trūkumas;
- Sunku išsirinkti tinkamą standartą;
- Nesutvarkytos vidaus procedūros.

Šiame skyriuje trumpai bus paminėti populiariausi šių dienų standartai, didesnis dėmesys bus skirtas ISO ir COBIT standartams. Pateiksiu šiu standartų išsamesne analizę, jų esminius panašumus ir skirtumus.

3.2 Saugumo standartai

ISO 27000 serija. Tarptautinė standartizacijos organizacija ISO informacijos apsaugos standartizavimui rezervavo seriją 27000. Šią standartų grupę sudaro šie, mus dominantys standartai:

- ISO 27000: Terminai ir apibrėžimai;
- ISO 27001: Informacijos apsaugos vadybos sistema IAVS (buvęs BS 7799-2). Standarte aprašyta Demingo PDCA (Planavimas – Įgyvendinimas – Matavimas - Gerinimas) ciklu pagrįsta informacijos apsaugos vadybos sistema. Standarto tikslas – padėti organizacijoms sukurti ir įgyvendinti IAVS;

- ISO 27002: Informacijos apsaugos priemonės (Buvęs ISO 17799). Šis standartas tai informacijos apsaugos priemonių rinkinys, apimantis organizacines ir technines saugumo priemones. Standarte aprašytos 133 saugumo priemonės suskirstytos į 11 sričių.[1]

CobIT standartas (angl. *control objectives for information and related technologies*). Pasaulio mastu pripažintas informacijos ir susijusių technologijų kontrolės priemonės standartas. CobIT standartas sukurtas kaip bendrai pritaikomas IT saugumo ir kontrolės praktikų rinkinys. Jame numatyti bendrieji IS valdymo, kontrolės, saugumo ir audito principai. [2]

ITIL - (angl. *Information Technology Infrastructure Library*) - ITIL verslo valdymo metodologija, orientuota į darbo optimizavimą bei kokybės užtikrinimą IT kompanijose ar įmonių IT padaliniuose. Santrumpa kilusi iš to, kad pirminis ITIL variantas susidėjo iš kelių dešimčių skirtingus IT įmonių procesus aprašančių knygų - IT valdymo bibliotekos. ITIL yra pripažintas standartais: D. Britanijos BS-15000 bei tarptautiniu ISO-20000, kartu ITIL yra suderinamas ir su visais ISO-9000 reikalavimais. ITIL modulių skaičius, einant laikui, keičiasi.[6]

Mokėjimų kortelių pramonės duomenų saugumo standartas (MKI DSS) nustato visapusiškus reikalavimus mokėjimo sąskaitų saugumui užtikrinti. Jis buvo išplėtotas remiantis MKI saugumo standartų tarybos mokėjimo savitumu, įskaitant American Express, Discover Financial Services, JCB, MasterCard Worldwide ir Visa International, kad padėtų palengvinti platų nuoseklių duomenų apsaugos priemonių pritaikymą globaliu mastu. MKI DSS yra daugiaaspektis saugumo standartas, apimantis saugumo valdymo reikalavimus, politiką, procedūras, tinklo sandarą, programinės įrangos sandarą ir kitas svarbias saugumo priemones. [7]

NIST SP 800-53 rev 2 šis standartas nustato gaires informacinių sistemų naudojimui vyriausybinėse organizacijose.
http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

3.3 ISO/IEC 17799:2005 ir COBIT 4.1 analizė

ISO/IEC 17799:2005
Šio standarto tikslas padėti įgyvendinti, prižiūrėti bei tobulinti organizacijos informacijos saugumo valdymą.
„Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas (tapatus ISO/IEC 27002:2005)“. Šis standartas yra Tarptautinės standartizacijos organizacijos (ISO) ir Tarptautinės elektrotechnikos komisijos (IEC) jungtinio technikos komiteto

ISO/IEC JTC 1 Informacijos technologija SC 27 Informacijos technologijos saugumo metodai pakomitečio parengto tarptautinio standarto ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management, kurį Lietuvos standartizacijos departamentas (LST TK 4 Informacijos technologija PK 1 Informacijos technologijos saugumo metodai) patvirtinimo būdu perėmė kaip Lietuvos standartą LST ISO/IEC
17799:2006 (en), lietuviškoji versija. Jis turi tą patį statusą, kaip ir patvirtinimo būdu perimto tarptautinio standarto oficialiosios versijos [1]. Standartas pateikia suprantamą požiūrį į informacijos apsaugą. Standartas pabrėžia rizikos valdymo svarbą ir aiškiai pasako, kad jums nereikia įdiegti kiekvienos atskiros rekomendacijos – tik tas, kurios yra aktualios. Standartas apima visas informacijos formas, įskaitant garsą ir grafiką, bei tokią mediją kaip mobilūs telefonai ir fakso aparatai.

ISO/IEC 17799:2005 standarto struktūra

ISO/IEC 17799:2005 nustato 132 saugumo valdymo svertus, sudarytus pagal 11 pagrindinių kategorijų kuriuose iš viso aprašomos 39 pagrindinės saugumo kategorijos, kad leistų skaitytojams nusistatyti konkrečius saugiklius, kurie būtų tinkami jų konkrečiam verslui ar konkrečiai atsakomybės sričiai.

Standartą sudaro šios dalys:

- Saugumo politika, tikslas -nustatyti valdymo kryptį ir užtikrinti informacijos saugumą atitinkančius verslo veiklos reikalavimus ir atitinkamus įstatymus rei reglamentus;
- Informacijos saugumo organizavimas (tikslas - valdyti informacijos saugumą organizacijoje).
- Turto valdymas (tikslas - pasiekti ir palaikyti tinkamą organizacijos turto apsaugą).
- Personalas ir informacijos saugumas (tikslas - užtikrinti, kad darbuotojai, rangovai ir trečios šalies atstovai supranta savo atsakomybę ir yra tinkami jiems paskirtoms užduotims atlikti bei mažinti vagystes, sukčiavimo ar piktnaudžiavimo informacijos apdorojimo priemonėmis riziką).
- Fizinis ir aplinkos saugumas (tikslas - išvengti nesankcionuotos fizinės prieigos, nuostolių ir trukdžių organizacijos veiklai ir informacijai).
- Komunikacijų ir operacijų valdymas (tikslas - užtikrinti tikslų ir saugų informacijos apdorojimo priemonių darbą).
- Prieigos valdymas (tikslas - valdyti prieigą prie informacijos).
- Informacijos sistemų komplektavimas, projektavimas ir priežiūra (tikslas - užtikrinti, kad saugumas būtų integrali informacijos sistemų dalis).
- Informacijos saugumo incidentų valdymas (tikslas - užtikrinti, kad apie su informacijos sistemomis susijusius informacijos saugumo įvykius ir silpnąsias vietas būtų pranešta laiku ir būtų galima imtis atsakomųjų veiksmų).[1]

- Atitiktis (tikslas - neutralizuoti verslo veiklos pertrūkius ir apsaugoti svarbiausius verslo veiklos procesus nuo didesnių informacijos sistemų gedimų arba nelaimių padarinių bei užtikrinti savalaikį verslo veiklos atnaujinimą).

COBIT 4.1

CobiT- IT procesų valdymo ir kontrolės modelis, skirtas įmonių vadovams, kontrolės ir rizikos valdymo specialistams, auditoriams. CobiT sistemiškai apjungia verslo rizikas, techninius klausimus, kontrolės bei vertinimo aspektus. Taipogi jis užpildo tam tikrą spragą tarp bendrų valdymo bei kontrolės standartų ir techninių IT saugumo, kokybės bei administravimo standartų.

Pagrindinė CobiT tema – orientacija į verslo poreikius. Jis skirtas ne tik vartotojams bei auditoriams, bet, svarviau, vadovybei ir verslo procesų savininkams, padedant suprasti ir valdyti IT teikiamus privalumus bei susijusias rizikas.[2]

CobiT nauda vadovams:

Geriausios IT valdymo, kontrolės ir saugos praktikos suteikia galimybę įvertinti įmonės būklę objektyviais kriterijais suteikia kriterijus palyginamumui. Palengvinamas sprendimų priėmimas dėl investicijų į IT saugumą ir kontrolę. Leidžia objektyviau įvertinti bei nuspręsti dėl priimtinos rizikos / kaštų balanso.

CobiT nauda vartotojams:

Vartotojai gali būti patikimiau užtikrinti dėl tinkamo teikiamų IT paslaugų saugumo ir kontrolės per sistemišką vidinį ar išorinį vertinimą / auditą remiantis geriausios praktikos metodologija.

CobiT sumažina vertinimų įvairovės problemas apjungdamas daugelio skirtingų standartų nuostatas į vieningą sistemą.

CobiT nauda auditoriams:

Sistemiškas rizikų analizės ir auditų planavimo įrankis.Medžiaga audito programai ir detalesniems audito žingsniams Galimybė pagįsti pastebėjimus geriausios praktikos gairėmis.

Sistemiškas IT procesų vertinimas ir pateikimas verslo vadovybei suprantama terminologija.

CobiT struktūra

CobiT metodologijoje informacija, reikalinga verslo tikslams, gaunama panaudojant IT resursus,

Kurie sistemiškai valdomi IT procesų visumos pagalba.

CobiT padengia keturis domeinus:

- Planavimas ir organizavimas

- Pirkimai ir įdiegimas
- Naudojimas ir aptarnavimas
- Stebėsena

Planavimas ir organizavimas aprašo informacijos ir technologijų panaudojima, kaip geriausiai jos gali būti panaudotas įmonėje, padedant pasiekti įmonės užsibrėžtus tikslus.

1 lentelė. Planavimas ir organizavimas

PO1	Apibrėžti strateginį IT planą
PO2	Apibrėžti informacinę architektūrą
PO3	Pasirinkti technologinę kryptį
PO4	Apibrėžti IT organizacinę struktūrą ir roles
PO5	Kontroliuoti IT investicijas
PO6	Komunikuoti vadovybės tikslus ir kryptį
PO7	Valdyti žmogiškuosius resursus
PO8	Užtikrinti išorinių reikalavimų vykdymą
PO9	Įvertinti ir valdyti riziką
PO10	Valdyti IT projektus

Pirkimai ir įdiegimas dalies procesai skirti rasti tinkamus ir optimalius būdus patenkinti vartotojų poreikius, teikti automatizuotas funkcijas, pedančias verslo procesams. Suteikti platformas, būtinas programinės įrangos funkcionavimui. Užtikrinti, kad vartotojai panaudoja programinę įranga ir technologijas tinkamai pagal paskirtį. Minimalizuoti neautorizuotų pakeitimų galimybę.[2]

2 lentelė. Pirkimai ir įdiegimas

AI1	Automatizavimo sprendimų paieška
AI2	Įsigyti ir prižiūrėti programinę įrangą
AI3	Įsigyti ir prižiūrėti technologinę infrastruktūrą
AI4	Sukurti ir atnaujinti IT naudojimo procedūras
AI5	Įdiegti ir akredituoti sistemas
AI6	Kontroliuoti IT sistemų pokyčius

Naudojimas ir aptarnavimas dalies procesai skirti supratimui kokis aptarnavimo lygis yra reikalingas, užtikrinti, kad trečių šalių uždaviniai yra aiškiai apibrėžti, yra vykdomi ir tenkina vartotojus. Užtikrinti adekvatų sistemų pajėgumą. Užtikrinti, kad informacinės sistemos veikia ir netgi didelės problemos atveju nuostoliai bus minimizuoti. Apsaugoti informaciją nuo neautorizuoto priėjimo, paskleidimo, pakeitimo, praradimo. Užtikrinti, kad svarbios IT funkcijos yra atliekamos reguliariai ir tvarkingai.[2]

3 lentelė. Naudojimas ir aptarnavimas

DS1	Apibrėžti ir užtikrinti tinkamą IT paslaugų lygį
DS2	Kontroliuoti trečiųjų šalių teikiamas paslaugas

DS3	Kontroliuoti sistemų pajėgumus ir apkrovą
DS4	Užtikrinti nuolatinį sistemų funkcionavimą
DS5	Užtikrinti sistemų saugumą
DS6	Identifikuoti ir paskirstyti IT kaštus
DS7	Apmokyti vartotojus
DS8	Teikti pagalbą vartotojams
DS9	Kontroliuoti sistemų konfigūraciją
DS10	Sekti, spręsti problemas ir skundus
DS11	Prižiūrėti duomenis
DS12	Prižiūrėti patalpas kuriose yra įranga
DS13	Užtikrinti kasdienį sistemų panaudojimą

Stebėjimo procedūrų pagrindinis tikslas užtikrinti, kad IT procesams keliami reikalavimai yra vykdomi, kad užtikrinamas nuolatinis iškeltų tikslų pasiekimas. Didinti pasitikėjimą įmone partnerių, klientų tarpe.[2]

4 lentelė. Stebėsena

M1	Prižiūrėti IT funkcijų atlikimą
M2	Įvertintinti vidinės kontrolės adekvatumą
M3	Užtikrinti trečiujų šalių auditą, garantą
M4	Organizaciškai remti audito procesą

ISO/IEC 17799:2005 ryšys su CobiT 4.1

Pagrindinis skirtumas tarp šių standartų tai, kad ISO 17799 standartas pagrinde orientuotas į saugumo valdymą, o CobiT orientuotas į verslo poreikius. CobiT pagal savo prigimtį yra kurkas platesnis nei ISO, jis sukurtas remiantis šių dienų problemomis su kuriomis susiduria verslo organizacijos, todėl nemažai dėmesio yra skiriama informacijos saugai, nes kaip jau minėta, saugumo problemos yra labai aktualios verslui, nuo jų priklauso įmonės patikimumas. Nepaisant to šie standartai nekonkuruoja vienas su kitu, atvirkščiai jie vienas kitą papildo siekiant užtikrinti organizacijų informacijos saugumą.

Žemiau, pateiktoje lentelėje, pateikiama kokias CobiT sritys atitinką ISO 17799 standartas ir kaip jis galėtų būti integruotas su CobiT.[2]

5 lentelė. ISO 17799 standarto atitikimas CobiT

CobiT sritys	1	2	3	4	5	6	7	8	9	10	11	12	13
Planavimas ir organizavimas	-	+	0	+	-	+	+	-	+	-			
Pirkimai ir įdiegimas	0	0	0	-	0	+							
Naudojimas ir aptarnavimas	-	0	-	+	+	-	-	0	0	-	+	+	0
Stebėsena	-	+	+	-									

ISO/IEC 17799:2005 standarto atitiktis CobiT procesams.
(+) Pilnas atitikimas, (0) Dalinis atitikimas, (-) Nėra atitikmens.

3.4 Išvados

Šiame skyriuje susipažinome su populiariausiais saugumo standartais. Kaip galima pastebėti jų yra labai įvarių, tačiau organizacijų poreikiai ir tipai irgi labai įvairūs, beto egzistuoja nemažai skirtingų teisinių reguliavimų skirtų organizacijoms. Pavyzdžiui, PCI DSS standartas, kuris turėtų būti taikomas organizacijoms, kurios vykdo operacijas susijusias su kredinėmis kortelėmis.

Trumpai apžvelges pagrindinius saugumo standartus, išskyriau du ISO 17799 ir CobiT, kurie mano manimu yra priimtiniausi, tinkamiausi telekomunikacinėms įmonėms.

ISO 17799 pagrindinė paskirtis užtikrinti organizacijos saugumo valdymą, tuo tarpu CobiT yra bendresnis, skirtas verslo organizacijomis ir apima ne tik saugumo tema, bet apskirtai visos organizacijos IT valdymą. Beto CobiT standartą yra lengviau pritaikyti, kadangi jis pateikia kontroles ir metrikas palengvinančias jo implementavimą.

Nepaisant to, kad remiantis abiem standartais galima spręsti saugumo problemas, jie vienas su kitu nekonkuruoja, o vienas kitą papildo. Abu standartai yra labai naudingi norint užtikrinti įmonės saugumą, todėl ketvirtame skyriuje atlikau šių standartų pritaikymo įvertinimą. Praktikoje abiejų įgyvendinimas gali būti problematiškas. Trečiame skyriuje buvo minėta, kad dauguma organizacijų neskiria pakankamai lėšų informacijos apsaugos valdymui, dėl to sertifikacijai, standartus reikia rinktis remiantis verslo poreikiais (jei nėta privalomų teisinių reikalavimų).

4. Standartų pritaikymas

4.1 Įvadas

Pastaruoju metu kompiuterių ir informacijos apsaugos srityje atsirado naujos savokios tokios kaip rotingo ir išmintingo asmens, reikiamo atsargumo ir reikiamo rūpesčio.

Verslo pasaulyje akcininkai, klientai, verslo partneriai ir valdžia tikisi, kad korporacijos darbuotojai ves verslą pagal priimtiną verslo praktiką laikantis teisės ir kitų reguliavimo priemonių nuostatų. Tai dažnai aprašoma kaip "protingo ir išmintingo asmens" taisyklė. Išmintingas asmuo laikosi reikiamo atsargumo, kad užtikrintų, jog viskas, kas būtina, yra atlikta, kad verslas operuotų pagal savo principus teisėtu, etišku būdu. Išmintingas asmuo taip pat yra kruopštus (atidus, dėmesingas, nuolatinis) besilaikantis reikiamo stropumo versle

Antra, kalbant apie reikiamą rūpestį, yra tęstinės veiklos – tai reiškia, kad žmonės tikrai daro dalykus, kuriais stebimi ir palaikomi apsaugos mechanizmai, šie veiksmai yra nuolatiniai.

Jais siekiama vis labiau apsaugoti informaciją, kad ją nepasinaudotų netinkamos institucijos ir nepadarytu didelės žalos vidutinėm ir stambiom įmonėm. Įmonių informacijos saugos pagrindas – patikima Informacijos saugumo valdymo sistema (ISVS), apimanti tiek organizacine (saugumo dokumentus, politika, procedūras, tvarka), tiek technologine (programines priemones ir/ar įranga, kuria realizuojami sprendimai) dali. Kad kuo geriau realizuoti saugumo politiką, procedūras ir tvarką rekomenduojama pasinaudoti tam tikrais saugumo standartais, vieniems jie tarnauja kaip rekomendacinė medžiaga, kitiems kaip privalomos vykdimo instrukcijos.

4.2 Informacijos saugumo tyrimo metodika

Pirmiausia yra labai svarbu, kad organizacija identifikuotu savo saugumo reikalavimus. Yra trys pagrindiniai saugumo reikalavimu šaltiniai, kuriais turėtu remtis organizacijos:

1) pirmasis šaltinis nustatomas vertinant organizacijos rizika, atsižvelgiant į bendrąją organizacijų verslo veiklos strategiją bei tikslus.

2) antrasis šaltinis yra teisiniai, įstatyminiai, reglamentiniai ir sutarčių reikalavimai bei socialinė-kultūrinė aplinka, kuriuos turėtų atitikti organizacija, jos prekybos partneriai, rangovai ir paslaugu teikėjai;

3) trečiasis šaltinis yra ypatingas informacijos apdorojimui taikomas principų, tikslų ir verslo veiklos reikalavimų rinkinys, kurį organizacija sukurią savo veiksmams paremti.

Buvo kuriamos anketos pagal TARPTAUTINIS STANDARTAS ISO/IEC 17799.Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas ir COBIT 4.1 leidinio metodologiją. Anketos buvo kuriamos kiekvienam standartų skyriui. Anketos buvo išsiųstos atitinkamų skyrių darbuotojams. Pagal gautus atsakymus į anketas buvo sudaroma lentelė, kuri

pavaizduota 4.3 standarto atitiktis skyriuje. CobiT atitikties lentelėse pateikiama ISO 17799 atitiktis konkrečiai CobiT kontrolei.

