LATVIJAS BANKA
EIROSISTĒMA

K. VALDEMĀRA IELA 2A, RĪGA, LV-1050, LATVIJA. TĀLRUNIS +371 67022300, E-PASTS INFO@BANK.LV, WWW.BANK.LV

Latvijas Bankas Finanšu tehnoloģiju uzraudzības pārvaldes rekomendētais kontrolsaraksts informācijas tehnoloģiju un drošības pārvaldības pašvērtējumam

Pēdējo reizi atjaunots: 02.06.2023.

Šī kontrolsaraksta mērķis ir sniegt atbalstu finanšu tirgus dalībniekiem, lai tie pašu spēkiem varētu novērtēt saskaņā ar Finanšu un kapitāla tirgus komisijas 2020. gada 8. septembra normatīvajiem noteikumiem Nr. 150 "Informācijas tehnoloģiju un drošības risku pārvaldības normatīvie noteikumi" (turpmāk – Noteikumi Nr. 150) saistošo prasību izpildi un ieviesto kontroļu esību informācijas tehnoloģiju (turpmāk – IT) un drošības pārvaldības procesos.

Saskaņā ar Noteikumu Nr. 150 3. punktu tirgus dalībnieks, ieviešot drošības pasākumus, ievēro proporcionalitātes principu un uz risku izvērtējumu balstītu pieeju, ņemot vērā konkrētā tirgus dalībnieka lielumu, darbības jomu, sarežģītību, riska pakāpi un pakalpojumus, kurus tas sniedz vai plāno sniegt. Apdrošināšanas un pārapdrošināšanas starpnieki un reģistrētie alternatīvo ieguldījumu fondu pārvaldnieki ievieš tās Noteikumu Nr. 150 prasības, kuras par nepieciešamām atzītas konkrētā tirgus dalībnieka aktuālajā IT risku analīzē.

Tirgus dalībnieks var izmantot kontrolsarakstā iekļautos jautājumus atbilstoši esošajam organizācijas IT un drošības pārvaldības procesu spēju brieduma līmenim un IT risku analīzē identificēto risku līmeņiem.

SATURA RĀDĪTĀJS

IT pārvaldības procesa apgabals	Risks, kas var iestāties nepietiekamas kontroles gadījumā	Ar esošās kontroles novērtējumu saistītie jautājumi	Atsauce uz Noteikumiem Nr. 150
VADĪBAS ATBILDĪBA UN ATBALSTS	*Ja nav noteikta atbildība par IT drošību un skaidri aprakstīti veicamie pienākumi, kā arī nav piešķirti IT drošības nodrošināšanai nepieciešamie resursi, tad pastāv risks, ka IT drošības risku iestāšanās dēļ var tikt apdraudēta organizācijas biznesa mērķu sasniegšana.*	• Vai organizācijas vadība ir noteikusi atbildīgo par IT drošību (organizācijas darbinieks vai ārpakalpojuma sniedzējs) un apņēmusies nodrošināt IT drošībai nepieciešamos resursus (finanses, cilvēku un tehniskie resursi)? • Kādi pienākumi ir deleģēti atbildīgajam par IT drošību? • Vai atbildīgajam par IT drošību ir nepieciešamās zināšanas un kompetence deleģēto pienākumu veikšanai? • Kādas aktivitātes atbildīgais par IT drošību īsteno savas kompetences celšanai? Vai organizācijas vadība sniedz tam nepieciešamo atbalstu?	Sadaļas 3.1. Vadības atbildība un atbalsts, 3.3. Informācijas drošības funkcija
ĀRPAKALPOJUMU VADĪBA	*Ja netiek pārvaldīti organizācijas ārpakalpojumi un no tiem izrietošie riski saistībā ar nedrošu IT izmantošanu un ierobežotas pieejamības informācijas neatbilstošu apstrādi, tad var ne tikai tikt apdraudēta organizācijas informācijas un tehnisko resursu drošība, bet arī drošības incidenta*	• Vai organizācija ir identificējusi funkcijas, kuras ir nodotas ārpakalpojumā un kuru ietvaros tiek izmantotas IT, kā arī tiek veikta ierobežotas pieejamības informācijas apstrāde? • Vai organizācija ir noslēgusi rakstveida vienošanos ar visiem ārpakalpojumu sniedzējiem par sniegtā ārpakalpojuma tvērumu un noteikusi pakalpojuma kvalitātes un drošības prasības ?	3.5. Ārpakalpojumu vadība

	rezultātā nodarīts kaitējums tās reputācijai.	• Kādas ir organizācijas iespējas nomainīt attiecīgos ārpakalpojumu sniedzējus vai arī pārņemt atpakaļ ārpakalpojumā nodotās funkcijas ? • Vai ir identificēti apakšuzņēmēji, kuri sadarbojas ar ārpakalpojumu sniedzējiem attiecīgo ārpakalpojumu nodrošināšanā, un šāda sadarbība izriet no līguma nosacījumiem? • Ja ārpakalpojumu ietvaros tiek izmantoti mākoņpakalpojumi, vai ir zināms, kurās valstīs tiek apstrādāta un glabāta organizācijas informācija? • Ja ar organizācijas klientiem saistītā informācija tiek apstrādāta trešajās valstīs, vai ir veikts ietekmes novērtējums saistībā ar fizisko personu datu apstrādi? • Vai ārpakalpojumu sniedzēji nodrošina datu rezerves kopēšanu sniegto mākoņpakalpojumu ietvaros? • Vai organizācija pati nodrošina vai organizē savu datu rezerves kopiju izveidi informācijai, kas tiek apstrādāta mākoņpakalpojumu ietvaros?	
RISKU PĀRVALDĪBA	*Ja organizācijā nav identificēti ārējie un iekšējie apdraudējumi un ar tiem saistītās IT drošības nepilnības un trūkumi, var iestāties neplānoti IT drošības riski, jo organizācija savlaicīgi nebūs veikusi visas*	• Vai organizācija ir noteikusi atbildīgo par IT drošības risku pārvaldības procesa nodrošināšanu? Kādi vēl ieinteresēto pušu pārstāvji tiek iesaistīti risku novērtēšanas procesā? • Kā organizācijā tiek īstenots IT drošības risku novērtēšanas process, un kāda metodoloģija	4. Risku pārvaldība 4.1. Organizācija un mērķi 4.3. Risku novērtējums un risku mazināšana

