DORA regulas prasības un ieviešana

Valters Bajārs
IT uzraudzības eksperts

30.10.2024

LATVIJAS BANKA
EIROSISTĒMA

DORA regulējuma mērķis ir izveidot visaptverošu ietvaru ES finanšu iestāžu digitālo darbības noturībai

Tieši piemērojam regula ES 2022/2544

Nacionālais digitālās darbības noturības likums

LB ir kompetentā iestāde

Prasības jāizpilda sākot ar 17.01.2025

Sektorāla un pārrobežu regulatīvo prasību harmonizēšana

Regulatīvi tehniskie standarti

IKT risku pārvaldība	IKT incidentu pārvaldība	Digitālās noturības testēšana	Trešo pušu IKT risku pārvaldība	Pārraudzība
RTS risku pārvaldības modelis un vienkāršotā IKT risku pārvaldība	RTS Kritēriji IKT incidentu klasifikācijai	RTS Draudu vadītas ielaušanās testēšanai (TLPT)	ITS informācijas reģistru formām	RTS uzraudzības harmonizēšanai
	ITS būtisku incidentu ziņošanas detaļām		RTS politikai IKT servisiem ko sniedz trešās puses	GL sadarbības nosacījumiem starp ESA un CA
	RTS būtisku incidentu ziņošanai		RTS kritērijiem lai novērtētu piegādātājus kritiskajām un svarīgajām funkcijām	
	GL zaudējumu novērtēšanai			

DORA piemēro finanšu vienībām

aktīviem piesaistītu žetonu emitentam

centrālajam darījumu partnerim

centrālajam vērtspapīru depozitārijam

darījumu reģistram

datu ziņošanas pakalpojumu sniedzējam

elektroniskās naudas iestādei

ieguldījumu brokeru sabiedrībai

ieguldījumu pārvaldes sabiedrībai

maksājumu iestādei

kolektīvās finansēšanas pakalpojumu sniedzējam

konta informācijas pakalpojumu sniedzējam

kredītiestādei

kredītreitingu aģentūrai

kriptoaktīvu pakalpojumu sniedzējam

kritiski svarīgu etalonu administratoram

tirdzniecības vietai

vērtspapīrošanas repozitorijam

DORA piemēro finanšu vienībām ar izņēmumiem

apdrošināšanas papildpakalpojuma starpniekam

apdrošināšanas sabiedrībai

apdrošināšanas starpniekam

pārapdrošināšanas sabiedrībai

pārapdrošināšanas starpniekam

alternatīvo ieguldījumu fonda pārvaldniekam

maksājumu iestādei

privātajam pensiju fondam

žiro norēķinu iestādei - nepiemēro

krājaizdevu sabiedrībai - nepiemēro

DORA regulējuma jomas

IKT risku pārvaldība

IKT risku pārvaldības sistēma ir bāzes elements visu prasību ieviešanā un tai jābūt integrētai kopējā risku pārvaldības struktūrā

Vadības struktūra uzņemas pilnīgu atbildību par IKT risku pārvaldību

IKT incidentu pārvaldība

FV ir spējīga reģistrēt un pārvaldīt visus ar IKT saistītus incidentus

Ieviestas procedūras un mehānismi, lai nodrošinātu integrētu visu IKT incidentu identifikāciju, uzraudzību, apstrādi un kontroli

