UDK 004.738.5:004.056:061.1EU

Regulatorne spremembe s področja tveganj povezanih z IKT

*Peter Špan**

REGULATORY CHANGES IN ICT AND SECURITY RISK MANAGEMENT

The adoption of the Digital Operational Resilience Act (DORA) eliminates the previous neglect of regulating qualitative rules in the management of operational risks at the first level of EU regulations and influences on competent authority approach on supervision ICT-related risk management in financial institutions The Bank of Slovenia recognizes that it will be necessary to strengthen the supervisory approach in the field of cyber risk management.

The impact of the DORA is mainly seen in more complex requirements for testing IT sistems, which will ensure financial entities to effectively manage ICT-related risks and in the management of critical third-party service providers, where inadequate handling could increase systemic risk. The introduction of a oversight framework for critical third-party ICT service providers, will provide by ESAs, should ensure mitigating outsourcing risk. In ICT incident reporting area requirements follow streamlining, centralization and gradual automation through the introduction of a single point for incident reporting (EU Hub). By agreeing to share information about cyber threats and vulnerabilities, awareness will be improved, better protection solutions can be implemented in a timely manner, and thus increase the opportunity of a faster and more effective response..

Technical standards and guidelines for DORA are being prepared. The first package of these regulations has already been developed and is in public consultation with stakeholders. It is expected to be approved in January 2024, while the second package will be provided by July 2024.

The new rules will affect the activities of financial institutions) and also on supervisors who are entrusted with additional tasks in the oversight of subjects.

At the begging, the activities will mainly be aimed at ensuring regulatory compliance, while further challenges will be related to the implementation of the adopted strategy that enables a high level of digital operational resilience

JEL K14 K24 O33

Uvod

Digitalna operativna odpornost predstavlja pomembno vlogo pri upravljanju operativnih tveganj. V industriji finančnih storitev namreč ustrezna raven odpornosti zmanjšuje možnosti prekinitve in izpadov storitev in s tem zagotavlja nemoteno delovanje notranjega trga EU.

Za krepitev digitalne operativne odpornosti finančnega sektorja je bila v Uradnem listu Evropske unije 27. decembra 2022 objavljena uredba o digitalni operativni odpornosti DORA 2022/2554 (nadalje: DORA), ki je začela veljati 16. januarja 2023, neposredna uveljavitev zahtev pa bo zagotovljena 17. januarja 2025.

DORA opredeli digitalno operativno odpornost kot »sposobnost finančnega subjekta, da vzpostavi, zagotavlja in pregleduje svojo operativno celovitost in zanesljivost, tako da neposredno ali posredno z uporabo storitev tretjih ponudnikov storitev IKT[1] zagotovi celoten sklop zmožnosti, povezanih z IKT, ki so potrebne za obravnavo varnosti omrežnih in informacijskih sistemov, ki jih uporablja finančni subjekt in ki omogočajo nadaljnje opravljanje in kakovost finančnih storitev, tudi v primeru motenj«, kar sposobnost finančnega subjekta širi oz. povezuje s sposobnostjo tretjih ponudnikov storitev.

Pri pripravi zahtev je zakonodajalec upošteval usmeritev, da morajo vsi finančni subjekti pri obravnavanju tveganja na področju IKT uporabljati enak postopek in pravila ob upoštevanju načela proporcionalnosti[2].

DORA uvaja nadzor sistemskih tveganj in tveganj koncentracije, ki jih predstavlja povečana odvisnost finančnega sektorja od tretjih ponudnikov storitev IKT, zato vzpostavlja nadzorni okvir na ravni EU za ključne ponudnike storitev IKT, katerega cilj je zagotoviti ustrezno upravljanje tveganj IKT, ki jih ti ključni ponudniki predstavljajo za finančne subjekte.

* mag. Peter Špan, svetovalec nadzornik, Banka Slovenije, peter.span@bsi.si

[1] Informacijsko-komunikacijska tehnologija.

[2] Upoštevanje velikosti in splošnega profila tveganja subjekta ter narave, obsega in kompleksnosti njih storitev, dejavnosti in poslovanja

Zaradi razdrobljenosti[3] in pomanjkanja kvalitativnih regulatornih zahtev glede upravljanja operativnega tveganja je bila DORA usmerjena tudi v konsolidacijo in nadgraditev zahtev glede upravljanja tveganja na področju IKT.
DORA prinaša harmonizacijo pravil v zvezi z operativno odpornostjo finančnega sektorja, ki se uporabljajo za 21 različnih vrst finančnih subjektov, medtem ko se v primeru direktive NIS2 – 2022/2555 (direktiva o varnosti omrežij in informacij[4]) in direktive CER – 2022/2557 ((11. člen in poglavja III, IV in VI direktive o odpornosti kritičnih subjektov in razveljavitvi direktive Sveta 2008/114/ES[5]) pri uveljavljanju določb uporablja načelo »lex specialis«.

V nadaljevanju so predstavljeni vzroki za nastanek novih predpisov, okvirna vsebina uredbe in trenutni status razvoja izvedbenih predpisov s predvidenim časovnim načrtom realizacije. Na podlagi pregleda posameznih poglavij uredbe so predstavljene predvidene spremembe in možni izzivi, s katerimi se bodo morale spoprijeti banke in nadzorniki.

1. Kronologija z vzroki za nastanek nove regulative

Visoka stopnja digitalizacije in medsebojne povezanosti povečuje tveganje na področju IKT. Celoten finančni sektor EU, ki zajema 22.000 finančnih subjektov, je pri delovanju svojih funkcij (npr. plačila, kliring, poravnave VP, kreditiranje in financiranje, operacije zalednih služb ..) odvisen od uporabe IKT rešitev, ki so vse bolj izpostavljene kibernetskim grožnjam in operativnim motnjam na področju IKT. Odvisnost od digitalizacije se je z medsebojnimi povezavami in odvisnostjo v okviru sektorja ter z uporabo infrastruktur tretjih ponudnikov storitev IKT še poglobila.
Evropska komisija (nadalje: Komisija) je marca 2018 izdala sporočilo za javnost »Akcijski načrt za finančno tehnologijo: za bolj konkurenčen in inovativen evropski finančni sektor«, kjer je poudarila, da je izjemno pomembno povečati odpornost finančnega sektorja EU.
Baselski odbor za bančni nadzor (BCBS) je v decembru 2018 nadzornim institucijam in bankam predstavil poročilo »Cyber Resilience: Range of Practices«, ki prikazuje uporabo različnih praks pri zagotavljanju kibernetske odpornosti po nacionalnih zakonodajah in pozval k krepitvi odpornosti finančnih sistemov.

V aprilu 2019 so evropski nadzorni organi (EBA ,EIOPA in ESMA; nadalje : ESA) oblikovali in izdali skupni tehnični nasvet glede upravljanja IKT tveganj in Komisiji predlagali, da z izboljšanjem zakonodaje na področju upravljanja tveganj povezanih z IKT omogoči okrepitev digitalno operativne odpornosti industrije finančnih storitev.
Evropski odbor za sistemska tveganja (ESRB) je v letnem poročilu za leto 2020 obravnaval in prepoznal možna sistemska kibernetska tveganja, ki bi ob realizaciji lahko vplivala na stabilnost finančnega sistema Unije v pogledu upada likvidnosti in izgube zaupanja v finančne trge.
Pred uvedbo DORA finančni subjekti v EU niso imeli celovitega regulatornega okvira za tveganja na področju IKT, kar je zahtevalo harmonizacijo ključnih zahtev glede digitalne operativne odpornosti. Dodaten izziv za pripravo nove regulative je predstavljala tudi necelovita obravnava upravljanja informacijske varnosti in potreba po harmonizaciji obstoječih pravil oz. določb. Zaradi delne obravnave tematike v različnih predpisih obstajajo vrzeli ali prekrivanja na pomembnih področjih (kot npr. poročanje o incidentih, povezanih z IKT, testiranje digitalne operativne odpornosti) ter neskladja, ki so posledica različnih nacionalnih pravil ali pa je prepoznana stroškovno neučinkovita uporaba prekrivajočih se pravil[6].