4.3 Informacijos saugumo ISO ir COBIT standartų atitikimas

4. Rizikos vertinimas ir priežiūra

6 lentelė. Rizikos vertinimas ir priežiūra

Standartas	Atitikimas įmonėje
*Standarto numeracija: **4.2 Saugumo rizikos priežiūra***	
4.1 Kiekvienai rizikos vertinimo metu nustatytai rizikai reikia taikyti tam tikrą rizikos priežiūros sprendimą. Galimi tokie rizikos priežiūros būdai:	
4.1.1 naudojamos tinkamos valdymo priemonių taikymas, siekiant sumažinti riziką	+
4.1.2 sąmoningas ir objektyvus rizikos prisiėmimas, užtikrina, jog ji aiškiai atitinka organizacijų politiką ir rizikos prisiėmimo kriterijus	+
4.1.3 rizikos perdavimas kitoms šalims, pavyzdžiui, draudikams ar tiekėjams	+
4.1.4 rizikos išvengimas, užkertamas kelias veiksmams, dėl kurių galėtų kilti rizika	+
4.2 Valdymo priemonės, kurios turėtų būti parinktos ir igyvendintos atsižvelgiant į rizikos vertinimo metu nustatytus reikalavimus užtikrina, kad rizika bus sumažinta iki priimtino lygio, atsižvelgiant į:	+
4.2.1 nacionalinių ir tarptautinių teisės aktų ir taisyklių reikalavimus bei apribojimus	+
4.2.2 organizacinius tikslus	+
4.2.3 eksplotacijos reikalavimus ir apribojimus	+
4.2.4 įgyvendinimo bei naudojimo išlaidas, susijusias su sumažinta rizika, kuri išlieka	+
4.2.5 proporcinga organizacijų reikalavimams ir apribojimams	+
4.2.6 poreikį subalansuoti investicijas į valdymo priemonių, skirtų žalos dėl atsiradusių saugumo spragų likvidavimui, įgyvendinimą bei naudojimą.	+

5. Saugumo politika

7 lentelė. Saugumo politika

Standartas	Atitikimas įmonėje
*Standarto numeracija: **5.1.1 Informacijos saugumo politikos dokumentas***	
5.1 Informacijos saugumo politikos dokumente yra skelbiama vadovybės įsipareigojimai ir aprašomas organizacijos požiūris, susijęs su informacijos saugumo valdymu	+
Standarto numeracija: ***5.1.2 Informacijos saugumo politikos priežiūra***	
5.2 Numatytas asmuo, kuris, vadovybės įgaliojimu, būtų atsakingas už informacijos saugumo politikos tobulinimą, peržiūrą ir įvertinimą	+
5.3 Atliekant informacijos saugumo politikos peržiūrą yra atsižvelgiama į valdymo peržiūros rezultatus. Yra apibrėžtos valdymo peržiūros procedūros bei numatytas	+

peržiūros atlikimo tvarkaraštis arba trukmė.	

6. Informacijos saugumo organizavimas

8 lentelė. Informacijos saugumo organizavimas

Standartas	Atitikimas įmonėje
Standarto numeracija: ***6.1.1 Vadovybės įsipareigojimas užtikrinti informacijos saugumą***	
6.1 Vadovybė:	
6.1.1 užtikrinti, kad informacijos saugumo tikslai būtų nustatyti, atitiktų organizacinius reikalavimus bei būtų integruoti į atitinkamus procesus	+
6.1.2 formuoti, peržiūrėti bei tvirtinti informacijos saugumo politiką	+
6.1.3 peržiurėti informacijos saugumo politikos įgyvendinimo veiksmingumą	+
6.1.4 numatyti aiškią kryptį ir suteikti akivaizdžią paramą, skatinancią saugumo Iniciatyvas	+
6.1.5 numatyti informacijos saugumui užtikrinti reikalingus išteklius	-
6.1.6 patvirtinti specifinių funkcijų ir atsakomybių, susijusių su informacijos saugumu, organizacijoje paskirstymą	+
6.1.7 inicijuoti planus ir programas, skatinančias informacijos saugumo suvokimą	+
6.1.8 užtikrinti informacijos saugumo valdymo priemonių įgyvendinimo Koordinavimą visos organizacijos mastu	+
Standarto numeracija: ***6.1.2 Informacijos saugumo koordinavimas***	
6.2 Atliekant paprastai informacijos saugumo koordinavimą vadovaujamasi:	
6.2.1 užtikrinti, kad su saugumu susijusios atliekamos veiklos atitinka informacijos saugumo politiką	+
6.2.2 nustatyti galimų neatitikimų pašalinimo būdus	+
6.2.3 patvirtinti informacijos saugumo metodologijas ir procesus, pavyzdžiui, rizikos vertinimą ar informacijos klasifikavimą	+
6.2.4 nustatyti svarbius su grėsmėmis susijusius pokyčius bei informacijos ir informacijos apdorojimo priemonių, skirtu reaguoti į grėsmes, atskleidimą	+
6.2.5 koordinuoti informacijos saugumo valdymo priemonių įgyvendinimą ir įvertinti jų adekvatumą	+
6.2.6 efektyviais būdais skatinti informacijos saugumo švietimą, mokymą ir supratimą visoje organizacijoje	+
6.2.7 įvertinti informaciją, gautą atliekant stebėjimą ir informacijos saugumo incidentų peržiurą, bei rekomenduoti atitinkamus atsakomuosius veiksmus, susijusius su nustatytais informacijos saugumo incidentais	+
Standarto numeracija: ***6.1.3 Atsakomybės už informacijos saugumą skyrimas***	
6.3 Už saugumą atsakingi asmenys gali pavesti atlikti su saugumu susijusias užduotis kitiems asmenims	+
6.3.1 turi būti paskirtas asmuo ar padalinys, atsakingas už kiekvieną turo vienetą ar saugumo procesą, bei šios atsakomybės ribos įformintos dokumentais	+
Standarto numeracija: ***6.1.4 Prieigos prie informacijos apdorojimo priemonių leidimas***	
6.4.1 Taikant naujas priemones turėtų būti gautas atitinkamas vadovybės leidimas, sankcionuojantis jų tikslą ir panaudojimą. Taip pat turėtų būti gautas vadovo, atsakingo už vietinės informacijos sistemos aplinkos saugumą, patvirtinimas, kad bus laikomasi visų saugumo politikų ir reikalavimų.	+
6.4.2 Tikrinama, ar techninė ir programinė įranga yra suderinta su kitais	+

sistemos komponentais	
Standarto numeracija: ***6.1.5 Konfidencialumo sutartys***	
6.5 Konfidencialumo arba informacijos atskleidimo sutartyse, remiantis teisinę galią turinčiomis sąvokomis,turėtų būti numatomi reikalavimai, skirti apsaugoti konfidencialią informaciją. Nustatomi konfidencialumo arba neatskleidimo sutarčių reikalavimai	+
Standarto numeracija: ***6.1.6 Ryšys su valdžios institucijomis***	
6.6 Organizacijoje yra numatytos procedūros, kuriose yra tiksliai nusakyta, kokiais atvejais ir kas turėtų susisiekti su valdžios institucijomis (pavyzdžiui, teisėsauga, ugniagesiais ar kontroliuojančiomis institucijomis) bei kaip turėtų būti pranešama apie aptiktus informacijos saugumo incidentus laiku, jei įtariama, kad galėjo būti pažeisti įstatymai.	+
Standarto numeracija: ***6.1.7 Ryšys su specialiomis interesų grupėmis***	
6.7 Palaikomi atitinkami ryšiai su specialių interesų grupėmis ar kitais specialistų saugumo forumais bei profesinėmis asociacijomis.	+
Standarto numeracija: 6.1.8 Nepriklausoma informacijos saugumo peržiūra	
6.8 Organizacijos informacijos saugumo valdymas ir jo įgyvendinimo būdai (t.y. valdymo tikslai, valdymo priemonės, politikos, procesai ir informacijos saugumo procedūros) nepriklausomų specialistų yra peržiūrimi periodiškai arba įvykus svarbiems saugumo įgyvendinimo pasikeitimams	+
Standarto numeracija: 6.2 Išorinės šalys	
6.9 Išorinei šaliai suteikiamos prieigos prie informacijos ir informacijos apdorojimo priemonių tipas.	+
Standarto numeracija: 6.2.1 Rizikų, susijusių su išorinėmis šalimis, nustatymas	
6.10 Prieš suteikiant prieigą prie organizacijos informacijos ir informacijos apdorojimo priemonių, turėtų būti nustatyta rizika, kylanti dėl trečiosios šalies dalyvavimo verslo procesuose, bei įgyvendinamos atitinkamos valdymo priemonės	+
6.10.1 leidžiamus prieigos metodus bei unikalių naudotojo identifikatorių ir slaptažodžių naudojimą ir valdymą	+
6.10.2 naudotojo prieigos sankcionavimo procedūrą ir privilegijas	+
6.10.3 pareiškimą, kad bet kokia nesankcionuota prieiga yra draudžiama	+
6.10.4 prieigos teisių panaikinimo arba ryšio tarp sistemų nutraukimo procedūras	+
6.12 Susitarimai dėl pranešimo, paskelbimo ir perspėjimo apie netikslią informaciją (pavyzdžiui, asmens duomenis), informacijos saugumo incidentus ir saugumo spragas	+
6.13 Apsaugota ir aprašyta kiekviena paslauga, kuri turi būti prieinama.	+

9. Turto tvarkymas

9 lentelė. Turto tvarkymas

Standartas	Atitikimas įmonėje
Standarto numeracija: 7.1.1 Turto aprašai	
7.1 Organizacija apibrėžia visą turtą bei šio turto svarbą įforminti dokumentuose	+
7.1.2 Turto aprašuose yra įtraukta visa būtina informacija, galinti padėti susigrąžinti turtą nelaimės atveju, įskaitant turto tipą, formą,vietą, informaciją apie atsarginę kopiją, informaciją apie licencijas bei verslo veiklos vertę.	+
Standarto numeracija: 7.2.1 Klasifikavimo gairės	
7.2 Klasifikuojant informaciją turėtų būti atsižvelgta į verslo veiklos poreikius.	+
7.2.1 Turto valdytoas turėtų apibrėžti turto klasifikaciją, periodiškai ją peržiūrėti bei užtikrinti, kad ji taikoma teisingai ir reikiamu lygiu.	+

Standarto numeracija: 7.2.2 Informacijos žymėjimas ir priežiūra	
7.3 Iš sistemose saugomos informacijos, kuri yra klasifikuojama kaip slapta arba pavojinga, išvedama informacija turėtų būti pažymėta (išvestyje) atitinkamu klasifikavimo ženklu. Svarstomas informacijos turtas apima spausdintus pranešimus, ekrano duomenis, įrašomas duomenų laikmenas (pavyzdžiui, juostas, diskus, kompaktinius diskus), elektroninius pranešimus ir perduodamus failus.	+

4 lent. (Turto tvarkymas)

8. Personalas ir informacijos saugumas

10 lentelė. Personalo ir informacijos saugumas

Standartas	Atitikimas įmonėje
8.1 Kandidatai į darbo vietas, rangovai ir trečios šalies atstovai deramai tikrinami	+
8.2 Darbuotojai, rangovai ir trečios šalies numatyti informacijos apdorojimo priemonių naudotojai pasirašo sutartį dėl saugumo užtikrinimo ir atsakomybės	+
Standarto numeracija: 8.1.1 Įsipareigojimai ir atsakomybės	
8.3 Pasirašoma saugumo įsipareigojimų ir atsakomybės sutartis ar joje yra visi paminėti punktai:	
8.3.1 įgyvendinti ir veikti pagal organizacijos inofrmacijos saugumo politikas	+
8.3.2 saugoti turtą nuo nesankcionuotos prieigos, paviešinimo, iškreipimo, sunaikinimo ar trukdžių	+
8.3.3 vykdyti konkrečius saugumo procesus ir veiklas	+
8.3.4 užtikrinti, kad konrečią veiklą vykdantis asmuo yra už ją atsakingas	+
8.3.5 pranešti apie saugumo įvykius ar potencialius įvykius, ar kitą su organizacija susijusią saugumo riziką	+
Standarto numeracija: 8.1.2 Patikra	
8.4 Įgyvendinimo rekomendacijos. Ar atliekant tikrinimus atsižvelgiama į atitinkamą privatumą, asmens duomenų apsaugą ir (arba) su įdarbinimu susijusią įstatyminę bazę? Jei tai leidžiama, ar tikrinami šie dalykai:	
8.4.1 pretendento gyvenimo aprašymas (jo išsamumas ir tikslumas)	+
8.4.2 pateiktų akademinių ir profesinių kvalifikacijų patvirtinimas	+
8.4.3 tapatybė (pasas arba panašus dokumentas)	+
8.4.4 smulkesnė informacija, pavyzdžiui, apie pretendeto reputaciją ar teistumą	-
8.4.5 pateiktos įtikinamos rekomendacijos	+
Standarto numeracija: Įdarbinimo nuostatai ir sąlygos	
8.5 Sutartyse yra šie numatyti įdarbinimo nuostatai ir sąlygos bei apibrėžtos jų ir organizacijos atsakomybės dėl informacijos saugumo:	
8.5.1 Visi darbuotojai, rangovai ir trečiosios šalies atstovai, kuriems yra suteikta prieiga prie slaptos informacijos yra pasirašę konfidencialumo arba informacijos neatskleidimo sutartis prieš suteikiant jiems prieigą prie informacijos apdorojimo priemonių	+
8.5.2 Darbuotojų, rangovų ir visų kitų naudotojų teisines atsakomybes ir teises, pavyzdžiui, susijusias su autorių teisių įstatymais ar duomenų apsaugos įstatymais	+
8.5.3 Atsakomybes už informacijos klasifikavimą ir organizacijos turto, susijusio su darbuotojo, rangovo ar trečiosios šalies atstovo prižiūrimomis informacijos sistemomis ir paslaugomis, valdymą	+
8.5.4 Darbuotojo, rangovo ar trečiosios šalies atstovo atsakomybes už informacijos, gautos iš kitų bendrovių ar įšorinių šalių, tvarkymą	+

8.5.5 Organizacijos atsakomybes už asmeninės informacijos, įskaitant su darbu organizacijoje ar bendradarbiavimu susijusios asmeninės informacijos, tvarkymą	+
8.5.6 Atsakomybes už veiksmus, atliekamus ne organizacijos patalpose ir nedarbo valandomis, pavyzdžiui, dirbant namie	-
8.5.7 Veiksmus, kurių bus imtasi, jei darbuotojas, rangovas ar trečiosios šalies atstovas nepaisys organizacijos saugumo reikalavimų	+
Standarto numeracija: 8.2 Informacijos saugumas įdarbinimo laikotarpiu	
8.6 Darbuotojai, rangovai ir trečiosios šalies atstovai yra tinkamai skatinami, turi deramą supratimą, kvalifikaciją ir yra apmokyti saugumo procedūrų ir tinkamo informacijos apdorojimo priemonių naudojimo	+
Standarto numeracija: 8.2.2 Informacijos saugumo supratimas, švietimas ir mokymas	
8.7 Mokymai pradedami nuo įvadinės informacijos, skirtos supažindinti su organizacijos saugumo politika ir galimybėmis. Tolesnio mokymo metu ar yra supažindinama su saugumo reikalavimais, teisine atsakomybe bei verslo veiklos valdymo priemonėmis.Apmokomi teisingai naudoti informacijos apdorojimo priemones pavyzdžiui, prisijungimo procedūra, programinės įrangos paketų naudojimas ar informacija apie drausmines nuobaudas)	+
Standarto numeracija: 8.2.3 Drausminė procedūra	
8.8 Darbuotojams, pažeidusiems saugumo reikalavimus, taikoma oficiali drausminė procedūra.	+
8.8.1 Pradedama vykdyti drausminė procedūra tik įsitikinus, kad buvo nesilaikyta saugumo reikalavimų	+
8.9 Darbuotojo, rangovo ar trečiosios šalies atstovo įdarbinimo sutartyje yra numatyta atsakomybė ir pareigos, kurios tebeturės galių ir pasibaigus šios įdarbinimo sutarties galiojimo laikui	+
8.10 Oficialiai numatyta, kad, pasibaigus įdarbinimo sutarties galiojimo laikui, turi būti grąžinta visa prieš tai išduota programinė įranga, darbiniai dokumentai ir įranga. Be to, turi būti grąžintas ir visas kitas organizacijos turtas, pavyzdžiui, nešiojami prietaisai, kreditinės kortelės, leidimai, programinė įranga, vadovai ir elektroninėse laikmenose laikoma informacija	+
8.10.1 Darbuotojo, rangovo ar trečiosios šalies atstovo įdarbinimo sutartyje numatyta atsakomybė ir pareigos, kurios tebeturės galią ir pasibaigus šios įdarbinimo sutarties galiojimo laikui	+/-
8.11 Prieigos prie organizacijos turto ar informacijos apdorojimo priemonių teisės yra apribojamos arba pašalinamos prieš pasibaigiant darbo sutarties galiojimo laikui arba pakeičiant pareigas.	+

4 lent. (Personalo ir informacijos saugumas)

9. Fizinis ir aplinkos saugumas

11 lentelė. Fizinis aplinkos saugumas

Standartas	Atitikimas įmonėje
Saugumo numeracija: 9.1 Saugios vietos	
9.1 Numatomos ir pagal galimybes įgyvendintos fizinėms saugumo aptvaroms skirtos priemonės	+
9.2 Fizine įėjimo kontrole	+
9.3 Įstaigų, patalpų ir priemonių apsauga	+
9.4 Apsauga nuo išorinių ir aplinkos grėsmių, atsižvelgiama į bet kokias galimas	+

grėsmes, susijusias su aplinka, pavyzdžiui, gretimų pastatų gaisrais, vandens nuotėkiu nuo stogo ar žemiau žemės lygio esančių patalpų apsėmimu, ar sprogimu gatvėje	
9.5 Darbas saugiosiose vietose	+
9.6 Siekiant išvengti nesankcionuotos prieigos, prieigos taškai, pavyzdžiui, pristatymo ir krovimo vietos, pro kurios nepageidaujami asmenys galėtų patekti į patalpas, ar yra prižiūrimos ir, esant galimybei, atskiriamos nuo informacijos apdorojimo priemonių	+
Saugumo numeracija: 9.2 Įrangos saugumas	
9.7 Siekiant apsaugoti įrangą:	
9.7.1 įrangos vieta yra parinkta taip, kad kiek galima yra sumažinta nereikalinga prieiga į darbo vietas	+
9.7.2 informacijos apdorojimo priemonės, kuriomis tvarkoma slapta informacija, yra išdėstytos taip, kad jų naudojimo metu su tuo nesusiję asmenys turėtų kuo mažesnę galimybę pamatyti šią informaciją; taip pat nuo nesankcionuotos prieigos yra apsaugotos informacijos laikymo priemonės	+
9.7.3 siekiant sumažinti reikiamą bendrosios apsaugos lygį, ypatingos apsaugos reikalaujantys elementai yra laikomi atskirai	+
9.7.4 siekiant kiek galima labiau sumažinti potencialiu fizinių grėsmių, pavyzdžiui, vagystės, gaisro, sprogimo, dūmų, vandens (ar vandens tiekimo sutrikimų), dulkių, vibracijos, cheminio poveikio, elektros tiekimo ar ryšių sutrikimų, elektromagnetinės radiacijos ar vandalizmo riziką, yra pritaikytos specialios valdymo priemonės	+
9.7.5 numatytos gairės, reglamentuojančios valgymą, gėrimą ir rūkymą šalia informacijos apdorojimo priemonių	+
9.7.6 yra stebimos aplinkos sąlygos, pavyzdžiui, temperatūros svyravimai ar drėgmės lygis, galinčios daryti nepalankią įtaką informacijos apdorojimo priemonėms	+
9.7.7 visuose pastatuose yra įrengti žaibolaidžiai, be to visose energijos ir ryšio linijose yra įrengti apsaugos nuo žaibo filtrai	+
9.7.8 pramoninės aplinkose yra numatytas ypatingų apsaugos priemonių, pavyzdžiui, klaviaturos plėvelių, naudojimas	-
9.7.9 siekiant sumažinti informacijos netekimo ar nutekėjimo riziką, yra atitinkamai saugoma slaptai informacijai apdoroti skirta įranga	+
9.8 Užtikrinamas kabelių saugumas	+
9.9 Prietaisai, kuriose laikoma slapta informacija yra fiziškai sunaikinami arba sunaikinta, pašalinta ar perrašyta juose laikoma informacija, naudojant metodus, kurie užtikrintų, kad originali informacija būtų nebeatstatoma, užuot naudojus standartines šalinimo arba formato funkcijas.	+

