

VALSTYBĖS ĮMONĖS CENTRINĖS HIPOTEKOS ĮSTAIGOS INFORMACINIŲ TECHNOLOGIJŲ AUDITO PASLAUGŲ PIRKIMO SUTARTIS

2016 m. ^{Nov 1} d. Nr. F3-5314(2016) / F3-14(2016)
Vilnius

Šią Valstybės įmonės Centrinės hipotekos įstaigos informacinių technologijų audito paslaugų pirkimo sutartį (toliau – Sutartis) sudarė **valstybės įmonė Centrinė hipotekos įstaiga**, atstovaujama direktoriaus Vaido Valikonio, veikiančio pagal valstybės įmonės Centrinės hipotekos įstaigos nuostatus, patvirtintus Lietuvos Respublikos teisingumo ministro 2015 m. rugpjūčio 25 d. įsakymu Nr. 1R-256 „Dėl biudžetinės įstaigos Centrinės hipotekos įstaigos pertvarkymo“, (toliau – Užsakovas) ir **UAB „PricewaterhouseCoopers“, veikianti pagal jungtinės veiklos sutartį su UAB „Blue Bridge“**, atstovaujama Konsultacijų skyriaus vadovo, partnerio Vido Venckaus, veikiančio pagal 2015 m. rugpjūčio 11 d. įgaliojimą, (toliau – Vykdytojas), toliau kartu ar atskirai vadinamos Šalimis.

1. SUTARTIES OBJEKTAS

1.1. Sutarties objektas – valstybės įmonės Centrinės hipotekos įstaigos tvarkomų registrų ir informacinių sistemų informacinių technologijų audito paslaugos (toliau – paslaugos), nurodytos Sutarties 1 priede „Reikalavimai paslaugoms“.

1.2. Vykdytojas įsipareigoja suteikti paslaugas Sutartyje ir jos prieduose numatytomis sąlygomis, o Užsakovas įsipareigoja priimti paslaugas ir sumokėti už jas Sutartyje nustatytomis sąlygomis ir tvarka.

1.3. Paslaugų teikimo vieta – valstybės įmonė Centrinė hipotekos įstaiga, Tilto g. 17, Vilnius.

1.4. Paslaugos pradedamos teikti nuo Sutarties įsigaliojimo dienos ir privalo būti suteiktos ne vėliau kaip per 2 mėnesius nuo Sutarties įsigaliojimo dienos.

2. SUTARTIES KAINA IR APMOKĖJIMO SĄLYGOS

2.1. Sutartyje nurodytų paslaugų kaina – 72 600,00 Eur (septyniasdešimt du tūkstančiai šeši šimtai eurų 0 ct), iš kurių pridėtinės vertės mokestis sudaro 12 600,00 Eur (dvylika tūkstančių šeši šimtai eurų 0 ct).

2.2. Į Sutarties kainą įskaičiuojama paslaugų kaina, visi mokesčiai ir rinkliavos bei kitos išlaidos, susijusios su Sutarties vykdymu.

2.3 Sutarties kaina Sutarties galiojimo laikotarpiu gali būti perskaičiuojama (didinama ar mažinama) pasikeitus (padidėjus ar sumažėjus) pridėtinės vertės mokesčiui, kuris turėjo tiesioginės įtakos Sutarties kainai. Raštiškai susitarus Užsakovui ir Vykdytojui, perskaičiuojama tik ta kainos dalis, kuriai turėjo įtakos pasikeitęs pridėtinės vertės mokestis ir tik pasikeitusio mokesčio dydžiu.

2.4. Už tinkamai suteiktas paslaugas Užsakovas su Vykdytoju atsiskaito mokėjimo pavedimu, pinigų pervesdamas į Vykdytojo sąskaitą ne vėliau kaip per 30 (trisdešimt) kalendorinių dienų nuo Paslaugų suteikimo akto (Sutarties 2 priedas) pasirašymo bei PVM

sąskaitos faktūros gavimo dienos. PVM sąskaita faktūra pateikiama ne vėliau kaip per 5 darbo dienas pasirašius Paslaugų suteikimo aktą.

3. ŠALIŲ ĮSIPAREIGOJIMAI

3.1. Vykdytojas patvirtina, kad yra ir visu šios Sutarties galiojimo metu bus pasirengęs Sutarties pagrindu ir joje nustatyta tvarka bei sąlygomis profesionaliai ir tinkamai suteikti Užsakovui paslaugas.

3.2. Vykdytojas įsipareigoja:

3.2.1. suteikti kokybiškas paslaugas, atitinkančias pasiūlyme ir Sutartyje bei jos 1 priede, taip pat viešojo pirkimo dokumentuose numatytus reikalavimus ir Sutartyje nurodytu terminu;

3.2.2. paslaugas teikti profesionaliai, apdairiai, rūpestingai, saugiai bei siekti išvengti bet kokio galimo interesų konflikto, vadovaudamasis Sutarties nuostatomis, galiojančių teisės aktų reikalavimais bei juose nustatytais apribojimais;

3.2.3. per 3 (tris) darbo dienas nuo Sutarties įsigaliojimo pateikti Projekto valdymo planą, nurodytą Sutarties 1 priede „Reikalavimai paslaugoms“.

3.2.4. suderinti pastabas Projekto valdymo planui ne vėliau kaip per 3 (tris) darbo dienas nuo Užsakovo pastabų pateikimo dienos ir pateikti galutinį Projekto valdymo planą;

3.2.5. nedelsiant pakeisti Sutarties 5 priede nurodytus atsakingus asmenis, jei atsakingi asmenys negali teikti paslaugų dėl objektyvių aplinkybių (laikinas nedarbingumas, darbo santykių pasibaigimas ir kitos priežastys), ir pateikti dokumentus patvirtinančius, kad naujai paskirti atsakingi asmenys atitinka reikalavimus, nustatytus viešojo pirkimo dokumentuose, taip pat naujai paskirtų atsakingų asmenų konfidencialumo pasižadėjimus ir pasižadėjimus saugoti asmens duomenų paslaptis;

3.2.6. nedelsiant, bet ne vėliau kaip iki darbo santykių pasibaigimo dienos, informuoti Užsakovą apie Vykdytojo paskirtų atsakingų asmenų darbo santykių pasibaigimą;

3.2.7. užtikrinti, kad visą Sutarties galiojimo terminą turės pakankamą atsakingų asmenų, atitinkančių pirkimo dokumentų reikalavimus, skaičių ir, kad jo atsakingi asmenys laikysis saugos, konfidencialumo reikalavimų bei neatskleis paslaugų teikimo metu sužinotos konfidencialios informacijos duomenų;

3.2.8. profesionaliai ir sąžiningai vykdyti įsipareigojimus pagal Sutartį;

3.2.9. pateikti parengtą dokumentaciją nurodytą Sutarties 1 priede „Reikalavimai paslaugoms“ Užsakovui derinimui prieš galutinį jos pateikimą ir, esant poreikiui, pataisyti (patobulinti) pagal Užsakovo pastabas ir pasiūlymus;

3.2.10. Užsakovui pateikus pastabas dėl netinkamai suteiktų paslaugų ar pateiktų dokumentų, nedelsiant, bet ne vėliau, kaip per 3 (tris) darbo dienas, ištaisyti Užsakovo nurodytus suteiktų paslaugų trūkumus, atsižvelgdamas į Užsakovo pastabas;

3.2.11. pateikti galutinius paslaugų teikimo rezultatus iki termino, nurodyto Sutarties 1.4 papunktyje, informant paslaugų suteikimą Paslaugų suteikimo aktu, kurį pasirašo Vykdytojas ir Užsakovas;

3.2.12. užtikrinti iš Užsakovo Sutarties vykdymo metu gautos ir su Sutarties vykdymu susijusios informacijos konfidencialumą bei apsaugą.

3.3. Užsakovas įsipareigoja:

3.3.1. suderintais terminais teikti Vykdytojui visą būtiną informaciją, reikalingą tinkamam paslaugų teikimui bei atsakyti į Vykdytojo paklausimus ne vėliau kaip per 5 (penkias) darbo dienas nuo paklausimo gavimo;

3.3.2. ne vėliau kaip per 5 (penkias) darbo dienas nuo Paslaugų suteikimo akto pateikimo, pasirašyti Paslaugų suteikimo aktą arba motyvuotai raštu atsisakyti pasirašyti Paslaugų suteikimo aktą.

3.3.3. sumokėti už kokybiškai ir laiku suteiktas paslaugas Sutartyje nustatyta tvarka.

4. ŠALIŲ ATSAKOMYBĖ

4.1. Už įsipareigojimų, prisiimtų Sutartimi, nevykdymą arba netinkamą vykdymą Šalys atsako Lietuvos Respublikos įstatymų nustatyta tvarka, atsižvelgdamos į Sutartyje nustatytus ypatumus.

4.2. Jei Vykdytojas nevykdo įsipareigojimų, nurodytų Sutarties 3.2.3 – 3.2.7 papunkčiuose Vykdytojas privalo sumokėti baudą, kurios dydis yra 1 (vienas) procentas nuo Sutarties kainos.

4.3. Jei Vykdytojas iki Sutartyje nustatyto termino nesuteikia paslaugų, nurodytų Sutarties 1.1 papunktyje, ir / arba iki Sutartyje nustatyto termino nepateikia audito ataskaitos ar Vykdytojo parengta ir Užsakovui pateikta audito ataskaita neatitinka reikalavimų, nustatytų Sutarties 1 priede „Reikalavimai paslaugoms“, Vykdytojas privalo sumokėti baudą, kurios dydis yra 10 (dešimt) procentų nuo Sutarties kainos.

4.4. Vykdytojas privalo sumokėti baudą per 10 (dešimt) darbo dienų nuo Užsakovo pareikalavimo raštu sumokėti baudą gavimo dienos.

4.5. Jei Užsakovas neatsiskaito su Vykdytoju už tinkamai suteiktas Paslaugas Sutartyje numatytais terminais, Vykdytojas turi teisę be oficialaus įspėjimo ir neribodamas kitų savo teisių gynimo būdų pradėti skaičiuoti 0,02 (dviejų šimtųjų) procento dydžio delspinigius nuo laiku nepervestos Paslaugų kainos už kiekvieną uždelstą dieną, skaičiuojant nuo Sutartyje nustatyto atsiskaitymo laikotarpio pabaigos iki dienos, kai visa reikalinga kaina buvo pervesta.

4.6. Jei Vykdytojas netinkamai vykdo savo sutartinius įsipareigojimus Sutartyje nustatytais terminais ir (arba) tampa akivaizdu, kad Vykdytojas nespės suteikti paslaugų iki Sutarties 1.4 papunktyje nustatyto termino, Užsakovas turi teisę Sutartį vienašališkai nutraukti įspėjęs Vykdytoją raštu prieš 10 (dešimt) darbo dienų, o įsipareigojimus netinkamai vykdęs Vykdytojas įsipareigoja apmokėti visas Užsakovo išlaidas, atsiradusias dėl netinkamo sutartinių įsipareigojimų vykdymo.

4.7. Tuo atveju, kai Užsakovas raštu informuoja Vykdytoją, kad esant nuo Užsakovo nepriklausančioms aplinkybėms, laiku nebus apmokėtos PVM sąskaitos faktūros, Vykdytojas įsipareigoja netaikyti delspinigių ar kitų prievolių įvykdymo užtikrinimo priemonių Užsakovo atžvilgiu.

5. NENUGALIMOS JĖGOS (FORCE MAJEURE) APLINKYBĖS

5.1. Šalis atleidžiama nuo atsakomybės už sutarties neįvykdymą, jeigu ji įrodo, kad sutartis neįvykdyta dėl aplinkybių, kurių ji negalėjo kontroliuoti bei protingai numatyti sutarties sudarymo metu, ir kad negalėjo užkirsti kelio šių aplinkybių ar jų pasekmių atsiradimui.

5.2. Nenugalimos jėgos (*force majeure*) aplinkybės nustatomos pagal Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklės, patvirtintas Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“.

5.3. Šalys apie nenugalimos jėgos aplinkybes praneša viena kitai per 3 (tris) darbo dienas. Jeigu nenugalimos jėgos aplinkybės tęsiasi ilgiau kaip 1 (vieną) mėnesį, bet kuri Šalis, pranešusi raštu prieš 10 (dešimt) darbo dienų, turi teisę nutraukti Sutartį.

6. SUTARTIES GALIOJIMAS

6.1. Sutartis įsigalioja nuo pasirašymo dienos ir galioja iki visiško Šalių įsipareigojimų įvykdymo. Jeigu Sutartis Šalių pasirašoma ne tą pačią dieną, laikoma, kad Sutartis įsigalioja tą dieną, kai ją pasirašo antroji Šalis.

6.2. Jei bet kuri šios Sutarties nuostata tampa ar pripažįstama visiškai ar iš dalies negaliojančia, tai neturi įtakos kitų Sutarties nuostatų galiojimui. Šiuo atveju tokia nuostata turi būti pakeista nuostata, atitinkančia teisės aktų reikalavimus ir kiek įmanoma artimesne Sutarties tikslui bei kitoms jos nuostatom.

6.3. Bet kokios Sutarties nuostatos negaliojimas ar prieštaravimas Lietuvos Respublikos įstatymams ar kitiems norminiams teisės aktams šioje Sutartyje neatleidžia Šalių nuo prisiimtų įsipareigojimų vykdymo.

6.4. Sutartis gali būti nutraukta abiejų Šalių rašytiniu susitarimu.

6.5. Užsakovas turi teisę atsisakyti visų arba dalies paslaugų arba nutraukti Sutartį, įspėjęs Vykdytoją raštu ne vėliau kaip prieš 5 (penkias) darbo dienas.

6.6. Sutarties nutraukimas neatleidžia Šalių nuo pareigos visiškai tarpusavyje atsiskaityti bei padengti kitus įsiskolinimus (pvz., delspinigius, nuostolius).

