Par Informācijas reģistra *(Register of Information, ROI)* iesniegšanu 2026. gadā

Finanšu tehnoloģiju uzraudzības pārvalde
dora@bank.lv

LATVIJAS BANKA
EIROSISTĒMA

Regulas (EU) 2022/2554 (DORA) īstenošana

Pamats IKT trešo pušu pakalpojumu sniedzēju reģistra uzturēšanai un ziņošanai

DORA regula (ES) 2022/2554

28. pants

nosaka finanšu vienību pienākumu uzturēt informācijas reģistru par visiem IKT trešo pušu pakalpojumiem

Komisijas īstenošanas regula (ITS) 2024/2956

- Precizē ROI struktūru, formātu un iesniegšanas kārtību
- Nodrošina vienotu datu vākšanu ES mērogā

Finanšu tirgus digitālās darbības noturības un mākslīgā intelekta izmantošanas likums

- Nostiprina DORA prasības nacionālā līmenī
- Nosaka atbildīgo iestādi un sankciju mehānismu par neiesniegšanu vai nekvalitatīviem datiem

DORA otrā līmeņa regulējuma kopsavilkums

Joma	Standarts	Apraksts
IKT risks	RTS 2024/1774	Prasības riska pārvaldības procesam
Incidentu klasifikācija	RTS 2024/1772	Kritēriji būtiskuma noteikšanai
Incidentu ziņošana	RTS 2025/301, ITS 2025/302	Ziņojumu saturs, termiņi un forma
TPP līgumu saturs	RTS 2024/1773	Minimālās līgumu prasības ar pakalpojumu sniedzējiem
Apakšlīgumi	RTS 2025/532	Noteikumi par tālāku ārpakalpojumu nodošanu
TPP reģistrs	ITS 2024/2956	Informācijas uzskaites un iesniegšanas formāts
TLPT testēšana	RTS 2025/1190	Draudos balstītu ielaušanās testu metodika un prasības

Par Informācijas reģistra (ROI) iesniegšanu 2026. gadā

Atbilstoši DORA prasībām, DORA subjekti uztur aktuālu **IKT trešo pušu pakalpojumu reģistru**.

Reģistru iesniegšanai sagatavo *xlsx* vai *xbrl-csv* formātā.

Latvijas Bankai **reizi gadā konsolidēti** iesniedz visi DORA subjekti, izņemot SI bankas.

SI bankas reģistru iesniedz **ECB** *xbrl-csv* formātā.

Latvijas Banka nosūta tālāk **EBA** *xbrl-csv* formātā.

Ziņošanas kanāli un termiņi

Informācijas reģistru (ROI) jāiesniedz līdz 2026. gada 1. martam.

ROI iesniegšanai var izmantot **vienu no divām veidnēm**, atbilstoši EBA taksonomijai:

- Excel formāta veidne, kas pieejama Latvijas bankas tīmekļvietnē
- XBRL formāta datne: EBA XBRL v4.2 (13/01/2026)

ROI iesniegšanai šogad piemēro ***Reporting framework 4.2*** (https://www.eba.europa.eu/risk-and-data-analysis/reporting-frameworks/reporting-framework-42)

Ja darbā ar IKT pakalpojumu sniedzējiem (trešajām personām) izmaiņas netiek konstatētas, **reģistrs tāpat jāuztur aktuālā redakcijā un katru gadu jāiesniedz**.

ECB tiešā uzraudzībā esošās finanšu iestādes **reģistru iesniedz ECB konsolidētā līmenī**.

LATVIJAS BANKA
EIROSISTĒMA

IKT pakalpojumu sniedzēju riska novērtējums kopējā IKT risku pārvaldības ietvarā

IKT risku pārvaldības ietvars ir **jādokumentē un jāpārskata vismaz reizi gadā**, kā arī pēc būtiskiem IKT **incidentiem** (6. panta 5. punkts)

1. **solis – IKT pakalpojumu sniedzēju riska novērtējums pirms līguma**: pirms līguma noslēgšanas jāveic novērtējums, vai pakalpojums sedz **kritisku vai svarīgu funkciju** (28. panta 3. punkts), un jāidentificē un jānovērtē attiecīgie riski (tostarp IKT koncentrācijas risks), jāveic "*due diligence*" un interešu konfliktu izvērtējums (28. panta 4. punkta a)–e) apakšpunkti).
2. **solis – reģistrs (ROI):** reģistrs par līgumattiecībām ar IKT pakalpojumu sniedzējiem ir **jāuztur un jāatjaunina iestādes līmenī un konsolidētā līmenī** (28. panta 3. punkts).
3. **solis – regulāra risku pārskatīšana kritiskajām/svarīgajām funkcijām**: vadības struktūrai, balstoties uz kopējo riska profilu un pakalpojumu mērogu/sarežģītību, regulāri jāpārskata identificētie riski par līgumiem, kas atbalsta kritiskas vai svarīgas funkcijas (28. panta 2. punkts).