5 lent. (Fizinis aplinkos saugumas)

10. Ryšių ir darbo procedūrų valdymas

12 lentelė. Ryšių ir darbo procedūros valdymas

Standartas	Atitikimas įmonėje
Standarto numeracija: 10.1.1 Darbo procedūrų įforminimas dokumentais	
10.1 Turėtų būti parengtos ir iformintos dokumentais sistemos veiklos, susijusios su informacijos apdorojimo ir ryšių priemonėmis, procedūros, pavyzdžiui, kompiuterio įjungimo ir išjungimo, atsarginių kopijų, įrangos priežiūros, laikmenų tvarkymo, kompiuterizuotų darbo vietų ir pašto priežiūros	+

valdymo bei saugumo procedūros	
10.2 Darbo procedūrose turėtų būti smulkiai apibūdinamas kiekvienos šių užduočių vykdymas:	
10.2.1 informacijos apdorojimas ir priežiūra	+
10.2.2 atsarginių kopijų darymas	+
10.2.3 tvarkaraščio reikalavimai, įskaitant abipusę priklausomybę nuo kitų sistemų,	+
10.2.4 artimiausio darbo pradžios ir paskutinio darbo pabaigos laikus	+
10.2.5 nurodymai, kaip tvarkyti klaidas ar kitas išimtines sąlygas, kurios kiltų atliekant darbus, įskaitant sisteminių paslaugų programų naudojimo apribojimus	+
10.2.6 ryšių palaikymas, kilus netikėtiems darbo arba techniniams sunkumams	+
10.2.7 specialios informacijos išvesties ir laikmenų priežiūros instrukcijos, pavyzdžiui, specialaus popierinių dokumentų naudojimo arba konfidencialios informacijos išvesties valdymo, įskaitant saugaus informacijos pašalinimo procedūras	+
10.2.8 sistemos kartotinio paleidimo ir atkūrimo procedūros, kurias reikia naudoti sisteminės klaidos atveju	+
10.2.9 audito eigos žurnalų ir informacijos apie prisijungimą prie sistemos Valdymas	+
Standarto numeracija: 10.1.2 Keitimų valdymas	
10.3 Operacinių sistemų ir taikomosios programinės įrangos keitimas turėtų būti griežtai vadovybės valdomas. Ypatingai turėtų būti atkreiptas dėmesys numatant šiuos dalykus:	
10.3.1 reikšmingų keitimų nustatymą ir registravimą	+
10.3.2.keitimų planavimą ir bandymą	+
10.3.3 galimos tokiu keitimų įtakos, įskaitant įtakos saugumui, vertinimą	+
10.3.4 siūlomų keitimų oficialaus patvirtinimo procedūrą	+
10.3.5 visų su tuo susijusių asmenų detalų informavimą apie pakeitimus	+
10.3.6 Pasirūpinta, kad nė vienas asmuo negaletų prieiti prie turto, jį keisti ar naudoti prieš tai negavęs tam leidimo.	+
Standarto numeracija: 10.1.4 Kūrimo, testavimo ir eksploatavimo priemonių atskyrimas	
10.3.6 atsarginių priemonių taikymo procedūras, įskaitant nutraukimo ir atkūrimo procedūras ir atsakomybes nesėkmingų pakeitimų ar nenumatytų ivykių atvejais	+
10.4 Numatytas eksploatavimo, testavimo ir kūrimo aplinkų, kurios yra būtinos norint išvengti operacinių nesklandumų, atskyrimo lygis ir įgyvendintos reikiamos valdymo priemonės	+
10.4.1 ar yranustatytos ir iformintos dokumentais sistemos perkėlimo iš kūrimo į darbinę būseną taisyklės	+
10.4.2 kūrimo ir eksploatavimo programinė įranga turėtų būti naudojama skirtingose sistemose ar skirtinguose kompiuteriuose bei skirtingose srityse ar kataloguose	+
10.4.3 kompiliavimo, redagavimo ir kitos sistemos paslaugų programos, kai Tam nėra reikalo, neturėtų būti pasiekiamos iš operacinės sistemos	+
10.4.4 testavimo sistemos aplinka turėtų kiek galima labiau atkartoti operacinės sistemos aplinką	+
10.4.5 siekiant sumažinti klaidos riziką, operacinių ir testavimo sistemų naudotojai turėtų naudoti skirtingus naudotojų profilius, o meniu turėtų būti pateikiamos atitinkamos atpažinimo žinutės	+
10.4.6 slapti duomenys neturėtų būti perkeliami į testuojamos sistemos aplinką	+

Standarto numeracija: 10.2 Trečios šalies teikiamų paslaugų valdymas	
10.5 Ar užtikrinamas ir, kai reikia, pagerinti sistemų parengtumą ir efektyvumą, Turėtų būti atliekamas sistemos derinimas bei stebėsena	+
10.5.1 Trečios šalies teikiamos paslaugos, ataskaitos ir kiti dokumentai, nuolat stebimi ir tikrinami.	+
10.5.2 Pokyčiai, susije su apsirūpinimu paslaugomis, įskaitant esamos informacijos saugumo politikos, procedūrų ir valdymo priemonių palaikymu ir tobulinimu, yra atliekami, atsižvelgiant į su tuo susijusių verslo veiklos sistemų ir procesų svarbą.	+
Standarto numeracija: 10.3 Sistemos planavimas ir priėmimas	
10.6 Nustatomi naujų informacijos sistemų, naujovinimo ir naujų versijų priėmimo kriterijai, šios sistemos išbandomos jas kuriat ir prieš jas priimant.	+
Standarto numeracija: 10.4 Apsauga nuo kenksmingų ir mobiliųjų programų	
10.7 Kenksmingų programų kontrolė turėtų būti grindžiama kenksmingų programų atpažinimo ir sistemos atitaisymo programine įranga, saugumo supratimu, tinkama sistemos prieiga ir valdymo priemonių keitimu	+
10.7.1 nustatoma oficiali politika, draudžianti naudoti nesankcionuotą programinę Įrangą	+
10.7.2 nustatoma oficiali politika, siekiant apsisaugoti nuo rizikos, susijusios su failų ir programinės įrangos gavimu iš išorinių tinklų, per juos arba kitą terpę, nurodant, kokių apsaugos priemonių turėtų būti imtasi	+
10.7.3 periodiškai peržiūrima sistemų, palaikančių svarbią reikšmę verslo veiklai turinčius procesus, programinė įranga ir duomenys; bet kurių nesankcionuotų failų arba nesankcionuotų pataisų buvimas turėtų būti oficialiai tiriamas	+
10.7.4 įdiegiama ir nuolat atnaujinama kenksmingų programų aptikimo ir sistemos atitaisymo programinė įranga, skirta tikrinti kompiuterius ir laikmenas, taikant ją kaip atsargumo ar įprastą priemonę; šiuo atveju reikėtų: įdiegiama ir nuolat atnaujinama kenksmingų programų aptikimo ir sistemos atitaisymo programinė įranga, skirta tikrinti kompiuterius ir laikmenas, taikant ją kaip atsargumo ar įprastą priemonę	+
10.7.5 apibrėžiamos ir įsisavinamos valdymo proceduros ir atsakomybės, susijusios su sistemų apsauga nuo kenksmingų programų, bei teikiami pranešimai apie kenksmingų programų puolimą ir atliekami atkūrimo veiksmai	+
10.7.6 parengiami reikiami verslo veiklos tęstinumo planai, numatant atkūrimo veiksmus po kenksmingų programų puolimo, įskaitant visas reikalingas duomenų ir programinės įrangos kopijavimo ir atkūrimo priemones	
10.7.7 įgyvendinamos procedūros, skirtos reguliariai rinkti informaciją, pavyzdžiui, registravimasis įi elektroninio pašto grupes ir (arba) tinklalapių, kuriuose pateikiama informacija apie naujas kenksmingas programas, reguliarus lankymas	+
10.7.8 įgyvendinamos procedūros, skirtos tikrinti informaciją, susijusią su kenksmingomis programomis, ir užtikrinama, kad įspėjimo suvestinės yra tikslios ir informatyvios; vadybininkai turėtu užtikrinti, kad siekiant atskirti klaidinančias įmitacijas ir tikras kenksmingas programas būtų pasitelkiamos tinkamos priemonės, pavyzdžiui, gerą reputaciją turintys žurnalai, patikimos interneto svetainės arba antivirusinės programinės įrangos tiekėjai; visi naudotojai turėtų būti informuoti apie klaidinančias imitacijas ir žinoti, kaip elgtis jas aptikus	+
Standarto numeracija: 10.5 Atsarginės kopijos	
10.8 Esant nelaimei arba duomenų laikmenų gedimui, turėtų būti numatytos tinkamos kopijavimo priemonės. Darant informacijos atsargines kopijas turėtų būti numatomos šios priemonės:	+
10.8.1 apibrėžtas būtinas atsarginės informacijos lygis	+

10.8.2 tikslus ir išsamus atsarginių kopijų registravimas ir įformintos dokumentais atkūrimo procedūros	+
10.8.3 atsarginių kopijų darymo apimtis (pavyzdžiui, pilnos ar dalinės kopijos) ir dažnumas turėtų atitikti organizacijos verslo veiklos reikalavimus, su tuo susijusios informacijos saugumo reikalavimus ir informacijos svarbą nenutrūkstamai organizacijos veiklai užtikrinti?	+
10.8.4 atsarginės kopijos turėtų būti laikomos atskiroje, pakankamai nutolusioje vietoje, kad, įvykus gedimams pagrindinėje darbo vietoje, jos nenukentėtų	+
10.8.5 atsarginei informacijai turėtų būti numatytas tinkamas fizinis ir aplinkos apsaugos lygis ,kuris atitiktų pagrindinei darbo vietai taikomus standartus; valdymo priemonės, kurios yra taikomos pagrindinės darbo vietos duomenu laikmenoms, turėtų būti taikomi ir atsarginei darbo vietai	+
10.8.6 atsarginės duomenų laikmenos, turėtų būti periodiškai išbandomos siekiant įsitikinti, kad avarijos atveju jomis galima pasikliauti	+
10.8.7 atkurimo procedūros turėtų būti nuolat tikrinamos ir išbandomos, kad būtų įsitikinta, ar jos yra veiksmingos ir gali būti įvykdomos operacinių procedūrų atkūrimui skirtu laiku	+
10.8.8 tais atvejais, kai svarbu išsaugoti konfidencialumą, atsarginės kopijos turėtų būti apsaugotos šifravimo priemonėmis	+
Standarto numeracija: 10.6 Tinklo apsaugos valdymas	
10.9 Tinklo vadybininkai turėtų taikyti valdymo priemones, kurios užtikrintų duomenų saugumą tinkluose ir apsaugotų su jais susijusias paslaugas nuo nesankcionuotos prieigos.	+
10.9.1 esant galimybei, atsakomybė už tinklo operacijas ir kompiuterines operacijas turėtų būti atskirta	+
10.9.2 turėtų būti numatyta atsakomybė už nuotolinės įrangos, įskaitant naudotojo vietoje esančią įrangą, valdymo procedūra	+
10.9.3 turėtų būti nustatomos specialios valdymo priemonės, skirtos išsaugoti viešaisiais tinklais ar bevieliais tinklais perduodamų duomenų konfidencialumą ir vientisumą bei apsaugoti su jais sujungtas sistemas ir taikomąsias programas ;siekiant išlaikyti tinklo paslaugų ir prijungtų kompiuterių parengtumą gali prireikti taikyti specialias valdymo priemones	+
10.9.4 turėtų būti atliekamas su saugumu susijusių veiksmų registravimas ir Stebėsena	+
10.9.5 siekiant optimizuoti organizacijai teikiamas paslaugas ir užtikrinti, kad valdymo priemonės būtų nuosekliai taikomos visoje informacijos apdorojimo infrastruktūroje, turėtų būti glaudžiai derinami valdymo veiksmai	+
10.10 Yra nustatoma ir periodiškai stebima tinklo tiekėjo galimybė saugiai administruoti sutartas paslaugas bei numatomos teisės atlikti auditą	+
10.11 Tinklo paslaugų saugumo priemonės tokios:	
10.11.1 technologijos, taikomos tinklo paslaugų saugumui užtikrinti, pavyzdžiui, tapatumo nustatymas, šifravimas ar tinklo ryšio valdymo priemonės	+
10.11.2 saugumo ir tinklo ryšio taisykles atitinkantys techniniai parametrai, reikalingi užtikrinti saugų ryšį	+
10.11.3 tinklo paslaugų naudojimo procedūros, skirtos, esant reikalui, apriboti prieigą prie tinklo paslaugų ar taikomųjų programų	+
Standarto numeracija: 10.7 Duomenų laikmenų priežiūra	
10.12 Duomenų laikmenos prižiūrimos ir fiziškai apsaugomos patikimoje ir saugioje aplinkoje.	+
10.12.1 Nebereikalingos laikmenos saugiai ir patikimai sunaikinamos, taikant	+

oficialias procedūras.	
10.12.2 Oficialiai numatytos ir parengtos informacijos priežiūros, apdorojojimo, saugojimo ir perdavimo procedūros.	+
10.12.3 Siekiant užtikrinti sistemos dokumentacijos saugumą, turėtų būti imtasi šių priemonių:	
10.12.4 sistemos dokumentacija turėtų būti patikimai saugoma	+
10.12.5 turėtų būti nustatytas kuo mažesnis galimų kreipčių į sistemos dokumentaciją skaicius, kurį turi patvirtinti taikomosios sistemos valdytojas	+
10.12.6 viešajame tinkle laikoma arba viešuoju tinklu perduodama sistemos dokumentacija turėtų būti tinkamai apsaugota	+
Standarto numeracija: 10.8 Keitimasis informacija	
10.13 Vadovaujamasi šiais elektroninio susirašinėjimo saugumo nurodymais:	
10.13.1 apsaugoti pranešimus nuo nesankcionuotos prieigos, modifikacijos ar paslaugos atsižadėjimo	+
10.13.2 užtikrinti, kad būtų nurodytas teisingas adresas ir deramai siunčiama	+
10.13.3 užtikrinti bendrą paslaugos patikimumą ir parengtumą	+
10.13.4 vadovautis teisiniais aspektais, pavyzdžiui, susijusiais su elektroniniais Parašais	+
10.13.5 prieš naudojantis išorinėmis viešosiomis paslaugomis, pavyzdžiui, skubiuoju paštu ar bendrojo naudojimo failais, turėtų būti gautas leidimas	+
10.13.6 jungiantis prie sistemos iš viešai prieinamų tinklų reikia naudotis aukštesniais tapatumo nustatymo lygmenimis	+
Standarto numeracija: 10.10 Stebėsena	
10.14 Turėtų būti numatytos valdymo priemonės, skirtos apsaugoti registravimo žurnalus nuo nesankcionuotų pakeitimų ir darbo nesklandumų:	
10.14.1 įrašytų pranešimų tipo keitimas	+
10.14.2 žurnalo failų taisymas ar šalinimas	+
10.14.3 žurnalo failo laikmenos talpos didinimas, skirtas registruotų įvykių pakeitimui arba seniau registruotų įvykių perrašymui	+
10.15 Administratoriaus ir operatoriaus žurnaluose turėtų būti pateikiama ši informacija:	
10.15.1 įvykio (sėkmingo įvykio arba gedimo) laikas	+
10.15.2 duomenys apie įvykį (pavyzdžiui, naudotus failus) arba gedimus (pavyzdžiui, klaida programoje ir veiksmus, kurių buvo imtasi ją šalinant	+
10.15.3 su įvykiu susijusi paskyra ir administratorius ar operatorius	+
10.15.4 su įvykiu susije veiksmai	
10.16 Klaidos, susijusios su informacijos apdorojimo ar ryšio sistemų nesklandumais, apie kurias praneša naudotojai arba sisteminės programos, turėtų būti registruojamos. Turėtų būti numatytos aiškios informacijos apie pranešamas klaidas tvarkymo taisyklės	+
10.16.1 įregistruotų klaidų peržiūra, siekiant užtikrinti, kad klaidos buvo sėkmingai ištaisytos	+
10.16.2 klaidų atitaisymo priemonių peržiūra, siekiant užtikrinti, kad valdymo priemonės taikomos teisingai ir atliekami veiksmai yra visiškai sankcionuoti	+
10.17 Saugumo valdymo priemonės, paslaugų pobūdis ir teikimo lygiai, numatyti su trečiosiomis šalimis dėl paslaugų tiekimo sudarytose sutartyse, yra trečiosios šalies įgyvendinami, vykdomi ir išlaikomi	+
10.18 Trečiosios šalies teikiamų paslaugų stebėsena ir peržiūra turėtų užtikrinti, kad yra laikomasi sutartyse numatytų saugumo nuostatų ir sąlygų ir, kad informacijos saugumo incidentai ir problemos yra deramai valdomi. Turėtų būti apibrėžti organizacijos ir trečiosios šalies santykiai ir procesai, valdant	+

paslaugą	
10.19 Pokyčiai, susiję su apsirūpinimu paslaugomis, įskaitant esamos informacijos saugumo politikos, procedūrų ir valdymo priemonių palaikymu ir tobulinimu, turėtų būti atliekami, atsižvelgiant į su tuo susijusių verslo veiklos sistemų ir procesų svarbą, ir pakartotinai įvertinus riziką:	+
10.19.1 pokyčiai, kuriuos turi įgyvendinti organizacija	+
10.19.2 pokyčiai, kuriuos savo paslaugų atžvilgiu turi taikyti trečioji šalis	+
10.20 Duomenų laikmenos yra prižiūrimos ir fiziškai apsaugomos	+
10.21 Taikant procedūras ir valdymo priemones, kuriomis vadovaujamasi naudojant elektronines komunikacijos priemones, skirtas keistis informacija	+
10.22 Svarstant verslo veiklos sistemų tarpusavio ryšio įtaką saugumui ir verslo Veiklai	+
10.22.1 žinomus administracinių ir apskaitos sistemų pažeidžiamumus, kai informacija keičiamasi tarp skirtingų organizacijos padalinių	+
10.22.2 informacijos pažeidžiamumą verslo veiklos ryšio sistemose, pavyzdžiui, telefoninių arba konferencinių pokalbių įrašymą, pokalbių konfidencialumą, faksimilių saugojimą, pašto tikrinimą, pašto paskirstymą	+
10.22.3 politiką ir atitinkamas valdymo priemones, skirtas valdyti keitimąsi Informacija	+
10.22.4 slaptos verslo veiklos informacijos skaidymo į skirtingas kategorijas atsisakymą, jeigu sistema neužtikrina reikiamo apsaugos lygio	+
10.22.5 prieigos prie tam tikrų asmenų, pavyzdžiui, su slaptais projektais dirbančio personalo, asmens bylų apribojimą	+
10.22.6 personalo, rangovų arba verslo veiklos partnerių kategorijas, kurioms yra numatytas leidimas naudoti sistemą, ir vietos, iš kurių prie jos galima prieiga	+
10.22.7 naudojimosi tam tikromis priemonėmis apribojimą atskiroms naudotojų Kategorijoms	+
10.22.8 naudotojų statuso atpažinimą, pavyzdžiui, organizacijos darbuotojų arba rangovų tuose kataloguose, kurie skirti kitiems naudotojams	+
10.22.9 sistemoje laikomos informacijos išsaugojimą ir atsarginių kopijų Darymą	+
10.22.10 atsarginių planų reikalavimus ir pasirengimo priemones	+
10.23 Vykdant interneto transakcijas ar taikomos saugumo priemonės	+
10.24 Reikiamas atskirų priemonių naudojimo stebėsenos lygis turėtų būti nustatomas atliekant rizikos vertinimą. Organizacijos taikomi stebėsenos veiksmai turėtų būti suderinti su visais reikiamais teisiniais reikalavimais. Šiuo atveju turėtų būti numatyta:	
10.24.1 sankcionuota prieiga	+
10.24.2 visos privilegijuotos operacijos	+
10.24.3 nesankcionuotos prieigos mėginimai	+
10.24.4 sistemos įspėjimai ar klaidos	+
10.25 Visų organizacijoje informacijos apdorojimo sistemų laikrodžiai sinchronizuoti pagal sutartą tikslų laiko šaltinį	+

