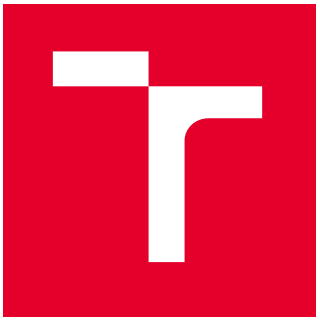


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

KYBERNETICKÁ BEZPEČNOST VE FINANČNÍ SPOLEČNOSTI PODLE SMĚRNICE DORA

CYBERSECURITY IN FINANCIAL INSTITUTIONS UNDER THE DORA DIRECTIVE

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — **Bc. Peter Cipka**

AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**

SUPERVISOR

BRNO 2025

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Peter Cipka**
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2024/25
Studijní program:	Informační management

Garant studijního programu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Kybernetická bezpečnost ve finanční společnosti podle směrnice DORA

Charakteristika problematiky úkolu:

Cíle práce
Teoretický úvod
Popis současného stavu
Návrh řešení
Ekonomické zhodnocení
Závěr

Cíle, kterých má být dosaženo:

Cílem práce je analyzovat implementaci kybernetických bezpečnostních rámců ve finančních společnostech v kontextu směrnice DORA, identifikovat klíčové rizika a navrhnout opatření na zvýšení odolnosti proti kybernetickým hrozbám.

Základní literární prameny:

DOUCEK Petr, Martin KONEČNÝ a Luděk NOVÁK, Řízení kybernetické bezpečnosti a bezpečnosti informací, Praha: Professional Publishing, 2020. ISBN 978-80-88260-39-4.

SEDLÁK Petr, Martin KONEČNÝ, Přeměna ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2023. ISBN 978-80-7623-110-8.

SEDLÁK Petr, Martin KONEČNÝ a kolektiv, Kybernetická (ne)bezpečnost. CERM, Akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

SEDLÁK Petr, Martin KONEČNÝ a kolektiv, Případové studie řízení kybernetické bezpečnosti. CERM, Akademické nakladatelství, 2024. ISBN 978-80-7623-126-9.

Pattison, A. (2022). DORA: A Guide to the EU Digital Operational Resilience Act. ISBN 978-1787784512.

European Commission (2022). Digital Operational Resilience Act (DORA): Regulatory Framework for Financial Services. Official Journal of the European Union.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2024/25

V Brně dne 9.2.2025

L. S.

doc. Ing. Miloš Koch, CSc. garant	prof. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Diplomová práca sa zaoberá analýzou a návrhom opatrení na zvýšenie kybernetickej bezpečnosti vo fin-techovej spoločnosti v kontexte požiadaviek Nariadenia DORA. Práca analyzuje špecifiká kybernetických hrozieb vo finančnom sektore, predstavuje legislatívny rámec DORA a zameriava sa na praktickú implementáciu jeho požiadaviek vo vybranej spoločnosti. V rámci analýzy súčasného stavu sú identifikované kľúčové nedostatky a potreba zásadných zmien v prístupe k riadeniu kybernetickej bezpečnosti. Na základe týchto zistení sú navrhnuté konkrétne procesy a opatrenia v podobe interných politík, dokumentov, stratégií a plánov. V závere je vykonané ekonomické zhodnotenie navrhnutých opatrení pomocou metodiky ROSI a Gordon-Loeb modelu, spolu s kvantifikáciou celkových nákladov na implementáciu DORA.

Kľúčové slová

nariadenie DORA, digitálna prevádzková odolnosť, riadenie rizík IKT, kybernetická bezpečnosť, finančné inštitúcie

Abstract

The thesis deals with the analysis and proposal of measures to increase cyber security in a fin-tech company in the context of the requirements of the DORA Regulation. The thesis analyses the specifics of cyber threats in the financial sector, presents the legislative framework of DORA and focuses on the practical implementation of its requirements in a selected company. The analysis of the current state of the art identifies key gaps and the need for fundamental changes in the approach to cybersecurity management. Based on these findings, specific processes and measures are proposed in the form of internal policies, documents, strategies and plans. Finally, an economic evaluation of the proposed measures is carried out using the ROSI methodology and the Gordon-Loeb model, along with a quantification of the total cost of DORA implementation.

Keywords

DORA regulation, digital operational resilience, ICT risk management, cybersecurity, financial institutions

Bibliografická citácia

CIPKA, Peter. Kybernetická bezpečnost ve finanční společnosti podle směrnice DORA. Online, diplomová práce. Petr SEDLÁK (vedoucí práce). Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2025. Dostupné z: https://www.vut.cz/studenti/zav-prace/detail/168676. [cit. 2025-05-13].

Čestné prehlásenie

Vyhlasujem, že predložená diplomová práca je pôvodná a vypracoval som ju samostatne. Vyhlasujem, že citácie použitých prameňov sú úplné a že som neporušil autorské práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 13. 5. 2025

Peter Cipka

autor

Poďakovanie

Ďakujem vedúcemu diplomovej práce, Ing. Petrovi Sedlákovi, za odborné vedenie, cenné rady a podporu. Vďaka patrí aj fintechovej inštitúcii za poskytnutie dôležitých informácií k praktickej časti práce. Rovnako ďakujem rodine a priateľom za neustálu podporu a motiváciu.

OBSAH

ÚVOD

Finančný sektor sa v súčasnosti nachádza v epicentre dynamickej digitálnej transformácie. Služby sa čoraz viac presúvajú do online prostredia, inovácie v podobe finančných technológií (FinTech) prinášajú revolučné zmeny a klienti očakávajú neustálu dostupnosť a bezpečnosť svojich prostriedkov a dát. Táto akcelerovaná digitalizácia však so sebou prináša aj eskalujúce kybernetické hrozby, ktoré sú sofistikovanejšie a cielenejšie než kedykoľvek predtým.

Navyše, dynamický vývoj technológií – vrátane umelej inteligencie a decentralizovaných finančných platforiem – prináša nielen nové príležitosti, ale aj špecifické riziká, na ktoré musia finančné inštitúcie reagovať proaktívne a systematicky. Finančné inštitúcie, ako správcovia citlivých údajov a kritickej infraštruktúry, sa tak stávajú primárnym terčom kybernetických útokov, ktorých následky môžu byť devastačné nielen pre samotné organizácie, ale aj pre stabilitu celého finančného systému.

Práve v tomto kontexte nadobúda mimoriadny význam európske nariadenie DORA (Digital Operational Resilience Act), ktoré predstavuje zásadný legislatívny rámec pre zabezpečenie digitálnej prevádzkovej odolnosti finančných subjektov. DORA reaguje na fragmentáciu predchádzajúcich regulačných prístupov a zavádza jednotné, komplexné požiadavky na riadenie IKT rizika, nahlasovanie incidentov, testovanie odolnosti a monitorovanie externých dodávateľov. Cieľom je nielen zvýšiť úroveň ochrany finančného sektora, ale aj zabezpečiť jeho schopnosť kontinuálne poskytovať služby aj v prípade závažných kybernetických incidentov.

Diplomová práca sa zameriava na analýzu a návrh opatrení na zvýšenie kybernetickej bezpečnosti vo vybranej fin-tech spoločnosti v kontexte požiadaviek nariadenia DORA. Práca reflektuje potrebu zásadnej zmeny v prístupe k riadeniu kybernetickej bezpečnosti, identifikuje kľúčové nedostatky v existujúcich procesoch a navrhuje konkrétne opatrenia, ktoré umožnia spoločnosti nielen splniť legislatívne požiadavky, ale aj zvýšiť svoju digitálnu odolnosť a konkurencieschopnosť. Prínosom je aj ekonomické zhodnotenie navrhovaných opatrení, ktoré umožňuje manažmentu kvalifikovane rozhodovať o investíciách do kybernetickej bezpečnosti.

Vzhľadom na rastúcu intenzitu a komplexnosť kybernetických hrozieb je systematické a strategické riadenie kybernetickej bezpečnosti v súlade s nariadením DORA nevyhnutnou podmienkou pre udržateľný rozvoj a stabilitu finančných inštitúcií v digitálnej ére. Táto práca preto ponúka nielen teoretický rámec, ale aj praktické odporúčania, ktoré môžu slúžiť ako inšpirácia pre ďalšie subjekty pôsobiace vo finančnom sektore.

Práca tak reflektuje potrebu systematického a premysleného prístupu k budovaniu robustného rámca kybernetickej bezpečnosti, ktorý je v dnešnom prepojenom digitálnom svete nevyhnutným predpokladom úspešného a bezpečného fungovania každej finančnej inštitúcie.

CIELE PRÁCE, METÓDY A POSTUPY SPRACOVANIA

Ciele práce

Hlavným cieľom diplomovej práce je analyzovať požiadavky Nariadenia DORA a na základe identifikovaných špecifík a nedostatkov v oblasti kybernetickej bezpečnosti vo vybranej FinTech spoločnosti, navrhnúť komplexný súbor konkrétnych opatrení.

Navrhovaný súbor opatrení bude klásť dôraz na praktickú realizovateľnosť a bude zahŕňať legislatívne a organizačné aspekty, ktoré sa premietnu do konkrétnych politík, dokumentov, stratégií a plánov. Ich primárnym účelom je posilniť digitálnu prevádzkovú odolnosť spoločnosti, zabezpečiť súlad s relevantnou legislatívou a vykonať ekonomické zhodnotenie navrhovaných riešení.

Metódy a postupy spracovania

Diplomová práca je koncipovaná ako komplexný výskumný a návrhový projekt, ktorý kombinuje teoretickú analýzu, empirickú diagnostiku a praktické prístupy v podobe návrhu praktických riešení, s cieľom analyzovať a posilniť kybernetickú bezpečnosť vo vybranej fintechovej spoločnosti a to v súlade s požiadavkami nariadenia DORA.

Práca je štruktúrovaná do štyroch hlavných častí: teoretické východiská, analýza súčasného stavu, návrh opatrení a ekonomické zhodnotenie. Tieto časti logicky nadväzujú a vytvárajú ucelený rámec pre splnenie stanovených cieľov. Na spracovanie jednotlivých častí boli použité viaceré vedecké a odborné metódy, ktoré sú podrobne opísané nižšie.

Teoretická časť práce je založená na systematickom prehľade odbornej literatúry, legislatívnych a regulačných dokumentov vrátane európskych nariadení, štandardov kybernetickej bezpečnosti a metóde desk research, využitej pri štúdii a analýze primárnych a sekundárnych informačných zdrojov. Využité boli metódy:

Analýza odbornej literatúry: Štúdium monografií, vedeckých článkov, zborníkov z konferencií a odborných štúdií zameraných na kybernetickú bezpečnosť a špecifiká finančného sektora.

Analýza legislatívnych dokumentov**:** Detailné štúdium Nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554 (Nariadenie DORA), súvisiacich delegovaných a vykonávacích aktov, ako aj relevantných národných právnych predpisov a medzinárodných štandardov (napr. normy ISO/IEC série 27000, odporúčania NIST).

Komparácia: Porovnávanie rôznych prístupov k riadeniu kybernetickej bezpečnosti a požiadaviek rôznych regulačných rámcov s cieľom zasadiť nariadenie DORA do širšieho kontextu.

Syntéza: Zhrnutie a integrácia poznatkov z rôznych zdrojov do uceleného teoretického rámca, ktorý slúži ako východisko pre analytickú a návrhovú časť práce.

