LATVIJAS
REPUBLIKAS
FINANŠU
MINISTRIJA

Informācijas tehnoloģiju sistēmu auditēšana

Finanšu ministrijas Iekšējā audita departamenta
Ministrijas sistēmu iekšējā audita nodaļā

nodaļas vecākā auditore Jūlija Adamoviča

19.03.2013.

Atziņas no ISACA (*Information Systems Audit and Control Association*) konferences

08.11.2012.

«...97% veiksmīgo uzbrukumu (hakeru / ļaundaru uzbrukumi iestādes informācijas sistēmām) varētu izvairīties ar **vienkāršām vai vidēji sarežģītām kontrolēm**…»

ISACA biedrs – SIA BITI pārstāvis Ēriks Dobelis

Statistika par 2012.gadu IS drošības jomā

FM IAD Ministrijas sistēmu iekšējā audita nodaļas pieredze:

1. IT sistēmu audits

2. Atsevišķu IT jomu pārbaude, veicot citus auditus.

Neatkarīgi no sistēmas (liela, maza, pazīstama, jauna) izpratni par sistēmas darbību auditors iegūst no intervijām, ārējiem / iekšējiem normatīviem aktiem, procedūrām, procesu aprakstiem.

Kur smelties idejas par IT?

Ārējie normatīvie akti, kas nosaka vispārīgās prasības informācijas sistēmas drošībai, t.sk. IT jomā

1. Informācijas tehnoloģiju drošības likums

Likuma mērķis ir uzlabot informācijas tehnoloģiju drošību, nosakot svarīgākās prasības, lai garantētu tādu būtisku pakalpojumu saņemšanu, kuru sniegšanai tiek izmantotas šīs tehnoloģijas.

2. Valsts informācijas sistēmu likums

Likums nosaka vienotu kārtību, kādā veido, reģistrē, uztur, lieto, reorganizē vai likvidē valsts informācijas sistēmas (VIS); regulē VIS pārziņu sadarbību; nosaka VIS turētāja funkcijas un valsts informācijas sistēmas datu subjekta tiesības un pienākumus; regulē VIS drošības pārvaldību; nosaka prasības, kas ievērojamas VIS savietotāju un integrētā VIS ietilpstošo VIS aizsardzībai.

3. Fizisko personu datu aizsardzības likums

Mērķis aizsargāt fizisko personu pamattiesības un brīvības, it īpaši privātās dzīves neaizskaramību, attiecībā uz fiziskās personas datu apstrādi.

4. MK 11.10.2005. noteikumi Nr.765„Valsts informācijas sistēmu vispārējās drošības prasības”

Nosaka VIS vispārējās drošības prasības.

5. MK 01.02.2011. noteikumi Nr.100 «Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība»

Papildus metodika

6. VARAM Informācijas sistēmu drošības pārbaudes vadlīnijas

Definēti valsts iestāžu pārziņā esošās informācijas sistēmu minimālās drošības prasības.

7. Iestādes iekšējie noteikumi IS drošības jomā:

7.1. IS drošības politika;

7.2. Informācijas sistēmu lietošanas kārtības;

7.3. Iekšējie noteikumi par informācijas sistēmas drošību atbildīgajām personām u.c.

FM IAD MSIAN prakse:

«Informācijas tehnoloģiju attīstības plānošana, īstenošana un kontrole»

Audita mērķis - gūt pārliecību, ka: iestādē «XXX» IT iegāde ir lietderīga un orientēta uz iestādes mērķu sasniegšanu; IT izmaksas ir efektīvas; jaunās IT tiek pienācīgi plānotas, ieviestas un kontrolētas.

1.risks: Izdevumi IT attīstībai nav pamatoti un nav lietderīgi.

1.1. kontrole: Tiek identificētas, apkopotas IT nepieciešamības, sistemātiski izvērtētas IT attīstības iespējas, nosakot prioritātes. Izvēlētais IT attīstības variants ir saskaņots ar vadību, vadība apstiprina IT attīstības plānus.

1.2. kontrole: Iepirkuma nodaļa izvērtē iesniegto jauno IT pieprasījumu atbilstību IT stratēģijai, «XXX» resursiem un piedāvā nepieciešamās korekcijas, sagatavojot tehnisko specifikāciju, piedaloties iepirkumu komisijā vai izmantojot jau noslēgtos līgumus ar IT piegādātājiem.

