Līgums Nr. 05-03/375
par centrālo IT sistēmu informācijas drošības pārvaldības izvērtējumu

Rīgā 2014. gada 4. novembrī

Valsts akciju sabiedrība „Tiesu namu aģentūra", reģistrācijas numurs 40003334410, juridiskā adrese Baldones iela 1B, Rīga, tās valdes locekles Santas Sausiņas personā, kura rīkojas saskaņā ar sabiedrības statūtiem, turpmāk tekstā - PASŪTĪTĀJS, no vienas puses, un

sabiedrība ar ierobežotu atbildību „Analytica", reģistrācijas numurs 40003823267, juridiskā adrese Malienas iela 30, Rīga, LV-1079, biroja adrese Ausekļa iela 22-3, Rīga, LV-1010, tās valdes locekles Ivetas Stepanovas personā, kura rīkojas saskaņā ar sabiedrības statūtiem, turpmāk tekstā – IZPILDĪTĀJS, no otras puses,

PASŪTĪTĀJS un IZPILDĪTĀJS abi kopā turpmāk tekstā - Puses, atsevišķi – Puse, pamatojoties uz iepirkuma „Centrālo IT sistēmu informācijas drošības pārvaldības izvērtējums", iepirkuma identifikācijas Nr TNA2014/30, rezultātiem, noslēdz šo līgumu, turpmāk – Līgums, par sekojošo:

1. LĪGUMA PRIEKŠMETS

1.1. PASŪTĪTĀJS uzdod un apņemas samaksāt, un IZPILDĪTĀJS ar saviem resursiem nodrošina PASŪTĪTĀJA centrālo IT sistēmu informācijas drošības pārvaldības izvērtējumu atbilstoši Līguma pielikumam Nr. 1, kas ir Līguma neatņemama sastāvdaļa, definētajiem nosacījumiem, turpmāk tekstā – Pakalpojums.

2. LĪGUMA KOPĒJĀ SUMMA

2.1. Līguma kopējā summa saskaņā ar finanšu piedāvājumu (Līguma pielikums Nr. 2) sastāda 29 200,00 EUR (divdesmit deviņi tūkstoši divi simti *euro* un 00 centi), ietverot pievienotās vērtības nodokli.

2.2. Līguma kopējā summā iekļautas visas izmaksas, kas saistītas ar Līguma izpildi, tai skaitā visi nodokļi un nodevas.

3. PUŠU SAISTĪBAS UN PIENĀKUMI

3.1. PASŪTĪTĀJA saistības un pienākumi:

3.1.1. veikt samaksu par kvalitatīvi un laikā sniegtu Pakalpojumu Līgumā noteiktajos termiņos un kārtībā;

3.1.2. savlaicīgi veikt IZPILDĪTĀJA izpildītā Pakalpojuma pieņemšanu;

3.1.3. nodrošināt IZPILDĪTĀJA pārstāvjiem iespēju piekļūt PASŪTĪTĀJA telpām darba laikā no plkst. 8.30 līdz 16.30, arī citos laika periodos par to iepriekš Pušu pilnvarotajām personām vienojoties;

3.1.4. nodrošināt IZPILDĪTĀJA pārstāvjiem pilnu pieeju informācijai, datiem, dokumentiem, telpām un darba vietām, kas nepieciešamas Līguma izpildei.

3.2. IZPILDĪTĀJA saistības un pienākumi:

3.2.1. sniegt Pakalpojumu Līgumā paredzētajā termiņā, apjomā un kvalitātē;

3.2.2. uzņemties pilnu materiālo atbildību par zaudējumiem, kuri nodarīti PASŪTĪTĀJAM un trešajām personām sakarā ar Līguma noteikumu pārkāpumu, ja IZPILDĪTĀJS tajos vainojams;

3.2.3. IZPILDĪTĀJA personālu, kuru tas iesaistījis Līguma izpildē, par kuru sniedzis informāciju PASŪTĪTĀJAM un kura kvalifikācijas atbilstību izvirzītajām prasībām PASŪTĪTĀJS ir vērtējis, pēc Līguma noslēgšanas drīkstēs nomainīt tikai ar PASŪTĪTĀJA rakstveida piekrišanu;

3.2.4. ievērot Līguma 3.1.3. punktā noteikto kārtību;

3.2.5. ievērot darba drošības prasības Pakalpojuma sniegšanas laikā.

4. PAKALPOJUMU IZPILDES TERMIŅŠ UN TO PIEŅEMŠANA

4.1. Pakalpojuma sniegšanas termiņš līdz 2014. gada 5. decembrim.

4.2. Pēc Pakalpojuma pilnīgas izpildes IZPILDĪTĀJS iesniedz PASŪTĪTĀJAM gala pieņemšanas - nodošanas aktu.

4.3. 5 (piecu) darba dienu laikā pēc pilnīgas Pakalpojumu sniegšanas tiek veikta pārbaude un parakstīts gala pieņemšanas - nodošanas akts. Ja pārbaudes laikā tiek konstatēti defekti, PASŪTĪTĀJS neparaksta gala pieņemšanas - nodošanas aktu un par to informē IZPILDĪTĀJU, kā rezultātā tiek sastādīts defektu akts, kas kļūst par Līguma neatņemamu sastāvdaļu. Defektu aktā tiek norādīti Pakalpojuma vai tā daļas defekti, kā arī šo defektu novēršanas kārtība un termiņi. Aktu paraksta abu Pušu pilnvarotie pārstāvji.

