VILNIAUS UNIVERSITETO
KAUNO FAKULTETAS

SOCIALINIŲ MOKSLŲ IR TAIKOMOSIOS INFORMATIKOS INSTITUTAS

Finansų technologijų studijų programa
Kodas 6211bx022

DAINORA ŠVETKAUSKAITĖ

MAGISTRO BAIGIAMASIS DARBAS

ĮMONĖS ATITIKTIES MOKĖJIMO KORTELIŲ PRAMONĖS DUOMENŲ SAUGUMO STANDARTUI (ANGL. *PCI DSS*) ĮVERTINIMO METODAS, GRINDŽIAMAS TOPSIS METODU

Kaunas 2025

VILNIAUS UNIVERSITETO
KAUNO FAKULTETAS

SOCIALINIŲ MOKSLŲ IR TAIKOMOSIOS INFORMATIKOS INSTITUTAS

DAINORA ŠVETKAUSKAITĖ

MAGISTRO BAIGIAMASIS DARBAS

ĮMONĖS ATITIKTIES MOKĖJIMO KORTELIŲ PRAMONĖS DUOMENŲ SAUGUMO STANDARTUI (ANGL. *PCI DSS*) ĮVERTINIMO METODAS, GRINDŽIAMAS TOPSIS METODU

Magistrantas_____
(parašas)

Darbo vadovas_____
(parašas)

_____
(darbo vadovo mokslo laipsnis, mokslo pedagoginis vardas, vardas ir pavardė)

Darbo įteikimo data
Registracijos Nr.

Kaunas 2025

TURINYS

SANTRUMPŲ SĄRAŠAS

PCI DSS (angl. *Payment Card Industry Data Security Standard*) – mokėjimo kortelių pramonės duomenų saugumo standartas.

PCI SSC (angl. *Payment Card Industry Security Standards Council*) - mokėjimo kortelių pramonės duomenų saugumo taryba.

CISP (angl. *Cardholder Information Security Program*) – kortelių informacijos saugumo programa.

BDAR (angl. *General Data Protection Regulation*) – bendrasis duomenų apsaugos reglamentas.

POS (angl. *Point of Sale*) – mokėjimo terminalas.

PAN (angl. *Primary Account Number*) – pirminis sąskaitos numeris.

CVV (angl. *Card Verification Value*) – kortelės saugumo kodas, patikrinimo reikšmė.

CID (angl. *Card Identification Value*) – kortelės saugumo kodas, identifikacijos reikšmė.

CAV (angl. *Card Authentication Value*) – kortelės saugumo kodas, autentifikacijos reikšmė.

PIN (angl. *Personal Identification Number*) – asmens identifikacinis kodas.

SAQ (angl. *Self-Assessment Questionnaire*) – savęs analizės klausimynas.

QSA (angl. *Qualified Security Assessor*) – atestuotas saugos vertintojas.

ASV (angl. *Approved Scanning Vendor*) – patvirtintas skenavimo paslaugų tiekėjas.

ROC (angl. *Report on Compliance*) – atitikties ataskaita.

ISA (angl. *Internal Security Assessor*) – vidinis saugos vertintojas.

PDF (angl. *Portable Document Format)* – atviro standarto formatas, skirtas elektroniniam dokumentui atvaizduoti.

PAVEIKSLŲ SĄRAŠAS

LENTELIŲ SĄRAŠAS

Švetkauskaitė Dainora (2025). A Method for Assessing a Company‘s Compliance with the PCI DSS Standard based on the TOPSIS Method. MBA Graduation Paper. Kaunas: Vilnius University, Kaunas Faculty, Intitute Social Sciences and Applied Informatics. 68 p.

SUMMARY

With the rapid growth of the number of electronic payments and increasing threats to information security, payment card data protection has become a key priority for organizations. The Payment Card Industry Data Security Standard (PCI DSS) is a widely recognized international information security standard that all organizations processing, storing, or transmitting cardholder data must comply with. It has been observed that many organizations face challenges in implementing PCI DSS requirements, ranging from insufficient compliance monitoring to ineffective risk management. The topic of this paper is a method for assessing a company's compliance with the PCI DSS based on the TOPSIS method. The large volume of electronic payments and the increasing number of cyber threats pose challenges for organizations, as it is becoming increasingly important to ensure not only formal but also actual compliance with PCI DSS requirements. In practice, there is often a lack of a structured and quantitatively based method that would allow for an objective assessment of the level of compliance and the identification of priority areas for improvement. The aim of this work is to accelerate the process of assessing a company's compliance with PCI DSS standard, which would allow for a systematic assessment of the organization's security status according to 12 PCI DSS requirements and assessment criteria. The method integrates assessments of the company's current level, desired security goals, and priorities. These main objects are used to calculate dynamic criteria weights and determine the overall level of compliance. During the analysis, the assessment method allows for identifying the weakest areas of security, determining the gap from the ideal level of compliance, and comparing improvement solutions. The TOPSIS method is used to evaluate software and hardware suppliers. It would show the optimal solution to be selected according to the company's strategic priorities. The synthesized results of the study showed that the TOPSIS method is a suitable and practical tool for assessing PCI DSS compliance, enabling objective, data-driven decisions, and targeted planning to improve the organization's PCI DSS standard compliance.

This paper has 67 pages, 15 tables and 35 pictures.

ĮVADAS

Įvade apžvelgiamas mokėjimo kortelių pramonės duomenų saugumo standarto temos aktualumas, aptariama jo reikšmė organizacijoms, apibrėžiami pagrindiniai iššūkiai. Apibrėžiamas darbo tikslas, problema, pagrindiniai uždaviniai, struktūra, analizuota literatūra.

TEMOS AKTUALUMAS

Šiuolaikinėje visuomenėje mokėjimo kortelės tapo vienu iš pagrindinių elektroninių atsiskaitymo būdų, suteikiančių vartotojams galimybę saugiai ir patogiai atlikti finansines operacijas. Mokėjimo kortelių duomenims techninius ir organizacinius reikalavimus nustato Mokėjimo kortelių pramonės duomenų saugumo standartas (angl. *PCI DSS*), kuris yra apibrėžiamas kaip tarptautinis informacijos saugumo standartas, reglamentuojantis mokėjimo duomenų apsaugą. Šis tarptautinis informacijos saugumo standartas padeda užtikrinti duomenų konfidencialumą, vientisumą ir prieinamumą, mažina finansinių sukčiavimų riziką. Tad PCI DSS suteikia organizacijoms struktūrizuotą techninių ir organizacinių reikalavimų rinkinį.

Mokslinėje literatūroje egzistuoja bendro pobūdžio audito ir rizikos vertinimo metodai, kurie nėra orientuoti tik į mokėjimo duomenų saugumo aspektus. Trūksta metodų, pritaikytų PCI DSS atitikties įvertinimui skirtingo tipo įmonėse. Įvertinimas vykdomas taikant SAQ, kuris apima platų spektrą skirtingų saugumo krypčių. Apibendrinant galima teigti, kad naudojant daugiakriterinį metodą sudaromos prielaidos sukurti metodiškai pagrįstą ir patikimą PCI DSS atitikties įvertinimo metodą.

PROBLEMOS IŠTYRIMO LYGIS

Informacijos saugumo, duomenų apsaugos ir atitikties standartų temos yra dažnai nagrinėjamos mokslinėje literatūroje. Įmonės veiklos atitikimo PCI DSS standarto reikalavimams įvertinimo metodas yra reikšminga, tačiau vis dar nepakankamai ištirta sritis moksliniu lygmeniu. Pasitaiko atvejų, kai standarto atitiktis laikoma tik „varnelės uždėjimo“ (angl. *check-the-box*) veikla, dėl kurios gali atsirasti atotrūkis tarp reguliavimo laikymosi ir tikrųjų saugumo poreikių (Folorunso, 2024). Tyrimai rodo, kad PCI DSS laikymasis sumažina duomenų pažeidimų riziką, tačiau kartu kelia iššūkių dėl aukštų įgyvendinimo kaštų, kompleksiškumo ir dažno versijų atnaujinimo (Joshi, 2024). Taigi, organizacijoms trūksta metodų, kaip tinkamai užtikrinti PCI DSS įvertinimo atitiktį.

Mokslinėje literatūroje galima rasti tyrimų, kurie analizuoja PCI DSS reikalavimus, jų taikymo ypatumus bei poveikį informacijos saugumui, tačiau dauguma jų yra orientuoti į teorinius aspektus. Pavyzdžiui, Joshi (2024) nustatė, kad PCI DSS atitiktis sumažina duomenų pažeidimų riziką, tuo tarpu Chippagiri ir Ramesh (2025) įrodė, kad PCI DSS įgyvendinimas sukelia kompleksinių sunkumų – sudėtingumas, resursų trūkumas, neatitikimai. Lietuvoje ir Baltijos regione PCI DSS atitikties klausimai vis dažniau tampa tyrimų objektu, tačiau vis dar daugiau dėmesio yra skiriama bendram kibernetinio saugumo reglamentavimui ir rizikos vertinimo procesams.

DARBO PROBLEMA

Įmonėms PCI DSS atitikties vertinimas reikalauja daug laiko ir išteklių, todėl TOPSIS metodu grindžiamas sprendimas leidžia šį procesą padaryti greitesnį, aiškesnį, pigesnį ir objektyvesnį.

DARBO OBJEKTAS

Įmonės atitikties PCI DSS standartui įvertinimo procesas.

DARBO TIKSLAS

Pagreitinti įmonės atitikties PCI DSS standarto kriterijams įvertinimo procesą.

DARBO UŽDAVINIAI

1. Išanalizuoti PCI DSS standarto struktūrą, reikšmę ir taikymo sritis.
2. Ištirti dažniausius iššūkius, susijusius su įmonės atitikties PCI DSS standarto įvertinimo procesu.
3. Identifikuoti pagrindinius kriterijus ir rodiklius, pagal kuriuos būtų galima įvertinti įmonės atitiktį PCI DSS standartui.
4. Sukurti įmonės atitikties PCI DSS reikalavimams įvertinimo metodą, naudojant TOPSIS metodą.
5. Patikrinti sukurtą metodą testiniais duomenų įrašais.

DARBO STRUKTŪRA

Pirmojoje darbo dalyje „PCI DSS standarto apžvalga“ nagrinėjamos standarto sąvokos, reikalavimai ir atitikimo lygiai. Pateikiami dažniausi iššūkiai, su kuriais susiduria įmonės, įgyvendindamos PCI DSS standartą. Antrojoje dalyje „Daugiakriterinio įvertinimo metodo TOPSIS teorinė analizė“ yra pristatomi TOPSIS metodo principai, skaičiavimo eiga ir jo taikymo galimybės vertinant sudėtingus sprendimus pagal kelis kriterijus. Trečiojoje dalyje „PCI DSS įvertinimo metodas“ aprašomi kriterijai, vertinimo skalės ir struktūra, reikalingi sukurti įmonės PCI DSS atitikties įvertinimo metodui. Ketvirtojoje dalyje „TOPSIS metodo taikymas įmonės PCI DSS atitikties analizei“ praktiškai pritaikomas TOPSIS metodas, įvertinami hipotetinių įmonių atitikties lygiai, nustatomos silpnosios sritys, pateikiami tiekėjų pasiūlymai ir suformuojamos išvados.

DARBE NAUDOTI LITERATŪROS ŠALTINIAI

Analizuojant teorinę dalį konkrečios literatūros pasirinkta tema nebuvo itin daug, daugiausiai buvo analizuojama PCI DSS standarto dokumentacija, buvo apjungta su pasirinkta darbo tema susijusi tiek lietuvių, tiek užsienio autorių mokslinė literatūra.

DARBO IR TYRIMO METODAI

Teorinėje dalyje buvo atlikta tarptautinių ir nacionalinių mokslinių šaltinių, dokumentų analizė. Tam buvo taikoma lyginamoji mokslinės literatūros analizė, sintezė, abstrahavimas ir sisteminimas. Šie metodai leido įvertinti esamas mokslines ir praktines nuostatas, susijusias su PCI DSS standarto taikymu, identifikuoti dažniausiai pasitaikančius atitikties iššūkius ir analizuoti TOPSIS metodą. Analitinėje dalyje reikalavimų grupavimui buvo naudojama teminė analizė, Likerto skalė, TOPSIS metodas. Taip pat buvo pasinaudota modeliavimo logika, vizualizuojant tyrimo logiką. Eksperimentinėje dalyje buvo sukurtas eksperimentinis įvertinimo metodas su testiniais duomenų įrašais.

DARBO TEORINĖ REIKŠMĖ

- Išanalizuota PCI DSS standarto samprata: apibrėžtos pagrindinės sąvokos, struktūra bei atlikta reikalavimų analizė, siekiant išgryninti pagrindines atitikties užtikrinimo kryptis.
- Įvertinti dažniausiai pasitaikantys iššūkiai, su kuriais susiduria įmonės įgyvendindamos PCI DSS reikalavimus.
- Teoriškai išnagrinėtas TOPSIS metodas, jo algoritmo eiga.

DARBO PRAKTINĖ REIKŠMĖ

- Šio darbo praktinė reikšmė pasireiškia sukurtu, TOPSIS metodu grindžiamu, įmonės atitikties PCI DSS standartui įvertinimo metodu, kuris gali būti pritaikytas realiose organizacijose sistemingam, objektyviam ir kiekybiškai pagrįstam saugumo būklės vertinimui.
- Siūlomas metodas suteikia galimybę įmonėms ne tik nustatyti esamą atitikties lygį, bet ir identifikuoti silpniausias saugumo sritis, reikalaujančias prioritetinio tobulinimo.
- Praktinis sprendimas sumažintų subjektyvaus įvertinimo įtaką, optimizuotų PCI DSS įvertinimo procesą ir leistų įmonėms, kurios neturi didelių finansinių išteklių, pasitikrinti savo silpnąsias ir stipriąsias puses bei gauti tiekėjų pasiūlymus su jų teikiama programine ar techninė įranga.

DARBO APRIBOJIMAI IR SUNKUMAI

Analitinė / Teorinė darbo dalys buvo gana sunkiai įgyvendinamos, nes mokslinės literatūros, tiesiogiai nagrinėjančios PCI DSS reikalavimų taikymą įvertinimo ir sprendimų priėmimo sistemų kontekste, nėra itin daug, daugiausiai naudotasi PCI DSS dokumentacija.

Eksperimentinė darbo dalis buvo realizuota testinės aplinkos pavidalu su testinių duomenų įrašais, tai leido patikrinti sprendimo funkcionalumą ir įvertinti metodo tinkamumą, tačiau realių įmonių duomenų panaudojimas būtų leidęs dar tiksliau įvertinti sukurto sprendimo praktinį pritaikomumą. Tačiau dėl konfidencialumo, duomenų apsaugos tokie duomenys nėra viešai prieinami.

DARBO STRUKTŪRA IR APIMTIS

Darbą sudaro įvadas, 4 darbo dalys, išvados. Pagrindinė darbo medžiaga apima 67 puslapius, įskaitant 15 lentelių, 35 paveikslus. Panaudotos literatūros sąrašą sudaro 43 šaltiniai.

Šio darbo rengimui bus pasitelkta dirbtinio intelekto (DI) sistema „ChatGPT“ versija GPT 5, GPT 5.1 ir GPT 5.2, kuri bus naudota pagalbai tikrinant skyrybą ir gramatiką, ir „Gemini 3“ – testinių duomenų įrašų generavimui. DI įrankiai bus naudojami kaip pagalbinė priemonė, laikantis akademinio sąžiningumo principų.

1. PCI DSS STANDARTO APŽVALGA

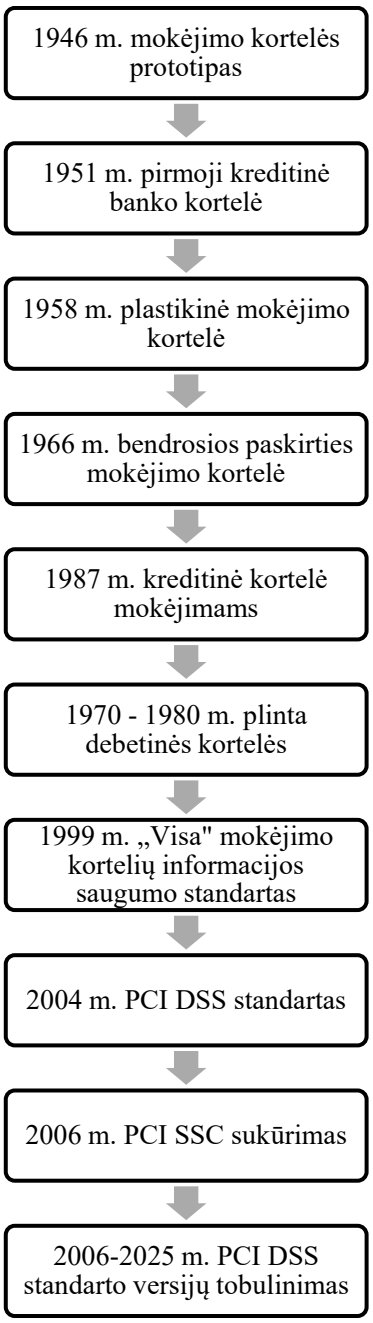
Pirmoje teorinėje dalyje aprašomas PCI DSS standartas, jo samprata, nuolat besikeičiančios versijos, kylantys pagrindiniai iššūkiai, norint jį įgyvendinti.

1.1. PCI DSS standarto samprata ir paskirtis

Mokėjimo kortelių pramonės duomenų saugumo standartas (toliau PCI DSS) yra pasaulinis duomenų saugumo standartas, skirtas apsaugoti mokėjimo kortelių duomenis nuo neteisėtos prieigos, sukčiavimo, duomenų nutekėjimo ir kitų kibernetinių grėsmių (Sakharova, 2012). Mokėjimo kortelės yra „banko ar kitos bendrovės išduota atsiskaitymo negrynaisiais pinigais priemonė“ (Visuotinė lietuvių enciklopedija, 2025), kuria galima atsiskaityti fizinėse prekybos vietose ir elektroninėje erdvėje.

Mokėjimo kortelių raida prasidėjo XIX a. pab., kai vartotojai naudojo kreditines monetas ir plokšteles. XX a. pradžioje naftos įmonės išleido lojalumo korteles, o 1946 m. sukurtas pirmasis elektroninio atsiskaitymo prototipas „Charg-It“ (Karayew, 2012). Vėliau pasirodė pirmosios kreditinės banko kortelės, plastikinės kortelės ir bendros paskirties kortelės, tarp jų – būsimosios „Visa“. 1970–1980 m. įvyko technologinis lūžis: atsirado magnetinės juostelės, POS terminalai ir realaus laiko mokėjimai, o kartu – ir saugumo grėsmės: klastojimai, duomenų ir mokėjimo kortelių vagystės, neteisėti skaitytuvai, kenkėjiškas darbuotojų elgesys (Sakharova, 2012). Taigi, negrynųjų pinigų atsiskaitymo operacijos tapo ne tik alternatyva grynųjų pinigų atsiskaitymams, bet ir sukėlė papildomus saugumo iššūkius.

Atsižvelgiant į augančias saugumo rizikas, dar 2001 m. „Visa“ sukūrė saugumo programą CISP (Gartner ir Carter, 2003), kuri apibrėžė savo saugumo normas su galimybe verslams priimti skaitmeninius mokėjimus, netrukus kitos mokėjimo kortelių organizacijos sekė jos pavyzdžiu ir sukūrė savo saugumo programas. Vis dėlto, skirtingų saugumo programų taikymas kėlė iššūkių prekybininkams. Todėl 2004 m., reaguodamos į augantį duomenų pažeidimų skaičių ir didėjantį skaitmenizavimą, penkios pagrindinės mokėjimo kortelių bendrovės („Visa“, „MasterCard“, „American Express“, „Discover Financial Services“ ir „JCB International“) sukūrė pirmąjį mokėjimo kortelių duomenis reglamentuojantį dokumentą PCI DSS (Chippagiri ir Ramesh, 2025). Atsižvelgiant į tai, kad pokyčiai finansų sektoriuje vyko nuolatos, pagrindinės mokėjimo kortelių bendrovės įkūrė konsorciumą, dar kitaip Mokėjimo kortelių pramonės saugumo standartų tarybą (toliau PCI SSC), kuri ėmėsi vieningo saugumo standarto tobulinimo. Bendri saugumo reikalavimai tarp įmonių leido suvienodinti mokėjimo kortelių duomenų saugumą ir laikytis bendro saugumo standarto. PCI SSC yra laikoma nepriklausoma grupe, kuri tapo atsakinga už PCI DSS standarto palaikymą ir plėtrą, siekiant sumažinti kibernetinių grėsmių rizikas bei užtikrinti mokėjimų saugumą pasauliniu mastu.



Šaltinis: sudaryta pagal internetinius šaltinius.

1 pav. PCI DSS atsiradimas

Pagrindinė PCI DSS standarto paskirtis yra užtikrinti, kad mokėjimo duomenų informacija būtų apsaugota visą jos gyvavimo ciklą – nuo informacijos surinkimo iki perdavimo ir saugojimo (PCI SSC, 2021). Taip pat šio standarto reikalavimų įgyvendinimas skatina organizacijas diegti prevencines priemones, kurios užtikrina informacijos saugumo konfidencialumą, prieinamumą ir vientisumą (McCallister et al., 2014). PCI DSS reikalavimų integravimas į organizacijos saugumo politiką padeda sumažinti duomenų pažeidimų, sukčiavimo (Gold, 2014) ir finansinių nuostolių riziką, kadangi yra nustatyti techniniai ir organizaciniai reikalavimai visiems mokėjimų ekosistemos dalyviams. Taigi, PCI

DSS yra esminis standartas, užtikrinantis ne tik techninį saugumą, bet ir vartotojų pasitikėjimą ne grynųjų pinigų operacijomis.

1.2. PCI DSS versijos nuo 1.0 iki 4.0.1

PCI DSS standarto tobulėjimas nuo pat pirmosios versijos atspindi dinamišką mokėjimo saugumo grėsmių mažėjimą ir technologinę pažangą mokėjimo kortelių pramonėje. Ankstyvosios standarto versijos buvo labiau orientuotos į pagrindinių techninių kontrolės priemonių – tinklo apsaugos, duomenų šifravimo ir prieigos valdymo – įtvirtinimą (PCI SSC, 2021). Keičiantis technologijoms, neužteko vien tik techninio saugumo valdymo, vėlesnės versijos yra papildytos rizikos vertinimo, nuolatinės atitikties palaikymo bei trečiųjų šalių valdymo nuostatomis (PCI SSC, 2024). Tad kiekviena šio standarto versija buvo tobulinama ir patyrė reikšmingų transformacijų (Liu et al., 2010). Apibendrinant galima teigti, kad PCI DSS raida atspindi bendrą informacijos saugumo standartų evoliuciją – nuo griežtai normatyvinių prie lankstesnių, rizikos vertinimu grįstų sistemų. Šis pokytis įmonėms padeda ne tik užtikrinti atitiktį, bet ir strategiškai valdyti mokėjimo kortelių duomenų saugumą.