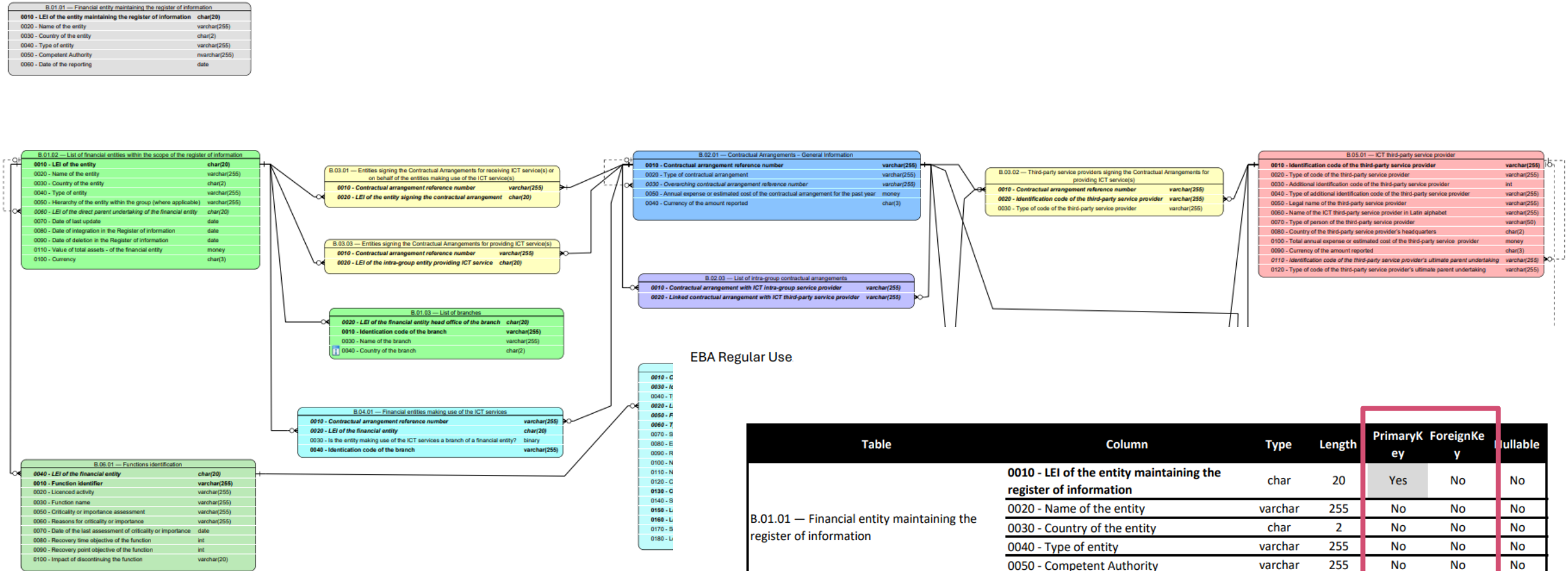
Jānodrošina precīza atbilstība EBA datu modelim

Jāievēro Excel veidnes struktūras nemainīgums – **aizliegts mainīt lapu secību, ievietot vai mainīt vietām kolonnas**.

Nedrīkst dzēst no Excel sagataves lapas, ja nav paredzēts tās pildīt. Sistēma sagaida **precīzu atbilstību EBA datu modelim**.

Katra ROI lauka formāts un saturs ir noteikts **ITS 2024/2956 I pielikumā "Norādījumi informācijas reģistra aizpildīšanai"**: Īstenošanas regula - ES - 2024/2956 - EN - EUR-Lex

EBA datu modelis (Data Model for DORA RoI.pdf)