4.4. Ja IZPILDĪTĀJS defektu aktā noteiktajā termiņā nenovērš defektus un sniedz nekvalitatīvu Pakalpojumu vai Pakalpojumu nepilnā apmērā, PASŪTĪTĀJS to nepieņem un IZPILDĪTĀJS maksā PASŪTĪTĀJAM Līguma 6.2. punktā noteikto soda naudu.

5. NORĒĶINU KĀRTĪBA

5.1. PASŪTĪTĀJS veic apmaksu par Pakalpojuma sniegšanu pēc Pakalpojuma izpildes un nodošanas-pieņemšanas akta parakstīšanas.

5.2. Samaksa par veiktajiem Pakalpojumiem tiek veikta ar pārskaitījumu uz Līguma 11. punktā norādīto IZPILDĪTĀJA bankas kontu.

5.3. Par apmaksas dienu tiek uzskatīta diena, kad PASŪTĪTĀJS veicis bankas pārskaitījumu par veiktajiem Pakalpojumiem uz IZPILDĪTĀJA kontu.

6. PUŠU MANTISKĀ ATBILDĪBA

6.1. Ja PASŪTĪTĀJS neveic samaksu par atbilstoši Līguma noteikumiem veiktajiem Pakalpojumiem Līgumā noteiktajos termiņos, IZPILDĪTĀJS ir tiesīgs pieprasīt kavējuma procentus 0,1 % apmērā no nesamaksātās summas par katru maksājuma termiņa nokavējuma dienu saskaņā ar IZPILDĪTĀJA iesniegto rēķinu, bet ne vairāk kā 10 % no Līguma kopējās summas.

6.2. Ja IZPILDĪTĀJS nesniedz kvalitatīvu Pakalpojumu noteiktajā laikā, tad IZPILDĪTĀJS maksā PASŪTĪTĀJAM līgumsodu 0,1 % apmērā no Līguma kopējās summas par katru nokavēto dienu saskaņā ar PASŪTĪTĀJA iesniegto rēķinu, bet ne vairāk kā 10 % no Līguma kopējās summas.

6.3. Līgumsoda samaksa neatbrīvo Puses no Līgumā noteikto saistību izpildes.

7. INFORMĀCIJAS AIZSARDZĪBA

7.1. Ja Līgums tieši nepilnvaro un/vai tas neizriet no kādas šī Līguma saistības, Puses apņemas saglabāt konfidencialitāti attiecībā uz informāciju, kas Pusei darīta zināma šī Līguma izpildē, ja tas atbilst Līguma 7.2. punktā norādītajai ierobežotas pieejamības informācijas definīcijai, paredzot, ka šāds noteikums neattiecas uz tādiem faktiem, informāciju, zināšanām, dokumentiem un/vai citām lietām, ja tās:

7.1.1. bija saņemšanas laikā publicētas vai citādi padarītas vispārpieejamas;

7.1.2. pēc tam, kad Puse tās saņēmusi, ir tikušas publicētas vai kļuvušas vispārēji publiski pieejamas citādā veidā nekā ar jebkādu to saņēmušās Puses darbību vai nodošanu;

7.1.3. saņemšanas laikā bija jau zināmas Pusei, kura tās saņēmusi, bez jebkādiem ierobežojumiem, attiecībā uz to atklāšanu;

7.1.4. bija pilntiesīgi saņemtas no trešās personas bez jebkādas to atklājušās Puses pieprasītās konfidencialitātes uzņemšanās;

7.2. Jēdzienu „Ierobežotas pieejamības informācija", Puses tulko Informācijas atklātības likuma izpratnē.

7.3. Puses apņemas nodrošināt, ka Līguma izpildes laikā to savstarpējā komunikācijā radusies informācija tiek klasificēta kā ierobežotas pieejamības un Puses apņemas nodrošināt tās aizsardzību cik tālu tas ir to spēkos.
7.4. IZPILDĪTĀJS apņemas nodrošināt, ka tas neizpaudīs Līguma izpildes laikā iegūto informāciju par PASŪTĪTĀJA informācijas un informācijas sistēmu drošību.

8. NEPĀRVARAMA VARA

8.1. Puses tiek atbrīvotas no atbildības par Līguma saistību nepildīšanu, ja tā rodas pēc Līguma noslēgšanas nepārvaramas varas vai ārkārtēju apstākļu ietekmes rezultātā, kurus attiecīgā no Pusēm (vai Puses kopā) nevarēja ne paredzēt, ne novērst, ne ietekmēt, un, par kuru rašanos nenes atbildību, tas ir, stihiskas nelaimes, kara darbība, katastrofas, epidēmijas, iekšējie nemieri, blokāde, masu demonstrācijas, streiki, normatīvie akti.
8.2. Katra no Pusēm, kuru Līguma ietvaros ietekmē nepārvaramas varas apstākļi, nekavējoties tiklīdz tas ir iespējams par to informē otru Pusi.
8.3. Ja kāda no Pusēm, kuras rīcību ietekmē nepārvarama vara bez objektīva iemesla neinformē otru Pusi par nepārvaramas varas apstākļu iestāšanos 3 (trīs) kalendāro dienu laikā, attiecīgā Puse netiek atbrīvota no Līguma saistību izpildes.
8.4. Gadījumā, ja nepārvaramas varas apstākļi turpinās ilgāk kā 30 (trīsdesmit) kalendārās dienas, Puses kopīgi risina jautājumu par Līguma turpmāko izpildi vai izbeigšanu. Līguma izbeigšanas gadījumā, kuras pamats ir nepārvarama vara, nevienai no Pusēm nav tiesības prasīt zaudējumu atlīdzību.