Lentelė 1

PCI DSS versijos nuo 1.0 iki 4.0.1

Versija	Išleidimo data	Pagrindiniai pakeitimai
1.0	2004 m. gruodis	Pirmoji versija, vienodinanti skirtingų kortelių bendrovių skirtingus duomenų saugos reikalavimus.
1.1	2006 m. rugsėjis	Prekybininkai raginami peržiūrėti visas internetines programas ir įdiegti ugniasienes papildomai duomenų saugai.
1.2	2008 m. spalis	Tinklo saugumo stiprinimas: belaidžių tinklų apsauga ir antivirusinės programinės įrangos diegimas.
1.2.1	2009 m. liepa	Redakciniai pataisymai.
2.0	2010 m. spalis	Patobulinti saugumo reikalavimai, siekta supaprastinti vertinimo procesą.
3.0	2013 m. lapkritis	Didesnis saugumo švietimas ir sąmoningumas tarp organizacijų, priimančių kreditines korteles.
3.1	2015 m. balandis	Pašalintas pasenęs šifravimo protokolas SSL; skatinamas TLS naudojimas.
3.2	2016 m. balandis	Sustiprinta autentifikacija (MFA privaloma administratoriaus prieigai) ir stebėsena.
3.2.1	2018 m. gegužė	Techninis ir aiškinamasis (terminų patikslinimo) atnaujinimas.
4.0	2022 m. kovas	Įvesti rizika grįsti įgyvendinimo metodai, sustiprintas MFA.
4.0.1	2025 m. kovas	Techninis ir aiškinamasis atnaujinimas, nėra naujų reikalavimų.

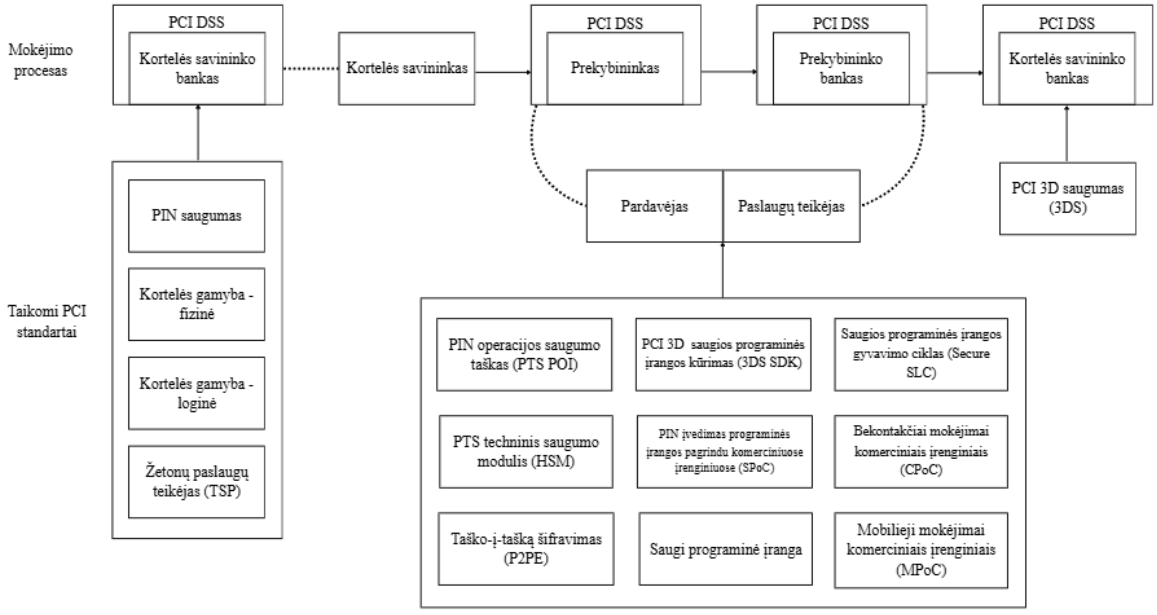
Šaltinis: sudaryta pagal Chippagiri ir Ramesh (2025) ir PCI SSC (2024).

1.3. **PCI saugumo standartų ekosistema**

PCI DSS standartas yra sukurtas siekiant apsaugoti mokėjimo kortelių duomenis viso mokėjimų ciklo metu. PCI DSS yra sutartinai privalomas visoms organizacijoms, kurios priima, perduoda ar saugo mokėjimo kortelių duomenis, kadangi atitiktis yra integruota į paslaugų teikimo sutartis su mokėjimo kortelių tinklais ir įgaliotais atsiskaitymų tvarkytojais. Dėl šios priežasties standartas yra laikomas privalomu reikalavimu praktikoje, siekiant užtikrinti galimybę saugiai valdyti negrynųjų pinigų mokėjimo operacijas.

PCI DSS yra pagrindinis PCI SSC administruojamas standartas. PCI SSC (2025) koordinuoja visą tarptautinę saugumo standartų ekosistemą, skirtą užtikrinti mokėjimo operacijų, programinės įrangos, aparatūros ir duomenų apsaugą visoje mokėjimo grandinėje. Mokėjimo kortelių pramonės programinės įrangos saugumo sistema (angl. *Payment Card Industry Software Security Framewor*k, toliau PCI SSF) papildo PCI DSS ir nustato reikalavimus saugiam programinės įrangos projektavimui, vystymui ir palaikymui, siekiant sumažinti pažeidžiamumų riziką. Mokėjimo kortelių pramonės PIN sandorių saugumas (angl. *Payment Card Industry PIN Transaction Security,* toliau PCI PTS) yra taikomas fizinėms mokėjimo priemonėms – banko kortelių skaitytuvams ir POS terminalams. Taigi, tai padeda reglamentuoti įrangos atsparumą manipuliacijoms ir užtikrinti PIN įvedimo saugumą.

Mokėjimo kortelių duomenų apsauga reikalauja kompleksiško požiūrio, nes mokėjimo procese dalyvauja daug skirtingų šalių (mokėjimo iniciatorius (kortelės savininkas) ir jo bankas, prekybininkas (įmonė) ir jo bankas). PCI DSS standartas yra taikomas visoms organizacijoms, dalyvaujančioms mokėjimo cikle, kadangi standartai padeda įgyvendinti saugias praktikas, technologijas ir procesus organizacijos viduje. Taigi, atsižvelgiant į standartą, PCI SSC (2025) yra sukūrusi mokėjimo kortelių pramonės (PCI) saugumo standartų ekosistemą:



Šaltinis: sudaryta pagal PCI SSC (2025).

2 pav. PCI saugumo standartų ekosistema

Ši supaprastinta PCI DSS standarto taikymo schema nurodo atsakomybę ne vien tik pagrindiniams mokėjimo proceso dalyviams, bet ir kitiems subjektams, kurie tiesiogiai dalyvauja visame mokėjimo kortelės duomenų gyvavimo cikle (PCI SSC, 2025). Kiekviename mokėjimo etape dalyvauja skirtingi subjektai, tad jų veiklai užtikrinti taikomi atitinkami PCI SSC saugumo standartai. Skirtingos mokėjimo proceso dalys apima įvairius technologinius komponentus ir yra reguliuojamos specializuotais standartais:

1. Kortelės išdavimas

Mokėjimo procesas prasideda nuo kortelės sukūrimo ir išdavimo savininkui, šį veiksmą atlieka bankas. Šiame etape yra taikomas saugumas:

- Fizinei kortelės gamybai – kortelės dizainas, lustų integravimas;
- Loginei kortelės gamybai – kortelės duomenų sukūrimas ir užšifravimas;
- Žetonų paslaugų teikėjams (virtualios kortelės ar žetonai, angl. *Token Service Provider,* TSP) – kortelės duomenys pakeičiami žetonu, atliekant mokėjimus.
- Sukuriamas saugus PIN kodas.

2. Atsiskaitymo vykdymas

Tuo metu, kai vartotojas atlieka atsiskaitymą už prekes ar paslaugas, mokėjimo duomenys keliauja per prekybininko ir jo banko valdymo sritį, todėl šiame etape taikomi PCI DSS reikalavimai bei papildomi standartai:

- PIN kodo apsauga (PTS) - įvestas PIN kodas turi būti saugiai perduotas, naudojant saugius mokėjimo terminalus bei šifravimo modulius.
- P2P šifravimas (P2PE) – technologija, kuri užšifruoja mokėjimo kortelės duomenis nuo jų įvedimo iki apdorojimo.
- Išorinės įrangos saugumo modulis (angl. *Hardware Security Module*, HSM) – naudojamas saugiam šifravimo raktų valdymui.

3. Sprendimų tiekėjų vaidmuo

Įmonės dažniausiai naudojasi trečiųjų šalių sprendimais – POS įrenginiais, mokėjimo terminalais, mobiliosiomis programėlėmis ar el. prekybos platformomis. Tokiais atvejais taikomi papildomi standartai:

- PIN įvedimas komercinėje įrangoje (SPoC);
- Vertinama, ar saugus programinės įrangos gyvavimo ciklas (Secure SLC);
- Mobiliųjų programėlių naudojimas mokėjimams atlikti (MPoC);
- Bekontakčiai (CPoC) atsiskaitymai vykdomi per komercinius įrenginius (pvz.: telefonus, planšetes).

4. Elektroninės prekybos atveju taikomas papildomas 3D Secure (3DS) standartas.

Atliekant mokėjimus internetu dažnai naudojamas 3D Secure autentifikavimo standartas, kurį tvirtina mokėjimo kortelės savininko bankas. Šis standartas užtikrina, kad vartotojas yra teisėtas kortelės

savininkas – pasitelkiant papildomas saugumo priemones (slaptažodį ar mobilųjį patvirtinimą autentifikavimui).

Tokiu būdu PCI saugumo standartų ekosistema apima ne tik bendrąsias organizacines ir technines kontrolės priemones, bet ir specializuotus standartus, orientuotus į konkretų technologinį kontekstą (PCI SSC, 2022). Įmonėms duomenų saugumo pažeidimai gali lemti finansines sankcijas, padidėjusius veiklos kaštus, prarastus klientus bei reputacinę žalą, kuri dažnai turi ilgalaikių pasekmių (Romanosky, 2016). Finansinėms institucijoms mokėjimo duomenų pažeidimai sukelia tiesioginius nuostolius dėl sukčiavimo, atsakomybes už kompensacijas, papildomas investicijas į rizikos mažinimo priemones (Anderson ir Moore, 2006). Vartotojams mokėjimo duomenų pažeidimas gali reikšti tapatybės vagystę, finansines netektis, pasitikėjimo skaitmeniniais atsiskaitymais sumažėjimą (Ghosh, 2021). Taigi, mokėjimo kortelių duomenų apsauga apima visą mokėjimų ekosistemą, kadangi saugos pažeidimas viename grandinės taške gali turėti pasekmes visai ekosistemai.

Sudaryta PCI ekosistema leidžia efektyviau valdyti rizikas įvairiuose mokėjimo proceso etapuose bei užtikrinti integralų duomenų apsaugos požiūrį. Kiekvienas mokėjimo ciklo dalyvis turi specifinių atsakomybių, o taikomi standartai padeda užtikrinti, kad:

- Mokėjimo kortelių duomenys nebūtų pavogti ar pakoreguoti;
- Būtų naudojamos tik saugios technologijos;
- Kiekvienas duomenų tvarkymo etapas būtų stebimas, audituojamas ir apsaugotas.

Taigi, toks kompleksinis saugumo modelis leidžia ne tik laikytis PCI DSS saugumo reikalavimų, bet ir sumažinti riziką, susijusią su mokėjimo kortelių duomenų nutekėjimu ar sukčiavimu (PCI DSS, 2025).

1.4. PCI DSS reikšmė įmonių informacijos saugai

Informacijos sauga yra viena esminių organizacijos veiklos aspektų, užtikrinančių duomenų apsaugą, verslo tęstinumą. Pagal Microsoft (2025) informacijos sauga apibūdinama kaip saugos priemonių visuma, kuri yra skirta apsaugoti konfidencialią įmonės informaciją nuo neteisėtos prieigos, naudojimo, piktnaudžiavimo, sunaikinimo, atskleidimo ar pakeitimo. Informacijos sauga apima asmenų ir organizacijų informacinių išteklių identifikavimą, pažeidžiamumų nustatymą, grėsmių prevenciją ir prevencinių priemonių bei tyrimų vykdymą, siekiant užtikrinti informacijos saugumą nuo nepageidaujamų rizikų ir incidentų (Ibrahimova, 2020). Bendru požiūriu, šie šaltiniai informacijos saugą apibūdina kaip informacijos apsaugą nuo neteisėtos prieigos, naudojimo, atskleidimo, sutrikdymo, keitimo ar sunaikinimo.

Pagal ISO/IEC 27000 (2016) standartą, informacijos sauga turi išlaikyti informacijos konfidencialumą, vientisumą ir prieinamumą, kurie kartu sudaro vadinamąjį CIA triadą – pagrindinį informacijos saugos principą. Pagal PCI DSS organizacijų pokyčius yra pastebima, kad saugumo kontrolės priemonės yra smarkiai keičiamos. Konfidencialumas užtikrina, kad informaciją gali pasiekti tik autorizuoti vartotojai pagal turimas atsakomybės ribas (Samonas ir Coss, 2014). Šis principas įgyvendinamas naudojant autentifikavimo, prieigos kontrolės bei šifravimo priemones, kurios apsaugo duomenis nuo neteisėto atskleidimo ar perėmimo. Vientisumas – tai informacijos sauga nuo neteisėto

keitimo ar ištrynimo, užtikrinant jos tikslumą ir išsamumą – svarbus veiksnys, atliekant sandorius (Samonas ir Coss, 2014). Vientisumo užtikrinimui yra naudojami duomenų kontrolės mechanizmai, skaitmeniniai parašai, kontrolinės sumos ir kiti panašūs rodikliai, kurie aptiktų ir užkirstų kelią neteisėtiems pakeitimams. Prieinamumas leidžia pasiekti tik autorizuotiems vartotojams reikalingą informaciją ir su ja susijusias paslaugas, taip išvengiant pavojingų klaidų ir patikimai informuoti vartotojus apie užduotis, kurias jie turi atlikti (Samonas ir Coss, 2014). Taigi, PCI DSS tiesiogiai siejasi su CIA triada, kadangi reikalavimai apima mokėjimo kortelių duomenų saugą nuo neteisėto duomenų atskleidimo, pakeitimo ar praradimo, išlaikant pagrindinius saugos principus.

1.5. **PCI DSS struktūra**

PCI DSS išskiria 12 pagrindinių techninių ir organizacinių saugumo reikalavimų, kurių laikymąsi privalo užtikrinti įmonės, tvarkančios vartotojų mokėjimo kortelių duomenis. Saugumo reikalavimai yra formalizuoti kriterijai, kurių pagrindu yra kuriamos saugias elektronines finansines operacijas apdorojančios sistemos. Išskiriami 6 pagrindiniai saugumo kontrolės tikslai, iš kurių suformuoti 12 pagrindinių saugumo reikalavimų (PCI DSS, 2024).

PCI DSS reikalavimai ir kontrolės tikslai sistemingai jungia tinklo saugumą, duomenų apsaugą, pažeidžiamumų valdymą ir saugumo politikos kūrimą, valdant mokėjimo kortelės savininko duomenis. Kontrolės tikslai ir reikalavimai persidengia, kad būtų sukurta išsami saugumo programa, apimanti tiek techninę kontrolę, tiek veiklos procesus, pripažįstant, kad veiksmingam saugumui reikalingas daugialypis požiūris (Chippagiri ir Ramesh, 2025). Taigi, reikalavimai ir tikslai padeda organizacijoms sukurti aiškų saugumo kontrolės įgyvendinimo planą, tuo pačiu užtikrinant, kad būtų atsižvelgta į visus svarbiausius mokėjimo kortelių saugumo aspektus.

Lentelė 2

Pagrindiniai PCI DSS kontrolės tikslai ir reikalavimai

Kontrolės tikslas	Reikalavimas
Saugaus tinklo ir sistemų kūrimas bei priežiūra	1. Įdiegti ir palaikyti tinklo saugumo kontrolės priemones.
	2. Taikyti saugias konfigūracijas visiems sistemos komponentams.
Apsaugoti mokėjimo kortelių savininkų duomenis	3. Apsaugoti mokėjimo kortelės savininko duomenis.
	4. Šifruoti kortelių savininkų duomenų perdavimą per atvirus, viešus tinklus.

Lentelė 3 tęsinys

Kontrolės tikslas	Reikalavimas
Palaikyti pažeidžiamumo valdymo programą	5. Apsaugoti visas sistemas nuo kenkėjiškų programų.
	6. Kurti ir palaikyti saugias sistemas ir taikomąsias programas.
Įgyvendinti stiprias prieigos kontrolės priemones	7. Riboti prieigą prie kortelių turėtojų duomenų pagal verslo poreikius.
	8. Identifikuoti ir autentifikuoti naudotojų prieigą prie sistemos komponentų.
	9. Riboti fizinę prieigą prie kortelių turėtojų duomenų.
Reguliariai stebėti ir testuoti tinklus	10. Stebėti ir registruoti prieigą prie visų išteklių ir kortelių turėtojų duomenų.
	11. Reguliariai testuoti saugumo sistemas ir tinklus.
Palaikyti informacijos saugumo politiką	12. Užtikrinti informacijos saugumo politiką, organizacijos politiką ir programas.

Šaltinis: sudaryta pagal Maria Yudit (2010), PCI DSS (2024).

1.6. **PCI DSS atitikties lygiai**

PCI DSS atitikties lygiai yra svarbi standartą taikančių įmonių klasifikavimo dalis, kuri leidžia diferencijuoti saugumo reikalavimus pagal verslo dydį ir atliekamų kortelių operacijų skaičių (PCI SSC, 2024). Įmonių klasifikavimas padeda efektyviau valdyti rizikas, nustatyti, kokio lygio audito, dokumentavimo ir saugumo kontrolės priemonės turi būti taikomos skirtingiems prekybininkams.

PCI DSS standartas skirsto įmones į keturis atitikties lygius, atsižvelgiant į jų atliekamų mokėjimo kortelių operacijų kiekį per 12 mėnesių laikotarpį. Toks skirstymas leidžia taikyti skirtingo griežtumo reikalavimus – kuo daugiau operacijų atlieka įmonė, tuo griežtesnė atitikties kontrolė taikoma. Šios organizacijos, kad išlaikytų atitikties statusą, privalo atlikti išsamius metinius vertinimus ir kas ketvirtį – tinklo skenavimus (Chippagiri ir Ramesh, 2025). Jei įmonė patiria saugumo pažeidimą, dėl kurio nuteka mokėjimo kortelių duomenys, ji gali būti automatiškai priskiriama aukštesniam atitikties lygiui, nepriklausomai nuo operacijų skaičiaus.

Lentelė 4

PCI DSS atitikties lygiai

Lygis	Operacijų skaičius (per 12 mėn.)	Reikalavimas
1 lygio prekybininkai	> 6 mln. operacijų (visais kanalais)	Ketvirtiniai tinklo skenavimai.
		Metiniai penetracijos testai.
		Metinis savęs įvertinimo klausimynas (SAQ).
		Atitikties patvirtinimo forma (AOC).
		Metinė atitikties ataskaita (ROC) su QSA.
2 lygio prekybininkai	nuo 1 mln. iki 6 mln. (visais kanalais)	Ketvirtiniai tinklo skenavimai.
		Metiniai penetracijos testai.
		Metinis savęs įvertinimo klausimynas (SAQ).
		Atitikties patvirtinimo forma (AOC).
		Metinė vidinė atitikties ataskaita (ROC).
3 lygio prekybininkai	nuo 20 000 iki 1 mln. (tik e. komercija)	Ketvirtiniai tinklo skenavimai.
		Metiniai penetracijos testai.
		Metinis savęs įvertinimo klausimynas (SAQ).
		Atitikties patvirtinimo forma (AOC).
4 lygio prekybininkai	< 1 mln. fizinių operacijų (< 20 000 e. komercija)	Ketvirtiniai tinklo skenavimai.
		Metiniai penetracijos testai.
		Metinis savęs įvertinimo klausimynas (SAQ).
		Atitikties patvirtinimo forma (AOC).

Šaltinis: sudaryta pagal Maria Yudit (2010), PCI DSS (2024).

Kiekvienai organizacijai reikia įsivertinti savo veiklos mastą, susieti jį su standartizuotais PCI DSS atitikties kriterijais ir tinkamai parinkti įvertinimo formą bei ataskaitų teikimo būdą. Todėl moksliniu požiūriu, rekomenduojama atlikti kelis struktūruotus žingsnius (PCI SSC, 2025):

1) **Kiekybiniai duomenys (mokėjimo kortelių operacijų dydžio analizė)** – paskutinių 52 savaičių (12 mėnesių) laikotarpio operacijų statistika, kad būtų galima įvertinti bendrą visų transakcijų apimtį iš visų priimamų mokėjimo tinklų.

2) **Kokybinės charakteristikos (duomenys iš finansinių institucijų)** – bankas ir kitos finansinės institucijos gali pateikti oficialią atliktų operacijų kiekio ataskaitą ir patikslinti, kokio lygio reikalavimai įmonei yra taikytini.

3) **SAQ (savęs vertinimo klausimynas) tinkamumo analizė** – organizacijos veiklos sritis, mokėjimų priėmimo kanalas, techninė architektūra lemia, kuris SAQ tipas yra tinkamas.

4) **Trečiųjų šalių patvirtinimas (konsultacijos su mokėjimo kortelių tinklu)** – galima kreiptis į mokėjimo kortelių tinklus, kai įmonės veikla yra sudėtinga, tarptautinė ar apima kelias IT architektūras, siekiant patvirtinti ar koreguoti lygio nustatymą.

Taigi, atsižvelgiant į struktūruotus žingsnius galima užtikrinti sklandų PCI DSS atitikties reikalavimų taikymo procesą. Tinkamas atitikties lygio nustatymas yra būtina sąlyga, norint sumažinti riziką ir efektyviau organizuoti PCI DSS reikalavimų įgyvendinimą.

1.7. Įvertinimo priemonės PCI DSS atitikties reikalavimams įgyvendinti

PCI DSS ir jį lydintys dokumentai yra bendras mokėjimo kortelių pramonės priemonių rinkinys, padedantis užtikrinti saugų kortelių turėtojų duomenų tvarkymą. Pats standartas suteikia praktinę sistemą, skirtą sukurti patikimą saugumo procesą, įskaitant saugumo incidentų prevenciją, aptikimą ir reagavimą į juos (PCI SSC, 2024).

„Verizon“ (2019) pateikia duomenis apie pilną PCI DSS standarto įmonių atitiktį, kuri 2016 m. buvo 55,4%, 2018 m. sumažėjo iki 36,7%, 2020 m. dar sumažėjo iki 27%. Šie duomenys atskleidžia kritinę tendenciją, kad dauguma organizacijų nesugeba išlaikyti ilgalaikės standarto atitikties. Vertinimo priemonės, skirtos PCI DSS atitikčiai organizacijose įgyvendinti yra rekomenduotinos, kad organizacijos galėtų įvertinti savo saugumo būklę, identifikuoti trūkumus ir pagrįsti atitiktį standartu. PCI DSS sistemoje naudojamos dvi pagrindinės patvirtinimo metodikos, skirtos konkretiems organizaciniams kontekstams patvirtinti: atitikties ataskaita ir savęs vertinimo klausimynas. PCI SSC prižiūri vertinimo priemones, kurios padeda lengviau įvertinti atitiktį PCI DSS reikalavimams (PCI SSC, 2024):

- **Savęs įvertinimo klausimynas** (angl. *Self-Assessment Questionnaire*, SAQ) – reikalavimų įgyvendinimo įvertinimo priemonė, skirta organizacijoms, kurios savarankiškai vertina savo PCI DSS atitiktį.
- **Atitikties patvirtinimo forma** (angl. *Attestation of Compliance*, AOC) – dokumentas, pateikiamas kartu su SAQ, kuriame organizacija pateikia, kad jos pateikti savęs vertinimo rezultatai yra tikslūs.
- **Atitikties ataskaita** (angl. *Report on Compliance*, ROC) – išsami ataskaita, parengta kvalifikuoto saugumo vertintojo (toliau QSA) arba vidinio saugumo vertintojo (toliau ISA), kurioje pateikiama ataskaita apie organizacijos atitikties lygį.
- **Penetracijos testai** (angl. *penetration tests*) – tikrinama organizacijos infrastruktūra ir bandoma sumažinti infrastruktūros pažeidžiamumą (t.y. simuliuojami kibernetiniai išpuoliai prieš organizacijos informacines sistemas, siekiant identifikuoti ir įvertinti apsaugos priemonių veiksmingumą).
- **Tinklo skenavimai** (angl. *network scans*) – patvirtintas skenavimo tiekėjas (toliau ASV) turi kas ketvirtį atlikti pažeidžiamumo skenavimą, kad nustatytų saugumo riziką įmonės sistemose, serveriuose ir tinkluose.