	nepieciešamās aktivitātes šādu risku pārvaldībai.	tiek izmantota šajā nolūkā? Vai izvēlētā metodoloģija ir apstiprināta un tiek nodrošināta konsekvence tās lietošanā? • Vai pēc risku analīzes veikšanas tiek sagatavots identificēto IT drošības risku pārvaldības plāns, ko apstiprina organizācijas vadība ? • Vai IT drošības risku pārvaldības plānā ir sniegta informācija par norādīto aktivitāšu prioritātēm, atbildīgajiem un izpildes termiņiem? • Kādos gadījumos un cik bieži tiek paredzēts veikt atkārtotu IT drošības riska novērtējumu? • Kā par nepieciešamajām aktivitātēm un noteiktajiem pienākumiem saskaņā ar IT drošības risku pārvaldības plānā noteikto tiek ikdienā komunicēts ar atbildīgajiem darbiniekiem ? • Kā tiek nodrošināta pārējo organizācijas darbinieku izpratnes veicināšana par identificētajiem IT drošības riskiem un sekām to iestāšanās gadījumā?	
RESURSU UZSKAITE UN KLASIFIKĀCIJA	*Ja organizācija nav identificējusi savus klasificētos informācijas resursus un to lietotājus, tad pastāv risks, ka organizācijas informācijas resursi var netikt atbilstoši aizsargāti pret nesankcionētu piekļuvi.*	• Vai organizācija ir identificējusi ar savām funkcijām saistītos informācijas resursus un klasificējusi tos pēc nozīmības? • Vai organizācija ir identificējusi par informācijas resursiem atbildīgās personas un rakstveidā deleģējusi tās veikt noteiktus resursu turētāja pienākumus?	4.2. Resursu uzskaite un klasifikācija, 48. punkts

		• Vai informācija par organizācijas informācijas resursiem un to turētājiem ir apkopota, un kas organizācijā ir atbildīgs par tās aktualizāciju?	
	Ja organizācija nav identificējusi ar tās klasificētajiem informācijas resursiem saistītos tehniskos resursus un par to uzturēšanu atbildīgās personas, tad pastāv risks, ka organizācijas tehniskie resursi var netikt atbilstoši aizsargāti pret nesankcionētu piekļuvi.	• Vai ir identificēti ar organizācijas klasificētajiem informācijas resursiem saistītie tehniskie resursi un veikta to klasifikācija? • Vai organizācija ir identificējusi par tehniskajiem resursiem atbildīgās personas un rakstveidā deleģējusi tās veikt noteiktus resursu turētāja pienākumus? • Vai informācija par organizācijas tehniskajiem resursiem un to turētājiem ir apkopota, un kas organizācijā ir atbildīgs par tās aktualizāciju?	4.2. Resursu uzskaite un klasifikācija 49. punkts
	Ja organizācija nespēj identificēt savu tehnisko resursu atrašanās vietu, kā arī attiecīgos to lietotājus, tad pastāv risks, ka organizācijas tehniskie resursi var tikt izmantoti neatbilstošā veidā, zaudēti vai arī nonākt organizācijai nepiederošu personu rīcībā.	• Kāda ir noteiktā kārtība attiecībā uz tehnisko resursu piešķiršanu darbiniekiem un to nodošanu atpakaļ organizācijai? Kurš organizācijā ir atbildīgs par šī procesa uzraudzību ? • Vai organizācijas tehniskie resursi tiek regulāri uzskaitīti un jebkurā brīdī iespējams identificēt personas, kuru lietojumā atrodas organizācijas datortehnika un citas ierīces ? • Vai organizācija ir informēta par to, kādi organizācijai piederoši tehniskie resursi atrodas darbinieku lietojumā, tiem strādājot attālināti?	4.2. Resursu uzskaite un klasifikācija 44. punkts