Analytická časť využíva kvalitatívne metódy zberu dát, najmä analýzu interných dokumentov vybranej fin-tech spoločnosti. Táto časť práce sa zameriava na posúdenie súčasného stavu v konkrétnej FinTech spoločnosti a identifikáciu rozdielov voči požiadavkám nariadenia DORA. Použité boli nasledujúce metódy:

Analýza interných dokumentov spoločnosti: Skúmanie existujúcich interných politík, smerníc, procesnej dokumentácie a technologickej infraštruktúry.

Riadené rozhovory alebo konzultácie: Získavanie doplňujúcich informácií a expertných názorov od relevantných zamestnancov alebo manažmentu spoločnosti.

GAP analýza (Analýza rozdielov): Porovnanie súčasného stavu implementovaných bezpečnostných opatrení a procesov v spoločnosti s požiadavkami Nariadenia DORA.

Návrhová časť je zameraná na tvorbu konkrétnych opatrení a odporúčaní na základe zistení z analytickej a teoretickej časti. Návrh zahŕňa organizačné, technické a procesné opatrenia, ktoré sú prispôsobené špecifikám analyzovanej spoločnosti a legislatívnym požiadavkám. Metodický postup zahŕňa:

Syntézu analytických zistení: Využitie identifikovaných nedostatkov ako podkladu pre návrh konkrétnych riešení.

Návrh politík, stratégií, plánov a dokumentov: Formulácia návrhov konkrétnych interných predpisov a dokumentácie (napr. stratégia digitálnej operačnej odolnosti, rámec riadenia rizík IKT, plán kontinuity činností) v súlade s požiadavkami DORA a špecifikami spoločnosti.

Aplikácia osvedčených postupov a štandardov: Využitie poznatkov z medzinárodných štandardov (napr. ISO/IEC 27000) a best practices pri tvorbe navrhovaných opatrení.

Ekonomické zhodnotenie navrhovaných opatrení je realizované pomocou kvantitatívnych metód, vrátane výpočtu návratnosti investícií do kybernetickej bezpečnosti (ROSI), Gordon-Loeb modelu a kvantifikácii nákladov. Tento prístup umožňuje manažmentu objektívne posúdiť efektívnosť a finančnú opodstatnenosť implementácie navrhovaných riešení.

Táto metodologická kombinácia umožňuje systematické a prakticky orientované spracovanie témy, ktoré je zároveň podložené aktuálnymi odbornými poznatkami a legislatívnymi požiadavkami v oblasti kybernetickej bezpečnosti finančného sektora.

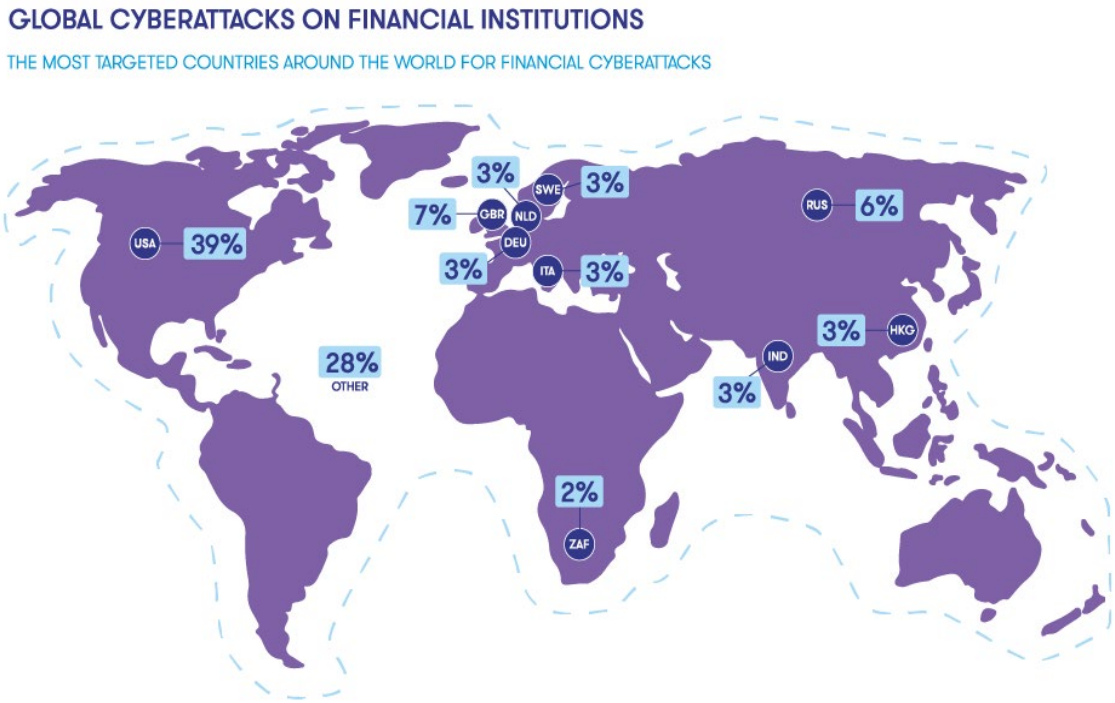
1 TEORETICKÉ VÝCHODISKÁ

1.1 Kontext a význam kybernetickej bezpečnosti v prostredí finančných inštitúcií

1.1.1 Význam kybernetickej bezpečnosti pre finančné inštitúcie

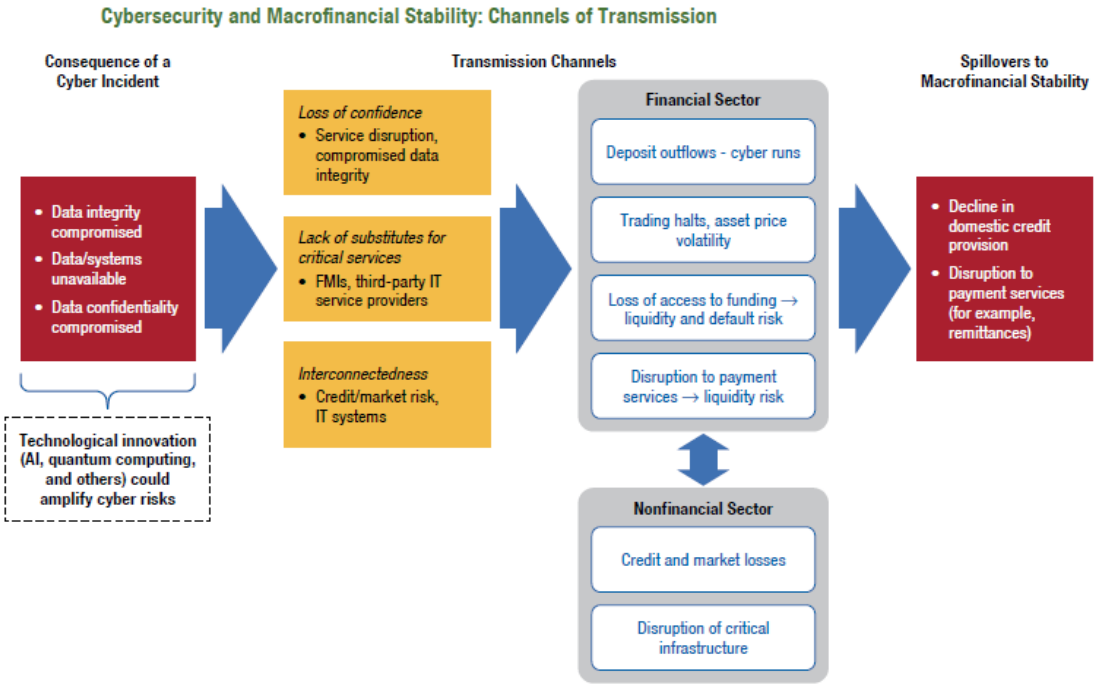
V súčasnom digitálnom svete predstavuje kybernetická bezpečnosť **kritickú prioritu pre finančné inštitúcie** a ich efektívne fungovanie. Vzhľadom na pokračujúcu digitalizáciu a automatizáciu finančných služieb, zameranú na efektívnejšie riadenie a pohodlie používateľov, sa zabezpečenie kybernetickej bezpečnosti stáva čoraz naliehavejšou výzvou. (1) (2)

Finančný sektor je totiž jedným z **najviac ohrozených odvetví** v dôsledku kybernetických útokov a bezpečnostných hrozieb. Táto zraniteľnosť vyplýva z rozsiahlych objemov finančných aktív, rozsiahlych databáz osobných údajov klientov a značnej závislosti od informačných technológií. (1) (2)



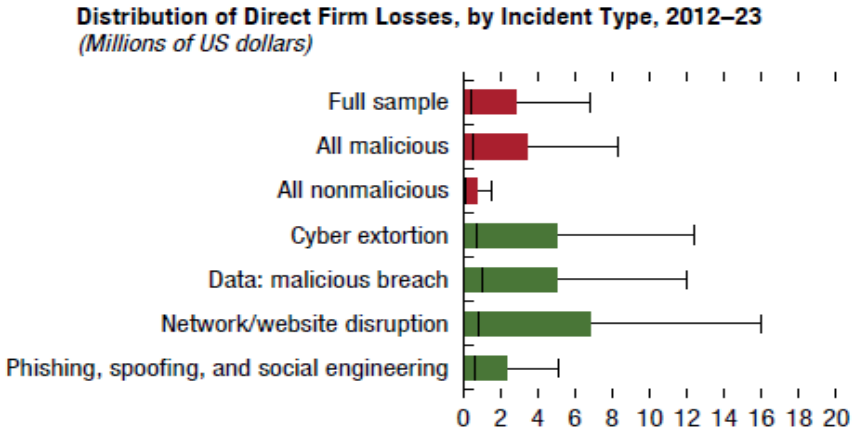
Obrázok č.1: Kybernetické útoky na finančné inštitúcie (Zdroj: swivelsecure.com/solutions/banking-finance/infographic-the-emerging-cybersecurity-threats-you-should-know/)

Kybernetická bezpečnosť sa tak stáva nielen otázkou technologickou, ale predovšetkým **záležitosťou obchodnou a rizikovou**. Dôsledky jej zlyhania môžu byť rozsiahle, od neschopnosti vykonávať základné prevádzkové procesy, cez stratu duševného vlastníctva, až po potenciálne významné poškodenie reputácie. (3)