9. STRĪDU IZSKATĪŠANA UN LĪGUMA IZBEIGŠANA

9.1. Ja viena Puse pārkāpusi kādu no Līguma noteikumiem, otrai Pusei ir tiesības iesniegt rakstveida pretenziju, kurā norādīts pārkāpuma raksturs un Līguma punkts, kuru Puse uzskata par pārkāptu.
9.2. Strīdus un nesaskaņas, kas var rasties Līguma izpildes rezultātā vai sakarā ar Līgumu, Puses atrisina savstarpēju pārrunu ceļā. Ja Puses nevar panākt vienošanos sarunu ceļā, tad domstarpības risināmas Latvijas Republikas normatīvajos aktos noteiktajā kārtībā.
9.3. PASŪTĪTĀJAM ir tiesības vienpusēji pārtraukt Līgumu 3 (trīs) darba dienas iepriekš rakstveidā brīdinot IZPILDĪTĀJU un nesamaksāt Līgumā noteikto samaksu, ja IZPILDĪTĀJS neveic Pakalpojumu, neievēro Pakalpojuma veikšanas nosacījumus vai nepilda Līguma saistības noteiktajā laikā vai apjomā.

10. CITI NOTEIKUMI

10.1. Līgums stājas spēkā ar brīdi, kad to parakstījusi pēdējā no Pusēm, un ir spēkā līdz brīdim, kad Puses ir izpildījušas savas Līgumā noteiktās saistības.
10.2. Ja kādai no Pusēm tiek mainīti rekvizīti (adrese, bankas rēķini u.c.), tā nekavējoties, bet ne vēlāk kā 3 (trīs) darba dienu laikā, rakstiski paziņo otrai Pusei.
10.3. PASŪTĪTĀJA pilnvarotais pārstāvis Līguma izpildes laikā ir Informācijas tehnoloģiju daļas vadītājs Sandis Vulis, tālrunis: 67804744, mob. tālrunis: 29255325, e-pasts: sandis.vulis.
10.4. IZPILDĪTĀJA pilnvarotais pārstāvis Līguma izpildes laikā ir Juris Pūce, tālrunis 67471283, mob. tālr. 26458931, e-pasts: juris.puce@analytica.lv.
10.5. Pilnvarotie pārstāvji ir atbildīgi par Līguma izpildes uzraudzīšanu, defekta akta sastādīšanu un parakstīšanu, Pakalpojuma pieņemšanas - nodošanas akta parakstīšanu, savlaicīgu rēķinu pieņemšanu, apstiprināšanu un nodošanu apmaksai.
10.6. Līgumu var papildināt vai grozīt Pusēm savstarpēji vienojoties. Jebkuras Līguma izmaiņas vai papildinājumi tiek noformēti rakstveidā un kļūst par Līguma neatņemamām sastāvdaļām.
10.7. Nepieciešamības gadījumā Puses rīko savstarpējas sanāksmes. Sanāksmes tiek rīkotas, pamatojoties uz vienas Puses rakstisku ierosinājumu un tiek sasauktas 2 (divu) darba dienu laikā no ierosinājuma iesniegšanas otrai Pusei. Sanāksmes laikā Puses konstatē

PASŪTĪTĀJA un/vai IZPILDĪTĀJA vajadzības un mērķus, vienojas par šo mērķu sasniegšanas metodēm. Pēc sanāksmes tiek sagatavots protokols, kuru paraksta abu Pušu pārstāvji un tas ir saistošs abām Pusēm Līguma izpildē.

10.8. Līgums sastādīts uz 4 (četrām) lapām ar 2 (diviem) pielikumiem uz 9 (deviņām) lapām, 2 (divos) eksemplāros, pa vienam eksemplāram katrai Pusei.

11. PUŠU PARAKSTI UN REKVIZĪTI

IZPILDĪTĀJS	**PASŪTĪTĀJS**
SIA „Analytica"	VAS „Tiesu namu aģentūra"
Reģ. Nr. 40003823267	Reģ. Nr. LV40003334410
Juridiskā adrese: Malienas iela 30,	Juridiskā adrese: Baldones iela 1B,
Rīga, LV-1079	Rīga, LV-1007
Biroja adrese: Ausekļa iela 22-3,	Banka: AS „SEB banka"
Rīga, LV-1010	Kods UNLALV2X
Banka: AS „DNB banka"	Konta Nr. LV64UNLA0002021469371
Kods RIKOLV2X	
Konta Nr. LV37RIKO0002013294482	
_____/I. Stepanova/	_____/S. Sausiņa/
2014. gada 4. novembrī	2014. gada 4. novembrī

Pielikums Nr.1
pie 2014. gada 4. novembra
līguma Nr. 05-03/375

TEHNISKAIS PIEDĀVĀJUMS

analytica

2 TEHNISKAIS PIEDĀVĀJUMS

Rīgā, 2014. gada 17. oktobrī

SIA „Analytica", reģ. nr. 40003823267, apņemas nodrošināt epirkuma „ Centrālo IT sistēmu informācijas drošības pārvaldības izvērtējums", identifikācijas Nr. TNA 2014/30, tehniskajā specifikācijā un darba uzdevumā norādītos uzdevumus:

2.1 DARBA UZDEVUMS

Apraksts
1. Atbilstības vērtējums standartā LVS ISO/IEC 27001:2013 noteiktajām pamatprasībām, zemāk uzskaitītajām pielikuma A kontrolēm un citām Pasūtītāja izvirzītajām prasībām
1.1. Informācijas drošības politika
1.1.1. Pamatnostādnes informācijas drošībai (A.5.1.1*)
1.1.2. Informācijas drošības pamatnostādņu pārskats (A.5.1.2*)
1.2. Informācijas drošības organizācija – iekšējā
1.2.1. Informācijas drošības funkcijas un pienākumi (A.6.1.1*)
1.2.2. Pienākumu nodalīšana (A.6.1.2*)
1.2.3. Informācijas drošība projektu vadībā (A.6.1.5*)
1.2.4. Nodarbinātības noteikumi un nosacījumi (A.7.1.2*)
1.2.5. Neatkarīga informācijas drošības pārskatīšana (A.18.2.1*)
1.3. Informācijas drošības organizācija – sadarbība ar trešajām pusēm
1.3.1. Informācijas drošības politika attiecībās ar piegādātāju (A.15.1.1.*)
1.3.2. Drošības atrunāšana piegādātāju līgumos (A.15.1.2*)
1.3.3. Informācijas un komunikāciju tehnoloģijas piegādes ķēde (A.15.1.3*)
1.4. Resursu pārvaldība
1.4.1. Līdzekļu inventarizācija (A.8.1.1*)
1.4.2. Līdzekļu īpašumtiesības (A.8.1.2*)
1.4.3. Līdzekļu pieņemama izmantošana (A.8.1.3*)
1.5. Informācijas resursu klasifikācija
1.5.1. Informācijas resursu klasifikācijas vadlīnijas un kārtība (A.8.2.1*, A.8.2.2*, A.8.2.3.)
1.6. Cilvēkresursu drošība
1.6.1. Darbinieku un trešās puses lomu un pienākumu noteikšana (A.6.1.1*)
1.6.2. Pienākumu nodalīšana (A.6.1.2*)
1.6.3. Darbinieku izglītošana par informācijas drošības jautājumiem (A.7.2.2*)
1.6.4. Disciplinārlietas process (A.7.2.3*)
1.6.5. Darblīguma pārtraukšanas process, ieskaitot piešķirtā inventāra atgriešanu, un pieejas tiesību anulēšanu (A.7.3.1*)
1.7. Telpas ar ierobežotu pieeju
1.7.1. Telpu drošības perimetra noteikšana (A.11.1.1*)
1.7.2. Piekļuves ierobežošanas kontroles ierobežotas pieejamības telpām (A.11.1.2*)
1.7.3. Telpu aizsardzība pret apkārtējās vides bojājumiem no uguns, aplūšanas, vandālisma vai citiem ārkārtas gadījumiem (A.11.1.4*)
1.7.4. Noteikumi darbam aizsargājamās telpās (A.11.1.5*)
1.7.5. Publiskās zonas nodalīšana no informācijas apstrādes resursiem (A.11.1.6*)
1.8. Aprīkojuma aizsardzība
1.8.1. Iekārtu (servertehnikas) aizsardzība pret elektropadeves traucējumiem (A.11.2.2*)
1.8.2. Datu kabeļu aizsardzība (A.11.2.3*)
1.8.3. Aprīkojuma izmantošana ārpus biroja telpām (A.11.2.6*)
1.8.4. Atbrīvošanās no informācijas apstrādes aprīkojuma (A.11.2.7*)