7. KONFIDENCIALUMAS IR DUOMENŲ SAUGA

7.1. Vykdytojas įsipareigoja laikytis konfidencialumo įsipareigojimų, neatskleisti tretiesiems asmenims jokios informacijos, gautos vykdant Sutartį, išskyrus tiek, kiek tai reikalinga Sutarties vykdymui, o taip pat nenaudoti konfidencialios informacijos asmeniniams ar trečiųjų asmenų poreikiams. Visa Užsakovo Vykdytojui suteikta informacija yra laikoma konfidencialia, nebent Užsakovas raštu patvirtins, kad tam tikra pateikta informacija nėra konfidenciali. Konfidencialia taip pat nėra laikoma informacija, kuri buvo viešai prieinama, arba Vykdytojas gali dokumentais įrodyti, kad informacija jam buvo teisėtai žinoma arba buvo pateikta trečiųjų asmenų, turėjusių raštu patvirtintą teisę atskleisti konfidencialią informaciją.

7.2. Konfidencialia informacija laikoma:

7.2.1 bet koku būdu išreikšta informacija (rašytinė, žodinė, elektroninė ar vizualinė), kuria Šalys apsieičia Sutarties vykdymo metu;

7.2.2. kita informacija, pažymėta kaip konfidenciali ar nors ir nepažymėta, bet pagal savo turinį ir pobūdį laikytina konfidencialia.

7.3. Konfidencialia informacija nelaikoma informacija, kuri:

7.3.1. yra viešai prieinama ar tapo viešai prieinama ne dėl kitos Šalies kaltės, taip pat informacija, kuriai Lietuvos Respublikos teisės aktai suteikia viešosios informacijos statusą;

7.3.2. buvo žinoma Vykdytojui prieš pasirašant Sutartį, ir ta informacija buvo gauta nepažeidžiant Lietuvos Respublikos įstatymų;

7.3.3. nėra laikoma konfidencialia pagal Šalių rašytinį susitarimą.

7.4. Kilus neaiškumui, ar informacija yra konfidenciali, Vykdytojas privalo kreiptis į Užsakovą dėl informacijos pobūdžio nustatymo.

7.5. Vykdytojo paskirti asmenys prieš pradėdami darbus privalo pasirašyti konfidencialumo pasižadėjimus (Sutarties 3 priedas), kuriuos Vykdytojas nedelsiant pateikia Užsakovui.

7.6. Vykdytojas užtikrina, kad Vykdytojo paskirti asmenys, dalyvaujantys Sutarties įgyvendinime, laikysis teisės aktuose numatytų asmens duomenų teisinės apsaugos reikalavimų bei pasirašys pasižadėjimą saugoti asmens duomenų paslaptis (Sutarties 4 priedas) ir įsipareigos saugoti asmens duomenų paslaptis perėjus dirbti į kitas pareigas arba pasibaigus darbo ar sutartiniams santykiams.

7.7. Vykdytojas įsipareigoja įgyvendinti tinkamas (atitinkančias Lietuvos ir Tarptautinių informacijos saugumo valdymo standartų reikalavimus) fizines, technines, programines ir organizacines priemones, skirtas konfidencialiai informacijai apsaugoti.

7.8. Vykdytojas bei jo paskirti asmenys, kurie sužino konfidencialią informaciją, gali ja naudotis tik tuo tikslu, dėl kurio ši informacija buvo atskleista, ir tik tiek, kiek būtina Šalių bendradarbiavimui.

7.9. Vykdytojas naudojasi konfidencialia informacija taip, kad būtų užtikrintas Sutarties įsipareigojimų vykdymas, bei konfidencialia laikomos informacijos saugumas ir neprieinamumas tretiesiems asmenims.

7.10. Jeigu Vykdytojas sužino ar pagrįstai įtaria, kad konfidenciali informacija gali būti atskleista tretiesiems asmenims, jis įsipareigoja imtis visų įmanomų priemonių konfidencialiai informacijai apsaugoti.

7.11. Vykdytojas įsipareigoja nedelsiant pranešti Užsakovui, jeigu sužino arba pagrįstai įtaria, kad konfidenciali informacija buvo neteisėtai atskleista tretiesiems asmenims.

7.12. Nutraukus Sutartį arba įgyvendinus tikslą, dėl kurio konfidenciali informacija buvo atskleista, Vykdytojas privalo sunaikinti visą iš Užsakovo gautą konfidencialią informaciją bei pateikti rašytinį patvirtinimą apie konfidencialios informacijos sunaikinimą nurodant naudotas informacijos naikinimo priemones.

7.13. Vykdytojui draudžiama daryti iš Užsakovo gautos konfidencialios informacijos kopijas.

7.14. Vykdytojas, savo veiksmais ir (arba) neveikimu pažeidęs ir (arba) netinkamai vykdamas konfidencialumo reikalavimus, įsipareigoja nedelsiant, gavęs Užsakovo pretenziją, sumokėti Užsakovui 2000 Eur (dviejų tūkstančių eurų) baudą ir atlyginti visus tiesioginius ir netiesioginius nuostolius, kurie atsiranda dėl Užsakovo Sutartyje numatytų konfidencialumo įsipareigojimų pažeidimo ir (arba) netinkamo vykdymo tiek, kiek nepadengia šiame papunktyje nurodyta baudos suma.

8. SUTARTIES ĮVYKDYMO UŽTIKRINIMAS

8.1. Sutarties įvykdymas privalo būti užtikrintas pateikiant banko garantiją arba draudimo bendrovės laidavimo raštą, kuriame nurodyta suma turi būti ne mažesnė kaip

5 000,00 Eur (penki tūkstančiai eurų, 0 ct). Jeigu Vykdytojas pateikia draudimo bendrovės išduotą sutarties įvykdymą užtikrinantį dokumentą, tai kartu su sutarties įvykdymo laidavimo draudimo raštu Vykdytojas turi pateikti ir pasirašytą draudimo liudijimą (polisą) bei dokumentą, patvirtinantį, kad draudimo įmoka už šį išduotą sutarties įvykdymo laidavimo draudimo raštą yra sumokėta.

8.2. Banko garantija (originalas) arba draudimo bendrovės laidavimo raštas (originalas) turi būti pateikiami ne vėliau kaip per 3 (tris) darbo dienas po Sutarties pasirašymo ir turi galioti ne trumpiau ne trumpiau kaip 30 (trisdešimt) kalendorinių dienų pasibaigus terminui, nurodytam Sutarties 1.4 papunktyje.

8.3. Banko garantija (originalas) arba draudimo bendrovės laidavimo raštas (originalas), Vykdytojui paprašius, grąžinami pasibaigus jų galiojimo laikui arba Vykdytojui tinkamai įvykdžius visus sutartinius įsipareigojimus (priklausomai nuo to, kuris iš nurodytų įvykių bus ankstesnis).

8.4. Sutarties įvykdymo garantija užtikrinama, kad Užsakovui bus atlyginti nuostoliai, atsiradę dėl to, kad Vykdytojas neįvykdė visų sutartinių įsipareigojimų ar vykdė juos netinkamai. Garantija pateikiama ta pačia valiuta, kokia atliekami mokėjimai. Jei Sutarties vykdymo metu garantiją išdavęs juridinis asmuo (garantas) negali įvykdyti savo įsipareigojimų, Užsakovas raštu pareikalauja Vykdytojo per 15 (penkiolika) dienų pateikti naują garantiją tomis pačiomis sąlygomis kaip ir ankstesnioji. Jei Vykdytojas nepateikia naujos garantijos, Užsakovas turi teisę vienašališkai nutraukti Sutartį.

8.5. Jei Vykdytojas nevykdo savo sutartinių įsipareigojimų, Užsakovas pareikalauja sumokėti visas sumas, kurias garantas įsipareigojo sumokėti. Prieš pateikdamas reikalavimą sumokėti pagal Sutarties įvykdymo garantiją, Užsakovas įspėja apie tai Vykdytoją raštu ir nurodo, dėl kokio pažeidimo pateikia šį reikalavimą.

9. KITOS SĄLYGOS

9.1. Sutarčiai aiškinti bei ginčams spręsti taikoma Lietuvos Respublikos teisė.

9.2. Vykdytojas Sutarties vykdymui pasitelkia subteikėją Advokatų kontorą Bukauskas ir partneriai. Sutartyje nurodytą subteikėją galima keisti, jei subteikėjas negali vykdyti Sutartyje numatytų įsipareigojimų (subteikėjo bankroto, likvidavimo, reorganizavimo atveju, subteikėjui praradus teisę teikti paslaugas) arba jei subteikėjas atsisako vykdyti Sutartyje numatytus įsipareigojimus. Vykdytojas pateikia Užsakovui rašytinį prašymą dėl Sutartyje nustatyto subteikėjo keitimo kitu subteikėju, nuroydamas tokio pakeitimo priežastis. Naujas (-i) subteikėjas (-ai) privalo atitikti subteikėjui (-ams) pirkimo, kurio pagrindu pasirašyta ši sutartis, sąlygų 3.10 papunktyje keliamą reikalavimą. Vykdytojas bet koku atveju atsako už visus pagal Sutartį priisiimtus įsipareigojimus, nepaisant to, ar jiems vykdyti bus pasitelkiami tretieji asmenys.

9.3. Visi ginčai, kylantys iš Sutarties, sprendžiami gera valia ir bendru Sutarties šalių sutarimu. Nepavykus ginčo išspręsti derybomis per 30 (trisdešimt) dienų nuo derybų pradžios, bet koks ginčas sprendžiamas Lietuvos Respublikos teismuose. Derybų pradžia laikoma diena, kurią viena iš Sutarties Šalių pateikė prašymą raštu kitai Šaliai su siūlymu pradėti derybas.

9.4. Sutarties sąlygos Sutarties galiojimo laikotarpiu negali būti keičiamos, išskyrus tokias Sutarties sąlygas, kurias pakeitus nebūtų pažeisti Lietuvos Respublikos viešųjų pirkimų įstatyme nustatyti principai ir tikslai ir tokiems Sutarties sąlygų pakeitimams yra gautas Viešųjų pirkimų tarnybos sutikimas.

9.5. Vadovaudamasis Lietuvos Respublikos viešųjų pirkimų įstatymo 18 straipsnio 11 dalimi, Užsakovas ne vėliau kaip per 10 (dešimt) dienų nuo Sutarties sudarymo paskelbia Sutartį ir Vykdytojo pasiūlymą Centrinėje viešųjų pirkimų informacinėje sistemoje. Vykdytojas neprieštaruoja, kad Vykdytojo pasiūlymas ir Sutartis būtų paskelbti teisės aktų nustatyta tvarka.

9.6. Už Sutarties vykdymą atsakingas Užsakovo atstovė, įgaliota pasirašyti Paslaugų suteikimo aktą: Informacinių technologijų departamento Informacinių technologijų plėtros ir priežiūros skyriaus vedėja Vaiva Norvilaitė, tel. (8 5) 231 3610, el. p. vaiva.norvilaitė@hipotekosistaiga.lt.

9.7. Už Sutarties vykdymą atsakingas Vykdytojo atstovas, įgaliotas pasirašyti Paslaugų suteikimo aktą: Konsultacijų skyriaus Vyr. projektų vadovas Audrius Leipus, tel. (8 5) 239 2302, el. p. audrius.leipus@lt.pwc.com.

9.8. Visi Sutarties priedai, pasirašyti Šalių, yra neatskiriama Sutarties dalis:

9.8.1. Sutarties 1 priedas „Reikalavimai paslaugoms“;

9.8.2. Sutarties 2 priedas „Paslaugų suteikimo aktas“;

9.8.3. Sutarties 3 priedas „Konfidencialumo pasižadėjimo forma“;

9.8.4. Sutarties 4 priedas „Pasižadėjimas saugoti asmens duomenų paslaptis“;

9.8.5. Sutarties 5 priedas „Vykdytojo paskirtų atsakingų asmenų sąrašas“.

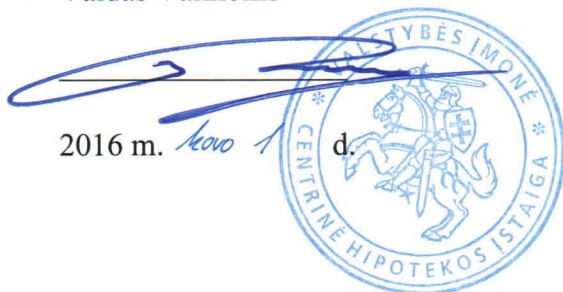
UŽSAKOVAS

Valstybės įmonė Centrinė hipotekos įstaiga

Tilto g. 17 LT-01101 Vilnius
Juridinio asmens kodas 188692535
Tel. (8 5) 231 3490

A. s. LT037300010124633266
„Swedbank“, AB
Banko kodas 73000

Direktorius
Vaidas Valikonis



2016 m. kovo 1 d.

VYKDYTOJAS

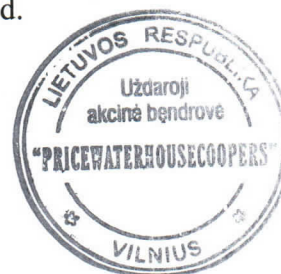
UAB „PricewaterhouseCoopers“, veikianti pagal jungtinės veiklos sutartį su UAB „Blue Bridge“

J. Jasinskio 16B, LT-03163 Vilnius
Juridinio asmens kodas 111473315
PVM mokėtojo kodas LT114733113
Tel. (8 5) 239 2300, faks. (8 5) 239 2301

A. s. LT037400010758123819
Bankas Danske Bank A/S Lietuvos filialas
Banko kodas 74000

Konsultacijų skyriaus vadovas, partneris
Vidas Venckus

2016 m. kovo 1 d. Direktorius
Rimvydas Jogėla



Teisės skyriaus
vyriausiasis specialistas

Edvardas Arštikys
2016-03-01

Teisės skyriaus vedėja

Giedrė Malikėnienė
2016-03-01

Finansų skyriaus vedėja

Vida Šimkūnaitė
2016-03-01

Informacinių technologijų plėtros
ir priežiūros skyriaus vedėja

Vaiva Norvilaitė
2016-03-01

2016 m. kovą 1 d.