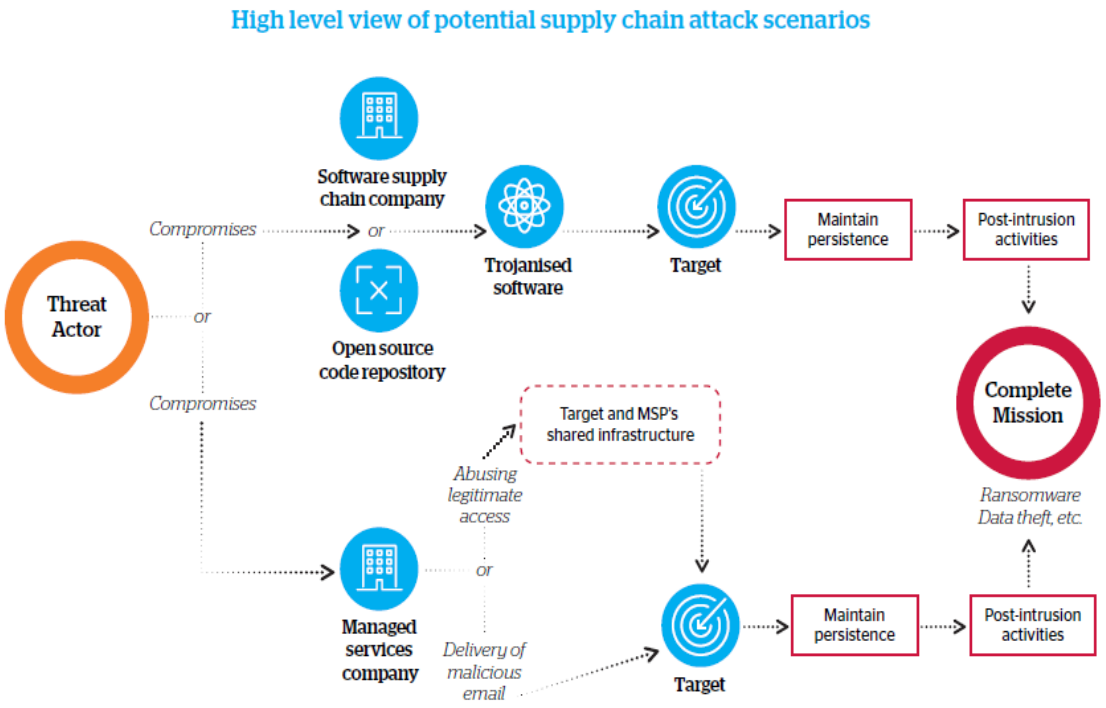
Obrázok č. 2 Kanály prenosu kybernetických incidentov (Zdroj: č. 7)

Je dôležité zdôrazniť, že **priame finančné straty** spôsobené kybernetickými útokmi predstavujú len časť celkových nákladov. Viac ako **90 % celkových nákladov** tvoria nepriame faktory, ako sú náklady na obnovu prevádzky, riešenie právnych sporov, ale najmä **reputačné škody.** (4)



Obrázok č. 3 Distribúcia priamych finančných strát podľa typu incidentu (Zdroj: č. 7)

Vzhľadom na vysokú mieru prepojenosti v rámci finančného sektora je riadenie rizík tretích strán rovnako dôležité. Mnohé finančné inštitúcie outsourcujú kritické bankové funkcie, pričom ich úroveň kybernetického rizika značne závisí od procesov a kontrol zavedených u ich dodávateľov. (5)

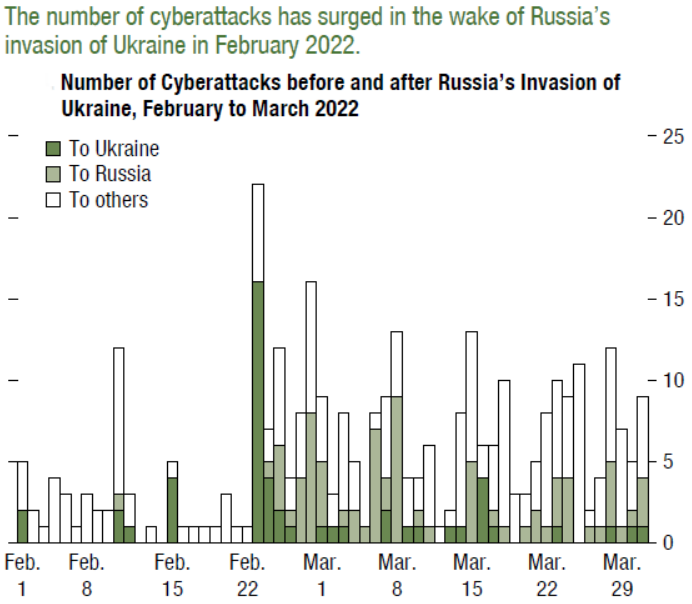


Obrázok č. 4 Scenár útoku cez dodávateľský reťazec (Zdroj: qbe.com/media/qbe/shared/files/cyber-intelligence-threat-whitepaper.pdf)

Rozvoj umelej inteligencie (AI) prináša nové možnosti, ale aj špecifické kybernetické riziká, na ktoré sa finančné inštitúcie musia pripraviť. Hoci AI môže posilniť kybernetickú bezpečnosť, zároveň môže byť cieľom útokov alebo môže byť zneužitá na vykonávanie sofistikovanejších podvodov. (6)

V kontexte rastúcich digitálnych hrozieb je pre finančné inštitúcie nevyhnutné **proaktívne budovať a neustále zlepšovať systémy kybernetickej bezpečnosti**. Tento prístup by mal zahŕňať vytvorenie silnej **kultúry kybernetickej bezpečnosti** v rámci celej organizácie, implementáciu **najnovších technológií** v oblasti kybernetickej bezpečnosti, zavedenie systému **nepretržitého monitorovania** a identifikácie hrozieb, ako aj detailné **plánovanie obnovy dát** po prípadných útokoch. (1) (2)

Skúsenosti z krajín zasiahnutých konfliktmi, ako je Ukrajina, poukazujú na kľúčovú úlohu strategických opatrení v oblasti kybernetickej bezpečnosti, vrátane geografickej diverzifikácie dátových centier a záložných systémov. (1) (2)



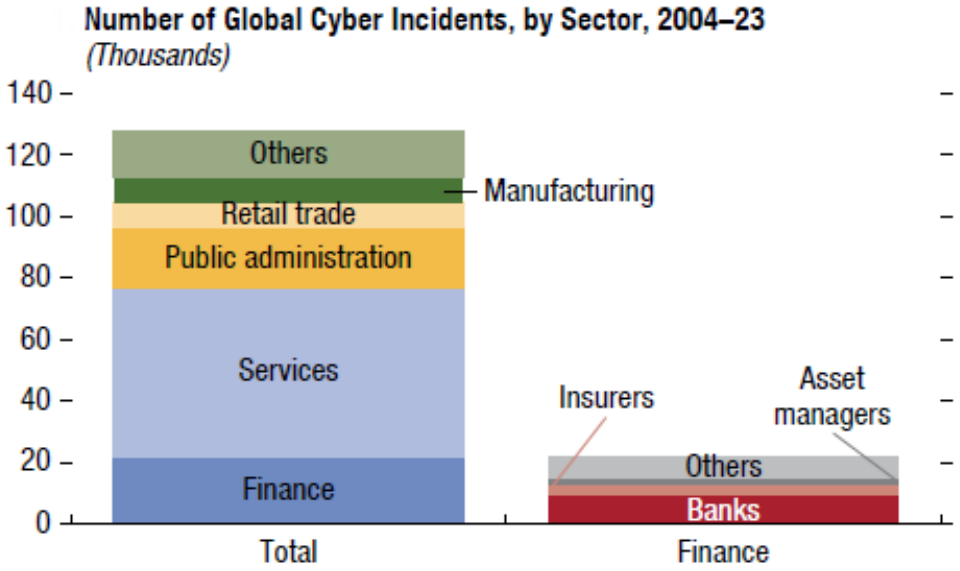
Obrázok č. 5 Kybernetické útoky po invázii na Ukrajinu (Zdroj: č.7)

Na záver, **kybernetická bezpečnosť nie je len technickou záležitosťou, ale strategickou prioritou pre finančné inštitúcie**. Jej efektívne riadenie je nevyhnutné pre udržanie dôvery klientov, zabezpečenie finančnej stability a dodržiavanie regulačných požiadaviek. Investície do kybernetickej bezpečnosti a neustále zlepšovanie bezpečnostných opatrení sú kľúčové pre odolnosť finančného sektora voči narastajúcim kybernetickým hrozbám. (7)

1.1.2 Špecifiká kybernetických hrozieb vo finančnom prostredí

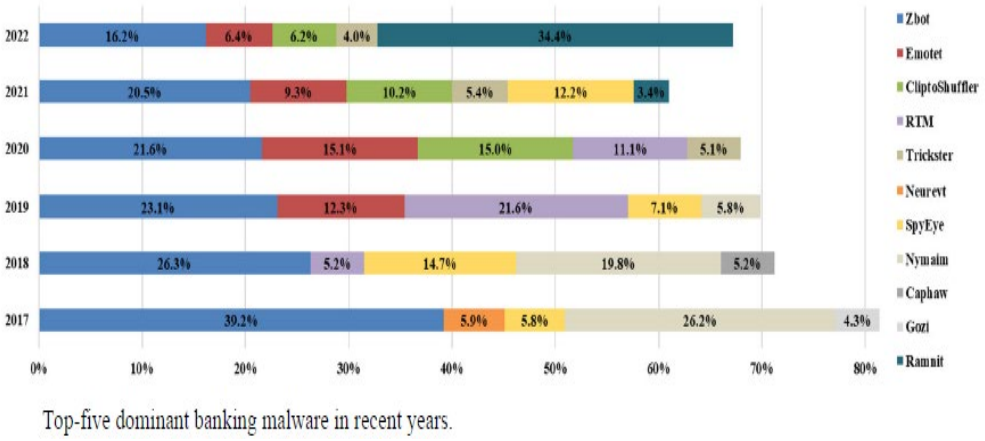
Špecifiká kybernetických hrozieb vo finančnom prostredí vyplývajú z jedinečnej povahy tohto sektora, ktorý sa pre kybernetických útočníkov javí ako mimoriadne atraktívny cieľ. Finančné inštitúcie sú zamerané na dáta a očakáva sa od nich poskytovanie služieb 24 hodín denne, 7 dní v týždni, čo ich robí obzvlášť zraniteľnými voči narušeniu. (8) (9)

Výskum ukazuje, že **finančný sektor je jedným z najviac postihnutých odvetví z pohľadu nákladov na kyberkriminalitu**. Primárnym motívom útočníkov je dosiahnutie finančného zisku, pričom banky patria medzi najčastejšie ciele, najmä ich segmenty retailového bankovníctva a služieb kreditných kariet. (8) (9)