Apraksts
1.9. Ekspluatācijas procedūras un pienākumi
1.9.1. 1. Informācijas sistēmu izstrādes, testēšanas un ekspluatācijas iekārtu nodalīšana (A.12.1.4*)
1.10. Trešās puses pakalpojumu piegāde
1.10.1. Drošības kontroļu un pakalpojumu līmeņu iekļaušana pakalpojumu līgumos; (A.15.2.1*)
1.10.2. Pakalpojumu uzraudzība (A.15.2.2*)
1.11. Sistēmas resursu plānošana un uzraudzība
1.11.1. Kapacitātes parametru uzraudzība (A.12.3.1*)
1.12. Aizsardzība pret ļaunprātīgu programmatūru
1.12.1. 1. Ļaunprātīgā koda identificēšana un preventīvās darbības (A.12.2.1*)
1.13. Datu rezerves kopēšana
1.13.1. 1. Datu rezerves kopiju procedūra (A.12.3.1*) un atbilstība
1.14. Rīcība ar datu nesējiem
1.14.1. 1. Datu nesēju lietošanas procedūra, ieskaitot atbrīvošanos no datu nesējiem (A.8.3.1*, A.8.3.2*, A.8.3.3*)
1.15. Informācijas apmaiņa iestādes ietvaros un ārpus tās
1.15.1. Informācijas apmaiņas noteikumi (A.13.2.1*)
1.15.2. Informācijas apmaiņas līgumi ar PMLP, Lursoft, VSAA (A.13.2.2*)
1.16. Datorlietotāju darbību monitorēšana
1.16.1. 1. Prasības audita pierakstiem un to veikšana (A.18.1.3*)
1.17. Pieejas tiesību vadība (Active directory domain TS.gov.lv; Horizon, www.tm.gov.lv, EDPS, Estapiks.gov.lv, darbam.ts.gov.lv, kdb.tm.gov.lv)
1.17.1. Pieejas tiesību vadības procedūra (A.9.1.1*)
1.17.2. Piekļuves tiesību piešķiršana/anulēšana (A.9.2.2*)
1.17.3. Priviliģēto lomu izmantošana/ierobežošana (A.9.2.3*)
1.17.4. Datorlietotāju paroļu vadība (A.9.2.4*, A.9.2.4*, A.9.2.5*)
1.17.5. Pieejas tiesību pārskatīšana (A.9.2.5*)
1.18. Lietotāju pienākumi
1.18.1. Aprīkojuma atstāšana bez uzraudzības (A.11.2.8*)
1.18.2. Tīra galda politika (A.11.2.9*)
1.19. Datortīkla pieejas vadība
1.19.1. Datortīkla servisu lietošanas politika (A.9.1.1*)
1.19.2. Lietotāju autentifikācija ārējiem tīkla savienojumiem (A.9.1.2*)
1.20. Operētājsistēmu (Active directory domain TS.gov.lv; Horizon, www.tm.gov.lv, EDPS, Estapiks.gov.lv, darbam.ts.gov.lv, kdb.tm.gov.lv) pieejas vadība
1.20.1. Utilītprogrammatūras lietošana (A.9.4.4*)
1.21. Informācijas sistēmu pieejas vadība
1.21.1. Pieejas tiesību piešķiršana saskaņā ar pieejas tiesību pārvaldības kārtību (A.9.1.1*)
1.22. Sistēmu failu drošība (Horizon, EDPS, Estapiks.gov.lv)
1.22.1. Sistēmas testa datu aizsardzība (A.14.3.1*)
1.22.2. Piekļuve pie pirmkoda (A.9.4.5*)
1.23. Drošība informācijas sistēmu (Horizon, www.tm.gov.lv, EDPS, Estapiks.gov.lv, darbam.ts.gov.lv, kdb.tm.gov.lv) izstrādei un atbalstam
1.23.1. Informācijas sistēmu izmaiņu vadības procedūra (A.14.2.2*)
1.23.2. Informācijas sistēmu izstrādes aizsardzība (A.14.1.1.*, A.14.1.2, A.14.1.3)
1.24. Ievainojamību pārvaldība
1.24.1. Ievainojamību identificēšanas un novēršanas kārtība (A.12.6.1*, A.12.6.2*)
1.25. Incidentu pārvaldība
1.25.1. Incidentu pārvaldības procedūra, ieskaitot darbinieku atbildības (A.16.1.1*, A.16.1.2), incidentu analīzi (A.16.1.4*), pierādījumu apkopošanu (A.16.1.7*)

Apraksts
1.26. Darbības nepārtrauktības nodrošināšana (atbilstoši standarta ISO/IEC 22301 prasībām) 1.26.1. Iestādes darbības nepārtrauktības plānošanas un risku novērtējums (A.17.1.1*) 1.26.2. Iestādes darbības nepārtrauktības realizācija (A.17.1.2*) 1.26.3. Iestādes darbības plāna testēšana un atkārtota pārvērtēšana (A.17.1.3*) 2. TM vietņu www.norwaygrants.tm.gov.lv, www.tm.gov.lv, https://epasts.tm.gov.lv/owa/, TM-DLU, www.estiesibas.lv, dokumentvedības sistēma (EDPS), Mikrostrategija, Horizon WEB, Estapiks.gov.lv, darbam.ts.gov.lv, kdb.tm.gov.lv drošības tests 2.1. Drošības tests, izmantojot automatizētu drošības interneta vietņu testēšanas rīku 2.1.1. Testēšanā jāiekļauj vismaz šādas pārbaudes: 2.1.1.1. Portu skanēšana 2.1.1.2. Web servisu versijas pārbaude 2.1.1.3. Web servera ievainojamību pārbaude 2.1.1.4. Parametru manipulācijas, izmantojot: 2.1.1.4.1. Cross-site scripting 2.1.1.4.2. Cross frame scripting 2.1.1.4.3. SQL injection 2.1.1.4.4. Cookies manipulation 2.1.1.4.5. Directory traversal 2.1.1.4.6. E-mail injection 2.1.1.4.7. File inclusion 2.1.1.4.8. Full path disclosure 2.1.1.4.9. PHP code injection 2.1.1.4.10. Script source code disclosure 2.1.1.4.11. URL redirection 2.1.1.5. Rezerves kopiju un citu lieko failu identificēšana 2.1.1.6. Administratīvo rīku pieejamība 2.1.1.7. Lietotāju vārda un paroles meklēšana 2.1.1.8. Vienkāršu paroļu identificēšana servisiem, kas aizsargāti ar parolēm 2.2. Konsultācijas un atbalsts ievainojamību novēršanai (līdz 3 cilvēkstundām): 2.3. Testēšanas atskaite: 2.3.1. Testēšanas atskaitē vismaz ir jānorāda: 2.3.1.1. Testa veikšanas datums, laiks un laikietilpība; 2.3.1.2. Veiktie testi un to apjoms; 2.3.1.3. Atklātās ievainojamības, kas grupētas vismaz 3 kategorijās (kritiska, vidēja, zema); 2.3.1.4. Testēšanas atskaitē katrai atklātai ievainojamībai norādīt aprakstu un instrukciju ievainojamības novēršanai.