2. Vsebina uredbe DORA in subjekti nadzora

Vsebina DORA

DORA opredeljuje zahteve za upravljanje tveganj na področju IKT kot del operativnega tveganja do finančnih subjektov in do nadzornih inštitucij preko ciljno usmerjenih vsebinskih področij:

- Poglavje II - Zmožnosti obvladovanja tveganj na področju IKT.
- Poglavje III - Obvladovanje, klasificiranje in poročanje o incidentih povezanih z IKT
- Poglavje IV - Testiranje operativne digitalne odpornosti.
- Poglavje V - Obvladovanje tveganj tretjih strani na področju IKT.
  Oddelek 1 - Ključna načela za obvladovanje tveganj tretjih strani na področju IKT
  Oddelek 2 - Okvir nadzora nad ključnimi tretjimi ponudniki storitev IKT
- Poglavje VI - Dogovori o izmenjavi informacij o grožnjah in ranljivostih

Subjekti nadzora

DORA se uporablja za 21 različnih vrst finančnih subjektov, med katere uvrščamo tudi vse banke in

[3] Zahteve so bile ločeno obravnavane v različnih pravnih aktih.

[4] Glej uvodno izjavo Direktive (EU) z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji (direktiva o varnosti omrežij in informacij II).

[5] Glej uvodno izjavo in 8. člen Direktive (EU) 2022/2557 z dne 14. decembra 2022 o odpornosti kritičnih subjektov.

[6] Razlike v regulativnih zahtevah ali pri nadzornih postopkih vplivajo predvsem na finančne subjekte, ki poslujejo na čezmejni podlagi.

hranilnice ter plačilne institucije, ki imajo dovoljenje Banke Slovenije za opravljanje storitev, z izjemo SID banke, kar je konkretneje navedeno v uvodu uredbe[7].

3. Izvedbeni akti in časovni načrt priprave predlogov

Za operativno izvedbo zahtev je DORA pooblastila ESA, da pripravijo skupne predloge izvedbenih aktov (tehnične standarde, smernice) z dvema glavnima rokoma za predložitev predlogov Komisiji, in sicer do **17. januarja 2024 (prvi paket)** in **17. julija 2024 (drugi paket)**. V nadaljevanju so predstavljeni posamezni izvedbeni akti po področjih uredbe. Dokumenti , ki so označeni s **krepko pisavo, sodijo v prvi paket predlogov** in so že v javni razpravi od 16. 6. 2023 (razprava bo končana septembra 2023), medtem ko bodo preostali dokumenti, z izjemo »Poziva glede svetovanja pri pripravi delegiranih aktov za nadzor nad zunanjimi izvajalci[8]«, dani v javno razpravo predvidoma do konca novembra 2023.

Poglavje II - Zmožnosti obvladovanja tveganj na področju IKT

- **RTS[9] o okviru za obvladovanje tveganj na področju IKT (15. člen) – prvi paket,**
- **RTS o poenostavljenem okviru za obvladovanje tveganj na področju IKT (16.3 člen) – prvi paket,**
- Smernice o letnih stroških in izgubah zaradi večjih IKT incidentov (11.1 člen).

Poglavje III - Obvladovanje, klasificiranje in poročanje o incidentih povezanih z IKT.

- **RTS o merilih za razvrščanje incidentov povezanih z IKT (18.3 člen) – prvi paket,**
- RTS o določitvi postopka poročanja večjih incidentov povezanih z IKT (20a člen),
- ITS[10] o vsebini poročanja o večjih incidentih povezanih z IKT (20b člen),
- Študija izvedljivosti glede nadaljnje centralizacije poročanja incidentov z vzpostavitvijo enotnega vozlišča (EU Hub) za večje incidente povezane z IKT (21. člen).

Poglavje IV - Testiranje operativne digitalne odpornosti

- RTS za opredelitev vidikov testiranja vdorov na podlagi groženj (26.1 člen).

Poglavje V – Obvladovanje tveganj tretjih strani na področju IKT - Oddelek 1

- **ITS za pripravo predloga registra informacij v zvezi z vsemi pogodbenimi dogovori o uporabi storitev IKT, ki jih opravljajo tretji ponudniki storitev IKT (28.9 člen) – prvi paket,**
- **RTS za podrobno opredelitev vsebine politike o uporabi storitev IKT v zvezi s kritičnimi ali pomembnimi funkcijami, ki jih zagotavljajo tretji ponudniki IKT storitev (28.10 člen) – prvi paket,**
- RTS za opredelitev elementov, ki v primeru sklepanja pogodb o storitvah, ki podpirajo kritične ali pomembne funkcije, določajo pogoje za sklepanje podizvajalskih pogodb (30.5 člen).

Poglavje V - Obvladovanje tveganj tretjih strani na področju IKT (Oddelek 2 - Okvir nadzora nad ključnimi tretjimi ponudniki storitev IKT)

- RTS o harmonizaciji pogojev za izvajanje nadzora (41. člen).
- Smernice o sodelovanju med evropskimi nadzornimi organi in pristojnimi nadzornimi organi glede strukture nadzora (32.7 člen).
- Poziv glede svetovanja pri pripravi delegiranih aktov[11], ki dopolnjujejo besedilo DORA v zvezi z merili za določitev tretjih ponudnikov storitev IKT kot ključnih (31.8 člen) in provizij, ki jih bodo morali ti ponudniki storitev plačati za nadzor (43.2 člen)[12].

4. Pregled zahtev uredbe DORA

Pri upravljanju tveganj, povezanih z IKT, in tveganj zunanjega izvajanja storitev velja, da so finančni subjekti (npr. kreditne in plačilne institucije) zavezani k upoštevanju regulatornih zahtev, ki jih določajo veljavne panožne smernice EBA (Smernice o notranjem upravljanju EBA/GL/2021/05, Smernice o upravljanju tveganj, povezanih z IKT in varnostjo EBA/GL/2019/04, Smernice o zunanjem izvajanju - EBA/GL/2019/02). Zahteve DORA in smernice EBA vsebinsko sledijo istim ciljem (upravljanje informacijske varnosti, upravljanje tveganj zunanjega izvajanja storitev IKT, notranje upravljanje), zato se jih upošteva komplementarno. Panožne smernice (EBA, EIOPA, ESMA) in mednarodni področni standardi (npr. ISO, NIST) so bili izhodišča za pripravo zahtev DORA[13].

[7] 40 odstavek uvoda DORA

[8] Med 26. majem in 23. junijem 2023 je bilo opravljeno javno posvetovanje z dokumentom za razpravo, namenjeno pripravi skupnih nasvetov evropskih nadzornih organov. Končno poročilo mora biti pripravljeno do 30. septembra 2023

[9] Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS) (delegirani predpis)

[10] Implementing Technical Standards (ITS) (implementacijski predpis)

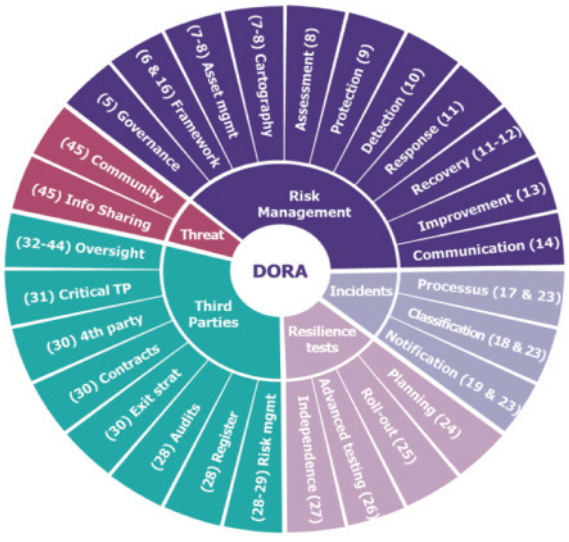
[11] Evropski nadzorni organi začenjajo razpravo o merilih za ključne tretje ponudnike storitev IKT in o pristojbinah za nadzor glej https://www.eiopa.europa.eu/esas-launch-discussion-criteria-critical-ict-third-party-service-providers-and-oversight-fees-2023-05-26_en

[12] Javna razprava je bila opravljena med 26. majem in 23. junijem 2023. Končno poročilo mora biti pripravljeno do 30. septembra 2023.