Lentelė 5

PCI DSS pagrindinės vertinimo priemonės

Kriterijus	Lygis	Atlieka	Dažnumas
SAQ	1-4	Pati organizacija arba QSA	Kartą per metus
AOC	1-4	Pati organizacija	Kartą per metus
ROC	1-2	QSA arba ISA	Kartą per metus
Penetracijos testai	1-4	Pati organizacija	Kartą per metus
Tinklo skenavimai	1-4	Pati organizacija	Kas ketvirtį

Šaltinis: sudaryta pagal PCI SSC (2025).

1.7.1. Įvertinimo klausimynų kategorijos

Kiekvienas SAQ variantas yra orientuotas į atitinkamas saugumo kontrolės priemones, skirtas konkretiems įmonių scenarijams – nuo paprastų operacijų iki sudėtingų el. prekybos aplinkų, užtikrinant tinkamą saugumo vertinimą. Patvirtinimo procesas apima išsamius dokumentacijos reikalavimus, įrodymų rinkimo procedūras ir konkrečias testavimo metodikas, skirtas kiekvienam kontrolės tikslui.

PCI DSS savęs vertinimo klausimynai yra esminė PCI DSS atitikimo proceso dalis. Ji leidžia organizacijoms nustatyti saugumo lygį ir parodyti PCI DSS atitiktį, supaprastinant atitikties reikalavimus. Anketos pildymas iš dalies pakeičia asmeninius auditus, o tai sudaro sąlygas mažoms įmonėms PCI DSS reikalavimų laikymosi patikrinimui (PCI SSC, 2025). Klausimynai sutrumpina atitikčiai įrodyti reikalingą laiką, o savęs vertinimas taip pat yra pigesnis nei išorės auditorių samdymas (PCI SSC, 2025).

Lentelė 6

Savęs įvertinimo klausimynų kategorijos

Savęs įvertinimo klausimynas	Aprašymas
SAQ A	Prekybininkai (el. prekyba arba užsakymai paštu/telefonu), kurie perduoda visas sąskaitos duomenų tvarkymo funkcijas PCI DSS patvirtintoms ir reikalavimus atitinkančioms trečiosioms šalims. Draudžiama elektroniniu būdu saugoti, apdoroti ar perduoti sąskaitos duomenis jų sistemose ar patalpose. Netaikoma tiesioginiams kanalams. Netaikoma paslaugų teikėjams.
SAQ A-EP	Elektroninės komercijos prekybininkai, kurie iš dalies perduoda mokėjimų apdorojimą PCI DSS patvirtintoms ir reikalavimus atitinkančioms trečiosioms šalims, ir kurių svetainė negauna sąskaitos duomenų, tačiau turi įtakos mokėjimo operacijos saugumui ir (arba) puslapio, kuriame priimami kliento sąskaitos duomenys, vientisumui. Draudžiama elektroniniu būdu saugoti, apdoroti ar perduoti sąskaitos duomenis jų sistemose ar patalpose. Taikoma tik el. prekybos kanalams. Netaikoma paslaugų teikėjams.

Lentelė 7 tęsinys

Savęs įvertinimo klausimynas	Aprašymas
SAQ B	Prekybininkai, naudojantys tik: - Spausdinimo aparatus be elektroninės sąskaitos duomenų saugyklos ir (arba); - Atskirus, išorinius terminalus be elektroninės sąskaitos duomenų saugyklos. Netaikoma el. prekybos kanalams. Netaikoma paslaugų teikėjams.
SAQ B-IP	Prekybininkai, naudojantys tik atskirus, PCI sąraše nurodytus, patvirtintus PIN transakcijų saugumo (angl. *PIN Transaction Security*, PTS) įrenginius (angl. *Point-of-Interaction*, POI) su IP ryšiu mokėjimų apdorojimui įrenginyje. Nėra elektroninio sąskaitos duomenų saugojimo. Netaikoma el. prekybos kanalams. Netaikoma paslaugų teikėjams.
SAQ C-VT	Prekybininkai, kurie rankiniu būdu įveda mokėjimo sąskaitos duomenis, atliekant kiekvieną operaciją, naudodami klaviatūrą į PCI DSS patvirtintą ir reikalavimus atitinkantį trečiosios šalies virtualaus mokėjimo terminalo sprendimą, naudodami izoliuotą skaičiavimo įrenginį ir saugiai prijungtą per žiniatinklio naršyklę. Nėra elektroninio sąskaitos duomenų saugojimo. Netaikoma el. prekybos kanalams. Netaikoma paslaugų teikėjams.
SAQ C	Prekybininkai, kurių mokėjimo programų sistemos yra prijungtos prie interneto, be elektroninio sąskaitų duomenų saugojimo. Netaikoma el. prekybos kanalams. Netaikoma paslaugų teikėjams.
SAQ P2PE	Prekybininkai naudoja tik patvirtintą, PCI standartą atitinkantį P2P šifravimą (angl. *Point-to-Point Encryption*, P2PE) sprendimą. Nėra prieigos prie aiškaus formato sąskaitos duomenų ir nėra elektroninio sąskaitos duomenų saugojimo. Netaikoma el. prekybos kanalams. Netaikoma paslaugų teikėjams.
SAQ SPoC	Prekybininkai, naudojantys komercinį mobilųjį įrenginį (pvz.: telefoną ar planšetinį kompiuterį) su saugiu kortelių skaitytuvu, įtrauktu į PCI SSC patvirtintų bendrojo ryšių palaikymo (angl. *Single Point of Contact*, SPoC) sprendimų sąrašą. Nėra prieigos prie aiškaus formato sąskaitos duomenų ir nėra elektroninio sąskaitos duomenų saugojimo. Netaikoma neautomatizuotam kortelės turėjimui, užsakymams paštu / telefonu ar el. prekybos kanalams. Netaikoma paslaugų teikėjams.

Lentelė 8 tęsinys

Savęs įvertinimo klausimynas	Aprašymas
SAQ D	SAQ D prekybininkams: visi prekybininkai, neįtraukti į aukščiau pateiktų SAQ tipų aprašymus. SAQ D paslaugų teikėjams: visi paslaugų teikėjai, kuriuos mokėjimo prekės ženklas apibrėžė kaip tinkamus pildyti SAQ.

Šaltinis: sudaryta pagal PCI SSC (2025).

1.8. **Iššūkiai įgyvendinant PCI DSS**

Iššūkiai, susiję su PCI DSS reikalavimų įgyvendinimu, dažnai apima techninius, organizacinius ir žmogiškuosius veiksnius. Rees (2010) aptaria keleto organizacijų iššūkius, įgyvendinant PCI DSS standarto atitiktį, nes visi reikalavimai yra rekomenduojami. Per pastaruosius metus nebuvo užfiksuota viešai patvirtintų didelio masto mokėjimo kortelių duomenų nutekėjimų, kurių priežastimi būtų aiškiai įvardytas tiesioginis PCI DSS reikalavimų nesilaikymas. 2017 m. atliktoje „GoAnywhere“ analizėje buvo išskirtos trys organizacijos, kurios patyrė finansinius ir reputacinius nuostolius būtent dėl to, kad pilnai neįgyvendino PCI DSS standartų. Todėl mažesnėms įmonėms nėra paprasta įgyvendinti ir nuolat užtikrinti atsinaujinančios PCI DSS standarto atitikties dėl reikalingų išteklių trūkumo (Boese, 2020).

Per nuolatinį vertinimo, taisymo ir ataskaitų teikimo procesą, kad atitiktų reikalavimus prekybininkas ar paslaugų teikėjas turi sumažinti saugumo pažeidimų riziką (PCI SSC, 2024). Pagrindiniai kortelių tinklai, tokie kaip „Visa“, „MasterCard“, „Discover“, „American Express“ ir „JCB“, įpareigoja prekybininkus ir paslaugų teikėjus pasiekti tam tikrus atitikties lygius (PCI SSC, 2024). Tačiau 12 reikalavimų yra netrivialūs įgyvendinti dėl jų sudėtingumo techniniu ir organizaciniu požiūriu. Pavyzdžiui, plačiai pripažįstama, kad saugumo raktų valdymą yra sudėtinga išlaikyti. Be to, standartas reikalauja nuolat vertinti savo saugumo programas, o tai daugeliui įmonių dažnai laikoma našta. Pastebėta, kad daugelis prekybininkų, vartotojų ir paslaugų teikėjų susiduria su sunkumais pritaikant standartus. Nepaisant to, PCI DSS lygio neatitiktis yra aukšta. Pasak „Visa“ 2016 m. tik 22 proc. didžiausių prekybininkų atitiko PCI reikalavimus (Alotaibi et al., 2016).

Kadangi PCI DSS reikalavimų įgyvendinimas reikalauja daug pastangų ir techninės kompetencijos, yra nemažai bendrovių, teikiančių atitikties sprendimus PCI DSS reikalavimų laikymuisi. Tačiau norint tinkamai įvertinti ir palyginti jų veiksmingumą, reikia išsamios informacijos apie įmonių galimybę įgyvendinti standartą ir atitinkamų tiekėjų apžvalgų (Wang et al., 2024). Standarto atitikties užtikrinimas sukelia nemažai iššūkių, todėl techninę ir programinę įrangą teikiančioms įmonėms yra daug plėtros galimybių. Pvz., prekybininkai ir bankai palaiko tiesioginius ryšius su klientais (Alotaibi et al., 2016), o klientų duomenys yra naudojami, kad būtų užtikrintos aukštos kokybės klientų aptarnavimo paslaugos. Kartais sunku sekti ir įvertinti duomenų poveikį, tad aktyvus duomenų naudojimas ir paplitimas yra akivaizdus iššūkis saugumo apsaugai (Wang et al., 2024). Nepaisant to, techninė pažanga ilgainiui gali paskatinti iš naujo įvertinti ir peržiūrėti dabartinį standartą, kuris pagerina įmonių saugumą.

1.8.1. Poveikis įmonių išlaidoms

Be standarto apimties, PCI DSS įgyvendinimas organizacijose dažnai apibūdinamas finansiškai ir strategiškai sudėtingu procesu dėl griežtų reikalavimų, painių gairių ir neapibrėžto įgyvendinimo elgsenos pobūdžio (Nanda et al., 2018). Nors didelėms ir mažoms įmonėms PCI DSS procedūros nesiskiria (Rees, 2012), paminima, kad mažos ar vidutinės įmonės dažnai neturi pakankamų informacinių technologijų išteklių ar saugumo kompetencijų, kad būtų pasiekta pilna standarto atitiktis (Nanda et al., 2018).

PCI DSS atitikties įgyvendinimo kaina priklauso nuo organizacijos dydžio, mokėjimo tinklų, kibernetinio saugumo specialistų, todėl užtikrinimas gali kainuoti nuo kelių šimtų iki milijonų piniginių vienetų (Chippagiri ir Ramesh, 2025).

Lentelė 9

Poveikis įmonių išlaidoms

Įmonės lygis	Atitikties įgyvendinimas	Galimas įgyvendinimo kainos rėžis	Galima bauda (mokama kasmet)
1	SAQ	1 tūkst. – 10 tūkst.	5 tūkst. – 10 tūkst. (gali siekti ir 50 tūkst.)
2	SAQ + Penetracijos testai	10 tūkst. – 50 tūkst.	25 tūkst. – 50 tūkst.
3	SAQ + Penetracijos testai	10 tūkst. – 50 tūkst.	10 tūkst. – 25 tūkst.
4	ROC su QSA	50 tūkst. – 250 tūkst. ir daugiau	5 tūkst. – 10 tūkst.

Šaltinis: sudaryta pagal internetinius šaltinius.

Norint ne tik įgyvendinti, bet ir valdyti PCI DSS standarto atitiktį įvairaus dydžio organizacijoms, yra jaučiamas finansinis poreikis, kadangi išlaidos yra reikalingo standarto įgyvendinimui ir priežiūrai (Chippagiri ir Ramesh, 2025). Pradines išlaidas sudaro infrastruktūros atnaujinimas, saugumo kontrolės diegimas ir konsultacinės paslaugos. Priežiūros išlaidos apima reguliarius vertinimus, technologijų atnaujinimus, nuolatines stebėsenos sistemas ir būtiną personalo mokymą (Chippagiri ir Ramesh, 2025). Mažos ir vidutinės įmonės susiduria su dideliais iššūkiais, nes turi atitikti tuos pačius reikalavimus kaip ir didelės organizacijos. Šis neproporcingas poveikis dažnai verčia mažesnes organizacijas priimti sudėtingus sprendimus dėl išteklių paskirstymo ir investicijų į saugumą.

1.8.2. Techninio sudėtingumo ir aiškinimo iššūkiai

Organizacijos patiria daugialypių sunkumų nuolat palaikydamos atitiktį – nepakanka vienkartinio įdiegimo, reikia nuolatinio stebėjimo, audito ir darbuotojų sąmoningumo ugdymo. Todėl organizacijos dažnai susiduria su sunkumais integruojant atitikties reikalavimus su jau turimomis technologijų infrastruktūromis bei senesnėmis specializuotomis verslo programomis (Chippagiri ir Ramesh, 2025).

Standarto apimtis skirtingoms organizacijoms turi įvairiapusę reikšmę, todėl kai kurie organizacijų projektų vadovai apimties nustatymą apibrėžia kaip projektą, ką daryti ir kaip jį įgyvendinti (Rees, 2010). PCI DSS 10 reikalavime reikalaujama, kad įmonės sektų ir stebėtų prieigas prie tinklo išteklių ir kortelių savininkų duomenų – reguliariai testuotų saugumo sistemas ir procesus. Taip pat dažnai susiduriama su sistemų senėjimu, silpna tinklo segmentacija, nepakankamu pažeidžiamumų testavimu ar silpna prieigos kontrole. Pasak Nanda et al. (2018) vienas iš reikšmingų iššūkių PCI DSS įgyvendinimo procese yra organizacijų tendencija selektyviai interpretuoti standarto reikalavimus, t. y. laikyti, jog privaloma taikyti tik tas nuostatas, kurios, jų manymu, tik tiesiogiai susijusios su jų veikla, taip praleidžiant bendrą sisteminį požiūrį į duomenų apsaugą. Atsižvelgiant į šiuos aspektus, PCI DSS reikalavimų įgyvendinimas reikalauja ne tik techninių sprendimų, bet ir strateginio planavimo, aiškaus apimties nustatymo bei nuolatinių organizacinių pastangų.

1.8.3. Išteklių reikalavimai priežiūrai

Nuolatinė PCI DSS atitikties priežiūra reikalauja didelių žmogiškųjų ir veiklos išteklių, todėl organizacijai kyla nuolatinių iššūkių. Įmonės turi parengti išsamias saugumo programas, į kurias būtų įtraukta reguliari vertinimo veikla, nuolatinė stebėsena, reagavimo į incidentus pajėgumai ir dokumentų tvarkymas (Chippagiri ir Ramesh, 2025), tad informuotumas, darbuotojų elgesys, saviveiksmingumas, vertė ir atitikties sąnaudos prisideda prie papildomų iššūkių (Clapper ir Richmond, 2016). Standarto reikalavimai apima ne tik techninį įgyvendinimą, bet ir mokymo programas, norint išlaikyti kvalifikuotus darbuotojus, gebančius suprasti ir įgyvendinti sudėtingus ir atsinaujinančius reikalavimus. Įmonėms, turinčioms ribotą darbuotojų skaičių, didžiausias iššūkis yra išlaikyti tinkamą kompetenciją ir suvaldyti išlaidų apribojimus, kad būtų kruopščiai subalansuoti ištekliai (Chippagiri ir Ramesh, 2025). Taigi, norint užtikrinti veiksmingą PCI DSS standarto įgyvendinimą, būtina ne tik techninė infrastruktūra, bet ir nuosekliai vykdomos mokymų programos, incidentų valdymas, įvertinimo procesai bei darbuotojų kompetencijos palaikymas.

2. DAUGIAKRITERINIO ĮVERTINIMO METODO TOPSIS TEORINĖ ANALIZĖ

Antrame teoriniame skyriuje atlikta daugiakriterinio metodo TOPSIS apžvalga, aprašyta jo samprata, veikimo principas ir pagrindiniai algoritmo etapai. Be to, skyriuje aptariami TOPSIS metodo privalumai ir ribotumai.

2.1. Daugiakriterinio sprendimų priėmimo metodų apžvalga

Jau keletą dešimtmečių sprendimo priėmimams vis dažniau naudojami daugiakriterinio įvertinimo metodai (angl. *Multi-Criteria Decision Making*, MCDM). Išskiriami du pagrindiniai daugiakriterinio įvertinimo metodai: MODM (angl. *Multi-Objective Decision Making*) – tai daugiakriterinis optimizacijos metodas, kai remiamasi prioritetų struktūromis, norint priimti sprendimą ir MADM (angl. *Multi-Attribute Decision Making*) – tai daugiakriterinis alternatyvų metodas, kai sprendimų priėmimas vykdomas tik po to, kai yra atliktas kriterijų vertinimas. Tad MODM orientuojasi į besitęsiančią sprendimų erdvę, kai MADM koncentruojasi į iš anksto nustatytas sprendimų alternatyvas (Madanchian ir Taherdoost, 2023). Todėl tyrime buvo pasirinktas vienas iš MADM metodų.

MADM problemos sprendimo būdas taiko sprendimų matricą, kur matrica yra dydžio ($M\ x\ N$), kur $A_1, A_2, \ldots, A_m$ yra galimos alternatyvos, kurį pasirenka sprendimų priėmėjas. $C_1, C_2, \ldots, C_n$, yra kriterijai, su kuriais skaičiuojami galutiniai sprendimai. x_{ij} yra alternatyvos A_{i} vertinimas atsižvelgiant į kriterijus C_j, o w_j yra kriterijaus svoris. $i = 1,2,3, \ldots, M$ ir $j = 1,2,3, \ldots, N$. Taigi, pradinis atvaizdavimas gali būti (Pavič ir Novoselac, 2013):

Lentelė 10

MADM problemos sprendimas

Kriterijus	C_1	C_2	$\cdots$	C_n
Svoris	w_1	w_2	$\cdots$	w_n
A_1	x_{11}	x_{12}	$\cdots$	x_{1n}
A_2	x_{21}	x_{22}	$\cdots$	x_{2n}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
A_m	x_{m1}	x_{m2}	$\cdots$	x_{mn}

Šaltinis: sudaryta Pavič ir Novoselac, 2013.

MADM turi keletą skirtingų metodų, kurie padeda palyginti ir suskirstyti įvairias turimas alternatyvas pagal prioritetus akademiniame kontekste. Atsižvelgiant į šio tyrimo tikslą, galima naudoti COPRAS (angl. *COmplex PRoportional ASsessment of projects*), TOPSIS (angl. *Technique for Order of Preference by Similarity to Ideal Solution*), VIKOR (serb. *VlseKriterijumska Optimizacija I*

Kompromisno Resenje) (Antuchevičienė et al., 2011) metodus. COPRAS – tai metodas, orientuotas į naudos ir sąnaudų kriterijus. TOPSIS – metodas renka „geriausią“ alternatyvą pagal tai, kaip ji yra arčiausiai yra teigiamo idealaus sprendimo ir toliausiai nuo neigiamo idealaus. VIKOR – metodas, kai naudojami tarpusavyje konfliktuojantys kriterijai ir reikia rasti bendrą sprendimą. Atsižvelgiant į tai, kad PCI DSS turi vertinamų kriterijų struktūrą ir didžiausias tikslas yra gauti aiškų ir objektyvų įmonės atitikties PCI DSS standartui įvertinimą, TOPSIS metodas laikytinas tinkamiausiu sprendimu.

Palyginus metodus pagal prioritetų nustatymą, TOPSIS buvo pasirinktas kaip vienas iš geriausių metodų, nes jis palengvina prioritetinių kriterijų išskyrimą iš sprendimų priėmimo matricos, palaiko hierarchijos procesą, padeda išvengti dviprasmiškumo.

2.2. **TOPSIS metodo samprata ir veikimo principas**

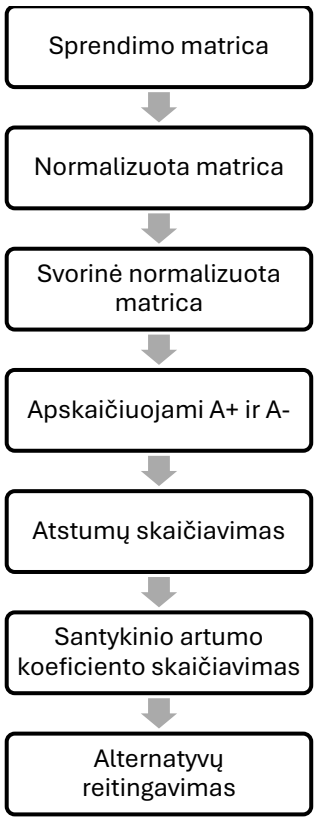
TOPSIS – tai technika, skirta prioritetų nustatymui pagal panašumą idealiam sprendimui, kuris sprendžia realias problemas, analizuodamas, lygindamas ir reitinguodamas alternatyvas, kad būtų pasirinktas geriausias ir tinkamiausias variantas, atsižvelgiant į reikiamus kriterijus (Madanchian ir Taherdoost, 2023). Kadangi PCI DSS vertinimas turi daug kriterijų, susideda iš tinklo kontrolės, prieigos apsaugos, konfigūracijos valdymo, rizikų mažinimo ir kt. Šiuo atveju, naudojant TOPSIS metodą, analizuojant visus PCI DSS reikalavimus, kiekvienam jų galima priskirti skirtingus svorius.

TOPSIS metodas leidžia apskaičiuoti įvertinimo lygį atitikčiai matematiškai, kadangi apima rėžio nuo „idealaus“ iki „blogiausio“ skaičiavimą. Kiekvienas tiekėjo produkto pasiūlymas yra traktuojamas kaip alternatyva, kuri vertinama pagal saugumą, įgyvendinimo laiką, vienkartinę ir mėnesinę kainą, reikalavimų aprėptį, palaikymo lygį. Toliau remiantis TOPSIS, atliekama verčių normalizacija, kuri leidžia suvienodinti turimus kriterijus. Todėl TOPSIS yra artimiausias idealiai alternatyvai ir dažnai labiausiai nutolęs nuo blogiausio varianto, o tai atitinka praktinį organizacijos tikslą – gauti maksimalų saugumo ir atitikties įvertį su ribotais resursais.