		• Vai organizācija nodrošina darbiniekiem nepieciešamo tehnisko atbalstu tiem piešķirtās datortehnikas un citu ierīču uzturēšanai, lai tiktu nodrošināta pilna to funkcionalitāte un atbilstoša darbība, saskaņā ar organizācijā noteikto IT drošības līmeni (pretvīrusu programmatūra, drošības atjauninājumi u. tml.)?	
INFORMĀCIJAS DROŠĪBAS POLITIKA	*Ja nav skaidri formulēts noteikumu mērķis, pastāv risks, ka var netikt nodrošināts nepieciešamais drošības līmenis, lai spētu atbilstoši aizsargāt organizācijai vērtīgo informāciju un tehnoloģijas.*	• Vai organizācijas vadība ir oficiāli apstiprinājusi noteikumus ? • Kāds ir noteikumos norādītais mērķis, un vai organizācijas vadībai ir skaidra izpratne par to? • Vai noteikumi ir veidoti saskaņā ar Noteikumu Nr. 150 prasībām un veicina tajos noteikto prasību ievērošanu? • Kam ir saistoši organizācijas izdotie noteikumi, un kādi pienākumi ir deleģēti noteikumos norādītajām pusēm? • Vai noteikumos ir norādīts, cik bieži un kādos apstākļos notiek to pārskatīšana un kurš organizācijā ir atbildīgs par to?	5.1. Informācijas drošības politika
	Ja darbinieki, darbuzņēmēji un ārpakalpojuma sniedzēji netiek iepazīstināti ar prasībām, kas jāievēro, izmantojot IT, tad pastāv risks, ka tās var tikt izmantotas neprasmīgi un neatbilstoši noteiktajam drošības līmenim, un tādējādi var tikt apdraudēta	• Kādos iekšējos dokumentos ir noteiktas organizācijas IT lietošanas prasības, un kam un kādos apstākļos ir pienākums tās ievērot? • Kā šīs atbildīgās puses tiek iepazīstinātas ar attiecīgo noteikumu saturu? Vai tiek skaidri noteikts, kādas tieši darbības ir kategoriski aizliegts veikt ar organizācijas informācijas un tehniskajiem resursiem	

	organizācijas informācijas un tehnisko resursu drošība.	(piemēram, kaitnieciska vai neatļauta satura izplatīšana un lejupielāde, nodošana lietojumā organizācijai nepiederošām personām, patvaļīga programmatūras instalēšana un aparatūras demontāža u. c.)?	
PIEEJAS TIESĪBU VADĪBA	*Ja organizācija nekontrolē pieejas tiesību saviem informācijas un tehniskajiem resursiem piešķiršanu un to, kādā apjomā piekļuve tiek nodrošināta, tad pastāv neautorizētu darbību un informācijas noplūdes risks.*	• Vai organizācijā jauna IT sistēmas lietotāja reģistrācija, tiesību piešķiršana, anulēšana un bloķēšana tiek veikta saskaņā ar dokumentētu pieprasījumu? Kā organizācija to ir noteikusi? • Vai tiek nodrošināts, ka lietotājam piekļuves tiesības tiek piešķirtas tikai tādā apjomā, kāds nepieciešams tiešo pienākumu izpildei (tiek ievērota labā prakse jeb "*least privilege principle*")? • Vai tiek nodrošināts, ka lietotājiem netiek piešķirta piekļuve resursiem, kurus nav paredzēts izmantot darba vajadzībām (tiek ievērota labā prakse jeb "*deny by default*")? • Vai organizācija uztur dokumentētu informāciju (lietotāju tiesību kartējumu), kas atspoguļo visu informācijas un tehnisko resursu un to lietotāju uzskaitījumu – kam un kādā apjomā lietotāja tiesības ir piešķirtas? Cik bieži šī informācija tiek pārskatīta, un kam ir pienākums to veikt?	5.3. Pieejas tiesību vadība

	Ja organizācija neveic pastiprinātu to lietotāju uzraudzību, kam tiek piešķirtas privileģētas lietošanas tiesības (IT administratori), un nav ieviesusi risku mazināšanas pasākumus atbilstoši identificētajam riska līmenim, tad šādi lietotāji, kas spēj neierobežoti piekļūt un brīvi rīkoties ar organizācijas informācijas un tehniskajiem resursiem, var kļūt par būtisku iekšējo apdraudējumu organizācijai gan cilvēka kļūdas, gan ļaunprātīgas rīcības gadījumā, t. sk. no IT administratoriem un ārpakalpojumu sniedzēju puses.	• Vai organizācija ir identificējusi visus IT un informācijas sistēmu (turpmāk – IS) lietotājus, kam ir piešķirtas privileģētas lietošanas tiesības ? • Kā organizācija nodrošina un ierobežo privileģēto tās informācijas un tehnisko resursu lietotāju tiesību piešķiršanu? • Kādi risku mazināšanas pasākumi ir ieviesti organizācijā privileģēto lietotāju tiesību ierobežošanai (pienākumu sadale starp vairākiem administratoriem, dalītās paroles u. c.)? • Kā organizācija nodrošina privileģēto lietotāju veikto darbību uzraudzību un šī procesa neatkarību (IT un IS administratori neuzrauga paši sevi)?	
LIETOTĀJA AUTENTISKUMA NOTEIKŠANA	*Ja nav iespējams identificēt katra IT un IS lietotāja veiktās darbības, tad pastāv risks, ka nesankcionētas piekļuves dēļ var tikt apdraudēta organizācijas IT drošība.*	• Vai organizācija nodrošina, ka katram IT lietotājam un administratoram tiek piešķirts unikāls lietotāja vārds? • Vai un kā organizācija ir noteikusi, ka darbiniekiem netiek atļauta citu fizisku personu lietotāju kontu izmantošana? • Ja pastāv izņēmuma situācijas, kad vienu lietotāja kontu izmanto vairāki darbinieki, kā tiek mazināti riski, kas rodas šāda konta koplietošanas gadījumā ? • Ja organizācijā izmanto arī tehnoloģiskos kontus, tad kā tiek nodrošināts, lai tos nevarētu izmantot fiziskas personas?	5.2. Lietotāja autentiskuma noteikšana

