LATVIJAS UNIVERSITĀTE
BIZNESA, VADĪBAS UN EKONOMIKAS FAKULTĀTE
EKONOMIKAS NODAĻA

Informāciju tehnoloģiju drošības pārvaldības uzlabošana uzņēmumā

Information technology security management improvement in the company

DIPLOMDARBS

Autors: Profesionālās bakalaura studiju programmas
E-biznesa un loģistikas vadības sistēmas
4. kursa students
Ernests Pikše
Studenta apl.: ep13057
Darba vadītājs: m.b.a., lektors p.i. Kārlis Praudiņš

Rīga 2017

Anotācija

Mūsdienās informācijas tehnoloģiju drošībai tiek pievērsta arvien lielāka uzmanība uzņēmējdarbības vidē, saistībā ar pieaugošo incidentu skaitu. Drošības pārvaldībai ir ļoti svarīga loma, lai uzņēmumi varētu nodrošināt biznesa nepārtrauktību, informācijas neizpaušanu, kā rezultātā nestu papildus pievienoto vērtību klientiem un veicinātu uzticamību investoru vidū. Bieži vien uzņēmumi uzbrukumu rezultātā cieš zaudējumus, taču neizpauž šo informāciju publiski, tādējādi pakļaujot riskam ne tikai uzņēmumu, bet arī tā klientus.

Diplomdarba mērķis ir, pamatojoties uz informācijas tehnoloģiju pārvaldības drošības standartiem, veikt uzņēmuma drošības novērtēšanu un izstrādāt priekšlikumus informācijas tehnoloģiju pārvaldības drošības uzlabošanai.

Darba uzdevumi:

1. Izanalizēt esošās uzņēmumu IT drošības tendences;
2. Izpētīt IT drošības pārvaldības standartus un vadlīnijas;
3. Novērtēt uzņēmuma informācijas tehnoloģiju drošību pamatojoties uz ISO/IEC 27001:2013 un ITIL standartu;
4. Veikt risku analīzi un dot priekšlikumus IT drošības pārvaldības uzlabošanai;
5. Izdarīt secinājumus par IT drošības pārvaldību uzņēmumā.

Veicot uzņēmuma IT drošības pārvaldības izvērtēšanu, darba autors secināja, ka uzņēmumā esošā IT drošības pārvaldība neatbilst pēc ISO/IEC 27001:2013 standarta un ITIL(v3) ietvara, tika konstatēts, ka uzņēmums ir pakļauts IT drošības riskam.

Atslēgas vārdi: IT drošības standarti, ISO 27001 standarts, IT pārvaldība, IT risks, IT dokumentācija.

Annotation

Nowadays, companies pay more attention to information technology security due to the security incidents. Security management has a significant role for businesses it ensures business continuity, information integrity, as result brings benefit to customers and promote credibility amongst potential investors. Often companies suffer losses, because of attacks, but do not disclose information publicly, so putting not only company under the risk, but its customers as well.

Diploma thesis purpose is to evaluate company's security assessment and give recommendations about security management based on IT standards and best practices. Tasks:

1. Analyze actual organization information technology security trends;
2. Research information technology security management standards and guidelines;
3. Evaluate the company's information technology security based on ISO/IEC 27001:2013 and ITIL standards;
4. Make risk assessment and give recommendations for IT security improvements;
5. Make conclusions about IT security management in company.

After evaluating company's compliances against IT security management standard author concluded that company IT security management does not comply with ISO / IEC 27001: 2013 standard and ITIL (v3) framework, it is under IT security risk.

Keywords: IT security standards, ISO 27001 standard, IT security management, IT risk, IT documentation.

Saturs

Apzīmējumu saraksts

IT- Informācijas tehnoloģijas

ITIL- Informāciju tehnoloģiju infrastruktūras ietvars

ISMS-Informācijas drošības pārvaldības sistēma

PDCA- Plāno, Dari, Pārbaudi, Rīkojies cikls

ISO- Internacionālā standartu organizācija

ISACA- Informācijas sistēmu audita un kontroles asociācija

IEC- Starptautiskā elektrotehniskā komisija

SLA- Pakalpojumu līmeņa vienošanās

VPN – Virtuālais privātais tīkls

SoGP- Labās prakses standarts

ISF- Starptautiskais drošības forums

OWASP- Ārējā tīkla aplikācijas drošības projekts

OSI- Atvērto sistēmu sadarbības bāzes etalona modelis

PPS- Projekta prasību specifikācija

PPA- Programmatūras projektēšanas apraksts

WAD- Windows aktīvā direktorija

Ievads

Informācijas drošības pārvaldība ir nepieciešama, jo pastāv neskaitāmi daudz informācijas drošības draudi, kas nodara zaudējumus finansēm un datiem, kā arī uzņēmuma tēlam, tādējādi pakļaujot riskam uzņēmuma reputāciju.

Organizācijas informācijas pieejamībai, integritātei un konfidencialitātei ir svarīga loma, lai uzņēmums varētu darboties nepakļaujot to riskiem. Jebkurai organizācijai ir informācija un dati, kas ir gana būtiski vai kritiski, lai uzņēmums veiksmīgi varētu veikt savu darbību.

Labā prakse ir ieviest un regulāri veikt pārbaudes, pamatojoties uz informācijas tehnoloģiju drošības standartiem un labās prakses vadlīnijām, taču tas prasa laiku un izpratni par procesiem, dokumentāciju un tehnoloģijām.

Joprojām pieaugošie draudi ir pamatojums, kāpēc ir nepieciešams ieviest dažāda veida drošības pasākumus, taču ne vienmēr uzņēmumi apzinās tā nepieciešamību. Organizācijās valda priekšstats, ka tā darbība netiek pakļauta informācijas tehnoloģiju drošības riskiem.

Diplomdarba mērķis ir, pamatojoties uz informācijas tehnoloģiju pārvaldības drošības standartiem, veikt uzņēmuma drošības novērtēšanu un izstrādāt priekšlikumus informācijas tehnoloģiju pārvaldības drošības uzlabošanai.

Darba uzdevumi:

1. Izanalizēt esošās uzņēmumu IT drošības tendences;
2. Izpētīt IT drošības pārvaldības standartus un vadlīnijas;
3. Novērtēt uzņēmuma informācijas tehnoloģiju drošību pamatojoties uz ISO/IEC 27001:2013 standartu un ITIL ietvaru;
4. Veidot priekšlikumus IT drošības pārvaldības uzlabošanai;
5. Izdarīt secinājumus par IT drošības pārvaldību uzņēmumā.

Pirmajā daļā darba autors apraksta informācijas tehnoloģiju drošības situāciju uzņēmumos un analizē informācijas tehnoloģiju drošības standartus, kā arī veic to salīdzinājumu. Otrajā daļa darba autors apraksta pētāmo uzņēmumu, kā arī novērtē uzņēmuma informācijas tehnoloģiju pārvaldību atbilstoši drošības standartiem. Trešajā daļā darba autors veic uzņēmuma risku analīzi, kā arī sniedz priekšlikumus uzņēmuma tālākas darbības uzlabošanai.

Diplomdarba izveides laikā tika izmantotas šādas metodes – teorētiskās daļas pētīšanas metode, datu salīdzināšana, sarunas, dokumentācijas izpētīšana un analīze.

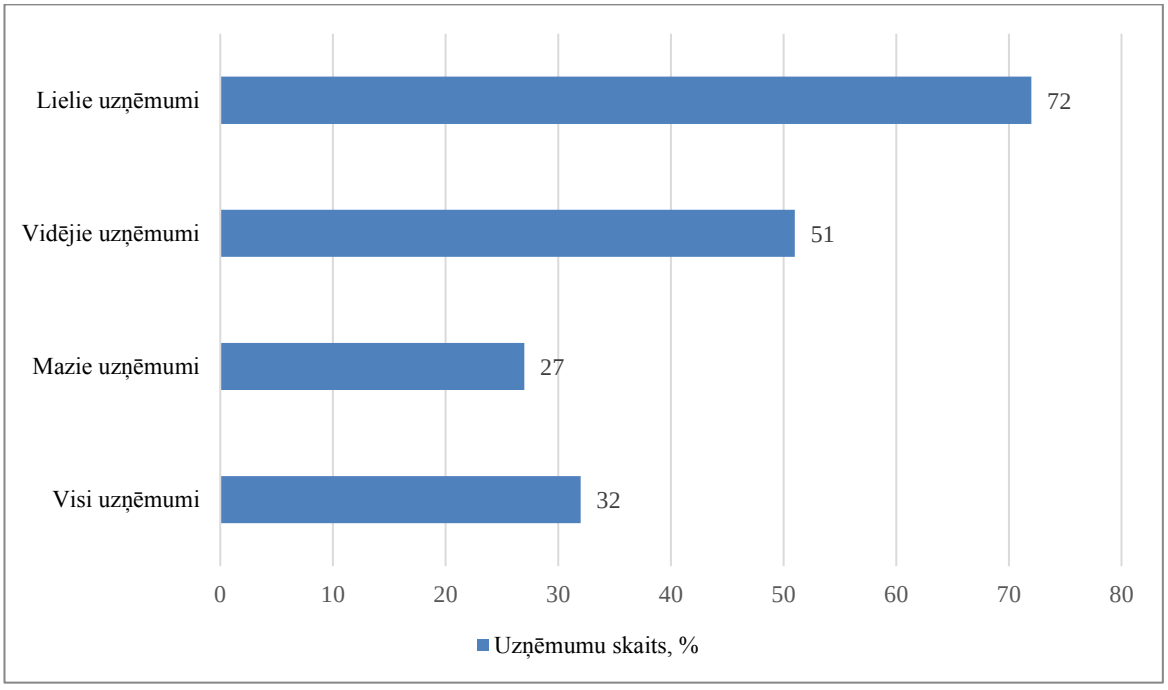
Pētījums tika veikts laika posmā no 2017. gada 20. marta 30. aprīlim, kura laikā tika intervēti uzņēmuma IT speciālisti.

1. IT DROŠĪBAS SITUĀCIJA UN TENDENCES

IT drošības politikas klātbūtne uzņēmumā nozīmē to, ka uzņēmums apzinās savu IT nozīmi un attiecīgi izrietošos potenciālos riskus. Turklāt, esoša IT drošības politika nozīmē stratēģiju, kā nosargāt datus un IT sistēmas, kā arī obligātās saistības visiem darbiniekiem. 2015.gada *Eurostat* pētījumā, kurā tika aptaujāti 148800 uzņēmumi kopumā no 1.5 miljoniem uzņēmumiem Eiropas Savienībā, kuros ir 10 vai vairāk darbinieki. [10]

No aptaujātajiem uzņēmumiem, 83% darbinieku skaits tajos ir 10-49, 14% uzņēmumu darbinieku skaits ir 50-249 un 3% uzņēmumu ir 250 vai vairāk darbinieku. No aptaujātajiem 32% uzņēmumi, kas atrodas Eiropas Savienībā formāli definējuši IT drošības politiku, augstākie rādītāji bija Zviedrijā - 51% un Portugālē - 49%, kur uzņēmumi bija ieviesuši IT drošības politiku. Formāli definētajai politikai vajadzētu atspoguļojas uz novērojumiem par saistītajiem IT drošības riskiem, kas palielina varbūtību drošības incidentu notikumiem, kā arī ietekmi uz uzņēmuma darbību. [10]

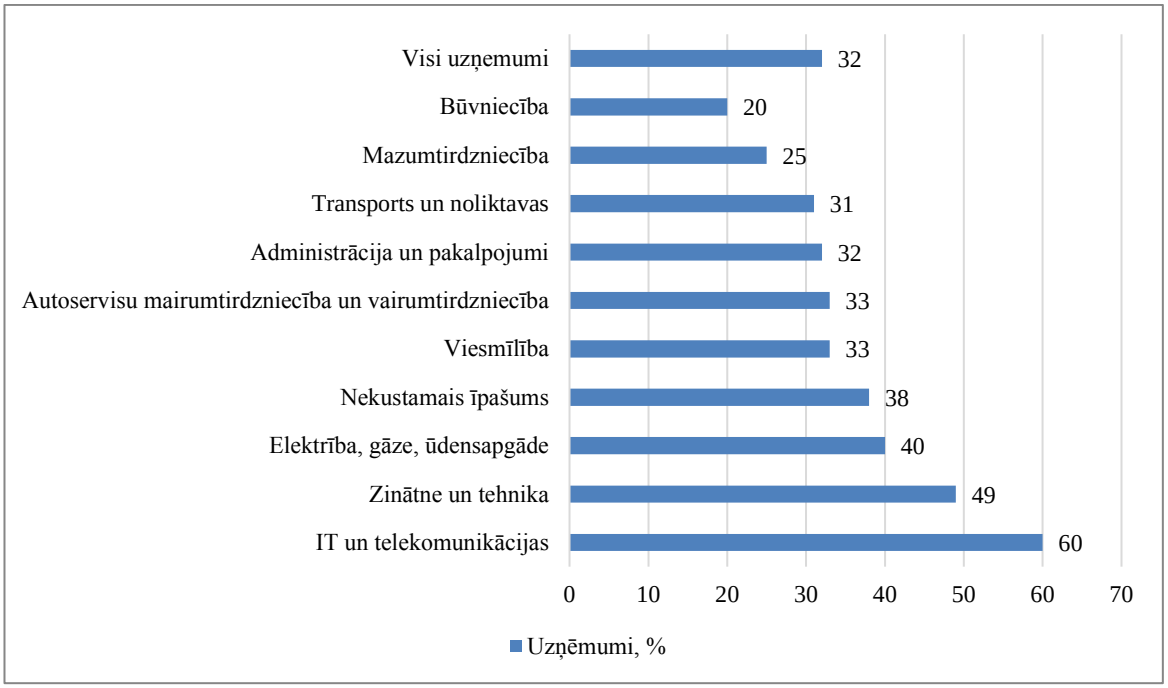
Attēlā 1.1 parādīts , ka lielie uzņēmumi, kam ir formāli noteikta IT drošības politika ir gandrīz trīs reizes vairāk, kā mazie uzņēmumi. [16]



1.1. attēls **Uzņēmumi ar formālu IT drošības politiku**

Aplūkojot IT drošības politikas esamību (skat. attēlu 1.2) uzņēmumos pēc nozarēm, lielākā daļa uzņēmumi, kuriem IT politika tika ieviesta ir saistīti ar IT un komunikāciju

aktivitātēm 49%. No uzskaitītajiem vismazāk uzņēmumu proporcionāli reģistrēti būvniecībā - 20%, mazumtirdzniecība -25%, transporta un noliktavu nozarē – 26%.[10]