Skirtingi atributai atspindi skirtingus kriterijus, todėl jie gali prieštarauti vieni kitiems, kiekvienas atributas gali turėti skirtingus matavimo vienetus. Taigi, pagal TOPSIS metodą skirtingi svoriai yra normalizuoti, kad jų suma būtų lygį vienetui.

2.3. **TOPSIS algoritmo etapai**

TOPSIS metodas turi tikslius matematinius žingsnius, kurie leidžia įvertinti ir reitinguoti alternatyvas pagal jų artumą idealiam sprendimui. Metodo algoritmas susideda iš keleto aiškiai apibrėžtų etapų, kurie užtikrina struktūruotą ir objektyvų daugiakriterinį vertinimą, žiūrint schemą (Madanchian ir Taherdoost, 2023):



Šaltinis: sudaryta pagal Madanchian ir Taherdoost (2023).

3 pav. TOPSIS algoritmo etapai

1 etapas. Sprendimo matricos sudarymas.

Pirmiausia, sudaroma sprendimo matrica $X_{ij} = \left[x_{ij}\right]_{mxn}$, kur:

- $i = 1,2,\cdots,m$ atitinka alternatyvas;
- $j = 1,2,\cdots,n$ atitinka kriterijus;
- x_{ij} nurodo skirtingų kriterijų reikšmes su skirtingais matavimo vienetais.

$$X = \begin{bmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{m1} & \cdots & x_{mn} \end{bmatrix}_{mxn} \quad (1)$$

2 etapas. Sprendimo matricos normalizavimas.

Kiekvienas kriterijus gali turėti skirtingus matavimo vienetus, kad būtų juos galima palyginti, svarbu atlikti skaičių normalizavimą:

$$r_{ij} = \frac{x_{ij}}{\sum_{i=1}^{m} {x_{ij}}^n} \quad (2)$$

Gaunama normalizuota matrica $R = \left[r_{ij}\right]_{mxn}$, kai r_{ij} priklauso intervalui $\langle 0,1 \rangle$.

3 etapas. Svertinės normalizuotos matricos sudarymas.

Svarbu sudaryti kriterijų svorio vektorių $W = (w_1, w_2, \dots, w_n)$, kuris padeda tikslingai paskirstyti svorius, tad svoriai turi tenkinti lygtį:

$$\sum_{j=1}^{n} w_j = 1 \quad (3)$$

Normalizuotos reikšmės dauginamos iš kriterijų svorių w_j:

$$v_{ij} = w_j r_{ij} = w_j \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}{}^n}} \quad (4)$$

Taip gaunama svertinė normalizuota matrica $V = \left[v_{ij}\right]_{mxn}$, kuri nurodo kriterijų svarbą vertinime.

4 etapas. Teigiamai idealaus ir neigiamai idealaus sprendimo nustatymas.

Nustatomi du hipotetiniai sprendimai:

- Teigiamas idealus sprendimas A^+ - svarbiausios kriterijų reikšmės;
- Neigiamas idealus sprendimas A^- - mažiausiai svarbios kriterijų reikšmės.

Jei kriterijus yra naudos tipo:

$$A^+ = \max_i v_{ij}, A^- = \min_i v_{ij} \quad (5)$$

Jei kriterijus yra sąnaudų tipo:

$$A^+ = \min_i v_{ij}, A^- = \max_i v_{ij} \quad (6)$$

5 etapas. Atstumų nuo teigiamai idealaus ir neigiamai idealaus sprendimo skaičiavimas.

Kiekvienai alternatyvai yra apskaičiuojami Euklido atstumai:

$$S_i^+ = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - v_{ij}^+\right)^2} \quad (7)$$

$$S_i^- = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - v_{ij}^-\right)^2} \quad (8)$$

6 etapas. Santykinio artumo koeficiento skaičiavimas.

Skaičiuojamas artumo idealiajam sprendimui koeficientas, kur

- $C_j = [0; 1]$;
- Alternatyvos rikiuojamos pagal C_j, $C_j = 1$ idealiausia, $C_j = 0$ blogiausia.

$$C_j = \frac{s_j^-}{s_j^+ + s_j^-} \quad (9)$$

7 etapas. Alternatyvų reitingavimas.

Alternatyvos reitinguojamos mažėjančia tvarka pagal C_j reikšmes. Didžiausią C_j vienetų reikšmę turinti alternatyva laikoma optimaliausia.

Taigi, TOPSIS metodo algoritmas susideda iš aiškių ir struktūruotų žingsnių.

2.4. **TOPSIS metodo privalumai ir trūkumai**

TOPSIS metodas yra laikomas vienu labiausiai taikomų daugiakriterinio sprendimo metodų dėl paprastumo, aiškios logikos ir plataus pritaikomumo. Mokslinėje literatūroje pabrėžiama, kad šis metodas efektyviai atspindi racionalų sprendimų priėmimo procesą, nes remiasi alternatyvos artumu idealiajam sprendimui ir tuo pačiu nutolimu nuo neigiamo sprendimo (Madanchian ir Taherdoost, 2023).

TOPSIS privalumai:

- Parodo žmogaus sprendimo pasirinkimo logiką;
- Skalės vertė apžvelgia geriausius ir blogiausius alternatyvius variantus;
- Gana paprastas skaičiavimo procesas, todėl jį galima pritaikyti skaitmeninėse skaičiuoklėse;
- Metodo žingsnių skaičius nepriklauso nuo kriterijų kiekio, todėl išlieka stabilus net ir esant dideliam kriterijų skaičiui;
- Kriterijų svorių nustatymas yra subjektyvus, todėl turi įtakos rezultatams;
- Leidžia vienu metu įvertinti ir kiekybinius, ir kokybinius kriterijus.

Taigi, dėl šių savybių TOPSIS metodas yra laikomas vienu universaliausių sprendimo metodų, sprendžiant sudėtingus vertinimo uždavinius.

TOPSIS trūkumai:

- Metodas naudoja Euklido atstumo skaičiavimą, o jis neturi galimybės atsižvelgti į kriterijų tarpusavio koreliaciją;
- Kartais nutinka taip, kad alternatyvos tuo pačiu metu gali būti artimos ir teigiamai, ir neigiamai idealioms vertėms;
- Pasitaiko atvejų, kai netiksliai apibrėžti duomenys gali būti nepakankamai tiksliai apdoroti.

Taigi, nors TOPSIS metodas turi šiek tiek trūkumų, tačiau metodas turi daugiau teigiamų savybių, kurios padeda išlaikyti metodo stabilumą ir sumažinti sprendimų neapibrėžtumo poveikį.

2.5. **TOPSIS metodo taikymo galimybės informacijos saugos vertinime**

Informacijos saugos vertinimas įmonėse yra gana sudėtingas procesas, kadangi tai apima daugybę skirtingų procesų ir technologinių priemonių. Vis dar nėra vieningo ir universalaus metodo, kuris leistų objektyviai apskaičiuoti organizacijos atitikties lygį informacijos saugos standartams. Du Preez ir Pieterse (2006) pabrėžia struktūruotų algoritmų kūrimą, kurie galėtų apskaičiuoti saugos atitikties koeficientą iš įvairių tipų duomenų – nominalių, ordinalių ir skaitinių. TOPSIS metodas yra tinkamas tais

atvejais, kai sprendimų priėmimui reikia integruoti tiek kokybinius, tiek kiekybinius duomenis (Madanchian ir Taherdoost, 2023).

Informacijos saugumo kontekste kiekvienas PCI DSS standarto reikalavimas gali būti laikomas atskiru kriterijumi, kuriam yra suteikiamas svoris. Apibendrinant galima teigti, kad TOPSIS metodas yra tinkamas ir moksliškai pagrįstas metodas įmonės informacijos saugos ir PCI DSS atitikties įvertinimui, nes:

- Leidžia kiekybiškai išreikšti atitikties lygį;
- Užtikrina rezultatų palyginamumą;
- Padeda identifikuoti silpnąsias vietas;
- Suformuoja galimas alternatyvas, atsižvelgiant į nustatytus svorius;
- Sudaro sąlygas objektyviam sprendimų priėmimui.

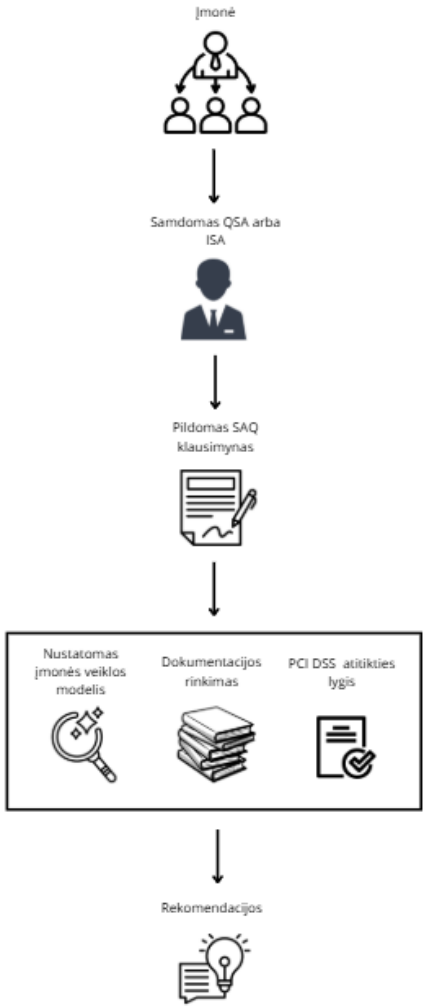
Taigi, TOPSIS metodas pasirenkamas kaip pagrindinė daugiakriterinio įvertinimo priemonė įmonės atitikties PCI DSS standarto įvertinimo metodo analizėje.

3. PCI DSS ĮVERTINIMO METODAS

Analitinėje dalyje apžvelgtos pagrindinės PCI DSS įvertinimo metodo dalys, tyrimo koncepcija, sprendimo esmė ir naujumas. Pateikti pagrindiniai reikalavimai ir kriterijai, reikalingi tolimesnei tyrimo analizei atlikti.

3.1. Tyrimo problemos koncepcija

Mokėjimo kortelių duomenų apsauga yra svarbi ne tik finansinėms institucijoms, kurios priima, tvarko ir apdoroja mokėjimo transakcijas, bet ir visai mokėjimo ekosistemai, kurią sudaro prekybininkai (įmonės) ir galutiniai vartotojai (kortelės savininkai). PCI DSS yra sukurtas siekiant užtikrinti mokėjimo kortelių duomenų apsaugą ir sumažinti sukčiavimo bei duomenų vagystės riziką. Tačiau praktikoje organizacijos susiduria su iššūkiais interpretuojant ir įgyvendinant šio standarto reikalavimus.



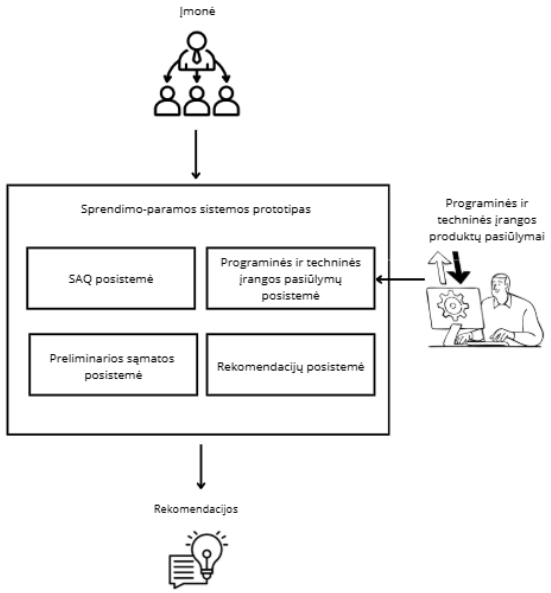
Šaltinis: sudaryta autoriaus.

4 pav. Tradicinė PCI DSS įvertinimo schema

Pateikta schema atspindi tradicinį PCI DSS atitikties įvertinimo procesą, kuris dažniausiai yra vykdomas rankiniu, konsultaciniu ir dokumentiniu būdu.

1. Įmonė samdo išorinį QSA arba vidinį ISA. Specialistas analizuoja įmonės veiklos sritį, mokėjimų priėmimo kanalus, duomenų srautus, IT architektūros tipus, technologijas ir sąveikas su mokėjimo kortelių duomenimis.
2. QSA arba ISA renka įmonės saugumo dokumentus, nagrinėja procedūras, įrodymus apie kontrolės priemonių veikimą ir t.t. Šis etapas laikomas vienu iš daugiausiai laiko ir resursų reikalaujančiu etapu.
3. Toliau vykdomas SAQ klausimyno pildymas, kuris yra rankinis, reikalauja daug laiko, priklauso nuo įmonės dokumentacijos kokybės, yra jautrus interpretacijoms.
4. Surinktus duomenis QSA apdoroja: įvertina atskirų kontrolės punktų atitiktį, identifikuoja spragas. Vertinimas yra subjektyvus ir grindžiamas eksperto patirtimi, todėl skirtingi auditoriai gali pateikti skirtingus vertinimus.
5. Tuomet rengiamos rekomendacijos, atsižvelgiant į neatitikimų sąrašą, reikiamų kontrolės priemonių įgyvendinimą. Šis etapas brangus, reikalauja papildomų konsultacijų, pakartotinių susitikimų, dokumentų korekcijų.

Esminė problema ta, kad procesas yra lėtas, brangus ir neefektyvus. Vertinimas pagrįstas žmogiškuoju faktoriumi, sunaudojama daug laiko, norint gauti galutinį rezultatą bei kainuoja daug lėšų. Taigi, tradicinis PCI DSS įvertinimo procesas yra imlus laikui, resursams, yra fragmentiškas, todėl įmonės neturi priemonės, kuri padėtų greitai įsivertinti savo atitikties lygį, suprasti ne tik neatitiktis, bet ir įgyvendinimo kainą, pasirinkti sprendimų tiekėjus.



Šaltinis: sudaryta autoriaus.

5 pav. Galimo įvertinimo metodo schema

Pateikta įvertinimo metodo schema iliustruoja siūlomo PCI DSS atitikties įvertinimo metodo logiką ir pagrindinius informacijos srautus. Metodas leistų sumažinti žmogiškųjų išteklių sąnaudas, padidinti atitikties analizės tikslumą bei pateikti reikalingas rekomendacijas apie programinės ir techninės įrangos tiekėjus. Ši schema parodo automatizuotą, duomenimis grįstą procesą, kuris leistų organizacijoms greitai įsivertinti savo atitikties lygį pagal suagreguotus SAQ klausimus ir gauti preliminarias rekomendacijas reikalingų programinės ir techninės įrangos produktų diegimui

1. Tradiciškai PCI DSS vertinimas reikalauja išankstinės konsultacijos su SAQ ar ISA, o kuriamas įvertinimo metodas leistų šį etapą pakeisti struktūrizuota automatizuota sąsaja – sprendimo-paramos sistema.
2. Procesas prasideda įmonei prisijungus prie sistemos ir užpildžius universalų SAQ klausimyną. Jis yra agreguotas iš skirtingų SAQ tipų, klausimai apjungti pasinaudojant temine analize. Kiekvienas klausimas vertinamas penkiabalėje Likerto skalėje, kur įmonė nurodo savo faktinę atitikties būklę. Kiekviena klausimų grupė turi skirtingą svorį pagal jos reikšmę PCI DSS įgyvendinimui.
3. Apskaičiavus įmonės atitiktį, jai nustatomas galimas rizikos lygis, atsižvelgus į neatitiktis yra pateikiamas rekomendacijų rinkinys, kuriame paminėtos programinės ir techninės įrangos priemonės norimo lygio pasiekimui.

3.2. **Tyrimo sprendimo esmė**

Didėjantis mokėjimo kortelių naudojimas elektroninėje prekyboje ir auganti kibernetinių grėsmių rizika kelia organizacijoms būtinybę užtikrinti saugų mokėjimo kortelių duomenų tvarkymą. PCI DSS standartas įpareigoja organizacijas įgyvendinti technines ir organizacines saugumo priemones.

Tyrimo sprendimo esmė – sukurti metodiškai pagrįstą ir praktiškai taikomą įvertinimo metodą, kuris leistų efektyviai įvertinti įmonės veiklos atitiktį PCI DSS standarto reikalavimams. Siūlomas metodas orientuotas į atitikties lygio įvertinimą, rizikos prognozę ir rekomendacinius tiekėjų pasiūlymus.

Sukurtas metodas sudarys galimybę:

- Struktūruotai įvertinti PCI DSS reikalavimų įgyvendinimo būklę pagal temines kategorijas;
- Nustatyti atitikties įvertinimo lygį naudojant aiškius kriterijus ir TOPSIS metodą;
- Identifikuoti kritines saugumo vietas ir prioritetines tobulinimo sritis;
- Parengti rekomendacijas, orientuotas į efektyvų resursų pasiskirstymą ir rizikų mažinimą.

Taigi, sprendimas grindžiamas automatizuotu požiūriu, apimančiu esamų saugumo kontrolės priemonių įvertinimą, trūkumų identifikavimą ir numatomų tobulinimo krypčių prognozavimą. Tai leistų organizacijai stiprinti informacijos saugumo kultūrą bei gauti preliminarias programinės ir techninės įrangos priemones, reikalingas PCI DSS atitikčiai.

3.3. **Tyrimo sprendimo motyvacija ir naujumas**

Didėjantis organizacijų priklausomumas nuo skaitmeninių mokėjimo sistemų ir auganti kibernetinių atakų rizika (Ell ir Gallucci, 2022) kelia būtinybę efektyviai užtikrinti mokėjimo kortelių

duomenų saugumą. Nors PCI DSS standartas pateikia išsamius reikalavimus, praktikoje daug įmonių susiduria su sunkumais, norint atitikti PCI DSS standarto reikalavimus, ypač mažesnės ar vidutinės įmonės. Dažnu atveju, organizacijos žino, kad privalo atitikti standartą, tačiau joms trūksta priemonių kaip įvertinti esamą būklę, nustatyti trūkumus ir suplanuoti įgyvendinimo etapus. Todėl kyla poreikis sukurti įvertinimo metodą, kuris padėtų organizacijoms suprasti savo pasirengimo lygį ir kryptingai planuoti tobulinimo procesus.

Siūlomo sprendimo naujumas siejamas su tuo, kad siūlomas metodas nėra tik atitikties patvirtinimo priemonė, o kartu pateikia rekomendacijas ir pirminius žingsnius prioritetinių sričių tobulinimui.

Siūlomas metodas išsiskiria tuo, kad jis veikia kaip PCI DSS atitikties vertinimo ir sprendimų-paramos sistemos prototipas, kuris:

1. Įvertina organizacijos lygį pagal PCI DSS temines sritis;
2. Identifikuoja konkrečias silpnąsias įmonės sritis ir rizikas, pasinaudojant TOPSIS metodu;
3. Generuoja rekomendacijas pagal du svorių nustatymo scenarijus;
4. Įtraukia sprendimų tiekėjų pasirinkimą, leidžiantį automatiškai susieti trūkstamas kontrolės priemones su siūlomomis technologijomis ar paslaugomis.

Tokiu būdu kuriamas ne tik įvertinimo įrankis, bet ir praktinis sprendimų planavimo metodas, leidžiantis organizacijoms pereiti nuo formalios atitikties sekimo prie strateginio mokėjimo duomenų saugumo valdymo.

3.4. **Vertinimo metodologinis pagrindimas**

Sistemingas ir praktiškai pritaikomas PCI DSS atitikties įvertinimo metodas turi turėti metodologinį pagrindimą. Tyrime taikoma teminė analizė, Likerto balų skalė ir TOPSIS metodas. Teminė analizė leidžia susisteminti ir logiškai sugrupuoti didelį kiekį PCI DSS reikalavimų, taip sumažinant vertinimo sudėtingumą ir palengvinant rezultatų interpretavimą. Teminė analizė, pasak Ahmed et al. (2025), kompleksinius veiklos aspektus leidžia nuosekliai sujungti į prasmines kategorijas ir taip identifikuoti vertinimo struktūrą, kuri atspindi nagrinėjamo reiškinio kontekstą. Todėl PCI DSS reikalavimai šiame tyrime yra sujungiami į temines kategorijas, atspindinčias skirtingas temas, susijusias su informacijos saugumu.

Teminė analizė yra metodas, skirtas identifikuoti, analizuoti ir struktūruoti reikšmines temas. Kadangi PCI DSS standartas susideda iš skirtingo detalumo reikalavimų, kuriuos vertinant kyla sudėtingumo ir interpretacijos neapibrėžtumo rizika, teminė analizė reikalavimus padeda sujungti į mažesnes prasmines grupes pagal jų funkcinę paskirtį ir semantinę prasmę. Taigi, ši logika gali būti taikoma kuriamame PCI DSS įvertinimo metode, kai vietoje atskirų punktų analizės, kiekvienas reikalavimas yra agreguojamas į konkrečias temas.

Vertinant PCI DSS reikalavimų įgyvendinimo lygį pagal temines kategorijas yra reikalinga vertinimo skalė. Šiame tyrime yra pasirenkama penkių balų Likerto tipo skalė, skirta matuoti požiūrį, nuomonę ar suvokimą mokslinių tyrimų kontekste. Kiekvienas skalės taškas atspindi sutikimo ar

nuomonės laipsnį, leidžiantį tyrėjams paversti subjektyvius atsakymus į kiekybiškai įvertinimus duomenis, skirtus statistinei analizei ir interpretavimui (Koo ir Yang, 2025). Penkių balų skalė yra viena iš labiausiai paplitusių ir pripažintų organizacijos valdymo ir saugumo įverčių praktikoje, nes užtikrina optimalų balansą tarp tikslumo ir vertinimo kokybės (Nemoto ir Beglar, 2014). Mokslinėje literatūroje didesnės (7-10 balų) skalės suteikia daugiau variacijos, tačiau taip padidinamas interpretacijos neapibrėžtumas, atsiranda didesnė subjektyvumo tikimybė (Taherdoost, 2019). Pasak Nemoto ir Beglar (2014), mažesnės (2-3 balų) skalės sukelia vertinimo tikslumo ribojimą, nes neleidžia tiksliai įvertinti nuostatų skirtumų. Taigi, šio tyrimo teminių kategorijų vertinime taikoma penkių balų Likerto tipo skalė.

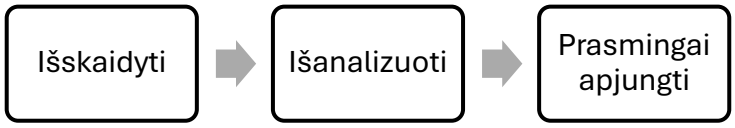
Kiekviena informacijos saugumo reikalavimų dalis, gauta atlikus teminę analizę, įvertinama atsižvelgiant į Likerto tipo penkių balų skalę (Joshi et al., 2015), kadangi ji leidžia įvertinti ne tik faktą, ar kontrolė įgyvendinta, bet ir įgyvendinimo kokybės, stabilumo ir nuoseklumo laipsnį. Pasak Nemoto ir Beglar (2014), penkių balų Likerto skalė suteikia pakankamai jautrumo rezultatų analizei, tačiau išlieka intuityviai suprantama ir pritaikoma praktikoje. Papildomas „0“ lygis apibrėžia procesų nebuvimą, tai leidžia įvertinti, kad kai kurie procesai nėra įgyvendinti.