[13] 47. odstavek uvoda DORA pravi »Ta uredba črpa navdih iz ustreznih mednarodnih, nacionalnih in panožnih najboljših praks, smernic, priporočil in pristopov k obvladovanju kibernetskih tveganj in spodbuja vrsto načel, ki lajšajo splošno strukturiranje obvladovanja tveganj na področju IKT. ....«

Na splošno je mogoče ugotoviti, da DORA in pripadajoči izvedbeni predpisi na posameznih področjih (npr. upravljanje ključnih tretjih ponudnikov IKT storitev, testiranje digitalne odpornosti z naprednimi tehnikami testiranj) zahteve po zagotavljanju upravljanja tveganj povezanih z IKT dodatno opredelijo oziroma poskrbijo za podrobnejšo opredelitev načina izvedbe (npr. opredelitev ključnih tretjih ponudnikov storitev IKT, opredelitev okvira nadzora nad ključnimi tretjimi ponudniki storitev IKT, opredelitev preizkuševalcev v procesu testiranja digitalne operativne odpornosti). Zagotavlja se racionalizacija nekaterih do sedaj ločenih zahtev (npr. združitev in poenotenje poročanja o incidentih). S širitvijo okvira nadzora subjektov (uvedba okvira nadzora ključnih tretjih ponudnikov storitev IKT) poskrbi DORA za krepitev digitalne operativne odpornosti finančnega subjekta[14], tretjih ponudnikov storitev IKT in posledično finančnega sektorja kot celote.
Za zmanjšanje vrzeli pri opredelitvi pojmov uvaja DORA enotno terminologijo. Uvedeni so nekateri novi pojmi (npr. digitalna operativna odpornost), zagotovljena je določena stopnja poenotenja izrazoslovja pri pojmih s področja upravljanja tveganj povezanih z IKT, ki se lahko tako pojavljajo v različnih pravnih aktih (npr. tveganje na področju IKT[15]).
Vsebinsko sestavo zahtev in navedbo konkretnih členov, kjer se tematika obravnava, prikazuje slika A.

Slika A - Ključne vsebine uredbe DORA z navedbo členov



Vir: RiskInsight[16]

[14] Za namen tega prispevka uvrščamo med finančne subjekte kreditne institucije, plačilne institucije in institucije za izdajo elektronskega denarja.

[15] NIST omenjeni pojem označuje kot kibernetsko varnostno tveganje (angl. Cybersecurity risk).

[16] https://www.riskinsight-wavestone.com/en/2023/02/dora-challenges-and-opportunities/

Poglavje II – Obvladovanje tveganj na področju IKT (od 5. do 16. člena)
Pri pripravi določil tega poglavja so bila pričakovanja usmerjena v vzpostavitev specifičnih ukrepov in kontrol za omejitev motenj na trgu in pri poslovanju strank, ki so posledica incidentov, povezanih z IKT. Zagotoviti se je želelo vključenost in odgovornost vodstvenega organa/uprave za obvladovanje tveganj IKT.
Zahteve tega poglavja obravnavajo upravljanje in organizacijo, vzpostavitev okvira upravljanja tveganj povezanih z IKT (osrednji del predstavlja strategija digitalne operativne odpornosti, podrobno je določena struktura omenjene strategije), sisteme in orodja IKT (določena je splošna zahteva po zagotavljanju zanesljivih, zmogljivih in tudi tehnično odpornih rešitev, ki omogočajo delovanje tudi v stresnih razmerah), proces obvladovanja IKT tveganj, varnostno kopiranje in obnovo podatkov iz varnostnih kopij, zahteva po stalnem učenju in razvoju ter aktivnost obveščanja zaposlenih in zunanjih deležnikov.
Z vidika **upravljanja in organizacije** so predvsem določene naloge uprave finančnega subjekta. Dodatno je izpostavljena zahteva po vzpostavitvi vloge na ravni višjega vodstva, ki naj bi zagotavljala nadzor oz. spremljavo dogovorov, sklenjenih s tretjimi ponudniki storitev IKT. Zahtevano je ustrezno zagotavljanje strokovnih kompetenc in obnavljanje znanja vodstva o upravljanju tveganj povezanih z IKT.

Okvir obvladovanja tveganj, sestavljen iz strategije, politik, postopkov in orodij, mora zagotoviti učinkovito obravnavo tveganj na področju IKT in s tem doseganje visoke stopnje digitalne operativne odpornosti. Zato mora biti celovito in ustrezno dokumentiran. Organizacijska struktura, ki naj bi ga izvajala, mora upoštevati jasno opredelitev in ločitev vlog. Uredba na tem mestu navaja, da je odgovornost za obvladovanje tveganj na področju IKT in nadzor nad njimi smiselno dodeliti nadzorni funkciji. Potreba po uveljavitvi modela 3 obrambnih linij verjetno predstavlja odziv na ugotovitev poročila BIS, kjer je bilo prepoznano, da se ustrezna organizacijska struktura za upravljanju tveganj na področju IKT, v nasprotju z drugimi vrstami tveganj (npr. kreditno, tržno tveganje), pri finančnih subjektih še ni v celoti uveljavila.
Proces obvladovanja tveganj povezanih z IKT (od 8. do 11. člena) je razdeljen po zgledu področnega standarda NIST na več funkcij (identificiranje, varovanje in preprečevanje, odkrivanje ter odzivanje in okrevanje), medtem ko se zahteve s področja učenja in razvoja s področja kibernetskih groženj in incidentov povezanih z IKT opirajo na priporočila mednarodnega standarda ISO.

Funkcija **Identificiranje** pojasnjuje potrebo po identifikaciji, klasifikaciji in dokumentiranju virov tveganja na področju IKT, poslovnih funkcij, ki jih podpirajo IKT sistemi, ter informacijskih sredstev in sredstva IKT. Dodatno je določena obveznost rednega (vsaj letnega) pregleda ustreznosti teh razvrstitev in ustrezne dokumentacije. Redno in vsaj enkrat letno je treba izvesti tudi posebno oceno tveganja na področju IKT za vse obstoječe sisteme. Funkcijo tvorijo posamezne kategorije (kot npr. Upravljanje sredstev IKT, Upravljanje tveganj na področju IKT, Strategija upravljanja tveganj itd.). Podrobnejša pojasnila izvajanja teh se pripravljajo v izvedbenih predpisih. Trenutno je na primer objavljen posvetovalni dokument o osnutkih RTS za nadaljnjo harmonizacijo orodij, metod, postopkov in politik na področju IKT za obvladovanje tveganj na področju IKT, kot je določeno v členih 15 in 16(3) DORA. Ustrezna delitev na kategorije je predvidena tudi za preostale funkcije, ki so v opredeljene v nadaljevanju.
V okviru funkcije **Varovanje in preprečevanje** je opredeljena potreba po zaščiti sistemov IKT in uporabi varnostnih orodij, politik in postopkov. Cilj je zagotoviti odpornost in razpoložljivost sistemov IKT ter ohraniti visoko stopnjo razpoložljivosti, avtentičnosti, celovitosti in zaupnosti podatkov. Opredeljena so načela za doseganje teh ciljev. Upoštevanje teh načel naj bi finančni subjekti dosegli z oblikovanjem, sprejetjem in izvajanjem politikih in protokolov (npr. za upravljanje omrežja, upravljanje dostopa do informacijskih sistemov, avtentikacijo, upravljanje sprememb itd.). Za zanesljivo upravljanje omrežja in infrastrukture in učinkovito upravljanje sprememb sta na ravni uredbe vzpostavljeni še dodatni določili[17].
Funkcija **Odkrivanje** predpisuje vzpostavitev mehanizmov za takojšnje odkrivanje neobičajne aktivnosti[18], težav v zvezi z zmogljivostjo omrežja in incidenti povezanimi z IKT. Zahtevana rešitev naj bi zagotavljala tudi odkrivanje posameznih točk, katerih odpoved bi povzročila odpoved celotnega IKT sistema«.[19] Delovanje mehanizma mora uveljaviti več-nivojski sistem nadzora s tehničnimi rešitvami samodejnega mehanizma za opozarjanje odgovornih. Poleg vzpostavitve in izvajanja aktivnosti odkrivanja je zahtevano, da se omenjeni mehanizmi redno preverjajo/testirajo v skladu z zahtevo po testiranju sistemov IKT.
Glede zagotavljanja funkcije **Odzivanje in okrevanje** se od finančnih subjektov pričakuje predvsem vzpostavitev politike neprekinjenega poslovanja na področju IKT. Določen je nabor ciljev[20], ki jim mora omenjena politika z izvajanjem doseči. Politiko neprekinjenega poslovanja se izvaja z dokumentiranimi dogovori, načrti, postopki in mehanizmi. Pričakuje se vzpostavitev, redno posodobljanje in testiranje načrtov neprekinjenega poslovanja, predvsem v povezavi s kritičnimi ali pomembnimi funkcijami, oddanimi v zunanje izvajanje ali zagotovljenimi z dogovori s tretjimi ponudniki storitev IKT. V načrte testiranja je treba vključiti scenarije kibernetskih napadov in preklopov med primarno in sekundarno infrastrukturo IKT in ob tem upoštevati obveznosti, ki izhajajo iz politik in postopkov varnostnega kopiranja in obnove podatkov. V zvezi z odzivanjem je predvideno poročanje pristojnim organom glede ocene skupnih letnih stroškov in izgub, ki nastanejo zaradi večjih incidentov, povezanih z IKT. Način in struktura priprave in poročanja teh podatkov bosta podrobneje opredeljena v skupnih smernicah (smernice za oceno skupnih letnih stroškov in izgub), ki je predvidena v drugem paketu izvedbenih predpisov.