Valstybės įmonės Centrinės hipotekos įstaigos
informacinių technologijų audito paslaugų
pirkimo sutarties Nr. F3-14(2016)
1 priedas

REIKALAVIMAI PASLAUGOMS

I BENDROJI INFORMACIJA

1. Pagrindinės valstybės įmonės Centrinės hipotekos įstaigos (toliau – Įmonė) veiklos sritys yra Lietuvos Respublikos hipotekos registro (toliau – Hipotekos registras), Testamentų, Turto arešto aktų, Vedybų sutarčių, Sutarčių, Įgaliojimų, Neveiksnių ir ribotai veiksmų asmenų registru valstybės registru ir Politinių partijų narių sąrašų informacinės sistemos (toliau – Informacinės sistemos, IS) tvarkymas. Hipotekos registras priskiriamas pirmos kategorijos pirmos kategorijos informacinėms sistemoms, o kiti tvarkomi valstybės registrai ir valstybės Politinių partijų narių sąrašų informacinė sistema – antros kategorijos informacinėms sistemoms, vadovaujantis Valstybės informacinių sistemų, registru ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716.

2. Informacinių sistemų valdytoja yra Lietuvos Respublikos teisingumo ministerija.

3. Hipotekos registre registruojamos sutartinės ir priverstinės hipotekos (įkeitimai), hipotekos (įkeitimo) sandoriai, teisės aktų nustatyta tvarka šio registro duomenys renkami, kaupiami, apdorojami, sisteminami, saugomi ir teikiami duomenų gavėjams. Hipotekos registro veiklą reglamentuoja Lietuvos Respublikos hipotekos registro nuostatai, patvirtinti Lietuvos Respublikos Vyriausybės 2001 m. spalio 18 d. nutarimu Nr. 1246 „Dėl Lietuvos Respublikos hipotekos registro nuostatų patvirtinimo“.

4. Testamentų registre registruojami Lietuvos Respublikos teritorijoje sudaryti ir notaro patvirtinti (priimti saugoti) testamentai, užsienio valstybėse sudaryti ir konsulinio pareigūno patvirtinti (priimti saugoti) testamentai, taip pat 1972 m. gegužės 16 d. Konvenciją dėl testamentų registravimo sistemos sukūrimo priėmusiose, ratifikavusiose arba prie jos prisijungusiose užsienio valstybėse sudaryti (priimti saugoti) testamentai, palikimo priėmimo faktai ir palikimo atsisakymo faktai teisės aktų nustatyta tvarka šio registro duomenys renkami, kaupiami, apdorojami, sisteminami, saugomi ir teikiami duomenų gavėjams. Testamentų registro veiklą reglamentuoja Testamentų registro nuostatai, patvirtinti Lietuvos Respublikos Vyriausybės 2001 m. gegužės 22 d. nutarimu Nr. 594 „Dėl Testamentų registro steigimo ir Testamentų registro nuostatų patvirtinimo“.

5. Turto arešto aktų registre registruojami teismų, antstolių, prokurorų, Valstybinės mokesčių inspekcijos prie Finansų ministerijos, kitų valstybės institucijų ir pareigūnų turto arešto aktai, kuriais laikinai priverstinai apribojamos teisės į Lietuvos Respublikoje esantį turtą jį areštuojant, teisės aktų nustatyta tvarka šio registro duomenys renkami, kaupiami, apdorojami, sisteminami, saugomi ir teikiami duomenų gavėjams. Turto arešto aktų registro veiklą reglamentuoja Turto arešto aktų registro nuostatai, patvirtinti Lietuvos Respublikos Vyriausybės 2002 m. kovo 5 d. nutarimu Nr. 314 „Dėl Turto arešto aktų registro nuostatų patvirtinimo“.

6. Vedybų sutarčių registre registruojamos vedybų, sugyventinių sutartys dėl bendrai įgyto ir naudojamo turto padalijimo pasibaigus bendram gyvenimui bei turto padalijimo faktai, teisės aktų nustatyta tvarka šio registro duomenys renkami, kaupiami, apdorojami, sisteminami, saugomi ir teikiami duomenų gavėjams. Vedybų sutarčių registro veiklą reglamentuoja Vedybų sutarčių registro nuostatai, patvirtinti Lietuvos Respublikos Vyriausybės 2002 m. rugpjūčio 13 d. nutarimu Nr. 1284 „Dėl Vedybų sutarčių registro nuostatų patvirtinimo“.

7. Sutarčių registre registruojamos pirkimo-pardavimo išsimokėtinai, kai neregistruojami daiktai įsigyti paslaugoms teikti arba įmonės verslui, pirkimo-pardavimo su atpirkimo teise, kai neregistruojami daiktai perkami paslaugoms teikti arba įmonės verslui, ir lizingo (finansinės nuomos), kurio dalykas yra neregistruojamas daiktas, skirtas naudoti verslo tikslais, sutartys, teisės aktų nustatyta tvarka šio registro duomenys renkami, kaupiami, apdorojami, sisteminami, saugomi ir teikiami duomenų gavėjams. Sutarčių registro veiklą reglamentuoja Sutarčių registro nuostatai, patvirtinti Lietuvos Respublikos Vyriausybės 2002 m. liepos 17 d. nutarimu Nr. 1158 „Dėl Sutarčių registro steigimo ir Sutarčių registro nuostatų patvirtinimo“.

8. Neveiksnių ir ribotai veiksnų asmenų registre registruojami asmenys, kurie teismo tvarka pripažinti neveiksniais tam tikroje srityje, asmenys, kurių civilinis veiksnumas tam tikroje srityje apribotas, nepilnamečiai nuo keturiolikos iki aštuoniolikos metų, kurių teisės savarankiškai disponuoti savo pajamomis ir turtu teismo sprendimu apribotos ar atimtos, globėjai ir rūpintojai, asmenys, sudarę pagalbos priimant sprendimus sutartis, pagalbą priimant sprendimus teikiantys asmenys, sritys, kuriose asmeniui teikiama pagalba priimant sprendimus, asmenų pateikti išankstiniai nurodymai. Teisės aktų nustatyta tvarka šio registro duomenys renkami, kaupiami, apdorojami, sisteminami, saugomi ir teikiami duomenų gavėjams. Neveiksnių ir ribotai veiksnų asmenų registro veiklą reglamentuoja Neveiksnių ir ribotai veiksnų asmenų registro nuostatai, patvirtinti Lietuvos Respublikos Vyriausybės 2010 m. gruodžio 15 d. nutarimu Nr. 1771 „Dėl Neveiksnių ir ribotai veiksnų asmenų registro steigimo ir jo nuostatų patvirtinimo“.

9. Įgaliojimų registre registruojami notarų ir konsulinių pareigūnų patvirtinti įgaliojimai, notarų patvirtintiems prilyginami įgaliojimai, informacinių technologijų priemonėmis sudaryti įgaliojimai, nurodyti Civilinio kodekso 2.139 straipsnio 2 dalyje, teisės aktų nustatyta tvarka šio registro duomenys renkami, kaupiami, apdorojami, sisteminami, saugomi ir teikiami duomenų gavėjams. Įgaliojimų registro veiklą reglamentuoja Įgaliojimų registro nuostatai, patvirtinti Lietuvos Respublikos Vyriausybės 2010 m. gruodžio 15 d. nutarimu Nr. 1770 „Dėl Įgaliojimų registro įsteigimo ir jo nuostatų patvirtinimo“.

10. Politinių partijų narių sąrašų informacinėje sistemoje (toliau – PPNSIS) teisės aktų nustatyta tvarka kaupiami ir teikiami duomenys apie politinių partijų narių sąrašus. Politinių partijų narių sąrašų informacinės sistemos veiklą reglamentuoja Politinių partijų narių sąrašų informacinės sistemos nuostatai, patvirtinti Lietuvos Respublikos teisingumo ministro 2011 m. vasario 22 d. įsakymu Nr. 1R-60 „Dėl Politinių partijų narių sąrašų informacinės sistemos nuostatų patvirtinimo“.

11. Įmonė taip pat tvarko vidaus administravimo informacines sistemas: dokumentų valdymo sistemą „KONTORA“, Darbo užmokesčio apskaitos programą „STEKAS“, buhalterinės apskaitos programą „SAIKAS“, Įmonės interneto svetainę hipotekosistaiga.lt, aktyvių katalogų sistemą „Active Directory“, vaizdo stebėjimo sistemą, Privilegijuotų vartotojų (administratorių) valdymo sistemą, įeigos kontrolės sistemą, patalpų apsaugos signalizacijos sistemą, IP telefonijos sistemą. Šiose sistemose tvarkoma su Įmonės vidaus administravimu susijusi informacija. Šios

sistemos, vadovaujantis Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašu, priskirtinos ketvirtos kategorijos informacinėms sistemoms.

12. Paslaugos turi būti suteiktos ne vėliau, kaip per 2 mėn. nuo Sutarties įsigaliojimo dienos.

II REIKALAVIMAI PASLAUGŲ APIMČIAI

13. Pirkimo objektą sudaro:

13.1. informacinių technologijų auditas:

13.1.1. Informacinių sistemų veiklos ir valdymo vertinimas;

13.1.2. Informacinių sistemų saugos vertinimas.

14. Teikiant paslaugas, turi būti atlikta – duomenų apie Įmonės tvarkomų informacinių sistemų esamą būseną ir valdymą bei saugos užtikrinimą surinkimas, susisteminimas, esamos situacijos analizė ir išvadų pateikimas bei rekomendacijų Įmonei dėl informacinių technologijų išteklių atitikties nustatytiems tikslams, jų valdymo, informacinių sistemų saugos užtikrinimo trumpuoju ir ilguoju periodu pateikimas, parengiant informacinių technologijų audito ataskaitą bei rizikos įvertinimo ataskaitą.

15. Informacinių technologijų audito tikslas:

15.1. įvertinti, ar turimi informaciniai ištekliai tenkina nustatytus tikslus ir veiklos poreikius;

15.2. įvertinti įdiegtų IT sprendimų racionalumą ir optimalumą;

15.3. apibrėžti informacinių sistemų ir IT infrastruktūros gyvavimo ciklo valdymo atitiktį organizacijos uždaviniams;

15.4. apibrėžti ir IT paslaugų valdymo atitiktį organizacijos uždaviniams;

15.5. pasiūlyti Įmonei tinkamas IT valdymo priemones ir būdus;

15.6. įvertinti informacinių sistemų avarinio atkūrimo ir veiklos tęstinumo planų bei taikomų duomenų saugos priemonių tinkamumą, užtikrinant garantuotą savalaikį IT paslaugų teikimo atnaujinimą remiantis Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“, nustatytais reikalavimais informacinių sistemų veiklos atstatymo terminams;

15.7. įvertinti informacinių sistemų informacinių technologijų saugos atitiktį Informacinių technologijų saugos atitikties vertinimo metodikoje nustatyta tvarka bei parengti informacinių technologijų saugos atitikties vertinimo ataskaitą, pastebėtų trūkumų šalinimo planą.

15.8. įvertinti ir apibrėžti duomenų saugos užtikrinimo priemones, kurios garantuotų turimos informacijos konfidencialumą, vientisumą ir prieinamumą;

15.9. parengti konkrečias audito rekomendacijas ir apibrėžti jas įgyvendinantį Įmonės veiksmų planą 3 metams.

16. Turi būti atlikta Įmonės IT veiklų organizavimo ir vykdymo analizė bei IT infrastruktūros fizinė analizė apimties ir panaudojimo aspektais Įmonės veiklos uždaviniams ir

funkcijoms įgyvendinti. Teikiant audito paslaugas, turės būti analizuojami Įmonės informacinių technologijų ištekliai:

16.1. IT veikla ir funkcijos (IT planavimas, administravimas, teikiamos paslaugos, sutarčių kontrolės vertinimas);

16.2. IT bendrieji ištekliai (duomenų centro patalpos, el. maitinimo ir vėdinimo infrastruktūra, duomenų perdavimo tinklai);

16.3. IT techninė įranga (tarnybinės statys, duomenų saugyklos, tinklo infrastruktūra);

16.4. IT programinė įranga (informacinės sistemos, duomenų bazės, sisteminė programinė įranga, operacinės sistemos, virtualios aplinkos);

16.5. IT paslaugos (bendrieji ištekliai, kaip paslauga, techninė ir programinė įranga, jos priežiūra ir palaikymas;

16.6. Apdorojama ir kaupiama informacija ir duomenys.

17. Turi būti įvertintas analizuojamų IT išteklių projektų valdymas, investicijų valdymas, informacinių vertybių ir turto valdymas, duomenų saugos valdymas, paslaugų teikimo valdymas, naudojamų standartų ir technologijų valdymas.

18. Audito apimtyje taip pat turės būti nustatyta Įmonės IT valdymo procesų atitiktis Įmonės veiklos poreikiams bei numatyti reikalingi jų pokyčiai (IT valdymas apima tokius ilgalaikius procesus, kaip kūrimas, tvarkymas, plėtros tikslų nustatymas, jų tvarkymo ir priežiūros organizavimas bei kontrolė ir pan.).

19. Siekiant atlikti IT valdymo būklės palyginimą „kaip yra“ ir „kaip turi būti“ ir pagrįsti reikalingą IT valdymo struktūrą bei vadovybės sprendimus investicijų srityje, audito metu turi būti identifikuoti pagrindiniai Įmonės IT valdymo procesai ir įvertintas jų gebos lygmuo (nevykdomas, vykdomas, valdomas, apibrėžtas, prognozuojamas arba optimizuojamas procesas), kuris apibūdina įvertinimą, ar procesas faktiškai atitinka savo paskirtį ir duoda reikiamų rezultatų.