Darbības noturības testēšana

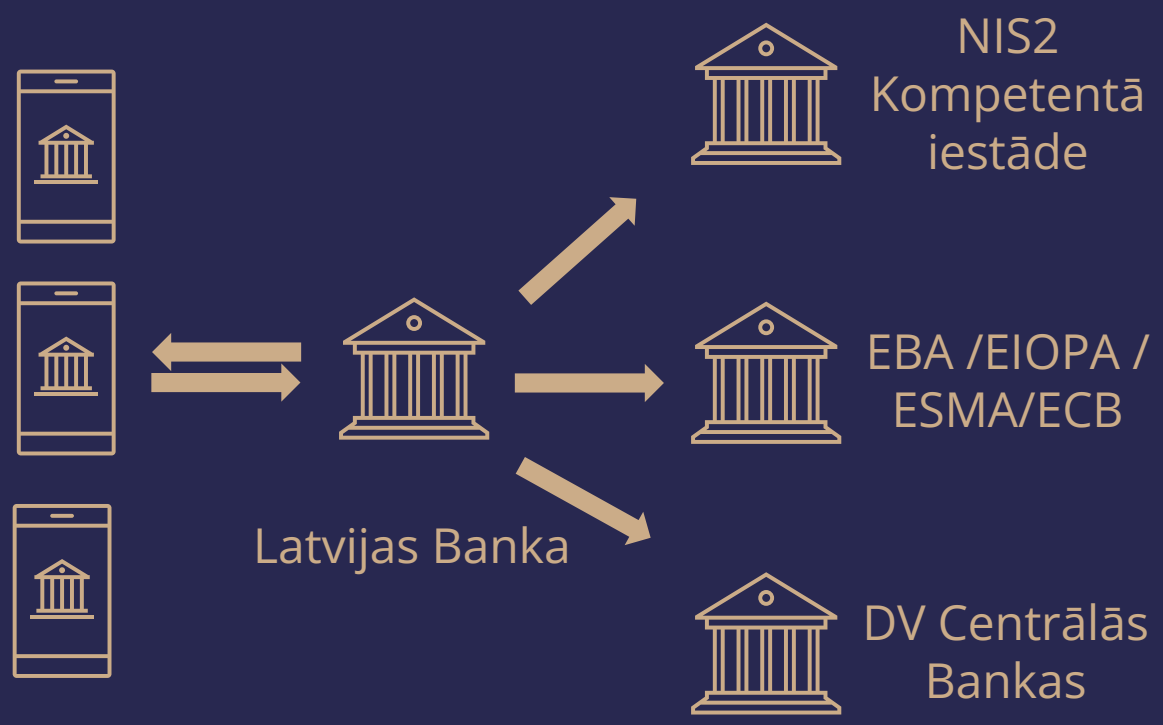
Lai spētu identificēt trūkumus un nepilnības digitālā noturībā, FV ir izveidojusi darbības noturības testēšanas programmu, kas papildina IKT risku pārvaldības sistēmu.

Trešo pušu IKT pakalpojumu sniedzēju pārvaldība

Esošie IKT pakalpojumu līgumi, kas atbalsta kritiskas vai svarīgas funkcijas jāpārjauno atbilstošo DORA prasībām.

Ar trešajām pusēm saistīto IKT risku pārvaldība ir integrēta iekšējā IKT risku pārvaldībā.