Varnostno kopiranje in obnova podatkov poleg osnovnih zahtev (to so vzpostavitev politik in postopkov, način obnove, zahteve za aktivacijo sistemov kopiranja, testiranja kopiranja in obnove, določanje redundantnih zmogljivosti) predvideva, da je v postopku obnavljanja iz varnostnih kopij podatkov z lastnimi sistemi treba uporabiti sisteme IKT, ki so fizično in logično ločeni od izvornega sistema. Cilje obnove in okrevanja[21] je treba določiti za vsako poslovno funkcijo posebej, pri čemer je treba preveriti, ali gre za kritično ali pomembno funkcijo in ali ima funkcija splošni učinek na učinkovitost trga. Cilji morajo biti postavljeni na način, da tudi v stresnih scenarijih zagotavljajo dogovorjene ravni storitev[22]. Dodatno mora biti posebna skrb usmerjena v ohranjanje celovitosti podatkov, ki med obnovitvijo podatkov po incidentu ne sme biti ogrožena (po rekonstrukciji so potrebni postopki preverjanja), kar velja tudi za zunanje deležnike.
Zahteva po zagotavljanju stalnega **učenja in razvoja** določa vzpostavljanje zmožnosti zbiranja informacij o ranljivostih in kibernetskih grožnjah in incidentih, še zlasti o kibernetskih napadih, ter analiziranje vpliva le-teh na digitalno operativno odpornost. Posledično so podrobneje

[17] Npr. drugi odstavek 9. člena v zvezi z infrastrukturo omrežnih povezav določa » .... finančni subjekti infrastrukturo omrežnih povezav načrtujejo na način, ki omogoča takojšnjo prekinitev ali segmentacijo, da se zmanjša na najmanjšo možno mero in prepreči širjenje negativnih učinkov, zlasti za medsebojno povezane finančne postopke«

[18] V okviru zagotavljanja procesa obvladovanja incidentov povezanih z IKT

[19] angl. Single Point of Failure (SPOF)

[20] Neprekinjenost pomembnih funkcij; učinkovit odziv na vse incidente, povezane z IKT; brez odlašanja aktivirati primerne ukrepe za te incidente; oceniti predhodne učinke, škodo in izgube; določiti komunikacijske ukrepe in ukrepe za obvladovanje kriz.

[21] angl. Recovery Time Objective (RTO) in Recovery Point Objective (RPO)

[22] angl. Service-Level Agreement (SLA)

opredeljene zahteve po učinkoviti naknadni analizi, ki mora biti opravljena po povzročitvi večjih incidentov. Konkretno gre za učinkovitost izvedenih ukrepov v pogledu hitrosti odzivanja ter določanja učinka in resnosti incidentov, povezanih z IKT, učinkovitost izvedbe forenzične analize[23], ustreznost postopka eskalacije problematike na višjo raven odločanja in učinkovito komuniciranje. Pri načrtovanju pregledov okvira obvladovanja tveganj na področju IKT je primerno upoštevati izkušnje pridobljene pri testiranju digitalne operativne odpornosti ali iz primerov dejanskega reševanja realiziranih incidentov, povezanih z IKT. Za krepitev zrelosti glede zagotavljanja digitalne operativne odpornosti je treba zagotoviti redno spremljavo učinkovitosti izvajanja strategije, spremljavo razvoja tveganj, obravnavo in analizo incidentov ter vzorcev kibernetskih napadov. Zahtevana je izdelava redne ocene tveganj na področju IKT. Višje vodstvo na področju IKT mora vsaj enkrat letno poročati upravi o ugotovitvah in podati priporočila.

Sestavni del obvladovanja tveganje je tudi primerno **obveščanje.** Omenjena aktivnost se urejuje predvsem z zahtevo po opredelitvi načrta obveščanja o krizi ter z zahtevo po oblikovanju in izvajanju politike obveščanja notranjih in zunanjih deležnikov o krizi. Dodatno se pričakuje, da bo zagotovljeno razlikovanje pri obveščanju zaposlenih glede na njihovo funkcijo (odgovorne osebe za obvladovanje tveganj – za odzivanje in okrevanje in zaposleni, ki morajo biti le obveščeni). Predvideno je tudi imenovanje vsaj ene odgovorne osebe, ki bo skrbela za izvajanje strategije obveščanja glede incidentov, povezanih z IKT(običajno gre za funkcijo, ki je pristojna za stike z javnostjo).

Za podrobnejše izvajanje uredbe sta bila v tem delu načrtovana dva izvedbena predpisa (RTS o okviru za obvladovanje tveganj na področju IKT, RTS o poenostavljenem okviru za obvladovanje tveganj na področju IKT), ki sta zaradi racionalnosti in enakega konteksta združeno pripravljena v enotnem osnutku.

Dodatno je treba pojasniti, da je uporaba poenostavljenega okvira za obvladovanje tveganj na področju IKT, ki jo predvideva 16. člen, predvidena le za pet kategorij manjših in manj povezanih finančnih subjektov[24] in ne velja za banke in hranilnice.

Poglavje III - Obvladovanje in razvrščanje incidentov, povezanih z IKT, ter poročanje o njih (od 17. do 23. člena)

Zahteve v tem poglavju opredeljujejo obvladovanje, klasificiranje in poročanje o večjih kibernetskih incidentih kakor tudi o operativnih ali varnostnih incidentih povezanih s plačili (slednji zadevajo kreditne in plačilne institucije, ponudnike storitev zagotavljanja informacij o računih, institucije za izdajo elektronskega denarja). Namen zahtev je uskladiti in centralizirati poročanje o incidentih, ki bi regulatorju omogočalo hiter odziv in preprečevalo morebitno širjenje negativnega vpliva po sistemu, za finančne subjekte pa bi pomenilo racionalizacijo poročanja večjih incidentov.

Postopek **obvladovanja incidentov** zajema odkrivanje, obvladovanje in obveščanje o incidentih. Poleg incidentov se evidentirajo tudi pomembne kibernetske grožnje. Postopki spremljanja in obravnavanja incidentov se vzpostavijo s ciljem prepoznavanja, dokumentiranja in obravnavanja temeljnih vzrokov. Postopek obsega določitev kazalnikov za zgodnje opozarjanje, načine za identifikacijo, kategoriziranje in razvrščanje incidentov glede na pomembnost storitev, organiziranost dela glede na različne scenarije incidentov, načrtovanje obveščanja deležnikov, postopek eskalacije poročanja o incidentu na višje ravni odločanja in postopke odziva za zmanjšanje učinka incidenta.