1.3.kontrole: Organizējot iepirkumu, tiek nodrošināta pretendentu piedāvājumu izvērtēšana atbilstoši Publisko iepirkumu likuma noteiktajam prasībām un tiek izvēlēts izdevīgākais piedāvājums.

1.4. kontrole: Tiek nodrošināta lietotāju apmācība.

1.5. kontrole: Tiek nodrošināta IT problēmu savlaicīga risināšana un IT atjaunošana.

2.risks. Jauno IT ieviešana mazina IT drošību «XXX»

2.1.kontrole. IS drošības pārvaldnieks ir iesaistīts jauno IT ieviešanas procesā, vērtējot iespējamus draudus IT videi un reģistrējot jauno IS resursu reģistrā.

2.2.kontrole. Tiek veikta jauno IT testēšana testa vidē, ja tas ir IS drošības pārvaldnieka lēmums.

2.3.kontrole. Tiek kontrolētas pieejas tiesības, ieviešot jauno IT un pēc tam.

Valsts informācijas sistēmu drošības audits

Audita mērķis: Sniegt vadībai pārliecību, ka «XXX» valsts IS atbilst LR normatīvo aktu prasībām un nodrošina informācijas konfidencialitāti, integritāti un pieejamību.

1.Risks. Konfidenciālās informācijas noplūde.

1.1.kontrole. Tiek veikta valsts IS reģistrācija un nepārtraukta valsts IS lietotāju saraksta aktualizācija

1.2. kontrole. Tiek veiktas regulāras pārbaudes iespējamo incidentu atklāšanai un atrisināšanai.

1.3.kontrole. Iegādājoties vai izstrādājot valsts IS vai IS papildinājumu, tiek veikti IS drošības paaugstināšanas preventīvie pasākumi (sākotnēja testēšana, izmaiņu vadība u.c.).

1.4.kontrole. Tiek nodrošināta lietotāju apmācība.

2.risks. IS nav lietderīga uzglabātās informācijas nepilnības dēļ.

2.1.kontrole. Tiek veiktas datu kvalitātes pārbaudes

2.2.kontrole. IS ir ieviesti automātiski datu ievades kontroles mehānismi.

3.risks. IS nav lietderīga datu nepieejamības dēļ.

3.1.kontrole. Ir ieviesti mehānismi valsts IS darba nepārtrauktībai.

3.2.kontrole. Ir ieviests mehānisms tehnisko problēmu savlaicīgai risināšanai.

Darbības nepārtrauktības audits

Audita mērķis: Sniegt vadībai pārliecību, ka «XXX» ir gatavs kritiskā situācijā atjaunot savu darbību optimālā laikā, pamatojoties uz izstrādāto risku analīzes balstīto darbības nepārtrauktības plānu, kas ietver visas iestāžu kritiskās pamatfunkcijas.

1.risks. Kritiskās situācijas gadījumā nav iespējams nodrošināt iestādes pamatfunkciju izpildi.

1.1.kontrole. Tiek veikta risku analīze, identificējot būtiskus iestādes riskus, to iespējamību, sekas un risku mazinošus faktorus.

1.2.kontrole. Ir ieviests vadības apstiprinātais process darbības nepārtrauktības nodrošināšanai iestādē.

1.3.kontole. Tiek veikta Darbības nepārtrauktības plāna atjaunošana, testēšana un atbildīgo darbinieku apmācība.

FM IAD MSIAN pieredze atsevišķu IT jomu pārbaudei

19.03.2013.