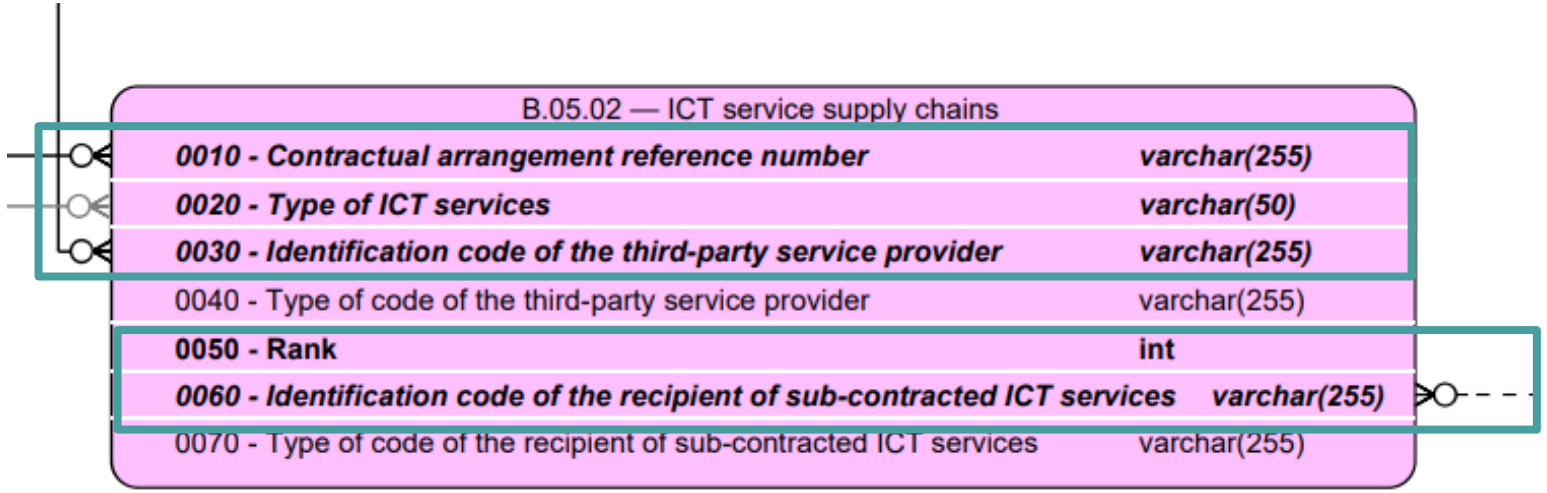


EBA Regular Use

Table	Column	Type	Length	PrimaryKey	ForeignKey	Nullable
B.01.01 — Financial entity maintaining the register of information	**0010 - LEI of the entity maintaining the register of information**	char	20	Yes	No	No
	0020 - Name of the entity	varchar	255	No	No	No
	0030 - Country of the entity	char	2	No	No	No
	0040 - Type of entity	varchar	255	No	No	No
	0050 - Competent Authority	varchar	255	No	No	No
	0060 - Date of the reporting	date	0	No	No	No
	0010 - LEI of the entity	char	20	Yes	No	No
	0020 - Name of the entity	varchar	255	No	No	No
	0030 - Country of the entity	char	2	No	No	No
	0040 - Type of entity	varchar	255	No	No	No
	0050 - Hierarchy of the entity within the					

Visās lapās jālieto vienoti, unikāli identifikatori

- Jāņem vērā, ka *primary key un foreign key* kolonnas (atbilstoši ERD diagrammai) vērtības nevar būt tukšas.
- **Katra ROI lauka formāts un saturs ir noteikts ITS 2024/2956 I pielikumā "Norādījumi informācijas reģistra aizpildīšanai":** Īstenošanas regula - ES - 2024/2956 - EN - EUR-Lex



TOC | B_05.02:ICT service supply chains

					Type of code to identify the ICT third-party service provider	Type of code to identify the recipient of sub-contracted ICT services
Contractual arrangement reference number between the financial entity or, in case of a group, the group subsidiary and the direct ICT third-party service provider	Type of ICT service	Identification code of the ICT third-party service provider	Identification code of the subcontractor	Rank in supply chain	0040	0070
Open	ICT Development	Open	Open	Open		

Visi iesūtītie informācijas reģistri tiek pakļauti divu veidu datņu pārbaudēm – tehniskās un datu kvalitātes

Precīzi juridiskie nosaukumi

Jāizmanto precīzi gan **pašu grupas uzņēmumu**, gan **pakalpojumu sniedzēju** juridiskie nosaukumi. Avots – Uzņēmumu reģistrs.

Pārskata periods ir 01.01.2025. - 31.12.2025.

Šogad pārskata periods ir 01.01.2025. - 31.12.2025., datumam katru gadu ir jāatbilst kalendārā gada ziņošanas periodam.

Arī mātes uzņēmumam jānorāda apakšuzņēmēji

Piemēram, ja mātes uzņēmums sniedz IKT pakalpojumus, ir jānorāda uzņēmumi, kas nodrošina IKT pakalpojumus mātes uzņēmumam.

Datnes nosaukums: DORA-ROI_20251231.xlsx

Atbilstoši EBA taksonomijai, datnes nosaukumā izmanto visus **lielos burtus: r, o, i.**

Piegādes ķēžu atspoguļošana

ROI jāatspoguļo IKT pakalpojuma visa zināmā piegādes ķēde (*Rank in supply chain*):

- Pirmā līmeņa apakšuzņēmēji (1),
- Otrā līmeņa apakšuzņēmēji (2),
- Trešā līmeņa apakšuzņēmēji (3), un tālāk (4, 5, ...), t. i., ķēde tiek veidota bez ierobežojuma, palielinot līmeni katram nākamajam apakšuzņēmējam, cik tālu tas ir zināms.