	Ja ieviestie lietotāju autentifikācijas līdzekļi nav pietiekami droši un efektīvi, tad pastāv risks, ka organizācijai nepiederošām personām izdosies salīdzinoši viegli iegūt leģitīmu lietotāju identitātes datus, lai nesankcionēti piekļūtu organizācijas tehniskajiem un informācijas resursiem.	• Vai visi lietotāju konti ir aizsargāti ar drošu paroli? Kādas prasības organizācija nosaka paroļu drošībai un to veidošanai? • Kādas prasības un kādā veidā tiek noteikts ievērot IT un IS lietotājiem attiecībā uz paroļu drošu lietošanu un uzglabāšanu (nedrīkst saglabāt paroles pārlūkprogrammā, pierakstīt un uzglabāt redzamā vietā, nedrīkst izpaust citiem lietotājiem u. c.)? • Vai organizācijas IT un IS ir iespējams ieviest un lietot vairāku faktoru autentifikāciju, un kādos gadījumos darbiniekiem ir pienākums to obligāti izmantot (attālinātais darbs, paroles nomaiņa, mākoņpakalpojumi u. tml.)?	
	Ja organizācijas IT administratoru autentifikācijas līdzekļiem netiek piemērotas drošības prasības atbilstoši identificētajam riska līmenim, tad pastāv risks, ka to drošības apdraudējuma īstenošanās gadījumā var tikt iegūta nesankcionēta un neierobežota piekļuve organizācijas tehniskajiem un informācijas resursiem, radot būtiskus draudus organizācijas drošībai.	• Kādas minimālās drošības prasības ir noteiktas privileģēto lietotāju kontu drošībai (atšķirīgs paroles garums, obligāta vairāku faktoru autentifikācijas lietošana u. c.)? • Vai ir identificēti iespējamie apdraudējumi saistībā ar IT administratoru kontu pārvaldību un veikti nepieciešamie ierobežojošie pasākumi? • Vai datortehnikas gala lietotājiem ir liegta pieeja attiecīgās iekārtas lokālā administratora kontam?	

DATU NESĒJU FIZISKĀ AIZSARDZĪBA	*Ja organizācija nenodrošina informācijas klasifikācijai atbilstošus drošības pasākumus, tad pastāv risks, ka atbilstības prasību neievērošanas rezultātā var tikt nopludināta, bojāta vai neatgriezeniski zaudēta organizācijai nozīmīga informācija, kā arī nodarīti materiālie zaudējumi vai kaitējums organizācijas reputācijai.*	• Kā organizācija regulē ārējo datu nesēju lietošanu, un kādas prasības tiek noteiktas to aizsardzībai pret nesankcionētu piekļuvi, ja tajos paredzēts glabāt klasificētu informāciju? • Vai organizācija ir ieviesusi aizsardzības pasākumus portatīvo datoru un mobilo ierīču datu nesēju aizsardzībai, ja pastāv iespēja uzglabāt tajos klasificēto informāciju? Vai ir aizliegta zibatmiņas karšu izmantošana darbstacijās? • Vai organizācija nodrošina nepieciešamos aizsardzības pasākumus arī papīra formātā esošas informācijas aizsardzībai pret nesankcionētu piekļuvi (papīra izdrukas koplietošanas iekārtās, slēdzami skapji, tīrā galda politika u. c.)?	5.5. Datu nesēju fiziskā aizsardzība
IT OPERĀCIJU DROŠĪBA	*Ja organizācija savlaicīgi neveic nepieciešamos pasākumus tehnisko resursu ievainojamību pārvaldībai, tad nepietiekamas drošības kontroles vai tās neesības dēļ var tikt apdraudēta organizācijas drošība.*	• Kas organizācijā ir atbildīgs par tehnisko resursu ievainojamību savlaicīgu identificēšanu un novēršanu? • Kam un kā organizācija ir deleģējusi pienākumus saistībā ar savlaicīgu organizācijas tehnisko resursu programmatūras atjauninājumu uzstādīšanu, un kurš ir atbildīgs par šī procesa uzraudzību ? • Kādas aktivitātes un ar kādu regularitāti organizācija veic tehnisko resursu ievainojamību identificēšanai, un kādi rīki tiek izmantoti šajā nolūkā?	5.6. IT operāciju drošība

		• Kā tiek organizēta identificēto drošības ievainojamību novēršana, un kā tiek nodrošināta šī procesa norises kontrole? • Ja organizācijā tiek gatavoti kādi pārskati par identificētajām drošības ievainojamībām un to novēršanai nepieciešamajām darbībām, kam un ar kādu nolūku tie tiek iesniegti?	
	Ja netiek veikta organizācijas tehnisko resursu konfigurācijas pārvaldība, tad pastāv risks, ka var tikt identificētas iekārtu konfigurācijas nepilnības un trūkumi, kuri var tikt izmantoti, lai ietekmētu tehnisko resursu drošību.	• Kā un kam organizācija ir deleģējusi pienākumu veikt aktivitātes saistībā ar tehnisko resursu iestatīšanu un tajos nepieciešamo izmaiņu veikšanu? • Kur un kādi minimālie drošības kritēriji ir noteikti iekārtu konfigurācijai ? • Vai tehnisko resursu konfigurācijas statusa informācija tiek dokumentēta? • Vai konfigurācijas pārvaldības procesā tiek izmantoti arī automatizēti tehniskie risinājumi? • Kam ir deleģēts pienākums veikt tehnisko resursu konfigurācijas pārbaudi, lai identificētu iespējamās drošības nepilnības vai trūkumus? Cik bieži šī pārbaude jāveic?	
DATORTĪKLU AIZSARDZĪBA	*Ja netiek nodrošināta pietiekama organizācijas datortīklu aizsardzība, tad pastāv risks, ka var tikt apdraudēti organizācijas informācijas un tehniskie resursi un ietekmēta organizācijas drošība.*	• Vai organizācija ir identificējusi, kādas iekārtas tiek izmantotas tās datortīklu darbības nodrošināšanai un kā tās tiek aizsargātas pret nesankcionētu piekļuvi? • Kurš organizācijā veic šo iekārtu tehnisko uzturēšanu un darbības uzraudzību? • Kādas iekārtas un tehniskie risinājumi tiek izmantoti datu plūsmas aizsardzības	5.7. Datortīklu aizsardzība