Šiame tyrime TOPSIS metodas pasirenkamas kaip pagrindinis vertinimo metodologinis pagrindas, kadangi šis metodas užtikrina objektyvų, struktūruotą ir matematiškai pagrįstą daugiakriterinį sprendimų įvertinimą. Skirtingo pobūdžio kriterijai yra integruojami į vieningą įvertinimo sistemą. Pagrindinė metodo esmė remiasi alternatyvų artumo idealiajam sprendimui principu bei padeda išskirti silpnąsias sritis, todėl tai tampa patikimu įrankiu sprendimų pagrindimui ir saugumo gerinimo prioritetų nustatymui. Šis metodas pasižymi lankstumu, kuris padeda kriterijų svorius pritaikyti pagal organizacijos specifiką.

3.5. **PCI DSS reikalavimų agregacija**

Atliekant PCI DSS reikalavimų struktūros formavimą, šio darbo klausimynui buvo pasirinktas įmonės vertinimo klausimynas (angl. *Self-Assesment Questionnaire*, SAQ) D formatas (PCI SSC, 2025). SAQ D yra išsamiausias klausimynas, padengiantis kitus vertinimo klausimynus. Jis apima visus 12 reikalavimų ir daugiau nei 250 smulkesnių specifinių kontrolės priemonių ir testavimo procedūrų. Kiti SAQ tipai yra skirti labiau ribotoms mokėjimų apdorojimo aplinkoms ir apriboja įvertinimą tik iki dalinio kontrolės nustatymo. Taigi, SAQ D buvo pasirinktas dėl savo universalumo visiems organizacijų tipams, nepriklausomai nuo infrastruktūros sudėtingumo, naudojamų technologijų ar mokėjimo duomenų apdorojimo būdų. Kai kurie PCI DSS punktai turi aiškią analogišką paskirtį (pvz.: 1.2.1-1.2.2 – abu atspindi konfigūracijos standartus ir jų taikymą). Todėl apjungti tie reikalavimai, kurie reguliuoja tą pačią technologinę ar valdymo procedūrą, reikalauja tos pačios atsakomybės ar organizacinio proceso, yra matuojami bendrais veikimo kriterijais (dokumentuota, įgyvendinta, atnaujinta ir pan.).

Didelis specifinių reikalavimų kiekis MCDM modelyje sukurtų perteklinį sudėtingumą ir apsunkintų ekspertinį svorių nustatymą. Šiame darbe taikomas teminis reikalavimų agregavimo metodas, kuris smulkius ir detalius klausimus padeda sujungti į logines grupes, remiantis jų turinio bei semantiniu panašumu.



Šaltinis: sudaryta autoriaus.

6 pav. Teminė klausimų analizė

SAQ D klausimynas yra sudarytas iš 251 klausimo. Suagregavus klausimus pagal temines grupes (pagrindinius 12 reikalavimų) iš viso gavosi 59 klausimai:

Lentelė 11

Suagreguoti klausimyno klausimai

Suagreguoti klausimai	
Nr.	**Klausimas**
1 Reikalavimas	**Įdiegti ir palaikyti tinklo saugumo kontrolės priemones.**
1	Kiek išsamiai yra dokumentuotos ir patvirtintos tinklo saugumo konfigūravimo taisyklės bei procedūros?
2	Kiek efektyviai ugniasienės (angl. f*irewalls*) riboja srautą, leidžiant tik būtinus verslui ryšius (ir blokuojant visa kita)?
3	Kiek tiksliai ir reguliariai atnaujinama tinklo topologijos ir duomenų srautų diagrama?
4	Kiek patikimai yra izoliuota kortelių duomenų aplinka (CDE) nuo viešojo interneto (DMZ zonos naudojimas)?
5	Kiek griežtai valdomi pokyčiai ugniasienių taisyklėse (ar kiekvienas pakeitimas yra autorizuojamas ir testuojamas)?
2 Reikalavimas	**Taikyti saugias konfigūracijas visiems sistemos komponentams.**
6	Kiek sistemų komponentų yra sukonfigūruoti pagal pripažintus saugumo standartus?
7	Kiek nuosekliai pašalinti arba pakeisti visi gamintojų numatytieji (angl. *default*) slaptažodžiai prieš diegiant įrangą?
8	Kiek efektyviai užtikrinamas serverių funkcijų atskyrimas (vienas serveris – viena pagrindinė funkcija)?
9	Kiek išsamiai pašalintos arba išjungtos visos nereikalingos paslaugos, protokolai ir programos?

Lentelė 8 tęsinys

Suagreguoti klausimai	
Nr.	**Klausimas**
10	Kiek patikimai užšifruota visa ne konsolinė (nuotolinė) administracinė prieiga prie sistemų?
3 Reikalavimas	**Apsaugoti mokėjimo kortelės savininko duomenis.**
11	Kiek griežtai laikomasi duomenų saugojimo ir naikinimo politikos (saugoma tik tai, kas būtina ir tik tiek, kiek būtina)?
12	Kiek patikimai užtikrinama, kad po autorizacijos niekada nesaugomi jautrūs kodai (CVV/CVC, PIN)?
13	Kiek nuosekliai maskuojamas kortelės numeris (PAN) ekranuose (rodomi tik pirmieji 6 ir paskutiniai 4 skaitmenys)?
14	Kiek stipriai užšifruoti duomenų bazėse saugomi kortelių numeriai (arba naudojama žetonizacija)?
15	Kiek saugiai valdomi kriptografiniai raktai (atskirti nuo duomenų, ribota prieiga, reguliariai keičiami)?
4 Reikalavimas	**Šifruoti kortelių savininkų duomenų perdavimą per atvirus, viešus tinklus.**
16	Kiek efektyviai valdomi saugumo sertifikatai (ar vengiama pasenusių, savarankiškai pasirašytų sertifikatų)?
17	Kiek griežtai techninėmis priemonėmis uždraustas PAN siuntimas neapsaugotais kanalais (el. paštu, SMS, pokalbių programėlėmis)?
18	Kiek patikimai apsaugoti belaidžiai tinklai, naudojami kortelių duomenų perdavimui?
5 Reikalavimas	**Apsaugoti visas sistemas nuo kenkėjiškų programų.**
19	Kiek sistemų (ypač darbo stočių) yra padengta aktyvia ir veikiančia antivirusine apsauga?
20	Kiek dažnai ir automatiškai atnaujinamos antivirusinės parašų bazės?
21	Kiek patikimai apribota vartotojų galimybė savavališkai išjungti antivirusinę apsaugą?
22	Kiek efektyviai naudojamos techninės priemonės ir techniniai sprendimai apsaugai nuo „Phishing“ atakų?
6 Reikalavimas	**Kurti ir palaikyti saugias sistemas ir taikomąsias programas.**
23	Kiek operatyviai (pvz., per 1 mėn. nuo išleidimo) įdiegiami kritiniai saugumo atnaujinimai?
24	Kiek nuosekliai programuotojai vadovaujasi saugaus kodo standartais (pvz.: OWASP) ir atliekamos kodo peržiūros?

Lentelė 8 tęsinys

Suagreguoti klausimai	
Nr.	**Klausimas**
25	Kiek reguliariai atliekama programinio kodo saugumo peržiūra prieš išleidžiant į gamybą ir, kiek programinė įranga apsaugota nuo dažniausių atakų (pvz.: SQL injekcijų, XSS, CSRF ir kt.)?
26	Kiek efektyviai viešosios interneto aplikacijos apsaugotos nuo atakų (pvz.: naudojant WAF) ir yra reguliariai tikrinamos?
27	Kiek griežtai kontroliuojami ir inventorizuojami mokėjimo puslapyje veikiantys skriptai (kad būtų išvengta „e-skimming“ atakų)?
7 Reikalavimas	**Riboti prieigą prie kortelių turėtojų duomenų pagal verslo poreikius.**
28	Kiek tiksliai prieigos teisės suteikiamos tik pagal darbuotojo pareigas ir tik toms sistemoms, vadovaujantis principu „būtina žinoti“ (angl. *need-to-know*)?
29	Kiek reguliariai (pvz., kas 6 mėn.) peržiūrimos ir atnaujinamos vartotojų prieigos teisės ir nebereikalingos teisės panaikinamos?
30	Kiek sistemų prieigos kontrolės mechanizmai nustatyti į „Deny All“ (drausti viską, kas neleista) režimą?
8 Reikalavimas	**Identifikuoti ir autentifikuoti naudotojų prieigą prie sistemos komponentų.**
31	Kiek vartotojų turi ir naudoja unikalius identifikavimo ID (draudžiama naudoti bendras/grupines paskyras)?
32	Kiek operatyviai panaikinama prieiga atleistiems darbuotojams nedelsiant, o neaktyvios paskyros išjungiamos per 90 dienų?
33	Kiek griežtai reikalaujama sudėtingų slaptažodžių (min 12 simbolių, raidės/skaičiai) ir keičiami, jei įtariamas kompromitavimas, bei jų periodinis keitimas?
34	Kiek plačiai naudojama daugiakomponentė autentifikacija (MFA) prisijungiant prie CDE (tiek lokaliai, tiek nuotoliniu būdu)?
35	Kiek griežtai ribojamas ir stebimas trečiųjų šalių prisijungimas prie sistemų?
9 Reikalavimas	**Riboti fizinę prieigą prie kortelių turėtojų duomenų.**
36	Kiek efektyviai kontroliuojamas fizinis patekimas į patalpas per serverius ar tinklo įrangą kortelėmis/biometrija ir stebimas vaizdo kameromis?
37	Kiek griežtai registruojami, identifikuojami ir visada lydimi darbuotojų jautriose zonose?
38	Kiek saugiai laikomos ir naikinamos fizinės laikmenos (popierius, USB, diskai) su kortelių duomenimis yra saugomos seifuose ir klasifikuojamos kaip konfidencialios?

Suagreguoti klausimai	
Nr.	**Klausimas**
39	Kiek reguliariai popieriniai dokumentai ir elektroninės laikmenos su duomenimis yra negrįžtamai sunaikinami (smulkinami), kai tampa nereikalingi?
40	Kiek reguliariai ir atidžiai yra tikrinami kortelių skaitytuvai (POS terminalai), siekiant aptikti klastojimo (angl. *skimming*) įrangą ar neteisėtus pakeitimus?
10 Reikalavimas	**Stebėti ir registruoti prieigą prie visų išteklių ir kortelių turėtojų duomenų.**
41	Kiek sistemų žurnalai (angl. *logs*) įjungti visiems sistemos komponentams ir fiksuoja visus veiksmus su kortelių duomenimis bei administratoriaus veiksmus?
42	Kiek detali informacija: vartotojo ID, įvykio tipas, data/laikas, sėkmė/nesėkmė, įvykio tipas fiksuojama žurnaluose?
43	Kiek patikimai audito žurnalai yra apsaugoti nuo modifikavimo ir kopijuojami į centralizuotą serverį?
44	Kiek reguliariai ir atidžiai peržiūrimi saugumo pranešimai ir kritiniai žurnalai?
45	Kiek ilgai saugomi audito įrašai (ar atitinka reikalavimą: 1 metai saugojimo, 3 mėn. greitai pasiekiami)?
11 Reikalavimas	**Reguliariai testuoti saugumo sistemas ir tinklus.**
46	Kiek reguliariai (pvz., kas ketvirtį) atliekami vidiniai tinklo pažeidžiamumų skenavimai, siekiant aptikti neautorizuotus belaidžius prisijungimo taškus?
47	Kiek operatyviai ištaisomos spragos, aptiktos ASV (angl. *Approved Scanning Vendor)* išorinio skenavimo metu*?*
48	Kiek reguliariai ir išsamiai atliekami įsilaužimo testai tiek iš vidaus, tiek iš išorės?
49	Kiek efektyviai veikia įsibrovimų aptikimo/prevencijos sistemos (IDS/IPS) ties CDE perimetru?
50	Kiek dažnai atliekamas belaidžių prieigos taškų skenavimas siekiant aptikti neautorizuotus įrenginius?
51	Kiek efektyviai ir išsamiai yra naudojami failų vientisumo stebėjimo įrankiai, pranešantys apie neautorizuotus sisteminių failų pakeitimus?
12 Reikalavimas	**Užtikrinti informacijos saugumo politiką organizacijos politiką ir programas.**
52	Kiek išsamiai parengta, atnaujinta ir išplatinta informacijos saugumo politika?
53	Kiek reguliariai atliekama rizikos analizė (angl. *Targeted Risk Analysis*) visiems PCI DSS reikalavimams?

Lentelė 8 tęsinys

Suagreguoti klausimai	
Nr.	**Klausimas**
54	Kiek aiškiai yra patvirtinta priimtino naudojimo politika (angl. *Acceptable Use Policy*) ir valdomas naudojamų technologijų sąrašas?
55	Kiek tiksliai dokumentuota ir kasmet patvirtinama PCI DSS taikymo sritis (angl. *scope*)?
56	Kiek procentų darbuotojų praeina kasmetinius saugumo mokymus (įskaitant apsaugą nuo sukčiavimo) priimant į darbą ir kasmet?
57	Kiek kruopščiai tikrinami kandidatai prieš įdarbinant į jautrias pozicijas, susijusias su CDE?
58	Kiek griežtai valdomi trečiųjų šalių paslaugų teikėjai (sutartys, atsakomybės, atitikties standartui tikrinimas)?
59	Kiek pasirengusi organizacija reaguoti į incidentus (ar yra sukurtas ir ištestuotas incidentų valdymo planas, veikiantis 24/7?)?

Šaltinis: sudaryta pagal PCI SSC (2025).

Pirmiausia, buvo išsamiai analizuoti pirminiai SAQ D klausimyno klausimai, siekiant nustatyti jų prasmę ir ryšį su PCI DSS reikalavimais. Remiantis semantiniu panašumu, klausimai, kurie turėjo panašią prasmę ir apima tą patį saugumo aspektą, buvo sujungti į vieną apibendrintą kriterijų. Taigi, įmonės atitikties PCI DSS standartui įvertinimo metodo kriterijų sistema buvo sudaryta, remiantis oficialiais PCI DSS reikalavimais ir SAQ D klausimynu.

3.6. **Vertinimo kriterijų nustatymas**

Atsižvelgiant į tai, kad PCI DSS standartas yra suskirstytas į 12 pagrindinių informacijos saugumo reikalavimų, agreguojant klausimus buvo suformuotas 59 klausimų, o kartu ir įvertinimo kriterijų rinkinys. Jie pažymėti numeriais nuo K1 iki K59. Įvertinimo kriterijai yra reikalingi vertinant kiekvieno programinės ir techninės įrangos tiekėjo siūlomus produktus. Kadangi yra vertinama kiekviena įmonė, tad vertinami ir tiekėjų siūlomi produktai.

Lentelė 12

Pagal suagreguotus klausimus išskirti įvertinimo kriterijai

Kriterijaus kodas	PCI DSS reikalavimas	Įvertinimo kriterijus
K1	1 reikalavimas	Dokumentuotų ir patvirtintų tinklo saugumo konfigūravimo taisyklių bei procedūrų išsamumas
K2	1 reikalavimas	Ugniasienių efektyvumas ribojant srautą tik būtiniems verslo ryšiams

Lentelė 13

tęsinys

Kriterijaus kodas	PCI DSS reikalavimas	Įvertinimo kriterijus
K3	1 reikalavimas	Tinklo topologijos ir duomenų srautų diagramų tikslumas ir reguliarus atnaujinimas
K4	1 reikalavimas	CDE izoliavimo nuo viešojo interneto patikimumas (DMZ naudojimas)
K5	1 reikalavimas	Ugniasienių taisyklių keitimų kontrolės ir autorizavimo griežtumas
K6	2 reikalavimas	Sistemų konfigūravimo pagal saugumo standartus (pvz., CIS) laikymasis
K7	2 reikalavimas	Numatytojo slaptažodžio pakeitimo užtikrinimas prieš diegiant įrangą
K8	2 reikalavimas	Serverių funkcijų atskyrimo nuoseklumas
K9	2 reikalavimas	Nereikalingų paslaugų, protokolų ir programų pašalinimas
K10	2 reikalavimas	Nuotolinės administracinės prieigos šifravimo patikimumas
K11	3 reikalavimas	Duomenų saugojimo ir naikinimo politikos laikymasis
K12	3 reikalavimas	Jautrių autentifikavimo duomenų nesaugojimas po autorizacijos
K13	3 reikalavimas	PAN maskavimo nuoseklumas ekranuose
K14	3 reikalavimas	Duomenų šifravimo ar žetonizacijos stiprumas
K15	3 reikalavimas	Kriptografinių raktų valdymo saugumas
K16	4 reikalavimas	Saugumo sertifikatų valdymo efektyvumas
K17	4 reikalavimas	PAN siuntimo neapsaugotais kanalais prevencijos griežtumas
K18	4 reikalavimas	Belaidžių tinklų apsaugos lygis
K19	5 reikalavimas	Antivirusinės apsaugos įdiegimo mastas
K20	5 reikalavimas	Antivirusinių parašų atnaujinimo reguliarumas
K21	5 reikalavimas	Vartotojų galimybės išjungti antivirusinę kontrolės ribojimas
K22	5 reikalavimas	Techninių priemonių efektyvumas prieš „*phishing“*
K23	6 reikalavimas	Saugių atnaujinimų diegimo operatyvumas
K24	6 reikalavimas	Saugios programavimo praktikos laikymasis
K25	6 reikalavimas	Programinio kodo saugumo peržiūrų reguliarumas
K26	6 reikalavimas	Viešųjų aplikacijų apsaugos nuo atakų veiksmingumas
K27	6 reikalavimas	Kodo kontrolės griežtumas „*e-skimming“* prevencijai
K28	7 reikalavimas	Prieigos teisės pagal „*need-to-know*“ principą
K29	7 reikalavimas	Vartotojų prieigos peržiūros reguliarumas
K30	7 reikalavimas	„*Deny All*“ režimo taikymas

Lentelė 14 tęsinys

Kriterijaus kodas	PCI DSS reikalavimas	Įvertinimo kriterijus
K31	8 reikalavimas	Unikalių vartotojų ID naudojimas
K32	8 reikalavimas	Neaktyvių paskyrų ir atleistų darbuotojų prieigos panaikinimas
K33	8 reikalavimas	Slaptažodžių sudėtingumo ir keitimo politika
K34	8 reikalavimas	Daugiakomponentės autentifikacijos naudojimas
K35	8 reikalavimas	Trečiųjų šalių prieigos kontrolė
K36	9 reikalavimas	Fizinės prieigos kontrolės efektyvumas
K37	9 reikalavimas	Lankytojų registravimas ir kontrolė jautriose zonose
K38	9 reikalavimas	Fizinių laikmenų saugojimo saugumas
K39	9 reikalavimas	Laikmenų ir dokumentų naikinimo reguliarumas
K40	9 reikalavimas	POS terminalų tikrinimo reguliarumas
K41	10 reikalavimas	Audito žurnalų aktyvavimo mastas
K42	10 reikalavimas	Žurnalų informacijos detalumas
K43	10 reikalavimas	Žurnalų apsaugos nuo modifikavimo patikimumas
K44	10 reikalavimas	Žurnalų peržiūros reguliarumas
K45	10 reikalavimas	Audito įrašų saugojimo laikotarpis
K46	11 reikalavimas	Pažeidžiamumų skenavimo reguliarumas
K47	11 reikalavimas	ASV spragų šalinimo operatyvumas
K48	11 reikalavimas	Penetracijos testavimo išsamumas
K49	11 reikalavimas	IDS/IPS efektyvumas
K50	11 reikalavimas	Belaidžių taškų stebėsenos dažnumas
K51	11 reikalavimas	Failų vientisumo stebėsenos efektyvumas
K52	12 reikalavimas	Saugumo politikos parengimo išsamumas
K53	12 reikalavimas	Rizikos analizės reguliarumas
K54	12 reikalavimas	Priimtino naudojimo politikos aiškumas
K55	12 reikalavimas	PCI DSS taikymo srities dokumentavimas
K56	12 reikalavimas	Darbuotojų saugumo mokymų apimtis
K57	12 reikalavimas	Kandidatų patikros griežtumas
K58	12 reikalavimas	Trečiųjų šalių valdymas
K59	12 reikalavimas	Incidentų valdymo pasirengimas

Šaltinis: sudaryta autoriaus pagal PCI SSC (2025).

Tiekėjų pasiūlymams papildomai naudojami trys kriterijai dėl tikslesnio pasiūlymų paskirstymo: įgyvendinimo trukmė, vienkartinė ir mėnesinė kainos.

Lentelė 15

Papildomi ekonominiai įvertinimo kriterijai

Kriterijaus kodas	Įvertinimo kriterijus
K60	Įgyvendinimo trukmė (d.)
K61	Vienkartinė kaina (eur)
K62	Mėnesinė kaina (eur)

Šaltinis: sudaryta autoriaus.

Apžvelgus sudarytus reikalavimų kriterijus, PCI DSS reikalavimai apima skirtingas sritis, todėl svarbu suvienodinti kriterijų įvertinimą. Be abejo, norint taikyti TOPSIS metodą būtina visus reikalavimus paversti kiekybiniais rodikliais, todėl kiekvienam kriterijui priskiriamas Likerto skalės įvertinimas nuo 0 („neįgyvendinta/nevykdoma“) iki 5 („optimizuota/ideali“) balų.

Lentelė 16

Įvertinimo skalė

Įvertinimas	Skalės paaiškinimas	Reikšmė
0	Neįgyvendinta (angl. *Incomplete*) kontrolė	Kontrolė neegzistuoja, procesai nevykdomi.
1	Pradinė (angl. *Initial*) kontrolė	Kontrolė egzistuoja, procesai vykdomi tik iš dalies. Atitikties užtikrinimo pastangos yra minimalios arba reaktyvios.
2	Vykdoma (angl. *Basic*) kontrolė	Kontrolė egzistuoja, bet procesai fragmentiški. Yra įdiegti tam tikri atitikties užtikrinimo procesai, tačiau jie yra nenuoseklūs.
3	Apibrėžta (angl. *Standardized*) kontrolė	Kontrolė vykdoma, tačiau nėra nuolatinės stebėsenos. Atitikties procesai yra dokumentuojami, standartizuoti visoje organizacijoje.
4	Valdoma (angl. *Proactive*) kontrolė	Kontrolė integruota į procesus ir reguliariai prižiūrima. Organizacija naudoja duomenis, kad proaktyviai valdytų ir numatytų atitikties riziką.
5	Optimizuota (angl. *Leading*) kontrolė	Kontrolė automatizuota, tobulinama. Atitikties valdymas yra dinamiškas, naudojant pažangias priemones ir įžvalgas nuolatiniam tobulinimui.

Šaltinis: sudaryta autoriaus.

Norint gauti rekomendacinius tiekėjų pasiūlymus, tiekėjai taip pat turi priskirti savo programinei ar techninei įrangai įvertį pagal kriterijus, atsižvelgiant į 5 balų skalės vertinimą:

Lentelė 17

Tiekėjų pasiūlymų įvertinimo skalė

Įvertinimas	Skalės paaiškinimas	Reikšmė
0	Nesiūlomas sprendimas	Tiekėjas nenurodo jokio sprendimo.
1	Minimalus sprendimas	Suteikiamas tik įrankis ar licencija sprendiniui, konfigūracija ir automatizacija neatliekama.
2	Bazinis sprendimas	Sprendimas turi bazinius nustatymus.
3	Standartinis sprendimas	Sprendimas sukonfigūruotas pagal gerąją praktiką, bet reagavimas į incidentus ir atnaujinimai – kliento atsakomybė.
4	Pažangus sprendimas	Automatizuotas sprendimas, galima integracija su kitomis sistemomis.
5	Valdoma paslauga	Tiekėjas siūlo pažangų įrangos sprendimą - valdymą (konfigūravimas, stebėsena ar reagavimas).