6 lent. (Ryšiu ir darbo proceduros valdymas)

11. Prieigos valdymas

13 lentelė. Prieigos valdymas

Standartas	Atitikimas įmonėje
Standarto numeracija: 11.1 Verslo veiklos prieigos valdymo reikalavimai	
11.1 Prieigos valdymo politika turėtų aiškiai nustatyti kiekvieno naudotojo arba naudotojų grupės prieigos valdymo taisykles ir teises. Prieigos valdymo priemonės yra loginės ir fizinės ir jos turi būti taikomos kartu. Naudotojams ir paslaugos teikėjams turėtų būti aiškiai suformuluoti verslo veiklos reikalavimai, kurių reikia laikytis vykdant kreipties priežiūrą	+
Standarto numeracija: 11.2 Naudotojų prieigos valdymas	
11.3 Prieigos valdymo procedura, skirta naudotojo registravimui ir išregistravimui	+
11.3.1 naudotojo unikalaus identifikatoriaus naudojimą, kad naudotojus būtų galima susieti atsakomybės saitais dėl jų veiksmų; grupinio unikalaus identifikatoriaus naudojimas turėtų būti leidžiamas tik tuo atveju, kai jis reikalingas dėl verslo veiklos ar darbo priežasčių, jis turėtų būti patvirtintas ir įformintas dokumentais	+
11.3.2 tikrinimą, ar naudotojas turi sistemos prižiūrėtojo įgaliojima naudotis informacijos sistema arba paslauga; vadovybė taip pat gali patvirtinti atskiras prieigos teises	+
11.3.3 tikrinima, ar suteiktas prieigos lygis tinka verslo veiklos tikslui ir atitinka organizacijos saugumo politiką, pavyzdžiui, ar nekliudo pareigų atskyrimui	+/-
11.3.4 naudotojams pateikiama raštiška jų prieigos teisių patvirtinimą	+
11.3.5 reikalavimą, kad naudotojai pasirašytų pareiškimą, jog jie supranta prieigos sąlygas	+
11.3.6 užtikrinimą, kad paslaugos teikėjai neaptarnautų prieigos kol neužbaigtos įgaliojimo suteikimo procedūros	+
11.3.7 oficialių įrašų apie visus įgaliotus naudotis paslauga asmenis palaikymą	+
11.3.8 nedelsiamą naudotojų, kurie pakeitė darba arba išėjo iš organizacijos, prieigos teisių panaikinima arba blokavimą	+
11.3.9 užtikrinimą, kad nereikalingi naudotojo identifikatoriai nebūtų suteikiami kitiems naudotojams	+
11.4 Privilegijos daugelio naudotojų sistemoms, kurioms reikia apsaugos nuo nesankcionuotos prieigos, suteikiamos pagal oficialų įgaliojimą	+
11.4.1 turėtų būti identifikuoti su kiekvienu sistemos produktu, pavyzdžiui, operacine sistema, duomenu bazės valdymo sistema ir kiekviena taikomaja programa susijusios prieigos privilegijos ir naudotojai, kuriems tos privilegijos bus suteikiamos	+
11.4.2 asmenims privilegijos turėtų būti suteikiamos remiantis jų poreikiu naudotis, be to, vienam atvejui po kito, t.y. tenkinami mažiausi jų funkcijų vykdymo reikalavimai ir, tiktai prireikus; ir tai turi atitikti prieigos valdymo politiką	+
11.4.3 įgaliojimo suteikimo procedūra ir įrašai apie visų privilegijų suteikimą turėtų būti prižiūrimi. Privilegijos neturėtų būti suteikiamos kol neužbaigtos įgaliojimo suteikimo procedūros	+
11.4.4 turėtų būti skatinama nusistovėjusios praktikos naudojimas, siekiant išvengti naudotojo poreikio gauti privilegijas	+
11.4.5 turėtų būti skatinama programų, kurias taikant būtų išvengta privilegijų poreikio, plėtra ir naudojimas	+
11.4.6 privilegijos turėtų būti skiriamos ne tiems, kurie yra įprasti verslo veiklos naudotojai, o kitiems naudotojams	+

Standarto numeracija: 11.3 Naudotojo atsakomybė	
11.5 Slaptažodžių skyrimas turėtų būti tvarkomas pasitelkiant oficialias tvarkymo procedūras.	+
11.5.1 naudotojai turėtų pasirašyti, jog sutinka laikytis asmeninių slaptažodžių konfidencialumo ir neatskleisti grupinių slaptažodžių pašaliniams; toks reikalavimas galėtų būti įtrauktas ir į įdarbinimo sutarties nuostatus ir sąlygas	+
11.5.2 tais atvejais, kai naudotojai patys turi susikurti savo slaptažodį, pradžioje jiems suteiktas pradinis laikinasis slaptažodis turėtų būti saugus ; turėtų būti numatyta, kad laikinąjį slaptažodį naudotojai pasikeis nedelsdami	+
11.5.3 numatytos procedūros, skirtos nustatyti naudotojū tapatumą prieš suteikiant naują ar laikinąjį slaptažodį, ar jį keičiant	+
11.5.4 laikinieji slaptažodžiai naudotojams turėtų būti suteikti saugiu būdu; juos suteikiant nedera naudotis trečiosios šalies paslaugomis ar siųsti juos neapsaugotu elektroninio laišku (atviru tekstu)	+
11.5.5 individualiems naudotojams suteikiami laikinieji slaptažodžiai turėtų būti unikalūs ir neatspėjami	+
11.5.6 naudotojai turėtų patvirtinti, kad slaptažodi gavo	+
11.5.7 kompiuterinėse sistemose laikomi slaptažodžiai turėtų būti nuolat apsaugoti	+
11.5.8 įdiegus sistemą ar programinę įrangą numatytieji pardavėjų slaptažodžiai turėtų būti pakeisti	+
11.6 Taikydama oficialias procedūras vadovybė turėtų periodiškai atlikti naudotojų prieigos teisių peržiurą	+
11.7 Iš naudotojų turėtų būti reikalaujama, kad parinkdami ir naudodami slaptažodžius, jie laikytųsi geros saugumo praktikos	+
11.8 Naudotojai turėtų užtikrinti, kad jų be priežiūros paliekama įranga būtų tinkamai apsaugota.Visi naudotojai supažindinti su saugumo reikalavimais ir procedūromis, skirtomis be priežiūros paliekamos įrangos apsaugai, ir savo atsakomybėmis dėl tokios apsaugos įgyvendinimo.	+
11.9 Taikant saugaus stalo ir saugaus ekrano politiką turėtų būti atsižvelgiama į informacijos klasifikavimą, teisinius reikalavimus ir sutarties sąlygas bei su tuo susijusias rizikas ir organizacijos kultūrinius aspektus	+
Standarto numeracija: 11.4 Tiklo prieigos valdymas	
11.10 Prieiga prie vidinio ir išorinio tinklo teikiamų paslaugų turėtų būti valdoma. Naudotojo prieiga prie tinklų ir tinko paslaugų neturėtų kelti pavojaus tinklo paslaugų saugumui	+
11.11 Naudotojams prieiga turėtų būti suteikiama tik prie tų paslaugų, kuriomis jiems aiškiai buvo suteikta teisė naudotis. Turėtų būti parengta tinklų ir tinklo paslaugų naudojimo politika.	+
11.11.1 Valdant nuotolinių naudotojų prieigą taikomi tinkami tapatumo nustatymo būdai	+
11.12 Vienas didelių tinklų saugumo valdymo metodų yra tinklų padalijimas į atskiras logines tinklo sritis, pavyzdžiui, organizacijos vidaus tinklo sritis ir išorinio tinklo sritis, kurių kiekviena apsaugoma apibrėžta saugumo aptvara. Atskirose loginėse tinklo srityse gali būti taikomi skirtingi valdymo priemonių rinkiniai, tokiu būdu atskiriant tinklo saugumo aplinkas, pavyzdžiui, viešai prieinamas sistemas, vidinius tinklus ir ypatingos svarbos turtą. Sritys turėtų būti apibrėžtos remiantis rizikos vertinimu ir skirtingais atskiros srities saugumo reikalavimais.	+
11.13 Naudotojo ryšio pajėgumai ribojami panaudojant tinklų sietuvą, kuris filtruotų duomenų srautą pagal iš anksto apibrėžtas lenteles ar taisykles.	+

11.14 Prisijungimo trukmės valdymo priemonės turėtų būti taikomos dirbant su slaptomis kompiuterinėmis programomis, ypač kai tai vyksta didelės rizikos vietose, pavyzdžiui, viešosiose arba išorinėse, už organizacijos saugumo valdymo ribų esančiose vietose.	+
11.15 Prieigos apribojimai turėtų būti grindžiami atskiru verslo veiklos programų reikalavimais. Prieigos valdymo politika turėtų atitikti organizacijos prieigos prie informacijos politiką	+
Standarto numeracija: 11.5 Operacinės sistemos prieigos valdymas	
11.16 Siekiant, kad prie operacinių sistemų galėtų prisijungti tik tam leidimą turintys naudotojai, turėtų būti naudojamos saugumo priemonės.	+
11.17 Norint sumažinti nesankcionuotos prieigos galimybę, kompiuterinėje sistemoje turėtų būti suprojektuota prisijungimo procedūra. Todėl prisijungimo metu turėtų būti atskleista kiek galima mažiau informacijos apie sistemą, kad nesankcionuotam naudotojui nebūtų suteikta nereikalinga pagalba.	+
11.18 Slaptažodžių tvarkymo sistemos turėtų būti interaktyvios ir pajėgios užtikrinti kokybiškų slaptažodžių naudojimą.	+
11.19 Darbo nutraukimo priemonė po tam tikro neveikimo laiko turėtų užverti seanso ekraną ir, dar po kurio laiko, užverti taikomosios programos langą ir atsijungti nuo tinklo.	+
Standarto numeracija: 11.6 Prieigos prie programų ir informacijos valdymas	
11.20 Loginė prieiga prie programinės įrangos ir informacijos turėtų būti leidžiama tik įgaliotiems naudotojams.	+
11.21 Atskiriant slaptas sistemas turėtų būti numatyti šie dalykai	+
11.21.1 sistemos prižiurėtojas turėtų aiškiai apibrėžti ir iforminti dokumentų taikomosios sistemos slaptumą	+
11.21.2 kai slapta taikomoji sistema veikia bendrojo naudojimo aplinkoje, taikomosios sistemos, kurių ištekliais naudojamasi bendrai ir kurioms gresia tos pačios rizikos, turėtų būti apibrėžtos ir patvirtintos slaptos taikomosios sistemos prižiurėtojo	+
Standarto numeracija: 11.7 Judrios kompiuterinės darbo priemonės ir nuotolinis darbo	
11.22 Kai naudojamos judriosios darbo priemonės, pavyzdžiui, užrašinės, delniukai, nešiojamieji kompiuteriai, lustinės kortelės ir mobilieji telefonai, imtasi ypatingų priemonių siekiant užtikrinti, kad verslo veiklos informacijai nebūtų keliamas pavojus.	+
11.22.1 Turėtų būti numatyta tinkama nuotolinės darbo vietos apsauga, pavyzdžiui, nuo įrangos ir informacijos vagystės, nesankcionuoto informacijos atskleidimo, neigaliotos nuotolinės prieigos prie vidinių organizacijos sistemų bei nuo piktnaudžiavimo šiomis darbo priemonėmis. Nuotolinis darbas turėtų būti sankcionuotas, vadovybės kontroliuojamas ir šioms darbo sąlygoms turėtų būti tinkamai pasirengta	+

12. Informacijos sistemų užsakymas, tobulinimas ir priežiūra

14 lentelė. Informacijos sistemų užsakymas, tobulinimas ir priežiūra

Standartas	Atitikimas įmonėje
Standarto numeracija: 12.1 Informacijos sistemų saugumo reikalavimai	
12.1 Nustatant valdymo priemonių reikalavimus turėtų būti numatyta, kad automatinės valdymo priemonės būtų sudėtinė sistemos dalis, ir atsižvelgta į rankinių valdymo priemonių palaikymo poreikį. Panašūs reikalavimai turėtų	+

būti keliami, kai reikia įvertinti taikomosioms verslo veiklos sistemoms taikomus programinės įrangos paketus, nepriklausomai nuo to, ar jie būtų organizacijos sukurti ar nupirkti	
12.2 Informacijos saugumo sistemos reikalavimai ir saugumo įgyvendinimo veiksmai turėtų būti taikomi jau ankstyvosiose informacijos sistemų projektavimo stadijose. Valdymo priemonės daug lengviau įgyvendinti ir prižiurėti kai jos įdiegtos projektų rengimo stadijoje, o ne jau įgyvendinant projektus arba dar vėliau dėl saugumo klaidų arba jo nebuvimo	+
Standarto numeracija: 12.2 Korektiškas programų veikimas	
12.3 Siekinat užtikrinti korektišką programų veikimą taikomosiose programose, įskaitant naudotojo patobulintas programas, turėtų būti įdiegtos reikiamos valdymo priemonės	+
12.3.1 Turėtų būti tikrinamos verslo veiklos įvedimo operacijos, esami duomenys (pavadinimai ir adresai, ribinės kredito vertės, naudotojo atskaitų numeriai), be to, lentelių parametrai (pavyzdžiui, pardavimo kainų, valiutos keitimo kursų, mokesčių tarifų)	+
12.4 Projektuojant ir įgyvendinant taikomąsias programas turėtų būti užtikrinta, kad vientisumo suardymą lemiančių apdorojimo klaidų rizika yra kiek galima sumažinta. Turėtų būti atsižvelgta į šias ypatingas sritis:	
12.4.1 papildymo, modifikavimo arba ištrynimo funkcijų, kurios taikomos duomenų keitimui, naudojimą	-
12.4.2 klaidingos programų paleidimo tvarkos arba paleidimo po buvusios apdorojimo klaidos išvengimo procedūras	+
12.4.3 programų naudojimą klaidoms ištaisyti, kad būtų užtikrintas taisyklingas duomenų apdorojimas	+
12.4.4 apsauga nuo atakų, dėl kurių įvyksta duomenų buferio perpildymas	+
12.5 Turėtų būti parengtas atitinkamu tikrinimų sąrašas, veiksmai įforminami dokumentais ir saugomi gauti rezultatai. Taikytinų tikrinimų pavyzdžiai gali būti šie:	
12.5.1 laiko arba paketo tikrinimai, siekiant suderinti duomenų failo balansus po transakcijos atnaujinimo	+
12.5.2 balanso tikrinimas, siekiant palyginti failo atvėrimo ir ankstesnio jo užvėrimo reikšmes	-
12.5.3 sistemos generuojamų įvedinių patikra	+
12.5.4 tarp centrinio ir nuotolinio kompiuterių perduodamų bei priimamų duomenų arba programinės įrangos vientisumo, autentiškumo ir kitų saugumo požymių tikrinimas	+
12.5.5 įrašų ir failų maišos kontrolinės sumos	+
12.5.6 tikrinimai, kurie laiduoja, kad taikomosios programos paleidžiamos tinkamu laiku	+
12.5.7 tikrinimai, kurie laiduoja, kad programos yra paleidžiamos tinkama tvarka, o klaidos atveju baigiamos ir kad tolesnis apdorojimas sustabdomas, kol bus ištaisytos klaidos	+
12.5.8 veiklos, susijusios su šiuo apdorojimu, registravimas	+
12.6 Taikomosios sistemos duomenų išvediniai turėtų būti patvirinti, siekiant užtikrinti, jog saugumos informacijos apdorojimas yra tikslus ir esamomis sąlygomis tinkamas. Išvedimo patvirtinimas gali apimti:	+
12.6.1 patikimumo tikrinimus, siekiant išbandyti, ar išvesties duomenys yra Priimtini	+
12.6.2 kontrolinius suderinamuosius skaiciavimus, siekiant garantuoti visų duomenų apdorojimą	-