20. Vertinimui turėtų būti naudojami tokie pagrindiniai gebos lygiai pagal Gebos brandos modelį (angl. *Capability Maturity Model CMM*), kuriuos procesas gali pasiekti:

20.1. 0 – Nevykdomas procesas (angl. *Incomplete Process*). Procesas neįgyvendintas arba nepasiekia jam keliamų tikslų;

20.2. 1 – Vykdomas procesas (angl. *Performed Process*). Vykdamas procesą yra pasiekiami proceso tikslai;

20.3. 2 – Valdomas procesas (angl. *Managed Process*). Vykdomas procesas įgyvendinamas valdomu būdu (planuojant, stebint ir pritaikant), proceso veiklos rezultatai yra sukuriami, kontroliuojami ir palaikomi;

20.4. 3 – Apibrėžtas procesas (angl. *Established Process*). Valdomas procesas įgyvendinamas apibrėžtu būdu ir pasiekia proceso rezultatus.

20.5. 4 – Prognozuojamas procesas (angl. *Predictable Process*). Apibrėžtas procesas vykdomas nustatytose ribose ir pasiekia proceso rezultatus.

20.6. 5 – Optimizuojamas procesas (angl. *Optimising Process*). Prognozuojamas procesas yra nuolatos tobulinamas, kad pasiektų nustatytus esamus ir numatomus veiklos tikslus.

21. Atliekant IT auditą turi būti įvertintos (bet neapsiribojant) šios IT valdymo sritys:

21.1. IT planavimo ir organizavimo srityje:

21.1.1. Pasirinktų IT valdymo metodų ir priemonių veiksmingumas;

21.1.2. IT organizacinė struktūra;

21.1.3. IT strategija;

- 21.1.4. IT tvarkų, standartų ir procedūrų parengimas ir jų laikymasis;
- 21.1.5. IT valdymo atitiktis organizacinei struktūrai ir organizacijos veiklos poreikiams;
- 21.1.6. IT išteklių ir investicijų paskirstymas ir panaudojimas;
- 21.1.7. IT plėtros ir priežiūros paslaugų teikimo ir sutarčių su išoriniais paslaugų teikėjais sudarymo tvarka;
- 21.1.8. Rizikų valdymas;
- 21.1.9. IT veiklos stebėjimo ir nepertraukiamo veikimo užtikrinimo tvarka.
- 21.2. Informacinių sistemų ir IT infrastruktūros gyvavimo ciklo valdymo srityje:
 - 21.2.1. veiklos poreikių nustatymas;
 - 21.2.2. IT projektų valdymo procedūros ir praktika;
 - 21.2.3. periodinė projektų eigos patikra;
 - 21.2.4. informacinių sistemų kokybės užtikrinimas;
 - 21.2.5. informacinių sistemų kūrimo ir testavimo procesai;
 - 21.2.6. pasirengimas diegimui;
 - 21.2.7. duomenų ir sistemų migravimas.
- 21.3. Informacinių sistemų ir IT infrastruktūros priežiūros procesų srityje:
 - 21.3.1. informacinės sistemos tinkamumo vertinimas po diegimo;
 - 21.3.2. periodiniai informacinių sistemų tinkamumo ir modifikavimo poreikių vertinimai;
 - 21.3.3. priežiūros procesai;
 - 21.3.4. informacinių sistemų (ar jų funkcijų) naikinimo procesai;
- 21.4. IT paslaugų teikimo srityje:
 - 21.4.1. paslaugų lygio susitarimų (angl. Service Level Agreement) valdymas;
 - 21.4.2. procesų ir procedūrų valdymas;
 - 21.4.3. duomenų tvarkymas;
 - 21.4.4. informacinės sistemos išteklių naudojimo ir veiklos stebėsenos metodai;
 - 21.4.5. konfigūracijų ir versijų valdymas;
 - 21.4.6. problemų ir incidentų valdymas;
 - 21.4.7. IT infrastruktūros funkcionalumas ir sąrankos valdymas.
- 21.5. Informacinių vertybių apsaugos srityje:
 - 21.5.1. duomenų saugos užtikrinimo tvarkos, procedūros ir parinktos priemonės;
 - 21.5.2. duomenų šifravimo panaudojimas;
 - 21.5.3. loginės prieigos kontrolės įgyvendinimas;
 - 21.5.4. fizinės prieigos kontrolės įgyvendinimas;
 - 21.5.5. aplinkos veiksnių kontrolės įgyvendinimas;
 - 21.5.6. tinklo infrastruktūros saugos priemonės;
 - 21.5.7. konfidencialios informacijos tvarkymo procesai ir procedūros;
- 21.6. Veiklos tęstinumo ir avarinio atkūrimo srityje:
 - 21.6.1. kopijavimo ir atstatymo procesai ir apimtis;
 - 21.6.2. veiklos tęstinumo ir atstatymo planai (angl. BCP – business continuity plan; DRP – disaster recovery plan).
- 22. Vykdytojas turės įvertinti Įmonės tvarkomų registrų ir informacinių sistemų (apimant, bet neapsiribojant):
 - 22.1. taikomąją programinę įrangą, analizuojant:
 - 22.1.1. naudojimo paskirtį;

22.1.2. pagrindines programinės įrangos įgyvendinamas funkcijas;
 22.1.3. įgyvendintą architektūrą (klasifikavimas pagal programinės įrangos architektūros tipus);

22.1.4. plėtros, palaikymo ir licencijavimo būdus;

22.1.5. naudojimo intensyvumą;

22.1.6. plėtros poreikius ir planus.

22.2. Sistemine programine įranga ir programų platformas (operacinės sistemos, taikomųjų programų (aplikacijų) serverių programinė įranga, duomenų bazių (saugyklų) valdymo sistemos, turinio valdymo sistemos, rezervinio kopijavimo sistemos, taikomosios programinės įrangos projektavimo ir kūrimo priemonės, taikomosios programinės įrangos integravimo priemonės (pvz., angl. *Enterprise Service Bus*); veiklos procesų ir darbo sekų modeliavimo ir vykdymo priemonės, žiniatinklio paslaugų (WS) įrankiai ir kt.), analizuojant:

22.2.1. naudojimo paskirtį ir konfigūraciją;

22.2.2. atitiktį techniniams, informacijos saugos poreikiams;

22.2.3. įsigijimo, atnaujinimo ir licencijavimo būdus;

22.2.4. atnaujinimo poreikius ir planus.

22.3. IT infrastruktūros techninę įrangą (tarnybinės stotys ir jose veikiantys virtualūs serveriai, duomenų saugyklos, diskų masyvai, juostiniai įrenginiai, nepertraukiamo maitinimo šaltiniai ir kt.) analizuojant:

22.3.1. pagrindines technines charakteristikas;

22.3.2. resursų panaudojimo lygį – intensyvumą;

22.3.3. eksploatacijos ir palaikymo sąlygas ir būdus;

22.3.4. funkcijas ir roles (gamybinės / vystymo / testavimo aplinkos, valdymo / palaikymo / veiklos funkcijos).

22.4. duomenų centrus (buvimo vieta, patalpos, plotai; įrengimas ir techninės sąlygos – aušinimo, elektros energijos tiekimo, rezervinio elektros energijos tiekimo, priešgaisrinės apsaugos, fizinės saugos ir veikimo tęstinumo, valdymo ir stebėsenos sąlygos; Įmonės globalus tinklas (uždaras, žinybinis/ atviras); rezervinio kopijavimo ir veiklos tęstinumo užtikrinimo įranga) analizuojant:

22.4.1. atitiktį techniniams, informacijos saugos poreikiams;

22.4.2. priežiūros ir eksploatacijos būdus ir atsakomybes;

22.4.3. naujumą ir modernumą;

22.4.4. modernizavimo ir plėtros poreikius bei planavimą;

22.4.5. galimybes plėsti ir/ar talpinti papildomus infrastruktūros išteklius.

22.5. esamą rezervinio kopijavimo sprendimą (įrankiai, konfigūracijos, duomenų kiekiai, procesai). Informacinių sistemų, duomenų bazių, sisteminės programinės įrangos, operacinių sistemų ir virtualių aplinkų funkcionalumo užtikrinimo reikalavimus, duomenų atsarginio kopijavimo ir atstatymo, avarinio atstatymo procesus bei informacinių sistemų saugos reikalavimų įgyvendinimą, RTO – maksimalų galimą duomenų atkūrimo laiką, RPO – maksimalų galimą duomenų praradimo laiką (angl. RTO - *recovery time objective*, RPO – *recovery point objective*).

22.6. infrastruktūros paslaugas ir poreikius joms (duomenų bazės, elektroninis paštas, vartotojų autentifikavimas, saugos užtikrinimas, IS veikimo ir funkcionalumo užtikrinimas).

22.7. IT išteklių naudojimo poreikius: duomenų kiekius ir srautus, vartotojų skaičiaus augimą, paslaugų lygio susitarimus, paslaugų pasiekiamumo lygius ir su tuo susijusius poreikius, naujas planuojamas paslaugas, ir/ar informacinės sistemas.

22.8. IT administravimo, apsaugos ir kontrolės sistemas, naudojamus standartus, tvarkas ir praktiką, informacinės sistemos procedūras ir naudotojui suteikiamas procesų valdymo priemonės.

22.9. IT organizacinę struktūrą, strateginio planavimo ir valdymo dokumentus, IT vystymo, įgyvendinimo ir priežiūros standartus bei procedūras.

22.10. naudojamus IS kūrimo metodus ir praktiką, projektų valdymo tvarką, IT paslaugų teikėjų parinkimą ir IT sutarčių vykdymo tvarką.

22.11. esamą paslaugų lygio valdymo praktiką ir susitarimus dėl paslaugų teikimo lygio, kuriuose apibrėžti konkretūs IT paslaugų lygio rodikliai.

22.12. saugos kontrolės ir saugos didinimo metodų taikymą, saugos incidentų registravimo ir apdorojimo procesus.

22.13. IS naudotojų loginės ir fizinės prieigos kontrolės būdus ir priemones, perimetro ir IS naudojamas duomenų apsaugos priemonės ir sprendimus.

22.14. konfidencialios informacijos saugojimo, atkūrimo, perdavimo ir naudojimo tvarką ir būdus.

23. Vertinant IT saugą turi būti atlikta:

23.1. Informacinių sistemų saugos atitikties standartams LST ISO/IEC 27001:2014, LST ISO/IEC 27002:2013 vertinimas. Šis vertinimas turi apimti (tačiau neapsiribojant):

23.1.1. esamos informacijos saugos valdymo sistemos atitikties standartų LST ISO/IEC 27001:2014, LST ISO/IEC 27002:2013 reikalavimams vertinimą pagal žemiau pateiktas sritis. Informacijos saugos politika. Šios srities vertinimas turi apimti informacijos saugos politikos, tikslų, procesų ir procedūrų, susijusių su rizikos mažinimu ir informacijos saugos didinimu, peržiūrą ir atitikimo šiam standartui vertinimą. Taip pat turi būti išanalizuotas ir įvertintas informacijos saugos politikos taikymas praktikoje patikrinant, ar ji yra nuolat atnaujinama pagal jos panaudojimo veikloje stebėjimo rezultatus.

23.1.2. informacijos saugos organizavimo vertinimą, apimant žemiau pateiktų informacijos saugos valdymo veiklų vertinimą:

- 23.1.2.1. vadovybės įsitraukimas į informacijos saugos valdymo veiklą;
- 23.1.2.2. atsakomybės už informacijos saugos valdymo veiklas paskirstymas;
- 23.1.2.3. atsakomybės už informacijos saugos valdymo veiklas aprašymas;
- 23.1.2.4. naujų taikomųjų sistemų priėmimas naudojimui;
- 23.1.2.5. konfidencialumo susitarimų naudojimas praktikoje;
- 23.1.2.6. bendradarbiavimas su interesų grupėmis;
- 23.1.2.7. informacijos saugos valdymo nepriklausomos peržiūros;
- 23.1.2.8. informacijos saugos rizikos, susijusios su išorinėmis organizacijomis, valdymas;
- 23.1.2.9. informacijos saugos valdymas, bendraujant su informacinių sistemų naudotojais;
- 23.1.2.10. informacijos saugos reikalavimų įgyvendinimas sutartyse su trečiosiomis šalimis.

23.1.3. turto valdymo ir tvarkymo vertinimas apimant žemiau pateiktų informacijos saugos valdymo veiklų vertinimą:

- 23.1.3.1. valdomo ir tvarkomo turto sąrašo pilnumo užtikrinimas;

23.1.3.2. atsakomybių už turto, naudojamo informacijos apdorojimui ir saugojimui paskirstymas;

23.1.3.3. informacijos apdorojimui skirtu turto naudojimas;

23.1.3.4. informacijos apdorojimui skirtu turto klasifikavimas;

23.1.3.5. informacijos apdorojimui skirtu turto identifikavimas.

23.1.4. žmogiškųjų išteklių saugumo vertinimas, apimant žemiau pateiktą informacijos saugos valdymo veiklą, žmogiškųjų išteklių valdymo srityje, vertinimą trimis aspektais:

23.1.4.1. prieš įsigalint darbo santykiams;

23.1.4.2. darbo santykių galiojimo metu;

23.1.4.3. pasibaigus ar pasikeitus darbo santykiams.

23.1.5. fizinis ir aplinkos saugumo vertinimas, apimant fizinės ir aplinkos saugos vertinimą informacijos saugos kontekste dviem aspektais:

23.1.5.1. tarnybinių stočių patalpų apsauga (pvz., perimetro apsauga, įėjimo apsauga, apsauga nuo išorinių grėsmių ir kt.);

23.1.5.2. priemonės, skirtos apsaugoti nuo įrangos praradimo, sugadinimo ar vagystės.