2.2 AUDITA VEIKŠANAS METODIKA

Atbilstība tiek vērtēta pēc CMMI gatavības stadijas vērtībām (uzskaitītas zemāk). Šis modelis ir pilnībā atbilstošs ISO 27001:2013 standarta prasībām un saistīto standartu (skatīt zemāk) prasībām:

Vērtība	Vērtības nosaukums	Kādos gadījumos jāpiešķir šāda vērtība
0	Neeksistējošs	Norādītais process neeksistē. Organizācija nav informēta, ka minētajam procesam vispār būtu jābūt vai tas ir nepieciešams
1	Sākotnējs	Organizācija ir informēta, ka ir nepieciešams atbilstošais process (ir identificētas ar to saistītas problēmas). Tomēr neeksistē standartizēts process, bet saistītie jautājumitiek tiek risināti katrā gadījumā individuāli. Nav skaidru vadības prasību vai vadības aktīvas iesaistes šajā procesā.
2	Pārvaldīts	Procesi ir izveidoti (ne obligāti aprakstīti) līdz fāzei, kur dažādi cilvēki veicot darbīb/izpildot procesu pieturās pie vienotiem principiem. Nav formalizētas apmācības vai komunikācijas par to kā procesam būtu jānorit, atbildība ir indivīda pusē. Process faktiski ir atkarīgs no indivīda zināšanām un prasmēm, pastāv augsta varbūtība kļūdām procesa norisē, īpaši, ja to veic cits/jauns cilvēks.
3	Definēts	Procedūras ir standartizētas (aprakstītas), dokumentētas un tiek komunicētas (t.sk. izmantojot apmācību sesijas). Tomēr to pielietošana ir atkarīga no indivīda izvēles vai zināšanām par to esamību. Tomēr iespējamās kļūdas un problēmas ir jau iespējams identificēt, kā arī to iespējamos cēloņus. Procedūras iespējams nav pieteikoši detalizētas, bet formalizē faktisko praksi.
4	Kvantitatīvi pārvaldīts	Ir iespējams uzraudzīt un monitorēt procedūru izpildes atbilstību paredzētajām, kā arī novērst nepilnības, kas saistītas ar to novirzēm no paredzētā vai kļūdām. Procesi tiek pastāvīgi uzlaboti un atbilst labai praksei. Automatizācija un dažādi tehniskie atbalsta rīki netiek izmantoti vai tiek izmantoti daļēji/nepilnīgi.
5	Optimizēts	Process noris atbilstoši nozares labākajām praksēm, procesā ir ietverta regulāra tā mērīšana un balstoties uz šiem mērījumiem notiek pastāvīga procesa uzlabošana. Process tiek salīdzināts ar industrijas metrikām vai citām organizācijām. Darba plūsmas ir automatizētas un tiek izmantoti tehniskie atbalsta rīki. Organizācija spēj ātri adaptēties izmaiņām procesos.

Atbilstība standartiem tiek vērtēta gan standarta pamatprasībām, gan ISO 27001:2013 pielikumā minētajām un klienta ieviešanai izvēlētajām kontrolēm (piem: ISO 27001 Pielikums A). Prasību vērtēšana notiek atbilstoši šādiem standartiem:

- LVS ISO/IEC 27001:2013 A (LVS ISO/IEC 27001:2014 L ir standarta latviskais tulkojums) *Informācijas tehnoloģija. Drošības paņēmieni. Informācijas drošības pārvaldības sistēmas. Prasības*
- LVS ISO/IEC 20000-1:2011 *Informāciju tehnoloģija. Pakalpojumu pārvaldība. 1. daļa: Prasības pakalpojumu pārvaldības sistēmai*
- ISO/IEC 22301:2012 *Societal security -- Business continuity management systems --- Requirements*
- LVS ISO/IEC 27007:2012 Informācijas tehnoloģija. Drošības paņēmieni. Vadlīnijas informācijas drošības pārvaldības sistēmas auditēšanai
- LVS EN ISO 19011:2012 Vadlīnijas pārvaldības sistēmu auditēšanai (ISO 19011:2011)

Katrai kontrolei atbilstoši ISO 27001:2013 un ISO 19011:2012 standartu prasībām tiks ievākti šādi pierādījumi (klasificēti atbilstoši pierādījumu ticamības pakāpei no ticamākā uz mazāk ticamu):

1. Fiziskie pierādījumi
   1.1. Jebkas, kas var tikt novērots, pārbaudīts, saskaitīts, inspicēts (piemēri: vadu esamība un izvietojums, utml)
2. Matemātiskie pierādījumi
   2.1. Auditora veiktas matemātiskas darbības (piemēram: izmantoto licenču skaita salīdzināšana ar nopirkto)
3. Apstiprinošie pierādījumi
   3.1. Iegūto pierādījumu verifikācija salīdzinot
4. Tehniskie pierādījumi
   4.1. Tehnisko resursu analīze (piem: ugunsmūra testi utml)
5. Analītiskie pierādījumi
   5.1. Savstarpēju sasaistu analīze (piem: auditācijas pierakstu pārskate)
6. Dokumentārie pierādījumi
   6.1. Dokumentu un to satura apsakte (piem: drošības politikas dokumenta izvērtējums)
7. Mutiskie pierādījumi
   7.1. Interviju laikā iegūtie pierādījumi (piem: darbinieku mutiski sniegtā informācija)