Razvrščanje pomembnosti incidentov in kibernetskih groženj poteka na podlagi meril (npr. za incidente: obseg in pomembnost strank, trajanje incidenta itd.; za grožnje: kritičnost storitev, kjer obstaja tveganje, geografska razpršenost ogroženosti itd.). Pravila razvrščanja (in pragovi pomembnosti za določanje večjih incidentov) so podrobneje pojasnjena v osnutku izvedbenega predpisa »RTS o merilih za razvrščanje incidentov povezanih z IKT (18.3 člen)«, ki je že v javni razpravi.

Finančni subjekt mora zagotoviti **poročanje pristojnemu organu o večjih IKT incidentih.**[25] V primeru pristojnosti več organov je mogoče določiti en sam organ, ki se mu pošilja poročilo. V primeru poročanja pomembnih kreditnih institucij prejemnik poročila obvesti tudi ECB. Obveščanje o pomembnih kibernetskih grožnjah je prostovoljno, v primeru poročanja pomembnih kreditnih institucij se o tem obvesti tudi ECB. Države imajo možnost sprejeti odločitev, da omenjene informacije delijo s skupino za odzivanje na incidente na področju računalniške varnosti (CSIRT). Ob večjem incidentu, ki bi finančno prizadel stranke, se mora

[23] Kakovost in hitrost

[24] Med te sodijo:
- mala in nepovezana investicijska podjetja;
- plačilne institucije, izvzete na podlagi Direktive (EU) 2015/2366,
- institucije, izvzete na podlagi Direktive 2013/36/EU, če se ne uporabi možnosti iz 4 odstavka 2. člena te uredbe,
- institucije za izdajo e-denarja, izvzete na podlagi Direktive 2009/110/ES,
- male institucije za poklicno pokojninsko zavarovanje.

[25] Predstavlja enotno in edino vstopno točko za oddajo obvestil oz. poročil.

te takoj obvestiti, medtem ko se v primeru pomembne kibernetske grožnje stranke obvesti le po potrebi, da te sprejmejo ukrepe za lastno zaščito. V zvezi s poročanjem incidentov je predvideno trifazno poročanje z začetnim obvestilom, vmesnim obvestilom in končnim poročilom[26]. Opredeljeni so tudi roki za posredovanje le-teh pristojnemu organu.
Po prejemu obvestil morajo pristojni organi poročilo dopolniti s podrobnostmi in ga posredovati različnim prejemnikom. EBA, ESMA, EIOPA in ECB po prejemu informacij in po posvetovanju z ENISA ter v sodelovanju z ustreznimi pristojnimi organi ocenijo, če je treba o incidentu obvestiti tudi pristojne organe v drugih državah. Podrobnejše izvajanje zahtev bo opisano v osnutkih izvedbenih predpisov »RTS o določitvi postopka poročanja večjih incidentov povezanih z IKT (20a člen), in »ITS o vsebini poročanja o večjih incidentih povezanih z IKT (20b člen)«. Omenjena predpisa sta uvrščena v drugi paket priprave in bosta Komisiji predstavljena do 17. julija 2024.
Poleg racionalizacije in vzpostavitve enotne točke poročanja je pomembna tudi **centralizacija poročanja o večjih incidentih, povezanih z IKT.** V ta namen se bo izdelala »Študija izvedljivosti glede nadaljnje centralizacije poročanja incidentov z vzpostavitvijo enotnega vozlišča (EU Hub) za večje incidente povezane z IKT«, ki je tudi uvrščena v drugi paket priprave dokumentacije. Določeni so potrebni elementi te študije (pogoji, koristi, zmožnosti, tehnične ureditve, stroški).
Predvidene so tudi **povratne informacije nadzornih organov**[27]**.** Po prejemu poročil pristojni organi potrdijo prejem in **po potrebi** zagotovijo povratne informacije ali visokonivojske smernice[28]. Dodatno je možna razprava o ukrepih finančnega subjekta, ki jih bo ta izvedel za zmanjšanje škodljivega vpliva.
Zahteve glede poročanja incidentov in priprave povratnih informacij veljajo tudi za primere operativnih ali varnostnih incidentov, ki so povezani s plačili.

Poglavje IV – Testiranje digitalne operativne odpornosti (od 24. do 27. člena)
Zahteve glede testiranja digitalne operativne odpornosti zajemajo splošne zahteve za izvajanje testiranja, testiranje sistemov in orodij IKT, napredno testiranje orodij, sistemov in postopkov IKT s pomočjo penetracijskega testiranja na podlagi analize groženj ter zahteve za preizkuševalce za izvedbo penetracijskega testiranja na podlagi analize groženj.

Splošne zahteve za izvajanje testiranja opredeljujejo namen testiranja digitalne operativne odpornosti (preverjanje pripravljenosti na incidente, odkrivanje pomanjkljivosti pri zagotavljanju odpornosti in ustreznost izvedbe korektivnih ukrepov). Pričakuje se vzpostavitev celovitega programa za testiranje digitalne operativne odpornosti, ki pri izvajanju upošteva načelo proporcionalnosti, krajino tveganj ter kritičnost informacijskih sredstev in storitev, ki jih finančni subjekt uporablja oz. ponuja. Program predvideva izvajanje različnih testiranj[29] s širokim naborom scenarijev in vključuje vrste ocen, testov, metodologij, praks in orodij, ki bodo uporabljena pri preverjanju. Testiranje izvajajo notranje ali zunanje neodvisne strani. V primeru izvedbe z notranjimi preizkuševalci je treba poskrbeti za zadostna sredstva in preprečiti nasprotja interesov. Vzpostaviti je treba postopke za prednostno obravnavo in odpravo težav, ki bi se pojavile med testiranjem, in potrebni validacijski postopek za ugotavljanje celovitosti obravnave prepoznanih pomanjkljivosti ali vrzeli. Najmanj enkrat letno je treba zagotoviti ustrezno testiranje vseh sistemov in aplikacij IKT, ki podpirajo kritične ali pomembne funkcije.

Preverjanje z naprednim testiranjem sistemov s pomočjo penetracijskega testiranja na podlagi analize groženj (angl. Threat-Led Penetration Testing (TLPT)) daje z višjo stopnjo zagotovil o ravni digitalne odpornosti inštitucije.
Finančne subjekte, ki morajo izvesti napredno testiranje na podlagi penetracijskega testiranja na podlagi analize groženj (v nadalje: napredno testiranje), določijo pristojni organi na podlagi različnih dejavnikov, npr. ocene učinkov (obseg storitev, ki jih izvaja finančni subjekt), ki bi vplivali na finančni sektor; pomislekov glede finančne stabilnosti in sistemske narave finančnega subjekta na državni ravni ali ravni EU; profila tveganja na področju IKT, stopnje zrelosti na področju IKT ali značilnosti vključene tehnologije) ob upoštevanju načela proporcionalnosti. Izvajanje naprednega testiranja je zahtevano vsaj vsaka 3 leta, pristojni organi lahko zahtevajo bolj pogosto izvajanje. Napredno testiranje mora obsegati pomembne funkcije in se izvaja na aktivnih produkcijskih sistemih, ki podpirajo take funkcije. Pred izvedbo testiranj je potrebna identifikacija sistemov, postopkov in tehnologij, ki podpirajo pomembne funkcije,

[26] Končana analiza osnovnega vzroka.

[27] ESA na anonimni podlagi in združeno enkrat letno zagotovi poročilo o večjih incidentih, povezanih z IKT (navede se število, narava in učinek incidentov, izvedene popravne ukrepe in nastale stroške), hkrati omenjeni organi izdajo opozorila in statistične podatke na visoki ravni za oceno groženj in ranljivosti na področju IKT.

[28] Zagotovi se dostop do relevantnih anonimiziranih informacij in do podatkov o podobnih grožnjah.