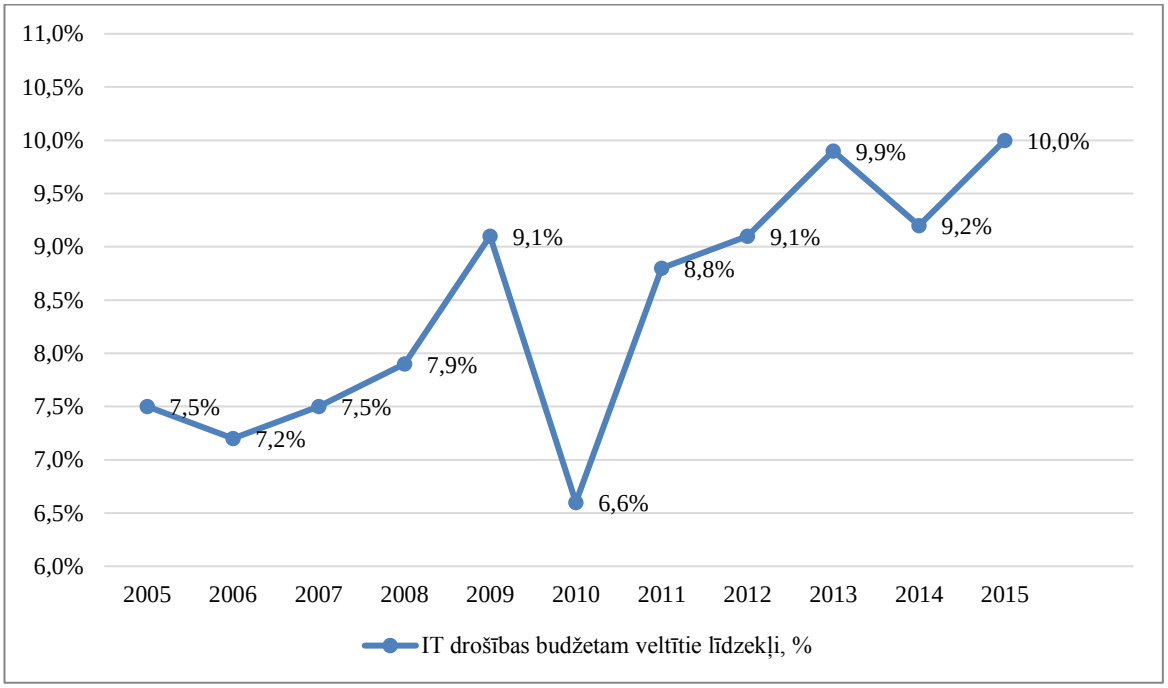
1.2. attēls **Uzņēmumi ar formālu IT drošības politiku pēc uzņēmuma nozares**

Riski, kas saistīti ar datu iznīcināšanu, iejaukšanos tajos, ļaunprātīga uzbrukuma vai cita neparedzēta incidenta rezultātā, tiek visvairāk uzsvērti uzņēmumu IT drošības politikās. [16]

Trīs risku tipi, kurus adresē uzņēmumi, kuriem ir formāli definēta IT drošības politika ir integritāte, konfidencialitāte un informācijas sistēmu pieejamība.[10] [4]

Lielākais procents uzņēmumu, kam ir formāli noteikta IT drošības politika, kas pievērš uzmanību ļaunprātīgu uzbrukumu vai neparedzētu incidentu riskam, kas rezultējās ar datu iznīcināšanu vai iejaukšanos ziņots Portugālē – 44% uzņēmumu. Līdzīgi uzņēmumi Portugālē ziņoja, ka otrs lielākais procents uzņēmumu, kam ir formāli noteikta IT drošības politika, kas pievēršas riskam ir nepieejami pakalpojumi, ko izraisījuši uzbrukumi no ārpuses (pakalpojumatteices uzbrukums) – 35%. [16]

Lielākais procents uzņēmumu ar noteiktu IT drošības politiku, kam ir noteikta IT drošības politika, kas pievērš uzmanību konfidenciālu datu izpaušanai, ko izraisījusi ielaušanās, pārveidošana vai pikšķerēšanas uzbrukumi, vai negadījumi ir ziņots Īrijā – 39%. Uzņēmumi Īrijā noteica IT drošības politikas visiem minētajiem riskiem – 35%.[10]

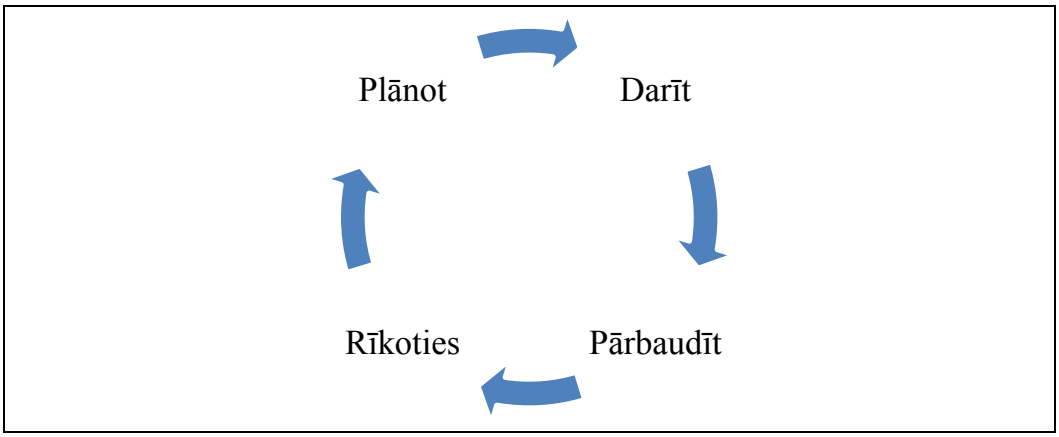


1.3. attēls **Uzņēmumu IT budžetam veltītie līdzekļi IT drošībai**

Nepieciešamība pēc informācijas drošības uzņēmumiem ir redzama no uzņēmumu pieaugošā IT drošības budžeta palielinājuma. Attēlā 1.3 parādīts procentuālais IT budžetam veltīto līdzekļu procentuālais apjoms laika posmā no 2005.-2015. gadam. Uzņēmumi paļaujas uz drošības tehnoloģijām ,piemēram, ugunsmūriem un ielaušanās noteikšanas sistēmām, lai pārvaldītu IT drošības riskus. Lai arī informācijas avoti par IT drošības tehniskajiem aspektiem pieaug, sabiedrībā joprojām tiek diskutēts par šo tehnoloģiju vērtību. [18]

1.1 ISO 27001:2013 standarts

Informācijas tehnoloģiju pārvaldības standarts precizē nosacījumus, lai nodrošinātu, ieviestu, lietotu, uzraudzītu, pārskatītu, saglabātu un uzlabotu labu informācijas drošības pārvaldības sistēmu. Šis standarts sevī iekļauj labāko informācijas drošības praksi ar četru posmu procesa pieeju – Plānot - Darīt - Pārbaudīt - Rīkoties jeb Deminga (*PDCA*) ciklu (skat. attēlu 1.4). Organizācijas var izvēlēties kontroles darīšanas fāzē, pamatojoties uz pirms tam iesniegto labās prakses sarakstu, taču organizācijas var arī izlaist kontroles, kas ir sarakstā, ja tiek pierādīts kā izņēmuma gadījums. ISO standarts uzņēmumus mudina ieviest papildus kontroles, kuras parāda, ka tiek pietiekoši pārvaldīti visi riski. [19] [9]



1.4. attēls **Deminga cikls**

• Plānošanas (*Plan*) posmā tiek novērtēti potenciālie riski, skaidri noteiktas juridiskās prasības un noteiktas atbildības, resursi, kontroles, riska pieņemšanas kritēriji un nepieciešamās procedūras, lai pasargātu uzņēmumu no drošības pārkāpumiem un gadījumos, kad tie iestājas pareizi spētu pārvaldītu tos. Pēc šī posma noslēgšanas, komandai vajadzētu augstākās vadības apstiprinājumu priekš atlikušo risku novēršanas un ieviešanas plāna pilnvarošanas, lai varētu virzīties uz nākamo posmu.

• Darīšanas (*Do*) posms ļauj drošības pārvaldības komandai ieviest plānu un pārvaldīt ikdienas drošības operācijas. [19]

• Pārbaudes (*Check*) posms ietver aktivitātes, kas atklāj mēģinājumus vai veiksmīgus pārkāpumus, nosakot, kā tas varēja notikt un kāda bija rīcība esošajā situācijā. Izskatot un izmērot ieviestās kontroles efektivitāti, ņemot vērā visas izmaiņas uzņēmuma struktūrā, darbiniekos, procesos, tehnoloģijās, kā rezultātā papildinot plānu ar nepieciešamajām izmaiņām.

• Rīcības (*Act*) posmā drošības pārvaldības komanda, izmantojot iegūtās zināšanas no iegūtās pieredzes, ievieš nepieciešamos uzlabojumus, kā arī paziņo par darbībām un uzlabojumiem ieinteresētajām personām, lai pārliecinātos, ka plāns apmierina to vajadzības. [19] [9] [11]

1.2 COBIT vadlīnijas

ISACA (Informācijas sistēmu audita un kontroles asociācija) tika dibināta ASV 1967. gadā, veicot revīzijas kontroli datoru sistēmām. 1969. gadā Stjuarts Tirnaeurs dibināja uzņēmumu ar nosaukumu EDP Auditoru Asociācija. 1976. gadā savu uzņēmumu attīstīja līdz

Izglītības fondam, pateicoties zināšanām un darbības stilam IT pārvaldības un kontroles jomā. [15]

Šobrīd ISACA pārstāv vairāk kā 75000 biedru no visas pasaules. Dalībnieki dzīvo un strādā vairāk nekā 160 valstīs un pārstāv visdažādākās jomas IT nozarē. COBIT pirmo reizi tika izdots 1996. gadā. COBIT ir IT pārvaldības sistēma, kas ļauj visiem vadītājiem 'aizpildīt plaisu' starp kontroles prasībām, tehniskajiem jautājumiem un uzņēmējdarbības riskiem.

COBIT uzlabojumi šobrīd organizācijām palīdz paaugstināt vērtību IT jomā, kā arī izceļ biznesa un IT mērķu ciešās saites, un vienkāršos COBIT regulējumus. Balstoties uz jau paveikto darbu, uzlabotu vecākās COBIT versijas. [20]

COBIT ietver 34 augstākā līmeņa procesus, kuri ietver 210 kontroles mērķus, kas ir kategorizēti 4 jomās: plānošana un organizēšana, iegāde un ieviešana, piegāde un atbalsts, uzraudzība un attīstība.

1. Plānošana un Organizēšana. Šis domēns izskaidro, kā IT ir jāizmanto, lai palīdzētu sasniegt uzņēmuma mērķus un izvirzītos uzdevumus.

2. Iegāde un Ieviešana. Šis domēns aptver darbības, kā, piemēram, iegādāties jaunas tehnoloģijas un izmantot tās uzņēmumā, kā arī palīdz nodrošināt darba īstenošanu laikā, izmantojot visus uzņēmumā esošos resursus. [20]

3. Piegāde un atbalsts. Domēns ietver tādas jomas, kā , piemēram, plānu izpildi, IT sistēmas un lietojumprogrammu rezultātu novērtēšanu.

4. Uzraudzība un attīstība. Šis domēns atbild par stratēģisku novērtēšanu, neatkarīgi no tā, vai pašreizējā IT sistēma joprojām atbilst mērķiem, kam tā tika izstrādāta.

5. COBIT un ISO/IEC27001:2013 savstarpēji nekonkurē, bet patiesībā savstarpēji papildina viens otru. COBIT aptver daudz plašāku teoriju nekā ISO/IEC 27001:2013. [20]

1.3 ITIL ietvars

ITIL trešās versijas (v3) drošības pārvaldības process apraksta strukturizētu drošības pielāgošanu organizāciju pārvaldībai. ITIL drošības pārvaldība ir veidota pamatojoties uz ISO/IEC 2700:2013 standartu, kā arī aptver visa veida organizācijas (tā skaitā saimniecisko darbības veicējus, bezpeļņas organizācijas, pārvaldes iestādes). Atsaucoties uz ISO/IEC 27001:2013 standartu, tas detalizēti apraksta prasības priekš ieviešanas, nostiprināšanas, izmantošanas, uzraudzības, pārbaudes, uzturēšanas un izlabošanas dokumentētam ISMS kontekstā ar organizācijas vispārējiem biznesa riskiem. ITIL paskaidro prasības par drošības kontroles ieviešanu, kas tiek individuāli pielāgots uzņēmumam vai uzņēmuma daļām. [12]

Galvenais mērķis drošības pārvaldībai ir garantēt, lai tiku nodrošināta informācijas drošība, pasargājot informāciju vērtību. Nosakot, kura informācija ir vērtīga ir jāņem vērā konfidencialitāte, integritāte un pieejamība, no tā izrietošie aspekti ir drošība, anonimitāte un informācijas pārbaudāmība. [13]

Mērķis drošības pārvaldībai var tikt sadalīts divās daļās:

1. Izpratne par drošības prasību definēšanu SLA un citas ārējās prasības, kas ir noteiktas likumdošanā, līgumos, iekšējā vai ārējā uzņēmuma politikā.

2. Izpratne par drošības pamatnostādnēm ir nepieciešama, lai garantētu organizācijas vadības nepārtrauktību, kā arī tas ir nepieciešams, lai varētu vienkāršot servisa līmeņa pārvaldību informācijas drošībai. Kad tas notiek, ir iespējams efektīvāk pārvaldīt ierobežotu daudzumu SLA, nekā pārvaldīt lielu daudzumu SLA. [13]

Drošības vadības procesi veidojas no SLA ar noteiktām drošības prasībām, likumdošanas un iekšējiem līgumiem. Šīs prasības var darboties, kā galvenie darbības indikatori (KPI), ko var izmantot par procesu vadībā un par pamatojumu rezultātiem drošības pārvaldības procesos.

Gala rezultātā informācija dod informācijas pamatojumu, lai realizētu SLA un ziņotu par atkāpēm no konkrētajām prasībām. Drošības pārvaldības procesi ir saistīti gandrīz vai ar visiem ITIL procesiem. Tomēr šī konkrētā sadaļa būs attiecināma ar servisa līmeņa vadību, incidentu pārvaldības procesos un izmaiņu pārvaldības procesos. [21]

1.4 Informācijas drošības labās prakses standarts

Informācijas drošības forums ir starptautiska, neatkarīga, bezpeļņas organizācija, kas ir vērsta uz salīdzinošo novērtēšanu un labo praksi informācijas drošības jomā. Tā tika izveidota 1989. gadā kā Eiropas Drošības forums, taču paplašināja savu misiju un dalību 1990. gadā. Šobrīd tā ietver simtiem biedru, tostarp lielu skaitu *Fortune 500* uzņēmumu, no Ziemeļamerikas, Āzijas un citām pasaules vietām . Dalībniekiem ir organizētas grupas nodaļās visā Eiropā, Āfrikā, Āzijā, Tuvajos Austrumos un Ziemeļamerikā. *ISF* galvenā mītne atrodas Londonā, Anglijā, taču ir arī darbinieki, kuri atrodas un pārstāv Ņujorku. [21]

ISF dalība ir starptautiska lielu organizāciju transporta, finanšu pakalpojumu, farmācijas, ražošanas, valdības, mazumtirdzniecības, mediju, telekomunikāciju, enerģētikas, transporta, profesionālus pakalpojumu un citus sektoru vidū. [22]

Labās prakses standarts (*SoGP*) pirmo reizi tika izlaists 1996. gadā Informācijas drošības forumā (*ISF*), un tā sīki dokumentē labāko praksi attiecībā uz informācijas drošību. Labās prakses standarts, kas ir brīvi pieejams, izriet no ISO/IEC 27001:2013 un COBIT

standartiem, un iezīmē funkcionālu informācijas drošības metodiku, pamatojoties gan uz pētījumiem , gan reālās pasaules pieredzi. [22]

Standarts ir mērķēts ap šādiem sešiem galvenajiem aspektiem:

1. Datoru uzstādīšanas. Šī darbība galvenokārt ir vērsta uz IT speciālistiem un apraksta aparatūru un programmatūru, kas nodrošina kritiskās biznesa lietojumprogrammas.

2. Kritiskajām biznesa lietojumprogrammām. Tās ir programmas, no kurām ir atkarīga organizācijas darbība. Šis aspekts ir galvenokārt vērsts uz izmaksu un ieguvumu analīzes īpašniekiem, cilvēkiem, kas atbild par biznesa procesiem un sistēmu ieviešanu.

3. Drošības pārvaldības. Drošības pārvaldības aspekts ir vērsts uz drošības lēmumu pieņēmējiem un auditoriem. Tā rīkojas vadības līmeņa lēmumu pieņemšana attiecībā uz drošības ieviešanu visā organizācijā.