Izraksts no auditējamās sistēmas «XXX» analīzes

Iesaistītās puses	Viņu uzdevumi, pienākumi / sistēmas
IS drošības pārvaldnieks	Seko līdzi IS drošības jautājumiem. Atbildīgs, lai informācija, kas tiek apstrādāta iestādē, būtu drošībā. Ir pieejama visa elektroniskā informācija (ko redz administratori)
Darbinieki, kas tiešā veidā apstrādā personu datus (personālvadība, grāmatvedība, apsardze, IT speciālisti)	• Personālvadības jautājumi (personu lieta), • grāmatvedības jautājumi (personas dati, lai aprēķinātu atalgojumu, nodokļus, atvieglojumus, pabalstus u.c.), • personu novērošana (videonovērošanas sistēmas/kameras), • IS un datu bāžu uzturēšana un apkalpošana (IT speciālistiem, kas apkalpo IS, ir iespēja piekļūt pie jebkuriem darbinieka datiem. Informāciju var iegūt gan no darbinieka datora, gan no Interneta, ko darbinieks ikdienā lieto, t.sk.. banku paroles, drošības kodi u.c.). Informācija, kas tiek apstrādāta manuālā veidā (vēstules, sarakste, videonovērošana).
Darbinieki, kas netiešā veidā apstrādā personu datus	Ir gan iekšējās IS, gan xx valsts informācijas sistēmas kurās tiešā/netiešā veidā tiek apstrādāti personu dati, t.sk.: • Iestāde «XXX» – x sistēma (Nosaukums); • Iestāde «XXX» – x sistēmas (nosaukums), • Iestāde «XXX» – x sistēmas; (Nosaukums) • Iestāde «XXX» – x sistēmas (Nosaukums). Katrai sistēmai ir sava specifika un to lietotāju apjoms ir dažāds. Vairumā gadījumos minētajās sistēmās ir iekļauti personu dati, un sistēmas lieto: • XXX un citu iestāžu darbinieki (skatīšanas vai rakstīšanas režīmā: darbam nepieciešamais apjoms atbilstoši kompetencei); • nodokļu maksātāji (skatīšanas vai lietošanas režīmā atbilstoši sistēmas specifikai). Informācija, kas tiek apstrādāta manuālā veidā (vēstules, sarakste). Iekšējās IS personu datu apstrādē XXX un tās padotības iestādēs: • XXX sistēma, kurā ir iekļauti gan tieši ar personu saistīta informācija (personas kods, amats, radinieki, slimības lapas, rīkojumi par amatu, dzīvesvieta, bankas konts u.c.), gan grāmatvedības dati (alga, nodokļi, apgādājamie, bankas konta numurs); • Videonovērošanas sistēma (personu attēls).

FM IAD MSIAN kārtība IA veikšanā:
«…Ja auditējamā funkcija vai process ir saistīts ar VIS vai datu bāzes lietošanu (funkcijas/ procesa īstenošana tiek veikta ar IS/datu bāzes palīdzību), auditors pārliecinās par minēto IS/ datu bāzes loģisko un fizisko aizsardzību»

Nr. p. k.	Prasība / Kritērijs	Jā	Nē	Komentāri (pierādījumi, iemesli)
1.	Uzskaitīt valsts informācijas sistēmas (turpmāk - IS), kuras lieto auditējamā funkcija vai auditējamā procesā.			
2.	Uzskaitīt datu bāzes, kuras lieto auditējamā funkcija vai auditējamā procesā.			
3.	Valsts un iekšējās IS ir reģistrētas atbilstoši tai paredzētai kārtībai (ārējo institūciju apstiprinājums par valsts IS reģistrācijas apliecinājumu; iekšējo IS – iestādes vadītāja apstiprinājums par IS reģistrāciju).			
4.	IS resursus lieto tās personas, kuriem tas ir nepieciešams (rakstīšanas, skatīšanas režīms). Faktiskais lietotāju skaits atbilst iestādes vadītāja apstiprinātā IS resursu reģistrā iekļautai informācijai.			
5.	Tiek nodrošināta IS lietotāju apmācība (pirms pieejas tiesību piešķiršanas, kā arī gadījumos, kad sistēma ir aktualizēta).			
6.	Katram lietotājam ir personiskā unikāla parole.			
7.	IS ir ieviesti automātiski datu ievades kontroles mehānismi (sistēma atpazīst matemātiskas un tehniskās kļūdas), un informē lietotāju par to. Datu ievades process ir izsekojams (var izsekot, kad un kādu informāciju IS lietotājs ir ievadījis).			
8.	Ir identificētas riskantākas jomas IS (lauki, šūnas) - tajos ievadītā informācijas datu kvalitāte tiek pārbaudīta pēc 4 acu principa (atbildīgā persona pārskata un saskaņo informāciju pirms nākošās operācijas uzsākšanas).			
9.	Ja IS informācijai var piekļūt no dienesta portatīvā datora, ir jāpārliecinās, ka ir ieviesti tādi paši drošības pasākumi kā 3.- 8.punktā.			

Atziņas no ISACA konferences (08.11.2012.)

«… IT iet pa priekšu juridiskiem aspektiem..»

Aizsardzības ministrijas pārstāvis

Paldies!