Katram apakšuzņēmējam ROI jānorāda, **kam tas sniedz apakšuzņēmuma pakalpojumu** (t. i., "*recipient*"), lai būtu **izsekojama ķēde** arī 2., 3. un tālākajos līmeņos (ITS 2024/2956 I pielikumā **"Norādījumi informācijas reģistra aizpildīšanai"**: Īstenošanas regula - ES - 2024/2956 - EN - EUR-Lex).

Lapas *B_05.02:ICT service supply chains* aizpildīšana

- Jāatspoguļo **IKT pakalpojuma visa zināmā piegādes ķēde** (*Rank in supply chain*)
- Sevišķi izteikti apakšuzņēmēji tiek izmantoti šādos pakalpojumos:

TOC	B_05.02:ICT service supply chains				
					Type of code to identify the ICT third-party service provider
Contractual arrangement reference number between the financial entity or, in case of a group, the group subsidiary and the direct ICT third-party service	Type of ICT service	Identification code of the ICT third-party service provider	Identification code of the subcontractor	Rank in supply chain	0040
A	ICT operation management (including maintenance)	46e4567e54	45646456	1	Company registration number (CRN)
B	Cloud services: PaaS	535345	3463463w	2	Company registration number (CRN)
C	Telecom carrier	3w 463674	w 4654745	1	Company registration number (CRN)
D	ICT security management services	3452q53	346w etw 34	3	Company registration number (CRN)
E	Hardware and physical devices	56456356	3543698	4	Company registration number (CRN)

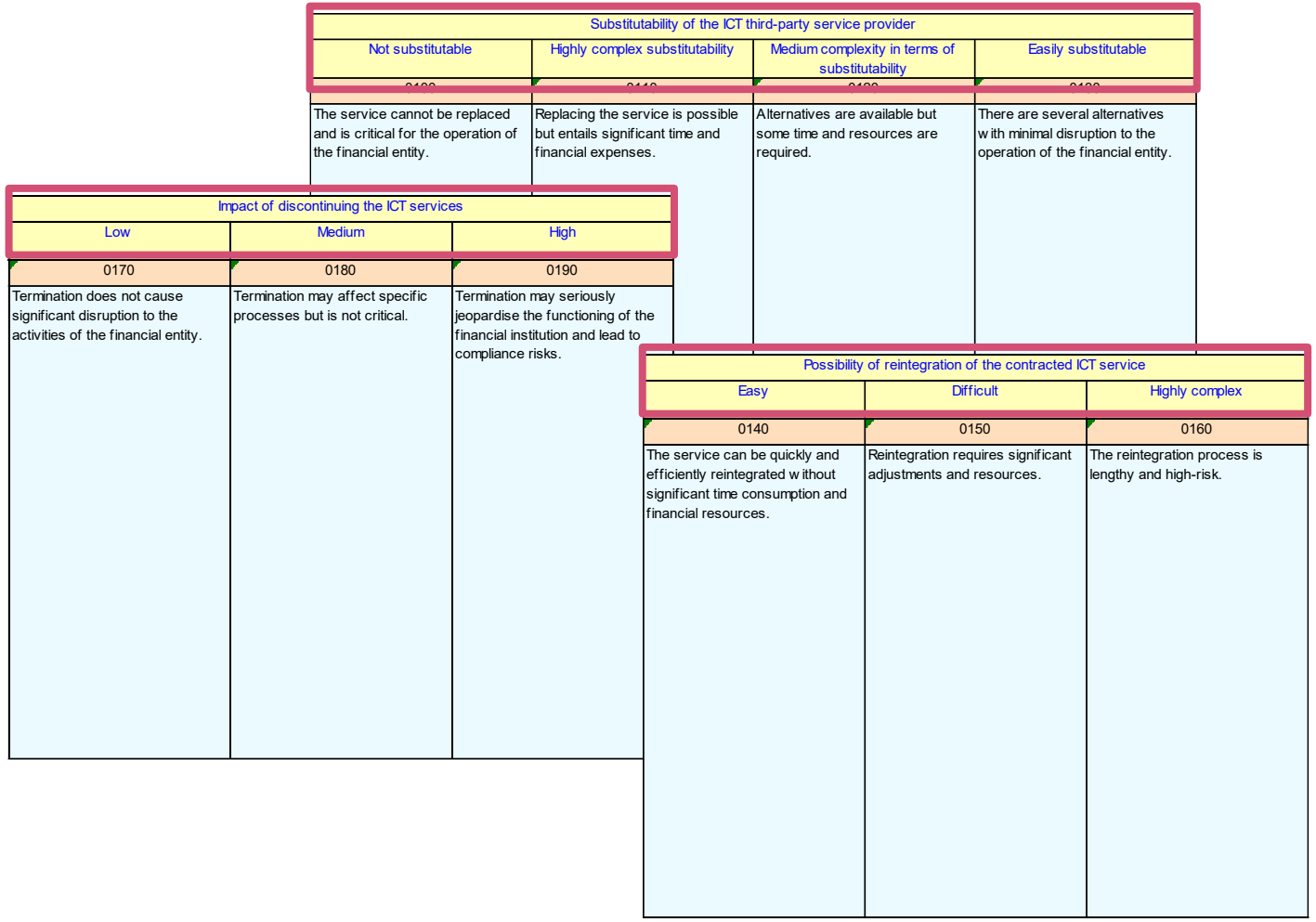
Lapas *B_99.01 Definitions from Entities* aizpildīšana