4. Tīkliem. Tīkli veido īpašu kategoriju, sakarā ar to drošības ievainojamību. Tās mērķis parasti ir tīkla pārvaldītāji, tīkla speciālisti un tīkla pakalpojumu sniedzēji. Tīkla aspekts ir vērsts uz tā būtību un organizācijas tīklu prasību īstenošanu.

5. Sistēmas attīstības. Šis aspekts ir adreses sistēmu izstrādātājiem un nodarbojas ar identifikāciju, izstrādājot un ieviešot sistēmas prasības.

6. Gala lietotāja vides. Gala lietotāja vide ir vieta, kurā indivīdi izmanto organizācijas sistēmas un lietojumprogrammas, lai atbalstītu biznesa procesus. Tāpēc šim aspekts ir tendence pievērsties biznesa vadītājiem un personām, kas ikdienā ir gala lietotāji. [4]

Datoru uzstādīšana un tīkli ir pamatā esošajai IT infrastruktūrai, uz kuras darbojas kritiskās biznesa lietojumprogrammas. Gala lietotāja vide ietver aizsardzības pasākumus, kas saistīti ar korporatīvajām un darbstaciju lietojumprogrammām, kas ir pieejamas uzņēmuma darbiniekiem. Sistēmas attīstība aplūko, kā jaunas lietojumprogrammas un sistēmas ir izveidotas, un drošības pārvaldība ir tā, kas nosaka augsta līmeņa virzienu un kontroli.

Pats standarts sastāv no paziņojumiem par principiem un mērķiem, ko paskaidro dokumentācija, aptverot ieviešanas rekomendācijas. Lai saglabātu savu vērtību strauji mainīgajā pasaulē, informācijas drošības standarts tiek pārskatīts un atjaunināts reizi divos gados. Papildus labas prakses standartiem, *ISF* divreiz gadā uzrauga salīdzinošās novarēšanas programmu, kas ir pazīstama kā informācijas drošības statusa aptauja (*Security Status Survey*).

1.5 ITIL vadlīniju un ISO 27001 standarta salīdzinājums

Darba autors priekš standartu un labās prakses metodoloģijas salīdzināšanas aplūkos ISO/IEC 27001:2013, tāpēc, ka tas ir visu izrietošo labās prakses metodoloģijas pamatā. ISO/IEC 27001:2013 ir internacionāls standarts, kas nosaka prasības izveidošanu, ieviešanu, uzturēšanu un pastāvīgu uzlabošanu ar Informācijas drošības vadības sistēmu (ISMS). To ir iespējams pielāgot jebkura tipa un izmēra organizācijai. Ieviešana un sertifikācija nav obligāta.[15] [14]

Kā labās prakses metodoloģiju darba autors izvirza ITIL ietvaru, tāpēc, ka tas sniegtu neformālu, pārbaudāmu priekšstatu par kontroļu ieviešanu uzņēmumā. Autors vēlas uzsvērt, ka starptautiskais ISO kvalitātes standarts ir formāls, kā rezultātā ieviestās kontroles ir aprakstītas, turpretim ITIL ietvars tiek izmantots, lai ieviestu patiesus uzlabojumus IT drošības pārvaldībā.

ITIL ietvars atspoguļo servisa pārvaldību, sniedzot norādījumus par sniegšanas kvalitātes IT pakalpojumu un procesiem, funkcijām un citām iespējām, kas nepieciešami, lai atbalstītu viņus. Tas ir piemērojams gandrīz vai katrai IT videi. Ieviešana nav sertifikācijas objekts. [3] [14]

1.1. tabula

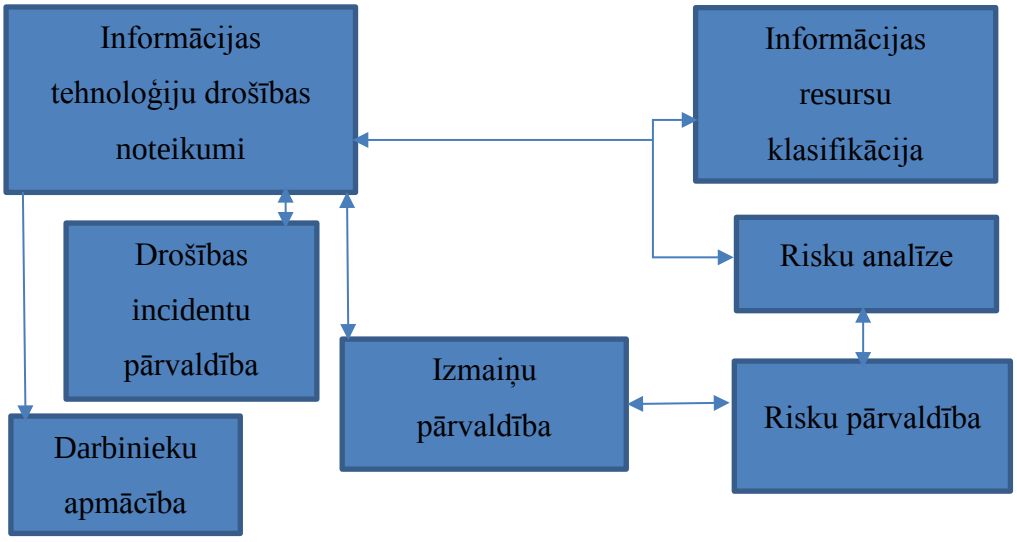
ISO 27001:2013 un ITIL atšķirības

PDCA cikls	ISO 27001:2013 punkti	ITIL posmi
Plānot	Punkts 4 – Organizācijas konteksts Punkts 5 – Vadība Punkts 6 – Plānošana Punkts 7 – Atbalsts	Pakalpojumu stratēģija Pakalpojumu projektēšana
Darīt	Punkts 8 – Darbības	Pakalpojuma restrukturizācija Pakalpojumu darbība
Pārbaudīt	Punkts 9 – Veiktspējas novērtēšana	Nepārtraukta pakalpojumu uzlabošana
Rīkoties	Punkts 10 – Uzlabošana	Nepārtraukta pakalpojumu uzlabošana

Tabulā 1.1. veiktais salīdzinājums parāda to, ka pielietojums gan ISO 27001:2013 standartam, gan ITIL(v3) ir tāda pati, taču pārbaudāmās kontroles ITIL vadlīnijām ir vērstas uz uzņēmuma un tās darbības sakārtošanu, taču standarta ISO/IEC 27001 kontroles ir vērtas uz sertifikāciju. Detalizēta ITIL un ISO27001:2013 kontroļu salīdzinājuma matrica ir aplūkojama Pielikumā Nr. 1. [15][6][14]

1.6 IT drošības pārvaldības dokumentācija

Galvenie IT drošības pārvaldības ieviešanas mērķi ir apliecināt to, ka institūcijas vadība nodrošina resursu drošību, kas paredz panākt konfidencialitāti, pieejamību un integritāti. Panākt to, lai būtu vienāda un plānveida pieeja jautājumiem, kas saistīti ar informācijas tehnoloģiju drošību. Apmācīt darbiniekus par informācijas tehnoloģiju drošības jautājumiem. Izstrādāt nepieciešamos drošības procedūras, dokumentus, kā arī ieviest tos uzņēmumā. [7][2]



1.5. attēls **IT drošības pārvaldības shēma**

Attēlā 1.5. redzamajā shēmā ir parādītas iestādes, IT drošības noteikumos obligāti iekļaujamās tēmas un to savstarpējā saistība. Shēma ir piemērs - izstrādājot iestādes IT drošības noteikumus, dokumentos iekļauj tēmas atbilstoši iestādes darbības specifikai.[8]

Papildus prasības izmaiņu pārvaldībai var papildināt ar sekojošu dokumentāciju:

- Resursu darba spēju atjaunošanas plānu,
- Portatīvo datoru izmantošanas noteikumiem,
- Ārējo datu nesēju izmantošanas noteikumiem,
- Virtuālo privāto tīklu (VPN) izmantošanas noteikumiem,

- Bezvadu interneta izmantošanas noteikumiem,
- Elektroniskā pasta izmantošanas noteikumiem.
- Iestādes iekšējo datu bāzu izmantošanas noteikumiem u.c.[7]

1.7 Iespējas un ierobežojumi uzņēmumiem

Lielākais izaicinājums uzņēmumiem ir panākt to, lai tā pakalpojumi būtu pieejami jebkurā situācijā: pakalpojumatteices vai ļaunprātīgas darbības gadījumā, kad tiek sabojāta, pārveidota vai nozagta informācija.

Pirmais solis uzņēmumam, kas vēlas ieviest drošu tīklu pirms tiek uzstādītas drošības iekārtas ir jānosaka visi esošie servisi un servisi, kas var tikt ieviesti tuvākajā laikā. [1]

Visam procesam jābūt sagrupētam secībā, lai definētu sekojošo:

- Paredzamie servisi;
- Publiskā mājaslapa;
- Publiskā mājaslapa ar drošiem norēķiniem internetā;
- *Intranet* mājaslapa ar drošu piekļuvi darbiniekiem;
- Vietne ar drošu piekļuvi sadarbības partneriem;
- Šifrētas un parakstītas elektroniskās vēstules;
- Bezvadu tīkla atbalsts;
- Satura serveri pieejami lejupielādei. [1]

2. IT DROŠĪBAS PĀRVALDĪBAS NOVĒRTĒJUMS

2.1 Iestādes apraksts

Iestāde, kurai darba autors veica novērtēšanu darbojas pakalpojumu sfērā. Uzņēmuma IT nodaļā strādā 5 darbinieki –divi no tiem ir IT administratori, divi atbalsta dienesta speciālisti, viens drošības pārvaldnieks. Uzņēmums strādā ar trīs IT pakalpojumu sniedzējiem – sistēmas apkalpojošo uzņēmumu, interneta mājaslapas uzturētāju, kā arī datu centra turētāju. Uzņēmuma tehniskais nodrošinājums sastāv no 17 darba stacijām, tā skaitā 3 portatīvajiem datoriem un viena tīkla printera. Uzņēmumam ir viens interneta savienojums, kas izmanto 2 serverus- vienu priekš grāmatvedības uzskaites un pakalpojumu nodrošināšanas sistēmām, failu uzglabāšanas un e-pasta, otru priekš rezerves kopiju glabāšanas.

Uzņēmuma IT darbinieki ir ar attiecīgu izglītību un prasmēm veikt savu darbu. IT nodaļas speciālisti regulāri apmeklē dažāda veida apmācības. IT dienests pēdējā gada laikā ieviesa grāmatvedības uzskaites sistēmu. Priekš pieejas tiesību pārvaldības tiek izmantota *Windows* servera aktīvā direktorija un skripti tīkla un sistēmu uzraudzībai.

Uzņēmumā ir izstrādāta IT drošības politika, informācijas tehnoloģiju klasifikācijas apraksts, lomu matrica, kā arī risku novēršanas plāns. Uzņēmumā ir uzsākts informācijas resursu risku analīzes process, kā arī nepabeigta anketa par klasifikācijas līmeņa piešķiršanu informācijas resursam.

Pieaugot darbinieku skaitam uzņēmumā, kā arī izmantotajām sistēmām, nākas saskarties ar jaunām problēmām, tāpēc uzņēmums vēlas sakārtot IT pārvaldības procesus un ieviest kontroles, kas uzlabotu uzņēmuma IT drošības pārvaldību.

2.2 Uzņēmumu prasības standartu ieviešanai

Kaut arī standarti ļauj organizācijām izmantot savu pieeju standarta ieviešanā, loģiski būtu izmantot strukturizētu pieeju ISMS pielietošanai.

Standarta ieviešanai piedāvātais plāns:

- Jānoskaidro pārvaldes ietvars – jāizveido projekts, jānosaka iekšējo un ārējo organizācijas kontekstu, jāidentificē uzņēmuma prasības, ieinteresētās personas un problēmas, jāidentificē ISMS apjoms, jāizvēlas nepārtrauktu uzlabojumu modeli un jānoskaidro, kāda ir uzņēmuma dokumentācija.
- Jāiegūst vadības uzticēšanos priekš ISMS, noteikt informācijas drošības politiku un jānosaka lomas.

• Jānosaka sistemātiska pieeja informācijas drošības riska novērtējumam un riska pieņemšanas kritērijiem.

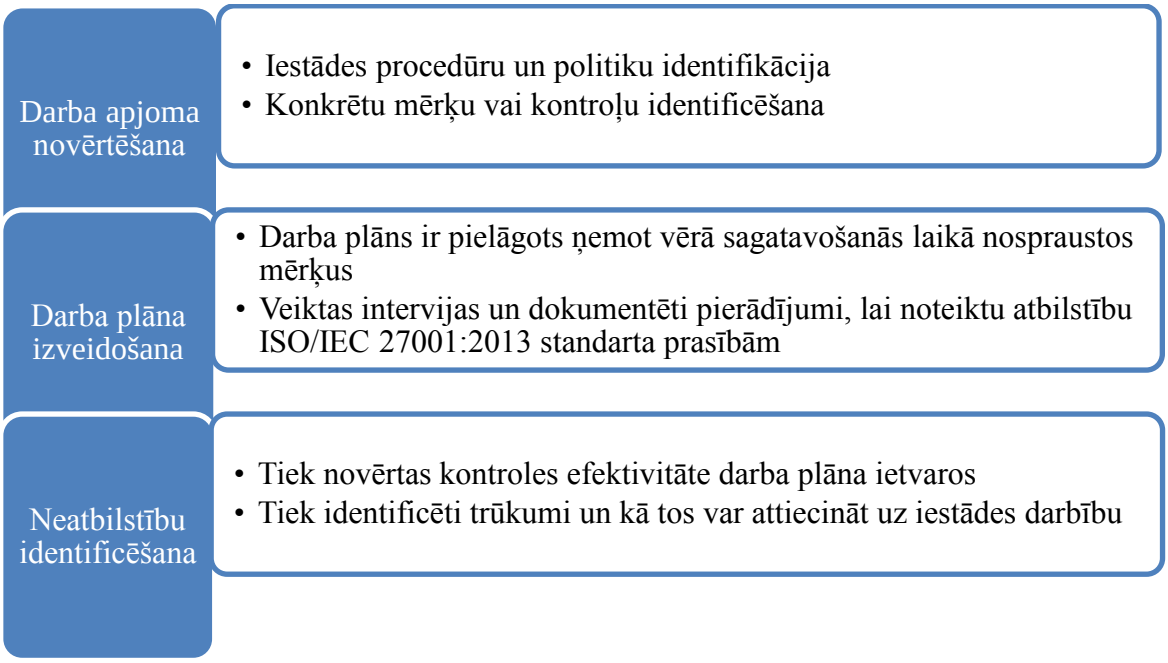
• Jāizveido riska novērtējumu, lai identificētu organizācijas nozīmīgos informācijas aktīvus un to riskus.

• Jānosaka un jāizvērtē iespējas priekš risku novēršanas, izvēloties kontroles, kuras jāievieš.

• Jāsagatavo ieteikumi priekš lietojamības un riska novēršanas plāna.

2.3 Atbilstību vērtējuma noteikšana ISO 27001:2013 standarta prasībām

ISO/IEC 27001:2013 drošības novērtējuma metodoloģija sastāv no pieejas, kura sadalīta vairākās fāzēs. Zemāk aprakstītas augsta līmeņa veiktās aktivitātes un katra līmeņa iekļautās apakš aktivitātes katras fāzes ietvaros, kuras tiks veiktas IT drošības novērtēšanā atbilstoši ISO/IEC 27001:2013 standarta prasībām (skat. attēlu 2.1.).



2.1. attēls **ISO 27001 standarta novērtēšanas plāns**

Saistībā ar trūkumu jeb neatbilstības novērtējumu, darba autors identificēs neatbilstības pret ISO / IEC 27001:2013 standarta prasībām, kas tiks aprakstītas zemāk redzamajā tabulā 2.1.