		nodrošināšanai, un kam ir tiesības mainīt šo iekārtu vai risinājumu konfigurāciju? • Vai informācija par organizācijas datortīkliem un to organizēšanu tiek dokumentēta, un kurš ir atbildīgs par šīs dokumentācijas uzturēšanu?	
PERSONĀLO DATORU UN IERĪČU AIZSARDZĪBA	*Ja organizācija nespēj identificēt savu darbinieku privātos tehniskos resursus un šo resursu lietotājus, kā arī to, kādam nolūkam šādi tehniskie resursi tiek lietoti, tad pastāv risks, ka nepietiekamu IT drošības aizsardzības pasākumu dēļ organizācijai var tikt radīts drošības apdraudējums.*	• Vai organizācijas darbinieku privātie tehniskie resursi, kam ir piekļuve organizācijas IT infrastruktūrai un informācijas resursiem, ir uzskaitīti un ir iespējams identificēt personas, kuru lietojumā tie atrodas ? • Kāda ir noteiktā kārtība darbinieku privāto tehnisko resursu izmantošanai organizācijā? Kurš organizācijā ir atbildīgs par šāda lietojuma saskaņošanu un veic regulāru uzraudzību ? • Kā organizācija gūst pārliecību par darbinieku privātās datortehnikas un ierīču atbilstību organizācijā noteiktajām drošības prasībām, lai tiktu nodrošināts, ka organizācijā netiek lietoti iekšējam regulējumam neatbilstoši tehniskie resursi? • Kam ir deleģēts pienākums veikt šādu ierīču sākotnējo praktisko pārbaudi, kā arī īstenot regulārās pārbaudes?	5.8. Personālo datoru un ierīču aizsardzība

	Ja organizācija nav noteikusi kārtību, kādā darbiniekiem ir atļauts izmantot savu privāto datortehniku un citas ierīces, tad pastāv risks, ka nepietiekamu drošības pasākumu dēļ var rasties drošības incidenti, kas var būtiski ietekmēt organizācijas darbību un funkciju nodrošināšanu.	• Kā organizācija regulē tās darbinieku privāto tehnisko resursu lietošanu? Kā organizācijas darbinieki tiek iepazīstināti ar šo kārtību? • Vai kārtībā ir noteikts, kādus informācijas resursus un kādos tehniskajos resursos ir atļauts glabāt un kādas prasības nepieciešams piemērot to aizsardzībai pret nesankcionētu piekļuvi (šifrējot u. tml.)? • Vai tiek noteikts, ka, lietotājam atstājot datoru bez uzraudzības, atsākt datora izmantošanu iespējams tikai tad, ja ir veikta lietotāja autentifikācija (piemēram, jāievada parole)? • Vai ir noteikts, ka darbinieku privātajai datortehnikai un ierīcēm, kas tiek izmantotas piekļuvei organizācijas IT infrastruktūrai un informācijas resursiem, ir jābūt aprīkotām ar pretvīrusu programmatūru un datorprogrammās jābūt uzstādītiem jaunākajiem drošības atjauninājumiem? • Vai tiek skaidri noteikts, kādas tieši darbības darbiniekiem ir kategoriski aizliegts veikt ar privātajiem resursiem, ja tie tiek lietoti piekļuvei organizācijas IT infrastruktūrai un informācijas resursiem (piemēram, kaitnieciska vai neatļauta satura izplatīšana un lejupielāde, nodošana lietojumā organizācijai nepiederošām personām, kādas noteiktas programmatūras instalēšana u. c.)? • Vai organizācija sniedz darbiniekiem nepieciešamo tehnisko atbalstu, lai nodrošinātu	