23.1.6. ryšių ir darbo procedūrų valdymo vertinimas, apimant žemiau pateiktą informacijos saugos valdymo veiklą vertinimą:

23.1.6.1. veiklos procedūrų nustatymas ir atsakomybių paskirstymas;

23.1.6.2. trečiųjų šalių teikiamų paslaugų valdymas;

23.1.6.3. taikomosios programinės įrangos kūrimas, testavimas ir priėmimas naudojimui;

23.1.6.4. apsauga nuo kenksmingos programinės įrangos, siekiant užtikrinti informacinės sistemos ir informacijos konfidencialumą, vientisumą ir prieinamumą;

23.1.6.5. atsarginių kopijų darymas;

23.1.6.6. duomenų perdavimo tinklo apsaugos valdymas;

23.1.6.7. duomenų laikmenų tvarkymas;

23.1.6.8. keitimasis informacija įmonės viduje ir su išorinėmis organizacijomis;

23.1.6.9. neautorizuoto priejimo prie informacijos stebėjimas.

23.1.7. Prieigos valdymo vertinimas apimant, žemiau pateiktą informacijos saugos valdymo veiklą vertinimą:

23.1.7.1. prieigos prie informacijos saugos politika;

23.1.7.2. informacinių sistemų naudotojų prieigos teisių valdymas;

23.1.7.3. apsaugos nuo nesankcionuotos prieigos prie informacijos ir ją apdorojančių informacinių sistemų valdymas;

23.1.7.4. apsaugos nuo nesankcionuotos prieigos prie duomenų perdavimo tinklo resursų valdymas;

23.1.7.5. apsaugos nuo nesankcionuotos prieigos prie operacinių sistemų valdymas;

23.1.7.6. apsaugos nuo nesankcionuotos prieigos prie elektroninės informacijos valdymas;

23.1.7.7. informacijos saugos naudojant mobilius įrenginius valdymas.

23.1.8. Taikomųjų sistemų užsakymo tobulinimo ir priežiūros vertinimas apimant žemiau pateiktą informacijos saugos valdymo veiklą vertinimą:

23.1.8.1. informacijos saugos reikalavimų įgyvendinimas formuluojant reikalavimus naujoms ar esamoms taikomosioms sistemoms;

23.1.8.2. saugus informacijos apdorojimas informacinėje sistemoje;

23.1.8.3. šifravimo metodų naudojimas siekiant užtikrinti informacijos konfidencialumą, vientisumą ir autentiškumą;

23.1.8.4. sisteminių rinkmenų saugumo užtikrinimas;

23.1.8.5. saugumo užtikrinimas kuriant ir prižiūrint taikomas sistemas;

23.1.8.6. techninio pažeidžiamumo valdymas.

23.1.9. Informacijos saugumo incidentų valdymo vertinimas apimant žemiau pateiktą informacijos saugos valdymo veiklų vertinimą:

23.1.9.1. informavimas apie informacinių sistemų saugos pažeidimus ir silpnąsias informacinių sistemų saugos vietas;

23.1.9.2. informacijos saugos incidentų valdymas.

23.1.10. Veiklos tęstinumo valdymo vertinimas apimant informacijos saugos valdymo veiklų, reikalingų užtikrinti informacinių sistemų veikimo nepertraukiamumą, vertinimą:

23.1.10.1. veiklos tęstinumas ir rizikos analizė;

23.1.10.2. veiklos tęstinumo planų tikrinimas, priežiūra ir koregavimas.

23.2. Atitikties nacionaliniams teisės aktams, reglamentuojantiems informacijos saugos valdymą, vertinimas, apimant žemiau pateiktą informacijos saugos valdymo veiklų vertinimą:

23.2.1. atitikimo teisiniams ir sutartiniais informacijos saugos reikalavimams užtikrinimas;

23.2.2. atitikimo informacinių sistemų saugos politikai ir standartams užtikrinimas;

23.2.3. informacinių sistemų saugos audito valdymas;

23.2.4. elektroninėje erdvėje teikiamų paslaugų, atitinkančių elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus, dalie, procentais nustatymas;

23.3. Išorinis informacinės sistemos saugumo vertinimas, kurio apimtyje atliekama:

23.3.1. Išorinio duomenų perdavimo tinklo perimetro patikrinimas (patikrinimas atliekamas turint minimalias žinias apie tikrinamų informacinių sistemų informacinių technologijų infrastruktūrą imituojant potencialaus įsilaužėlio iš interneto veiksmus):

23.3.1.1. informacijos apie tiriamą objektą surinkimas iš viešai prieinamų šaltinių;

23.3.1.2. perimetro tinklo mazgų, pasiekiamų iš interneto, nustatymas;

23.3.1.3. perimetro tinklo mazguose veikiančių serverių ir kitų tinklo įrenginių operacinių sistemų ir programinės įrangos nustatymas ir žinomų pažeidžiamumų patikrinimas;

23.3.1.4. perimetro tinklo mazguose veikiančių servisų nustatymas ir žinomų pažeidžiamumų patikrinimas bei konfigūracijos analizė (papildomos informacijos apie sistemas surinkimas per klaidų, sisteminius pranešimus, servisų programinę realizaciją);

23.3.1.5. nustačius pažeidžiamumus, atliekamas įsilaužimo testas.

23.3.2. Jei aptinkama iš interneto pasiekiamų paslaugų (angl. service), reikalaujančių naudotojo autentifikacijos, tuomet atliekamas išorinės paslaugos slaptažodžių auditas. Tikrinama, ar naudojami patikimi slaptažodžiai, ar įmanoma juos atspėti arba parinkti, ar saugos sistemos pastebi tokius bandymus ir informuoja administratorius, ar imamasi tinkamų reagavimo veiksmų.

23.4. Žiniatinklio taikomųjų programų (5 vnt. www.igaliojimai.lt, <https://registrai.hipotekosistaiga.lt/hisrep2010>, <https://registrai.hipotekosistaiga.lt/etaar/etaar/>, <https://registrai.hipotekosistaiga.lt/trps>, www.hipotekosistaiga.lt) ir žiniatinklio paslaugų saugumo vertinimas, kurio apimtyje:

23.4.1. turi būti patikrintos visos žiniatinklio paslaugos, priklausantys/susiję su aukščiau paminėtomis žiniatinklio taikomosiomis programomis, atlikti įsilaužimų testai.

23.4.2. turi būti atliktas žiniatinklių taikomųjų programų ir žiniatinklio paslaugų saugumo patikrinimas neturint naudotojo prisijungimo:

23.4.2.1. naudojamų technologijų identifikavimas (platforma, programavimo metodai ir priemonės);

23.4.2.2. žiniatinklio paslaugos konfigūracijos patikrinimas (darbinės direktorijos pakeitimas, žiniatinklio paslaugos teisių eskalavimas, informacijos atskleidimas per klaidų pranešimus);

23.4.2.3. pažeidžiamumų paieška (vartotojo autentifikavimo mechanizmo patikrinimas, sesijos vientisumo patikrinimas, įvedamos informacijos apdorojimo patikrinimas, programinio kodo integralumo patikrinimas, klaidų pranešimų apdorojimas, sisteminės informacijos atskleidimas, serviso konfigūravimo klaidos ir pan.) ne mažiau kaip trimis populiariausiais automatizuotais žiniatinklio pažeidžiamumo skeneriais;

23.4.2.4. rankinis automatizuotos paieškos rezultatų patikrinimas;

23.4.2.5. rankinis pažeidžiamumų patikrinimas pagal visus „OWASP Testing Guide“ metodikos punktus, neapsiribojant „OWASP Top 10“ pažeidžiamumais.

23.4.3. Turi būti atliktas žiniatinklio taikomųjų programų ir žiniatinklio paslaugų saugumo patikrinimas prisijungus kaip legalus sistemos naudotojas:

23.4.3.1. serviso konfigūracijos patikrinimas (darbinės direktorijos pakeitimas, serviso teisių eskalavimas, informacijos atskleidimas per klaidų pranešimus ir pan.);

23.4.3.2. tikrinama, ar visų tipų (įskaitant nutolusius naudotojus) nurodytų informacinės sistemos naudotojai negali plėsti savo teisių sistemoje, atlikti veiksmų ir/arba gauti duomenis, nesusijusius su jų tiesioginių pareigų vykdymu;

23.4.3.3. pažeidžiamumų paieška (vartotojo autentifikavimo mechanizmo patikrinimas, sesijos vientisumo patikrinimas, įvedamos informacijos apdorojimo patikrinimas, programinio kodo integralumo patikrinimas, klaidų pranešimų apdorojimas, sisteminės informacijos atskleidimas, serviso konfigūravimo klaidos) ne mažiau kaip trimis populiariausiais automatizuotais žiniatinklio pažeidžiamumo skeneriais;

23.4.3.4. rankinis automatizuotos paieškos rezultatų patikrinimas;

23.4.3.5. rankinis pažeidžiamumų patikrinimas pagal visus „OWASP Testing Guide“ metodikos punktus, neapsiribojant „OWASP Top 10“ pažeidžiamumais.

23.4.4. Sistemos kritinės apkrovos testas. Sistema tikrinama generuojant užklausas iš vienos, nustatytų techninių parametrų tarnybinės stoties ir stebimas atsakymo laikas. Testo tikslas įvertinti tolygiai didinamo užklausų kiekio poveikį sistemos greitaveikai, nesukeliant sistemos darbingumo sutrikdymo.

23.4.5. Saugos sistemų įvykių žurnalų įrašų analizė, tikrinant ar šių įrašų pakanka įsibrovimo bandymams užfiksuoti, įsibrovėliui ir jo panaudotiems įsibrovimo metodams identifikuoti bei įvykiams atkurti. Tikrinama, ar įrašų saugojimo laikas atitinka minimalų informacinei sistemai reikalaujamą įrašų saugojimo laiką.

23.5. Duomenų teikimui naudojamų technologijų saugumo vertinimas, kurio apimtyje:

23.5.1. turi būti išanalizuoti ir ištestuoti visi būdai, naudojami duomenų teikimui automatinio būdu pagal duomenų teikimo sutartis:

23.5.1.1. technologinis duomenų teikimo priemonių ir būdų pažeidžiamumų patikrinimas;

23.5.1.2. duomenų apsaugos algoritmų vertinimas, identifikuojant ar nėra galimybės panaudoti nepakankamai saugius algoritmus ar šifravimo, autentifikavimo raktų ilgius.

23.5.1.3. tipinių įsilaužimo veiksmų, naudojamų informacijos perėmimui, atlikimas;

23.5.1.4. patikrinimas, ar sutarčių šalys negali eskaluoti savo teisių ar pasiekti daugiau informacijos nei joms priklauso pagal susitarimus.

23.5.2. Turi būti pateiktos ekspertinės saugumo konsultantų išvados ir rekomendacijos saugiam technologiniam duomenų teikimui.

23.6. Vidinis informacinės sistemos saugumo vertinimas, kurio apimtyje:

23.6.1. turi būti patikrintos informacinės sistemos tvarkytojų (su institucija suderinta imtis, kuri atspindi visų tipų kompiuterizuotų darbo vietų techninės ir programinės įrangos konfigūracijas, naudojamas operacines sistemas ir taikomąją programinę įrangą) kompiuterizuotos darbo vietos (ne mažiau kaip 10% visų informacinės sistemos naudotojų darbo vietų skaičiaus (turi būti nurodytas tikslus darbo vietų skaičius). Detalesnė informacija turi būti suderinta su institucija projekto plano parengimo metu.

23.6.2. kompiuterizuotų darbo vietų saugumo patikrinimas (naudojant anoniminį/nesankcionuotą prisijungimą ir/arba turint naudotojo prisijungimo duomenis):

23.6.2.1. tikrinamas kompiuterizuotų darbo vietų operacinių sistemų ir jose veikiančių taikomųjų programų atnaujinimo lygis ir ar jos nėra pažeidžiamos remiantis žinomomis saugumo spragomis;

23.6.2.2. tikrinamas, ar kompiuterizuotų darbo vietų operacinėse sistemose, taikomoseiose programose nėra įdiegta galinčių kelti grėsmę nuotoliniu būdu pasiekiamų perteklinių paslaugų.

23.6.2.3. tikrinamas kompiuterizuotų darbo vietų ir jose veikiančių taikomųjų programų konfigūracijos saugumas;

23.6.2.4. tikrinama, ar naudotojai negali plėsti savo teisių sistemoje, atlikti veiksmus ir/arba gauti duomenis, nesusijusius su jų tiesioginių pareigų vykdymu;

23.6.2.5. tikrinama, ar nutolusios darbo vietos prieigos teisės nesudaro prielaidos saugumo incidentui;

23.6.2.6. kiti testai pagal Vykdytojo naudojamą metodologiją.

23.6.3. Duomenų bazių valdymo sistemų patikrinimas:

23.6.3.1. tikrinamas DBVS atnaujinimo lygis ir konfigūracijos saugumas (laisva prieiga, per didelės naudotojų ar programų teisės, galimybė vykdyti sisteminės komandas iš DBVS);

23.6.3.2. tikrinama, ar naudotojai negali eskaluoti savo teisių sistemoje, atlikti veiksmus ir/arba gauti duomenis, nesusijusius su jų tiesioginių pareigų vykdymu;

23.6.3.3. kiti testai pagal Vykdytojo naudojamą metodologiją.

23.6.4. Bendraujant su Įmonės atsakingais darbuotojais nagrinėjama duomenų perdavimo tinklo architektūra saugumo požiūriu.

23.6.5. Remiantis surinkta informacija, patikrinimo metu nustatyta realia padėtimi, geriausiąją praktika ir standartais, įvertinamas vidinio duomenų perdavimo tinklo saugumas.