[29] Test ranljivosti, analiza odprtokodnega sistema, test varnosti omrežja, pregled programske opreme, analiza razlike, test fizične varnost, pregled izvorne kode, test na podlagi scenarijev, integralni test, vdorni oziroma penetracijski test.

ter storitev IKT, ki podpirajo pomembne funkcije in so oddane v zunanje izvajanje. Finančni subjekti sami določijo, katere funkcije bodo zajeli v testiranje in določijo obseg izvedbe testiranja, ki pa ga morajo potrditi še pristojni organi. V obseg testiranj so lahko vključeni tudi tretji ponudniki storitev IKT. Finančni subjekt mora sprejeti ustrezne zaščitne ukrepe tudi v zvezi s sodelovanjem tretjih ponudnikov storitev IKT v naprednem testiranju[30]. V primeru uporabe notranjih preizkuševalcev je treba vsak tretji zaporedni test opraviti z zunanjim preizkuševalcem. Uporabo notranjih preizkuševalcev za izvedbo naprednega testiranja mora predhodno odobriti pristojni javni organ za zadeve povezane s penetracijskim testiranjem. Možna je izvedba skupnega testiranja, ki se opravi v primerih, ko tretji ponudnik zagotavlja IKT storitve več finančnim subjektom hkrati. Tretji ponudnik storitev IKT in finančni subjekt se pisno dogovorita o možnosti, da ponudnik storitev IKT sklene pogodbeni dogovor o izvedbi testiranja neposredno z zunanjim preizkuševalcem.
Od pomembnih kreditnih institucij se zahteva, da za napredno testiranje uporabijo le tiste zunanje preizkuševalce, ki izpolnjujejo zahteve za preizkuševalce za izvedbo penetracijskega testiranja na podlagi analize groženj, kot so določene v 27. členu DORA.
Po končanem testiranju se zahteva, da finančni subjekt javnemu organu, ki je na nacionalni ravni odgovoren za zadeve, povezane s penetracijskim testiranjem na podlagi analize groženj v finančnem sektorju[31], predloži povzetek relevantnih ugotovitev, sanacijske načrte in dokumentacijo, ki dokazuje, da je bilo testiranje izvedeno v skladu z zahtevami. Omenjeni organ izda potrdilo, da je bilo testiranje izvedeno v skladu z zahtevami. Finančni subjekti morajo pristojni organ uradno obvestiti o potrdilu ter predložiti povzetek o relevantnih ugotovitvah in sanacijskem načrtu.
Za podrobnejša pojasnila glede meril za določitev finančnih subjektov, ki morajo opraviti napredno testiranje: standardi za notranje preizkuševalce, zahteve testiranja glede obsega, metode, rezultati ter vrste sodelovanja nadzornih organov, ki je potrebno za izvedbo naprednega testiranja (tudi vzajemnega priznavanja v primeru delovanja finančnega subjekta v več državah), je v pripravi osnutek regulatornih tehničnih standardov. Kot del drugega paketa izvedbenih predpisov bo Komisiji predložen do 17. julija 2024.

[30] Odgovornost za izpolnjevanje zahtev naprednega testiranja ostaja na finančnemu subjektu.

[31] Če tovrstni organ ni imenovan, lahko pristojni organ, z izjemo določanja finančnih subjektov, ki morajo izvesti napredno testiranje, prenese naloge (potrditev obsega testiranja, odobravanje preiskovalcev, potrjevanje testiranj) na drug pristojni organ.

Poglavje V/I – Obvladovanje tveganj tretjih strani na področju IKT (od 28. do 44. člena)

Oddelek I - **Ključna načela za dobro obvladovanje tveganj tretjih strani na področju IKT**
Zahteve za obvladovanje tveganj tretjih strani na področju IKT določajo načela, predhodna ocena tveganja koncentracije na področju IKT na ravni subjekta in opredelitev ključnih pogodbenih določil.
Za učinkovito upravljanje tveganja tretjih strani na področju IKT se zahteva sklenitev pogodbenih dogovorov in obvladovanje zadevnega tveganja z upoštevanjem načela proporcionalnosti[32]. Finančni subjekt mora sprejeti strategijo glede tveganja tretjih strani na področju IKT (le-ta vključuje politiko o uporabi zunanjih storitev IKT, ki podpirajo pomembne funkcije), ki jo mora redno pregledovati. Naloga uprave je redno pregledovanje tveganja v zvezi s pogodbenimi dogovori za storitve IKT, ki podpirajo pomembne funkcije.
Od finančnega subjekta se pričakuje, da vzpostavi in posodablja register informacij v zvezi z vsemi pogodbenimi dogovori o uporabi storitev IKT. Zahtevano je redno letno poročanje pristojnim organom o sklenjenih dogovorih. Poročilo zajema informacijo o številu novih dogovorov, kategorije tretjih ponudnikov, vrste pogodbenih dogovorov ter storitve in funkcije IKT, ki jih ti opravljajo. Pristojni organ lahko zahteva predložitev celotnega registra informacij. Pristojni organi morajo biti pravočasno obveščeni tudi o načrtovanem pogodbenem dogovoru o uporabi storitev IKT, ki bodo podpirale kritične ali pomembne funkcije.
Pred uporabo tretjega ponudnika storitev IKT mora institucija oceniti, če storitev podpira pomembno funkcijo in če so izpolnjeni vsi pogoji za sklenitev pogodbenega dogovora. Oceniti je treba vsa pomembna tveganja, vključno s tveganjem koncentracije, in opraviti skrbni pregled ponudnika storitev IKT ter preveriti, če obstaja možnost nasprotja interesov, ki bi nastala s sklenitvijo dogovora.
Pri sklepanju dogovorov mora biti finančni subjekt pozoren na sposobnost izpolnjevanja standardov informacijske varnosti. Pomembna je tudi privolitev ponudnika glede uveljavitve pravic do dostopa, inšpekcijskih pregledov in revizij pri tretjem ponudniku storitev IKT. Pogodbeni dogovori morajo omogočati prekinitev dogovora v primeru določenih okoliščin (npr. znatna kršitev predpisov ali pogodbe ipd.).

[32] Upoštevajo se narava, obseg, zapletenost in pomen odvisnosti, povezanih z IKT; tveganja, ki izhajajo iz pogodbenih dogovorov o uporabi storitev IKT, kritičnost ali pomen posamezne storitve ter možen učinek na neprekinjenost in dostopnost storitev.

Finančni subjekt mora v primeru, ko najete storitve IKT podpirajo pomembne funkcije, sprejeti učinkovite izhodne strategije. Pogodbe morajo omogočati prekinitev brez motenj v dejavnosti subjekta ali omejitev skladnosti z zakonskimi zahtevam. Izhodni načrti morajo biti dokumentirani, testirani in redno pregledovani. Zagotoviti je treba alternativne rešitve, ki omogočajo, da se lahko storitve IKT prenese k drugemu ponudniku ali pa se storitev prevzame v lastno izvajanje.
Osnutek tehničnih standardov za vzpostavitev standardnih predlog za namene registra informacij, vključno z informacijami, ki so skupne vsem pogodbenim dogovorom o uporabi storitev IKT, je v pripravi. Ravno tako je v pripravi osnutek regulativnih tehničnih standardov, ki bodo podrobneje opredelili vsebino politike o uporabi storitev IKT, ki podpirajo kritične ali pomembne funkcije in jih opravljajo tretji ponudniki storitev IKT. Oba osnutka sta že v javni razpravi. Rok za predložitev obeh tehničnih standardov Komisiji je 17. januar 2024.

Predhodna ocena tveganja koncentracije na področju IKT na ravni subjekta je sestavni del identificiranja in ocenjevanja tveganj tretjih ponudnikov storitev IKT. Pri tem finančna institucija preveri, če storitve IKT ni mogoče enostavno nadomestiti, če obstaja večje število pogodb za podporo kritičnih funkcij z istim ponudnikom, ter preveri koristi in stroške alternativnih rešitev. V primeru oddajanja storitev IKT, ki podpira pomembne funkcije, v nadaljnje podizvajanje izvajalcu, ki ima sedež v tretji državi, je treba preveriti morebitne omejitve (npr. lokalna zakonodaja, skladnost s pravili EU glede zagotavljanja varstva podatkov).