Lai nodrošinātu atbilstību ISO 27001 prasībām, atsevišķi audita laikā tiks identificēti arī audita riski, kas saistās ar šādiem iespējamajiem riskiem:

1. Noteikšanas risks – risks, ka auditors nepamana būtisku neatbilstību audita laikā
2. Kontroles risks – risks, ka konkrēta izvēlētā kontrole nenodrošina nepieciešamo aizsardzības līmeni
3. Saistītais risks – risks, ka IDPS strādā neefektīvi dēļ ārējiem faktoriem (industrijas risks)

Kopējam darbam tiks izstrādāts atbilstošs audita plāns, katrai kontrolei norādot paredzēto efktīvāko pierādījumu ievākšanas metodi.

Vērtējums tiks sniegts atbilstoši ISO 19011 norādītajai un ISO 9001 norādītajai skalai:

- Atbilstība
- Rekomendācija
- Neatbilstība
- Būtiska neatbilstība

2.3 OSSTMM UN OWASP

2.3.1 IEVAINOJAMĪBU PĀRBAUDE

Pretendents ievainojamības pārbaudes veiks pēc OSSTMM (Open-Source Security Testing Methodology Manual) un OWASP (Open Web Application Security Project) metodoloģijas, kur attiecīgās darbības galvenais mērķis ir identificēt, izprast un verificēt tīkla infrastruktūras vājās vietas, konfigurācijas kļūdas un ievainojamības. OSSTMM metodoloģija ir pilnībā savietojama ar OWASP TOP 10 identificēto ievainojamību kopumu pārbaudi.
Pēc iegūtajiem rezultātiem tiks izveidotas testēšanas atskaites, kur detalizēti atspoguļota informācija par testēšanas procesu un sasniegtajiem rezultātiem. Testi ietver tiešsaistes datubāzes izmeklēšanu un adrešu sarakstus, kas ir specifiskas katrai sistēmai un tīklam, kas tiek testēti, izmantojot automatizētus rīkus.

Ievainojamību pārbaudes sagaidāmais rezultāts:

- Pakalpojuma ievainojamības;
- Sistēmas un lietojumprogrammu jauninājumu statuss
- Saraksts ar pakalpojuma novēršamajām ievainojamībām;
- Saraksts ar redzamajām un neredzamajām piekļuves aizsargātajām zonām;
- Saraksts ar faktiskajām ievainojamībām (atņemot "nepamatoti norādītās" (*false positives*)
- Saraksts ar iekšējām vai DMZ sistēmām;
- Saraksts ar elektroniskā pasta, serveru un citiem pieņemtajiem nosaukumiem;
- Tīkla karte (plānojums).

Veicamās darbības:

1. Integrēt testos pašlaik populārākos skenerus un uzlaušanas rīkus;
2. Piemērot mērķa organizāciju pret pašlaik populārākajiem skenēšanas rīkiem;
3. Mēģināt noteikt ievainojamības lietojumprogrammu un sistēmu tipam;
4. Mēģināt atrast pakalpojumu ievainojamības;
5. Mēģināt noteikt lietojumprogrammu un pakalpojumu tipu pēc ievainojamībām;
6. Veikt papildus testēšanu vismaz ar 2 (diviem) automatizētiem ievainojamību noteikšanas rīkiem;
7. Noteikt visas ievainojamības saistībā ar lietojumprogrammatūrām;
8. Noteikt visas ievainojamības saistībā ar operētājsistēmām;
9. Noteikt ievainojamības visām līdzīgām sistēmām, kas arī var radīt ietekmi uz mērķa sistēmām;
10. Verificēt visas ievainojamības, kas noteiktas izpētes laikā (*false positives* un *false negatives*)
11. Verificēt visus pozitīvus.

2.3.2 SERVISU NOLIEGŠANA

Sagaidāmais rezultāts:

- Saraksts ar vājajiem Interneta punktiem;
- Izveidotas bāzlīnijas normālam lietojumam;
- Saraksts ar sistēmas uzvedību pie intensīva lietojuma;
- Saraksts ar DoS testu ievainojamajām sistēmām.

Veicamās darbības:

1. Verificēt, ka administratīvais konts un sistēmas faili un resursi ir pietiekami aizsargāti un ir piešķirts „Least Privilege";
2. Pārbaudīt sistēmas ekspozīcijas ierobežojumus tīkliem, kas uzskatāmi par „non-trusted";

3. Verificēt, ka bāzlīnijas ir nodrošinātas priekš normāla sistēmas lietojuma;
4. Verificēt, kādas procedūras tiek pielietotas, kas reaģē uz neregulārām aktivitātēm;
5. Verificēt reakcijas uz imitētas negatīvas informācijas (propagandas) uzbrukumiem;
6. Veikt serveru un tīkla slodzes testus pie intensīva lietojuma.