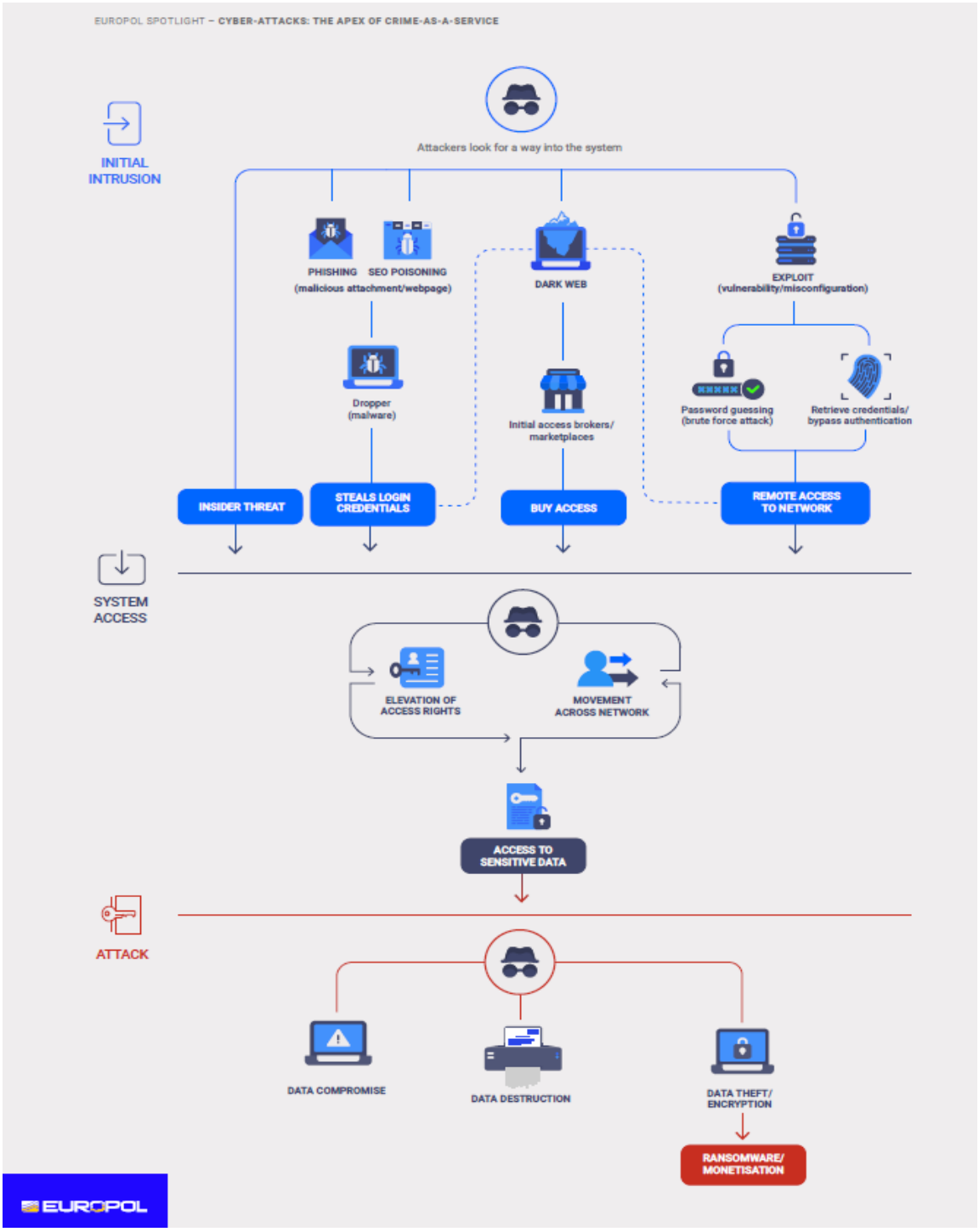
Obrázok č. 6 Počet kybernetických incidentov podľa sektorov (Zdroj: č.7)

Medzi najvýznamnejšie špecifiká kybernetických hrozieb vo finančnom prostredí patrí **prevažujúce využitie malvéru** ako hlavného vektora útoku. Malvér sa používa na infiltráciu systémov s cieľom krádeže údajov, narušenia prevádzky alebo získania neoprávneného prístupu. (9) (10) (11)



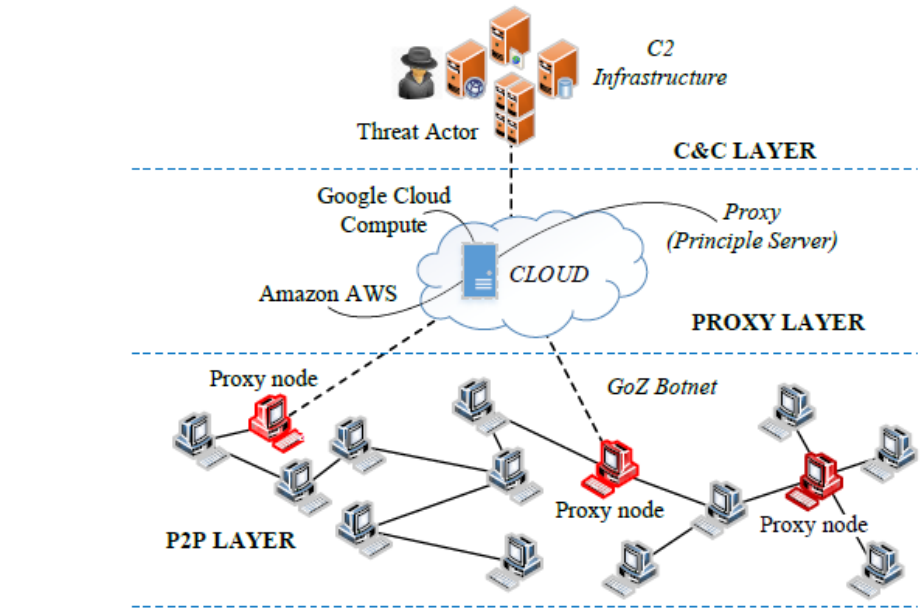
Obrázok č. 7 Najčastejšie bankové malvéry (Zdroj: č.7)

Okrem tradičných foriem malvéru sa objavuje aj *"Crimeware-as-a-service"* **(CaaS)**, čo predstavuje novú komoditu založenú na **cloud computingu**, ktorá uľahčuje šírenie a vykonávanie kybernetických útokov (10)



Obrázok č. 8 Postupnosť kybernetického útoku od prieniku po zneužitie dát v rámci modelu Crime-as-a-Service (Zdroj: europol.europa.eu/cms/sites/default/files/documents/Spotlight%20Report%20-%20Cyber-attacks%20the%20apex%20of%20crime-as-a-service.pdf)

Špecifickým príkladom závažného malvéru je **GameOver Zeus (GoZ)**, ktorý je široko rozšíreným finančným malvérom, schopným zneužiť cloudové prostredia a cieli na používateľov finančných služieb prostredníctvom rôznych zariadení. Typické správanie GoZ útokov zahŕňa snahu o zachytenie a exfiltráciu bankových prihlasovacích údajov a iných informácií v čo najkratšom čase. (9) (10)



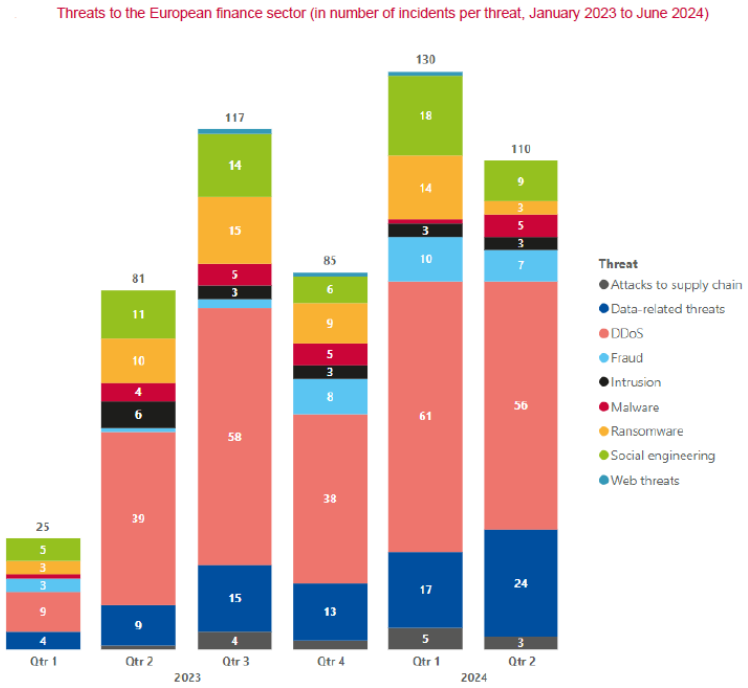
The infrastructure of GameOver Zeus botnet.

Obrázok č. 9 Architektúra botnetu GameOver Zeus (Zdroj:č.10)

Ransomvér (vydieračský softvér): Zameraný na zablokovanie prístupu k systémom alebo údajom a následné požadovanie výkupného za ich obnovenie. (12)

Phishing (podvodné e-maily a správy): Predstavuje sociálne inžinierstvo zamerané na získanie prihlasovacích údajov, bankových informácií alebo iných citlivých dát prostredníctvom falošných správ, ktoré sa tvária ako dôveryhodné zdroje. Vo finančnom sektore je obzvlášť významný **CEO fraud (podvodné e-maily od vrcholového manažmentu)** a **Business email compromise (kompromitácia firemných e-mailov)**. (11) (13)

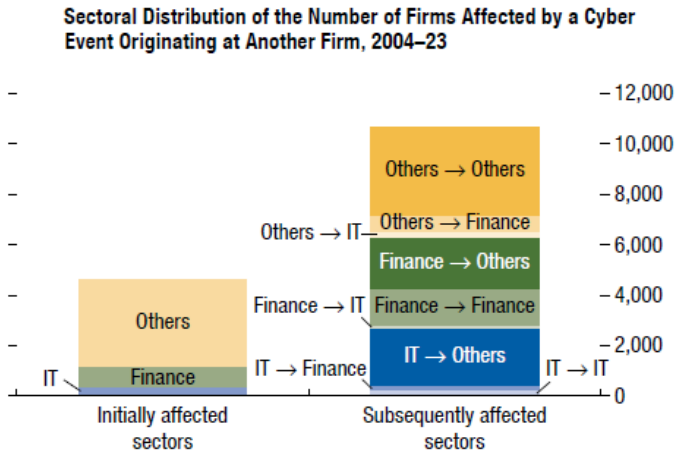
Distribuované útoky odmietnutia služby (DDoS) predstavujú ďalšiu kritickú hrozbu, schopnú narušiť kontinuitu poskytovaných finančných služieb. Závažnou podkategóriou sú **nízkofrekvenčné DDoS útoky (LR-DDoS)**, ktoré sú pre tradičné systémy detekcie a firewallové riešenia ťažko odhaliteľné a neutralizovateľné. (9) (10)



Obrázok č. 10 Kybernetické hrozby vo finančnom sektore EÚ (január 2023 – jún 2024) (Zdroj: enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf)

Finančné inštitúcie sú taktiež vystavené rizikám **priemyselnej špionáže**, pričom malé a stredné podniky (SMEs) s obmedzenými zdrojmi sú obzvlášť zraniteľné voči úniku citlivých informácií. (9)

Špecifiká finančného sektora spočívajú v jeho **vysokej prepojenosti**, kde úspešný kybernetický útok na jednu inštitúciu môže mať domino efekt a ohroziť stabilitu celého systému, pričom reputačné škody a narušenie dôvery klientov predstavujú ďalšie významné riziká. (14)



Obrázok č. 11 Dopady kybernetických útokov medzi sektormi (Zdroj:č.7)

1.1.3 Prehľad vybraných kybernetických incidentov vo finančnom sektore

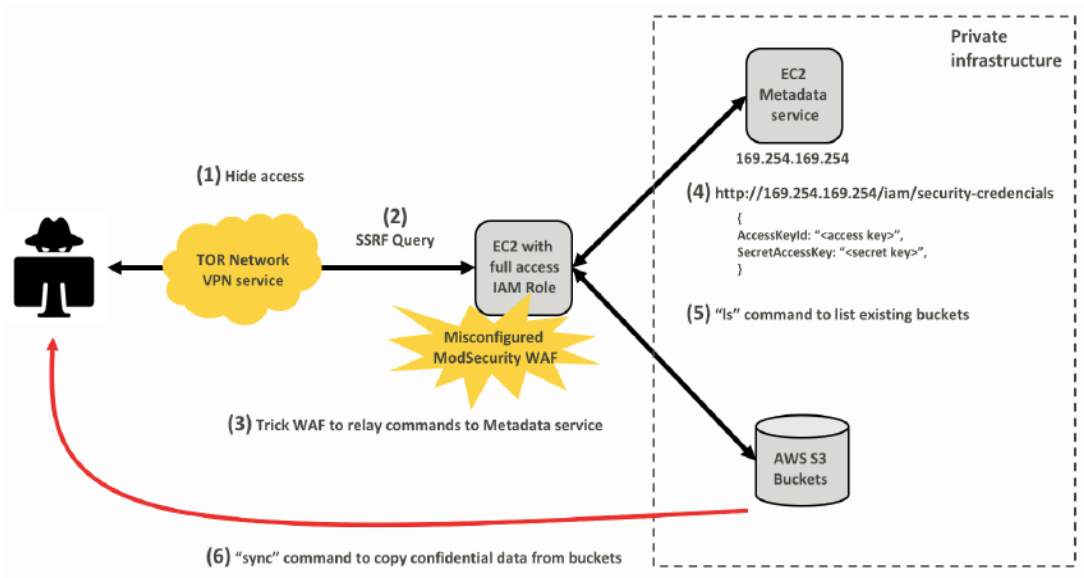
Narastajúca digitalizácia finančného sektora prináša so sebou zvýšenú expozíciu voči kybernetickým hrozbám. Nasledujúce vybrané incidenty ilustrujú rôznorodosť, závažnosť a dopady týchto hrozieb na finančné inštitúcie a ich klientov.