		privātās datortehnikas un ierīču atbilstošu lietojumu, saskaņā ar noteikto IT drošības līmeni organizācijā (pretvīrusu programmatūra, drošības atjauninājumi u. tml.)?	
INFORMĀCIJAS DROŠĪBAS APMĀCĪBA UN DROŠĪBAS APZINĀŠANĀS VEICINĀŠANA	*Ja organizācijā nav ieviesta informācijas drošības izpratnes veicināšanas programma, lai nodrošinātu, ka organizācijas darbinieki tiek sistemātiski izglītoti par organizācijā noteikto IT drošības kārtību un atbilstošas IT lietošanas prasībām, kā arī par aktuālajiem IT drošības apdraudējumiem un riskiem, tad pastāv risks, ka darbinieku nepietiekamas drošības izpratnes un iekšējam regulējumam neatbilstošas rīcības rezultātā organizācijai var tikt radīti iekšējie drošības apdraudējumi.*	• Vai organizācijas vadība ir noteikusi atbildīgo par informācijas drošības izpratnes veicināšanas apmācības organizēšanu un nodrošina tam nepieciešamos resursus? • Kā un ar kādu regularitāti tiek īstenota šī organizācijas darbinieku izglītošana informācijas drošības jautājumos, lai mazinātu personāla kļūdas, krāpšanu, resursu ļaunprātīgu izmantošanu vai citu veidu apdraudējumus ? • Kurš ir atbildīgs par apmācības satura nodrošināšanu, un kādas tēmas ir obligāti iekļautas informācijas drošības izpratnes veicināšanas programmā? Kā un cik bieži notiek satura pārskatīšana? • Vai apmācības laikā darbinieki tiek informēti par to, kā reaģēt, sastopoties ar dažādu veidu apdraudējumiem (jo īpaši sociālās inženierijas), lai nepieļautu organizācijā noteiktās drošības kārtības pārkāpumus? • Kā ar apmācības palīdzību tiek veicināta darbinieku izpratne par tādu situāciju atpazīšanu, kas varētu būt drošības notikumi vai incidenti, lai par to tiktu operatīvi informēti atbildīgie organizācijas darbinieki?	5.11. Informācijas drošības apmācība un drošības apzināšanās veicināšana

		• Vai organizācijā tiek īstenota kādu noteiktu mērķa grupu izglītošana tieši tām specifiskajos informācijas drošības jautājumos – organizācijas vadība, darbinieku tiešie vadītāji, informācijas un tehnisko resursu turētāji?	
	Ja netiek veikta regulāra organizācijas darbinieku zināšanu pārbaude informācijas drošības jomā, tad pastāv risks, ka organizācija nespēs nodrošināt nepieciešamo IT drošības līmeni un savlaicīgi gūt pārliecību par nepietiekamu organizācijas darbinieku izpratni kādos tai būtiskos informācijas drošības jautājumos.	• Kā un ar kādu regularitāti tiek nodrošināta organizācijas darbinieku zināšanu pārbaude informācijas drošības izpratnes jautājumos? • Vai organizācijā tiek veiktas kādas papildu izglītojošās aktivitātes darbiniekiem ar zemu sniegumu informācijas drošības zināšanu pārbaudes testos ? • Vai darbiniekiem tiek veiktas apmācības kampaņas un testi par pikšķerēšanu?	
		• Kā tiek nodrošināta esošās informācijas drošības izpratnes veicināšanas programmas satura salāgošana ar organizācijas noteikto IT drošības līmeni un darbinieku zināšanu pārbaužu laikā identificētajiem riskiem?	

AUDITĀCIJAS PIERAKSTU PĀRVALDĪBA	*Ja netiek nodrošināta IS lietotāju veikto darbību reģistrēšana auditācijas pierakstos, tad nav iespējams pārliecināties, kad un kādas darbības ir veiktas informācijas sistēmā, tai pieslēdzoties ar konkrētajam lietotājam atļauto piekļuves veidu un pilnvērtīgi īstenot informācijas drošības uzraudzību organizācijā.*	• Vai visām IS, kas tiek izmantotas informācijas apstrādei, tiek veidoti auditācijas pieraksti? • Vai auditācijas pierakstiem reģistrētā informācija tiek saglabāta vienā vai vairākās vietās? Vai auditācijas pieraksti tiek aizsargāti? • Kāda informācija pēc noklusējuma tiek saglabāta IS auditācijas pierakstos? • Kāda veida informāciju vēl būtu nepieciešams reģistrēt, lai pastiprinātu uzraudzību ? • Par kādu laika periodu tiek nodrošināta informācijas saglabāšana auditācijas pierakstos? Vai tas ir noteikts arī kādā iekšējā dokumentā? • Ja auditācijas pierakstu failā(-os) esošā informācija tiek dzēsta pakāpeniski, aizstājot to ar jauno informāciju, vai iespējams, ka var tikt zaudēta informācija arī par tādām IS veiktajām darbībām, kas ietilpst noteiktajā uzraudzības periodā? • Vai nepastāv tāds maksimālais auditācijas pierakstu faila(-u) lieluma ierobežojums, kas rada manuālas iejaukšanās nepieciešamību uzraudzības periodā ietilpstošo ierakstu zaudēšanas riska novēršanai?	6.2. Auditācijas pierakstu pārvaldība

	Ja netiek nodrošināta regulāra auditācijas ierakstu pārskatīšana, lai īstenotu IS lietotāju veikto darbību uzraudzību, pastāv risks, ka savlaicīgi var netikt atklāti drošības pārkāpumi un incidenti un var tikt apdraudēta organizācijas informācijas drošība.	• Vai ir noteikta atbildība par auditācijas pierakstu pārskatīšanu? • Vai atbildīgajam ir nepieciešamās prasmes un kompetence, lai spētu kvalitatīvi veikt šādus pienākumus? • Ar kādu regularitāti tiek pārskatīti auditācijas pieraksti? • Vai ir ieviesti kādi tehniskie risinājumi, lai atvieglotu darbu ar auditācijas pierakstu uzraudzību un pārskatīšanu? • Kā tiek nodrošināta auditācijas pierakstu uzraudzības procesa kontrole, un kurš organizācijā it atbildīgs par to?	
	Ja netiek nodrošināta auditācijas pierakstu droša uzglabāšana, pastāv risks, ka drošības pārkāpuma vai incidenta gadījumā tie var tikt koriģēti vai izdzēsti un nebūs iespējams rekonstruēt lietotāju veiktās darbības ar IS un tehnoloģijām.	• Vai organizācijā ir identificētas visas personas, kurām iespējams piekļūt IS auditācijas pierakstiem, lai veiktu tādas manipulācijas ar tiem, kas ietekmē informācijas drošību? • Vai IS nav izveidoti tādi privileģēto lietotāju konti, kuru īpašniekiem pēc noklusējuma ir tiesības piekļūt auditācijas pierakstu saturam, un šādus kontus vienlaikus mēdz lietot vairākas personas? • Vai organizācijā ir ieviestas tādas drošības uzraudzības sistēmas, kas reģistrē aizdomīgas lietotāju darbības ar auditācijas pierakstiem, un vai šādos gadījumos var nekavējoties ziņot par procesa uzraudzību atbildīgajiem?	