Būtiski raksturot:

- trešās puses **pakalpojuma aizvietojamību** *(substitutability),*
- ietekme, ja **IKT pakalpojums tiek pārtraukts** *(impact of discontinuing ICT services)*,
- IKT pakalpojuma **reintegrācijas iespēja** *(possibility of reintegration)* - iespējas pārņemt atpakaļ trešajai personai deleģētās funkcijas izpildi.

Jānorāda, piemēram:

- konkrēts pakalpojums,
- galvenie infrastruktūras elementi,
- galvenās sistēmas /komponenti un integrāciju skaits,
- datu plūsma,
- *lock-in* faktori, specializēts *know-how*
- izmaksu un līguma ierobežojumi.



Substitutability of the ICT third-party service provider

Not substitutable	Highly complex substitutability	Medium complexity in terms of substitutability	Easily substitutable
The service cannot be replaced and is critical for the operation of the financial entity.	Replacing the service is possible but entails significant time and financial expenses.	Alternatives are available but some time and resources are required.	There are several alternatives with minimal disruption to the operation of the financial entity.

Impact of discontinuing the ICT services

Low	Medium	High
0170	0180	0190
Termination does not cause significant disruption to the activities of the financial entity.	Termination may affect specific processes but is not critical.	Termination may seriously jeopardise the functioning of the financial institution and lead to compliance risks.

Possibility of reintegration of the contracted ICT service

Easy	Difficult	Highly complex
0140	0150	0160
The service can be quickly and efficiently reintegrated without significant time consumption and financial resources.	Reintegration requires significant adjustments and resources.	The reintegration process is lengthy and high-risk.

Lapas *B_06.01:Functions identification* aizpildīšana

Jānorāda iemesli, ja **funkcijas traucējumi var radīt būtisku ietekmi** uz iestādes darbību, klientiem, tirgu kopumā *(Reasons for criticality or importance).*

	Licenced activity	Function name	Criticality or importance assessment	Reasons for criticality or importance
Identifier of the operational/business function of an entity	0020	0030	0050	0060
F1	Payment services	Deposits in the Banka of Latvia Noguldījums Latvijas Bankā	Yes	The disruption of the function or failures can materially negatively effect the compliance with the effective laws and regulations and conditions and obligation of the authorization.
F2	Lending activities	Consumers loans Patēriņa kredīti	Yes	
F3	Payment services	Payment accounts Norēķinu konti	Yes	
F4	Payment services	Saving accounts Krājkonti (Krājkase)	Yes	
F5	Payment services	Term deposits Terminnoguldījumi	Yes	

Piemērs: Funkcijas pārtraukšana tieši ietekmē [klientu pamatpakalpojumu / licencēto darbību], un dīkstāve virs [*Maximum tolerable downtime, MTD*] rada būtisku risku (piem., [ziņošanas pienākumi, līgumu izpilde, klientu līdzekļu pieejamība]). Funkcija apstrādā aptuveni [x] darījumus dienā ar kopējo vērtību [y], un traucējumi rada ietekmi uz [saistītie procesi/sistēmas]. Ir pieejams [manuāls/alternatīvs] risinājums tikai [ilgums/ierobežojumi], tādēļ funkcija tiek klasificēta kā kritiska vai svarīga.

Lapas *B_07.01:Assessment of the ICT services* aizpildīšana

Jānorāda alternatīvi pakalpojumu sniedzēji, kas sniegs pierādījumu par riska analīzes veikšanu (*Identification of alternative ICT TPP*).

	Substitutability of the ICT third-party service provider	Reason if the ICT third-party service provider is considered not substitutable or difficult to be substitutable	Identification of alternative ICT TPP
Type of ICT service	0050	0060	0120
Cloud services: SaaS	Highly complex substitutability	Lack of real alternatives and difficulties in migrating or reintegrating	Temenos FISERV Oracle
Cloud services: SaaS	Highly complex substitutability	Difficulties in migrating or reintegrating	Worldline DECTA Enfuse
Cloud services: SaaS	Highly complex substitutability	Difficulties in migrating or reintegrating	SALV (Estonia) ComplyAdvantage (UK) HawkAI (Germany)
Cloud services: SaaS	Highly complex substitutability	Difficulties in migrating or reintegrating	Ingain (Latvia) Scorify (Lithuania) Apello (Austria)
Cloud services: SaaS	Highly complex substitutability	Difficulties in migrating or reintegrating	SIA Fintecor
Cloud services: PaaS	Highly complex substitutability	Lack of real alternatives and difficulties in migrating or reintegrating	Amazon Web Services Google Cloud Platform
Cloud services: PaaS	Highly complex substitutability	Lack of real alternatives and difficulties in migrating or reintegrating	CRM: Salesforce (ASV) Creatio (ASV) Zoho (Indija) ERP: Horizon (Latvija) SAP S/4HANA (Vācija) Epicor (ASV)
Cloud services: PaaS	Highly complex substitutability	Lack of real alternatives and difficulties in migrating or reintegrating	Opticom (Latvia) Squalio (Latvia) DPA (Latvia)