Lai novērtētu uzņēmuma IT drošības pārvaldības atbilstību pret ISO / IEC 27001:2013 standarta prasībām, darba autors novērtēs IT drošību pret ISO / IEC 27001:2013 noteiktajām prasībām.

Prasība pret dokumentāciju:

1. Pilnībā ieviestas kontroles gadījumā prasītā dokumentācija ir izstrādāta, tā ir vadības apstiprināta, tās aktuālā versija ir atbilstoša biznesa un drošības prasībām;

2. Daļēji ieviestas kontroles gadījumā prasītā dokumentācija ir izstrādāta, bet tā, piemēram, nav vēl vadības apstiprināta, vai, piemēram, izstrādāta un apstiprināta dokumentācija, bet nav pilnīgi atbilstoša esošajām biznesa un drošības prasībām, taču tai ir risku mazinoši apstākļi, ko nosedz kāda no citām kontrolēm;

3. Nav ieviestas kontroles gadījumā prasītā dokumentācija, tā nav izstrādāta, līdz ar to neizpildās arī pārējie nosacījumi.

Nav attiecināms gadījumā, ja kontrole netiek ietverta pārbaužu tvērumā vai kopīgi vienojoties ar uzņēmumu tiek nolemts, ka konkrēto kontroli nav nepieciešams novērtēt.

Prasība pret kontrolēm, kuras tiek izpildītas praksē un kurām jābūt definētām procedūrās:

1. Pilnībā ieviestas kontroles gadījumā, kādā no procedūrām ir definētas prasības pret to, kas noteikts kontrolē, kā arī ir iespējams pārliecināties, ka šīs prasības tiek izpildītas praksē;

2. Daļēji ieviestas kontroles gadījumā – vai nu nevienā no procedūrām nav definētas noteiktās prasības, bet ir iespējams pārliecināties, ka šīs prasības tiek izpildītas praksē, vai arī kādā no procedūrām tās ir definētas, bet nav iespējams pārliecināties, ka tās tiek izpildītas realitātē;

3. Nav ieviestas kontroles gadījumā nevienā no procedūrām, nav definētas noteiktās prasības, kā arī nav iespējams pārliecināties, ka tās tiek izpildītas praksē;

4. Nav attiecināms gadījumā, ja kontrole netiek ietverta pārbaužu tvērumā vai, kopīgi vienojoties ar uzņēmumu, tiek nolemts, ka konkrēto kontroli nav nepieciešams novērtēt.

5. Jāņem vērā, ka ISO 27001:2013 standarts ir attiecināms uz organizāciju un organizācijas informācijas drošības pārvaldības sistēmu kā tādu, nevis uz konkrētu organizācijas IS. ISO 27001 standarts nosaka prasības, kā izveidot, ieviest, uzturēt un nepārtraukti pilnveidot organizācijas informācijas drošības pārvaldības sistēmu organizācijas ietvaros. Pārbaužu ietvaros darba autors primāri vērtēs kontroles, kuras var attiecināt uz ISO 27001:2013 standarta prasībām.

2.4 IT atbilstības novērtējums ISO 27001:2013 standarta prasībām

Zemāk ir pievienota tabula 2.1. ar ISO 27001:2013 standarta prasību kontrolēm, novērojumiem, kā arī atbilstības novērtējums (2 – pilnībā ieviests, 1 – daļēji ieviests, 0 – nav ieviests un N/A – nav attiecināms), kurā novērtēta uzņēmuma IT drošības pārvaldība. Pētījuma ietvaros tiek aprakstīts novērojums un tā darbības. Drošības novērtējuma ietvaros darba autors veica sarunas ar atbildīgajiem darbiniekiem un analizēja pieejamo dokumentāciju.

2.1.tabula

IT drošības novērtējums pret ISO 27001:2013 standarta prasībām

Kontroles nosaukums	**Novērojumi**	**Atbilstība**
4.Organizācijas konteksts		
4.1.Organizācijas un tās konteksta izprašana	Sarunas laikā tika identificēts, ka nav formāli noteikti atbildību sadalījumi par to, kas pārvaldīs, uzturēs un sekmēs informācijas sistēmas drošības attīstību. Papildus tam atbildīgo personālu amata aprakstos netika identificēti pienākumi par sistēmas informācijas drošības pārvaldību.	2
4.2.Ieinteresēto pušu vajadzību un vēlmju izprašana	Ieinteresētajām pusēm nav formāli noteikta atbildīgā puse par sistēmas informācijas drošības pārvaldības sistēmas uzturēšanu. Līdz šim neviena no interesētajām pusēm nav pārraudzījusi informācijas sistēmas drošību.	2
4.3.Informācijas drošības vadības sistēmas darbības sfēras noteikšana	Ņemot vērā, ka nav noteiktas atbildības saistībā ar sistēmu, tādējādi pārbaudes laikā nebija iespējams pārliecināties par dokumentētu atbildības sadalījumu par IS, kas formāli pārvaldīs, uzturēs un sekmēs informācijas drošības sistēmas attīstību.	2
4.4.Informācijas drošības vadības sistēma	Skatīt punktus 4.1. - 4.3.	2
5.Vadība		
5.1.Vadība un saistības	Informācijas sistēmu drošības noteikumi ir apstiprināti no vadības, tādā veidā atbalstot	3

Kontroles nosaukums	Novērojumi	Atbilstība
	nepieciešamību ieviest informācijas drošības pārvaldības sistēmu. Informācijas drošības pārvaldības prasības tiek integrētas procesos. Informācijas sistēmu drošības noteikumi nodrošina ietvaru informācijas drošības mērķiem un veicina informācijas drošības pārvaldības sistēmas turpmāku attīstību.	
5.2.Politika	Uzņēmumā ir izstrādāti informācijas drošības noteikumi.	3
5.3.Organizācijas lomas, atbildības un autoritātes	Saistībā ar sistēmas informācijas drošības pārvaldību nav noteiktas atbildības un lomas.	2
6.1.Darbības risku novēršana un iespējas		
6.1.1.Vispārējā plānošana	Sistēmai nav formāli noteiktas atbildības par sistēmas informācijas drošību, kā arī nav skaidri noteikta sistēmas informācijas drošības pārvaldības sistēma.	2
6.1.2.Informācijas drošības risku novērtēšana	Novērtēšanas laikā darba autors identificēja, ka saistībā ar sistēmai nav veikta formāla risku analīze.	2
6.1.3.Informācijas drošības risku novēršana	Novērtēšanas laikā darba autors identificēja, ka sistēmai nav veikta risku analīze un attiecīgi izstrādāts risku novēršanas plāns (tajā skaitā iestādes veiktajām risku analīzēm darba autors neidentificēja izstrādātus risku novēršanas plānus un atbildīgos darbiniekus par plānu ieviešanu).	2
6.2.Informācijas drošības mērķi un to sasniegšanas plānošana		
6.2.Informācijas drošības mērķi un to sasniegšanas plānošana	Uzņēmumā ir ieviesti informācijas drošības noteikumi.	3
7.Atbalsts		
7.1.Resursi	Nepieciešamības gadījumā ir iespējams piesaistīt	3

Kontroles nosaukums	**Novērojumi**	**Atbilstība**
	papildus resursus.	
7.2.Spējas	Darbiniekiem regulāri tiek veiktas apmācības par sistēmas izmantošanu.	3
7.3.Informētība	Visiem darbinieki, kuri stājas darbā, ir jāiepazīstas ar drošības noteikumiem un jāapliecina, ka ar tiem ir iepazinušies. Papildus tam tiek veiktas ikgadējas apmācības par informācijas drošību.	3
7.4.Komunikācija	Visiem darbinieki, kuri stājas darbā, ir jāiepazīstas ar drošības noteikumiem un jāapliecina, ka ar tiem ir iepazinušies. Papildus tam tiek veiktas ikgadējas apmācības par informācijas drošību.	3
7.5.Dokumentētā informācija (7.5.1., 7.5.2. un 7.5.3.)	Nav izstrādātas visas procedūras un priekšraksti, kuri ir noteiktas ISO 27001 standartā.	2
8.Darbības		
8.1.Operatīva plānošana un kontrolēšana	Informācijas drošības pārvaldnieks un iestādes vadība ir atbildīga par informācijas drošības pārvaldības sistēmas plānošanu, ieviešanu un kontroli, lai sasniegtu informācijas drošības pārvaldības sistēmas noteiktos mērķus un prasības.	3
8.2.Informācijas drošības risku novērtējums	Skatīt sadaļu 6.1.	2
8.3. Risku novēršana	Skatīt sadaļu 6.1.	2
9.Veiktspējas novērtēšana		
9.1.Monitorings, mērīšana, analizēšana un novērtēšana	Informācijas drošības pārvaldības sistēmas monitorings, mērīšana, analizēšana un novērtēšana ir iestādes vadības un informācijas drošības pārvaldnieka pārziņā. Pārbaudes laikā tika identificēts, ka saistībā ar veiktajām pārbaudēm pēc to rezultātiem nav pieejami	2

Kontroles nosaukums	Novērojumi	Atbilstība
	identificēto risku novērtēšanas vai mazināšanas plāni un plānotas korektīvas darbības.	
9.2.Iekšējā auditēšana	Uzņēmumam tiek veikti gan ārējie auditi, gan iekšējie auditi (no trešās puses) saistībā ar informācijas drošību.	3
9.3.Vadības pārskatīšana	Novērtēšanas laikā tika noskaidrots, ka audita rezultātus pārskata no uzņēmuma vadības puses.	3
10.Uzlabošana		
10.1.Neatbilstības un rīcība to atrisināšanai	Darba autoram nebija iespēja pārliecināties par veikto pārbaužu neatbilstību atrisināšanas plāniem, to cēloņu analīzi un veiktajām darbībām, lai tos novērstu.	N/A
10.2. Nepārtraukta uzlabošana	Uzņēmuma ietvaros tiek veikti iekšējie un ārējie auditi, lai uzlabotu informācijas drošības pārvaldības sistēmas uzlabošanu.	3
A.5.Informācijas drošības politika		
A.5.1.1.Informācijas drošības politika	Uzņēmumam ir izstrādāti informācijas drošības noteikumi. Informācijas drošības noteikumos ir atrunāta kārtība par informācijas resursu lietošanu, piekļuvi, rezerves kopiju pārvaldību, datu nesēju lietošanu un citiem informācijas drošības aspektiem	3
A.5.1.2.Informācijas drošības politikas pārskatīšana	Novērtēšanas laikā tika noskaidrots, ka uzņēmumam ir pārskatīta informācijas drošības dokumentācija pēdējā gada laikā.	3
A.6.Informācijas drošības organizēšana		
A.6.1.1.Informācijas drošības lomas un atbildības	Skatīt 4. sadaļu.	2
A.6.1.2.Pienākumu nošķiršana	Skatīt 4. sadaļu.	2
A.6.1.3. Kontakti ar varas institūcijām	Uzņēmuma darbībai nav nepieciešama komunikācija ar varas iestādēm.	
A.6.1.4.Kontakti ar	Tiek uzturēta saziņa ar drošības speciālistiem	3

Kontroles nosaukums	**Novērojumi**	**Atbilstība**
speciālām interešu grupām	saistībā ar informācijas drošības jautājumiem.	
A.6.1.5.Informācijas drošības projektu vadība	Saistībā ar sistēmas izstrādi pārbaudes laikā tika noskaidrots, ka informācijas drošības pārvaldnieks nav aktīvi iesaistījies sistēmas izstrādes ietvaros, ņemot vērā to, ka nav formāli nozīmētas atbildības par sistēmas uzturēšanu.	2
A.7.Drošība attiecībā uz cilvēku resursiem		
A.7.1.1.Uzticamības pārbaudīšana	Uzņēmumā ir iekšējās procedūras, kuras periodiski jāiziet visiem darbiniekiem.	3
A.7.1.2.Nodarbinājum noteikumi	Uzņēmumā visi darbinieki strādā ar līgumiem, kā arī darbiniekiem ir jāiepazīstas ar informācijas drošības noteikumiem pirms darba uzsākšanas.	3
A.7.2.1.Vadības pienākumi	Novērtēšanas laikā darba autors identificēja, ka līguma ietvaros ar izstrādātāju dokumentācijā ir atrunātas drošības prasības kā, piemēram, pakalpojumi atbilst noteiktajām informācijas drošības prasībām un pakalpojums atbilst informācijas sistēmu un resursu drošības politikai un lietošanas noteikumiem un *Open Web Application Security Project* vadlīnijām	3
A.7.2.2.Informācijas drošības informēšana, izglītošana un apmācība	Visiem darbinieki, kuri stājas darbā, ir jāiepazīstas ar drošības noteikumiem un jāapliecina, ka ar tiem ir iepazinušies. Papildus tam tiek veiktas ikgadējas apmācības par informācijas drošību.	3
A.8.Aktīvu pārvaldība		
A.8.1.1.Inventāra saraksts	Uzņēmuma inventāra saraksts tiek uzturēts grāmatvedības vajadzībām	3
A.8.1.2.Atbildība par aktīviem	Atbildība par aktīviem ir atrunāta līgumā.	3
A.8.1.3.Pieļaujamā aktīvu izmantošana	Pieļaujamā aktīvu izmantošana ir atrunāta līgumā, kā arī iekšējās procedūrās.	3

2.1. tabulas 5. turpinājums

Kontroles nosaukums	**Novērojumi**	**Atbilstība**
A.8.1.4.Aktīvu nodošana atpakaļ	Darba autors neidentificēja vienotu aktīvu reģistru, kurā būtu uzskaitīti iestādes IT aktīvi, kā piemēram datori, telefoni u.c.	2
A.8.2.1.Informācijas klasifikācija	Novērtēšanas laikā darba autors neidentificēja iestādes izstrādāto informācijas klasifikācijas noteikumu piemērošanu saistībā ar sistēmas ieviešanu.	2
A.8.2.2.Informācijas iezīmēšana	Novērtēšanas laikā tika identificēts, ka iestādes drošības dokumentācija netiek iezīmēta atbilstoši klasifikācijai.	2
A.8.2.3.Darbības ar aktīviem	Pārbaudes laikā netika identificēta procedūra par aktīvu pārvietošanu, darbībām ar aktīviem (tajā skaitā zibatmiņām), ņemot vērā informācijas klasifikācijas noteikumus.	1
A.8.3.1.Darbības ar zibatmiņām	Iestādē nav ieviesti ierobežojumi zibatmiņu iekārtu lietošanai, kā arī netiek filtrēta datu plūsma, lai identificētu un bloķētu neautorizētas datu plūsmas.	1
A.8.3.2.Zibatmiņu likvidēšana	Nav atrunāta kārtība par zibatmiņu likvidēšanu.	1
A.8.3.3.Zibatmiņu pārvietošana	Nav atrunāta kārtība par zibatmiņu pārvietošanu.	1
A.9.Piekļuves kontroles		
A.9.1.1.Piekļuves kontroles politika	Pārbaudes laikā tika identificēts, ka sistēmai ir izstrādāta piekļuves kontroles politika, kā arī pārbaudes laikā tika identificēts, ka ir izstrādāta dokumentēta procedūra pie pieejas tiesību piešķiršanu priviliģētiem lietotājiem. Ir ieviesta sistēmas lietotāju lomu matrica, kas definē piekļuves tiesības dažādiem sistēmas lietotājiem.	3
A.9.1.2. Piekļuve tīklam un tīkla servisiem	Lai piekļūtu tīklam, tiek pieprasīta autentifikācija.	3
A.9.2.1.Lietotāju	Uzņēmumā ir ieviests formāls lietotāju	3