Hacknutie účtu americkej Komisie pre cenné papiere a burzy (SEC) na sociálnej sieti (január 2024).

- **Príčina a priebeh:** Neoprávnený prístup k účtu SEC na sociálnej sieti viedol k zverejneniu podvodného oznámenia týkajúceho sa schválenia bitcoinového fondu obchodovaného na burze (ETF).
- **Rozsah a dôsledky:** Incident mal okamžitý vplyv na **volatilitu trhu**, keďže cena bitcoinu najprv prudko vzrástla a následne klesla. Hoci počet incidentov na podobných inštitúciách bol relatívne stabilný (10 až 20 ročne), tento konkrétny prípad ukázal, ako **ľahko môže byť narušená dôvera a stabilita trhov prostredníctvom dezinformácií šírených cez digitálne platformy**. (7)

Data breach spoločnosti Capital One (júl 2019).

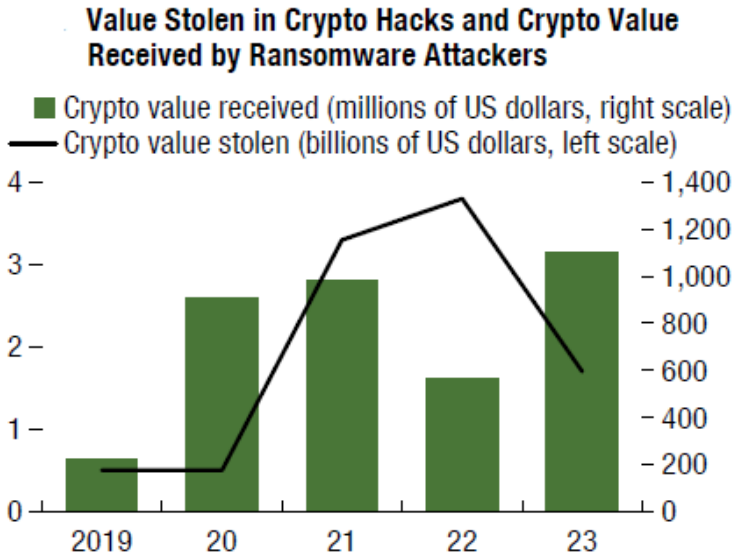
- **Príčina a priebeh:** Kybernetický útok na americkú banku Capital One viedol k **úniku dát približne 106 miliónov zákazníkov**. Analýza incidentu ukázala na zneužitie zraniteľností a **nedostatočné implementovanie bezpečnostných kontrol**.
- **Rozsah a dôsledk**y: Únik dát mal **rozsiahly dopad na súkromie zákazníkov** a **viedol k finančným stratám** pre spoločnosť v podobe pokút a nákladov na nápravu. Incident spochybnil účinnosť **existujúcich noriem a politík kybernetickej bezpečnosti** pri prevencii rozsiahlych únikov dát a vyvolal otázky o účinnosti implementovaných opatrení. (15)



Obrázok č. 12 Priebeh útoku na Capital One (Zdroj:15)

Hack platformy Poly Network (2021).

- **Príčina a priebeh:** Útok na platformu decentralizovaného financovania (DeFi) Poly Network viedol k **odcudzeniu kryptomien v hodnote viac ako 600 miliónov dolárov**. Incident demonštroval **rastúce zameranie kybernetických útokov na sektor kryptoaktív**, ktorý sa stáva čoraz významnejšou súčasťou finančného systému. Útoky často cielia na kryptoburzy, platformy a tzv. horúce peňaženky.
- **Rozsah a dôsledky:** Tento rozsiahly kybernetický zločin podčiarkol **vysokú mieru rizika spojenú s decentralizovanými finančnými službami** a potrebu **zlepšenia bezpečnostných opatrení** v tomto dynamicky sa rozvíjajúcom odvetví. Hoci sa časť odcudzených prostriedkov neskôr vrátila, incident vážne narušil **dôveru v bezpečnosť DeFi platforiem**. (7)



Obrázok č. 13 Ukradnutá a prijatá hodnota v kryptomenách (Zdroj: č. 7)

1.2 Regulácia kybernetickej bezpečnosti podľa nariadenia DORA

1.2.1 Legislatívne východiská a implementačný rámec DORA

1.2.1.1 Princípy a legislatívne základy DORA

Nariadenie o digitálnej prevádzkovej odolnosti finančného sektora (Digital Operational Resilience Act – DORA) predstavuje významný krok v regulácii kybernetickej bezpečnosti a prevádzkovej odolnosti v rámci finančného systému Európskej únie. (16)

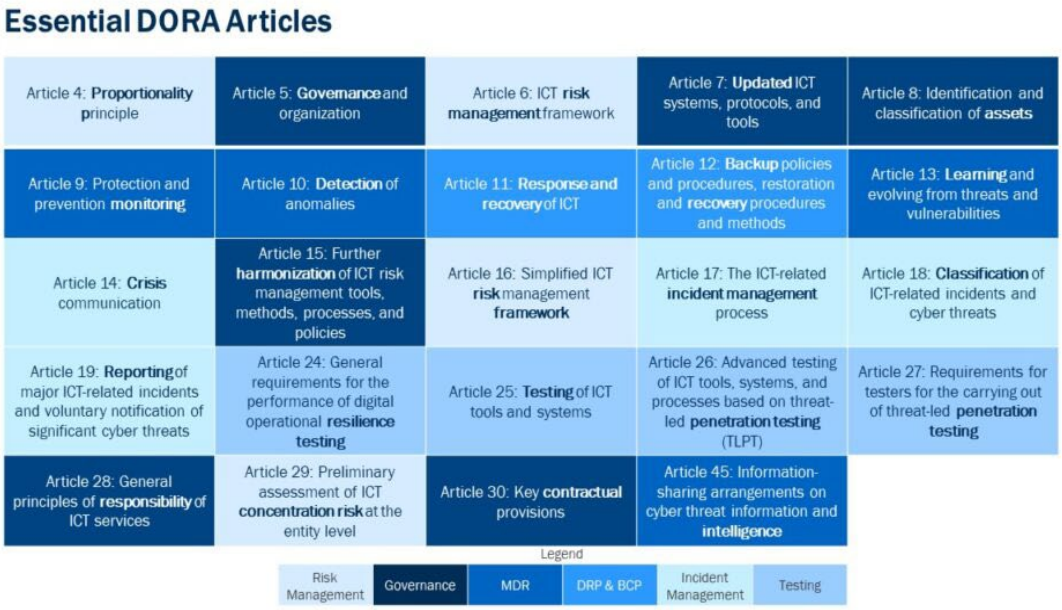
Nariadenie DORA vzniklo ako reakcia na rastúcu úlohu informačných a komunikačných technológií (IKT) v poskytovaní finančných služieb a na významné ekonomické a systémové riziká spojené s potenciálnym narušením kritických IKT systémov. (17)

Jeho **pôvod** pramení z identifikovaných legislatívnych rozdielov a nerovnakých vnútroštátnych regulačných prístupov v oblasti dohľadu nad prevádzkovými aspektmi informačných a komunikačných technológií v rámci finančného sektora. (16)

Pred prijatím nariadenia DORA bola oblasť kybernetickej bezpečnosti a prevádzkovej odolnosti vo finančnom sektore **regulovaná fragmentovane**, jednotlivé členské štáty uplatňovali odlišné prístupy, pričom chýbal jednotný rámec, čo viedlo k rozdielnej úrovni ochrany a regulačnej náročnosti v rámci EÚ . (18)

Skutočnosť, že ustanovenia týkajúce sa IKT rizika boli na úrovni Únie riešené len čiastočne, viedla k **nedostatkom a prekrývaniu sa existujúcich pravidiel** v kľúčových oblastiach, ako je nahlasovanie incidentov súvisiacich s IKT a testovanie digitálnej prevádzkovej odolnosti, ako aj k nezrovnalostiam vyplývajúcim z odlišných vnútroštátnych predpisov. (16)

Hlavným **účelom** nariadenia DORA je **konsolidovať a vylepšiť rôzne existujúce pravidlá týkajúce sa IKT rizika** a po prvýkrát **spojiť všetky ustanovenia týkajúce sa digitálneho rizika vo finančnom sektore do jedného legislatívneho aktu.** (16)



Obrázok č. 14 Prehľad hlavných článkov nariadenia DORA (Zdroj: datos-insights.com/blog/ready-for-dora-compliance/)

Zároveň má zabezpečiť, aby finančné inštitúcie v EÚ boli schopné udržať **nepretržité poskytovanie služieb** a ich kvalitu, a tým zachovať **stabilitu finančného systému EÚ** v prípade akéhokoľvek potenciálneho narušenia alebo hrozby pre prevádzkovú odolnosť v súvislosti s ich využívaním IKT. (19)

Týmto spôsobom DORA **vypĺňa medzery a odstraňuje nezrovnalosti** v predchádzajúcich právnych aktoch, a to aj v súvislosti s používanou terminológiou. Nariadenie výslovne upravuje spôsobilosti v oblasti riadenia IKT rizika, nahlasovania incidentov, testovania prevádzkovej odolnosti a monitorovania externého IKT rizika. (16)

Medzi **hlavné princípy** nariadenia DORA patrí **zavedenie spoľahlivého, komplexného a dobre zdokumentovaného rámca riadenia IKT rizika** pre všetky finančné subjekty. Tento rámec má umožniť finančným subjektom rýchlo, efektívne a komplexne riešiť IKT riziko a zabezpečiť vysokú úroveň digitálnej prevádzkovej odolnosti. Rámec zahŕňa stratégie, politiky, postupy, IKT protokoly a nástroje potrebné na riadnu ochranu všetkých informačných aktív a IKT aktív. (16)

Dôležitým princípom je aj **zodpovednosť riadiaceho orgánu** finančného subjektu, ktorý nesie konečnú zodpovednosť za riadenie IKT rizika a za zavedenie politík zameraných na zabezpečenie vysokých štandardov dostupnosti, pravosti, integrity a dôvernosti údajov. (16)