2.3.3 INTERNETA LIETOJUMPROGRAMMATŪRAS TESTĒŠANA

Interneta lietojumprogrammatūras testēšanai izmanto dažādas programmatūras testēšanas metodes, lai atrastu serveru/klientu lietojumprogrammatūras drošības kļūdas. Veicamais tests ir pielāgojams jebkurai izstrādātajai lietojumprogrammatūrai, kas izveidota interneta lietojumam, neskatoties kāda programmēšanas valoda vai tehnoloģija tika izmantota.

Sasniedzamais rezultāts:

- Saraksts ar lietojumprogrammām;
- Saraksts ar lietojumprogrammu komponentēm;
- Saraksts ar lietojumprogrammu ievainojamībām;
- Saraksts ar lietojumprogrammu sistēmas uzticamībām (trusts).

Veicamās darbības:

Izstrādes līmeņa izpēte

1. Sadalīt vai dekonstruēt bināro kodu, ja tas ir pieejams;
2. Izmeklēt servera/klienta lietojumprogrammatūras protokola specifikāciju;
3. Izmeklēt programmas loģiku no kļūdu/atkļūdošanas ziņojumiem un programmas uzvedību/sniegumu;

Autentificēšana

4. Atrast iespējamo lietojumprogrammatūras paroļu uzminēšanas piekļuves punktu;
5. Atrast derīgus validēšanās datus (*login*) ar paroļu minēšanu
6. Apiet autentifikācijas sistēmu (*spoofed tokens*);
7. Apiet autentifikācijas sistēmu ar atkārtotu autentifikācijas informāciju (*replay authentification information*);
8. Izpētīt lietojumprogrammatūras loģiku, nosakot kā tās saglabā/uztur autentifikācijas sesijas – secīgu neveiksmju skaitu;
9. Izpētīt lietojumprogrammatūras piekļuves kontroles ierobežojumus – piekļuves atļaujas, pieteikšanās sesijas ilgumu, tukšgaitas ilgumu;

Sesiju vadība

10. Izpētīt sesijas vadības informāciju – vienlaicīgi esošo sesiju skaitu, uz IP bāzētu (*IP-based*) autentifikāciju, uz lomām bāzētu (*role-based*) autentifikāciju, uz identitātes bāzētu (*identity-based*) autentifikāciju, *cookie* lietojumu, sesijas ID URL kodēšanas virkni, sesijas ID apslēptajā HTML lauka mainīgajos un citus;
11. Izpētīt sesijas ID secību un formātu;
12. Izpētīt sesijas ID, kas satur IP adrešu informāciju; pārbaudīt vai attiecīgā sesijas informācija ir atkal iegūstama, izmantojot citu ierīci;
13. Izpētīt sesijas vadības ierobežojumus – joslas platuma lietojumu, failu nolādēšanas/augšupielādēšanas ierobežojumus, transakciju ierobežojumus un citus;
14. Ievākt par daudz informācijas ar tiešu URL, tiešām instrukcijām, *action sequence jumping* un/vai lappušu izlaišanu;
15. Ievākt sensitīvu informāciju, izmantojot *man-in-the-middle* uzbrukumus;
16. Injicēt papildus/viltus/lieku informāciju, izmantojot Sessesion-Hijacking tehnikas;
17. Iegūtās informācijas atkārtota nodošana aplikācijai ar mērķi to apmuļķot

Manipulācija ar datu ievadi

18. Atrast ierobežojumus definētajiem mainīgajiem un protokola vērtumam – datu garums, datu tips, izveides formās un citi;
19. Izmantot izcili garas rakstzīmju virknes, lai atrastu lietojumprogrammatūras bufera pārpildes ievainojamības;
20. Izveidot ķēdes veida savienojumu lietojumprogrammatūras komandu ieejas virknēm;
21. Veikt SQL injekcijas;
22. Veikt *Cross-Site Scripting*;
23. Izmeklēt neatļautu direktoriju/failu piekļuvi ar ceļu/direktoriju, veicot darbības lietojumprogrammatūras ieejas virknēs;
24. Izmantot īpašas URL kodētas/šifrētas virknes, un/vai *Unicode* kodētas/šifrētas virknes, lai apietu lietojumprogrammatūras ievades datu validācijas mehānismus;
25. Izpildīt tālvadības komandas caur *„Server Side Include"*;
26. Veikt manipulācijas ar sesiju/patstāvīgajiem *cookies,* lai apietu vai izmainītu servera (*server-side*) tīmekļa lietojumprogrammatūras loģiku;
27. Veikt manipulācijas ar slēptā lauka mainīgajiem HTML veidlapās, lai apietu vai izmainītu servera (*server-side*) tīmekļa lietojumprogrammatūras loģiku;
28. Veikt manipulācijas ar *„Referrer"*, *„Host"* un citiem HTTP protokolu mainīgajiem, lai apietu vai izmainītu servera (*server-side*) tīmekļa lietojumprogrammatūras loģiku;
29. Izmantot neloģisku/neatļautu datu ievadi, lai pārbaudītu lietojumprogrammatūras kļūdu apstrādes rutīnas un, lai atrastu noderīgus atkļūdošanas/kļūdu lietojumprogrammatūras ziņojumus.

Atbilstošās metodes ietver un vēl papildina Pasūtītāja prasīto testēšanas apjomu. Darba rezultāti tiks sniegti atbilstoši prasītajai trīs līmeņu vērtēšanas sistēmai.

SIA „Analytica" valdes locekle
Iveta Stepanova

z.v.