Kontroles nosaukums	**Novērojumi**	**Atbilstība**
reģistrācija un bloķēšana	reģistrācijas un bloķēšanas process, lai lietotājiem būtu iespēja piekļūt sistēmai.	
A.9.2.2.Piekļuves nodrošināšana	Lietotāju tiesību piešķiršana tiek veikta no administratoru puses.	3
A.9.2.3.Priviliģēto piekļuves tiesību pārvaldība	Pārbaudes laikā tika identificēts, ka ir izstrādāta dokumentēta procedūra par pieejas tiesību piešķiršanu priviliģētiem lietotājiem.	3
A.9.2.4. Slepenas lietotāju autentifikācijas informācijas pārvaldība	Netika identificēti pārkāpumi slepenas lietotāju autentifikācijas informācijas pārvaldībā	3
A.9.2.5. Lietotāju piekļuves tiesību revīzija	Pārbaudes laikā tika noskaidrots ka tiek formāli pārskatītas lietotāju tiesības un lietotāju piekļuves. Lietotāju piekļuves tiesību revīzija tiek veikta pēc pašu administratoru iniciatīvas.	3
A.9.2.6.Lietotāju tiesību atcelšana vai koriģēšana	Lietotāju tiesību atcelšanai un koriģēšanai tiek izmantota WAD.	3
A.9.3.1.Slepenas autentifikācijas informācijas lietošana	Uzņēmuma ietvaros autentificēšanās nolūkos, lai piekļūtu informācijas resursiem, tiek izmantoti droši paroļu iestatījumi. Autentifikācija notiek caur WAD.	3
A.9.4.1.Informācijas piekļuves ierobežošana	Ir ieviesta autorizācija un autentifikācija, kas ierobežo piekļuvi informācijai.	3
A.9.4.2.Drošas pieteikšanās priekšraksti	Tiek lietota WAD, kas nodrošina piekļuvi domēnam, tīkla diskiem un datortīklam.	3
A.9.4.3. Paroļu pārvaldības sistēma	Pārbaudes laikā tika identificēts, ka pašlaik nav noteikti paroļu politikas iestatījumu sarežģītība, kā arī lietotājam nav iespēja pašam nomainīt paroli, lai piekļūtu sistēmai.	1
A.9.4.4.Priviliģēto utilītprogrammu lietošana	Administratori ikdienā izmanto divus kontus - vienu ārkārtas vajadzībām, otru ikdienas organizatoriskajām darbībām.	3
A.9.4.5.Programmatūras	Programmatūras pirmkodu glabā uz attālināta	3

Kontroles nosaukums	Novērojumi	Atbilstība
pirmkoda piekļuves kontrolēšana	servera.	
A.10.Kriptogrāfija		
A.10.1.1.Kriptogrāfiskās vadīklas lietošanas politika	Nav izstrādāta politika par kriptogrāfisko kontroļu lietošanu, taču uzņēmumā tiek izmantota kriptogrāfija visiem atmiņas veidiem.	2
A.10.1.2.Šifratslēgu pārvaldība	Skatīt A.10.1.1.	2
A.11.Vides drošība un fiziskā drošība		
A.11.1.1.Fiziskās drošības perimetrs	Uzņēmumam ir ieviests drošības perimetrs ar apsardzi, videonovērošanas kamerām un ieejas kontroli.	3
A.11.1.2.Fiziskās piekļuves vadīklas	Apmeklētājiem ir jāieraksta žurnālā serveru telpas apmeklējums, kā arī pie serveru telpas ieejas 24 stundas diennaktī ir apsardze un piekļuve serveru telpas apmeklējumam var notikt tikai atbildīgo darbinieku pavadībā.	1
A.11.1.3.Biroju, kabinetu un informācijas apstrādes līdzekļu aizsardzība	Informācijas apstrādes līdzekļu cietie diski ir šifrēti un aizsargāti ar paroli. Fiziskā atslēgu aizsardzība informācijas apstrādes līdzekļiem nav ieviesta.	2
A.11.1.4.Aizsardzība pret ārējiem un ar vidi saistītiem draudiem	Serveru telpa tiek apsargāta un tajā ir ugunsdrošības detektori. Nav aizsardzība pret mitrumu. Nav automātisks durvju aizvēršanas mehānisms.	2
A.11.1.5.Darba drošības zonās	Uzņēmumā ir ieviests drošības zonējums, kur piekļuve tiek pārvaldīta, izmantojot lietotājiem piešķirtās elektroniskās identifikācijas un autorizācijas kartes.	3
A.11.1.6.Ekspedīcijas un kraušanas zona		
A.11.2.1.Tehnisko līdzekļu	Informācija tiek glabāta serveros, kuri ir izveidoti	3

Kontroles nosaukums	Novērojumi	Atbilstība
izvietošana un aizsardzība	fiziski aizsargātos datu centros. Piekļuve datu centriem ir atsevišķiem darbiniekiem, kuriem tas ir nepieciešams darba pienākumu veikšanai.	
A.11.2.2.Inženieraprīkojums	Nav ieviesti elektrības pārrāvumu atjaunošanas mehānismi. Serveru telpās ir ieviesta gaisa kondicionēšana, internets un elektrības ievads.	2
A.11.2.3.Kabeļu drošība	Novērtēšanas laikā netika identificēti sakaru kanāli, kuri nebūtu pasargāti pret fiziskiem bojājumiem.	3
A.11.2.4.Tehnisko līdzekļu uzturēšana	Nav skaidri noteiktas atbildības par sistēmas tehnisko resursu uzturēšanu.	2
A.11.2.5.Aktīvu pārvietošana	Nav noteikti noteikumi saistībā ar aktīvu pārvietošanu.	2
A.11.2.6.Tehnisko līdzekļu un aktīvu drošība ārpus organizācijas telpām	Nav noteikti noteikumi saistībā ar aktīvu pārvietošanu.	2
A.11.2.7.Droša tehnisko līdzekļu likvidēšana vai nodošana citādai izmantošanai	Droša tehnisko līdzekļu likvidēšana vai nodošana citādai izmantošanai nav aprakstīta.	2
A.11.2.8.Neuzraudzīti lietotāju tehniskie līdzekļi	Uzņēmumā ir noteikts, ka neuzraudzītiem tehniskajiem resursiem ir jābloķē piekļuve.	3
A.11.2.9.Tukša darbgalda un tukša ekrāna politika	Iestādes ietvaros nav atrunāta kārtība par tukša darbagalda un tukša ekrāna politiku.	2
A.12.Ekspluatācijas drošība		
A.12.1.1.Dokumentēti ekspluatācijas priekšraksti	Saistībā ar sistēmu pārbaudes laikā tika identificēts, ka nav pieejama administratora rokasgrāmata vai citi sistēmas ekspluatācijas priekšraksti.	1
A.12.1.2.Izmaiņu pārvaldība	Saistībā ar sistēmu, ņemot vērā, ka visas izmaiņas tiek veiktas pasūtītāja un izpildītāja līguma ietvaros, PPS un citu dokumentu pieejamība norāda par konsekventu izmaiņu	2

Kontroles nosaukums	Novērojumi	Atbilstība
	pārvaldību. Novērtēšanas laikā tika identificēts, ka iestādei nav izstrādāta formāla izmaiņu pārvaldības procedūra, kas aprakstītu, kā jāpārvalda programmatūras izmaiņas, programmatūras izmaiņas galvenos procesus izmaiņu pārvaldības procesā, kā arī atbildīgos darbiniekus šajā procesā.	
A.12.1.3.Darba jaudas pārvaldība	Saistībā ar sistēmas darba jaudas pārvaldību pārbaudes laikā darba autors neidentificēja monitoringa sistēmas, kas uzraudzītu sistēmas darba jaudu. Papildus tam pašlaik nav plānoti pasākumi saistībā ar pieeju, kā tiks veiktas prognozes par sistēmas darba jaudu un nepieciešamajiem resursiem, kā arī nav noteikti atbildīgie darbinieki par darba jaudas uzraudzību un plānošanu.	1
A.12.1.4.Izstrādes un testēšanas struktūrvienību nodalīšana no ekspluatācijas struktūrvienībām	Pārbaudes laikā tika noskaidrots, ka iestādes telpās ir izvietota sistēmas infrastruktūra, taču sistēma nav nodota ar sistēmas testa vidi.	1
A.12.2.1.Vadīklas pret vīrusiem	Novērtēšanas laikā tika identificēts, ka uz iestādes darbstacijām tiek izmantotas pretvīrusu programmatūras. Taču drošības testēšanas laikā tika identificēts, ka sistēmā ir iespējams augšupielādēt kaitīgus failus.	2
A.12.3.1.Informācijas dublējumkopijas	Novērtēšanas laikā tika noskaidrots, ka procedūrā saistībā ar izmaiņām Sistēmā nav veiktas izmaiņas procedūrā.	2
A.12.4.1.Notikumu reģistrēšana	Pašlaik nav formāli noteikti kādi notikumi jeb auditācijas pieraksti ir jāveic sistēmā, kā arī nav noteikta atbildīgā persona par regulāru auditācijas pierakstu pārskatīšanu.	2
A.12.4.2.Audita žurnālu	Pārbaudes laikā tika noskaidrots, ka auditācijas	3

Kontroles nosaukums	Novērojumi	Atbilstība
informācijas aizsardzība	pieraksti tiek glabāti nošķirtā vietā no sistēmas. Sistēmas lietotāji ar priviliģētām tiesībām var modificēt un dzēst audita pierakstus.	
A.12.4.3.Administratoru un operatoru žurnāli	Pārbaudes laikā tika identificēts, ka administratoru aktivitātes tiek auditētas, taču saistībā ar to, ka sistēma nav formāli nodota iestādē nav noteiktas atbildības par auditācijas pierakstu regulāru pārskatīšanu.	2
A.12.4.4.Pulksteņu sinhronizēšana	Laiks tiek sinhronizēts ar domēna kontrolieri.	3
A.12.5.1.Programmatūras uzstādīšana uz ekspluatējamām sistēmām	Pārbaudes laikā tika identificēts, ka nav izstrādāti priekšraksti, kā sistēma tiek uzstādīta uz produkcijas vidi un kas ir atbildīgs par minēto procesu.	1
A.12.6.1.Tehnisko ievainojamību pārvaldība	Drošības testēšanu ir ieteicams veikt regulāri visos OSI līmeņos.	2
A.12.6.2.Ierobežojumi programmatūras instalācijai	Uzņēmuma darbinieki nav spējīgi instalēt programmatūru darba stacijās. Programmatūru instalēt var tikai IT administratori.	3
A.12.7.1.Informācijas sistēmas audita vadīklas	Audita prasības ir definētas PPS, taču prasības par audita pierakstu aizsardzību un kontroles dizains novērtēšanas laikā nebija pieejams.	2
A.13.Sakaru drošība		
A.13.1.1.Tīkla vadīklas	Iestādes ietvaros nav ieviests datu noplūšanas aizsardzības risinājums.	2
A.13.1.2.Tīkla pakalpojumu drošība	Uz doto brīdi nebija noteiktas prasības par sistēmas nepieejamību un monitoringu.	2
A.13.1.3.Nošķiršana tīklos	Pārbaudes laikā tika identificēts, ka sistēmas publiski pieejamais tīmekļa serveris nav nodalīts no sistēmas pārējās infrastruktūras.	1
A.13.2.1.Informācijas pārsūtīšanas politikas un priekšraksti	Informācijas pārsūtīšanas politikas un priekšraksti ir aprakstīti procedūrās „Informācijas sistēmu un resursu drošības noteikumi” un	3

Kontroles nosaukums	Novērojumi	Atbilstība
	"Informācijas klasificēšanas noteikumi".	
A.13.2.2.Nolīgumi par informācijas pārsūtīšanu	Interviju laikā darba autors noskaidroja, ka līgumos ar ārējām pusēm ir definētas drošības prasības un noteiktas atbildības.	3
A.13.2.3.Elektroniskā ziņojumapmaiņa	Uzņēmuma ietvaros elektroniskai ziņu apmaiņai tiek izmantoti e-pasti.	3
A.13.2.4.Konfidencialitātes vai neatklāšanas vienošanās	Darbinieki, stājoties darba tiesiskajās attiecībās, parakstās par konfidencialitātes ievērošanu. Līgumos ar sadarbības partneriem ir noteikta konfidencialitāte, kā arī pienākumi un atbildība.	3
A.14.Sistēmu iegāde, izstrāde un uzturēšana		
A.14.1.1.Informācijas drošības prasību analīze un specificēšana	Novērtēšanas laikā, analizējot PPS un PPA Sistēmas dokumentāciju, tika identificētas informācijas drošības prasības attiecībā uz sistēmu.	3
A.14.1.2.Lietotņu pakalpojumu drošības nodrošināšana publiskajā tīklā	Drošības pārbaudes laikā tika identificēti tehniski riski saistībā ar datu šifrēšanu.	2
A.14.1.3.Aizsardzība lietotņu pakalpojumu darījumiem	Drošības pārbaudes laikā tika identificēti tehniski riski saistībā ar datu šifrēšanu.	2
A.14.2.1.Droša izstrādes politika	Pārbaudes laikā tika identificēts, ka saistībā ar sistēmu nav atrunātas sistēmas drošas izstrādes vadlīnijas un pēc kādām drošības prasībām izstrādātājam būtu jāizstrādā sistēma. Izstrādātājam nav formāli izstrādāta drošas izstrādes politika un vadlīnijas, pēc kurām ir jāizstrādā programmatūra vai izmaiņas. Dažas ar drošību saistītas prasības tika atrunātas sistēmas PPS ietvaros.	2
A.14.2.2.Sistēmu izmaiņu	Novērtēšanas laikā iestādes ietvaros netika	2

Kontroles nosaukums	**Novērojumi**	**Atbilstība**
vadīklas priekšraksti	identificēta izmaiņu pārvaldības procedūra.	
A.14.2.3.Tehniskā revīzija, lietotņu pēc operētājsistēmu grozījumiem	Darba autoram nebija iespēja pārliecināties par veikto pārbaužu neatbilstību.	N/A
A.14.2.4.Pakotņu grozījumu ierobežošana	Novērtēšanas laikā tika noskaidrots, ka izstrādātās sistēmas kodam netiek veikta koda caurskate, lai noteiktu, vai kods nesatur kaitīgu funkcionalitāti.	2
A.14.2.5.Drošas sistēmas izstrādes principi	Pārbaudes laikā netika identificēti formāli atrunāti un dokumentēti drošas sistēmas izstrādes principi sistēmai. Dažas ar drošību saistītas prasības tika atrunātas sistēmas PPS ietvaros.	2
A.14.2.6.Droša izstrādes vide	Uzņēmumā ir izveidota droša izstrādes vide, kurā piekļuve ir tikai autorizētiem darbiniekiem un izstrādātājiem. Testa vidē tiek izmantoti anonīmi dati.	3
A.14.2.7.Citai organizācijai nodota izstrāde	Sistēma izstrādāta balstoties uz līgumu	3
A.14.2.8.Sistēmas drošības testēšana	Sistēmas drošības testēšana tiek veikta no darba neatkarīgas trešās puses.	3
A.14.2.9.Sistēmas akcepttestēšana	Novērtēšanas laikā tika novērots, ka sistēmai ir veikti formāli akcepttesti.	3
A.14.3.1.Testa datu aizsardzība	Novērtēšanas laikā tika novērots, ka testējamā Sistēmā netiek lietoti dati, kuri ir konfidenciāli vai būtiski. Testēšanas ietvaros tiek ģenerēti nejauši dati.	3
A.15.Piegādātāju saistības		
A.15.1.1.Informācijas drošības politika piegādātāju saistībām	Novērtēšanas laikā netika identificēta procedūra, kas reglamentētu kārtību, kādā ir veicama trešo pušu sniegto pakalpojumu informācijas drošības uzraudzīšana un auditēšana.	2
A.15.1.2.Drošības jautājumu kārtošana	Novērtēšanas laikā tika novērots, ka testējamā Sistēmā netiek lietoti dati, kuri ir konfidenciāli	3