Kontaktinformācija jautājumiem, kas ir saistīti ar failu iesniegšanu un to tehniskām pārbaudēm

FAS / Paaugstinātās drošības sistēma

ds.info@bank.lv vai pa tālruni 67022756

Elektronisko pārskatu sistēma

IS_Stat@bank.lv vai tālruņiem 67022299, 67022715 (izmanto MI, ENI)

Latvijas Bankas gaidas trešo pušu IKT pakalpojumu pārvaldībā finanšu tirgus dalībnieku uzraudzības kontekstā

LATVIJAS BANKA
EIROSISTĒMA

Ievads

Saskaņā ar Regulas (ES) 2022/2554 3. panta 21. punktu un tās skaidrojumiem par trešo pušu informācijas un komunikācijas tehnoloģiju (IKT) pakalpojuma definīciju ir noteikts, ka –

IKT pakalpojumi ir digitālie un datu pakalpojumi, ko ar IKT sistēmu starpniecību pastāvīgi sniedz vienam vai vairākiem iekšējiem vai ārējiem lietotājiem –

tostarp aparatūras nodrošināšanas pakalpojumi un ar aparatūru saistīti pakalpojumi, kas ietver tehniskā atbalsta sniegšanu, izmantojot programmatūru vai aparātprogrammatūras atjauninājumus, ko veic aparatūras nodrošinātājs, izņemot tradicionālos analogās telefonijas pakalpojumus.

Tādējādi IKT pakalpojums ir **jebkurš digitāli sniegts pakalpojums, kas atbalsta finanšu iestādes darbību vai kritiskos procesus**, un ko nodrošina ārējais pakalpojumu sniedzējs (t. sk. grupas līmenī).

Trešo pušu IKT pakalpojumu neatbilstošas pārvaldības sekas

Nekontrolēti un plaši **darbības traucējumi** un būtiska ietekme uz iestādes darbību (reputācija, līgumsodi un kompensācijas)

Koncentrācijas riski un kritiska atkarība no viena piegādātāja (sistēmiska krīze)

Nepietiekama **IKT un datu drošība** (neatbilstība regulējumam, pārkāpumi un sodi)

Incidentu nepietiekama ziņošana un trūkumi koordinācijā (reputācija, kavējumi un sodi)

Neizstrādāta vai **neefektīva izejas stratēģija** (pakalpojuma nepieejamības riski, neapzinātas un augstas izmaksas)

Neidentificēti un **nepārvaldīti apakšuzņēmēji** (nezināmi riski, nepietiekama IKT un datu drošība, neatbilstība regulējumam un sodi)

Kopsavilkums par DORA prasībām trešo pušu IKT pakalpojumu pārvaldībai

Trešo pušu IKT pakalpojumu reģistra uzturēšana (28. pants un Komisijas Īstenošanas regula 2024/2956)

Kritisku trešo pušu IKT pakalpojumu identificēšana un ziņošana regulatoram (28. panta 4.-5. punkts)

IKT pakalpojumu uzraudzība un pārvaldība (25.-27. pants)

IKT koncentrācijas riska pārvaldība (29. pants)

Ziņošana par būtiskiem incidentiem vai līgumu izmaiņām (19.-21. pants un 26. pants)

Līguma minimālo prasību noteikšana (27. pants)

Trešās puses riska pārvaldība (19. pants)

Gatavība sadarbībai ar regulatoru (20. un 28. pants)

Eiropas uzraudzības iestāžu jeb *European Supervisory Authorities (EBA, EIOPA and ESMA)* noteiktie ES līmeņa kritiskie pakalpojumu sniedzēji

[European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act - European Insurance and Occupational Pensions Authority]

18 November 2025

In accordance with Article 31(9) of the Digital Operational Resilience Act, the list of designated critical ICT third-party service providers at Union level (in alphabetic order) is the following:

- Accenture plc
- Amazon web Services EMEA Sarl
- Bloomberg L.P.
- Capgemini SE
- Colt Technology Services
- Deutsche Telekom AG
- Equinix (EMEA) B.V.
- Fidelity National Information Services, Inc.
- Google Cloud EMEA Limited
- International Business Machine Corporation
- InterXion HeadQuarters B.V.
- Kyndryl Inc.
- LSEG Data and Risk Limited
- Microsoft Ireland Operations Limited
- NTT DATA Inc.
- Oracle Nederland B.V.
- Orange SA
- SAP SE
- Tata Consultancy Services Limited