Finančni subjekt mora v pogodbene dogovore vključevati predpisane bistvene elemente (jasen in celovit opis vseh funkcij in storitev IKT; lokacija, kjer se funkcija izvaja; določbe o razpoložljivosti, avtentičnosti, celovitosti in zaupnosti v zvezi z varstvom podatkov itd.), medtem ko je treba za pogodbe o uporabi storitev IKT, ki podpirajo pomembne funkcije, poleg omenjenih elementov zagotoviti še dodatne določbe (celoviti opisi ravni storitev, odpovedni roki, zahteve po testiranju storitev IKT, zahteve po sodelovanju v penetracijskem testiranju, zahteve po stalnem spremljanju uspešnosti, izhodne strategije).
Za podrobnejše izvajanje zahtev bo oblikovan osnutek regulativnih tehničnih standardov, kjer se bodo natančneje opredelili elementi, ki jih mora finančni subjekt določiti in oceniti pri podizvajanju storitev IKT, ki podpirajo kritične ali pomembne funkcije. Rok za predložitev izvedbenega predpisa Komisiji je 17. julija 2024.

Poglavje V/II – Obvladovanje tveganj tretjih strani na področju IKT
Oddelek II - **Okvir nadzora nad ključnimi tretjimi ponudniki storitev IKT**

DORA prinaša nov način nadzora nad ključnimi tretjimi ponudniki storitev IKT, ki predstavlja širjenje pooblastil evropskih nadzornikov. Okvir nadzora opredeljuje imenovanje/določanje ključnih tretjih ponudnikov storitev IKT, določa strukturo okvira nadzora in naloge glavnega nadzornika, določa način usklajevanja med glavnimi nadzorniki ter pojasni, s kakšnimi pooblastili ta razpolaga v EU, medtem ko so za izvrševanja pooblastil zunaj EU določeni dodatni pogoji. Podrobneje so predstavljena pooblastila glavnega nadzornika (zahteva po predložitvi informacij, splošne preiskave, inšpekcijski pregledi, stalni nadzor) in harmonizacija pogojev, ki omogoča izvajanje nadzorniških dejavnosti ter nadomestila za izvajanje nadzora.
Določena so merila za **imenovanje ključnih tretjih ponudnikov storitev IKT** (npr. sistemski učinek na stabilnost finančnih storitev, sistemska narava oz. pomen finančnih subjektov, ki so odvisni od zadevnega ponudnika itd.). ESA preko skupnega odbora na podlagi teh meril določijo oz. imenujejo tretjega ponudnika storitev IKT in poskrbijo za vsakoletno objavo posodobljenega seznama ključnih tretjih ponudnikov storitev IKT na ravni EU. Pristojni organi pa so zavezani, da na letni ravni nadzorniškemu forumu zagotavljajo ustrezna poročila (seznam dogovorov s tretjimi ponudniki storitev IKT), da lahko ESA na podlagi teh ocenijo odvisnost finančnih subjektov od tretjih ponudnikov.

Opredeljena je **struktura okvira nadzora** (zagotavlja ga pododbor skupnega odbora ESA - nadzorniški forum[33]) in sestava nadzorniškega foruma, ki ima opredeljene naloge, kot npr. letna ocena rezultatov in ugotovitev nadzorniških dejavnosti, usklajevalni ukrepi za krepitev digitalne operativne odpornosti itd. Hkrati forum ponuja podporo nalogam skupnega odbora in glavnemu nadzorniku.
Za podrobno razlago zahtev so v pripravi smernice o sodelovanju med ESA in pristojnimi organi, ki zajemajo podrobne postopke in pogoje za razdelitev in izvajanje nalog med pristojnimi organi in evropskimi nadzornimi organi ter podrobnosti glede izmenjave informacij.
Smernice so del drugega paketa dokumentacije, ki bo Komisiji predložen v potrditev do 17. julija 2024.

[33] Vsaka država članica imenuje ustrezni pristojni organ, katerega član osebja je predstavnik na visoki ravni.

Glavni nadzornik predstavlja glavno kontaktno točko za vsa vprašanja glede nadzora. Zagotavlja izvedbo določenih nalog (kot npr. izvajanje ocene kritičnih tretjih ponudnikov storitev glede zagotavljanja učinkovitega sistema za obvladovanje tveganj na področju IKT, osredotočeno na zagotavljanje informacijske varnosti[34]). Glavni nadzornik je odgovoren za sprejem podrobnega in jasno obrazloženega individualnega načrta nadzora vsakega kritičnega tretjega ponudnika, ki vsebuje opis letnih ciljev ter načrtovanih ukrepov v zvezi z nadzorom.
Za učinkovit nadzor ESA je predvideno **operativno usklajevanje** glede postopka izvajanja nadzorne strategije in vzpostavitev nadzorne mreže za potrebe usklajevanja priprav, za izvajanje dejavnosti nadzora nad ključnimi ponudniki IKT ter usklajevanje glede ukrepov. Za opisane zahteve pripravi glavni nadzornik skupni protokol o nadzoru.
Pri **izvajanju nalog nadzora** v zvezi s ključnimi tretjimi ponudniki storitev IKT **ima glavni nadzornik različna pooblastila** (npr. zahteva po informacijah in dokumentaciji, splošne preiskave in inšpekcijski pregledi[35], izdaja priporočil, določanje pogojev, pod katerimi lahko tretji ponudniki zagotavljajo storitve IKT, odločanje o podizvajanju ponudnikov, zahteva po opustitvi nadaljnjih dogovorov o podizvajanju itd.). Pred izvrševanjem pooblastil se posvetuje z nadzorniškim forumom. Pri neposrednem izvrševanju pooblastil pregleda mu pomaga pregledniška ekipa, katere sestavo[36] in kompetence določa 40. člen.
Pričakuje se, da ključni tretji ponudniki storitev IKT sodelujejo z glavnim nadzornikom. V primeru popolnega ali delnega neizpolnjevanja ukrepov lahko glavni nadzornik sprejme odločitev o periodični denarni kazni, ki jo mora razkriti javnosti.
Za izvajanje pooblastil zunaj EU mora glavni nadzornik upoštevati dodatne pogoje (npr. za izvedbo pregleda v tretji državi mora biti pristojni organ tretje države obveščen in ne sme nasprotovati pregledu). ESA je pooblaščen, da sklene s pristojnim organom tretje države dogovor o sodelovanju, pri čemer so v DORA določeni elementi dogovora.
Podrobnejše izvajanja zahtev v zvezi z okvirom nadzora bo določeno z osnutkom RTS za informacije za prostovoljno imenovanje ključnega ponudnika in strukturo potrebnih informacij, ki jih mora ta predložiti. S tehničnimi standardi bodo določena tudi podrobnejša merila za sestavo pregledniških ekip in podrobnosti glede ocene pristojnih organov o ukrepih, ki so jih ključni tretji ponudniki storitev IKT sprejeli na podlagi priporočil glavnega nadzornika. Izvedbeni predpis je del drugega paketa in bo na voljo za potrditev do 17. julija 2024.
Predpisan je tudi postopek komuniciranja med glavnim nadzornikom in ključnim tretjim ponudnikom storitev IKT (npr. 60 dnevni rok za odgovor glede upoštevanja priporočila) in pogoji za javno razkritje neskladnosti. Določeni so tudi postopek in merila za uporabo skrajnega ukrepa, ki ga izdajo pristojni organi, na primer zahteve po ustavitvi uporabe storitev, če subjekti ne obravnavajo tveganj iz priporočil. Glavni nadzornik lahko na zahtevo zagotovi dodatna pojasnila o izdanih priporočilih.
Glavni nadzornik zaračuna storitve nadzora ključnemu tretjemu ponudniku storitev v obliki nadomestil za izdatke za nadzor (npr. stroški dela pregledniške ekipe, storitve neodvisnih strokovnjakov itd.). Znesek nadomestila je sorazmeren z ustvarjenim prometom ponudnika. Za podrobnejše izvajanje te zahteve bo oblikovan osnutek delegiranega akta, ki bo določil višino nadomestil in način njihovega plačila. Osnutek bo predložen Komisiji do 17. julija 2024.