		Vai pastāv iespēja dzēst auditācijas pierakstus tādā veidā, ka nav iespējams identificēt lietotāju, kas to izdarījis? • Vai tiek nodrošināta auditācijas pierakstu kopiju veidošana un to aizsardzība pret nesankcionētu piekļuvi? Kurš organizācijā ir atbildīgs par to? • Vai organizācija zina, kur tiek glabātas auditācijas pierakstu kopijas un kādā veidā tām iespējams piekļūt?	
DATU REZERVES KOPĒŠANA	*Ja netiek nodrošināta regulāra datu rezerves kopiju veidošana, pastāv risks, ka drošības incidenta, kā arī tehniskas kļūmes vai cilvēka kļūdas rezultātā var tikt neatgriezeniski zaudēta organizācijai vērtīga informācija un nodarīti gan materiālie zaudējumi, gan kaitējums reputācijai, kā arī ietekmēta organizācijas biznesa mērķu sasniegšana.*	• Vai ir identificēta vērtīgā informācija, kuras zaudēšanas gadījumā var tikt apgrūtināta, apturēta vai kā citādi ietekmēta organizācijas darbība un tai nodarīti materiālie zaudējumi vai kaitējums reputācijai? • Kā (manuāli vai automātiski), kādā veidā (visu datu vai tikai mainīto datu kopijas) un ar kādu biežumu tiek veidotas organizācijai nepieciešamās datu rezerves kopijas, un vai organizācija tam ir nodrošinājusi vajadzīgos tehniskos resursus? • Vai organizācija ir noteikusi atbildīgo par datu rezerves kopiju veidošanu? • Kā tiek īstenota datu rezerves kopēšanas procesa uzraudzība, un kurš organizācijā ir atbildīgs par to?	6.3. Datu rezerves kopēšana

	Ja netiek nodrošināta regulāra iegūto datu rezerves kopiju kvalitātes pārbaude, tad pastāv risks, ka nepieciešamības gadījumā var izrādīties neiespējami atjaunot organizācijai nozīmīgu informāciju, ja datu rezerves kopēšanas laikā notikusi tehniska kļūme vai pieļautas cilvēka kļūdas.	• Vai organizācija ir noteikusi kādam atbildību par datu rezerves kopiju kvalitātes pārbaudes veikšanu? • Kā un cik bieži tiek īstenota datu rezerves kopiju kvalitātes pārbaude? Vai atjaunošanas process ir dokumentēts? • Kāda rīcība tiek paredzēta, ja pārbaudīto datu kopiju kvalitāte izrādās neatbilstoša vai datu atjaunošana no kopijām nav iespējama?	
	Ja netiek gūta pārliecība par to, kādā laikā iespējams īstenot informācijas atjaunošanu no datu rezerves kopijām, tad pastāv risks, ka nebūs iespējams savlaicīgi nodrošināt organizācijas darbības nodrošināšanai nozīmīgu informāciju un var tikt ietekmēta organizācijas biznesa mērķu sasniegšana.	• Vai organizācijai ir zināms maksimāli pieļaujamais laika intervāls, kurā var tikt pieļauti neplānoti pārtraukumi tās biznesa procesos, jo nav pieejama attiecīgo funkciju nodrošināšanai nepieciešamā informācija un nestrādā IS? • Vai ir zināms, kādā laika intervālā iespējams veikt informācijas atjaunošanu no datu rezerves kopijām, lai spētu nodrošināt organizācijas darbību iepriekš neplānota pārtraukuma gadījumā? Vai ir noteikts maksimālais laiks, kurā sistēma vai process jāatjauno pēc negadījuma, jeb RTO un maksimālais laika	

		periods, par kuru var zaudēt datus negadījuma rezultātā, jeb RPO? • Kad un cik bieži tiek īstenotas pārbaudes, lai gūtu pārliecību, ka organizācija spēj nodrošināt tās informācijas atjaunošanu no rezerves kopijām, iekļaujoties maksimāli pieļaujamā dīkstāves laika intervālā? Vai tiek sagatavoti testa protokoli? • Kam ir deleģēta atbildība par šāda veida pārbaužu veikšanu, un kādiem vēl organizācijas pārstāvjiem ir pienākums piedalīties šajā procesā?	
	Ja datu rezerves kopijas netiek uzglabātas droši, lai pasargātu tās no vides riskiem (plūdi, ugunsgrēks u. tml.), kiberuzbrukumiem, kā arī nesankcionētas piekļuves, tad pastāv risks, ka nepieciešamības gadījumā nebūs iespējams atjaunot organizācijai nozīmīgu informāciju, ja datu rezerves kopijas būs iepriekš tikušas sabojātas vides risku, kiberuzbrukuma vai ļaunprātīgas rīcības rezultātā.	• Kur tiek uzglabātas organizācijas datu rezerves kopijas, un vai šajā vietā ir piemēroti apstākļi ārējās un iekšējās vides radīto apdraudējumu mazināšanai? • Vai organizācijai ir informācija par lietotājiem, kuriem ir tiesības piekļūt datu rezerves kopijām? • Kā tiek nodrošināta organizācijas datu rezerves kopiju aizsardzība pret kiberuzbrukumiem un nesankcionētu piekļuvi kopiju uzglabāšanas un transportēšanas laikā? • Kurš organizācijā ir atbildīgs par to, lai tiktu nodrošināta datu rezerves kopiju droša uzglabāšana un noteikto aizsardzības prasību ievērošana?	