Šaltinis: sudaryta autoriaus.

3.7. Įvertinimo metodika ir skaičiavimo logika

PCI DSS reikalavimai yra gana sudėtingi ir reikalauja žmogiškųjų ir finansinių išteklių. Norint palengvinti įvertinimo procesą įmonėms, kurios dar tik planuoja įgyvendinti PCI DSS standarto reikalavimus, yra svarbu pateikti kuo mažiau išteklių reikalaujantį pasiūlymą. Įvertinimo metodika kurta siekiant objektyviai įvertinti įmonių atitiktį PCI DSS reikalavimams ir tiekėjų galimybes prisidėti prie organizacijos atitikties.

Tad pirmiausia, Įvertinimo procesas pradedamas nuo kokybinių PCI DSS reikalavimų konvertavimo kiekybiniais duomenimis. Kaip ir minėta, yra suagreguoti 59 SAQ klausimyno kriterijai ir 3 papildomi kriterijai alternatyvoms, siekiant gauti kuo detalesnį įvertinimą, pasitelkiant semantinį ir turinio panašumus. Tuomet kiekvienas klausimas yra vertinamas Likerto skalėje. Toliau gauti įverčiai sudaro sprendimų matricą, kur eilutės yra galimos sprendimų alternatyvos, o stulpeliai – suagreguoti kriterijai:

Lentelė 18

TOPSIS analizės lentelė

Kriterijus	C_1	C_2	⋯	C_{62}
A_1	$x_{1\,1}$	$x_{1\,2}$	⋯	$x_{1\,62}$
A_2	$x_{2\,1}$	$x_{2\,2}$	⋯	$x_{2\,62}$
⋮	⋮	⋮	⋱	⋮
A_m	$x_{m\,1}$	$x_{m\,2}$	⋯	$x_{m\,62}$

Šaltinis: sudaryta Pavič ir Novoselac, 2013.

Toliau vartotojas nustato kiekvieno kriterijaus svarbą, kuriems pagal tai yra priskiriami svoriai. Pagal daugiakriterinių metodų mokslinius šaltinius kriterijai neturi būti laikomi lygiaverčiais (Zavadskas ir Turskis, 2011). Kuo daugiau klausimų grupėje, tuo daugiau rizikų ji apima. Atitiktį standartui galima apskaičiuoti naudojant skirtingus svorius, pasinaudojant sprendimo matrica. Tiekėjai teikdami savo pasiūlymus įvertina produktus penkių balų skalėje, atsižvelgdami į PCI DSS reikalavimus. Tad naudojant TOPSIS metodą tiekėjų pasiūlymų vertinimas yra reikalingas, norint įmonei pateikti tinkamus variantus.

4. TOPSIS METODO TAIKYMAS PCI DSS ATITIKTIES ANALIZEI

Ketvirtame tyrimo skyriuje aptariamas TOPSIS metodo taikymas PCI DSS atitikties analizei, apibrėžiamos pagrindinės charakteristikos, kriterijų grupavimas ir pagrindinės sprendimo-paramos sistemos prototipo dalys.

4.1. Vertinamų įmonių ir tiekėjų charakteristika

Vertinimui pasirinkti susintetinti duomenys, naudotasi „Gemini 3“ dirbtinio intelekto įrankiu. Analizei panaudota 1000 susintetintų įmonių ir tiekėjų duomenų įrašų. Tiekėjų pasiūlymai generuoti atsižvelgiant į PCI DSS reikalavimus. Tiekėjai skiriasi teikiamų paslaugų apimtimi, kainomis, technologiniu požiūriu atskiruose segmentuose. Įmonių duomenys įvairūs, sugeneruoti skirtingi įmonių rizikos scenarijai. Kiekviena organizacija vertinama pagal 59 klausimus, atsakymai į juos atspindi visų 12 PCI DSS reikalavimų grupių įgyvendinimo lygį.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Imone	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11	K12	K13	K14	K15	K16
2	Imone_0001	0	0	0	0	0	4	4	2	3	2	1	1	1	1	3	
3	Imone_0002	2	2	5	3	5	0	0	0	0	0	5	5	4	2	1	
4	Imone_0003	4	2	1	3	1	4	2	4	2	4	0	0	0	0	0	
5	Imone_0004	1	3	3	4	2	3	1	2	2	2	2	3	1	2	4	
6	Imone_0005	1	2	3	5	4	3	4	2	5	3	2	2	1	5	2	
7	Imone_0006	1	4	2	2	3	2	1	1	3	3	3	1	1	5	2	
8	Imone_0007	2	1	3	3	3	2	3	2	2	1	3	3	3	5	3	
9	Imone_0008	2	5	1	5	4	4	5	2	1	4	1	2	2	2	4	
10	Imone_0009	1	5	5	4	2	1	1	4	4	5	4	3	5	1	4	
11	Imone_0010	3	2	4	2	4	4	2	1	4	1	4	2	5	4	5	
12	Imone_0011	4	2	1	3	5	3	4	5	2	1	3	3	2	1	4	
13	Imone_0012	1	1	4	5	2	1	1	3	4	1	3	2	3	2	2	
14	Imone_0013	3	2	3	4	3	3	2	5	1	1	4	2	1	3	4	
15	Imone_0014	3	4	4	5	4	1	1	1	2	1	5	3	2	2	1	
16	Imone_0015	3	5	4	3	5	4	4	2	3	3	3	5	2	3	2	
17	Imone_0016	2	2	4	4	3	5	4	1	1	2	1	1	5	4	5	
18	Imone_0017	3	4	1	3	2	1	1	4	5	5	5	2	5	4	1	
19	Imone_0018	2	3	2	1	5	5	2	2	5	2	4	1	2	2	3	
20	Imone_0019	4	4	4	3	2	5	4	2	5	3	3	2	5	2	1	
21	Imone_0020	4	3	2	1	4	5	1	2	2	3	4	5	5	4	1	
22	Imone_0021	5	4	1	3	3	1	3	2	3	3	4	2	4	2	2	
23	Imone_0022	3	2	5	3	2	5	3	4	4	3	2	5	4	3	2	
24	Imone_0023	5	4	2	2	1	4	3	1	4	1	3	4	1	2	4	
25	Imone_0024	1	2	1	5	5	3	5	2	2	4	4	4	5	1	5	
26	Imone_0025	5	5	1	4	2	4	3	1	4	2	2	2	5	4	1	
27	Imone_0026	2	3	1	1	2	3	4	4	5	1	2	3	4	2	3	

7 pav. Įmonių duomenų įrašų pavyzdys

Tiekėjų spektras apima pagrindines PCI DSS reikalavimų sritis: kibernetinio ir fizinio saugumo sritis: tinklo, sistemų, programinės įrangos saugumą, prieigos kontrolę ir kitus svarbius informacijos saugumo veiksnius. Tiekėjai vertinti pagal tai, kiek jų teikiami programinės ar techninės įrangos sprendimai gali prisidėti prie konkrečių PCI DSS saugumo standarto reikalavimų įgyvendinimo.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	Tiekejas	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11	K12	K13	K14	K15	K16	K17	K18
2	Tiekejas_0001	5	5	5	5	5	5	5	5	5	1	5	3	2	5	2	1	5	
3	Tiekejas_0002	3	3	1	5	5	5	1	2	5	4	3	4	4	1	4	3	3	
4	Tiekejas_0003	5	3	5	5	4	1	3	4	1	5	4	5	2	5	5	3	1	
5	Tiekejas_0004	5	2	3	3	5	5	3	5	4	4	2	4	5	5	2	1	2	
6	Tiekejas_0005	3	1	3	4	3	1	2	5	2	3	4	4	5	5	4	4	2	
7	Tiekejas_0006	1	3	4	5	3	4	1	3	1	5	3	2	1	5	5	3	5	
8	Tiekejas_0007	5	1	1	5	3	2	4	5	3	5	2	1	1	5	5	3	3	
9	Tiekejas_0008	5	2	4	5	5	3	2	4	5	5	4	2	1	5	5	4	4	
10	Tiekejas_0009	2	1	5	5	3	4	4	2	1	5	4	4	5	5	5	2	5	
11	Tiekejas_0010	5	5	3	5	4	3	3	5	3	5	4	4	5	5	5	3	4	
12	Tiekejas_0011	1	4	1	5	3	1	3	5	2	5	4	4	3	5	5	2	1	
13	Tiekejas_0012	5	3	1	3	5	4	3	4	2	1	3	3	4	5	5	1	5	
14	Tiekejas_0013	4	1	2	5	3	1	2	2	3	4	2	1	3	3	5	3	5	
15	Tiekejas_0014	2	2	5	5	2	4	2	2	5	1	3	3	3	3	2	5	4	
16	Tiekejas_0015	4	3	3	5	1	1	2	5	4	5	1	1	2	5	5	3	2	
17	Tiekejas_0016	4	2	3	4	4	5	1	2	2	4	2	1	1	5	1	3	5	
18	Tiekejas_0017	1	1	3	4	3	2	5	1	1	3	5	2	4	3	5	1	1	
19	Tiekejas_0018	3	3	3	5	5	2	4	2	4	5	5	4	1	5	5	4	1	
20	Tiekejas_0019	2	4	5	5	5	1	4	1	3	5	2	3	1	5	5	3	3	
21	Tiekejas_0020	4	1	4	5	3	2	5	1	2	5	2	1	4	5	5	5	2	
22	Tiekejas_0021	1	2	2	5	2	3	5	3	1	5	4	3	3	5	5	3	3	
23	Tiekejas_0022	3	5	4	5	3	1	5	5	5	5	3	3	5	5	5	1	4	
24	Tiekejas_0023	4	4	4	5	1	5	1	1	1	5	3	1	2	5	2	5	5	
25	Tiekejas_0024	4	2	3	5	2	5	5	2	5	2	1	5	3	1	5	4	4	
26	Tiekejas_0025	2	1	1	5	1	4	1	1	3	5	5	2	3	5	5	2	2	
27	Tiekejas_0026	1	3	1	5	2	3	5	2	4	5	3	2	5	5	5	5	2	

8 pav. Tiekėjų duomenų įrašų pavyzdys

4.2. PCI DSS įvertinimo kriterijų formavimo principai

Įvertinimo kriterijai buvo suformuoti remiantis PCI DSS 12 pagrindinių reikalavimų struktūra. Klausimyno klausimai perkelti į K1-K59 kriterijų sistemą, kur kiekvienas kriterijus turi savo unikalų kodą, priklauso konkrečiam PCI DSS reikalavimui (1-12), atitinka saugumo aspektą, kurį galima kiekybiškai įvertinti.

Įmonė pildo klausimyną ir gauna preliminarią atitiktį 12 PCI DSS reikalavimams. Eksperimentiniame bandyme naudojamas suagreguotas 59 klausimų pagal SAQ D formą klausimynas, kuriame visi punktai yra sujungti į temines grupes pagal semantinį ir turinio panašumą. Kiekviena teminė grupė apima klausimą, kurį įvertina penkių balų Likerto skalėje (nuo 0 – „neįgyvendinta“ iki 5 – „optimizuota“) tam, kad būtų galima sumažinti įvertinimo triukšmą, išvengti panašios reikšmės klausimų bei vėliau turimas vertes pritaikyti TOPSIS metodui.

PCI DSS brandos skalės paaiškinimas

Įvertinimas	Lygis	Reikšmė
0	Neįgyvendinta	Kontrolė neegzistuoja, procesai nevykdomi.
1	Pradinė	Kontrolė egzistuoja, bet procesai minimalūs arba reaktyvūs.
2	Vykdoma	Procesai fragmentiški, egzistuoja tik dalinis atitikties užtikrinimas.
3	Apibrėžta	Procesai dokumentuoti ir standartizuoti, bet stebėsena ribota.
4	Valdoma	Kontrolė integruota į procesus, vyksta reguliari priežiūra.
5	Optimizuota	Kontrolė automatizuota, nuolat tobulinama.

Šaltinis: sudaryta autoriaus.

9 pav. Likerto skalės paaiškinimas įmonėms.

4.3. **Programinės ir techninės įrangos kriterijų grupavimas**

Kiekvienas tiekėjas turi galimybę įvertinti savo siūlomą produktą ir norimą pagerinti įmonės sritį pagal PCI DSS reikalavimus penkiabalėje skalėje. Kadangi kai kurie siūlomi produktai gali gerinti tik tam tikras sritis, buvo sudaryta galima paslaugų analizė, kaip pvz.:

Lentelė 19

Pavyzdinis galimas tiekėjų pasiūlymų grupavimas

PCI DSS reikalavimas	Programinės ir techninės įrangos pasiūlymai	Galimi stiprinami kriterijai
Reikalavimas 1	Ugniasienės, tinklo segmentavimas	K1-K5
Reikalavimas 2	Saugios konfigūracijos	K6-K10
Reikalavimas 3	Kortelių duomenų apsauga	K11-K15
Reikalavimas 4	Duomenų perdavimo apsauga	K16-K18
Reikalavimas 5	Antivirusinė apsauga	K19-K22
Reikalavimas 6	Programų apsauga	K23-K27
Reikalavimas 7	Prieigos kontrolė	K28-K30
Reikalavimas 8	Vartotojų identifikavimas ir autentifikavimas	K31-K35
Reikalavimas 9	Fizinis saugumas	K36-K40
Reikalavimas 10	Log‘ų valdymas	K41-K45
Reikalavimas 11	Testavimas ir stebėsena	K46-K51
Reikalavimas 12	ISMS, politika ir rizika	K52-K59

Šaltinis: sudaryta autoriaus.

K1-K59 yra priskiriami naudos kriterijams – kuo didesnis balas, tuo geriau, K60-K62 yra kaštų kriterijai – kuo mažesnė vertė, tuo geriau.

Kiekvienam kriterijui galima priskirti balų vertinimą (nuo 0 – „nesiūlomas sprendimas“ iki 5 – „valdoma paslauga“). Kriterijų grupavimas vyko pagal temines grupes ir atsižvelgiant į pagrindinius 12 reikalavimų. Analizėje įvertinant tiekėjų įtaką organizacijos saugumui kriterijai buvo įvertinti taip, kad juos būtų galima susieti su realia saugumo įranga ar paslaugomis.

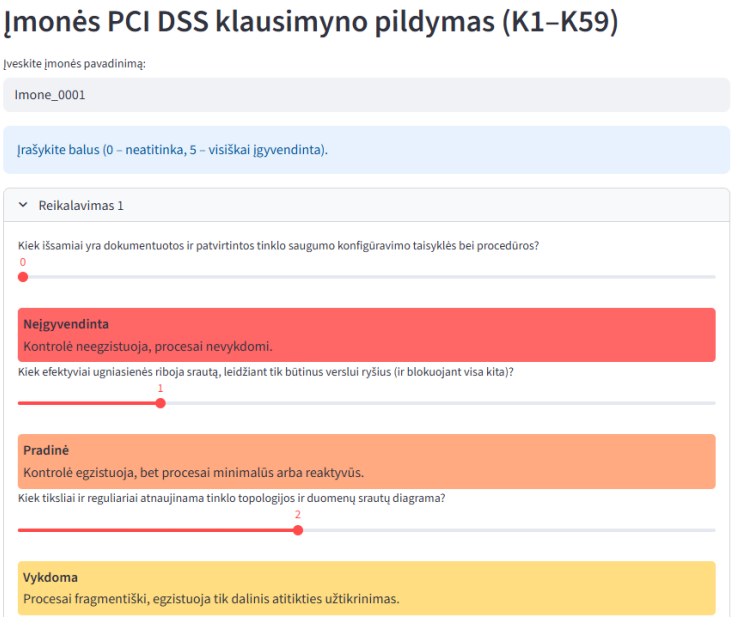
PCI DSS Likerto skalės paaiškinimas

Įvertinimas	Lygis	Reikšmė
0	Nesiūlomas sprendimas	Tiekėjas nenurodo jokio sprendimo.
1	Minimalus sprendimas	Pateikiamas tik įrankis/licencija, nėra konfigūravimo.
2	Bazinis sprendimas	Sprendimas turi bazinius nustatymus.
3	Standartinis sprendimas	Gerosios praktikos konfigūracija, be incidentų valdymo.
4	Pažangus sprendimas	Automatizuotas sprendimas, integruojamas su kitomis sistemomis.
5	Valdoma paslauga	Tiekėjas pilnai valdo sprendimą: konfigūracija, stebėsena, reagavimas.

10 pav. Likerto skalės paaiškinimas tiekėjų paslaugoms

4.4. Įmonės savęs įvertinimo klausimyno pildymas

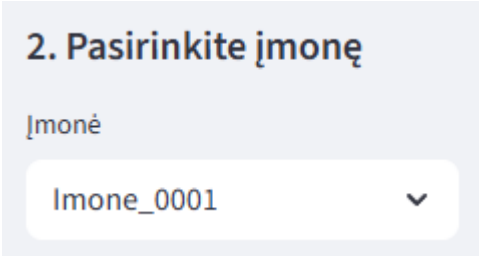
Kiekviena įmonė gali užpildyti klausimyną, kuris yra sudarytas remiantis SAQ D forma. Klausimynas apima 59 klausimus, kurie yra sugrupuoti pagal pagrindinius PCI DSS reikalavimus. Kiekvieną klausimą galima įvertinti balais nuo 0 iki 5, tai parodo atitinkamą įmonės lygį atitikčiai. Skirtingoms įmonėms toks įvertinimo būdas leidžia sistemai individualiai nuspręsti esamą įmonės atitikties balą, atsižvelgiant į skirtingas saugumo kryptis. Savęs įvertinimo rezultatai yra naudojami daugiakriteriniam rezultatų skaičiavimui ir bendram atitikties lygiui nustatyti. Taigi, pagal įverčius toliau pateikiami individualizuoti pasiūlymai pagal kiekvienos organizacijos poreikius.



11 pav. Įmonės klausimyno pildymas

4.5. Įmonės duomenų apžvalga

Tyrimo metu yra analizuojamas nemažas kiekis skirtingų įmonių pavyzdžių, todėl duomenys yra saugomi sistemos duomenų rinkinyje. Po duomenų įkėlimo galima peržiūrėti sistemoje esančių įmonių duomenis.



12 pav. Duomenų apie įmonę pasirinkimas

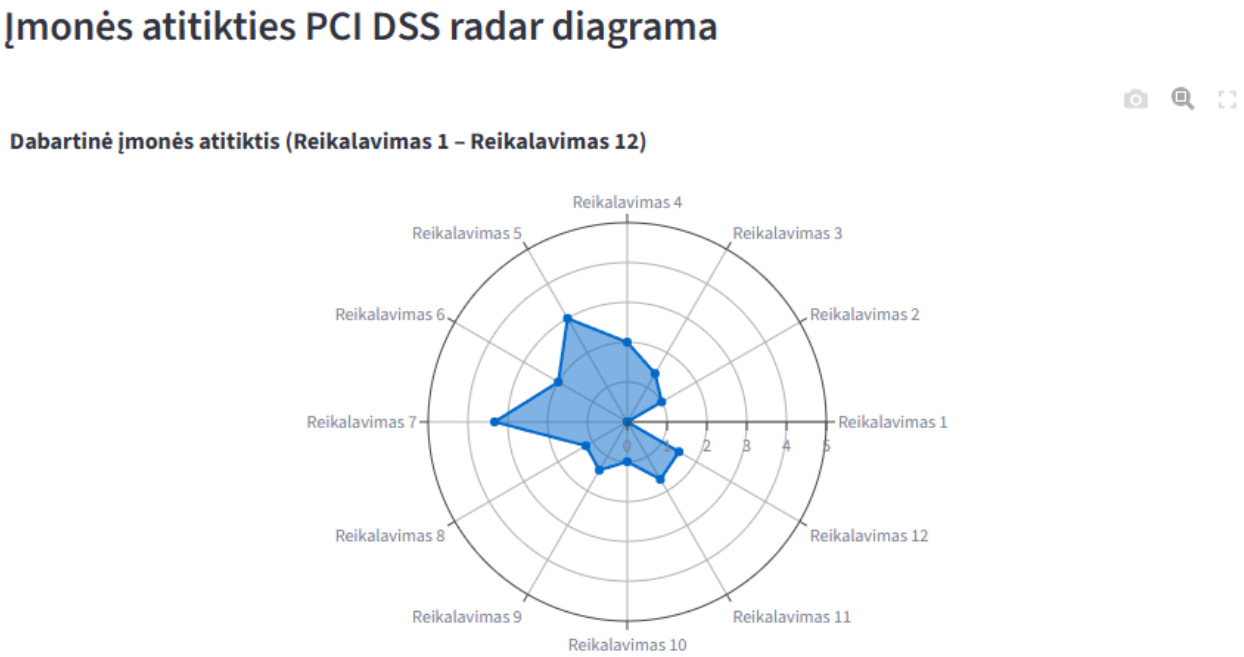
Pasirinkus atitinkamą įmonę, sistema apskaičiuoja ir pateikia jos atitiktį kiekvienam PCI DSS reikalavimui, agreguojant klausimyno atsakymus į reikalavimų grupes. Pateikiamas preliminarus visų PCI DSS reikalavimų atitikties rezultatas.

Reikalavimas	Vidurkis (0–5)
Reikalavimas 1	0.000
Reikalavimas 2	1.000
Reikalavimas 3	1.400
Reikalavimas 4	2.000
Reikalavimas 5	3.000
Reikalavimas 6	2.000
Reikalavimas 7	3.333
Reikalavimas 8	1.200
Reikalavimas 9	1.400
Reikalavimas 10	1.000

13 pav. Pasirinktos įmonės duomenų santrauka

Apskaičiuoti reikalavimų rezultatai pateikiami *Radar* diagramos pavidalu. *Radar* tipo diagrama iliustruoja, kiek įmonei trūksta balų iki idealios atitikties (šiuo atveju 100 proc. PCI DSS atitikties

kiekvienam reikalavimui). Žvelgiant į *Radar* tipo diagramą galima lyginti atitiktį skirtingiems PCI DSS reikalavimams. Ilgesnės diagramos ašys nurodo didesnę atitiktį konkrečiam PCI DSS reikalavimui, trumpesnės ašys iliustruoja silpnąsias saugumo sritis. Pavyzdinėje diagramoje įmonės stipriausia sritis yra Reikalavimas 7 – 3.333, silpniausia Reikalavimas 1 – 0.