Ziņošana par būtiskiem IKT Incidentiem

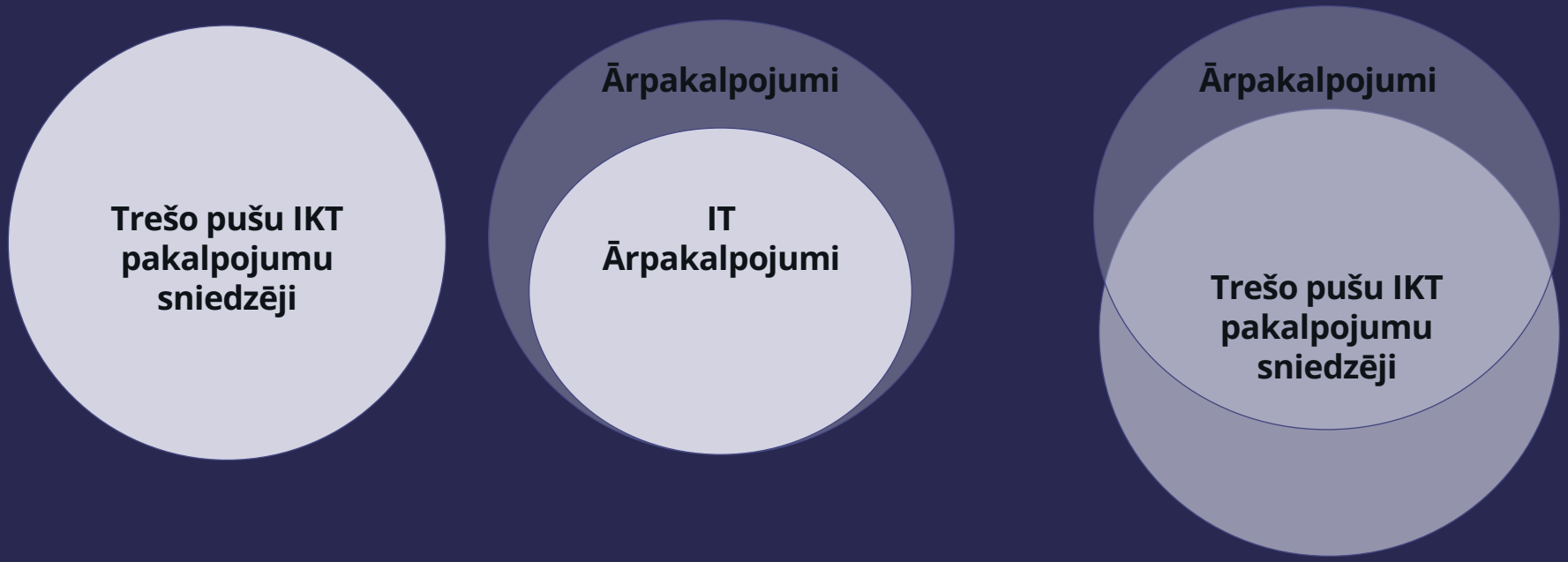


- Finanšu vienības ziņo LB par nozīmīgiem IKT incidentiem
- Incidentus klasificē kā nozīmīgus pēc primārajiem un sekundārajiem kritērijiem
- FV jāiesniedz sākotnējais, starpziņojums un noslēdzošais ziņojums. Noslēdzošais ziņojums satur cēloņu analīzi un ierobežošanas pasākumus
- € Jāaprēķina un jāziņo ikgadējie IKT incidentu izraisītie zaudējumi

IKT incidentu klasifikācijas kritēriji

- Ietekmēto klientu skaits
- Datu zaudējumi (CIA)
- Ietekmēto transakciju un/vai partneru skaits
- Ietekmētas kritiskās funkcijas
- Reputācijas ietekme
- Ģeogrāfiskā izplatība
- Incidenta ilgums
- Ekonomiskā ietekme

IKT trešo pušu pakalpojumu sniedzēji



DORA definīcija

Esošā EBA GL definīcija

Draudu vadītas ielaušanās testi (TLPT)

Atbilstoši proporcionalitātes principam TLPT testi ir piemēroti FV ar sistēmisku ietekmi un augstu brieduma līmeni. LB un ECB strādā pie 3 gadu testu plāna nozīmīgajām kredītiestādēm, par ko izvēlētajām iestādēm tiks laicīgi paziņots.

LB tiks apstiprināta kā kompetentā iestāde par TLPT testiem. ECB ir kompetentā iestāde nozīmīgo kredītiestāžu testēšanai sadarbībā ar LB

Kompetentās iestādes apstiprina testējamās FV, un testējamās jomas.

FV ir jāizmanto ārējais draudu izlūkdatu piegādātājs

Tests ir vērsts uz produkcijas sistēmām, kas atbalsta kritiskās funkcijas

Testu tvērums ir multisektorāls un var ietvert arī iestādes ārpus finanšu sektora, kā arī var notikt vairākās DV un FV vienlaicīgi

Kā sagatavoties 17.01.2025

Visām finanšu vienībām 17.01.2025. jābūt gatavām izpildīt regulas prasības.

Latvijas Banka piemēros riskos bāzētu un proporcionālu uzraudzības pieeju. Uzraudzības līmenis un pieeja mainīsies atkarībā no finanšu vienības darbības veida, mēroga, vispārējā risku profila, sniegto pakalpojumu sarežģītības un ietekmes uz tirgu.

Katrai finanšu vienībai ir unikāla situācija un brieduma līmenis sākot ieviest DORA regulas prasības.

Izvērtēt uzņēmuma IKT kontekstu ,veikt gatavības analīzi, sekot RTS publicēšanai un publiskajām konsultācijām

Apstiprināt ieviešanas plānu, nodrošināt vadības atbalstu un budžetu. Uzsākt politikas dokumentu pārskatīšanu. Pēc nepieciešamības piesaistīt ārējos resursus

Uzsākt sarunas ar trešo pušu pakalpojumu sniedzējiem par līgumu izmaiņām. Sagatavot informācijas reģistru (RoI) iesniegšanai.

Sagatavot un notestēt būtisku IKT incidentu klasifikācijas un ziņošanas procesu

Paldies par uzmanību!

Ar DORA ieviešanu un atbilstību saistītiem jautājumiemdora@bank.lv

EBA informācijas vietne Digital Operational Resilience Act | European Banking Authority.