INCIDENTU PĀRVALDĪBA	*Ja netiek identificēti tādi notikumi (kļūme, kiberuzbrukums, nesankcionēta piekļuve u. tml.), kas var ietekmēt organizācijas informācijas un tehnisko resursu drošību, tad var iestāties risks, ka organizācija savlaicīgi nespēs novērst attiecīgo notikumu sekas un tiks radīti drošības incidentam piemēroti apstākļi.*	• Kāda veida pasākumi organizācijā ir ieviesti, lai reālajā laikā nodrošinātu tādu notikumu atklāšanu, kas ietekmē informācijas un tehnisko resursu drošību? • Kam organizācija ir deleģējusi pienākumu nodrošināt šos uzraudzības pasākumus ikdienā? • Vai organizācijas informācijas un tehnisko resursu lietotāji ir informēti, kā atpazīt situācijas, kad varētu tikt apdraudēta informācijas un tehnoloģiju drošība?	6.4. Incidentu pārvaldība
	Ja drošības incidenti netiek reģistrēti, tad pastāv risks, ka var būt noticis drošības incidents, par kuru organizācija nav tikusi savlaicīgi informēta, lai uzsāktu incidenta novēršanas darbus.	• Kas organizācijā ir atbildīgs par drošības incidentu reģistrēšanu? • Kā organizācijā tiek nodrošināta komunikācija ar šo atbildīgo personu? • Kur tiek reģistrēta informācija par drošības incidentiem, un kam organizācijā ir piekļuve šai informācijai? • Kādu informāciju organizācijas darbiniekam obligāti nepieciešams sniegt, lai incidents tiktu reģistrēts? Kā un kam jāziņo par incidentiem? • Vai informācija par drošības incidentiem tiek dokumentēta vēl kādā veidā (atsevišķs reģistrs elektroniskā vai papīra formātā u. tml.)? • Vai informācijas un tehnisko resursu lietotāji ir informēti, kā rīkoties, kamēr incidents vēl nav reģistrēts un nav saņemtas norādes par turpmāko rīcību?	

	Ja savlaicīgi netiek veikta drošības incidentu novēršana, tad pastāv risks, ka to sekas var izrādīties neprognozējamas, un tā rezultātā var tikt traucēta organizācijas darbība, kā arī rasties nesamērīgi materiālie zaudējumi, t. sk. kaitējums organizācijas reputācijai.	• Vai organizācijā pastāv skaidri noteikta rīcības kārtība, kādā tiek īstenota reģistrēto incidentu apstrāde? • Kam ir deleģēta atbildība koordinēt reģistrēto incidentu novēršanu? Kā drošības incidenta gadījumā notiek saziņa ar šo atbildīgo? • Vai organizācija ir noteikusi, kādu incidentu gadījumos ir nepieciešams informēt vai iesaistīt organizācijas vadību? • Vai ir zināmi atbildīgie, un kādos gadījumos tie organizācijas vārdā par notikušo incidentu komunicēs ar ieinteresētajām pusēm (uzraudzības iestādes, klienti, prese u. c.) ? • (Ja organizācija ir maksājumu pakalpojumu sniedzējs, vai tā novērtē notikušos incidentus atbilstoši FKTK 93. noteikumu kritērijiem un sasniedzot būtiska incidenta klasifikācijas līmeni, ziņo par to Latvijas bankai?	Maksājumu pakalpojumu sniedzējiem arī FKTK noteikumu Nr.93 "Normatīvie noteikumi par ziņošanu par būtiskiem maksājumu pakalpojumu incidentiem"
	Ja netiek veikta drošības incidentu izmeklēšana un situācijas analīze, lai noskaidrotu incidentu rašanās iemeslus un identificētu ar tiem saistītās nepilnības vai trūkumus organizācijā, tad pastāv risks, ka šāda veida drošības incidenti varētu rasties atkārtoti.	• Kam organizācijā ir deleģēta atbildība par incidentu izmeklēšanu? Vai šim atbildīgajam ir nepieciešamās zināšanas un kompetence, lai spētu attiecīgos pienākums pildīt? • Kā tiek nodrošināta incidentu izmeklēšanai nepieciešamo pierādījumu vākšana un saglabāšana? • Kāda informācija obligāti jādokumentē incidenta izmeklēšanas rezultātā, un kā tā tiek dokumentēta? • Vai par organizācijas informācijas un tehnisko resursu uzturēšanu atbildīgajiem tiek sniegti	

		norādījumi par incidenta iemesliem un to, kā novērst vai mazināt šādu notikumu turpmāku atkārtošanos? Vai un kā tiek noteiktas darbības incidenta iemeslu mazināšanai? • Vai tiek sagatavoti ziņojumi, pārskati vadībai?	