23.6.6. Patikrinamas informacinių sistemų administratorių, informacinės sistemos saugos įgaliotinio ir kitų atsakingų darbuotojų gebėjimas bendrauti ir bendradarbiauti atakos metu, patikrinant ar institucijos darbuotojai žino su kuo ir kada bendrauti, kaip ir ką informuoti institucijoje ir kada, kokiais atvejais ir kam pranešti apie įvykusį incidentą.

23.6.7. Turi būti atliktas įsilaužimų aptikimo gebėjimų patikrinimas – ar įsilaužimai aptinkami pagal detalumo ir greičio reikalavimus, nustatytus *SANS 20 Critical Security Controls* metodikoje arba lygiavertėje.

23.7. Duomenų perdavimo tinklo įrenginių saugumo vertinimas, kurio apimtyje:

23.7.1. tikrintinų duomenų perdavimo tinklo įrenginių sąrašas turi būti suderintas su institucija projekto valdymo plano parengimo metu.

23.7.2. tikrinama galimybė nukreipti tinklo srautą į auditoriaus kompiuterį ir tokiu būdu perimti konfidencialius duomenis ir/ar slaptažodžius.

23.7.3. Komutatoriams turi būti atlikti šie saugumo testai:

23.7.3.1. aparatinės ir programinės įrangos identifikavimas;

23.7.3.2. komutatoriuje veikiančių paslaugų/tarnybų nustatymas;

23.7.3.3. žinomi įrangos pažeidžiamumai;

23.7.3.4. patikrinta ARP atakų, DHCP atakų, VTP atakų, MAC adresų ir MAC adresų lentelės atakų galimybė;

23.7.3.5. patikrinta STP atakų, DTP atakų, VLAN atakų, CDP atakų, LLDP atakų galimybė;

23.7.3.6. patikrinta 802.1X atakų, HSRP atakų, VRRP atakų galimybė;

23.7.3.7. valdymo kanalų Telnet, SSH, HTTP, HTTPS, Console, Aux, SNMP, TFTP, FTP saugumo patikra;

23.7.4. institucijos pateiktų konfigūracijų patikra ir analizė pagal įrangos gamintojo geriausias praktikas.

23.7.5. Maršrutizatoriams turi būti atlikti šie saugumo testai:

23.7.5.1. aparatinės ir programinės įrangos identifikavimas;

23.7.5.2. maršrutizatoriuje veikiančių paslaugų/tarnybų nustatymas;

23.7.5.3. žinomi įrangos pažeidžiamumai;

23.7.5.4. patikrinta ARP atakų, HSRP atakų, VRRP atakų, CDP atakų, NTP atakų galimybė;

23.7.5.5. patikrintas *Finger* paslaugos pasiekiamumas;

23.7.5.6. patikrinta IP adresų klastojimo galimybė ir maršrutizavimo pagal šaltinio adresus galimybė;

23.7.5.7. dinaminių maršrutizavimo protokolų RIP, EIGRP, OSPF, BGP ir kitų atakų testavimas;

23.7.5.8. valdymo kanalų Telnet, SSH, HTTP, HTTPS, *Console*, *Aux*, SNMP, TFTP, FTP saugumo patikra;

23.7.5.9. institucijos pateiktos konfigūracijos patikra ir analizė pagal įrangos gamintojo geriausias praktikas.

23.7.5.10. Gebėjimas apdoroti įrenginių generuojamų įvykių žurnalus ir įrenginius valdančių administratorių gebėjimas pastebėti atakas.

23.7.6. Atliekami kiti testai pagal Vykdytojo naudojamą metodologiją.

23.8. Elektroninio pašto apsaugos sistemų efektyvumo vertinimas, kurio apimtyje:

23.8.1. Tikrinamos elektroninio pašto laiškų antraštės siekiant gauti papildomą informaciją apie elektroninio pašto ir kitas vidines sistemas.

23.8.2. Tikrinama, ar įmanoma persiųsti elektroninius laiškus su prisegtu priede kenksmingu programiniu kodu.

23.8.3. Tikrinama, ar įmanoma persiųsti elektroninius laiškus su šifruotais priedais.

23.8.4. Tikrinama, ar įmanoma persiųsti elektroninius laiškus su vykdomosiomis bylomis.

23.8.5. Tikrinama, ar įmanoma persiųsti elektroninius laiškus su nuorodomis į Phishing URL ar patalpintą kenksmingą programinį kodą žiniatinklio (angl. web) serveryje.

23.8.6. SMTP serverio saugumo patikrinimas iš išorės.

23.8.7. Atliekami kiti testai pagal Vykdytojo naudojamą metodologiją.

23.9. Informacinės sistemos veiklos atkūrimo po įsilaužimo vertinimas, kurio apimtyje:

23.9.1. Turi būti atliktas informacinės sistemos veiklos atstatymo po įsilaužimo auditas, įvertinant institucijos gebėjimus atkurti informacinės sistemos veiklą per ir po:

23.9.1.1. informacinės sistemos programinio kodo ir duomenų pakeitimo, dalinio ar visiško ištrynimo;

23.9.1.2. elektroninės paslaugos trikdymo atakos (angl. Denial of Service, DOS).

V. REIKALAVIMAI ATASKAITOMS

24. Ataskaitos turi būti rengiamos etapais, pateikiant kiekvieno etapo rezultatus, juos pristatant ir aptariant su Įmonės atsakingais darbuotojais.

25. Vykdytojas audito ataskaitoje turi **susisteminti ir pateikti informaciją** apie IT valdymo bei informacinių sistemų veiklos esamą situaciją ir poreikius, atlikti surinktos informacijos analizę bei įvertinti atotrūkį tarp esamos situacijos ir Įmonės poreikių bei sritį reglamentuojančių teisės aktų, standartų ir „gerosios praktikos“ reikalavimų, (apimant bet neapsiribojant):

25.1. IT infrastruktūros srityje:

25.1.1. IT infrastruktūros bendruosius išteklius;

25.1.2. IT infrastruktūros techninę įrangą;

25.1.3. IT infrastruktūros programinę įrangą;

25.1.4. IT infrastruktūros paslaugas;

25.1.5. IT infrastruktūros konfigūracijų valdymą, plėtros planavimą, našumo ir apkrovos valdymą, IT infrastruktūros funkcionalumo atstatymo valdymą, procesų automatizavimo lygį, kitus stebėjimo ir valdymo įrankius;

25.1.6. informacinių sistemų architektūrą ir ryšius su IT infrastruktūros ištekliais;

25.1.7. informacinių sistemų, duomenų bazių, sisteminės programinės įrangos, operacinių sistemų ir virtualių aplinkų funkcionalumo užtikrinimo reikalavimus, duomenų atsarginio kopijavimo ir atstatymo, avarinio atstatymo procesus, RTO ir RPO;

25.1.8. informacinių sistemų saugos reikalavimų įgyvendinimą;

25.1.9. duomenų saugos stebėjimui ir užtikrinimui skirtą funkcionalumą.

25.2. IT planavimo ir organizavimo srityje:

25.2.1. IT valdymo sistemos veiksmingumą, siekiant nustatyti, ar priimami IT srities sprendimai ir veikla atitinka, organizacijos strateginiams tikslams.

25.2.2. IT organizacinę struktūrą ir žmogiškųjų išteklių (personalo) valdymą, siekiant nustatyti, ar jie palaiko organizacijos strateginius tikslus.

25.2.3. IT strategiją, jos keitimo ir atnaujinimo, pritaikant prie organizacijos strateginių tikslų, tvarką.

25.2.4. IT tvarkas, standartus ir procedūras, jų atitiktį IT strategijai ir teisės aktams bei keitimo ir naudojimo organizacijoje tvarką.

25.2.5. esamos kokybės vadybos sistemos tinkamumą ir efektyvumą, bei jų atitiktį organizacijos strategijai ir tikslams.

25.2.6. IT valdymą ir vykdomą IT valdymo kontrolę, apibrėžiant atitiktį organizacijos tvarkoms, standartams ir procedūroms.

25.2.7. IT resursų panaudojimo ir įsigijimo prioritetus, investicijų apimtis, paskirstymą bei atitiktį organizacijos strategijai ir tikslams.

25.2.8. IT sutarčių sudarymo ir valdymo tvarkas, jų atitiktį organizacijos strategijai ir tikslams.

25.2.9. rizikos valdymo praktiką, nustatant, ar su organizacijos IT susijusi rizika yra tinkamai valdoma.

25.2.10. organizacijos veiklos tęstinumo planą, siekiant nustatyti organizacijos gebėjimą tęsti esminę veiklą, sutrikus IT veikimui.

25.3. Informacinių sistemų gyvavimo ciklo srityje:

25.3.1. informacinių sistemų įsigijimo, kūrimo, priežiūros ir likvidavimo planų bei investicijų atitiktį veiklos tikslams ir poreikiams.

25.3.2. projektų valdymo praktiką siekiant nustatyti, ar yra valdoma rizika ir ar veiklos reikalavimai yra pasiekiami ekonomiškai veiksmingiausiu būdu. Nustatyti, ar projektai vykdomi laikantis planuotų terminų, parengiant dokumentaciją ir darbų būsenos ataskaitas.

25.3.3. informacinių sistemų apibrėžimo, specifikavimo, analizės, projektavimo, kūrimo ir testavimo fazių atitiktį standartams, apibrėžtoms procedūroms ir taikytiniams teisės aktams bei išorės sąsajų reikalavimams.

25.3.4. pasirengimą informacinių sistemų diegimui ir migravimui į gamybinę aplinką siekiant nustatyti, ar atliktos projekte numatytos veiklos, parengtos pateiktys, patenkinti veiklos poreikiai.

25.3.5. IS diegimo projektų rezultatus ir jų vadovybinį vertinimą, įsitikinant ar projektas pasiekė numatytus rezultatus.

25.4. Informacinių sistemų priežiūros srityje:

25.4.1. informacinių sistemų funkcionalumo peržiūras, nustatant jų atitiktį organizacijos tikslams.

25.4.2. paslaugų lygio valdymo praktiką siekiant įvertinti, ar apibrėžtas ir valdomas vidaus ir išorės paslaugų teikėjų teikiamų paslaugų lygis.

25.4.3. išorės paslaugų teikėjų valdymo praktiką, siekiant nustatyti, ar taikoma kontrolė užtikrina tinkamą paslaugų teikimo lygmenį.

25.4.4. sistemos procesus ir sistemos naudotojo įrankius, siekiant nustatyti, ar valdomi pastovūs ir nereguliarūs sistemos procesai.

25.4.5. informacinių sistemų techninę priežiūrą, siekiant nustatyti jos veiksmingumą ir valdymo tvarką;

25.4.6. duomenų administravimo praktiką, duomenų bazių optimizaciją ir integralumą;

25.4.7. informacinės sistemos išteklių naudojimo ir veiklos stebėsenos priemonių pakankamumą.

25.4.8. problemų ir incidentų valdymą siekiant nustatyti, ar įvykiai, problemos ir klaidos yra registruojami, analizuojami ir sprendžiami laiku.

25.4.9. atliekamų konfigūravimo ir programinių pakeitimų versijų valdymo tvarką bei pakeitimų planavimo, dokumentavimo ir atlikimo procesus ir jų laikymąsi.

25.4.10. kopijuojamos informacijos apimtį ir tvarką, atsarginio kopijavimo ir atstatymo galimybes, užtikrinant informacijos prieinamumą.

25.4.11. organizacijos veiklos atkūrimo planą, nustatant, ar pagal jį galimas IT atstatymas, esant kritiniams sutrikimams.

25.5. Informacijos saugos valdymo ir saugos užtikrinimo srityje:

25.5.1. informacijos saugos politiką, standartus ir procedūras, jų išsamumą ir atitiktį visuotinai priimtai praktikai.

25.5.2. loginės saugos užtikrinimo priemonių kūrimą, diegimą ir stebėseną užtikrinant duomenų konfidencialumą, vientisumą ir prieinamumą.

25.5.3. duomenų klasifikavimo, atitinkančio nustatytus saugos reikalavimus įgyvendinimą.

25.5.4. fizinės prieigos ir aplinkos kontrolės priemonių kūrimą, diegimą ir stebėseną.

25.5.5. procesų ir procedūrų, naudojamas saugant, atkuriant perkeltant ir šalinant informaciją, tinkamumą;

25.5.6. technologines saugos užtikrinimo priemones ir jų įgyvendinimo efektyvumą.

25.6. Vertinant Informacijos saugos valdymo sistemos atitiktį LST ISO/IEC 27001:2013, LST ISO/IEC 27002:2014 arba lygiaverčiams standartams audito apimtyje turi būti pateiktas įvertinamas, ar informacijos saugos kontrolės priemonės realizuotos ir yra valdomos pagal minėtų arba lygiaverčių standartų reikalavimus. Vertinimas turi būti detalizuotas pagal kiekvieną šiuose standartuose apibrėžtą informacijos saugos kontrolės priemonę nurodant sritis, kuriose buvo pastebėti trūkumai, ir pateikiant jų aprašymus.

25.7. Informacijos saugos valdymo sistemos atitikties standartams didinimo veiksmų plane turi būti numatyti reikalingi atlikti veiksmai, siekiant padidinti informacijos saugos valdymo sistemos atitikimą standartų reikalavimams bei šiems veiksams atlikti reikalingi ištekčiai arba pagrindimai, kodėl vienas ar kitas reikalavimas nėra taikytinas, taip pat reikalingus atlikti veiksmus siekiant sertifikuoti informacijos saugos valdymo sistemos atitikimą LST ISO/IEC 27001:2013 standartui.