12.6.3 pakankamos informacijos pateikimą skaitytojui arba tolesnei apdorojimo sistemai, siekiant nustatyti informacijos atitikimą, užbaigtumą, tikslumą ir klasifikavimą	+
12.6.4 reagavimo į išvedinio patvirtinimo bandymus procedūras	+
12.6.5 visų duomenų išvedimo procedūroje dalyvaujancių darbuotojų atsakomybių Apibrėžimą	+
12.6.6 visų su duomenų išvedimo patvirtinimo procedūromis susijusių veiksmų Registravimą	+
Standarto numeracija: 12.3 Šifravimo valdymo priemonės	
12.7 Rengiant šifravimo politiką, turėtų būti numatyti šie dalykai:	
12.7.1 vadovybė turėtų skatinti šifravimo metodų taikymą visoje organizacijoje, iskaitant bendruosius verslo veiklos informacijos apsaugos principus	+
12.7.2 rizikos vertinimu pagrįstas reikiamas apsaugos lygis turėtų būti nustatytas atsižvelgiant į naudojamo šifravimo algoritmo tipą, patikimumą ir kokybę	+
12.7.3 šifravimo priemonių taikymą, siekiant apsaugoti slaptą informaciją, perduodamą mobiliomis ar keiciamosiomis laikmenomis, įtaisais ar ryšio linijomis	+
12.7.4 deramą rakto valdymą, įskaitant šifravimo raktų apsaugos metodus ir šifruotos informacijos atgavimo būdus tuo atveju, kai raktai pametami, atskleidžiami ar pažeidžiami	+
12.7.5 pareigas ir atsakomybes, pavyzdžiui, kas yra atsakingas už: 1) politikos įgyvendinimą; 2) raktų valdymą, įskaitant raktų kūrimą	+
12.7.6 standartus, kuriuos reikia perimti ir veiksmingai taikyti visoje organizacijoje (t.y. kokius sprendimus taikyti atskiriems verslo veiklos procesams)	+
12.7.7 šifruotos informacijos naudojimo poveikį valdymo priemonėms, kurias taikant pasikliaujama turinio apžiūra	-
Standarto numeracija: 12.4 Sisteminių failų saugumas	
12.8 Turėtų būti valdoma prieiga prie sisteminių failų ir programos pirminio kodo, o informacijos technologijų projektai ir palaikymo veiksmai turėtų būti vykdomi saugiai. Turėtų būti rupinamasi, kad į bandymo aplinką nepatektų slaptų duomenų	+
12.9 Siekiant apsaugoti darbo duomenis, naudojamus atliekant testavimą turėtų būti vadovaujamasi:	
12.9.1 prieigos valdymo procedūros, kurios taikomos darbinėms taikomosioms sistemoms, taip pat turėtų būti taikomos ir testuojant taikomasias sistemas	+
12.9.2 kiekvieną kartą, kai testuojant taikomąją sistemą yra kopijuojama darbinė informacija, turėtų būti gautas atskiras leidimas	+/-
12.9.3 atlikus testavimą, darbinė informacija turėtų būti nedelsiant ištrinta iš testavimui naudotos taikomosios sistemos	+
12.9.4 darbinės informacijos kopijavimas ir naudojimas turėtų būti registruojamas, siekiant išlaikyti auditui reikiamus duomenis	+
Standarto numeracija: 12.3 Pirminio programos teksto prieigos valdymas	
12.10 Siekiant išvengti nesankcionuotų funkcijų įivedimo ir per klaidą atliktų pakeitimų, turėtų būti griežtai valdoma prieiga prie programos pirminio teksto ir su tuo susijusių dokumentų (pavyzdžiui, projektų, specifikacijų, patikrinimo ir patvirtinimo planų). Pirminio programos teksto atveju tai galima pasiekti saugant jį centrinėje pirminių tekstų saugykloje, pageidautina, kad tai būtų programos išteklių bibliotekos. Siekiant valdyti prieigą prie tokių programos išteklių bibliotekų taip, kad būtų sumažinta kompiuterio programų	

sugadinimo tikimybė	
12.11 Jei tai įmanoma atlikti, taikomųjų ir darbo programų keitimo valdymo proceduros turėtų sudaryti vieną visumą	
Standarto numeracija: 12.5 Kūrimo ir priežiūros saugumas	
12.12 Pardavėjo pateikti programinės įrangos paketai turėtų būti kiek galima ilgiau nemodifikuojami. Tais atvejais, kai programinės įrangos paketą reikia modifikuoti	+
12.13 Siekiant apriboti informacijos nutekėjimo riziką, pavyzdžiui, kai tam pasitelkiami paslėpti kanalai, turėtų būti imtasi šių priemonių	+
12.14 Užsakant programinės įrangos kūrimo darbus atsižvelgiama į :	
12.14.1 licencijos sąlygas, kodo nuosavybės ir intelektinės nuosavybės teises	+
12.14.2 atliekamų darbų kokybės ir tikslumo atestavimą	+
12.14.3 įsipareigojimus, prisiimamus dėl nesklandumų, už kuriuos atsakinga trečioji šalis	+
12.14.4 prieigos teises atlikto darbo kokybės ir tikslumo auditui	+
12.14.5 sutarties reikalavimus, keliamus programų kokybei ir saugumui	+
12.14.6 testavimą prieš įdiegiant, siekiant aptikti kenksmingą programą ar Trojos arklį	+
Standarto numeracija: 12.6 Techninio pažeidžiamumo valdymas	
12.15 Nustačius potencialias techninio pažeidžiamumo grėsmes, turėtų būti imtasi atitinkamų savalaikių atsakomųjų veiksmų. Siekiant užtikrinti veiksmingą techninio pažeidžiamumo procesų valdymą	+

13. Informacijos saugumo incidentų valdymas

15 lentelė. Informacijos saugumo incidentų valdymas

Standartas	**Atitiktis įmonėje**
13.1 Visiems darbuotojams, rangovams ir trečiųjų šalių atstovams turėtų būti žinoma apie jų atsakomybę pranešti apie bet kokį su informacijos saugumu susijusį įvykį kiek įmanoma greičiau. Be to, jie turėtų būti supažindinti su pranešimo apie informacijos saugumo įvykius procedūromis ir žinoti, kur tokiu atveju kreiptis	+
13.2 Siekiant išvengti informacijos saugumo incidentų, visi darbuotojai, rangovai ir treciosios šalies atstovai turėtų kiek įmanoma greiciau pranešti apie šiuos nesklandumus savo vadovybei arba tiesiogiai savo paslaugos teikė-jams. Pranešimo mechanizmas turėtų būti kiek įmanoma lengvesnis ir prieinamesnis. Jie turėtų žinoti, kad jokiomis aplinkybėmis jiems negalima patiems mėginti panaikinti įtariamų trūkumų	+
Standarto numeracija: 13.2 Informacijos saugumo incidentų ir tobulinimo valdymas	
13.3 . Turėtų būti ne tik pranešama apie informacijos saugumo įvykius ir silpnasias vietas, bet, stebėjimas. Taikant informacijos saugumo incidentų valdymo procedūras turėtų būti vadovaujamasi šiomis gairėmis:	+
13.3.1 turėtų būti numatytos procedūros, skirtos tvarkytis su įvairių tipų informacijos saugumo incidentais	+
13.3.2 be įprastų planų nenumatytiems atvejams, taikomos procedūros taip pat turėtų apimti …..	
13.3.3 turėtų būti vedami audito žurnalai ir renkami bei saugomi panašūs įrodymai, kuriuos galima būtų panaudoti	+
13.3.4 veiksmai, skirti atkurti saugumą po pažeidimo ir ištaisyti sistemos	+

klaidas turėtų būti atidžiai ir oficialiai valdomi	
13.4 Informacija, gauta atlikus informacijos saugumo incidentų įvertinimą, turėtų būti panaudojama, siekiant nustatyti pasikartojancius ar didelės įtakos turinčius incidentus	+
13.5 Turėtų būti numatytos vidinės procedūros, kurių būtų laikomasi renkant ir pateikiant įrodymus drausminiam procesui, atliekamam pačios organizacijos	+
13.5.1 įrodymų teisėtumas, t.y. ar įrodymais galima būtų remtis teisme	+
13.5.2 įrodymu pagrįstumas, t.y. įrodymų kokybė ir išsamumas	+

14 Verslo veiklos tęstinumo valdymas

16 lentelė. Verslo veiklos tęstinumo valdymas

Standartas	Atitiktis įmonėje
14.1 Informacijos saugumo įtraukimas į verslo veiklos tęstinumo procesą:	
14.1.1 organizacijai aktualiu rizikų tikimybės ir poveikio supratimą, įskaitant svarbiausių verslo veiklos procesų įdentifikavimą	+
14.1.2 viso turto, susijusio su svarbiausiomis verslo veiklos procedūromis, Įdentifikavimą	+
14.1.3. poveikio, kurį verslo veiklai gali daryti dėl informacijos saugumo incidentų įvyke pertrūkiai, supratimą (svarbu atrasti sprendimus, reguliuojančius tiek mažesnius, tiek rimtus, organizacijos gyvybingumui galinčius kelti grėsmę incidentus) ir informacijos apdorojimo priemonėms keliamų verslo veiklos tikslų nustatymą	+
14.1.4 tinkamų draudimo sutarčių sudarymą, kurios gali būti bendrojo verslo veiklos tęstinumo užtikrinimo bei darbo rizikos valdymo dalis	+
14.1.5 papildomų prevencinių ir grėsmę mažinančių valdymo priemonių įdentifikavimą ir įgyvendinimą	+
14.1.6 pakankamą finansinių, organizacinių, techninių ir aplinkos išteklių įdentifikavimą, atsižvelgiant į numatytus informacijos saugumo reikalavimus	+
14.1.7 personalo saugumo užtikrinimą bei informacijos apdorojimo priemonių ir organizacijos nuosavybės apsaugos užtikrinimą	+
14.1.8 numatytą verslo veiklos tęstinumo strategiją atitinkančių verslo veiklos tęstinumo planų, kuriuose atsižvelgiamą į informacijos saugumo reikalavimus, formulavimą ir įforminimą dokumentais	+
14.1.9 periodišką numatytų planų ir procesų bandymą ir koregavimą	+
14.1.10 užtikrinima, kad verslo veiklos tęstinumo valdymas yra pritaikytas prie organizacijos procedūrų ir struktūros; atsakomybė už verslo veiklos tęstinumo valdymą organizacijoje turėtų būti skiriama tinkamu lygmeniu	+
14.2 Atliekant verslo veiklos tęstinumo rizikos vertinimus turėtų dalyvauti visi verslo veiklos ištekliu ir procesų valdytojai. Vertinant turėtų būti atsižvelgta į visus verslo veiklos procesus ir nederėtų apsiriboti vien informacijos apdorojimo priemonių vertinimu, tačiau reikėtų atsižvelgti ir į visus su informacijos saugumu susijusius aspektus. Siekiant pilnai nustatyti organizacijos verslo veiklos tęstinumo reikalavimus, svarbu įvertinti skirtingų rizikos aspektų tarpusavio ryšius. Atliekant vertinimą, rizikos turėtų būti nustatytos, apskaiciuotos bei išdėstytos pagal grėsmių lygį ir tai turėtų būti daroma atsižvelgiant į organizacijos specifiką atitinkančius kriterijus bei tikslus, pavyzdžiui, svarbiausius išteklius, pertrūkio poveikį, didžiausią galimą prastovos trukmę ir atkūrimo prioritetus	+

14.3 Planuojant verslo veiklos tęstinumą, turėtu buti:	+
14.3.1 numatyta ir sutarta dėl visų atsakomybių ir verslo veiklos tęstinumo Procedūrų	
14.3.2 nustatytas priimtinas informacijos ar paslaugu praradimo lygis	+
14.3.3 numatytos operacinės procedūros, kurių reikia laikytis laukiant kol bus pilnai atlikti atkūrimo darbai	+
14.3.4 iformintos dokumentais numatytos procedūros ir veiksmai	+
14.3.5 personalas deramai apmokytas taikyti numatytas procedūras ir veiklas, įskaitant krizių valdymą	+/-
14.3.6 tikrinami ir atnaujinami planai	
14.4 Verslo veiklos tęstinumo planavimo struktūra turėtų atitikti nustatytus informacijos saugumo reikalavimus, joje turėtų būti numatyta:	
14.4.1 planų aktyvinimo sąlygos, aprašant prieš kiekvieno plano aktyvinimą atliekamas procedūras (kaip įvertinti situaciją, ka reikia įtraukti ir kt.	+
14.4.2 avarinės procedūros, aprašant veiksmus, kurių reikia imtis po incidento, kai kyla pavojus verslo veiklos operacijoms	+
14.4.3 atsarginės procedūros, aprašant veiksmus, kurių reikia imtis, siekiant nukreipti pagrindinius verslo veiklos veiksmus arba paslaugų palaikymą alternatyviose laikinose vietose ir per reikalingą laikotarpį atkurti verslo veiklą	+
14.4.4 laikinos darbo procedūros, kurių reikia laikytis laukiant kol bus visiškai atlikti atkūrimo darbai	+
14.4.5 atkūrimo procedūros, aprašant veiksmus, kurių reikia imtis, siekiant grįžti prie įprastu verslo veiklos operacijų	+
14.4.6 priežiūros tvarkaraštis, nurodant, kaip ir kada planas bus tikrinamas, ir plano priežiūros procedūros	+
14.4.7 supratimo, švietimo ir mokymo veikla, skirta verslo veiklos testinumo supratimui ir jo veiksmingumui užtikrinti	+
14.4.8 asmenų atsakomybės, aprašant, kas yra atsakingas už tam tikros plano sudedamosios dalies vykdyma.	+

15. Atitiktis

17 lentelė. Atitiktis

Standartas	Atitiktis įmonėje
15.1 Informacijos sistemų projektavimas, paleidimas, naudojimas ir valdymas gali būti įstatymo, reglamento ir sutarties saugumo reikalavimų objektas. Turėtų būti kreipiamasi į organizacijos teisės konsultantus arba tinkamos kvalifikacijos teisės specialistus patarimo dėl ypatingų teisinių reikalavimų. Intelektinės nuosavybes užtikrinimas.	+
15.1.1 Oficialūs dokumentai apsaugoti nuo netekties, sunaikinimo arba klastojimo, atsižvelgiant į įstatymų, reglamentų, sutarčių ar verslo veiklos reikalavimus.	+
15.1 Turėtų būti numatyta ir igyvendinta organizacijos duomenu apsauga ir privatumo politika. Su šia politika turėtų būti supažindinti visi darbuotojai, susije su asmeninės informacijos apdorojimu	+
15.2 Visi naudotojai turėtu tiksliai žinoti jiems suteiktos prieigos apimtį bei tai, kad taikomos stebėjimo proceduros, leidžiancios atsekti nesankcionuotus veiksmus. Tai galima užtikrinti, suteikiant jiems raštiškus leidimus, kurių	+

kopija jie turėtų pasirašyti, o organizacija ją saugoti. Organizacijos darbuotojai, rangovai ir trečiosios šalies atstovai turėtų būti informuoti, jog bet kokia prieiga yra draudžiama, išskyrus tą, kuriai jiems suteikiamas leidimas	
15.3 . Taikomos šifravimo valdymo priemonės turėtų atitikti visas su tuo susijusias sutartis, įstatymus ir reglamentus. Kad būtų užtikrintas atitikimas su visomis susijusiomis sutartimis, istatymais ir reglamentais, turi būti numatyta	+
15.3.1 šifravimo funkcijoms atlikti skirtos techninės ir programinės kompiuterių įrangos importo ir (arba) eksporto apribojimai	+
15.3.2 techninės ir programinės kompiuterių įrangos, papildytos šifravimo funkcijoms atlikti skirtomis priemonėmis, importo ir (arba) eksporto apribojimai	+
15.3.3 šifravimo naudojimo apribojimai	+
15.3.4 privalomi arba savo nuožiūra taikomi atitinkamų valstybės institucijų prieigos prie techninės arba programinės įrangos šifruotos informacijos metodai, skirti užtikrinti turinio konfidencialumą	+
Standarto numeracija: 15.2 Atitiktis saugumo politikoms ir standartams bei techninis suderinamumas	
15.4 Informacijos sistemų saugumas turėtų būti periodiškai peržiurimas (Šios peržiuros turėtų būti atliekamos remiantis atitinkamomis saugumo politikomis ir techninėmis platformomis, be to, informacijos sistemos turėtų būti audituojamos, ar atitinka saugumo įgyvendinimo standartus ir dokumentais įformintos saugumo valdymo priemonės	+
15.5 Techninio suderinamumo tikrinimas turėtų būti atliekamas „rankiniu budu“ (esant reikalui, pasitelkiamos ir atitinkamos programinės įrangos priemonės) patyrusio sistemos inžinieriaus ir (arba) taikant automatines priemones, gebančias sukūrti techninę ataskaitą, kuri būtų perduodama vertinti technikos specialistui	+
Standarto numeracija: 15.3 Informacijos sistemų auditas	
15.6 Siekiant kiek galima labiau sumažinti verslo veiklos pertrukiu rizika, tur!tu buti kruopščiai planuojami ir suderinami audito reikalavimai ir su operacin !s sistemos tikrinimais susije veiksmai.	+
15.6.1 audito reikalavimai turėtų būti derinami su atitinkamais vadovybės atstovais	+
15.6.2 tikrinimu ribos turėtų būti suderintos ir kontroliuojamos	+
15.6.3 atliekant tikrinimus turėtų būti naudojama prieiga tik prie skaitymui skirtos programinės įrangos ir duomenų	+
15.6.4 kita, ne skaitymo, prieiga turėtų būti leidžiama tik prie atskirų sistemos failų kopijų, kurios pasibaigus auditui turėtų būti ištrinamos arba tinkamai apsaugomos, jei pagal audito dokumentacijos reikalavimus šiuos failus būtina išlaikyti	+
15.6.5 tikrinimams atlikti skirti ištekliai turėtų būti aiškiai įdentifikuoti ir prieinami	+
15.6.6 reikalavimai, keliami specialiam arba papildomam apdorojimui, turėtų būti įdentifikuoti ir suderinti	+
15.6.7 kiekviena prieiga turėtų būti stebima ir registruojama žurnale, šitaip užtikrinant audito galimybę; svarbiu duomenų ar sistemu atveju turėtų būti registruojamas ir prieigos laikas	+
15.6.8 visos procedūros, reikalavimai ir atsakomybės turėtų būti įformintos Dokumentais	+
15.6.9 auditą atliekantys asmenys turėtų būti nepriklausomi nuo audituojamos Veiklos	+
15.7 Informacijos sistemų audito priemonės, pavyzdžiui, programinė įranga ar duomenų failai, turėtų būti atskirti nuo projektavimo ar operacinių sistemų bei nelaikomos laikmenų bibliotekose ar naudotojams prieinamose srityse,	+

nebent joms būtų skiriama papildoma apsauga	

COBIT 4.1

PO1 Planavimas ir organizavimas

IT strategijos planavimas yra reikalingas tam, kad valdyti visus IT resursus atsižvelgiant į verslo strategiją ir prioritetus. IT funkcijos ir verslo akcininkai yra atsakingi užtikrinant, kad būtų realizuotos optimalios vertybės iš projektų ir paslaugų portfelių. Strateginis planas užtikrina, kad akcininkai suprastų IT galimybes, identifikuotų žmogiškų resursų reikalingumą ir išgrynintų kokio lygio investicijų gali prireikti. Pagrindinis tikslas rasti balansą tarp IT galimybių ir realių verslo poreikių.

PO1 IT strategijos plano apibrėžimas

18 lentelė. IT strategijos plano apibrėžimas

CobiT 4.1 kontrolės	Atitiktis įmonėje
PO1.1 IT turto valdymas	+
PO1.2 Verslo ir IT reguliavimas (IT išlyginimas su verslo strategija)	+
PO1.3 Esamo našumo įvertinimas	+
PO1.4 IT strategijos planas	+
PO1.5 IT taktiniai planai	+
PO1.6 IT portfelio valdymas	+

PO2 Informacijos architektūra

Informacinių sistemų funkcijos sukuria ir reguleriai atnaujina verslo informacijos modelį ir apibrėžią kokias sistemas optimizuoti, kad būtų naudojama ši informacija. Tai iškelia tikslą sukurti korporatyvinės informacijos žodyną su organizacijos duomenų taisyklėmis, duomenų klasifikacijos schema ir saugumo lygiais.Šis procesas patobulina kokybės valdymo sprendimų priėmima, užtikrinant, kad patikima ir saugi informacija yra pateikta ir tai padeda racionalizuoti informacinų sistemų resursus, kad jie atitiktų verslo strategiją.
Pagrindinis tikslas užtikrinti optimalų informacinių sistemų sąryšį.