14 pav. Įmonės stipriausių ir silpniausių sričių *Radar* diagrama

4.6. Įmonės atitikties rizikos vertinimas

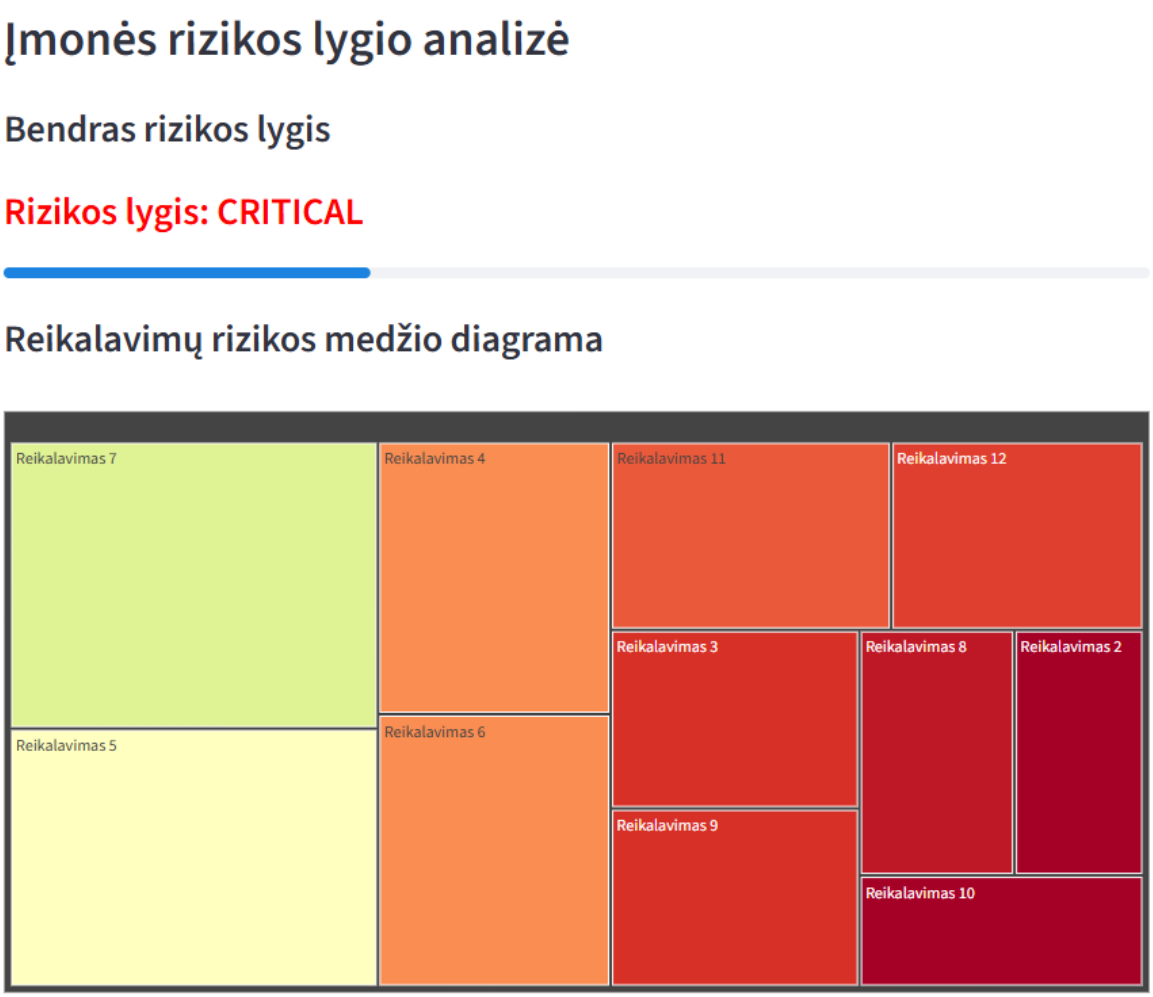
Kiekviena įmonė įvertina savo atitiktį pagal 59 kriterijus, kur kiekvienas kriterijus vertinamas 0-5 skalėje. PCI DSS reikalavimų neatitikimas sukelia tam tikrą riziką įmonei. Įmonės rizika (R_i, kai $i = 1,2,\ldots 12$) yra interpretuojama kaip nepakankamas saugumo kontrolės įgyvendinimo lygis. Rizikos vertinimas vyksta pagal atitikimą kiekvienam reikalavimui, priskiriant organizaciją vienam iš keturių rizikos lygių: žemam (*LOW*), vidutiniam (*MEDIUM*), aukštam (*HIGH*) ar kritiniam (*CRITICAL*).

Lentelė 20

Rizikos lygiai

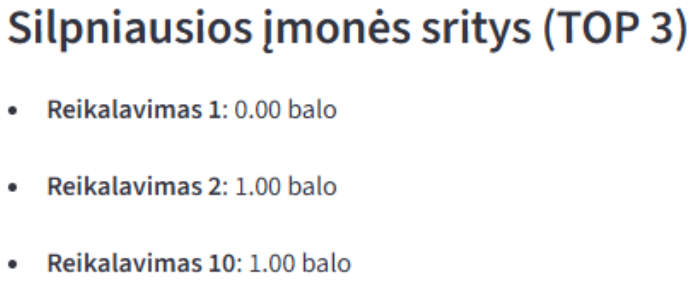
Atitikties balas	Rizikos lygis
$R_i \geq 4$	Žemas
$3 \leq R_i < 4$	Vidutinis
$2 \leq R_i < 3$	Aukštas
$R_i < 2$	Kritinis

Šaltinis: sudaryta autoriaus.



15 pav. Bendras įmonės rizikos lygis

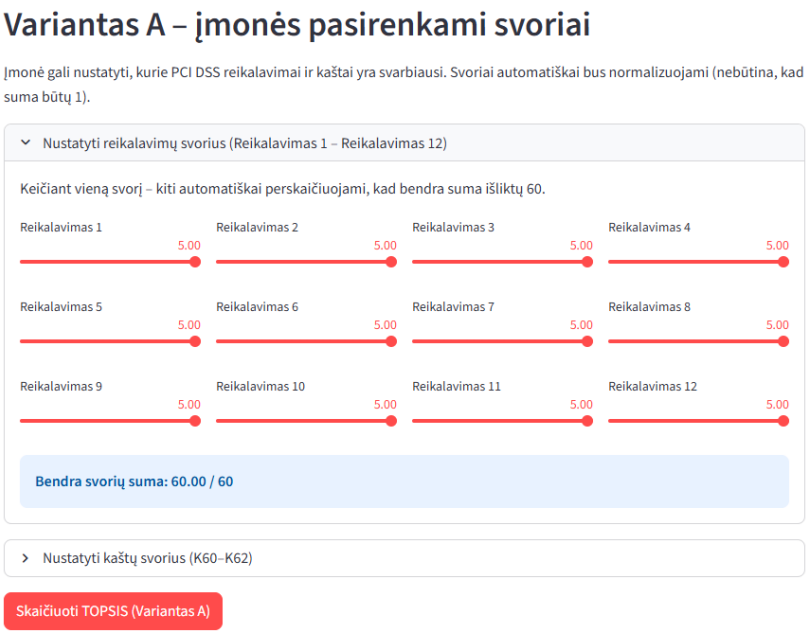
Šiuo atveju įmonės rizika vertinama kritiniu lygiu, kadangi daugelis reikalavimų yra žemiau 2 balų ribos. Tad atsižvelgus į tai kiekvienai įmonei yra išskiriamos trys silpniausios sritys lyginant visus įmonės atitikties balus - tai įmonės prioritetinės sritys (reikalingos tobulinimui). Jas svarbu išskirti, norint sumažinti riziką ir padidinti įmonės atitikties balą PCI DSS reikalavimams.



16 pav. Išskirtos silpniausios įmonės sritys

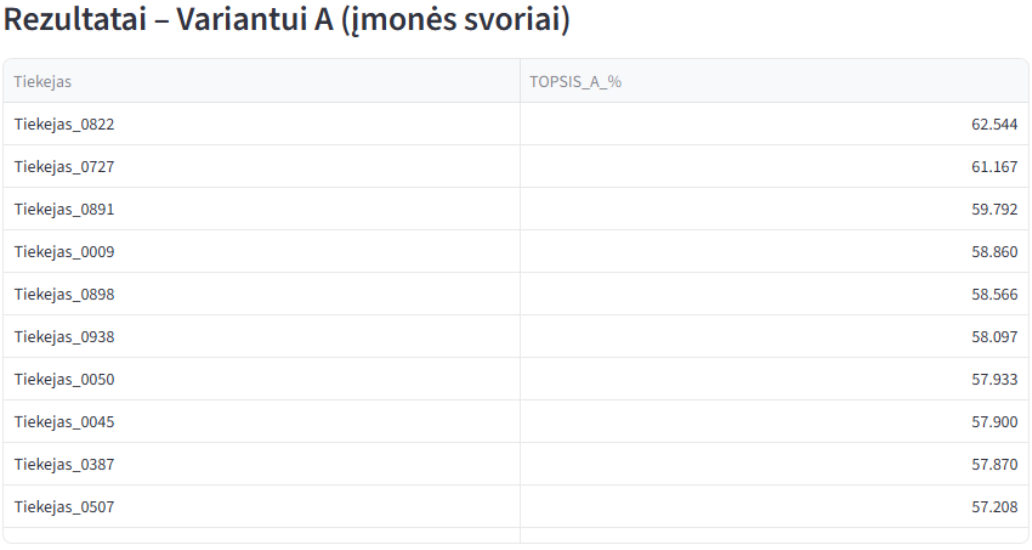
4.7. Skirtingi įmonės svorių skaičiavimai

Variantas A – įmonė pati nusprendžia, kurias sritis ji norėtų tobulinti. Didinant ar mažinant vieno reikalavimo svarbą, kiti atitinkamai dinamiškai keičiasi. Šis svorių nustatymo būdas atspindi subjektyvų sprendimo priėmimo scenarijų. Variantas A leidžia įvertinti skirtingas prioritetines sritis, modeliuoti skirtingas realias situacijas. Reikalavimo svoriai tolygiai yra paskirstomi visiems kriterijams:



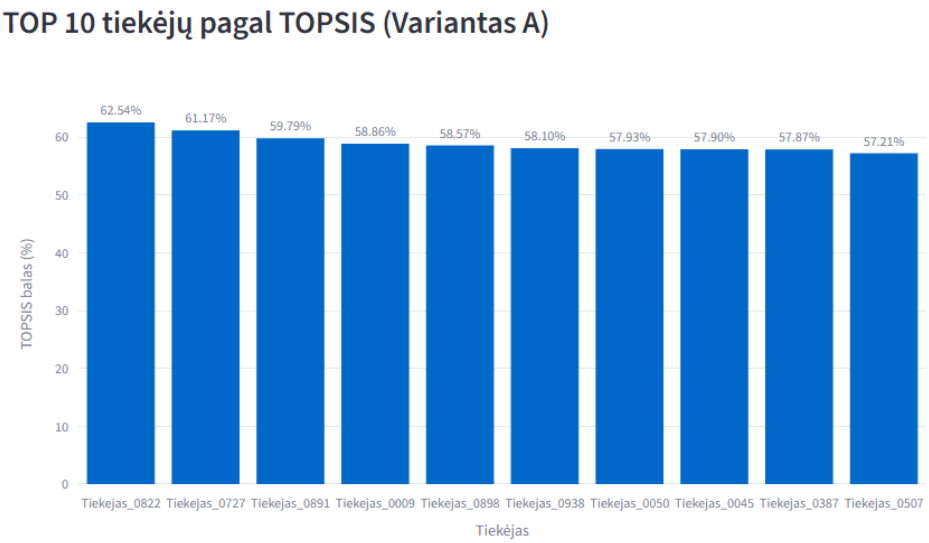
17 pav. Įmonės pasirinkti svoriai

Atsižvelgiant į tai, kad visas sritis ši įmonė norėtų vienodai gerinti, geriausiu tiekėju, atlikus TOPSIS analizę, išrenkamas Tiekejas_0822 – atitiktis 62.544%.



18 pav. Atlikta TOPSIS analizė ir gauti rezultatai pagal įmonės pasirinktus svorius

Grafike pavaizduoti 10 įmonei labiausiai tinkamų tiekėjų pagal jos pasirinktus svorius. Šiuo atveju dešimties tiekėjų balai svyruoja minimaliai, kadangi nėra tikslingai atsižvelgiama į silpnąsias įmonės sritis. Taigi, sprendimas yra gana jautrus svorių pasiskirstymui, net ir nedideli svorių pakeitimai gali lemti kitokius rezultatus.

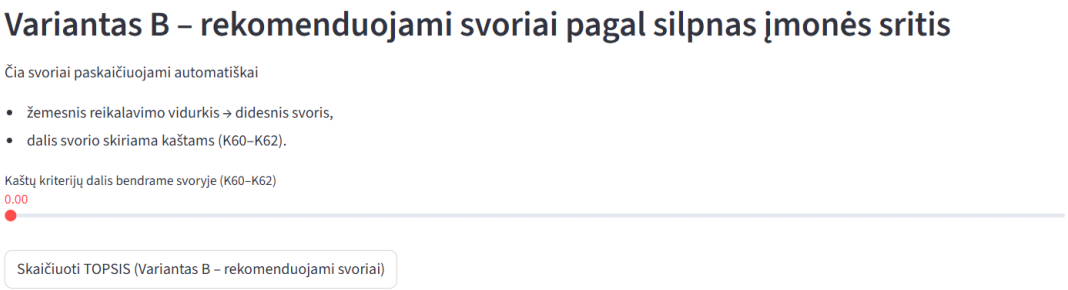


19 pav. Sureitinguoti tiekėjai pagal varianto A pasirinkimus

20 pav. Sėkmingo apskaičiavimo pranešimas

Išskirti pagrindiniai 10 tiekėjų buvo nustatyti pagal pasirinktus įmonės prioritetus (subjektyvus variantas), kadangi tiekėjai užtikrino aukščiausius balus tam tikruose reikalavimuose.

Variantas B – svoriai paskirstyti pagal silpniausias įmonės sritis. Šuo atveju kriterijų svoriai nėra nustatomi subjektyviai, jie apskaičiuojami remiantis faktiniu įmonės atitikties įverčiu. Įmonė gali nustatyti tik dalį bendro svorio: sprendimo įgyvendinimo trukmės, vienkartinių ir mėnesinių išlaidų svarbą. Skirtumas nuo Varianto A toks, kad tai sumažina sprendimų subjektyvumą, labiau orientuojasi į saugumo spragų tobulinimą ir tiekėjai reitinguojami taikant duomenimis grįstą svorių pasiskirstymą.



21 pav. Rekomenduojami svoriai pagal įmonės silpniausias sritis

Atsižvelgiant į tai, kad silpniausios įmonės sritys yra Reikalavimai 1, 2, 10, geriausiu tiekėju, atlikus TOPSIS analizę, išrenkamas Tiekejas_0993.

Rezultatai – Variantui B (rekomenduojami svoriai)

Tiekejas	TOPSIS_B_%
Tiekejas_0993	83.821
Tiekejas_0045	80.690
Tiekejas_0711	79.357
Tiekejas_0370	79.207
Tiekejas_0143	76.957
Tiekejas_0868	76.700
Tiekejas_0354	75.408
Tiekejas_0949	74.206
Tiekejas_0313	74.147
Tiekejas_0803	74.000

22 pav. Geriausio tiekėjo paaiškinimas pagal variantą B

23 pav. Sėkmingo apskaičiavimo pranešimas

Šis tiekėjas Tiekejas_0993 buvo parinktas pagal TOPSIS metodą, atsižvelgiant į silpniausias įmonės sritis. Jis turi aukščiausius balus pagrindinėse vertinimo srityse – 83.821%. Daugumoje kriterijų šis tiekėjas pasiekė idealią atitiktį, tai rodo aukštą teikiamo produkto vertę bei tinkamus strateginius tikslus tolimesniam įmonės PCI DSS atitikties gerinimui.

Šis tiekėjas reikšmingai prisideda prie silpnesnių įmonės sričių stiprinimo. Įmonė mažiausią atitiktį turi pirmame, antrame ir dešimtame reikalavimuose, tad tiekėjas šių reikalavimų gerinimui gali suteikti savo siūlomus produktus. Tiekėjo balas reikalavime vienas yra 4.6, antrame – 2.2, dešimtame 3.2. Apibendrinant, šis tiekėjas galėtų prisidėti prie silpniausių įmonės reikalavimų gerinimo.

Kodėl šis tiekėjas rekomenduojamas?

Tiekėjo stipriausios sritys (TOP 3):

- Reikalavimas 2: vidutinis balas **5.00**
- Reikalavimas 1: vidutinis balas **4.60**
- Reikalavimas 3: vidutinis balas **4.60**

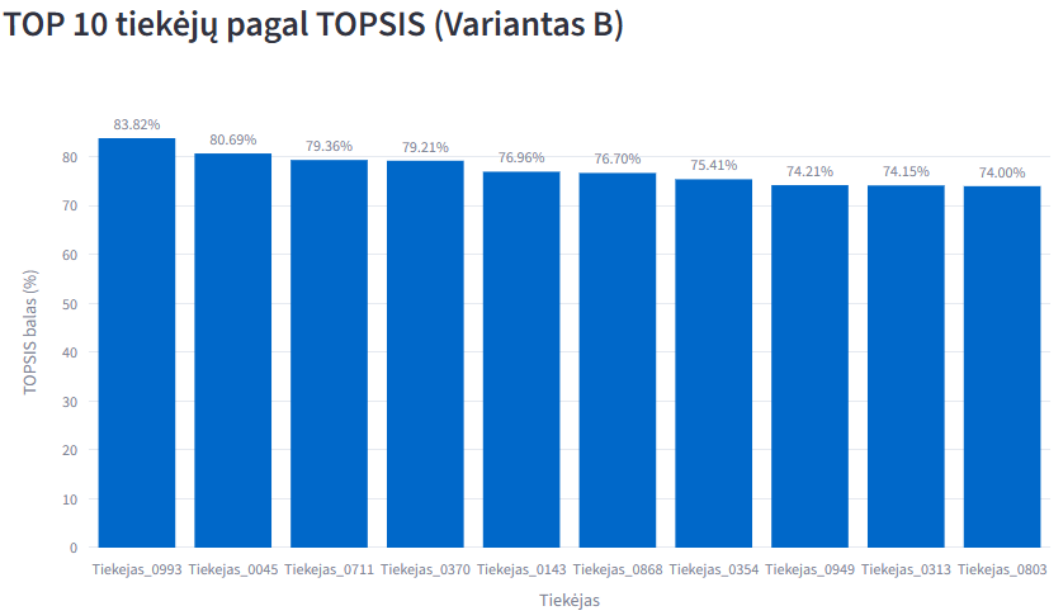
Įmonės silpniausios sritys:

- Reikalavimas 1: dabartinis įmonės vidurkis **0.00**
- Reikalavimas 2: dabartinis įmonės vidurkis **1.00**
- Reikalavimas 10: dabartinis įmonės vidurkis **1.00**

Įvertinimas: Tiekėjo stipriausios sritys sutampa su įmonės silpniausiomis vietomis (Reikalavimas 2, Reikalavimas 1), todėl jo sprendimai yra ypač tinkami greitam PCI DSS atitikties pagerinimui.

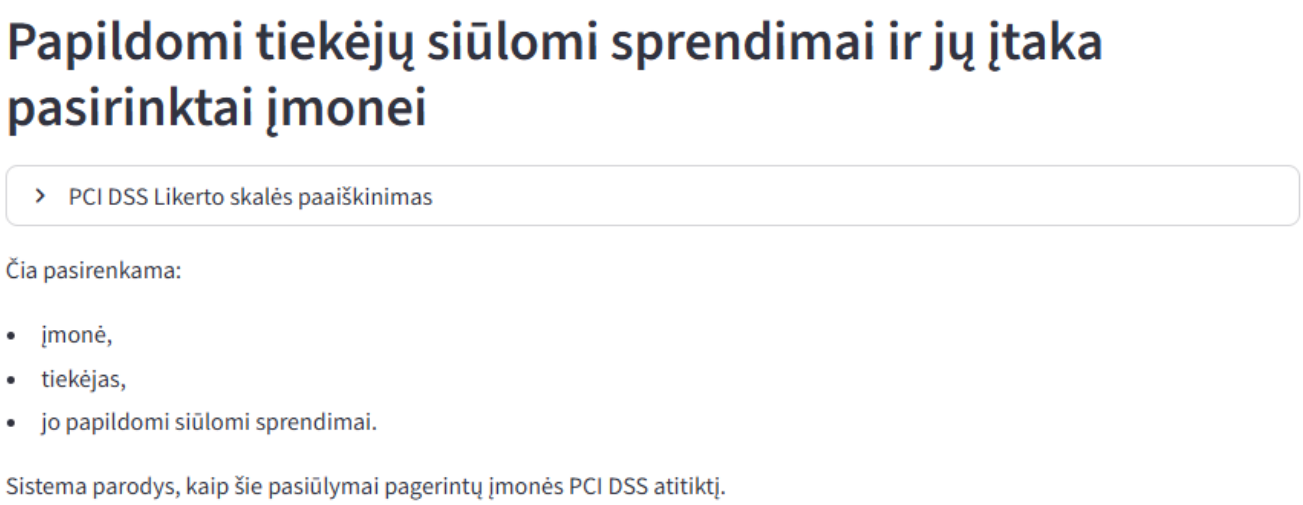
24 pav. Geriausio tiekėjo paaiškinimas pagal variantą B

Grafike atsispindi dešimties geriausių tiekėjų reitingas pagal TOPSIS variantą, atsižvelgiant į jos silpniausias sritis. Didžiausią balą pasiekė Tiekejas_0993, kuris remiantis daugiakriterinio vertinimo rezultatais yra labiausiai tinkantis pagal silpnąsias įmonės sritis. Antrasis ir trečiasis tiekėjai taip pat užtikrina gana aukštą atitikties balą. Šiuo atveju svoriai ir atitikties lygiai pasižymi didesne variacija, todėl nagrinėjamų tiekėjų siūlomi sprendimai optimaliai atitinka tiek techninius kriterijus, tiek taikomus kaštų ribojimus.



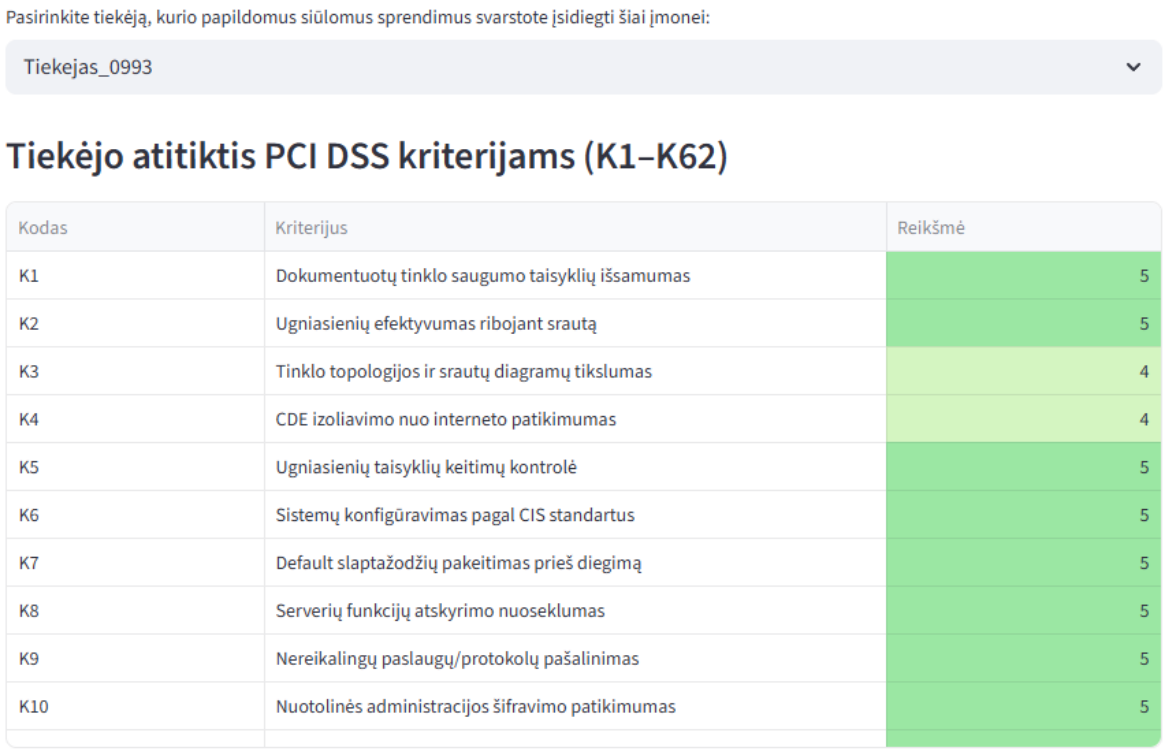
25 pav. Sureitinguoti tiekėjai pagal varianto B pasirinkimus

Atsižvelgiant į turimus tiekėjų balus galima peržiūrėti tiekėjų siūlomus programinius ir techninius sprendimus.