Kontroles nosaukums	Novērojumi	Atbilstība
nolīgumos ar piegādātājiem	vai svarīgi un testēšanas ietvaros tiek ģenerēti nejauši dati.	
A.15.1.3.Informāciju un komunikāciju tehnoloģiju piegādātāju ķēdē	Balstoties uz interviju laikā iegūto informāciju, darba autors noskaidroja, ka pakalpojumu piegāde tiek regulēta ar savstarpējiem līgumiem, kuros ietverta atbildība, pienākumi, kā arī konfidencialitātes atrunas.	3
A.15.2.1.Pakalpojumu sniedzēju pārraudzīšana un revidēšana	Sadarbība ar ārējiem piegādātājiem notiek uz līgumu pamata. Līgumos ir definētas saistības, kā arī rīcība saistību neizpildes gadījumā.	3
A.15.2.2.Pakalpojumu grozījumu pārvaldība	Grozījumi tiek veikti kā esošā līguma pielikums.	3
A.16. Informācijas drošības incidentu pārvaldība		
A.16.1.1.Atbildības un priekšraksti	Pārbaudes laikā netika identificēti priekšraksti par sistēmas informācijas drošības incidentu atbildībām, lai nodrošinātu ātru, efektīvu un strukturizētu reaģēšanu uz informācijas drošības incidentiem.	2
A.16.1.2. Ziņošana par informācijas drošības notikumiem	Pārbaudes laikā tika noskaidrots, ka nav izstrādāti priekšraksti, kas noteiktu ziņošanu par informācijas drošības incidentiem un caur kādiem informācijas kanāliem to darīt sistēmas ietvaros.	2
A.16.1.3.Ziņošana par nedrošībām	Darbinieki un sistēmas pārvaldītāja trešās puses, ar kurām ir noslēgtas līgumiskas attiecības, būtu jābūt informētiem par informācijas nedrošību ziņošanu, ja tādas tiek identificētas.	2
A.16.1.4.Novērtējums un lēmums par informācijas drošības notikumiem	Sistēmai nav izstrādāta kārtība, kādā veidā tiek pieņemti lēmumi un novērtējumi par informācijas drošības notikumiem.	2
A.16.1.5.Reaģēšana uz informācijas drošības	Pārbaudes laikā tika identificēts, ka nav izstrādāta dokumentēta kārtība, kā tiek reaģēts uz	1

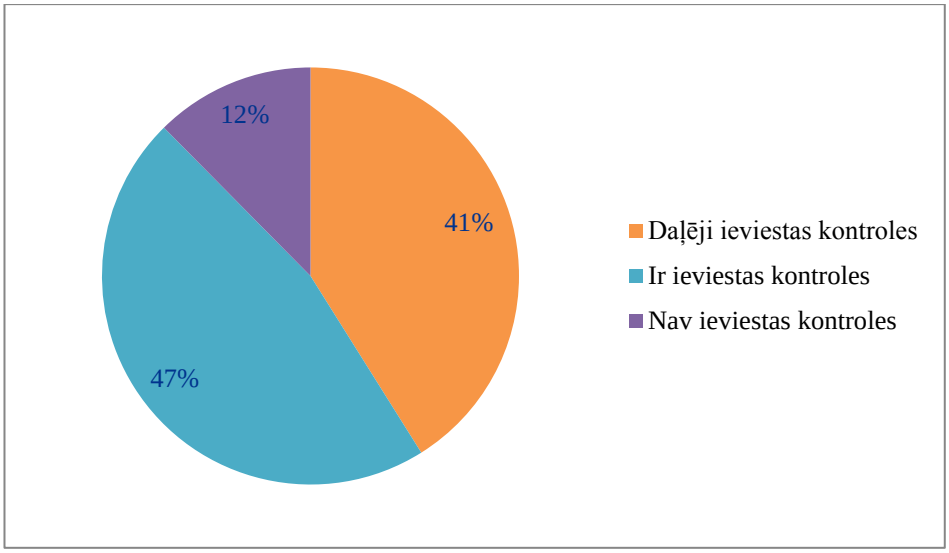
Kontroles nosaukums	Novērojumi	Atbilstība
incidentiem	informācijas drošības incidentiem.	
A.16.1.6. Mācīšanās no informācijas drošības incidentiem	Pārbaudes laikā tika identificēts, ka nav dokumentēta, nedz ieviesta kārtība par informācijas drošības incidentu mācīšanos - zināšanas, kuras iegūtas no informāciju drošības incidentu analīzes un atrisināšanas, jāizmanto, lai samazinātu incidentu iespējamību nākotnē.	1
A.16.1.7.Liecību vākšana	Pārbaudes laikā tika identificēts, ka nav izstrādāta kārtība, kā identificējami, savācami un uzglabājami drošības incidentu pierādījumi.	2
A.17.Organizācijas darbības nepārtrauktības pārvaldība informācijas drošības aspektā		
A.17.1.1.Informācijas drošības nepārtrauktības plānošana	Pārbaudes laikā tika identificēts, ka nav formāli plānota informācijas drošības nepārtrauktība nelabvēlīgu apstākļu gadījumā (dabas katastrofas vai krīzes situācijās).	2
A.17.1.2.Informācijas drošības nepārtrauktības ieviešana	Pārbaudes laikā tika identificēts, ka sistēmai nav izveidoti, dokumentēti, ieviesti, uzturēti procesi un kontroles, lai nodrošinātu nepārtrauktības līmeņa prasības informācijas drošībai nelabvēlīgu apstākļu situācijā.	2
A.17.1.3.Informācijas drošības nepārtrauktības apstiprināšana, pārskatīšana un novērtēšana	Pārbaudes laikā tika identificēts, ka saistībā ar to, ka nav formāli ieviesta darbības nepārtrauktība, nav veiktas regulāras informācijas drošības nepārtrauktības pārbaudes, lai nodrošinātu, ka ieviestās kontroles ir efektīvas negaidītas situācijas ietvaros.	2
A.17.2.1.Informācijas apstrādes iekārtu pieejamība	Pārbaudes laikā tika identificēts, ka sistēmai nav noteikts drošības līmenis, ņemot vērā sistēmas pieejamības prasības.	1
A.18.Atbilstība normām		
A.18.1.1.Attiecīgo tiesisko normu un līgumisko prasību	Novērtēšanas laikā tika noskaidrots, ka tiek pārvaldītas attiecīgās tiesiskās normas un līgumi	3

Kontroles nosaukums	Novērojumi	Atbilstība
noskaidrošana	par prasību noskaidrošanu	
A.18.1.2.Intelektuālā īpašuma tiesības	Līgumos ir atrunātas autortiesības un konfidencialitāte.	3
A.18.1.3.Ierakstu aizsardzība	Uzņēmumā ir ieviestas tehniskas un administratīvas kontroles ierakstu aizsardzībai.	3
A.18.1.4.Personu identificējošas informācijas privātums un aizsardzība	Pārbaudes laikā tika identificēts, ka sistēmā nav noteiktas personu datu aizsardzības kontroles.	1
A.18.1.5.Kriptogrāfisko vadīklu reglamentēšana	Novērtēšanas laikā netika identificētas kriptogrāfiskās vadīklas.	1
A.18.2.1.Neatkarīga informācijas drošības pārskatīšana	Novērtēšanas laikā tika noskaidrots, ka tiek veiktas neatkarīgas informācijas drošības pārskatīšana katru gadu	3
A.18.2.2.Atbilstība drošības politikai un standartiem	Novērtēšanas ietvaros tika noskaidrots, ka uzņēmuma vadība ir atbildīga par atbilstību noteiktiem standartiem un informācijas drošības politikai.	3
A.18.2.3.Tehniskās atbilstības pārskatīšana	Novērtēšanas laikā tika identificēts, ka nav veikti neatkarīga ielaušanās testēšana gan iekšējam tīklam un publiski pieejamajai infrastruktūrai.	2

Pēc veiktajiem novērojumiem tika noskaidrots, ka uzņēmumā nav ievērotas visas ISO 27001:2013 standartā minētās prasības, kas saistītas ar IT dokumentācijām, kā arī uzņēmuma politiku. Uzņēmuma IT drošības pārvaldības galvenās nepilnības ir saistītas ar to, ka nepieciešams noteikt atbildīgās personas un to iesaisti procesos, jānosaka formālu drošības lomu sadalījumu, kā arī rīcību dažādās nestandarta situācijās. Galvenās iekšējās politikas, kuras nepieciešams pārskatīt saistībā ar formālu risku analīzi, aktīvu reģistru izveidi, zibatmiņas lietošanas un iznīcināšanas politiku izstrādāšanu, incidentu pārvaldības plānu, personas datu aizsardzības un kriptogrāfijas kontroles mehānismu ieviešanu.

Kontroļu atbilstības kopsavilkumam darba autors piedāvā veikt apkopojumu par ISO/IEC 27001:2013 standarta kontroļu atbilstībām. Apkopojot uzņēmuma IT drošības pārvaldības atbilstību (izmantojot metodoloģiju, kas pievienota pielikumā Nr.2) pret 129 ISO/IEC 27001:2013 standartā aprakstītajām kontrolēm, tika noskaidrots, ka uzņēmuma IT drošības kontroles ir ieviestas 60 ietvarā aprakstītajām kontrolēm jeb 47% gadījumu.

Uzņēmuma IT drošības pārvaldībā daļēji ir ieviestas 53 standartā aprakstītās kontroles jeb 41% gadījumu, taču nav ieviestas 16 kontroles jeb 12% gadījumu. Skatīt attēlu 2.2.

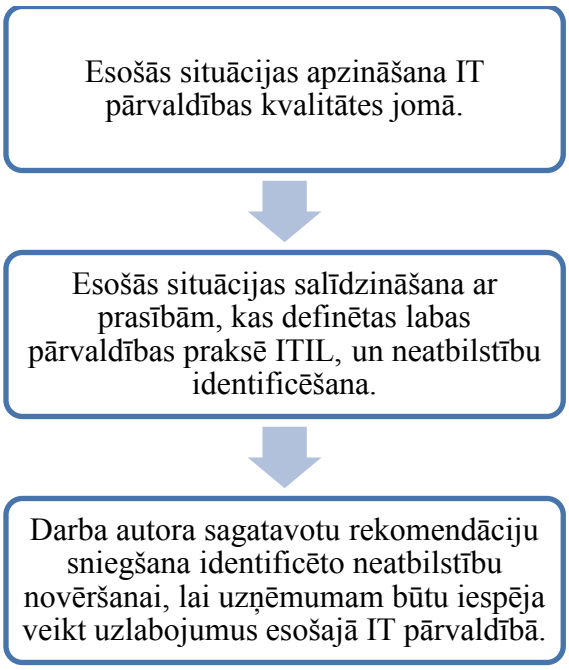


2.2. attēls **Apkopojums par atbilstību ISO 27001 standartam**

Standartā ISO 27001:2013 tiek formāli aprakstītas kontroles, kādas uzņēmumam ir nepieciešamas, lai tā IT drošības pārvaldība atbilstu aplūkotajam standartam. Priekš uzņēmuma IT drošības pārvaldības izvērtējuma darba autors nākošajā nodaļā piedāvā novērtēt atbilstību labās prakses ITIL ietvaram, kas ļautu uzņēmumam saprast, kādi ir konkrētie procesi, kas tiek pakļauti IT drošības riskiem. Šāda veida labās prakses novērtēšana ļautu uzņēmumam noteikt, kādas ir konkrētās darbības, kurām ir nepieciešams pievērst uzmanību.

2.5 Atbilstību vērtējuma noteikšana ITIL vadlīniju prasībām

Pētījuma laikā tika apzinātas ITIL prasības, kuras uzņēmumam ir jāievēro, lai būtu nodrošināta IT pārvaldība. Tika veikta esošās situācijas analīze attiecībā pret IT pārvaldības prasībām. Esošās situācijas apzināšanā tika izskatīta uzņēmuma saistītā dokumentācija un veiktas sarunas ar atbildīgajiem darbiniekiem. Esošā situācija uzņēmumā tika salīdzināta ar prasībām, kas tika identificētas ITIL ietvarā, rezultātā identificējot atbilstības, daļējas atbilstības vai neatbilstības uzņēmuma IT pārvaldības procesos. Gala rezultātā darba autors sniedz rekomendācijas identificēto neatbilstību novēršanai vai to radīto risku mazināšanai, lai uzņēmumam būtu iespēja veikt uzlabojumus esošajā IT pārvaldībā. Aprakstītā darba novērtēšanas plāns ir parādīts attēlā 2.3. [5]



2.3. attēls **ITIL ietvara novērtēšanas plāns**

2.6 IT drošības pārvaldības novērtēšana pret ITIL vadlīnijām

Tabulā 2.2 tiek aprakstīts IT drošības pārvaldības novērtējums, par pamatu izmantojot ITIL ietvaru. Tajā tiek ietverts kontroles nosaukums, novērojumi (sadaļā tiek aprakstīts identificētais novērojums), kā arī kontroļu atbilstība ITIL ietvaram" (1 – nav atbilstoši prasībai un 2 - daļēji atbilstoši prasībai; 3 – pilnībā atbilstoši prasībai. Drošības novērtējuma ietvaros darba autors veica sarunas ar atbildīgajiem darbiniekiem un analizēja pieejamo dokumentāciju.

2.2.tabula

IT drošības novērtējums pret ITIL standarta prasībām

Kontroles nosaukums	**Novērojumi**	**Atbilstība**
1.Pakalpojumu stratēģija		
1.1.IT pakalpojumu stratēģijas pārvaldība	Tika identificēts, ka tiek veikts neformāls stratēģiskais pakalpojumu novērtējums.	2
1.2.IT pakalpojumu portfeļa pārvaldība	Interviju laikā netika identificēti apstākļi, ka jauniem vai mainītiem pakalpojumiem netiktu definēti vēlamie rezultāti.	3
1.3.IT finanšu pārvaldība	Sarunas laikā tika identificēts, ka tiek iesniegti formāli pieprasījumi izmaiņu pārvaldībai.	1

Kontroles nosaukums	Novērojumi	Atbilstība
1.4.Pieprasījumu pārvaldība	Sarunas laikā ar atbildīgajiem darbiniekiem netika identificēti apstākļi, ka pakalpojumi netiktu regulāri pārskatīti.	3
1.5.Biznesa attiecību pārvaldība	Tā kā sarunas laikā tika identificēts, ka netiek saņemtas atsauksmes par IT departamenta sniegtajiem pakalpojumiem, to apstrāde nevar tikt pārbaudīta.	2
2.Pakalpojumu projektēšana		
2.1.Projektēšanas koordinācija	Sarunu laikā tika identificēts, ka neformāli tiek koordināti un noteikti pakalpojumu projektēšanas resursi un iespējas.	2
2.2.Pakalpojumu kataloga pārvaldība	Tika identificēts, ka nav izstrādāts pakalpojumu katalogs darbības nepārtrauktības plāna procedūra.	1
2.3.Pakalpojumu līmeņa pārvaldība	Sarunu laikā tika identificēts, ka neformāli tiek definēti rezultāti jauniem pakalpojumiem vai lielām izmaiņām.	1
2.4.Risku pārvaldība	Novērtēšanas laikā darba autors identificēja, ka sistēmai nav veikta risku analīze un attiecīgi izstrādāts risku novēršanas plāns	2
2.5.Resursu ietilpības pārvaldība	Netika identificēti apstākļi, ka biznesa vajadzības un plāni netiktu izteikti pakalpojumu un IT infrastruktūras kapacitātes un veiktspējas prasībās.	3
2.6.Pieejamības pārvaldība	Pārbaudes laikā tika identificēts, ka no IT departamenta puses faktiskā informācija par pieejamību netiek noteikta un analizēta, kā arī biznesa puse formāli nav noteikusi tai nepieciešamos pieejamības laikus.	2
2.7.IT pakalpojumu nepārtrauktības pārvaldība	Pārbaudes laikā tika identificēts, ka nav izstrādāta procedūra saistībā ar IT pakalpojumu nepārtrauktības nodrošināšanu.	3
2.8.Informācijas drošības pārvaldība	Nav formāli noteiktas IT speciālistu lomas un atbildības.	2
2.9.Atbilstības pārvaldība	Sarunu laikā netika identificēti apstākļi, ka netiktu	3