19 lentelė. Informacijos architektūra

CobiT 4.1 kontrolės		Atitiktis įmonėje
PO2.1 Įmonės informacijos architektūros modelis		+
PO2.2 Įmonės duomenų žodynas ir duomenų sintaksės taisyklės	7.1.1 Turto aprašai 11.1.1 Prieigos valdymo politika	+
PO2.3 Duomenų klasifikavimo gairės	7.2.1 Klasifikavimo gairės. 10.7.1 Keičiamųjų duomenų laikmenų tvarkymas. 10.8.1 Keitimosi informacija politikos ir procedūros 10.8.2 Keitimosi informacija sutartys 11.1.1 Prieigos valdymo politika	+
PO2.4 Vientisumo valdymas		+

PO3 Technologinės kryptys
Informacijos paslaugų funkcijos nustato technologijos kryptį, kad palaikytį verslą.
Pagrindinis tikslas panaudoti esamas ir naujas technologijas verslo strategijos realizavimui.

20 lentelė. Technologinės kryptys

CobiT 4.1 kontrolės		Atitiktis įmonėje
PO3.1 Technologinės krypties planavimas	5.1.2 Informacijos saugumo politikos peržiūra 14.1.1 Informacijos saugumo įtraukimas į verslo veiklos tęstinumo procesą 14.1.5 Verslo veiklos tęstinumo planų tikrinimas, priežiūra ir koregavimas	+
PO3.2 Technologijos infrastruktūros planavimas		+
PO3.3 Ateities tendencijų ir reguliavimų stebėjimas	6.1.1 Vadovybės įsipareigojimas užtikrinti informacijos saugumą	+
PO3.4 Technologijos standartai	10.3.2 Sistemų priėmimas 10.8.2 Keitimosi informacija sutartys 11.7.2 Nuotolinis darbas	+
PO3.5 IT architektūros gairės ir standartai	6.1.1 Vadovybės įsipareigojimas užtikrinti informacijos saugumą	+

PO4 IT organizacinę struktūrą ir roles
IT organizacija yra apibrėžta atsižvelgiant į reikalavimus personalui, sugebejimams, funkcijoms, atsakingumui, įgaliojimui, rolei ir vadovavimui. Tokia organizacija yra įtvrintinta į IT procesų konstrukciją kuri užtikriną skaidrumą ir kontrę. Pagrindinis tikslas užtikrinti vidinių IT paslaugų teikimą.

21 lentelė. IT organizacinė struktūra ir vaidmenys

CobiT 4.1 kontrolės		Atitiktis įmonėje
PO4.1 IT procedūrų konstrukcija		+
PO4.2 IT strategijos komitetas		+
PO4.3 IT valdymo komitetas	6.1.1 Vadovybės įsipareigojimas užtikrinti informacijos saugumą	+
PO4.4 Organizacijos IT funkcijos	6.1.1 Vadovybės įsipareigojimas užtikrinti informacijos saugumą 6.1.2 Informacijos saugumo koordinavimas 6.1.3 Atsakomybės už informacijos saugumą skyrimas	+
PO4.5 IT organizaciniai principai	6.1.1 Vadovybės įsipareigojimas užtikrinti informacijos saugumą 6.1.2 Informacijos saugumo koordinavimas	+
PO4.6 Rolių ir atsakomybės įkūrimas	6.1.2 Informacijos saugumo koordinavimas 6.1.3 Atsakomybės už informacijos saugumą skyrimas 6.1.5 Konfidencialumo sutartys 8.1.1 Įsipareigojimai ir atsakomybės 8.1.2 Patikra 8.1.3 Įdarbinimo nuostatai ir sąlygos 8.2.2 Informacijos saugumo supratimas, švietimas ir mokymas 15.1.4 Duomenų apsauga ir asmeninės informacijos privatumas	+

PO4.7 Atsakomybė už IT kokybę patikimumą		+
PO4.8 Atsakomybė už riziką ir saugumą	6.1.1 Vadovybės įsipareigojimas užtikrinti informacijos saugumą 6.1.2 Informacijos saugumo koordinavimas 6.1.3 Atsakomybės už informacijos saugumą skyrimas 8.1.1 Įsipareigojimai ir atsakomybės 8.2.1 Vadovybės atsakomybės 8.2.3 Drausminė procedūra 15.1.1 Galiojantys įstatymai 15.1.2 Intelektinės nuosavybės teisės 15.1.3 Organizacijos oficialių dokumentų apsauga 15.1.4 Duomenų apsauga ir asmeninės informacijos privatumas 15.1.6 Šifravimo valdymo priemonių reglamentavimas 15.2.1 Atitiktis saugumo politikoms ir standartams	+
PO4.9 Duomenų ir sistemų nuosavybė	6.1.3 Atsakomybės už informacijos saugumą skyrimas 7.1.2 Turto valdymas 9.2.5 Įrangos, esančios ne organizacijos patalpose, saugumas	+
PO4.10 Priežiūra	6.1.2 Informacijos saugumo koordinavimas 6.1.3 Atsakomybės už informacijos saugumą skyrimas 7.1.3 Priimtinas turto naudojimas 8.2.1 Vadovybės atsakomybės	+
PO4.11 Pareigų atskyrimas	8.2.1 Vadovybės atsakomybės 10.1.3 Pareigų atskyrimas 10.1.4 Kūrimo, testavimo ir eksploatavimo priemonių atskyrimas 10.6.1 Tinklo valdymo priemonės	+
PO4.12 IT personalas (skaičius ir kompetencija)		+
PO4.13 Esminis IT personalas (pagrindinių rolių apibrėžimas)		+/-
PO4.14 Sutartys ir procedūros su personalų	6.1.5 Konfidencialumo sutartys 6.2.1 Rizikų, susijusių su išorinėmis šalimis, nustatymas 6.2.3 Saugumo reikalavimai sutartyse su trečiosiomis šalimis 9.1.5 Darbas saugiosiose vietose 15.1.5 Netinkamo naudojimosi informacijos apdorojimo priemonėmis prevencija	+
PO4.15 Struktūra ir vaidmenys	6.1.6 Ryšys su specialiomis interesų grupėmis 6.1.7 Ryšys su valdžios institucijomis	+

PO5 IT investicijos
Pagrindinis tikslas užtikrinti IT finansavimą ir finansų panaudojimo kontrolę.

22 lentelė. IT investicijos

CobiT 4.1 kontrolės		Atitiktis įmonėje
PO5.1 Finansinio valdymo principai		+
PO5.2 IT biudžeto prioritizavimas		+
PO5.3 IT biudžetavimas	5.1.2 Informacijos saugumo politikos peržiūra	+
PO5.4 Išlaidų valdymas	5.1.2 Informacijos saugumo politikos peržiūra 13.2.2 Mokymasis iš informacijos saugumo incidentų	+
PO5.5 Nuolaidų valdymas		+

16 lent. (IT investicijos)

PO6 Vadovybės tikslai ir kryptys
Pagrindinis tikslas užtikrinti, kad darbuotojai žino ir supranta vadovybės iškeltus IT tikslus.

CobiT 4.1 kontrolės		Atitiktis įmonėje
PO6.1 IT politika ir kontrolių aplinka	5.1.1 Informacijos saugumo politikos dokumentas 13.2.1 Atsakomybės ir procedūros	+
PO6.2 Įmonės IT riziką ir kontrolių principai	5.1.1 Informacijos saugumo politikos dokumentas 6.2.2 Saugumo reikalavimai dirbant su klientais 7.1.3 Priimtinas turto naudojimas 8.2.2 Informacijos saugumo supratimas, švietimas ir mokymas 8.3.2 Turto grąžinimas 9.1.5 Darbas saugiosiose vietose 9.2.7 Nuosavybės perkėlimas 10.7.3 Informacijos priežiūros procedūros 10.8.1 Keitimosi informacija politikos ir procedūros 10.9.3 Viešoji informacija 11.1.1 Prieigos valdymo politika 11.3.1 Slaptažodžių naudojimas 11.3.2 Be priežiūros paliekama naudotojo įranga 11.3.3 Saugaus stalo ir saugaus ekrano politika 11.7.1 Judriosios darbo vietos ir ryšio priemonės 11.7.2 Nuotolinis darbas 12.3.1 Šifravimo valdymo priemonių naudojimo politika 15.1.2 Intelektinės nuosavybės teisės 15.1.5 Netinkamo naudojimosi informacijos apdorojimo priemonėmis prevencija 15.2.1 Atitiktis saugumo politikoms ir standartams	+
PO6.3 IT politikų valdymas	5.1.1 Informacijos saugumo politikos dokumentas	+

	5.1.2 Informacijos saugumo politikos peržiūra 6.1.1 Vadovybės įsipareigojimas užtikrinti informacijos saugumą 8.1.1 Įsipareigojimai ir atsakomybės	
PO6.4 Politika, standartų ir standartų vystimas	6.1.1 Vadovybės įsipareigojimas užtikrinti informacijos saugumą 6.1.8 Nepriklausoma informacijos saugumo peržiūra 6.2.3 Saugumo reikalavimai sutartyse su trečiosiomis šalimis 8.2.2 Informacijos saugumo supratimas, švietimas ir mokymas	+
PO6.5 IT tikslų ir krypčių ryšiai	5.1.1 Informacijos saugumo politikos dokumentas 6.1.1 Vadovybės įsipareigojimas užtikrinti informacijos saugumą 6.1.2 Informacijos saugumo koordinavimas	+

PO7 žmogiškų resursų valdymas
Pagrindinis tikslas įdarbinti ir išlaikyti kompetetingą IT darbuotojų komandą.

24 lentelė. Žmogiškųjų išteklių valdymas

CobiT 4.1 kontrolės		Atitiktis įmonėje
PO7.1 Personalo įdarbinimas ir išlaikymas	8.1.1 Įsipareigojimai ir atsakomybės 8.1.2 Patikra 8.1.3 Įdarbinimo nuostatai ir sąlygos	+
PO7.2 Personalo kompetencijos	8.1.1 Įsipareigojimai ir atsakomybės 8.2.2 Informacijos saugumo supratimas, švietimas ir mokymas	+
PO7.3 Vaidmenys ir atsakomybės	8.1.1 Įsipareigojimai ir atsakomybės 8.1.3 Įdarbinimo nuostatai ir sąlygos 8.2.1 Vadovybės atsakomybės	+
PO7.4 Personalo mokymas	8.2.2 Informacijos saugumo supratimas, švietimas ir mokymas	+
PO7.5 Dependence upon individuals		+
PO7.6 Personalo išgryninimo procedūros	8.1.2 Patikra	+
PO7.7 Darbuotojų darbo našumo vertinimas	8.2.2 Informacijos saugumo supratimas, švietimas ir mokymas	+
PO7.8 Darbo pakeitimas ir panaikinimas	8.2.3 Drausminė procedūra 8.3.1 Atsakomybė, nustojus galioti darbo sutarčiai 8.3.2 Turto grąžinimas 8.3.3 Prieigos teisių panaikinimas	+

PO8 Kokybės valdymas
Pagrindinis tikslas užtikrinti teisinių ir sutartinių reikalavimų vykdymą IT srityje.

25 lentelė. Kokybės valdymas

CobiT 4.1 kontrolės		Atitiktis įmonėje
PO8.1 Kokybės valdymo sistema		+
PO8.2 IT standartų ir kokybės praktikos		+
PO8.3 Plėtros standartai	6.1.5 Konfidencialumo sutartys	+

	6.2.3 Saugumo reikalavimai sutartyse su trečiosiomis šalimis 12.5.5 Užsakomasis programinės įrangos kūrimas	
PO8.4 Klientai (į klientus orentuotas kokybės valdymas)		+
PO8.5 Tęstinumo tobulinimas.		+
PO8.6 Kokybės matavimai ir peržiūra		+

PO9 IT rizikų valdymas
Pagrindinis tikslas užtikrinti, kad rizikos faktoriai yra identifikuoti ir pašalinti

26 lentelė. IT rizikų valdymas

CobiT 4.1 kontrolės		Atitiktis įmonėje
PO9.1 IT rizikų valdymo gidas	14.1.1 Informacijos saugumo įtraukimas į verslo veiklos tęstinumo procesą 14.1.2 Verslo veiklos tęstinumas ir rizikos vertinimas	+
PO9.2 Rizikų konteksto nustatymas	14.1.1 Informacijos saugumo įtraukimas į verslo veiklos tęstinumo procesą 14.1.2 Verslo veiklos tęstinumas ir rizikos vertinimas	+
PO9.3 Įvykių įdentifikavimas	13.1.1 Pranešimai apie informacijos saugumo įvykius 13.1.2 Pranešimai apie saugumo silpnąsias vietas	+
PO9.4 Rizikų įvertinimas	5.1.2 Informacijos saugumo politikos peržiūra 14.1.2 Verslo veiklos tęstinumas ir rizikos vertinimas	+
PO9.5 Reagavimas į rizikas		+
PO9.6 Rizikų valdymo plano palaikymas		+

19 lent. (IT rizikų valdymas)

PO10 IT projektų valdymas
Pagrindinis tikslas nustatyti uždavinius, baigti projektus laiku ir biudžeto rėmuose.

27 lentelė. IT projektų valdymas

CobiT 4.1 kontrolės	Atitiktis įmonėje
PO10.1 Programos valdymo gidas	+
PO10.2 Projekto valdymo gidas	+
PO10.3 Projekto valdymo vizija	+
PO10.4 Akcininkų sankcijos (*angl. commitment*)	+
PO10.5 Projekto ribos	+
PO10.6 Projekto fazės iniciacija	+
PO10.7 Projekto plano integravimas	+
PO10.8 Projekto resursai	+
PO10.9 Projekto rizikų valdymas	+
PO10.10 Projekto kokybės planas	+

PO10.11 Projekto pakeitymų valdymas	+
PO10.12 Projekto planavimas naudojant patikimumo metodus	+
PO10.13 Projekto stebėjimas	+
PO10.14 Projekto uždarymas	+

Pirkimai ir įdiegimas
Naujų aplikacijų ar funkcijų poreikis reikalauja, kad būtų atlikta analize prieš įsigijima ar diegimą, kad užtikrinti verslo reikalavimus efektyviais ir saugiais būdais.

AI1 automatizavimo sprendimų paieška
Pagrindinis tikslas rasti tinkamus ir optimalius būdus patenkinti vartotojų poreikius

28 lentelė. Automatizavimo sprendimų paieška

CobiT 4.1 kontrolės		Atitiktis įmonėje
AI1.1 Verslo funcionio ir techninių reikalavimų apibrėžimas ir palaikymas	8.2.2 Informacijos saugumo supratimas, švietimas ir mokymas 10.1.1 Darbo procedūrų įforminimas dokumentais 10.3.2 Sistemos priėmimas	+
AI1.2 Rizikų analizės raportavimas	11.6.2 Slaptų sistemų atskyrimas 12.1.1 Saugumo reikalavimų analizė ir aprašas	+
AI1.3 Alternatyvių sprendimų identifikavimas		+
AI1.4 Reikalavimų patvirtinimas	10.3.2 Sistemos priėmimas	+

AI2 Programinės įrangos įsigyjimas ir priežiūra
Pagrindinis tikslas teikti automatizuotas funkcijas, padedančias verslo procesams

29 lentelė. Programinės įrangos įsigijimas ir priežiūra

CobiT 4.1 kontrolės		Atitiktis įmonėje
AI2.1 Aukšo lygio (*angl. High-level*) dizainas		+
AI2.2 Detalizuotas dizainas		+
AI2.3 Aplikacijų kontrolė ir auditaviškumas	10.10.1 Audito registravimas 10.10.5 Klaidų registravimas 12.2.1 Įvedinių patikra 12.2.2 Vidinio informacijos apdorojimo valdymas 12.2.3 Pranešimų vientisumas 12.2.4 Išvedinių patikra 13.2.3 Įrodymų rinkimas 15.3.1 Informacijos sistemų audito valdymo priemonės 15.3.2 Informacijos sistemų audito priemonių apsauga	+
AI2.4 Aplikacijų saugumas ir pasiekiamumas	7.2.1 Klasifikavimo gairės 10.3.2 Sistemos priėmimas 11.6.2 Slaptų sistemų atskyrimas 12.1.1 Saugumo reikalavimų analizė ir aprašas 12.2.3 Pranešimų vientisumas 12.3.1 Šifravimo valdymo priemonių naudojimo politika 12.4.3 Pirminio programos teksto	+/-

	prieigos valdymas 12.5.2 Techninė programos peržiūra pakeitus operacinę sistemą 12.5.4 Informacijos nutekėjimas 15.3.2 Informacijos sistemų audito priemonių apsauga	
AI2.5 Įsigitos programinės įrangos konfigūracija ir implementacija	12.5.3 Programinės įrangos paketų keitimų apribojimai	+
AI2.6 Esamų sistemų atnaujinimas	12.5.1 Keitimų valdymo procedūros	+
AI2.7 Programinės įrangos kūrimas	12.5.5 Užsakomasis programinės įrangos kūrimas	+
AI2.8 Programinės įrangos kokybės užtikrinimas	10.3.2 Sistemos priėmimas	+
AI2.9 Aplikacijos reikalavimų valdymas		+
AI2.10 Programinės įrangos palaikymas ir priežiūra		+

AI3 Techninės infrastruktūros įsigyjimas ir pirežiūra
Pagrindinis tikslas suteikti platformas, būtinas programinės įrangos funkcionavimui

30 lentelė. Techninės infrastruktūros įsigijimas ir pirežiūra

CobiT 4.1 kontrolės		Atitiktis įmonėje
AI3.1 Technologinės infrastruktūros įsigyjimo planas		+
AI3.2 Infrastruktūros resursų apsauga ir pasiekiamumo palaikymas	12.1.1 Saugumo reikalavimų analizė ir aprašas	+
AI3.3 Infrastruktūros valdymas	9.1.5 Darbas saugiosiose vietose 9.2.4 Įrangos priežiūra 12.4.2 Sistemos testavimo duomenų apsauga 12.5.2 Techninė programos peržiūra pakeitus operacinę sistemą 12.6.1 Techninio pažeidžiamumo valdymas	+
AI3.4 Testavimo aplinka	10.1.4 Kūrimo, testavimo ir eksploatavimo priemonių atskyrimas	+

AI4 IT naudojimo procedūrų sukūrimas ir atnaujinimas
Pagrindinis tikslas užtikrinti, kad vartotojai panaudoja programinę įrangą ir technologijas tinkamai, pagal paskirtį

31 lentelė. IT naudojimo procedūrų sukūrimas ir atnaujinimas

CobiT 4.1 kontrolės		Atitiktis įmonėje
AI4.1 Eksplotacijos sprendimų planavimas		+
AI4.2 Žinių perdavimas verslo valdymui		+
AI4.3 Žinių perdavimas galutiniams vartotojams		+
AI4.4 Žinių perdavimas palaikymui	10.1.1 Darbo procedūrų įforminimas dokumentais 10.3.2 Sistemos priėmimas 10.7.4 Sistemos dokumentacijos saugumas 13.2.2 Mokymasis iš informacijos saugumo incidentų	+

AI5 Sistemų diegimas ir akreditacija

Pagrindinis tikslas užtikrinti, kad programinė įranga tinka pageidaujamai paskirčiai

32 lentelė. Sistemų diegimas ir akreditacija

CobiT 4.1 kontrolės		Atitiktis įmonėje
AI5.1 Įsigijimo kontrolė	6.1.5 Konfidencialumo sutartys	+
AI5.2 Sutarčių su tiekėjais valdymas	6.1.5 Konfidencialumo sutartys 6.2.3 Saugumo reikalavimai sutartyse su trečiosiomis šalimis 10.8.2 Keitimosi informacija sutartys 12.5.5 Užsakomasis programinės įrangos kūrimas	+
AI5.3 Tiekiejų pasirinkimo procedūros		+
AI5.4 IT resursu akreditacija		+