Galvenie organizācijas pienākumi trešo pušu IKT pakalpojumu pārvaldībā

1. **Ziņošanas gatavība Latvijas Bankai:**
   slēdzot jaunu līgumu par nozīmīgu IKT pakalpojumu vai veicot būtiskas izmaiņas esošā līguma ietvaros.
2. **Kritiski nozīmīgu IKT pakalpojumu identificēšana:**
   identificēt visas trešo pušu vienošanās, izvērtējot to kritiskumu un nozīmīgumu iestādes darbībai, lai turpmāk nodrošinātu šādu IKT pakalpojumu pastiprinātu uzraudzību.
3. **Trešo pušu IKT pakalpojumu riska pārvaldības sistēmas izveide:**
   pārvaldības dokumentācijas ieviešana, riska novērtējuma veikšana pirms sadarbības uzsākšanas un risku pārvaldības sadarbības laikā.
4. **Atbilstības līgumu noteikumiem kontrole:**
   pakalpojuma apraksts, drošības prasības, auditēšanas tiesības, apakšuzņēmēju iesaistes nosacījumi, prasības incidentu ziņošanai, līgumu izbeigšanas noteikumi un izeja stratēģijas.
5. **Trešo pušu reģistra ieviešana un uzturēšana:**
   jāizveido un jāuztur reģistrs par visiem IKT pakalpojumu sniedzējiem, ietverot regulējumā noteikto informācijas kopumu, kā arī jānodrošina gatavība iesniegt reģistru pēc Latvijas Bankas pieprasījuma.

Ziņošana par jaunu nozīmīgu IKT pakalpojumu (jauns līgums)

- ✓ Izvērtēt IKT **pakalpojuma** atbilstību iestādes biznesa vajadzībām un izvērtēt tā **kritiskumu un nozīmi** iestādes darbības kontekstā.
- ✓ Veikt IKT pakalpojuma **risku analīzi**, tai skaitā izvērtējot koncentrācijas risku (obligāta prasība **nozīmīgam IKT pakalpojumam**), un noteikt nepieciešamos risku pārvaldības pasākumus, tostarp paredzot pakalpojuma izbeigšanas stratēģiju.
- ✓ Izvērtēt **līguma** projekta **atbilstību** DORA prasībām un veikt satura precizējumus pēc nepieciešamības, iespēju robežās identificējot i**esaistītos apakšuzņēmējus** un to nozīmi līguma darbības ietvaros.
- ✓ Informēt Latvijas Banku savlaicīgi **par plānoto sadarbību ar nozīmīgu** trešās puses IKT **pakalpojuma sniedzēju** un iesniegt nepieciešamo dokumentāciju izskatīšanai.
- ✓ Klasificēt attiecīgo IKT pakalpojumu un **ievietot** informāciju par to **trešo pušu reģistrā.**
- ✓ Izstrādāt/pārskatīt iestādes **darbības nepārtrauktības plānus**, lai nodrošinātu attiecīgās trešās puses iesaisti un incidentu ziņošanu, atbilstoši DORA prasībām.

Ziņošana par izmaiņām nozīmīga IKT pakalpojuma kontekstā (esošs līgums)

- ✓ Izvērtēt plānoto **izmaiņu apjomu un būtiskumu** esošā IKT pakalpojumu līgumā ar trešo pusi (pēc nepieciešamības atkārtoti izvērtēt pakalpojumu kritiskumu un nozīmi iestādei).
- ✓ Veikt **sākotnējo vai atkārtoto** IKT pakalpojumu risku analīzi (būtisku izmaiņu gadījumā), identificējot jaunus darbības riskus vai izmaiņas esošajā IKT pakalpojuma risku ainavā, un noteikt jaunus vai pārskatīt esošos risku pārvaldības pasākumus.
- ✓ Pārskatīt līguma satura un plānoto izmaiņu atbilstību **DORA prasībām**, veicot grozījumus pēc nepieciešamības (jo īpaši **incidentu** ziņošanas jautājumos).
- ✓ **Savlaicīgi informēt** Latvijas Banku par plānotajām izmaiņām un iesniegt nepieciešamos dokumentus izskatīšanai (līgums, risku analīze, pakalpojuma novērtējums u.c.).
- ✓ Aktualizēt informāciju par līguma izmaiņām **trešo pušu reģistrā**, pārskatīt iestādes darbības nepārtrauktības dokumentāciju, lai tiktu veicināta trešo pušu un to apakšuzņēmēju **faktiska** iesaiste plānošanā un testēšanā.