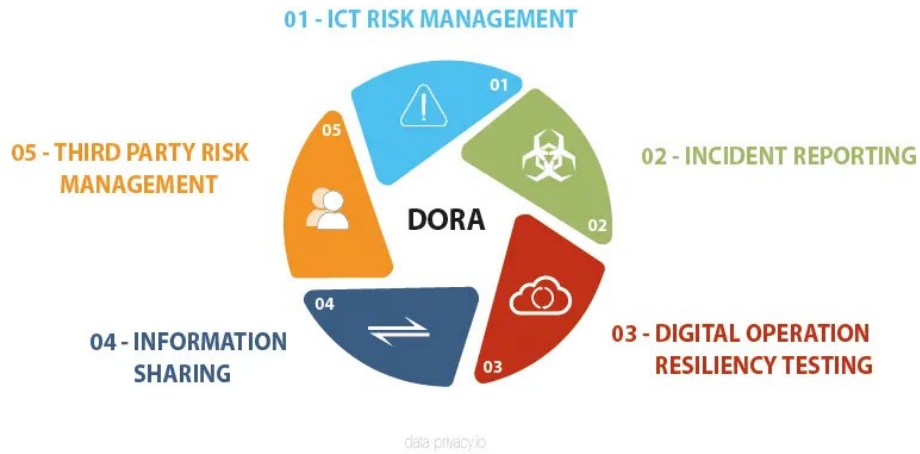
Nariadenie zároveň rešpektuje **zásadu proporcionality**, umožňujúc uplatňovanie zjednodušeného rámca riadenia IKT rizika pre určité finančné subjekty, najmä mikropodniky a subjekty podliehajúce zjednodušenému režimu. (16)

DORA predstavuje vo vzťahu k smernici (EÚ) 2022/2555 **lex specialis**, čím zvyšuje úroveň harmonizácie v oblasti digitálnej odolnosti, zároveň však zachováva silný vzťah s horizontálnym rámcom Únie v oblasti kybernetickej bezpečnosti. (16)

DORA je súčasťou **Balíka pre digitálne financie**, ktorý okrem iného zahŕňa Stratégiu pre digitálne financie (DFS), nariadenie MiCA (o trhoch s kryptoaktívami) a pilotný režim pre infraštruktúry trhu založené na DLT. (19)

1.2.1.2 Analýza požiadaviek nariadenia DORA

Nariadenie o digitálnej prevádzkovej odolnosti vo finančnom sektore (DORA) **ukladá finančným inštitúciám záväzné požiadavky** v oblasti riadenia rizík informačných a komunikačných technológií (IKT), nahlasovania incidentov, testovania odolnosti a riadenia rizík tretích strán. Cieľom je posilniť digitálnu prevádzkovú odolnosť finančných subjektov. (16) (20)



Obrázok č. 15 Kľúčové oblasti nariadenia DORA (Zdroj: data-privacy.io/dora-regulation-primer/)

Medzi **kľúčové požiadavky nariadenia DORA**, ktoré musia finančné inštitúcie implementovať, patria nasledovné oblasti.

1.2.1.2.1 Zavedenie rámca riadenia a kontroly

- Finančné subjekty musia vytvoriť **interný rámec riadenia a kontroly** na dohľad nad činnosťami riadenia rizík organizácie. Hoci samotné nariadenie stanovuje pomerne stručné požiadavky v tejto oblasti, ide o potenciálne jednu z najdôležitejších častí súladu s DORA. Zriadený riadiaci orgán bude nevyhnutný na zabezpečenie dodržiavania nariadenia. (21)

1.2.1.2.2 Rámec riadenia IKT rizika

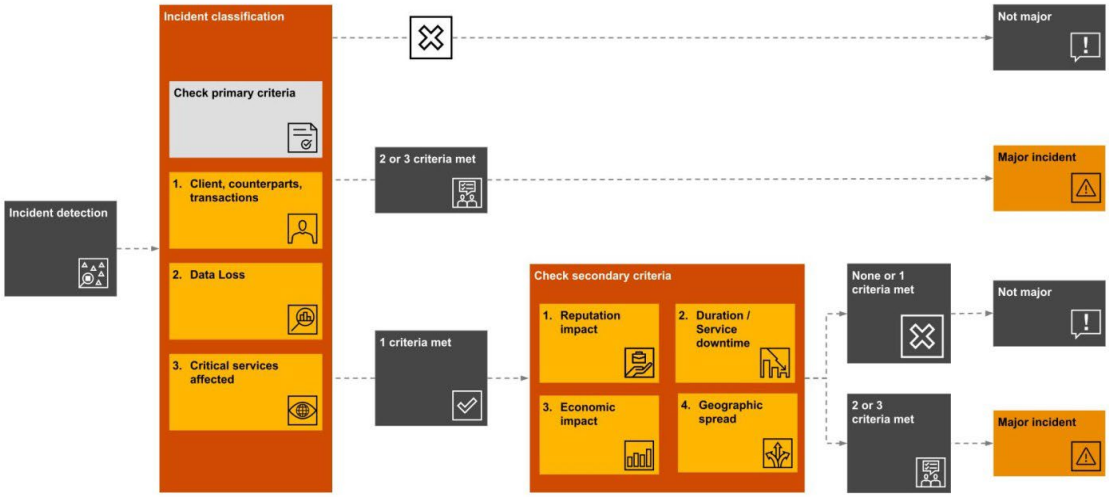
- Finančné subjekty musia zaviesť **spoľahlivý, komplexný a dobre zdokumentovaný rámec riadenia IKT rizika** ako súčasť ich celkového systému riadenia rizika. Tento rámec má umožniť **rýchle, efektívne a komplexné riadenie IKT rizika** a zabezpečiť vysokú úroveň digitálnej prevádzkovej odolnosti. (16)
- Rámec zahŕňa **stratégie, politiky, postupy, IKT protokoly a nástroje** potrebné na riadnu ochranu všetkých informačných aktív a IKT aktív. (16)
- **Riadiaci orgán** finančného subjektu **nesie konečnú zodpovednosť za riadenie IKT rizika**. Je povinný zavádzať politiky na zabezpečenie **vysokých noriem dostupnosti, pravosti, integrity a dôvernosti údajov**. (16)

- Riadiaci orgán **schvaľuje a pravidelne preskúmava stratégiu digitálnej prevádzkovej odolnosti** vrátane **tolerancie IKT rizika** a politiky týkajúce sa využívania externých poskytovateľov IKT služieb. (16)
- Finančné subjekty iné než mikropodniky musia **zriadiť funkciu na monitorovanie dojednaní s externými poskytovateľmi IKT služieb** alebo určiť člena vrcholového manažmentu zodpovedného za dohľad nad príslušnými rizikovými expozíciami. (16)
- Členovia riadiaceho orgánu si musia **aktívne udržiavať dostatočné znalosti a zručnosti** potrebné na pochopenie a posúdenie IKT rizika. (16)
- Súčasťou rámca je aj **politika kontinuity činností v oblasti IKT** a vykonávanie **analýzy vplyvu na činnosti (BIA)**. (16)
- Pre špecifickú podmnožinu finančných subjektov sa môže zaviesť **zjednodušený rámec riadenia rizika IKT**. (18)
- Súvisiaca vypracovaná dokumentácia k identifikovaným IKT funkciám a aktívam sa musí pravidelne, minimálne raz ročne, **prehodnocovať**. (21)

1.2.1.2.3 Nahlasovanie incidentov súvisiacich s IKT

- Finančné subjekty musia zaviesť **mechanizmy na rýchle odhaľovanie anomálnych činností** a incidentov súvisiacich s IKT. Tieto mechanizmy často využívajú **systémy monitorovania sietí a informačných systémov**, **nástroje na analýzu logov** a systémy detekcie narušení. (16)
- Po odhalení incidentu nasledujú **jasne definované procesy riadenia incidentov**, ktoré zahŕňajú **identifikáciu, sledovanie, zaznamenávanie a kategorizáciu incidentov**. **Automatické mechanizmy varovania** informujú príslušných zamestnancov zodpovedných za reakciu. (16)
- Na účely nahlasovania sa vyžaduje **jednotný zjednodušený rámec**. Hoci nariadenie priamo nešpecifikuje technológie pre nahlasovanie, predpokladá sa využitie **zabezpečených komunikačných kanálov** na odosielanie informácií príslušným orgánom. (16)
- Incidenty súvisiace s IKT sa **klasifikujú podľa ich priority a závažnosti** na základe **kritérií** ako počet dotknutých klientov, trvanie incidentu, geografický rozsah, strata údajov, kritickosť zasiahnutých služieb a hospodársky vplyv. (16)

- **Závažný incident súvisiaci s IKT** má veľký nepriaznivý vplyv na siete a informačné systémy podporujúce kritické alebo dôležité funkcie finančného subjektu. (16)
- Finančné subjekty **klasifikujú kybernetické hrozby ako významné** na základe kritickosti ohrozených služieb, počtu potenciálne dotknutých klientov a geografického rozloženia rizík. (16)



Obrázok č. 16 Klasifikácia závažnosti kybernetického incidentu podľa kritérií DORA (Zdroj: linkedin.com/pulse/dora-update-how-do-you-report-major-ict-related-incidents-schulz/)

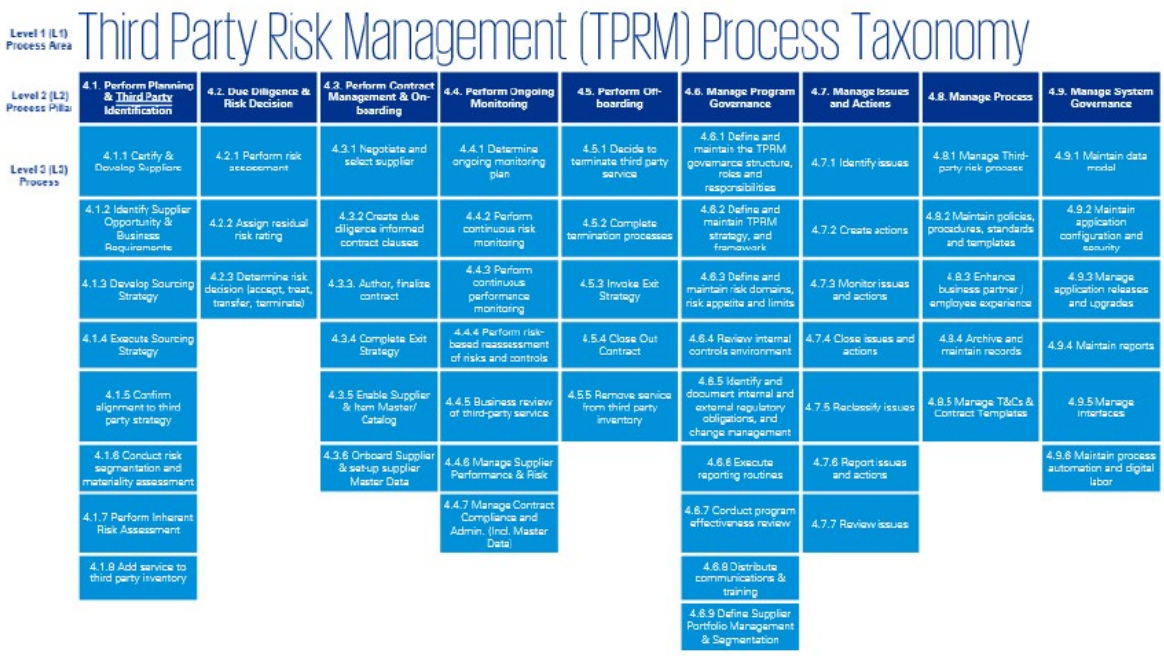
1.2.1.2.4 Testovanie digitálnej prevádzkovej odolnosti