AI6 IT sistemų pokyčių kontrolė
Pagrindinis tikslas minimizuoti neautorizuotų pakeitimų galimybę

33 lentelė. IT sistemų pokyčių kontrolė

CobiT 4.1 kontrolės		Atitiktis įmonėje
AI6.1 Pakeitimų standartai ir procedūros	10.1.2 Keitimų valdymas 12.5.3 Programinės įrangos paketų keitimų apribojimai	+
AI6.2 Įtakos apibrėžimas, prioritizavimas ir autorizavimas	10.1.2 Keitimų valdymas 12.5.1 Keitimų valdymo procedūros 12.5.3 Programinės įrangos paketų keitimų apribojimai 12.6.1 Techninio pažeidžiamumo valdymas	+
AI6.3 Kritiniai pakeitimai	10.1.2 Keitimų valdymas 11.5.4 Sistemos paslaugų programų naudojimas 12.5.1 Keitimų valdymo procedūros 12.5.3 Programinės įrangos paketų keitimų apribojimai 12.6.1 Techninio pažeidžiamumo valdymas	+
AI6.4 Pakeitimų statuso stebejimas ir raportavimas	10.1.2 Keitimų valdymas	+
AI6.5 Pakeitimų proceso uždarymas ir dokumentacija	10.1.2 Keitimų valdymas	+

Tiekimas ir palaikymas
DS1 IT paslaugų lygio apibrėžimas ir užtikrinimas.
Pagrindinis tikslas pasiekti bendrą supratimą apie tai, koks aptarnavimo lygis yra reikalingas

34 lentelė. IT paslaugų lygio apibrėžimas ir užtikrinimas

CobiT 4.1 kontrolės		Atitiktis įmonėje
DS1.1 Paslaugų lygio valdymo gidas	10.2.1 Paslaugų teikimas	+
DS1.2 Paslaugų apibrėžimas	10.2.1 Paslaugų teikimas	+
DS1.3 Paslaugų lygio sutartis	10.2.1 Paslaugų teikimas	+
DS1.4 Operacinio lygio sutartis		+

DS1.5 Stebėjimas ir raportavimas apie paslaugų lygio priskirimą	10.2.2 Trečiosios šalies teikiamų paslaugų stebėsena ir peržiūra 10.2.3 Trečiosios šalies paslaugų keitimo valdymas	+
DS1.6 Paslaugų lygio sutartčių peržiūra		+

DS2 Trečiomis šalimis tiekiamų paslaugų kontrolė
Pagrindinis tikslas užtikrinti, kad trečiųjų šalių vieta ir uždaviniai yra aiškiai apibrėžti, yra vykdomi ir tenkina vartotojus

35 lentelė. Trečiomis šalimis tiekiamų paslaugų kontrolė

CobiT 4.1 kontrolės		Atitiktis įmonėje
DS2.1 Visų ryšių su tiekėjais įdentifikavimas	6.2.1 Rizikų, susijusių su išorinėmis šalimis, nustatymas	+
DS2.2 Ryšių su tiekėjais valdymas	6.2.3 Saugumo reikalavimai sutartyse su trečiosiomis šalimis 10.2.3 Trečiosios šalies paslaugų keitimo valdymas 15.1.4 Duomenų apsauga ir asmeninės informacijos privatumas	+
DS2.3 Tiekėjų rizikų vertinimas	6.2.1 Rizikų, susijusių su išorinėmis šalimis, nustatymas 6.2.3 Saugumo reikalavimai sutartyse su trečiosiomis šalimis 8.1.2 Patikra 8.1.3 Įdarbinimo nuostatai ir sąlygos 10.2.3 Trečiosios šalies paslaugų keitimo valdymas 10.8.2 Keitimosi informacija sutartys	+/-
DS2.4 Tiekėjų našumo stebėjimas	6.2.3 Saugumo reikalavimai sutartyse su trečiosiomis šalimis 10.2.1 Paslaugų teikimas 10.2.2 Trečiosios šalies teikiamų paslaugų stebėsena ir peržiūra 12.4.2 Sistemos testavimo duomenų apsauga 12.5.5 Užsakomasis programinės įrangos kūrimas	+

DS3 Sistemų pajėgumų ir apkrovų kontrolė
Pagrindinis tikslas užtikrinti adekvatų sistemų pajėgumą, optimalų panaudojimą

36 lentelė. Sistemų pajėgumų ir apkrovų kontrolė

CobiT 4.1 kontrolės		Atitiktis įmonėje
DS3.1 Našumo planavimas	10.3.1 Pajėgumų valdymas	+
DS3.2 Esamas našumas	10.3.1 Pajėgumų valdymas	+
DS3.3 Ateityje numatomas našumas	10.3.1 Pajėgumų valdymas	+
DS3.4 IT resursų buvimas		+
DS3.5 Stebėjimas ir raportavimas		+

DS4 Nuolatinio sistemų funkcionalumo užtikrinimas

Pagrindinis tikslas užtikrinti, kad informacinės sistemos veikia, ir netgi didelės problemos atveju nuostoliai bus minimizuoti

37 lentelė. Nuolatinio sistemų funkcionalumo užtikrinimas

CobiT 4.1 kontrolės		Atitiktis įmonėje
DS4.1 IT tęstinumo gidas	6.1.6 Ryšys su valdžios institucijomis 6.1.7 Ryšys su specialiomis interesų grupėmis 14.1.1 Informacijos saugumo įtraukimas į verslo veiklos tęstinumo procesą management process 14.1.2 Verslo veiklos tęstinumas ir rizikos vertinimas 14.1.4 Verslo veiklos tęstinumo planavimo struktūra	+
DS4.2 IT tęstinumo planas	6.1.6 Ryšys su valdžios institucijomis 6.1.7 Ryšys su specialiomis interesų grupėmis 14.1.3 Tęstinių planų, apimančių informacijos saugumą, sudarymas ir įgyvendinimas	+
DS4.3 Kritiniai IT resursai	14.1.1 Informacijos saugumo įtraukimas į verslo veiklos tęstinumo procesą management process 14.1.2 Verslo veiklos tęstinumas ir rizikos vertinimas	+
DS4.4 IT tęstinumo plano palaikymas	14.1.5 Verslo veiklos tęstinumo planų tikrinimas, priežiūra ir koregavimas	+
DS4.5 IT tęstinumo plano testavimas	14.1.5 Verslo veiklos tęstinumo planų tikrinimas, priežiūra ir koregavimas	+
DS4.6 Apmokymai susije su IT tęstinumo planu	14.1.5 Verslo veiklos tęstinumo planų tikrinimas, priežiūra ir koregavimas	+/-
DS4.7 IT tęstinumo plano distribucija	14.1.5 Verslo veiklos tęstinumo planų tikrinimas, priežiūra ir koregavimas	+
DS4.8 IT paslaugų atsatymas ir atnaujinimas	14.1.1 Informacijos saugumo įtraukimas į verslo veiklos tęstinumo procesą 14.1.3 Tęstinių planų, apimančių informacijos saugumą, sudarymas ir įgyvendinimas	+
DS4.9 Rezervinių kopijų saugojimas atskirai nuo produkcinių sistemų	10.5.1 Atsarginės informacijos kopijos	+
DS4.10 Peržiūros po atnaujinimų ir atstatymų	14.1.5 Verslo veiklos tęstinumo planų tikrinimas, priežiūra ir koregavimas	+

DS5 Sistemų saugumo užtikrinimas

Pagrindinis tikslas apsaugoti informaciją nuo neautorizuoto priėjimo, paskleidimo, pakeitimo, praradimo.

38 lentelė. Sistemų saugumo užtikrinimas

CobiT 4.1 kontrolės		Atitiktis įmonėje
DS5.1 IT saugumo valdymas	6.1.1 Vadovybės įsipareigojimas užtikrinti informacijos saugumą 6.1.2 Informacijos saugumo koordinavimas 6.2.3 Saugumo reikalavimai sutartyse su trečiosiomis šalimis 8.2.2 Informacijos saugumo supratimas, švietimas ir mokymas	+
DS5.2 IT saugumo planas	5.1.1 Informacijos saugumo politikos dokumentas 5.1.2 Informacijos saugumo politikos peržiūra 6.1.2 Informacijos saugumo koordinavimas 6.1.5 Konfidencialumo sutartys 8.2.2 Informacijos saugumo supratimas, švietimas ir mokymas 11.1.1 Prieigos valdymo politika 11.7.1 Judriosios darbo vietos ir ryšio priemonės 11.7.2 Nuotolinis darbas	+
DS5.3 Tapatumo valdymas	11.2.3 Naudotojų slaptažodžių tvarkymas 11.3.1 Slaptažodžių naudojimas 11.4.1 Tinklo paslaugų naudojimo politika 11.5.1 Saugios prisijungimo procedūros 11.5.2 Naudotojo atpažinimas ir tapatumo nustatymas 11.5.3 Slaptažodžių tvarkymo sistema 11.5.5 Darbo seanso nutraukimas 11.5.6 Prisijungimo laiko ribojimas 11.6.1 Informacijos prieigos ribojimas	+
DS5.4 Sisteminių vartotojų valdymas	6.1.5 Konfidencialumo sutartys 6.2.1 Rizikų, susijusių su išorinėmis šalimis, nustatymas 6.2.2 Saugumo reikalavimai dirbant su klientais 8.1.1 Įsipareigojimai ir atsakomybės 8.3.1 Atsakomybė, nustojus galioti darbo sutarčiai 8.3.3 Prieigos teisių panaikinimas 10.1.3 Pareigų atskyrimas 11.1.1 Prieigos valdymo politika 11.2.1 Naudotojų registravimas 11.2.2 Privilegijų valdymas 11.2.4 Naudotojų prieigos teisių peržiūra	+
DS5.5 Saugumo testavimas ir stebėjimas	11.3.1 Slaptažodžių naudojimas 11.5.1 Saugios prisijungimo procedūros 11.5.3 Slaptažodžių tvarkymo sistema 11.6.1 Informacijos prieigos ribojimas	+

DS5.6 Saugumo incidentų apibrėžimas	6.1.8 Nepriklausoma informacijos saugumo peržiūra 10.10.2 Stebėsenos sistemos naudojimas 10.10.3 Žurnalo duomenų apsauga 10.10.4 Administratoriaus ir operatoriaus žurnalai 12.6.1 Techninio pažeidžiamumo valdymas 13.1.2 Pranešimai apie saugumo silpnąsias vietas 15.2.2 Techninio suderinamumo tikrinimas 15.3.1 Informacijos sistemų audito valdymo priemonės	+
DS5.7 Saugumo technologijų apsauga	8.2.3 Drausminė procedūra 13.1.1 Pranešimai apie informacijos saugumo įvykius 13.1.2 Pranešimai apie saugumo silpnąsias vietas 13.2.1 Atsakomybės ir procedūros 13.2.3 Įrodymų rinkimas	+
DS5.8 Šifravimo raktų valdymas	9.1.6 Viešos prieigos, pristatymo ir krovimo vietos 9.2.1 Įrangos vietos parinkimas ir apsauga 9.2.3 Kabelių apsauga 10.6.2 Tinklo paslaugų saugumas 10.7.4 Sistemos dokumentacijos saugumas 10.10.1 Audito registravimas 10.10.3 Žurnalo duomenų apsauga 10.10.4 Administratoriaus ir operatoriaus žurnalai 10.10.5 Klaidų registravimas 10.10.6 Laikrodžių sinchronizavimas 11.3.2 Be priežiūros paliekama naudotojo įranga 11.3.3 Saugaus stalo ir saugaus ekrano politika 11.4.3 Tinklų įrangos atpažinimas 11.4.4 Nuotolinė diagnostinio ir sąrankos prievado apsauga 11.5.1 Saugios prisijungimo procedūros 11.5.4 Sistemos paslaugų programų naudojimas 11.5.5 Darbo seanso nutraukimas 11.5.6 Prisijungimo laiko ribojimas 11.6.2 Slaptų sistemų atskyrimas 11.7.1 Judriosios darbo vietos ir ryšio priemonės 11.7.2 Nuotolinis darbas 12.4.1 Operacinės programinės įrangos valdymas 12.6.1 Techninio pažeidžiamumo valdymas 13.1.2 Pranešimai apie saugumo silpnąsias vietas 13.2.3 Įrodymų rinkimas 15.2.2 Techninio suderinamumo tikrinimas	+

	15.3.2 Informacijos sistemų audito priemonių apsauga	
DS5.9 Neleistinos programinės įrangos draudimas, detektavimas ir šalinimas	10.4.1 Apsauga nuo kenksmingų programų and correction 10.4.2 Apsauga nuo mobiliųjų programų	+
DS5.10 Tinklo saugumas	6.2.1 Rizikų, susijusių su išorinėmis šalimis, nustatymas 10.6.1 Tinklo valdymo priemonės 10.6.2 Tinklo paslaugų saugumas 11.4.1 Tinklo paslaugų naudojimo politika 11.4.2 Išorinio ryšio naudotojų tapatumo nustatymas 11.4.3 Tinklų įrangos atpažinimas 11.4.4 Nuotolinė diagnostinio ir sąrankos prievado apsauga 11.4.5 Tinklų atskyrimas 11.4.7 Tinklo maršrutų valdymas 11.6.2 Slaptų sistemų atskyrimas	+
DS5.11 Jautrios informacijos pasikeitimas	6.1.5 Konfidencialumo sutartys 6.2.1 Rizikų, susijusių su išorinėmis šalimis, nustatymas 10.8.1 Keitimosi informacija politikos ir procedūros 10.8.2 Keitimosi informacija sutartys 10.8.3 Fizinių duomenų laikmenų pervežimas 10.8.4 Elektroninis susirašinėjimas 10.9.1 Elektroninė prekyba 11.4.2 Išorinio ryšio naudotojų tapatumo nustatymas	+

DS6 IT kaštų įdentifikavimas ir paskirstymas
Pagrindinis tikslas užtikrinti suvokimą apie realią IT paslaugų kainą.

39 lentelė. IT sąnaudų įdentifikavimas ir paskirstymas

CobiT 4.1 kontrolės	Atitiktis įmonėje
DS6.1 Paslaugų apibrėžimas	+
DS6.2 IT apskaita	+
DS6.3 Kainų modeliavimas ir apmokestinimas	+
DS6.4 Kainų modelio valdymas	+

DS7 Vartotojų apmokymas
Pagrindinis tikslas užtikrinti, kad vartotojai naudojasi technologija, yra supažindinti su rizika ir atsakomybe.

40 lentelė. Vartotojų apmokymas

CobiT 4.1 kontrolės		Atitiktis įmonėje
DS7.1 Mokymų poreikio įdentifikavimas	8.2.2 Informacijos saugumo supratimas, švietimas ir mokymas	+
DS7.2 Mokymų užtikrinimas	8.2.2 Informacijos saugumo supratimas, švietimas ir mokymas	+

DS7.3 Mokymų įvertinimas	+

DS8 Pagalbos vartotojams tiekimas
Pagrindinis tikslas užtikrinti, kad vartotojų patirtos problemos yra sprendžiamos

41 lentelė. Pagalbos vartotojams tiekimas

CobiT 4.1 kontrolės		Atitiktis įmonėje
DS8.1 Techninė pagalba (*angl. service desk*)	14.1.4 Verslo veiklos tęstinumo planavimo struktūra	+
DS8.2 Vartotojų skundų registravimas	13.1.1 Pranešimai apie informacijos saugumo įvykius 13.1.2 Pranešimai apie saugumo silpnąsias vietas 13.2.1 Atsakomybės ir procedūros 13.2.3 Įrodymų rinkimas	+
DS8.3 Incidentų eskalavimas	13.1.2 Pranešimai apie saugumo silpnąsias 13.2.3 Įrodymų rinkimas 14.1.1 Informacijos saugumo įtraukimas į verslo veiklos tęstinumo procesą 14.1.4 Verslo veiklos tęstinumo planavimo struktūra	+
DS8.4 Incidentų uždarymas	13.2.2 Mokymasis iš informacijos saugumo incidentų 13.2.3 Įrodymų rinkimas	+
DS8.5 Raportavimas(raportavimas apie paslaugų našuma ir kokybę)	13.2.2 Mokymasis iš informacijos saugumo incidentų	+

DS9 Sistemų konfigūracijos kontroliavimas
Pagrindinis tikslas identifikuoti visus IT komponentus, patikrinti jų fizinį egzistavimą, užkirsti kelią neleistiniems pakeitimams.

42 lentelė. Sistemų konfigūracijos kontroliavimas

CobiT 4.1 kontrolės		Atitiktis įmonėje
DS9.1 Konfigūracijos repozitoriumas	7.2.2 Informacijos žymėjimas ir priežiūra 12.4.1 Operacinės programinės įrangos valdymas 12.4.2 Sistemos testavimo duomenų apsauga	+
DS9.2 Konfigūracijos elementų identifikavimas ir valdymas	7.1.1 Turto aprašai 7.1.2 Turto valdymas 7.2.2 Informacijos žymėjimas ir priežiūra 10.7.4 Sistemos dokumentacijos saugumas 11.4.3 Tinklų įrangos atpažinimas 12.4.2 Sistemos testavimo duomenų apsauga 12.5.3 Programinės įrangos paketų keitimų apribojimai 12.6.1 Techninio pažeidžiamumo valdymas 15.1.5 Netinkamo naudojimosi	+

	informacijos apdorojimo priemonėmis prevencija	
DS9.3 Konfigūracijos vientisumo užtikrinimas	7.1.1 Turto aprašai 10.7.4 Sistemos dokumentacijos saugumas 12.5.2 Techninė programos peržiūra pakeitus operacinę sistemą 15.1.5 Netinkamo naudojimosi informacijos apdorojimo priemonėmis prevencija	+

DS10 Problemų ir skundų sekimas ir sprendimas

Pagrindinis tikslas užtikrinti, kad problemos yra sprendžiamos, priežastys identifikuojamos ir išvengiama problemos pasikartojimo

43 lentelė. Problemų ir skundų sekimas ir sprendimas

CobiT 4.1 kontrolės		Atitiktis įmonėje
DS10.1 Problemų identifikavimas ir klasifikavimas	13.2.2 Mokymasis iš informacijos saugumo incidentų	+
DS10.2 Problemų sprendimas	13.2.2 Mokymasis iš informacijos saugumo incidentų	+
DS10.3 Problemų uždarymas		+
DS10.4 Incidentų ir problemų valdymo, konfigūracijos integracija		+

DS11 Duomenų priežiūra

Pagrindinis tikslas užtikrinti, kad duomenys išlieka pilni, tikslūs ir galiojantys įvedimo, atnaujinimo, saugojimo, išvedimo metu.

44 lentelė. Duomenų priežiūra

CobiT 4.1 kontrolės		Atitiktis įmonėje
DS11.1 Verslo reikalavimai duomenų valdymui	10.8.1 Keitimosi informacija politikos ir procedūros	+
DS11.2 Saugymas ir išsaugojimo susitarimas	10.5.1 Atsarginės informacijos kopijos	+
DS11.3 Medijos bibliotekų valdymo sistema	10.7.1 Keičiamųjų duomenų laikmenų tvarkymas 15.1.3 Organizacijos oficialių dokumentų apsauga	+
DS11.4 Dispozicija	9.2.6 Saugus įrangos naikinimas arba pakartotinis naudojimas 10.7.1 Keičiamųjų duomenų laikmenų tvarkymas 10.7.2 Duomenų laikmenų naikinimas	+
DS11.5 Rezervinių kopijų darymas ir atstatymas	10.5.1 Atsarginės informacijos kopijos	+
DS11.6 Saugumo reikalavimai duomenų valdymui	10.5.1 Atsarginės informacijos kopijos 10.7.3 Informacijos priežiūros procedūros 10.8.3 Fizinių duomenų laikmenų pervežimas 10.8.4 Elektroninis susirašinėjimas 12.4.2 Sistemos testavimo	+

	duomenų apsauga 12.4.3 Pirminio programos teksto prieigos valdymas	

DS12 Patalpų kuriuose yra įranga priežiūra
Pagrindinis tikslas užtikrinti tinkamą fizinę aplinką, saugančią darbuotojus ir įrangą nuo natūralių ir žmogaus sukeltų nelaimių.