26. IT audito ataskaitą turi sudaryti:

26.1. IT audito atlikimo pagrindas, audito kiekvienos dalies vykdytojai, audito trukmė ir terminai, audituojamas laikotarpis ir kt.;

26.2. tikrintų objektų aprašymas, patikrinimo eiga;

26.3. audituojamo objekto analizė, aplinkos analizė;

26.4. audito metu nustatyti faktai (neatitikimai, trūkumai ir pan.), palyginimas kaip turėtų būti, lyginant su ta padėtimi, kuri yra;

26.5. audito išvados dėl įdiegtų informacinių technologijų sprendimų optimalumo ir atitikties saugos reikalavimams bei jų valdymo:

26.5.1. IT planavimo ir organizavimo srityje,

26.5.2. IT įsigijimo, diegimo ir priežiūros srityje,

26.5.3. IT paslaugų teikimo srityje;

26.5.4. duomenų saugos valdymo ir užtikrinimo srityje (tame tarpe pateiktos informacinių sistemų saugos reikalavimų atitikties vertinimo ir pažeidžiamumų vertinimo ataskaitos).

26.5.5. detalus rekomendacijų aprašymas ilgajam ir trumpajam periodui:

26.5.5.1. siūlomų diegti IT valdymo standartų ir procesų aprašymas;

26.5.5.2. teisinio reglamentavimo pokyčių aprašymas ir reikalingų, taisyklių ar tvarkų sąrašas;

26.5.5.3. organizacinių pokyčių aprašymas;

26.5.5.4. funkcinių IS pokyčių aprašymas;

26.5.5.5. techninių ir technologinių IS pokyčių aprašymas;

26.5.5.6. Rizikos valdymo planas;

26.5.5.7. veiksmų ir priemonių planai metams;

26.5.6. rekomendacijų įgyvendinimo kaštų apimtis ir analizė;

26.5.7. išvados ir rekomendacijų apibendrinimai:

26.5.7.1. vertinimo metu nustatytų faktų įtakos audituojamai veiklai įvertinimas ir išvados;

26.5.7.2. pasiūlymai ir rekomendacijos, kaip ištaisyti neigiamą faktų įtaką, nustatytą audito metu;

26.5.7.3. priedai (prie ataskaitos pridėti eilės tvarka sunumeruoti darbo dokumentai).

27. IT vertinimo metu nustatyti faktai turi būti detalčiai aprašyti nurodant:

27.1.1.1. kriterijus – nurodoma kokiais standartais, priemonėmis arba lūkesčiais remtasi, atliekant įvertinimą ir/arba patikrinimą;

27.1.1.2. būklę – faktinė padėtis, kuri buvo nustatyta tikrinimo metu;

27.1.1.3. priežastis – nurodomos priežastys, kodėl yra skirtumų tarp tos būklės, kokia ji turėtų būti ir faktinės būklės;

27.1.1.4. poveikį – kas atsitinka arba gali atsitikti dėl esamos būklės;

27.1.1.5. rekomendacijas – ką reikėtų daryti, kad situacija pagerėtų.

28. IT vertinimo metu nustatytų silpnų vietų, klaidų ir neatitikimų sąrašas bei siūlomi sprendimai turi būti pagrįsti patiekiamais audito metu surinktais dokumentais ir apklausų protokolais.

29. Audito ataskaitoje turi būti aprašyta siekiama IS valdymo ir veiklos būsena ir reikalingos IS veiklos tęstinumo ir avarinio atstatymo sąlygos bei pateiktos išvados apie atotrūkį tarp esamos situacijos ir siekiamos būsenos.

30. Audito ataskaitoje turi būti pateikti detalūs pasiūlymai dėl IT valdymo veiklų, procesų ir organizacijos vidaus reglamentavimo tobulinimo krypčių, pritaikant juos IT valdymo praktikai ir standartams bei naudotinų priemonių ir jų diegimo tvarkos. IT funkcinės veiklos srityje turi būti pateiktos:

30.1. IT infrastruktūros tobulinimo technologinės rekomendacijos, jų alternatyvos bei veiksmų planas, nurodant atotrūkio tarp esamos situacijos ir poreikių taškus ir sprendimų rekomendacijas atotrūkio mažinimui;

30.2. IS architektūros pokyčių aprašymas, tenkinantis apibendrintus veiklos poreikius ir optimizavimo galimybes bei paslaugų teikimo gerinimo būdus;

30.3. pagrįsti rekomenduojami technologiniai ir funkciniai sprendimai, tenkinantys apibendrintus IS plėtros poreikius;

30.4. IT saugos stebėjimo ir užtikrinimo, bei duomenų apsaugos sprendimų vystymo rekomendacijos trumpuoju ir ilguoju periodu.

31. Audito ataskaitoje turi būti apibrėžti ir siūlomi IT valdymo procesai, pateikiant:

31.1. būtinų IT valdymo procesų ir procedūrų, sąrašą;

31.2. pritaikytų organizacijos poreikiams IT procesų ir procedūrų aprašymus;

31.3. IT valdymo procesų ir procedūrų diegimo ir naudojimo atsakomybių matricos ir organizacinės struktūros pakeitimų rekomendacijos.

31.4. IT valdymo srityje audito ataskaitoje turi būti pateiktos rekomendacijos, kaip trumpuoju (6-12 mėn.) periodu sumažinti atotrūkį tarp esamos situacijos ir Įmonės poreikių, o taip pat dėl IT valdymo tobulinimo bei IS vystymo ilguoju periodu – 3 metų laikotarpiui. Audito ataskaitoje turi būti pateikta IT skiriamų ir numatomų siūlomoms veikloms ir priemonėms diegti finansinių išteklių analizė, išskiriant:

31.5. IT plėtros ir modernizavimo kaštus;

31.6. IT administravimo ir valdymo kaštus;

31.7. IT infrastruktūros palaikymo ir eksploatavimo kaštus;

31.8. Personalo išlaikymo ir kvalifikacijos kėlimo kaštus.

32. Informacinės sistemos saugos reikalavimų atitikties vertinimo srityje turi būti parengta:

32.1. apibendrinta informacijos sistemos saugos reikalavimų atitikties vertinimo ataskaita, nesigilinant į konkrečius pažeidžiamumus ar technines detales, kurioje atspindėtų statistika, tendencijos, bendra saugumo būklė, pavojingiausi pažeidžiamumai, saugumo trūkumai ir prioritetizuotos saugumo gerinimo kryptys, o taip pat turi būti parengta detali technologinių pažeidžiamumų ataskaita techniniams specialistams, kurioje aprašyta:

32.1.1. tikrinti objektai;

32.1.2. tikrinimo tikslai ir testavimo eiga;

32.1.3. visos atakos ir visi saugumo testai, kurie buvo atlikti pagal Vykdytojo naudojamą įsilaužimų testavimo metodologiją.

32.2. Pažeidžiamumų vertinimo ataskaitos rezultatai pateikiami tokia struktūra:

32.2.1. testo numeris ir pavadinimas;

32.2.2. testo/atakos paskirtis, siekiamas tikslas ir trumpas aprašymas;

32.2.3. testo objektai, taikiniai (IP adresai, prievadų numeriai, atakuoti URL parametrai, atakuotų žiniatinklio formų parametrai ir kt.);

32.2.4. testui/ataakai naudoti programiniai/aparatiniai įrankiai ir priemonės;

32.2.5. testo/atakos turinys, parašas, naudoto kenksmingo programinio kodo išeities tekstas, žiniatinklio užklausų parametrų reikšmės ir kt.;

32.2.6. testo rezultatas (sėkmingas, nesėkmingas);

32.2.7. testo ar testavimo įrankio išdavos (angl. output) ir pažeidžiamumo buvimo/nebuvimo įrodymai;

32.2.8. testo rezultatai, išvados, pažeidžiamumo pašalinimo rekomendacijos, šalinimo planas (suderintas su institucija).

32.3. Pažeidžiamumų vertinimo ataskaitoje turi būti pateikiami visi galimi įsilaužimų scenarijai – detalios aprašytos veiksmų seka, kaip išnaudoti vieną ar kitą saugumo trūkumą (pateikiama tik esant technologiniams pažeidžiamumams). Ataskaita turi leisti iš karto identifikuoti labiausiai pažeidžiamas informacinių sistemų vietas ir didžiausius trūkumus, o atlikus pakartotinius pažeidžiamumų įvertinimus ateityje, leisti palyginti gautus rezultatus ir įvertinti pokyčius. Kartu su ataskaita turi būti pateiktos skenavimo/testavimo priemonės ir testų rezultatai.

33. Kartu su rekomendacijomis turi būti pateikti veiksmų planai, kuriuose būtų įvardijamos priemonės, pateiktys, vykdytojai, terminai bei prognozuojamos finansavimo apimtys. Veiksmų planai turi būti parengti atsižvelgiant į:

33.1. programinės įrangos efektyvų panaudojimą;

- 33.2. IT techninės įrangos ir duomenų centrų infrastruktūros efektyvų panaudojimą;
- 33.3. reikalingų žmogiškųjų išteklių ir kompetencijos užtikrinimą;
- 33.4. IT ir su IT susijusių veiklų organizavimą ir finansavimo mechanizmo efektyvumą;
- 33.5. tinkamą su IT susijusių prekių ir paslaugų pirkimų organizavimą.

VI. REIKALAVIMAI PASLAUGŲ TEIKIMUI

34. Įmonės tvarkomų registrų ir informacinių sistemų informacinių technologijų audito paslaugos turi būti teikiamos vadovaujantis IS audito standartais, taisyklėmis ir geriausiaja praktika.

35. Įmonės tvarkomų valstybės registrų ir informacinių sistemų informacinių technologijų auditas turi būti atliktas, įvertinant informacinių sistemų plėtros ir modernizavimo, informacinių paslaugų valdymo ir informacijos saugos valdymo priemonių ir metodų atitiktį plačiausiai taikomų standartų ir metodikų (pvz. COBIT, ISO/IEC 20000-1:2011 arba lygiaverčių) reikalavimams ir gerajai praktikai bei nustatant atitiktį IT valdymo sritį reglamentuojantiems teisės aktais.

36. Informacinės sistemų sauga turi būti vertinama vadovaujantis šiais teisės aktais ir metodikomis:

- 36.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu;
- 36.2. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716;
- 36.3. Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832;
- 36.4. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. Nr. 1V-156;
- 36.5. Bendraisiais reikalavimais organizacinėms ir techninėms duomenų saugumo priemonėms, patvirtintais Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71.
- 36.6. Lietuvos standartais LST ISO/IEC 27001:2013 ir LST ISO/IEC 27002:2014;
- 36.7. Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo technika“ grupės standartais;
- 36.8. kitais informacijos ir informacinių sistemų saugą reglamentuojančiais teisės aktais.

37. Informacinės sistemos saugos vertinimas turi būti atliktas pagal viešai žinomą ir pripažintą atvirą ar komercinę pažeidžiamumų įvertinimo metodiką (angl. Penetration Testing Methodology). Pasiūlyme turi būti pateiktas metodikos aprašymas, pakankamas metodikai įvertinti pagal ekonominio naudingumo atitinkamą kriterijų. Pasiūlyme būtina nurodyti metodikos pavadinimą bei nuorodą į jos aprašymą.

38. Audito metu naudojami atitikties kriterijai turi būti objektyvūs, išsamūs, tinkami audituojamam objektui, išmatuojami, suprantami, plačiai pripažinti, autoritetingi ir suprantami Įmonei. Turi būti žinomi atitikties kriterijų pasirinkimo šaltiniai, o patys kriterijai suderinti su Įmone. Taip pat Vykdytojas turės suderinti su Įmone paslaugų teikimo metu naudojamus vertinimo būdus, metodus ir priemones.

39. Paslaugų rezultatai turi būti gaunami, naudojant šiuos metodus – interviu, teisės aktų ir vidinių organizacijos dokumentų analizę, fizinę apžiūrą.

40. Atliekant auditą, turės būti numatyti IT audito standartais paremti ir atlikti darbai, apimantys pagrindines audito sritis:

40.1. parengta ir įgyvendinta rizika pagrįsta IT audito strategija;

40.2. aprašyti siekiami audito tikslai ir pateiktys;

40.3. suplanuoti ir atliktos audito dalys, siekiant nustatyti, ar informacinės sistemos yra apsaugotos, kontroliuojamos ir tenkina veiklos lūkesčius (saugumo ir įsilaužimų testavimams turi būti parengtas ir su įmone suderintas atskiras detalus darbų planas su kalendoriniu grafiku);

40.4. pateiktos audito išvados ir rekomendacijos pagrindinėms suinteresuotosioms šalims;

41. pateiktas veiksmų planas atotrūkiui nuo standartų reikalavimų sumažinti ir audito rekomendacijoms įgyvendinti.

42. Auditas turi būti atliekamas ir ataskaitos dokumentai turi būti rengiamas etapais, pateikiant Įmonei kiekvieno etapo rezultatus, juos pristatant ir aptariant su Įmonės atstovams.

43. Pradėdamas vykdyti Sutartį, Vykdytojas privalės parengti ir suderinti su Įmone Įmonės tvarkomų registrų ir informacinių sistemų IT audito atlikimo projekto (toliau – Projektas) valdymo planą, kuriame turi būti pateikiama (apimant, bet neapsiribojant):

43.1. numatomų naudoti įrankių ir metodų aprašymas ir jų taikymo pagrindimas;

43.2. projekto darbų grafikas;

43.3. komunikavimo planas;

43.4. rizikos valdymo planas;

43.5. kokybės valdymo planas.

44. Projekto valdymo planas turi būti pateiktas Įmonei per 3 darbo dienas nuo Įmonės tvarkomų registrų ir informacinių sistemų informacinių technologijų audito paslaugų pirkimo sutarties pasirašymo. Plane turi būti detalizuotas paslaugų atlikimas: nurodyti konkretūs veiksmai, jų vykdymo terminai, kita aktuali informacija.

45. Pastabos Projekto valdymo planui turi būti suderintos ne vėliau, kaip per 3 darbo dienas kai jas pateikia Įmonė, pateikiant galutinį Projekto valdymo plano dokumentą. Esant poreikiui, paslaugų teikimo metu projekto valdymo plano dokumentas, suderinus su įmone, gali būti patikslintas ar papildytas.