- Finančné subjekty musia **pravidelne testovať svoje IKT systémy** a personál s cieľom posúdiť účinnosť ich spôsobilostí v oblasti prevencie, odhaľovania, reakcie a obnovy. (16)
- Testovanie zahŕňa **širokú škálu nástrojov a opatrení**, od posúdenia zraniteľností po pokročilé testovanie prostredníctvom **penetračného testovania na základe konkrétnej hrozby (TLPT)**. (16)
- **TLPT je vyžadované len od finančných subjektov, ktoré spĺňajú určité kritériá**, napríklad veľké systémové úverové inštitúcie. (16)

- Finančné subjekty posúdia, na ktoré **kritické alebo dôležité funkcie** sa má TLPT vzťahovať, a rozsah testovania validujú príslušné orgány. (16)
- Ak sú do rozsahu TLPT zahrnutí **externí poskytovatelia IKT služieb**, finančný subjekt prijme opatrenia na zabezpečenie ich účasti. (16)
- Požiadavky na TLPT sú špecifikované prostredníctvom **RTS**, ktoré sú v súlade s rámcom **TIBER-EU** (Purple – Teaming, Control Team). (22)
- Mikropodniky vykonávajú testy **kombináciou prístupu založeného na riziku** so **strategickým plánovaním testovania IKT**, zohľadňujúc rozsah zdrojov a naliehavosť rizík. (16)

1.2.1.2.5 Riadenie rizika IKT tretích strán

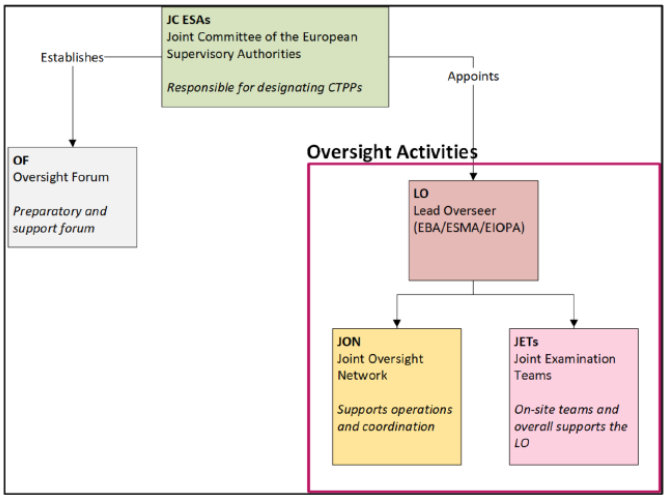
- Finančné subjekty musia **monitorovať riziká** vyplývajúce z ich závislostí na **externých poskytovateľoch IKT služieb**. (16)
- Pri riadení rizík tretích strán v oblasti IKT je potrebné **zohľadniť povahu, rozsah, zložitosť a význam závislostí na IKT**. (23)
- Pred uzavretím zmluvného dojednania musia subjekty vykonať **dôkladnú analýzu,** pri výbere a posudzovaní externých poskytovateľov IKT služieb. (16)
- Finančné subjekty sú povinné **viesť a aktualizovať register informácií** o všetkých zmluvných dojednaniach o využívaní IKT služieb. Tento register má slúžiť na **vyhodnotenie kritickosti IKT tretích strán**. (16) (24)
- Finančné subjekty **aspoň raz ročne nahlasujú** príslušným orgánom informácie o nových, plánovaných a ukončených dojednaniach o využívaní IKT služieb. (24)
- Pre IKT služby podporujúce **kritické alebo dôležité funkcie** musia finančné subjekty zaviesť stratégie ukončenia angažovanosti. (16)
- Zmluvné dojednania musia obsahovať **kľúčové ustanovenia** týkajúce sa napríklad opisov služieb, úrovní služieb, prístupu k údajom a povinností spolupráce. (16)
- Nariadenie zavádza **rámec dozoru na úrovni EÚ pre kritických externých poskytovateľov IKT služieb**. Kritickí poskytovatelia budú podliehať dohľadu určeného hlavného orgánu dozoru. (16)



Obrázok č. 17 Taxonómia procesov riadenia rizík tretích strán v rámci TPRM frameworku (Zdroj: assets.kpmg.com/content/dam/kpmg/be/pdf/2023/DORA-webinar-TPRM-210923.pdf)

1.2.1.2.5.1 Riadenie rizika IKT tretích strán - Dohľad nad kritickými poskytovateľmi IKT tretích strán

- Nariadenie zavádza **rámec dohľadu na úrovni EÚ** pre CTPP (Critical Third-Party Provider), ktorý zahŕňa ich označovanie, ustanovenie hlavného orgánu dohľadu (Lead Overseer), vytvorenie spoločnej siete dohľadu (Joint Oversight Network - JON) a Fóra dohľadu (Oversight Forum). (18)



Obrázok č. 18 Schéma dohľadu nad kľúčovými poskytovateľmi IKT (Zdroj: č.18)

1.2.1.2.6 Mechanizmy zdieľania informácií

- Nariadenie umožňuje finančným inštitúciám dobrovoľne zdieľať informácie a spravodajské informácie o kybernetických hrozbách. Účasť na takýchto mechanizmoch zdieľania informácií je potrebné oznámiť príslušným orgánom. (18) (23)

1.2.1.2.7 Technické štandardy a špecifikácia požiadaviek (RTS a ITS)

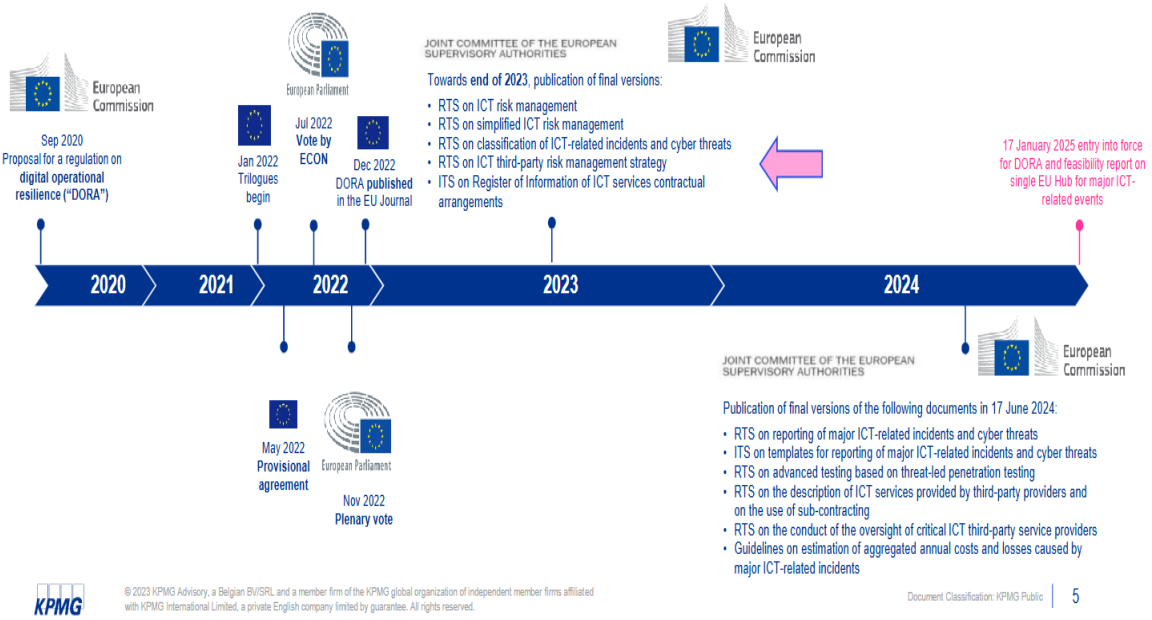
- Je dôležité poznamenať, že **špecifické detaily požiadaviek** sú rozpracované v technických štandardoch, ktoré vypracovali kľúčové orgány. Tieto **regulačné technické štandardy (RTS)** a **implementačné technické štandardy (ITS)** pokrývajú rôzne oblasti, ako napríklad kritériá pre klasifikáciu incidentov, štandardné šablóny pre hlásenie incidentov a register informácií, politiky riadenia IKT rizika a podobne. (21) (23)

1.2.1.3 Historický vývoj a implementačný harmonogram

Historicky kľúčové míľniky:

- **Posledné desaťročia**: Využívanie IKT začalo plniť kľúčovú úlohu v oblasti poskytovania finančných služieb, stalo sa zásadným pre každodenné funkcie finančných subjektov. (16)
- **Po finančnej kríze v roku 2008**: Reformy posilnili finančnú odolnosť, ale bezpečnosť IKT a digitálna odolnosť neboli stredobodom pozornosti regulačného programu. (16)
- **September 2020**: Európska komisia publikovala návrh nariadenia DORA s cieľom posilniť kontinuitu a kvalitu finančných služieb v prípade digitálnych hrozieb, pričom osobitný dôraz bol kladený na nové technológie (napr. cloud, DLT, AI, ML) a riziká spojené so závislosťou od tretích strán. (19)
- **Pred rokom 2022**: Existujúce právne akty EÚ riešili IKT riziko len čiastočne, čo viedlo k nedostatkom a nezrovnalostiam v oblastiach ako nahlasovanie incidentov a testovanie digitálnej prevádzkovej odolnosti. Rozdiely vnútroštátnych prístupov vytvárali prekážky pre vnútorný trh. (16)

- **Leto 2022**: Vyjednávači EÚ dosiahli detailnú technickú dohodu o obsahu DORA. (16)
- **14. december 2022:** Formálne prijatie nariadenia DORA (23)
- **27. december 2022**: Nariadenie DORA bolo publikované v Úradnom vestníku Európskej únie. (16)
- **16. január 2023**: Nariadenie DORA vstúpilo do platnosti. Cieľom nariadenia je konsolidovať a vylepšiť požiadavky na IKT riziko a zaviesť rámec dohľadu nad kritickými externými poskytovateľmi IKT služieb. (16) (25)



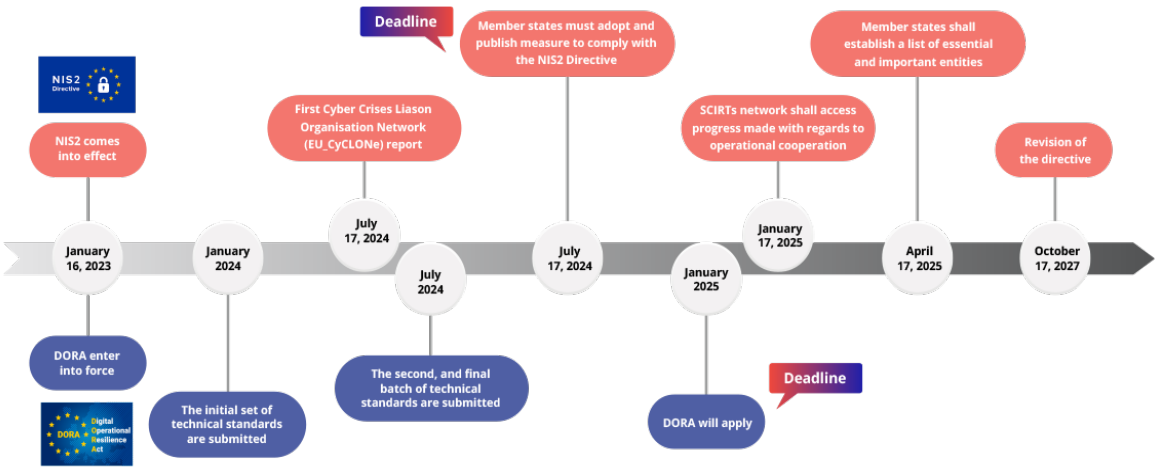
Obrázok č. 19 Časová os legislatívneho procesu a implementácie nariadenia DORA vrátane RTS a ITS (Zdroj: assets.kpmg.com/content/dam/kpmg/be/pdf/2023/DORA-webinar-SecOps-23-11.pdf)