45 lentelė. Įrangos patalpų priežiūra

CobiT 4.1 kontrolės		Atitiktis įmonėje
DS12.1 Vietos ir išdėstimo parinkimas	9.1.1 Fizinė saugumo aptvara 9.1.3 Įstaigų, patalpų ir priemonių apsauga 9.1.6 Viešos prieigos, pristatymo ir krovimo vietos	+
DS12.2 Fizinės saugos priemonės	9.1.1 Fizinė saugumo aptvara 9.1.2 Fizinė įėjimo kontrolė 9.1.3 Įstaigų, patalpų ir priemonių apsauga 9.2.5 Įrangos, esančios ne organizacijos patalpose, saugumas 9.2.7 Nuosavybės perkėlimas	+
DS12.3 Fizinė prieiga	6.2.1 Rizikų, susijusių su išorinėmis šalimis, nustatymas	+
DS12.4 Apsauga nuo aplinkos faktorių	9.1.4 Apsauga nuo išorinių ir aplinkos grėsmių 9.2.1 Įrangos vietos parinkimas ir apsauga 9.2.2 Komunalinės paslaugos 9.2.3 Kabelių apsauga	+
DS12.5 Fizinio turto valdymas	9.2.2 Komunalinės paslaugos 9.2.4 Įrangos priežiūra	+

DS13 Kasdieninių sistemų panaudojimo užtikrinimas
Pagrindinis tikslas užtikrinti, kad svarbios IT funkcijos yra atliekamos reguliariai ir tvarkingai.

46 lentelė. Kasdieninių sistemų panaudojimo užtikrinimas

CobiT 4.1 kontrolės		Atitiktis įmonėje
DS13.1 Procedūros ir instrukcijos	10.1.1 Darbo procedūrų įforminimas dokumentais 10.7.4 Sistemos dokumentacijos saugumas	+
DS13.2 Darbų tvarkaraščio sudarymas		+
DS13.3 IT infrastruktūros stebėjimas		+
DS13.4 Jautrūs dokumentai ir išviesties įrenginiai (fizinė apsauga jautriai informacijai ir įrenginiams)		+
DS13.5 Prevenciniai sisteminių įrenginių (*angl. hardware*) palaikymo darbai	9.2.4 Įrangos priežiūra	+

Stebėsena
Efektyvus IT našumo valdymas reikalauja monitoringo procedūrų. Monitoringas reikalingas,

kad būti užtikrinama, kad reikiami veiksmai atlikti atsižvelgiant į reikiamus reikalavimus ir politikas.

ME1 IT funkcijų atlikimo priežiūra
Pagrindinis tikslas užtikrinti, kad IT procesams keliami reikalavimai yra vykdomi.

47 lentelė. IT funkcijų atlikimo priežiūra

CobiT 4.1 kontrolės		Atitiktis įmonėje
ME1.1 Stebėsenos gidas		+
ME1.2 Stebimų duomenų apibrėžimai	10.10.2 Stebėsenos sistemos naudojimas	+
ME1.3 Stebėsenos metodai		+
ME1.4 Našumo vertinimas		+
ME1.5 Vadovų raportavimas		+
ME1.6 Korekciniai veiksmai		+

ME2 Vidinės kontrolės adekvatumo įvertinimas
Pagrindinis tikslas užtikrinti nuolatinį iškeltų tikslų pasiekimą, procesų laikymąsi.

48 lentelė. Vidinės kontrolės adekvatumo įvertinimas

CobiT 4.1 kontrolės		Atitiktis įmonėje
ME2.1 Vidinių kontrolių monitoringo gidas	5.1.1 Informacijos saugumo politikos dokumentas 15.2.1 Atitiktis saugumo politikoms ir standartams	+
ME2.2 Priežiūros peržiūra	5.1.2 Informacijos saugumo politikos peržiūra 6.1.8 Nepriklausoma informacijos saugumo peržiūra 10.10.2 Stebėsenos sistemos naudojimas 10.10.4 Administratoriaus ir operatoriaus žurnalai 15.2.1 Atitiktis saugumo politikoms ir standartams	+
ME2.3 Kontrolių išimtys	15.2.1 Atitiktis saugumo politikoms ir standartams	+
ME2.4 Kontrolių įsivertinimas	15.2.1 Atitiktis saugumo politikoms ir standartams	+
ME2.5 Vidinių kontrolių patikimumas	5.1.2 Informacijos saugumo politikos peržiūra 6.1.8 Nepriklausoma informacijos saugumo peržiūra 10.10.2 Stebėsenos sistemos naudojimas 10.10.4 Administratoriaus ir operatoriaus žurnalai 15.2.1 Atitiktis saugumo politikoms ir standartams 15.2.2 Techninio suderinamumo tikrinimas 15.3.1 Informacijos sistemų audito valdymo priemonės	+
ME2.6 Vidinės kontrolės pas trečias šalis	6.2.3 Saugumo reikalavimai sutartyse su trečiosiomis šalimis 10.2.2 Trečiosios šalies teikiamų	+

	paslaugų stebėsena ir peržiūra 15.2.1 Atitiktis saugumo politikoms ir standartams	
ME2.7 Korekciniai veiksmai	5.1.2 Informacijos saugumo politikos peržiūra 15.2.1 Atitiktis saugumo politikoms ir standartams	+

ME3 Trečių šalių audito, garanto užtikrinimas
Pagrindinis tikslas didinti pasitikėjimą įmone partnerių, klientų tarpe.

49 lentelė. Trečių šalių audito, garanto užtikrinimas

CobiT 4.1 kontrolės		Atitiktis įmonėje
ME3.1 Išorinio reguliavimo ir kontraktinio laukimosi reikalavimų identifikavimas	6.1.6 Ryšys su valdžios institucijomis 15.1.1 Galiojantys įstatymai 15.1.2 Intelektinės nuosavybės teisės 15.1.4 Duomenų apsauga ir asmeninės informacijos privatumas	+
ME3.2 Atsako į išorinius reikalavimus optimizavimas		+
ME3.3 Suderinamumas su išoriniais reikalavimais	15.2.1 Atitiktis saugumo politikoms ir standartams 15.2.2 Techninio suderinamumo tikrinimas	+
ME3.4 Suderinimo patikimumas	15.2.1 Atitiktis saugumo politikoms ir standartams 15.2.2 Techninio suderinamumo tikrinimas	+
ME3.5 Integruotas raportavimas		+

ME4 Organizacinis audito proceso rėmimas
Pagrindinis tikslas didinti pasitikėjimą įmone, pasinaudoti pasaulinės IT praktikos pasiekimais

50 lentelė. Organizacinis audito proceso rėmimas

CobiT 4.1 kontrolės		Atitiktis įmonėje
ME4.1 Establishment of an IT governance framework		
ME4.2 Strateginis išlyginimas		+
ME4.3 Vertės perdavimas		+
ME4.4 Resursų valdymas		+
ME4.5 Rizikų valdymas		+
ME4.6 Našumo matavimas		+
ME4.7 Nepriklausomas užtikrinimas	5.1.2 Informacijos saugumo politikos peržiūra 6.1.8 Nepriklausoma informacijos saugumo peržiūra 10.10.2 Stebėsenos sistemos naudojimas	+

ISO standarto atitikimas telekomunikacinės įmonės tinklo ir technologijų saugumo reikalavimams

51 lentelė. ISO atitikimas įmonės saugumo reikalavimams

Įmonės reikalavimai	**ISO atitiktis**
1. Informacijos klasifikavimas	7.2 Informacijos klasifikavimas
2. Sistemų klasifikavimas	-
3. Rizikos vertinimas ir priežiūra	4 Rizikos vertinimas ir priežiūra
4. Formalizuotas plėtros procesas	-
5. Kūrimo, testavimo ir eksploatavimo priemonių atskyrimas	10.1.4 Kūrimo, testavimo ir eksploatavimo priemonių atskyrimas
6. Formalios dokumentuotos pakeitimų valdymo procedūros	12.5.1 Keitimų valdymo procedūros
7. Programinės įrangos paketų keitimų apribojimai	12.5.3 Programinės įrangos paketų keitimų apribojimai
8. Užsakomasis programinės įrangos kūrimas	12.5.5 Užsakomasis programinės įrangos kūrimas
9. Sistemos priėmimas	10.3.2 Sistemos priėmimas
10a. Sistemos testvimo duomenų apsauga	12.4.2 Sistemos testvimo duomenų apsauga
10b. Patikrinimo ir patvirtinimo procedūros	-
11. Darbo procedūros ir atsakomybės	10.1 Darbo procedūros ir atsakomybės
12. Trečiosios šalies teikiamų paslaugų valdymas	10.2 Trečiosios šalies teikiamų paslaugų valdymas
13. Sistemos planavimas ir priėmimas	10.3 Sistemos planavimas ir priėmimas
14. Apsauga nuo kenksmingų programų	10.4 Apsauga nuo kenksmingų programų
15. Atsarginės kopijos	10.5 Atsarginės kopijos
16. Tinklo valdymo priemonės	10.6.1 Tinklo valdymo priemonės
17. Viešųjų tinklo paslaugų apsauga	-
18. Viešųjų tinklo paslaugų, pasiekiamumo, saugumo valdymas	-
19. Reagavimas į brukalus	-
20. Reagavimas į atkirtimo nuo paslaugos atakas	-
21. Keitimasis informacija ir duomenų laikmenų priežiūra	10.7 Duomenų laikmenų priežiūra 10.8 Keitimasis informacija
22. Stebėsena	10.10 Stebėsena
23. Šifravimo valdymo priemonės	12.3 Šifravimo valdymo priemonės
24. Operacinės programinės įrangos valdymas	12.4.1 Operacinės programinės įrangos valdymas
25. Programinės įrangos paketų keitimų apribojimai	12.5.3 Programinės įrangos paketų keitimų apribojimai
26. Techninė programos peržiūros pakeitus operacinę sistemą	12.5.2 Techninė programos peržiūros pakeitus operacinę sistemą
27. Sistemos testavimo duomenų apsauga	12.4.2 Sistemos testavimo duomenų apsauga
28. Pirminio programos teksto prieigos valdymas	12.4.3 Pirminio programos teksto prieigos valdymas
29a. Techninio pažeidžiamumo valdymas	12.6.1 Techninio pažeidžiamumo valdymas
29b. Patikrinimo ir patvirtinimo procedūros	-
Naudotojų prieigos valdymas	11.2 Naudotojų prieigos valdymas
Tinklo prieigos valdymas	11.4 Tinklo prieigos valdymas
Operacinės sistemos prieigos valdymas	11.5 Operacinės sistemos prieigos valdymas
Prieigos prie programų ir informacijos valdymas	11.6 Prieigos prie programų ir informacijos valdymas
Atitiktis	15 Atitiktis

4.4 Išvados

Išanalizavus įmonę pagal informacijos saugumo ISO standartą pastebėta, kad informacijos saugumą keliuose skyriuose reiktų peržiūrėti ir sustiprinti, kad pilnai atitiktų ISO standarto reikalavimus. Analizėje pagal CobiT taip pat pastebėti keli neatitikimai. 52 ir 53 lentelėse pateikti bendri apibendrinimai. Atlikus ISO standarto analizę pagal įmonės saugumo reikalavimus, pastebėta, kad įmonė yra iškėlusi kelis reikalavimus kurie nėra numatyti ISO standarte. Pavyzdžiui telekomunikacinėje įmonėje keliamas saugumo reikalavimas viešųjų telekomunikacinių tinklų paslaugų saugumui, kas ISO standarte nėra numatyta, o įmonei tai yra labai svarbu. Iš to galima daryti išvadas, kad aklai pasikliauti saugumo standartais negalima, būtina įvertinti rizikas su kokiomis gali susidurti įmonė ir tik tuomet vadovautis standartų rekomendacijomis.

52 lentelė. Bendra lentelė (ISO)

4. Rizikos vertinimas ir priežiūra	Pilnai atitinka
5. Saugumo politika	Pilnai atitinka
6. Informacijos saugumo organizavimas	Vienas nedidelis trūkumas, informacijos saugumui užtikrinti reikia padydinti finansavimą. (Pagal statistiką, dauguma įmonių nepakankamai skiria lėšų informacijos saugumui užtikrinti)
7. Turto tvarkymas	Pilnai atitinka
8. Personalas ir informacijos saugumas	Rasti trūkumai, kad nėra tikrinamas teistumas, nėra iki galo suderinta atsakomybė dirbant namie (pastaba: LR įstatimuose tai irgi nėra sutvarkyta). Tūrėtų būti peržiūrėtos sutartys darbuotojų ir trečiosios šalies atstovų ir numatyti atsakomybes, kurios tebeturėtų galią ir pasibaigus įdarbinimo sutarties galiojimo laikui.
9. Fizinis ir aplinkos saugumas	Rastas trūkumas, pramoninėse aplinkose nėra numatytas ypatingų apsaugos priemonių, pavyzdžiui, klaviatūros plėvelių naudojimas. Tačiau šis trūkumas tirtai įmonei nėra aktualus.
10. Ryšių ir darbo procedūrų valdymas	Pilnai atitinka
11. Prieigos valdymas	Nedidelis trūkumas, reikėtų atnaujinti prieigų valdymo taisykles, kad suteiktų prieigų lygiai tiktų verslo veiklos tikslui ir atitiktų organizacijos saugumo politiką.
12. Informacijos sistemų užsakymas, tobulinimas ir priežiūra	Šiame skyriuje trūkumų rasta daugiausia. Trūksta: - Papildymo, modifikavimo arba ištrynimo funkcijų, kurios taikomos duomenų keitimui, naudojimą. - Balanso tikrinimo, siekiant palyginti failo atvėrimo ir ankstesnio jo užvėrimo reikšmes. - Kontrolinių suderinamumo skaiciavimų, siekiant garantuoti visų

	duomenų apdorojimą. - Šifruotos informacijos naudojimo poveikį valdymo priemonėms, kurias taikant pasikliaujama turinio apžiūra. - Kiekvieną kartą, kai testuojant taikomąją sistemą yra kopijuojama darbinė informacija, turėtų būti gautas atskiras leidimas.
13. Informacijos saugumo incidentų valdymas	Pilnai atitinka
14. Verslo veiklos tęstinumo valdymas	Trūksta krizių valdymo apmokymų.
15. Atitiktis	Pilnai atitinka

53 lentelė. Bendra lentelė (CobiT)

1. Planavimas ir organizavimas	Vienas nedidelis trūkumas, patartina peržiūrėti IT personalo darbuotojų vaidmenys, sudaryti esminio IT personalo sąrašus.
2. Pirkimai ir įdiegimas	Vienas nedidelis trūkumas, aplikacijų saugume ir pasiekiamume, patartina peržiūrėti ISO standarto atitikmenis.
3. Tiekimas ir palaikymas	Rasta pora nedidelių trūkumų tiekėjų rizikų vertinime ir apmokymai susije su IT tęstinumo planu. Patarimaperžiūrėti biudžetą skirta šiems mokymams ir paruošti krizinių situacijų valdymo planus.
4. Monitoringas	Pilnai atitinka

5. Bendros išvados

Baigiamojo darbo tikslas – tarptautinių informacijos saugumo standartų pritaikymo įvertinimas įmonėje. Atlikta informacijos saugumo problemų analizė. Pateikiau pagrindinius metodus, kokiais reikėtų remtis norint užtikrinti organizacijos saugumą, tai rizikų vertinimas, kontrolės, informacijos klasifikavimas, verslo tęstinumo planavimas. Apžvelgiau pagrindinius informacijos apsaugos kriterijus, žinant juos, galima efektyviai planuoti informacijos apsaugos valdymo įgyvendinimą ir nustatyti organizacijos saugumo reikalavimus. Atlikau dviejų saugumo standartų ISO/IEC 17799:2005 ir CobiT 4.1 analizę, pateikiau jų esminius panašumus ir skirtumus. Remiantis gautais rezultatais galima daryti išvadą, kad organizacija, kuri nori kuo labiau užtikrinti informacijos saugumą, turėtų naudoti abiejus standartus.

Išanalizavus įmonę pagal informacijos saugumo ISO 17799 ir CobiT 4.1 standartus pastebėta, kad informacijos saugumą keliuose skyriuose reiketų peržiūrėti ir sustiprinti. Analizuojant įmonę pagal ISO standartą pastebėti smulkūs trūkumai personalo ir informacijos saugume, fiziniame ir aplinkos saugume, ryšių ir darbo procedūrų valdyme, informacijos sistemų užsakyme, tobulinime ir priežiūroje. Reikėtų atkreipti dėmesį į šiuos smulkius trūkumus ir kur reikia susitiprinti saugumą. Analizuojant įmonę pagal CobiT standartą pastebėta, kad įmonė beveik pilnai atitinka šį standartą, reikėtų patobulinti tik kelias kontroles susijusias su esminio IT personalo vaidmenimis, skiriamu saugumui biudžetu, verslo tęstinumo planavimu.

Analizuojant ISO standartą pagal įmonės tinklo ir saugumo reikalavimus, pastbėta, kad ISO standarte nėra numatytas sistemų klasifikavimas, formalizuotas plėtros procesas, viešųjų tinklo paslaugų apsaugos procesas, patikrinimo ir patvirinimo procedūrų skirtų sistemų testavimo duomenų apsaugai ir techninio pažeidžiamumo valdymui. Nėra numatytas reagavimas į brukalų ir paskirstytų atkirtimo nuo paslaugos atakų. Iš to galima daryti išvadas, kad aklai pasikliauti saugumo standartais negalima, reikia būtinai įvertinti rizikas su kokiomis gali susidurti įmonė ir pagal tai suformuoti saugumo reikalavimus.

Tik gerai išmanant informacijos saugumo problemas, įvertinus visas rizikas ir pagal tai suformavus tikslus galima vadovautis standartų rekomendacijomis.

Darbo rezultatai bus panaudoti įmonės veikloje.

6. Literatūros sąrašas

[1]. Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas (tapatus ISO/IEC 17799:2005)

[2]. Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit

[3]. Alan Calder; Steve Watkins. 2008. IT Governanc:. A Manager`s guide to data security and ISO 27001/ISO 27002 4th edition. Kogan Page. 385 p. ISBN 978074945271

[4]. Harold F. Tipton, Kevin Henry. 2008. Official (ISC)2® guide to the CISSP® CBK®. (ISC) 1023 p. ISBN 0-8493-8231-9

[5]. Vidiniai įmonės dokumentai

[6]. ITIL [interaktyvus]. Wikipedia.org [žiūrėta 2009.03.01] Prieiga per internetą: < http://lt.wikipedia.org/wiki/ITIL >

[7]. *Payment card industry data security Standard.* [interaktyvus]. Wikipedia.org [žiūrėta 2009.04.03] Prieiga per internetą: < http://en.wikipedia.org/wiki/PCI_DSS >

Priedas