DORA (DIGITĀLĀS OPERACIONĀLĀS NOTURĪBAS AKTS): PRASĪBAS, IEVIEŠANA UN REGULATORA UZRAUDZĪBA ATBILSTĪBAS FUNKCIJU NODROŠINĀŠANAI

Kursa apraksts:

DORA (Regula (ES) 2022/2554 par finanšu sektora digitālo darbības noturību) ir spēkā no 2025. gada 17. janvāra, un tā ir viena no nozīmīgākajām jaunajām prasībām, kas skar ne tikai IT, bet arī atbilstības (*compliance*) funkciju. Šis viendienas kurss sniedz praktisku skatu uz to, kas DORA ietvaros tiek gaidīts no atbilstības, kādas ir konkrētās prasības, ko nepieciešams sagatavot un ieviest, kā izanalizēt, cik DORA prasības attiecas tieši uz jūsu uzņēmumu (proporcionalitāte), kā ieviešanu pielāgot uzņēmuma lielumam un riska profilam, un ko šajā jomā pārbauda regulators. Kursa laikā lektore dalīsies ar praktiskiem piemēriem un ieteikumiem, kā strukturēt DORA ieviešanas projektu.

Mērķa auditorija:

- Atbilstības, risku pārvaldības un iekšējā audita speciālisti finanšu iestādēs,
- MLRO un citi par atbilstību atbildīgie darbinieki, kuriem DORA ietvaros jāsadarbojas ar IT un drošības funkciju,
- IT drošības un operacionālās noturības speciālisti, kam nepieciešams izprast regulatora un atbilstības skatpunktu,
- Vadītāji un projektu vadītāji, kas atbild par DORA prasību ieviešanu uzņēmumā.

Lektors:

AML/CFT un atbilstības jomas eksperts Natālija Sorokina

Datums, laiks: 2026. gada 28. oktobris 10:00 – 13:20

Valoda: Latviešu

Vieta: Zoom platforma

Dalības maksa: Dalības maksa ir EUR 150,00 +PVN. Reģistrējoties līdz 18.09.2026 dalības maksa ir EUR 110,00 EUR+PVN. Par dalībnieku skaitu 3+ no vienas iestādes tiks piemērota atlaide 10% no rēķinu summas.

DORA (DIGITĀLĀS OPERACIONĀLĀS NOTURĪBAS AKTS): PRASĪBAS, IEVIEŠANA UN REGULATORA UZRAUDZĪBA ATBILSTĪBAS FUNKCIJU NODROŠINĀŠANAI

Vebināra programma:

10:00 - 10:05	Ievads
10:05 - 11:35	**1. sesija** **DORA: nozīme, tvērums, proporcionalitāte un piecu pīlāru prasības** ● DORA (Regula (ES) 2022/2554) vispārīgs raksturojums: mērķis, struktūra, spēkā stāšanās 2023. gada 16. janvārī un piemērošana no 2025. gada 17. janvāra ● Kāpēc DORA ir svarīgs tieši compliance funkcijai, nevis tikai IT: pārvaldības atbildība valdes/padomes līmenī, sankciju un reputācijas risks, saikne ar esošajām AML/CFT un iekšējās kontroles prasībām ● Tvērums (Art. 2) un galvenie izņēmumi; proporcionalitāte (Art. 4 un Art. 16) — kā analizēt, cik pilnībā DORA prasības attiecas tieši uz jūsu uzņēmumu, t.sk. vienkāršotais režīms maziem/nesaistītiem subjektiem un mikrouzņēmumiem ● Praktiska metode uzņēmuma piemērojamības noteikšanai: subjekta statusa noskaidrošana → proporcionalitātes līmeņa noteikšana → riska profila izvērtējums ● Piecu pīlāru prasību pārskats: 1) IKT risku pārvaldības ietvars; 2) IKT incidentu klasifikācija un ziņošana (sākotnējais, starpposma un galīgais ziņojums); 3) digitālās noturības testēšana, t.sk. TLPT (TIBER-EU); 4) IKT trešo pušu risku pārvaldība (Register of Information, līguma klauzulas, kritisko pakalpojumu sniedzēju (CTPP) uzraudzība); 5) informācijas apmaiņa par kiberdraudiem
11:35 - 11:50	Pārtraukums
11:50 - 13:10	**2. sesija** **Sagatavošanās, ieviešana un regulatora uzraudzība** ● Ko praktiski nepieciešams sagatavot: dokumentu un pierādījumu saraksts (politikas, reģistrs, līgumu pielikumi, incidentu žurnāli, testēšanas atskaites, valdes protokoli) ● Kā ieviest DORA prasības atbilstoši uzņēmuma vajadzībām: gap analīze → konstatējumu prioritizācija pēc riska → pakāpeniska ieviešana → pārbaude un uzturēšana ● Ko compliance/iekšēji jāpārbauda: valdes iesaiste un dokumentēšana, IKT reģistra datu kvalitāte, incidentu ziņošanas gatavība, līgumu klauzulas, testēšanas pierādījumi

	• Ko pārbauda regulators (Latvijas Banka) un ES uzraudzības iestādes (EBA/ESMA/EIOPA): reģistra datu kvalitāte, IKT pārvaldības dokumentācija, incidentu žurnāli, testēšanas artefakti, līgumi; Latvijas Bankas 2026. gada uzraudzības prioritātes • Nozares aktuālā situācija: ESA "dry run" pārbaudes rezultāti un secinājumi, kā tos izmantot iekšējai gatavības pašnovērtēšanai; kam sekot līdzi tālāk (Digital Omnibus iniciatīva un iespējamās izmaiņas ziņošanas kārtībā)
13:10 - 13:20	**Noslēgums** Kursa kopsavilkums un praktisks pārbaudes saraksts (checklist) DORA gatavības pašnovērtējumam. Atbildes uz jautājumiem.

Bonusa materiāls: DORA pārbaudes saraksts (checklist)

- Vai ir dokumentēts un valdes/padomes līmenī apstiprināts IKT risku pārvaldības ietvars, un vai tas tiek periodiski pārskatīts?
- Vai ir noskaidrots, kura DORA subjektu kategorija (Art. 2) un proporcionalitātes līmenis (pilnais režīms vai Art. 16 vienkāršotais režīms) attiecas tieši uz uzņēmumu?
- Vai ir izveidots un regulāri atjaunots IKT trešo pušu informācijas reģistrs (Register of Information) atbilstoši standartizētajiem veidlapu formātiem?
- Vai līgumos ar IKT pakalpojumu sniedzējiem, kas atbalsta kritiskas/svarīgas funkcijas, ir DORA obligātās klauzulas (izbeigšanas tiesības, audita tiesības, apakšuzņēmuma nosacījumi)?
- Vai ir izstrādāta un pārbaudīta IKT incidentu klasifikācijas un ziņošanas kārtība (sākotnējais, starpposma un galīgais ziņojums) atbilstoši noteiktajiem termiņiem?
- Vai tiek veikta digitālās noturības testēšana atbilstoši uzņēmuma lielumam, un — ja piemērojams — vai ir novērtēta TLPT (threat-led penetration testing) piemērojamība?
- Vai ir skaidrs, kā uzņēmums seko līdzi jaunumiem (Latvijas Banka, EBA/ESMA/EIOPA vadlīnijas, Digital Omnibus iniciatīva)?