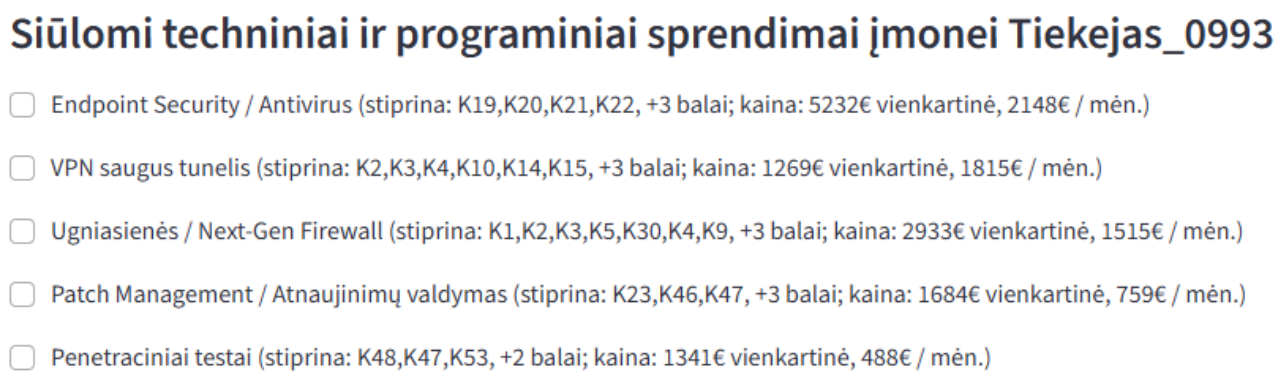
26 pav. Papildomų paslaugų pasirinkimas

Pasirinkus atitinkamą tiekėją galima peržiūrėti jo siūlomo sprendimo atitiktį skirtingiems kriterijams.



27 pav. Tiekėjo siūlomų paslaugų reikšmė

Kiekvienas tiekėjas siūlo programinius ar techninius sprendimus, kurie pagerintų įmonės atitiktį, pateikiant jų įgyvendinimo laikotarpį, vienkartinę ir mėnesinę kainą.



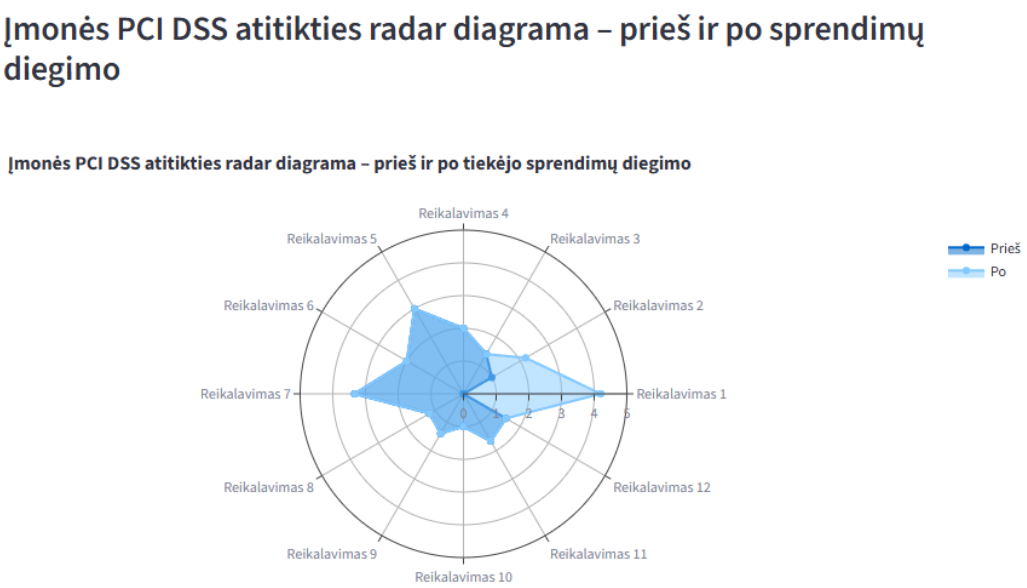
28 pav. Tiekėjo apžvalga

Atsižvelgiant į tai, kad kiekviena įmonė siekia kuo aukštesnės atitikties reikalavimams, galima peržiūrėti, kurios įmonės sritys labiausiai pagerėtų po tiekėjo siūlomo sprendimo įgyvendinimo.

	Būsena	Imone	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10	K11	K12	K13
0	Prieš	Imone_0001	0	0	0	0	0	1	1	1	1	1	1	1	1
1	Po	Imone_0001	3	5	5	5	3	1	1	1	4	4	1	1	1

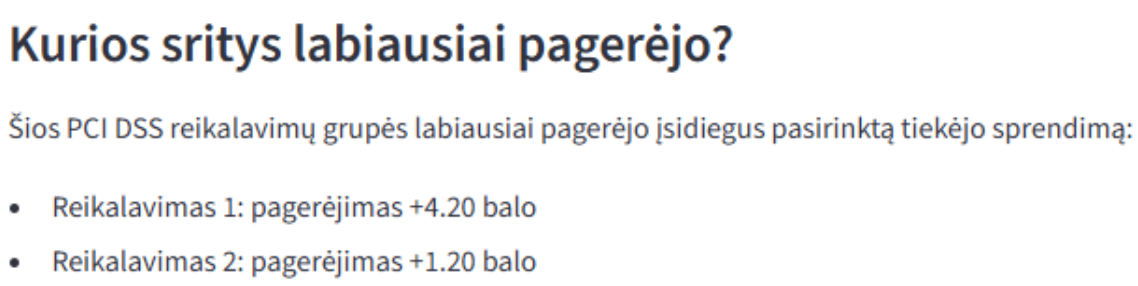
29 pav. Įmonės atitikties pagerėjimas po tiekėjo paslaugų integravimo

Radar diagrama iliustruoja pradinę įmonės atitiktį PCI DSS reikalavimams ir pateikia galimą po tiekėjo siūlomo sprendimo įgyvendinimo.



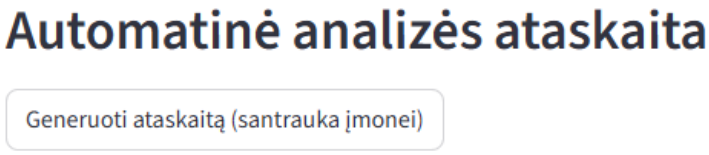
30 pav. Įmonės atitiktis po papildomų spendimų diegimo diagramos pavidalu

Trumpai apibūdinamos labiausiai pagerintos sritys, kurias patobulintų tiekėjo siūlomas sprendimas, pateikiamas preliminarus balas, kiek balų tam tikro reikalavimo atitiktis padidėtų.

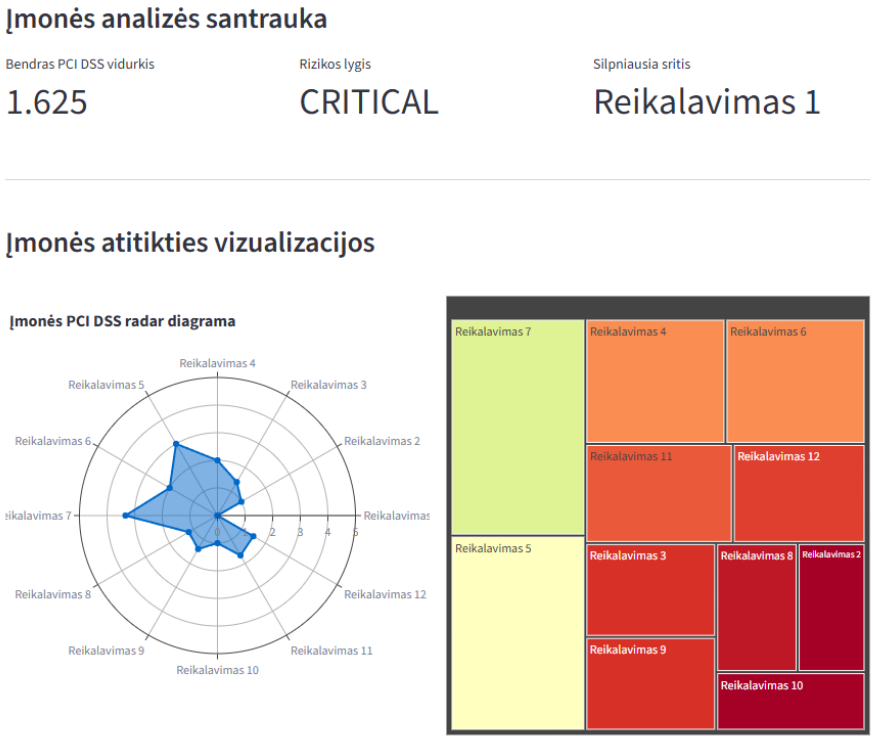


31 pav. Galutinė išvada, kurios sritys pagerėtų įsidiegus tiekėjo siūlomus produktus

Sugeneravus išvadas kiekviena įmonė turi galimybę susikurti trumpą analizės atskaitą su pagrindiniais duomenimis PDF formatu apie savo PCI DSS atitiktį ir silpniausias sritis.

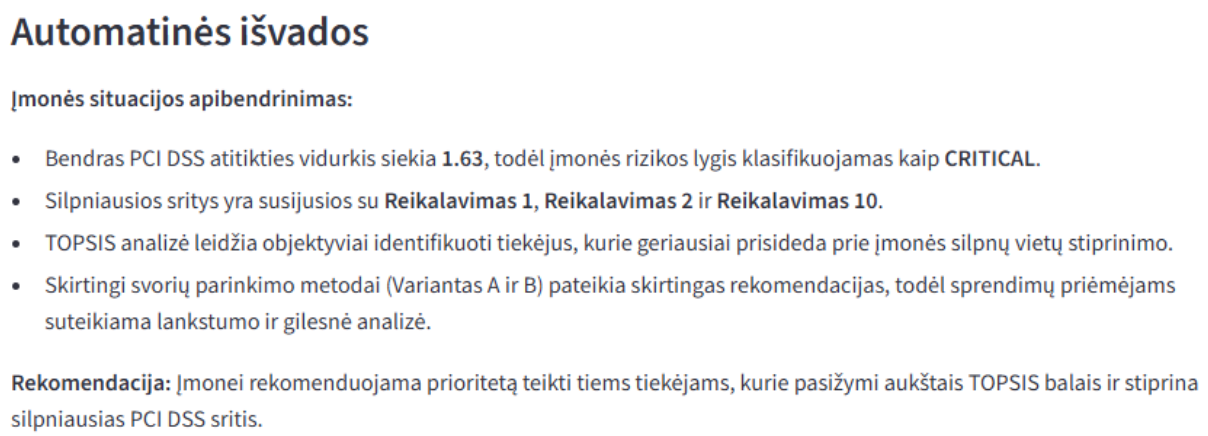


32 pav. Galima analizės ataskaita



33 pav. Trumpa įmonės analizės santrauka

Įmonės analizės santrauka pateikia pagrindinius reikalavimus, apibūdinančius esamą PCI DSS atitiktį. Nurodomas bendras PCI DSS vidurkis ir kiti įmonei reikšmingi rodikliai.



34 pav. Pateikiamos trumpos išvados

Pagal gautą įmonės ataskaitą yra pateikiamos trumpos išvados.

35 pav. Mygtukas analizės PDF atsisiuntimui.

Paspaudus mygtuką yra galimybė gauti trumpą įmonės analizę PDF formatu, žiūrint 1 Priedas.

Taigi, buvo išanalizuotas sprendimų-palaikymo sistemos prototipas, kuris leidžia nustatyti įmonės PCI DSS atitikties įvertį ir pasirinkti optimaliausią tiekėjo siūlomą sprendimą. Sistemoje naudojamas struktūruotas reikalavimų metodas, įmonių įsivertinimo klausimynas ir daugiakriterinis sprendimų priėmimo metodas. Vertinimo klausimynas leido apjungti skirtingus kriterijus į pagrindinius PCI DSS reikalavimus. Atsižvelgiant į gautus rezultatus, yra identifikuojamos silpniausios organizacijos sritys bei skirtingi svorių pasiskirstymo scenarijai. Variantas A įmonei leidžia pačiai nusistatyti svorius, kai Variantas B atsižvelgia į silpniausias sritis ir pateikia rizika grįstą svorių pasiskirstymo rezultatą.

IŠVADOS

1. Išanalizavus PCI DSS standarto struktūrą, nustatyta, kad standartas yra struktūruotas, turi 6 pagrindinius kontrolės tikslus, kurie apima 12 reikalavimų. Atlikta teminė analizė, nuspręsta sugrupuoti klausimus į mažesnes dalis tam, kad būtų galima naudoti TOPSIS metodą tolimesnei analizei.
2. Pagrindiniai iššūkiai, kylantys vertinant PCI DSS atitiktį, yra šie: kompleksiška IT infrastruktūra, dokumentacijos trūkumas, riboti finansiniai ir žmogiškieji ištekliai bei kiti organizacijos resursai. Atitiktis vertinama fragmentiškai, neįtraukiant organizacinių ir valdymo elementų, todėl įvertinimo rezultatai gali būti subjektyvūs ir sunkiau palyginami.
3. Identifikuoti pagrindiniai kriterijai ir rodikliai, leidžiantys sistemingai įvertinti įmonės atitiktį PCI DSS standartui. Pagrindiniai kriterijai išskirti pagal savęs įvertinimo klausimyną (59 klausimai) bei papildomus kainos ir įgyvendinimo trukmės rodiklius (3 klausimai). Kriterijai parinkti, atsižvelgiant į pagrindinius 12 PCI DSS reikalavimų. Įvertinimui pasirinkta Likerto tipo skalė nuo 0 iki 5, atsižvelgiant į tai, kad ši skalė ne tik nurodo balą, bet ir turi atitinkamą paaiškinimą.
4. Sukurtas įmonės atitikties PCI DSS įvertinimo metodas, grįstas TOPSIS daugiakriteriniu sprendimų priėmimo metodu. TOPSIS metodas leidžia apjungti tiek kiekybinius, tiek kokybinius kriterijus į bendrą indeksą. Atsižvelgiant į nustatytus kriterijų svorius, galima nustatyti, kuri alternatyva yra arčiausiai „idealaus“ atitikties sprendimo (atitikties 100 proc.).
5. Patikrinus sukurtą įvertinimo metodą su 1000 testinių duomenų įrašų, metodo rezultatai atspindi kriterijų įtaką galutiniam alternatyvų pasirinkimui (šiuo atvejų siūlomų tiekėjų), o keičiant kriterijų svorius ar rodiklių reikšmes rezultatas atitinkamai keičiasi ir prognozuoja alternatyvų pozicijų pasikeitimus.

LITERATŪRA

1. Ahmed, S. K., Mohammed, R. A., Nashwan, A. J., Ibrahim, R. H., Abdalla, A. Q., Ameen, B. M. M., & Khdhir, R. M. (2025). Using thematic analysis in qualitative research. *Journal of Medicine, Surgery, and Public Health*, *6*, 100198.
2. Alotaibi, M., Furnell, S., & Clarke, N. (2016, December). *Information security policies: A review of challenges and influencing factors*. In 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 352-358). IEEE.
3. Anderson, R., & Moore, T. (2006). The economics of information security. *science*, *314*(5799), 610-613
4. Antucheviciene, J., Zakarevicius, A., & Zavadskas, E. K. (2011). Measuring congruence of ranking results applying particular MCDM methods. *Informatica*, *22*(3), 319-338.
5. Boese, G. L. IV. (2020). *Cybersecurity Compliance Frameworks: A Comparative Study of Implementation Challenges.*
6. Chippagiri, S., & Ramesh, A. (2025). PCI DSS: A Critical Analysis of Implementation, Effectiveness, and Legislative Impact in Payment Card Security.
7. Clapper, D., & Richmond, W. (2016). SMALL BUSINESS COMPLIANCE WITH PCI DSS. *Journal of Management Information & Decision Sciences*, *19*(1).
8. du Preez, D. W., & Pieterse, V. (2006). Calculating Compliance Standards. In *ISSA* (pp. 1-11).
9. Ell, M., & Gallucci, R. (2022). *Cyber security breaches survey 2022*. Department for Digital, Culture, Media and Sport.
10. ES (2024). *Bendrasis duomenų apsaugos reglamentas (BDAR)*. Prieiga per internetą: https://eurlex.europa.eu/LT/legal-content/summary/general-data-protection-regulation-gdpr.html
11. Folorunso, A., Wada, I., Samuel, B., & Mohammed, V. (2024). *Security compliance and its implication for cybersecurity*. *World Journal of Advanced Research and Reviews, 24*(01), 2105-2121.

12. Gartner, W. B., & Carter, N. M. (2003). Entrepreneurial behavior and firm organizing processes. Acs, ZJ & Audretsch, DB (Eds.). Handbook of entrepreneurship research: An interdisciplinary survey and ıntroduction, science & business media içinde (pp. 195-221).

13. Ghosh, G. (2021). Adoption of digital payment system by consumer: a review of literature. *International Journal of Creative Research Thoughts*, *9*(2), 2320-2882.

14. Gold, S. (2014). *The evolution of payment card fraud*. *Computer Fraud & Security, 2014*(3), 12-17.

15. Ibrahimova, A. N. (2020). The defintions of information and security; history of information security development. *Vilnius University Open Series*, 48-57.

16. ISO/IEC (2016). *ISO/IEC Directives Part 2: Principles and rules for the structure and drafting of ISO and IEC documents*. Prieiga per internetą: https://www.iso.org/sites/directives/current/part2/index.xhtml

17. Jalayer, F. S., & Nabiollahi, A. (2016). Ranking criteria of enterprise information security architecture using fuzzy TOPSIS. *Int. J. Comput. Sci. Inf. Technol*, *8*, 45-59.

18. Joshi, A., Kale, S., Chandel, S., & Pal, D. K. (2015). Likert scale: Explored and explained. *British journal of applied science & technology*, *7*(4), 396.

19. Joshi, P. K. (2024). Achieving PCI-DSS Compliance in Payment Gateways: A Comprehensive Approach. *Journal of Technology and Systems*, *6*(7), 13-31.

20. Karayew, D. (2012). *The history of credit cards* (Doctoral dissertation, Видавництво СумДУ).

21. Koo, M., & Yang, S. W. (2025). Likert-type scale. *Encyclopedia*, *5*(1), 18.

22. Liu, J., Xiao, Y., Chen, H., Ozdemir, S., Dodle, S., & Singh, V. (2010). *A survey of payment card industry data security standard*. *IEEE Communications Surveys & Tutorials, 12*(3), 287-303.

23. Madanchian, M., & Taherdoost, H. (2023). A comprehensive guide to the TOPSIS method for multi-criteria decision making. *Madanchian M, Taherdoost H. A comprehensive guide to the TOPSIS method for multi-criteria decision making. Sustainable Social Development*, *1*(1), 2220.

24. María, Y. (2010). *PCI DSS case study: Impact in network design and security*. *Rochester Institute of Technology*.

25. McCallister, E., Grance, T., & Scarfone, K. (2014). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) Recommendations of the National Institute of Standards and Technology (2010)*.

26. Microsoft (2025). Informacijos saugos („InfoSec“) apibrėžimas. Prieiga per internetą: https://www.microsoft.com/lt-lt/security/business/security-101/what-is-information-security-infosec

27. Nanda, A., Popat, P., & Vimalkumar, D. (2018). Navigating Through Choppy Waters of PCI DSS Compliance. Advances in Information Security, Privacy, and Ethics, 99– 140.

28. Nemoto, T., & Beglar, D. (2014, November). Likert-scale questionnaires. In *JALT 2013 conference proceedings* (Vol. 108, No. 1, pp. 1-6).

29. Pavić, Z., & Novoselac, V. (2013). Notes on TOPSIS method. *International Journal of Research in Engineering and Science*, *1*(2), 5-12.

30. PCI Security Standards Council (2025). *PCI Security Standards*. https://www.pcisecuritystandards.org/standards/

31. PCI Security Standards Council (2021). Payment Card Industry Qualified Data Security Company Requirements. Prieiga per internetą: https://listings.pcisecuritystandards.org/documents/QSA_Qualification_Requirements_v4.0.pdf.

32. PCI Security Standards Council (2022). *Document Library: PCI DSS and Related Standards*. https://www.pcisecuritystandards.org/document_library

33. PCI Security Standards Council (2024). *Payment Card Industry Data Security Standard. Requirements and Testing Procedures. Version 4.0.1*

34. Rees, J. (2010). *The challenges of PCI DSS compliance*. *Computer Fraud & Security, 2010*(12), 14–16. https://doi.org/10.1016/s1361-3723(10)70156-1

35. Rees, J. (2012). *Tackling the PCI DSS challenges*. *Computer Fraud & Security, 2012*(1), 15-17. https://doi.org/10.1016/S1361-3723(12)70009-X

36. Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121-135.

37. Sakharova, I. (2012, June). *Payment card fraud: Challenges and solutions*. In *2012 IEEE international conference on intelligence and security informatics* (pp. 227-234). IEEE.

38. Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3).

39. Taherdoost, H. (2019). What is the best response scale for survey and questionnaire design; review of different lengths of rating scale/attitude scale/Likert scale. *International Journal of Academic Research in Management (IJARM)*, *8*.

40. Verizon (2019). *2019 Data Breach Investigations Report*. https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executivebrief.pdf

41. Verizon (2019). *2019 Payment Security Report*. https://enterprise.verizon.com/resources/reports/2019-payment-securityfullreport-bl.pdf

42. Visuotinė Lietuvių Enciklopedija (2025). Mokamoji kortelė. Prieiga per internetą: https://www.vle.lt/straipsnis/mokamoji-kortele/

43. Wang, W., Sadjadi, S. M., & Rishe, N. (2024, May). A Survey of Major Cybersecurity Compliance Frameworks. In *2024 IEEE 10th Conference on Big Data Security on Cloud (BigDataSecurity)* (pp. 23-34). IEEE.

44. Zavadskas, E. K., & Turskis, Z. (2011). Multiple criteria decision making (MCDM) methods in economics: an overview. *Technological and economic development of economy*, *17*(2), 397-427.

PRIEDAI

1 PRIEDAS

PCI DSS atitikties analizės ataskaita PDF formatu

PCI DSS atitikties analizės ataskaita

Įmonė: Imone_0001
Bendras atitikties vidurkis: 1.625
Rizikos lygis: CRITICAL

Silpniausios sritys:

- Reikalavimas 1: 0.000
- Reikalavimas 2: 1.000
- Reikalavimas 10: 1.000

TOPSIS – Variantas A (TOP 5)

Tiekejas	TOPSIS (%)
Tiekejas_0822	62.796
Tiekejas_0009	59.325
Tiekejas_0507	57.869
Tiekejas_0046	56.599
Tiekejas_0960	56.405

TOPSIS – Variantas B (TOP 5)

Tiekejas	TOPSIS (%)
Tiekejas_0993	83.821
Tiekejas_0045	80.690
Tiekejas_0711	79.357
Tiekejas_0370	79.207
Tiekejas_0143	76.957