Poglavje VI – Dogovori o izmenjavi informacij (45. člen)

Dogovori o izmenjavi informacij in obveščevalnih podatkov o kibernetskih grožnjah

Ozaveščanje o kibernetskih grožnjah povečuje digitalno operativno odpornost tako, da omogoča omejitev širjenja kibernetskih groženj in krepi obrambne zmožnosti ter tehnike odkrivanja groženj in posledično vpliva na izboljšanje odzivanja in okrevanja.
Zaželeno je, da si finančni subjekti (in tretji ponudniki storitev IKT) med seboj izmenjujejo informacije in obveščevalne podatke o kibernetskih grožnjah. Izmenjava mora potekati v okviru zaupanja vredne skupnosti, ki z dogovori zagotavlja ustrezno zaščito informacij z občutljivo naravo (npr. spoštovanje poslovne zaupnosti, varstva osebnih podatkov). Pri izmenjavi je možna uporaba namenskih informacijskih platform. Finančni subjekti morajo pristojne organe obvestiti o tovrstnem sodelovanju.

5. Morebitni izzivi

Povečanje odvisnosti od IKT in odvisnosti od finančnih subjektov od tretjih ponudnikov storitev IKT, ki ponujajo storitve večjemu naboru subjektov, ob morebitni nizki stopnji digitalne operativne odpornosti omenjenih partnerjev, poleg povečanja izpostavljenosti tveganjem povezanim z

[34] Ocena zajema 9 različnih področij informacijske varnosti.

[35] Pooblastila so podrobneje pojasnjena od 37. do 40. člena DORA.

[36] Pregledniško skupino sestavlja osebje iz ESA, osebje ustreznih pristojnih organov, ki nadzorujejo finančne subjekte, ki jim ključni tretji ponudnik storitev IKT zagotavlja storitve IKT. Na prostovoljni ravni se lahko pridruži predstavnik pristojnega nacionalnega organa iz države članice, v kateri ima sedež ključni tretji ponudnik storitev IKT.

IKT, povečuje tudi izpostavljenost sistemskemu tveganju. Predstavljena regulativa si prizadeva za uvedbo novih in ostrejših pravil, ki jih mora upoštevati širši krog subjektov, ki sodelujejo v finančni industriji. Namen regulative je višja raven digitalne operativna odpornosti tako posameznega subjekta kot tudi sistema kot celote. Izboljšanje odpornosti naj bi se zagotovilo z upoštevanjem zahtev predstavljenih v petih ključnih poglavjih uredbe.

Finančni subjekti, ki so v pristojnosti Banke Slovenije, so z večjim delom zahtev že seznanjeni prek panožnih smernic in jih je večina že uspela zadovoljivo integrirati v lastni proces upravljanja operativnih tveganj. Pri tem je treba opozoriti, da so tokratne zahteve usmerjene v bolj podrobno in sistematično opredeljevanje zahtev ter v izboljšanje obstoječih praks pri obvladovanju tveganj povezanih z IKT, kar bo od subjektov zahtevalo dodatne napore za posodobitev okvira upravljanja teh tveganj in povečevalo stroške zaradi potrebnih investicij v dodatne zmogljivosti in nadgradnjo varnostnih rešitev.

Med največje spremembe je mogoče uvrstiti zahteve po testiranju digitalne operativne odpornosti, kjer so se te z izvajanjem naprednega testiranja izenačile z zahtevami, ki so bile predvidene za kritično infrastrukturo. Uvedba okvira skupnega nadzora ESA nad ključnimi tretjimi ponudniki storitev IKT s celotno paleto pooblastil in možnih ukrepov nadzornika predstavlja novost, ki si bo prizadevala za povečanje stopnje informacijske varnosti teh ponudnikov in bo skrbela za omejevanje sistemskih tveganj.

Dodatno lahko na izboljšanje digitalne operativne odpornosti vpliva ustreznejša pripravljenost na odziv, ki je posledica ustreznega obsega uspešno opravljenih zahtevnih testiranj in ob tem pridobljenih izkušenj o načinu ukrepanja v primeru pojavitve incidenta. Učinkovit sistem prepoznavanja in poročanja večjih incidentov ter ukrepanja na podlagi povratnih informacij preprečuje enostavno in hitro širitev incidentov v druga okolja. Spodbujanje medsebojne izmenjave informacij, ki so koristne za organizacijo obrambe pred novimi kibernetskimi grožnjami, izboljšuje kakovost odziva v primeru kibernetskega incidenta.

Pri tem se je treba zavedati, da bi moralo zagotavljanje skladnosti z zahtevami DORA finančnim subjektom predstavljati le prvi korak na poti k ciljni stopnji digitalne operativne odpornosti subjekta, ki bi morala biti dokumentirana v strategiji in bi predstavljala potencial subjekta za razvoj oz. prilagajanje poslovnega modela zahtevam trga. Za doseganje želenega stanja je treba vključiti vodstvene strukture, ki morajo prevzeti iniciativo za uvajanje potrebnih sprememb. Ustrezno zagotovilo, da so si upravljalni organi zadali resen cilj na področju informacijske varnosti, je določitev digitalne operativne odpornosti za enega od kazalnikov pri ocenjevanju uspešnosti uprave na področju doseganja poslovnih ciljev.

Finančni subjekti bodo morali najprej opraviti ustrezno analizo razlikovanja glede skladnosti z novo regulativo in sprejeti načrt za uskladitev z novimi zahtevami ter zagotoviti redno spremljavo učinkovitosti realizacije in po potrebi sprejeti korektivne ukrepe.

Za doseganje omenjenih ciljev (regulatorna skladnost, digitalna operativna odpornost kot konkurenčna prednost) bodo morali finančni subjekti zagotoviti ustrezne kadrovske in finančne vire. Pri tem bodo večji finančni subjekti in subjekti, ki si lahko obetajo pomoč v okviru svoje finančne skupine, v določeni prednosti, ker bodo lažje dostopali do potrebnih strokovnih znanj in kompetenc ter obsega virov, medtem ko manjši finančni subjekti praviloma težje pravočasno zagotovijo ustrezne kadrovske in finančne vire.

Zaradi pomanjkanja nadzorniških praks v zvezi z nekaterimi novimi regulatornimi zahtevami so se pred novimi izzivi znašli tudi nadzorniki. Za vzpostavitev učinkovitega nadzora nad novimi subjekti (ključni tretji ponudniki storitev IKT) se bodo morali nadzorniki soočiti s potrebnimi organizacijskimi prilagoditvami in poskrbeti za ustrezne vire in strokovno usposabljanje.

Literatura in viri:

Uredba (EU) 2022/2554 evropskega parlamenta in sveta o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32022R2554

Direktiva (EU) 2016/1148 evropskega parlamenta in sveta o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji

https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Direktiva (EU) 2022/2557 evropskega parlamenta in sveta o odpornosti kritičnih subjektov in razveljavitvi Direktive Sveta 2008/114/ES https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32022L2557&qid=1693820389394

EK, sporočilo za medije : Finančna tehnologija: Komisija sprejela ukrepe za konkurenčnejše in inovativnejše finančne trge https://ec.europa.eu/commission/presscorner/detail/sl/IP_18_1403

BIS, poročilo Basel Committee on Banking Supervision, Cyber resilience: Range of practices

https://www.bis.org/bcbs/publ/d454.pdf

ESAs, Skupni nasvet EK glede tveganj IKT in kibernetske varnosti

https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf

ESRB, letno poročilo 2020 : Systemic cyber risk

ttps://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200219~61abad5f20.en.html

EBA, Smernice o upravljanju tveganj povezanih z IKT, nov 2019

https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/Updated%20Translations/880827/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management_COR_SL.pdf

EBA. Smernice o zunanjem izvajanju, februar 2019

https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2761380/e19a89c6-dd8d-4b0c-8aca-0905ed82c2df/EBA%20revised%20Guidelines%20on%20outsourcing_SL.pdf?retry=1

EBA, Smernice o notranjem upravljanju, julij 2021

https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/EBA-GL-2021-05%20Guidelines%20on%20internal%20governance/translations/1021309/GL%20on%20internal%20governance%20under%20CRD_SL%20-%20updated.pdf?retry=1

NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, USA, 16 April 2018 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf)

ISO/IEC 27032/2012 Information technology — Security techniques — Guidelines for cybersecurity

ltps://store.pecb.com/products/isoiec-27032-guidelines-for-cybersecurity#:~:text=ISO%2FIEC%2027032%3A2012%20provides%20guidance%20for%20improving%20the%20state,internet%20security%2C%20and%20critical%20information%20infrastructure%20protection%20%28CIIP%29.