46. Projekto vykdymo metu Vykdytojas turės išanalizuoti surinktą informaciją ir parengti Įmonės tvarkomų valstybės registrų ir informacinių sistemų audito ataskaitą, kurioje atskirai turi būti aprašyta ir įvertinta informacinių sistemų esama būseną, sauga ir valdymas bei pateiktos „gerąją praktiką“ ir standartais paremtos rekomendacijos.

47. Vykdydamas projektą Vykdytojas turės surinkti ir išanalizuoti informaciją apie Įmonės IS būseną, IT valdymą ir informacijos saugos užtikrinimą.

48. Turės būti surinkta ir apibendrinta informacija apie esamą IS situaciją ir jos veikimo atitikimą organizacijos poreikiams bei turimus infrastruktūros išteklius ir Įmonės poreikius IT infrastruktūros ištekliams (bendriesiems, techninei ir programinei įrangai, infrastruktūros paslaugoms ir stebėjimo bei valdymo įrankiams). Taip pat turi būti surinkta informacija apie IT veiklą, susijusią su informacinių sistemų plėtra ir priežiūra: IT veiklos planavimą ir organizavimą, IT programinės ir techninės įrangos plėtros poreikių surinkimo, inicijavimo, planavimo ir diegimo valdymą, informacinių sistemų priežiūros ir aptarnavimo bei duomenų saugos užtikrinimo valdymą.

49. Ne vėliau kaip per 2 mėn. nuo sutarties įsigaliojimo dienos Vykdytojas turės surinkti reikalingą informaciją, atlikti auditą, parengti ir pristatyti audito rezultatus Įmonės atsakingiems asmenims ir priduoti Įmonės audito ataskaitos dokumentą.

50. Audito ataskaitoje aprašoma atlikta analizė ir pateikiami audito rezultatai, įvardijant riziką, trūkumus, tobulintinas sritis ir patiekiant rekomendacijų diegimo planus.

51. Visą parengtą dokumentaciją (rezultatus) prieš galutinį jos pateikimą tiekėjas privalo suderinti su Įmone. Esant poreikiui, parengti dokumentai turi būti pataisyti (patobulinti) pagal perkančiosios organizacijos pastabas ir pasiūlymus.

52. Nustačius esminius trūkumus, su Įmone suderinami tokių trūkumų pašalinimo veiksmai.

53. Audito ataskaitos dokumentuose pateikiami duomenys ir informacija turi būti patikima, o pateikiamos išvados ir pasiūlymai – pagrįsti standartais ir teisės aktais.

54. Ataskaitoje pateikiama informacija turi būti išsami ir paremta atlikta analize.

55. Galutiniai paslaugų teikimo rezultatai (dokumentai) turi būti pateikiami tvarkingi ir susisteminti, apiforminti ir įrišti būdu, leidžiančiu ilgalaikį jų saugojimą ir naudojimą.

56. Visi pateikiami dokumentai turi būti parengti lietuvių kalba. Įmonei pateikiama: spausdintas dokumentų egzempliorius ir šifruota kompiuterinė laikmena MS Word (*.docx) formatu; vykdytiems pristatymams parengtos skaidrės pateikiamos MS PowerPoint (*.pptx) formatu.

UŽSAKOVAS

Valstybės įmonė Centrinė hipotekos įstaiga

Direktorius
Vaidas Valikonis

2016 m. kovo 1 d.



VYKDYTOJAS

UAB „PricewaterhouseCoopers“, veikianti pagal jungtinės veiklos sutartį su UAB „Blue Bridge“

Konsultacijų skyriaus vadovas, partneris
Vidas Venckus

Direktorius
Rimvydas Jogėla

2016 m. kovo 1 d.



Teisės skyriaus
vyriausiasis specialistas
Edvardas Arštikys
2016-03-01

Teisės skyriaus vedėja
Giedrė Malikėnienė
2016-03-01

Finansų skyriaus vedėja

Vida Šimkūnaitė

2016-03-01

Informacinių technologijų plėtros
ir priežiūros skyriaus vedėja

Vaiva Norvilaitė

2016-03-01

2016 m. kovas 1 d.

Valstybės įmonės Centrinės hipotekos įstaigos
informacinių technologijų audito paslaugų
pirkimo sutarties Nr. F3-14(2016)
2 priedas

(Paslaugų suteikimo akto forma)

PASLAUGŲ SUTEIKIMO AKTAS

2015 m.

d.

Vilnius

Vadovaudamiesi 2015 m. _____ d. valstybės įmonės Centrinės hipotekos įstaigos (toliau – Užsakovas) ir UAB „PricewaterhouseCoopers“, veikiančios pagal jungtinės veiklos sutartį su UAB „Blue Bridge“ (toliau – Vykdytojas), sudaryta Valstybės įmonės Centrinės hipotekos įstaigos informacinių technologijų audito paslaugų pirkimo sutartimi Nr. _____, Vykdytojas ir Užsakovas sudarė šį Paslaugų suteikimo aktą:

1. Vykdytojas suteikė, o Užsakovas priėmė šias paslaugas:

(išvardinamos suteiktos paslaugos, nurodant jų pavadinimą, apimtį, paslaugų teikimo laikotarpį perduodamus dokumentus, nurodant puslapių skaičių);

2. Paslaugų suteikimo aktas sudarytas dviem egzemplioriais, po vieną Vykdytojui ir Užsakovui.

Priėmė

Valstybės įmonė Centrinė hipotekos
įstaiga

(Nurodomas atstovas)

Suteikė

UAB „PricewaterhouseCoopers“, veikianti
pagal jungtinės veiklos sutartį su UAB „Blue
Bridge“

(Nurodomas atstovas)

UŽSAKOVAS

Valstybės įmonė Centrinė hipotekos įstaiga

Direktorius
Vaidas Valikonis

2016 m. kovas 1 d.



VYKDYTOJAS

UAB „PricewaterhouseCoopers“, veikianti
pagal jungtinės veiklos sutartį su UAB „Blue
Bridge“

Konsultacijų skyriaus vadovas, partneris
Vidas Venckus

2016 m. kovas 1 d.

Direktorius
Rimvydas Jogėla

Toisės skyriaus
vyriausiasis specialistas

Edvardas Arštikys

2016-03-01

Toisės skyriaus vedėja

Giedrė Malikėnienė

2016-03-01

Finansų skyriaus vedėja

Vida Šimkūnaitė

2016-03-01

Informacinių technologijų plėtros
ir priežiūros skyriaus vedėja

Vaiva Norvilaitė

2016-03-01

2016 m. koovo 1 d.

Valstybės įmonės Centrinės hipotekos įstaigos informacinių technologijų audito paslaugų pirkimo sutarties Nr. F3-14(2016)
3 priedas

(Konfidencialumo pasižadėjimo forma)

KONFIDENCIALUMO PASIŽADĖJIMAS

201_ m. _____ d.

Vilnius

Aš, _____, būdamas UAB „PricewaterhouseCoopers“, veikiančios pagal jungtinės veiklos sutartį su UAB „Blue Bridge“, paskirtu specialistu ir atlikdamas 2016 m. _____ d. Valstybės įmonės Centrinės hipotekos įstaigos informacinių technologijų audito paslaugų pirkimo sutartyje Nr. _____ (toliau – Sutartis) numatytas paslaugas:

- **įsipareigoju** saugoti paslapyje ir tik Sutarties įsipareigojimų vykdymo tikslais naudoti valstybės įmonės Centrinės hipotekos įstaigos patikėtą man konfidencialią informaciją, kuri man taps žinoma teikiant paslaugas pagal Sutartį, saugoti ją tokiu būdu, kad tretieji asmenys neturėtų galimybės su ja susipažinti ar pasinaudoti, o pasibaigus Sutarties galiojimui visą su Sutarties vykdymu susijusią, mano turimą, informaciją UAB „PricewaterhouseCoopers“, veikiančią pagal jungtinės veiklos sutartį su UAB „Blue Bridge“, kad UAB „PricewaterhouseCoopers“, veikianti pagal jungtinės veiklos sutartį su UAB „Blue Bridge“ informaciją sunaikintų arba perduotų valstybės įmonei Centrinei hipotekos įstaigai. Šis įsipareigojimas negalioja tuomet, kai būsiu įpareigotas valstybės įmonės Centrinės hipotekos įstaigos patikėtą man konfidencialią informaciją atskleisti pagal Lietuvos Respublikos įstatymus.

- **žinau**, kad, Lietuvos Respublikos įstatymų ir kitų teisės aktų nustatyta tvarka turėsiu atlyginti valstybės įmonei Centrinei hipotekos įstaigai ir kitiems susijusiems asmenims turtinę ir neturtinę žalą, padarytą dėl šio įsipareigojimo nevykdymo arba netinkamo vykdymo, atsakyti už savo veiksmus Lietuvos Respublikos įstatymų ir kitų teisės aktų nustatyta tvarka.

Šis įsipareigojimas galios visą Sutarties vykdymo laiką ir neribotą laiką po Sutarties pasibaigimo, nepriklausomai nuo užimamų pareigų ir darbovietės, kurioje aš dirbsiu.

(Darbuotojo pareigos, vykdant Sutartį)

(parašas)

(vardas pavardė)

(Asmens, dalyvavusio
pasirašant konfidencialumo
pasižadėjimą, pareigos,)

(parašas)

(vardas pavardė)

UŽSAKOVAS

Valstybės įmonė Centrinė hipotekos įstaiga

VYKDYTOJAS

UAB „PricewaterhouseCoopers“, veikianti pagal jungtinės veiklos sutartį su UAB „Blue Bridge“

Direktorius
Vaidas Valikonis

Konsultacijų skyriaus vadovas, partneris
Vidas Venckus

Direktorius
Rimvydas Jogėla

2016 m. koovo 1 d.

Teisės skyriaus
vyriausiasis specialistas

Edvardas Arštikys

2016-03-01

Teisės skyriaus vedėja

Giedrė Malikėmenė

2016-03-01

2016 m. koovo 1 d.

Finansų skyriaus vedėja

Vida Šimkūnaitė

Informacinių technologijų plėtros
ir priežiūros skyriaus vedėja

Vaiva Norvilaitė

2016-03-01

2016 m. Novo 1 d.

Valstybės įmonės Centrinės hipotekos įstaigos
informacinių technologijų audito paslaugų
pirkimo sutarties Nr. F3-14 (2016)
4 priedas

(Pasižadėjimo saugoti asmens duomenų paslaptis forma)

PASIŽADĖJIMAS SAUGOTI ASMENS DUOMENŲ PASLAPTIS

(Paslaugų teikėjo pavadinimas)

201_ m. _____ d.
Vilnius

Darbuotojo pasižadėjimas saugoti asmens duomenų paslaptį

Aš suprantu:

- kad savo darbe naudosis asmens duomenis, kurie negali būti pranešti neįgaliesiems asmenims ar institucijoms;
- kad netinkamas asmens duomenų tvarkymas gali užtraukti atsakomybę pagal Lietuvos Respublikos įstatymus;
- kad draudžiama perduoti ar dalintis su kitais asmenimis tarnybos viduje ar už jos ribų slaptažodžiais ir kitais duomenimis, leidžiančiais programinių ar techninių priemonių pagalba naudotis asmens duomenimis bet kokioje formoje.

Aš pasižadu:

- tvarkyti asmens duomenis, vadovaudamasis Lietuvos Respublikos įstatymais ir kitais teisės aktais, taip pat pareiginiais nuostatais ir taisyklėmis, reglamentuojančiomis man patikėtas asmens duomenų tvarkymo funkcijas;
- neatskleisti tvarkomos informacijos nei vienam asmeniui tiek tarnybos viduje, tiek už jos ribų, kuris nėra įgaliotas naudotis šia informacija;
- pranešti savo vadovui apie bet kokią įtartiną elgesį ar situaciją, kurie gali kelti grėsmę asmens duomenų saugumui.

Aš žinau:

- kad už bet kokią šio pasižadėjimo nesilaikymą turėsiu atsakyti pagal galiojančius Lietuvos Respublikos įstatymus;
- kad šis pasižadėjimas galios visą mano darbo laiką šioje įstaigoje ir pasibaigus darbo santykiams per visą asmens duomenų teisinės apsaugos galiojimo laikotarpį (pagal Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 4 str.);
- kad duomenų subjektas turi teisę reikalauti atlyginti turtinę žalą, padarytą netinkamai saugant, neteisėtai pakeitus ar kitaip iškraipius, perdavus, paskelbus asmens duomenis arba jeigu asmens duomenys pasidarė neteisingi dėl duomenų valdytojo kaltės; kad duomenų subjektas taip pat turi teisę reikalauti, kad jam būtų atlyginta tokių veiksmų padaryta moralinė žala.

Aš esu susipažinęs su Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu ir Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais asmens duomenų apsaugą.

(Darbuotojo pareigos, vykdančios sutartį)

(parašas)

(vardas pavardė)

UŽSAKOVAS

Valstybės įmonė Centrinė hipotekos įstaiga

Direktorius
Vaidas Valikonis



2016 m. Novo 1 d.
Teisės skyriaus
vyriausiasis specialistas

Edvardas Arštikys

2016-03-01

Teisės skyriaus vedėja

Giedrė Malikienė

2016-03-01

VYKDYTOJAS

UAB „PricewaterhouseCoopers“, veikianti
pagal jungtinės veiklos sutartį su UAB „Blue
Bridge“

Konsultacijų skyriaus vadovas, partneris
Vidas Venckus

Direktorius
Rimvydas Jogėla

2016 m. Novo 1
2016-03-01
Finansų skyriaus vedėja

Vida Čimaitė

Informacinių technologijų plėtros
ir priežiūros skyriaus vedėja

Vaiva Norvilaitė

2016-03-01