2.2. tabulas 2. turpinājums

Kontroles nosaukums	Novērojumi	Atbilstība
	nodrošināts, ka IT pakalpojumi, procesi un sistēmas ir atbilstošas uzņēmuma politikām un prasībām, kā arī ikgadēji tiek pasūtīts ārējo pakalpojumu sniedzēju nodrošināts IT audits, kura laikā tiek pārskatīti procesi, sistēmās un dokumentācija.	
2.10.Arhitektūras pārvaldība	Pārbaudes laikā tika identificēts, ka nav definēta vīzija turpmākajai tehnoloģiskajai attīstībai, balstoties uz pakalpojumu stratēģiju un jaunajām pieejamām tehnoloģijām.	2
2.11.Piegādātāju pārvaldība	Sarunu laikā netika identificēti apstākļi, ka nav izstrādāta piegādātāju stratēģija, kas sniedz norādījumus un standartus produktu un pakalpojumu iepirkumiem.	3
3.Pakalpojumu restrukturizācija		
3.1.Izmaiņu pārvaldība	Pārbaudes laikā tika identificēts, ka uzņēmuma ietvaros nav definētas ārkārtas izmaiņas, līdz ar to nevar tikt secināts, vai tās tiek novērtētas, autorizētas un ieviestas iespējami īsā laika periodā.	2
3.2.Izmaiņu novērtēšana	Sarunu laikā netika identificēti apstākļi, ka būtiskas izmaiņas netiktu novērtētas to ierosināšanas fāzē pirms tās tiek virzītas uz izmaiņu plānošanas fāzi. No atbildīgo personu puses tika uzsvērts, ka būtiskas izmaiņas tiek diskutētas valdes sēdēs.	3
3.3.Projektu pārvaldība (pārejas plānošana un atbalsts)	Interviju laikā tika identificēts, ka tiek izmantots divu plašāk izmantoto projektu vadības metožu – ūdenskrituma un *agile* – pamatprincipi.	2
3.4.Lietojumprogrammu izstrāde	Interviju laikā netika identificēti apstākļi, ka netiktu nodrošināts, ka lietojumprogrammas un sistēmas, kas nodrošina nepieciešamo funkcionalitāti IT pakalpojumiem, ir pieejamas.	3

2.2. tabulas 3. turpinājums

Kontroles nosaukums	Novērojumi	Atbilstība
3.5.Versionēšanas un uzstādīšanas pārvaldība	Interviju laikā netika identificēti apstākļi, ka netiktu nodrošinātas vadlīnijas un atbalsts versiju uzstādīšanai	3
3.6.Pakalpojumu validācija un testēšana	Interviju laikā netika identificēti apstākļi, ka nav detalizēti noteikts, kā versiju materiāli tiks testēti un veikta kvalitātes nodrošināšana. Tiek definēts testēšanas koncepts un noteikti testa scenāriji, kas tiks izmantoti pakalpojumu validācijai.	3
3.7.Pakalpojumu konfigurācijas pārvaldība	Interviju laikā netika identificēti apstākļi, ka nebūtu definēta un uzturēta pamatā esošā konfigurācijas modeļa struktūra ar mērķi saglabāt visu informāciju par konfigurācijas vienumiem.	3
3.8.Zināšanu pārvaldība	Tika identificēts, ka nav izstrādāts un ieviests dokumentēts uzņēmuma IT departamenta zināšanu katalogs, kurā varētu vākt, analizēt un uzglabāt materiālus.	2
4.Pakalpojumu darbība		
4.1.Notikumu pārvaldība	Interviju laikā netika identificēti apstākļi, ka netiktu izveidoti un uzturēti mehānismi, kas ģenerē nozīmīgus notikumus un efektīvus nosacījumus filtrēšanai un korelācijai.	3
4.2.Incidentu pārvaldība	Pārbaudes laikā tika secināts, ka nav skaidrs, kā rīkoties ar incidentiem.	2
4.3.Pieprasījumu izpilde	Pārbaudes laikā nebija iespēja pārliecināties, ka pieprasījumu ieraksti tiek iesniegti finmāla kvalitātes pārbaudei.	2
4.4.Pieejas tiesību pārvaldība	Pārbaudes laikā tika identificēts, ka nav izstrādāta lietotāju lomu matrica, kā rezultātā visiem lietotājiem nav nodefinētas konkrētas lomas ar konkrētām pieejas tiesībām atbilstoši amatam.	2
4.5.Problēmu pārvaldība	Pārbaudes laikā tika identificēts, ka nav nodefinēta uzņēmuma ietvaros problēmu pārvaldība (kas ir	2

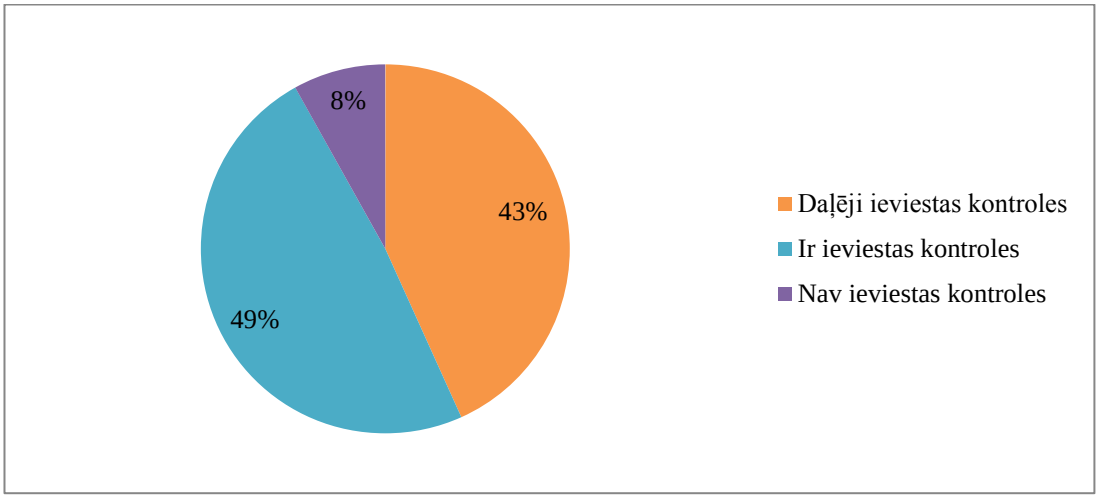
Kontroles nosaukums	**Novērojumi**	**Atbilstība**
	problēma, kad incidents kļūst par problēmu, kā rīkoties situācijās u.tml.).	
4.6.IT darbību kontrole	Pārbaudes laikā tika identificēts, ka IT pakalpojumi un tos atbalstošā infrastruktūra tiek pārraudzīta un kontrolēta, tai skaitā dublējumkopiju un atjaunošanas aktivitātes, rutīnas uzturēšana u.tml.	3
4.7.Iekārtu pārvaldība	Pārbaudes laikā netika identificēti apstākļi, ka vide, kurā atrodas IT infrastruktūra, netiktu atbilstoši pārvaldīta.	3
4.8.Lietojumprogrammu pārvaldība	Pārbaudes laikā tika identificēts, ka tiek veikta lietojumprogrammatūras pārvaldība visos tās dzīves cikla posmos, tomēr tika identificētas dažas nepilnības: Netiek veikta koda pārskatīšana no drošības viedokļa; Koda pārskatīšanai netiek piemērots neviens no starptautiski atzītām vadlīnijām (piem., OWASP *Code Review Guide*); Uzņēmuma ietvaros lietojumprogrammatūras testēšanu veic izmaiņu pieprasītāji un biznesa analītiķi, nav IT testētāji; Lietojumprogrammatūras izstrādes ietvaros netiek izmantoti automātiski testēšanas rīki.	2
4.9.Tehniskā pārvaldība	Pārbaudes laikā tika identificēts, ka tiek nodrošinātas tehniskās zināšanas un atbalsts attiecībā uz IT infrastruktūras pārvaldīšanu.	3
5.Nepārtraukta pakalpojumu uzlabošana		
5.1.Pakalpojumu pārskatīšana	Pārbaudes laikā tika identificēts (kā arī pats audits tika veikts ar šādu mērķi), ka biznesa pakalpojumi	3

2.2. tabulas 5. turpinājums

Kontroles nosaukums	Novērojumi	Atbilstība
	un infrastruktūras pakalpojumi tiek regulāri pārskatīti ar mērķi uzlabot pakalpojumu kvalitāti, kur tas ir nepieciešams, un atrastu ekonomiski izdevīgākos veidus, kā nodrošināt pakalpojumu, kur tas iespējams.	
5.2.Procesu novērtēšana	Pārbaužu laikā tika noskaidrots, ka netiek veikti procesu auditi ar mērķi sertificēt procesu atbilstību ar konkrētu standartu prasībām un šādi auditi arī netiek plānoti.	2
5.3.Nepārtrauktas pakalpojumu uzlabošanas iniciatīvas definīcija	Interviju lakā netika identificēti apstākļi, ka netiktu definētas konkrētas iniciatīvas ar mērķi uzlabot pakalpojumus un procesus.	3
5.4.Nepārtrauktas pakalpojumu uzlabošanas iniciatīvas pārraudzība	Interviju laikā netika identificēti apstākļi, ka netiktu pārbaudīts, ka uzlabošanas iniciatīvas tiek izpildītas atbilstoši plānam.	3

Pēc veiktajiem novērojumiem tika noskaidrots, ka uzņēmumā nav ieviestas visas ITIL ietvarā minētās prasības, kas saistītas ar uzņēmuma pakalpojumiem un finansēm. Uzņēmuma IT drošības pārvaldības galvenās nepilnības ir saistītas ar to, ka nav izstrādāts darbības nepārtrauktības plāna pakalpojuma katalogs, neformāli tiek definēti rezultāti jauniem pakalpojumiem vai lielām izmaiņām, kā arī tiek iesniegti formāli pieprasījumi izmaiņu pārvaldībai.

Apkopojot uzņēmuma IT drošības pārvaldības atbilstību (izmantojot metodoloģiju, kas pievienota pielikumā Nr.2) pret 37 ITIL ietvarā aprakstītajām kontrolēm uzņēmumā tika noskaidrots, ka uzņēmuma IT kontroles ir ieviestas 18 ietvarā aprakstītajām kontrolēm jeb 49% gadījumu. Uzņēmuma IT drošības pārvaldībā daļēji ir ieviestas 16 ITIL ietvarā aprakstītās kontroles jeb 43% gadījumu, taču nav ieviestas 3 ITIL prasības jeb 8% gadījumu. Skatīt attēlu 2.4.



2.4. attēls **Apkopojums par atbilstību ITIL ietvaram**

3. IT RISKU ANALĪZE UN IETEIKUMI

3.1 IT pārvaldības risku analīze

Uzņēmuma riski tiek apzināti, lai noteiktu, kuri ir uzņēmuma vājie punkti un būtu iespējams noteikt kāda ir šo risku ietekme uz uzņēmuma darbību. Risku pārvaldības metodika tiek balstīta uz starptautisko projektu vadības metodoloģiju PRINCE2, kurā, pamatojoties uz novērtējuma laikā identificētajiem riskiem, tiek veikta analīze (skat. tabulu 3.1). Riska apraksts veidots ņemot vērā iepriekš identificētās problēmas uzņēmuma IT drošības pārvaldībā. Lai būtu iespējams noteikt šī riska iedarbību, tiks izmantota ietekmes un varbūtības matrica, kuru ir iespējams aplūkot Pielikumā Nr.3. Pēc iespējamo risku analīzes izvērtēšanas tiek sniegtas rekomendācijas riska novēršanas aktivitātēm, kā arī noteiktas atbildīgās personas, kas šo risku pārvalda. [17]

3.1.tabula

IT drošības pārvaldības riski un to novēršanas aktivitātes

Riska apraksts	**Ietekme**	**Varbūtība**	**Riska līmenis**	**Novēršanas aktivitāte**	**Atbildīgais**
1.Pastāv risks, ka uzņēmuma aktīvu nepareizas izmantošanas dēļ var tikt nodarīti zaudējumi uzņēmumam	1	1	Ļoti zems	Ieviest aktīvu lietošanas noteikumus uzņēmumā un iekļaut tematiku darbinieku apmācībās.	IT drošības pārvaldnieks
2.Pastāv risks, ka nepareizas zibatmiņas lietošanas rezultātā var tikt inficēts iekšējais tīkls	3	2	Augsts	Noteikt zibatmiņu lietošanas noteikumus iekšējā drošības politikā.	IT drošības pārvaldnieks
3.Pastāv risks, ka neuzmanīgi atbrīvojoties no datu nesējiem tiek	2	1	Zems	Noteikt zibatmiņu lietošanas noteikumus iekšējā drošības politikā.	IT drošības pārvaldnieks

3.1. tabulas 1. turpinājums

Riska apraksts	Ietekme	Varbūtība	Riska līmenis	Novēršanas aktivitāte	Atbildīgais
pakļauta riskam uzņēmuma informācija					
4.Paroļu pārvaldīšanas sistēmas neesamība rada risku, ka ir iespējams vieglāk piekļūt informācijas resursiem	2	1	Zems	Jāievieš paroles pārvaldības nosacījumi izmantojot labās prakses ieteikumus.	IT administrators
4.Uzņēmuma fiziskās piekļuves iespējas rada drošības risku, ka neautorizēta persona var piekļūt datiem.	2	1	Zems	Nepieciešams ieviest stingrākas kontroles fiziskās pieejas pārvaldībai.	IT drošības pārvaldnieks
5.Netiek uzraudzīti pieslēgšanās mēģinājumi sistēmām, kas rada iespējas uzbrucējiem ielauzties sistēmā.	2	2	Vidējs	Visiem pieslēgšanās gadījumiem jābūt reģistrētiem auditācijas p	IT administrators
6.Uzņēmumā nav incidentu pārvaldības plāns, kā arī incidenti netiek uzskaitīti, radot risku, ka	2	1	Zems	Nepieciešams ieviest incidentu reģistru un jāaplūko dažādi scenāriji no kuriem jāatjauno IT infrastruktūra, kā arī	IT drošības pārvaldnieks

3.1. tabulas 2. turpinājums

Riska apraksts	Ietekme	Varbūtība	Riska līmenis	Novēršanas aktivitāte	Atbildīgais
uzņēmuma darbinieki var pieņemt nepareizus lēmumus.				jāizveido incidentu pārvaldības plānu.	
7.Publiski pieejamais serveris nav nodalīts no pārējās infrastruktūras radot risku, ka tas tiek apdraudēts no ārpuses.	3	2	Augsts	Uzņēmumam nepieciešams glabāt iekšējo informāciju citviet, tādējādi neatklājot uzbrucējam galveno serveri.	IT drošības pārvaldnieks
8.Nav noteiktas kriptogrāfijas vadlīnijas uzņēmumā radot risku, ka tiek nepareizi pārvaldīta šī funkcija.	1	1	Ļoti zems	Izmantojamiem resursiem jāapraksta kriptogrāfijas izmantošanas kārtība un jāiepazīstina ar to uzņēmuma darbinieki.	IT drošības pārvaldnieks
9.Uzņēmumā nav noteikti formāls nepārtrauktības plāns, radot risku, ka uzņēmuma darbība var tikt pārtraukta.	2	2	Vidējs	Uzņēmumā nepieciešams ieviest darbības nepārtrauktības plānu izanalizējot visus uzņēmumā esošos riskus.	Uzņēmuma vadība

Riska apraksts	Ietekme	Varbūtība	Riska līmenis	Novēršanas aktivitāte	Atbildīgais
10.Uzņēmumā tiek noteikti formāli izmaiņu pieprasījumi, kas rada risku, ka izmaiņas var būtiski mainīt pakalpojumus	1	3	Vidējs	Nepieciešams veidot darba grupas, kuru laikā tiek pārskatīti izmaiņu pieprasījumi.	IT atbalsta dienesta speciālists

3.2 Ieteikumi uzņēmumam

Izrietot no konstatētajām neatbilstībām, pamatojoties uz uzņēmuma novērtēšanu pēc ISO/IEC 27001:2013 standarta un ITIL ietvara un riskiem, kā arī ņemot vērā esošo situāciju, lai uzņēmumā būtu iespējams veikt uzlabojumus IT drošības pārvaldībā, darba autors iesaka:

1. Pārskatīt IT atbildīgo personas lomas un to atbildību;
2. Izstrādāt IT drošības vadlīnijas, ārpakalpojumu pārvaldības, izmaiņu pārvaldības, drošības incidentu pārvaldības procedūras;
3. Pārskatīt ISMS ietvaru (datu glabāšanas vietas, datu apstrādes un pārraides veidus, datu izmantotājus un veidus, kā attiecīgās personas piekļūst datiem);
4. Izveidot biznesa, IT un kiberdrošības risku pārvaldības struktūras;
5. Identificēt aizsargājamos uzņēmuma dārgumus - kritiskos ieņēmumu veidus, biznesa procesus, aktīvus un telpas, noskaidrot, kam ir pieeja tiem;
6. Identificēt apdraudējumus, izvērtēt informācijas drošības riskus;
7. Aktualizēt procedūras, nodrošināt kontroles - datu/notikumu vākšanu, pārvaldību, analīzi, ziņošanu un reaģēšanu uz notikumiem;
8. Plānot un veikt iekšējā un ārējā audita pārbaudes;
9. Pārraudzīt, plānot un veikt neatbilstību novēršanu un ISMS uzlabojumu ieviešanu.