Izaicinājumi trešo pušu IKT pakalpojumu izvērtēšanā un ziņošanā

Ja **tradicionālie ārpakalpojumi ietver trešo pušu IKT pakalpojumus**, tad informācija par tiem ir jāiekļauj trešo pušu IKT pakalpojumu reģistrā.

Tradicionālie ārpakalpojumi, kas ietver nozīmīgus trešo pušu IKT pakalpojumus nereti **var tikt pārvaldīti arī pēc DORA ietvara**, ja pastāv pilnīga atkarība no IKT pakalpojumiem.

Nozīmīgiem trešo pušu IKT pakalpojumu līgumiem **nav nepieciešama atļaujas saņemšana** no Latvijas Bankas, taču ir **nepieciešams savlaicīgi informēt** Latvijas Banku.

Eiropas uzraudzības iestādes jeb *European Supervisory Authorities (ESA)* var ierobežot vai likt pārtraukt sadarbību gadījumos, kad IKT pakalpojumu sniedzējs ir kritiskā trešā puse un tiek konstatēti būtiski riski.

Labās prakses īstenošana trešo pušu IKT pakalpojumu pārvaldībā

1. **Centralizēta pārvaldība** (reģistra ieviešana un uzturēšana pēc vienotas pieejas; atbilstošās veidnes izmantošana) **un klasifikācija** pēc kritiskuma līmeņa un kategorijas (atbilstoši Komisijas Īstenošanas regulā noteiktām prasībām: S01-S19).
2. **Biznesa ietekmes analīze** *(Business Impact analysis, BIA)*, lai novērtētu kritisko funkciju un pakalpojumu **ietekmi**, un biznesa procesu **atkarības** no trešo pušu IKT pakalpojumiem.
3. **Izejas stratēģijas izstrāde** (plāns līguma darbības pārtraukšanai un pakalpojuma sniedzēja maiņai, piegādātāju un izmaksu savlaicīga izvērtēšana).
4. **Darbības nepārtrauktības testēšana** (regulāra, scenārijos balstīta testēšana, sadarbībā ar pakalpojumu sniedzējiem, testu rezultātu dokumentēšana un RTO/RPO atbilstības mērījumu veikšana).
5. **Augstākās vadības iesaiste un uzraudzības nodrošināšana** (regulāri ziņojumi vadībai par trešo pušu riskiem; riska analīzē un ieguvumu/zaudējumu analīzē balstīta lēmumu pieņemšana un informācijas dokumentēšana).

Rekomendācijas un iespējas trešo pušu IKT pakalpojumu pārvaldības pilnveidošanai

1. **Starptautiskie standarti:**
   - ISO/IEC 27036 Informācijas drošības vadlīnijas piegādes ķēdes un piegādātāju attiecību pārvaldībai,
   - ISO/IEC 27001 & 27002 – Informācijas drošības pārvaldības sistēmas ieviešanas standarts,
   - ISO/IEC 22301 – Biznesa nepārtrauktības pārvaldības sistēma,
   - ISO/IEC 20000-1 – IT pakalpojumu pārvaldības standarts.

2. **Kiberdrošības labā prakse:**
   - ENISA vadlīnijas mākoņpakalpojumu un ārpakalpojumu drošībai,
   - NIST SP 800-161 Rev. 1 Kiberdrošības prakses piegādes ķēžu risku pārvaldībā.

3. **Finanšu tirgus vadlīnijas:**
   - EBA Vadlīnijas ārpakalpojumu pārvaldībai (EBA/GL/2019/02) maksājumu iestādēm,
   - EIOPA vadlīnijas par mākoņpakalpojumu izmantošanu (EIOPA-Bos-20/002) apdrošināšanas nozarei,
   - ESMA vadlīnijas par ārpakalpojumiem un mākoņpakalpojumiem vērtspapīru tirgus dalībniekiem (ESMA50-157-2403).

2026. gada izaicinājumi un prioritātes IKT jomā kopumā

ROI

Nodrošināt kvalitatīvākus, precīzākus un plašākus datus. Samazināt kļūdas un stiprināt tirgus dalībnieku izpratni.

Datu integritāte

Atbilstoši DORA pamatvirzieniem, fokusēties uz datu autentiskumu, integritāti un dublēšanas risinājumiem, līdz šim mazāk akcentētā jomā.

Mākslīgais intelekts

Piemērot uzraudzības prasības augsta riska MI sistēmām un ierobežotas pārredzamības MI sistēmu riska mazināšanas pasākumus.

Paldies par uzmanību!

Kontaktinformācija:

FAS / Paaugstinātās drošības sistēma

ds.info@bank.lv vai pa tālruni 67022756

Elektronisko pārskatu sistēma

IS_Stat@bank.lv vai tālruņiem 67022299, 67022715 (izmanto MI, ENI)

Finanšu tehnoloģiju uzraudzības pārvalde

dora@bank.lv

LATVIJAS BANKA
EIROSISTĒMA