Galvenie uzņēmuma veiktās risku analīzes laikā identificētie trūkumi:

1. Nepareizas zibatmiņas lietošanas rezultātā var tikt inficēts iekšējais tīkls.

2. Netiek uzraudzīti pieslēgšanās mēģinājumi sistēmām, kas rada iespējas uzbrucējiem ielauzties sistēmā.

3. Publiski pieejamais serveris nav nodalīts no pārējās infrastruktūras radot risku, ka tas tiek apdraudēts no ārpuses.

4. Uzņēmumā nav noteikti formāls nepārtrauktības plāns, radot risku, ka uzņēmuma darbība var tikt pārtraukta.

5. Uzņēmumā tiek noteikti formāli izmaiņu pieprasījumi, kas rada risku, ka izmaiņas var būtiski mainīt pakalpojumus

8. SECINĀJUMI UN PRIEKŠLIKUMI

Diplomdarbā "Informāciju tehnoloģiju drošības pārvaldības uzlabošana uzņēmumā" ir aprakstīta uzņēmuma IT drošības pārvaldība un sniegts tās novērtējums pamatojoties uz starptautiskajiem standartiem, kā arī labo praksi, ko ikviens uzņēmums var izmantot IT drošības uzlabošanā. Darba ietvaros tika veikta risku analīze, kas palīdz izprast ar ko uzņēmums riskē nenovēršot nepilnības IT drošības pārvaldībā, kā arī sniedz ieteikumus tālākajām darbībām saistībā ar IT drošības pārvaldības uzlabojumiem.

Veicot uzņēmuma IT drošības pārbaudes un izvērtējot uzņēmumā esošo dokumentāciju, kā arī iegūstot informāciju no uzņēmuma darbiniekiem, var secināt to, ka uzņēmuma IT drošības pārvaldība neatbilst starptautiskajam standartam ISO/IEC 27001:2013, pamatojoties uz to, ka, piemēram, uzņēmumam nav ieviests darbības nepārtrauktības plāns, incidentu apstrādes plāns, kā arī konstatētas citas nepilnības uzņēmuma dokumentācijā. Uzņēmumā netiek nodrošināta atbilstība IT drošības labās prakses ietvaram ITIL(v3) pamatojoties uz to, ka tika konstatētas neatbilstības saistībā ar iekšējām procedūrām, ko nebija ievērojuši uzņēmuma darbinieki.

Veicot uzņēmuma iekšējās darbības izvērtēšanu, pamatojoties uz IT drošības pārvaldības standartiem, kā arī labās prakses vadlīnijām var secināt to, ka uzņēmuma IT drošības novērtēšanai liela nozīme ir pieredzējušam informācijas tehnoloģiju ekspertam no ārpuses, kas pārzina uzņēmuma iekšējos procesus un spēj izprast uzņēmuma iekšējo dokumentāciju, tādējādi spējot veikt kvalitatīvu un izmantojamu IT drošības pārvaldības novērtējumu ar kura palīdzību novērst esošās informācijas drošības neatbilstības.

IT drošības incidenti atstāj ietekmi uz uzņēmuma finansēm, datiem un tēlu, tie ir saistīti ar informācijas integritātes, konfidencialitātes vai pieejamības problēmām. Tāpēc tika veikta risku analīze, lai varētu identificēt riska pakāpi, kā arī sniegt ieteikumus uzņēmumam par to, kuras kontroles nepieciešams ieviest uzņēmumā, lai riski ar augstas pakāpes nozīmi neīstenotos.

Diplomdarbā tika veikts salīdzinājums starp ISO/IEC 27001:2013 standartu, kas aptver uzņēmuma formālo IT drošības pārvaldību, gan arī praktisko IT drošības ITIL(v3) ietvaru, darba ietvaros tika analizēta informācija arī par ISF informācijas drošības labās prakses standartu, COBIT vadlīnijām, kā arī meklēta informācija par saistošo IT drošības pārvaldības dokumentāciju, kas tika ņemta vērā pētnieciskā darba ietvaros.

IZMANTOTĀ LITERATŪRA UN AVOTI

1) Raymond P., 14.09.2016, IT "Security Risk Control Management: An Audit Preparation Plan", Apress, 311.lpp.;

2) Cavusoglu H., Mishra B., Raghunathan S., 01.03.2005, "The Value of Intrusion Detection Systems in Information Technology Security Architecture", 46.lpp.;

3) Sheikhpour R.,Modiri N.,2011., "Mapping Approach of ITIL ServiceManagement Processes to ISO/IEC 27001Controls", 124.lpp.;

4) Ciampa M.,2004, "Security Awareness", Course Technology, 256.lpp.;

5) Calder A., Watkins S., 2012., "IT Governance", Cover Image, 380.lpp.;

6) Sykes M., Landman N., 2013, [tiešsaite] [skatīts 06.04.2017]. Pieejams: http://www.foxit.com/wp-content/uploads/ITIL-and-ISO27001-v3.pdf

7) Cert, IT drošības pārvaldība [tiešsaite] [skatīts 27.03.2017]. Pieejams: https://cert.lv/lv/valsts-un-pasvaldibu-iestadem/it-drosibas-parvaldiba

8) Cert, IT drošības pārvaldības shēma [tiešsaiste] [skatīts 28.03.2017]. Pieejams: https://cert.lv/uploads/Iest%C4%81d%C4%93m/IT_dp_shema20111011web.pdf

9) Fogalin K., 2009., Improving the Management of Information Security in Canadian Government Departments, [tiešsaiste] [skatīts 09.04.2017]. Pieejams: https://www.sans.org/reading-room/whitepapers/leadership/improving-management-information-security-canadian-government-departments-33063

10) Eurostat-Statistics Explained, [tiešsaiste] [skatīts 01.04.2017]. Pieejams: http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises

11) The ISO 27000 Directory, An Introduction To ISO 27001 (ISO27001), [tiešsaite] [skatīts 20.03.2017]. Pieejams: http://www.27000.org/iso-27001.htm

12) ITIL security management, [tiešsaiste] [skatīts 19.03.2017]. Pieejams: https://www.doc-developpement-durable.org/file/Projets-informatiques/cours-&-manuels-informatiques/ITIL/ITIL%20security%20management_Wikipedia-En.pdf

13) Itil service management, [tiešsaiste] [skatīts 07.05.2017]. Pieejams: http://www.itil-service-management-shop.com/

14)Leal. R., 27001 Academy, ISO 27001 vs. ITIL: Similarities and differences, [tiešsaiste] [skatīts 09.05.2017]. Pieejams: https://advisera.com/27001academy/blog/2016/03/07/iso-27001-vs-itil-similarities-and-differences/

15)Security Procedure, Comparison between COBIT, ITIL and ISO 27001, [tiešsaiste] [skatīts 16.05.2017].Pieejams:http://beefchunk.com/documentation/security-management/comparison_between_COBIT_ITIL_and_ISO_27001.pdf

16) SANS Institute InfoSec Reading Room, IT Security Spending Trends, [tiešsaiste] [skatīts 03.04.2017].Pieejams:https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697

17) Probability And Impact Matrix, [tiešsaiste] [skatīts 25.04.2017] Pieejams: http://www.justgetpmp.com/2012/02/probability-and-impact-matrix.html

18) Share of IT budgets spent on IT security 2005-2015, Percentage of total IT budgets spent on IT security from 2005 to 2015, as of February 2016, [tiešsaite] [skatīts 16.05.2017]. Pieejams:https://www.statista.com/statistics/536764/worldwide-it-security-budgets-as-share-of-it-budgets/

19) Bulsuk K., Taking the First Step with the PDCA (Plan-Do-Check-Act) Cycle, 2009.,[tiešsaiste] [skatīts 19.05.2017]. Pieejams: http://www.bulsuk.com/2009/02/taking-first-step-with-pdca.html

20) Aligning CobiT 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit, [tiešsaite] [skatīts 17.04.2017].
Pieejams:http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit_res_Eng_1108.pdf

21) Academy of Economic Studies Bucharest, Information Security Standards, [tiešsaite] [skatīts 02.04.2017].
Pieejams:http://www.jmeds.eu/index.php/jmeds/article/viewFile/Information-Security-Standards/pdf

22) The 2011 Standard of Good Practice for Information Security, 2011., [tiešsaite] [skatīts 09.04.2017]. Pieejams: https://www.uninett.no/webfm_send/730

1. PIELIKUMS

ISO/IEC 27001:2013 salīdzinājuma matrica pret ITIL v3 ietvaru

ISO/IEC 27001:2013 standarts / ITIL ietvars	A5.Drošības politika	A6.Informācijas drošības organizēšana	A7.Drošība attiecībā uz cilvēku resursiem	A8.Aktīvu pārvaldība	A9.Piekļuves kontroles	A10.Vides drošība un fiziskā drošība	A11.Ekspluatācijas drošība	A12.Sakaru drošība	A13Sistēmu iegāde, izstrāde un uzturēšana	A15Piegādātāju saistības	A16Informācijas drošības incidentu pārvaldība
1.Pakalpojumu stratēģija											
1.1.IT pakalpojumu stratēģijas pārvaldība						X					
1.2.IT pakalpojumu portfeļa pārvaldība											
1.3.IT finanšu pārvaldība											
1.4.Pieprasījumu pārvaldība											
1.5.Biznesa attiecību pārvaldība											

2.Pakalpojumu projektēšana											
2.1.Projektēšanas koordinācija											
2.2.Pakalpojumu kataloga pārvaldība		**X**									
2.3.Pakalpojumu līmeņa pārvaldība											
2.4.Risku pārvaldība											
2.5.Resursu ietilpības pārvaldība						**X**					
2.6.Pieejamības pārvaldība						**X**					
2.7.IT pakalpojumu nepārtrauktības pārvaldība		X			**X**	**X**				**X**	
2.8.Informācijas drošības pārvaldība	**X**	**X**				**X**	**X**				
2.9.Atbilstības pārvaldība											
2.10.Arhitektūras pārvaldība		**X**				**X**		**X**			
2.11.Piegādātāju pārvaldība		**X**				**X**		**X**			
3.Pakalpojumu restrukturizācija											
3.1.Izmaiņu pārvaldība		**X**			**X**	**X**	**X**	**X**	**X**		
3.2.Izmaiņu novērtēšana		**X**			**X**	**X**		**X**			

3.3.Projektu pārvaldība (pārejas plānošana un atbalsts)								**X**			
3.4.Lietojumprogrammu izstrāde											
3.5.Versionēšanas un uzstādīšanas pārvaldība						**X**					
3.6.Pakalpojumu validācija un testēšana						**X**		**X**			
3.7.Pakalpojumu konfigurācijas pārvaldība			**X**		**X**	**X**		**X**		**X**	
3.8.Zināšanu pārvaldība											
4.Pakalpojumu darbība											
4.1.Notikumu pārvaldība						**X**					
4.2.Incidentu pārvaldība		**X**			**X**	**X**			**X**		
4.3.Pieprasījumu izpilde											
4.4.Pieejas tiesību pārvaldība		**X**		**X**	**X**		**X**	**X**			
4.5.Problēmu pārvaldība		**X**							**X**		
4.6.IT darbību kontrole											
4.7.Iekārtu pārvaldība											
4.8.Lietojumprogrammu pārvaldība											

4.9.Tehniskā pārvaldība											
5.Nepārtraukta pakalpojumu uzlabošana											
5.1.Pakalpojumu pārskatīšana									**X**		
5.2.Procesu novērtēšana						**X**					
5.3.Nepārtrauktas pakalpojumu uzlabošanas iniciatīvas definīcija		**X**		**X**			**X**				
5.4.Nepārtrauktas pakalpojumu uzlabošanas iniciatīvas pārraudzība		**X**									

2. PIELIKUMS

Atbilstības noteikšanas metodoloģija

Novērtējums	Skaidrojums
3 - Atbilst	Pilnībā ieviestas kontroles
2 - Daļēji atbilst	Daļēji ieviestas kontroles
1 - Neatbilst	Nav ieviestas kontroles
N/A	Nav attiecināms

3. PIELIKUMS

Ietekmes un varbūtības matrica

Ietekme \ Varbūtība	**3 – Augsta**	**2 – Vidēja**	**1 – Zema**
3 – Augsta	9 – Ļoti augsts	6 – Augsts	3 – Vidējs
2 – Vidēja	6 – Augsts	4 – Vidējs	2 – Zems
1 – Zema	3 – Vidējs	2 – Zems	1 – Ļoti zems

DOKUMENTĀRĀ LAPA

Diplomdarbs „Informāciju tehnoloģiju drošības pārvaldības uzlabošana uzņēmumā" izstrādāts LU Biznesa, vadības un ekonomikas fakultātē.

Ar savu parakstu apliecinu, ka pētījums veikts patstāvīgi, izmantoti tikai tajā norādītie informācijas avoti un iesniegtā darba elektroniskā kopija atbilst izdrukai.

Autors: Ernests Pikše _____ __.__.2017

Rekomendēju darbu aizstāvēšanai
Vadītājs: m.b.a., lektora p.i. Kārlis Praudiņš _____ __.__.2017

Recenzents: lektors Ilze Baļčūne _____ __.__.2017

Darbs iesniegts Ekonomikas nodaļā _____
(datums)
Metodiķe: Larisa Staņuka _____

Darbs aizstāvēts Profesionālā bakalaura studiju programmas "E- biznesa un loģistikas vadības sistēmas" Valsts pārbaudījuma komisijas sēdē __.06.2017. prot. Nr. ___

Komisijas sekretāre: M. biz. vad., lektore Kristīne Rozīte _____