Implementačný harmonogram:

Nariadenie DORA vstúpilo do platnosti **16. januára 2023**. Finančné inštitúcie majú **24 mesiacov** na implementáciu nových pravidiel. Kľúčové dátumy a míľniky implementačného harmonogramu sú nasledovné. (25)

- **16. január 2023: Nariadenie DORA vstúpilo do platnosti**. (25)
- **Do 17. januára 2024**: Európske orgány dohľadu (ESA) predložia Komisii **návrh vykonávacích technických predpisov (ITS) na stanovenie štandardných vzorov pre register informácií o zmluvných dojednaniach s externými poskytovateľmi IKT služieb**. (16)

- **Do 17. júla 2024:**
    - ESA vydajú **usmernenia o spolupráci medzi európskymi orgánmi dohľadu a príslušnými orgánmi.**
    - ESA predložia Komisii **návrh regulačných technických predpisov (RTS) na upresnenie informácií pre dobrovoľné určenie za kritického externého poskytovateľa IKT služieb, obsah informácií poskytovaných hlavnému orgánu dozoru a kritériá na určenie zloženia spoločného prieskumného tímu.** (16)
- **Do 17. júla 2024**: Finančné subjekty by mali zohľadniť novozavedené zásady v zmluvách o poskytovaní služieb outsourcingu a v zmluvách s dodávateľmi. (20)
- **Do 17. januára 2025:**
    - ESA predložia Európskemu parlamentu, Rade a Komisii **správu o predpokladoch na zriadenie jednotného centra EÚ pre nahlasovanie incidentov**. (16)
    - **Finančné subjekty musia implementovať požiadavky nariadenia DORA** do svojich stratégií, politík, postupov a systémov riadenia rizík. (25)
- **Do 17. januára 2025**: ESA predložia Komisii návrh RTS bližšie špecifikujúci podrobný obsah politiky v súvislosti so zmluvnými dojednaniami o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie, ktoré poskytujú externí poskytovatelia IKT služieb. (16)
- **17. január 2025:** Začiatok **uplatňovania** nariadenia DORA. Od tohto dátumu nadobúdajú právnu záväznosť všetky požiadavky stanovené nariadením DORA voči regulovaným finančným subjektom. (23)



Obrázok č. 20 Časová os implementácie smernice NIS2 a nariadenia DORA (Zdroj: avepoint.com/uk/lp/nis2-dora-compliance)

1.2.2 Subjekty spadajúce pod DORA

1.2.2.1 Kategorizácia regulovaných finančných subjektov

Podľa nariadenia DORA sa za **finančné subjekty** považujú :

a) Úverové inštitúcie

b) Investičné spoločnosti

c) Poskytovatelia služieb informácií o účte

d) Platobné inštitúcie , vrátane platobných inštitúcií s výnimkou podľa smernice (EÚ) 2015/2366

e) Inštitúcie elektronických peňazí

f) Poskytovatelia služieb týkajúcich sa kryptoaktív

g) Centrálne depozitáre cenných papierov

h) Centrálne protistrany

i) Obchodné miesta

j) Archívy obchodných údajov

k) Správcovia alternatívnych investičných fondov

l) Správcovské spoločnosti podnikov kolektívneho investovania do prevoditeľných cenných papierov (PKICPP)

m) Poskytovatelia služieb vykazovania údajov

n) Poisťovne a zaisťovne

o) Sprostredkovatelia poistenia, zaisťovací sprostredkovatelia a sprostredkovatelia doplnkového poistenia

p) Inštitúcie zamestnaneckého dôchodkového zabezpečenia

q) Ratingové agentúry

r) Správcovia kritických referenčných hodnôt

s) Poskytovatelia služieb hromadného financovania

t) Archívy sekuritizačných údajov

u) **Externí poskytovatelia IKT služieb** (16)

Obrázok č. 21 Typy organizácií, na ktoré sa vzťahuje pôsobnosť nariadenia DORA (Zdroj: cpl.thalesgroup.com/compliance/emea/data-security-compliance-dora-resilience-act)

Naopak, z rozsahu pôsobnosti sú vylúčené **poštové žirové inštitúcie** (poštové finančné inštitúcie) a **subjekty Európskeho systému centrálnych bánk**. (23)

Hoci sa nariadenie DORA vzťahuje na prevažnú väčšinu firiem pôsobiacich v oblasti finančných služieb v EÚ, **zohľadňuje existujúce významné rozdiely medzi týmito subjektmi**, a to najmä **čo sa týka ich veľkosti a celkového rizikového profilu** a **systémovej dôležitosti**. V súlade so **zásadou proporcionality** nariadenie rozlišuje **medzi rôznymi kategóriami finančných subjektov**, pričom pre niektoré z nich stanovuje **zjednodušený rámec riadenia rizík v oblasti IKT**. (16) (20)

Do tejto kategórie (zjednodušeného rámca) patria:

- **Malé a neprepojené investičné spoločnosti**
- **Malé inštitúcie zamestnaneckého dôchodkového zabezpečenia**, ktoré spĺňajú určité podmienky týkajúce sa počtu členov a sú vylúčené z rozsahu pôsobnosti smernice (EÚ) 2016/2341.
- **Inštitúcie vyňaté** podľa smernice 2013/36/EÚ
- **Platobné inštitúcie** uvedené v článku 32 ods. 1 smernice (EÚ) 2015/2366 a **inštitúcie elektronických peňazí** uvedené v článku 9 smernice 2009/110/ES, ak boli vyňaté v súlade s vnútroštátnym právom transponujúcim tieto právne akty Únie. Naopak, tie platobné a elektronické peňažné inštitúcie, ktoré neboli vyňaté, podliehajú všeobecnému rámcu DORA.
- **Mikropodniky.** (16)

Táto kategorizácia umožňuje **cielené uplatňovanie požiadaviek**, čím sa zabezpečuje primeraná úroveň digitálnej prevádzkovej odolnosti v celom finančnom sektore EÚ, bez zbytočnej administratívnej záťaže pre menšie a menej rizikové subjekty. (16)

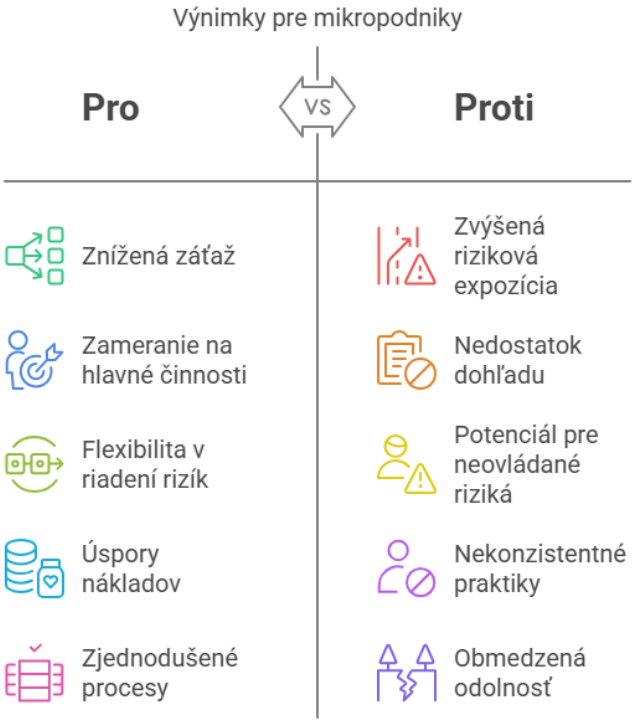
Navyše, zahrnutie externých poskytovateľov IKT služieb do rozsahu pôsobnosti nariadenia predstavuje **proaktívny krok k riešeniu narastajúcej závislosti finančných subjektov na týchto službách**. (16)

1.2.2.2 Výnimky a zjednodušený režim pre mikropodniky

Od finančných subjektov, ktoré sa kvalifikujú ako **mikropodniky** alebo podliehajú zjednodušenému rámcu riadenia IKT rizika, **sa nevyžaduje**, aby:

- ustanovili funkciu monitorovania dojednaní o využívaní IKT služieb s externými poskytovateľmi
- určili člena vrcholového manažmentu zodpovedného za dohľad nad súvisiacimi rizikami (súvisiacou rizikovou expozíciou a príslušnou dokumentáciou)
- priradili zodpovednosť za riadenie IKT rizika a dohľad nad ním osobe vykonávajúcej kontrolnú funkciu a zabezpečili primeranú úroveň nezávislosti tejto osoby
- zdokumentovali a preskúmali aspoň raz ročne rámec riadenia IKT rizika
- vykonávali hĺbkové posúdenia po rozsiahlych zmenách infraštruktúry

- pravidelne vykonávali vnútorný audit rámca riadenia IKT rizika
- pravidelne vykonávali analýzy rizík v súvislosti s pôvodnými IKT systémami
- zabezpečovali nezávislé vnútorné audítorské preskúmania vykonávania plánov reakcie a obnovy v oblasti IKT
- mali vytvorenú funkciu krízového riadenia.
- rozšírili testovanie kontinuity činnosti a plánov reakcie a obnovy tak, aby sa v nich zachytili scenáre prechodu medzi primárnou infraštruktúrou IKT a redundantnými zariadeniami
- oznamovali odhad súhrnných ročných nákladov a strát spôsobených závažnými incidentmi súvisiacimi s IKT
- udržiavali redundantné IKT kapacity.
- informovali vnútroštátne príslušné orgány o zmenách vykonaných na základe preskúmaní realizovaných po penetračných testoch na základe konkrétnej hrozby (TLPT). (16)



Obrázok č. 22 Výhody a nevýhody uplatnenia výnimiek DORA pre mikropodniky (Zdroj: Vlastné spracovanie)

Čo sa týka testovania digitálnej prevádzkovej odolnosti, **mikropodniky** vykonávajú testy tak, že kombinujú **prístup založený na riziku** so **strategickým plánovaním testovania IKT**. Pritom náležite zohľadňujú potrebu zachovať vyvážený prístup medzi rozsahom zdrojov a časom venovaným testovaniu a naliehavosťou, typom rizika, kritickosťou informačných aktív a poskytovaných služieb, ako aj schopnosťou finančného subjektu podstupovať predvídané riziká. (16)

Plány reakcie a obnovy v oblasti IKT **nepodliehajú nezávislému vnútornému audítorskému preskúmaniu v prípade mikropodnikov**, na rozdiel od ostatných finančných subjektov. (16)

Väčšie a systémovo významnejšie finančné inštitúcie (veľké systémové úverové inštitúcie, burzy cenných papierov, centrálne depozitáre cenných papierov a centrálne protistrany) podliehajú širšej úrovni kontroly vzhľadom na ich potenciálny systémový význam. (16) (25)

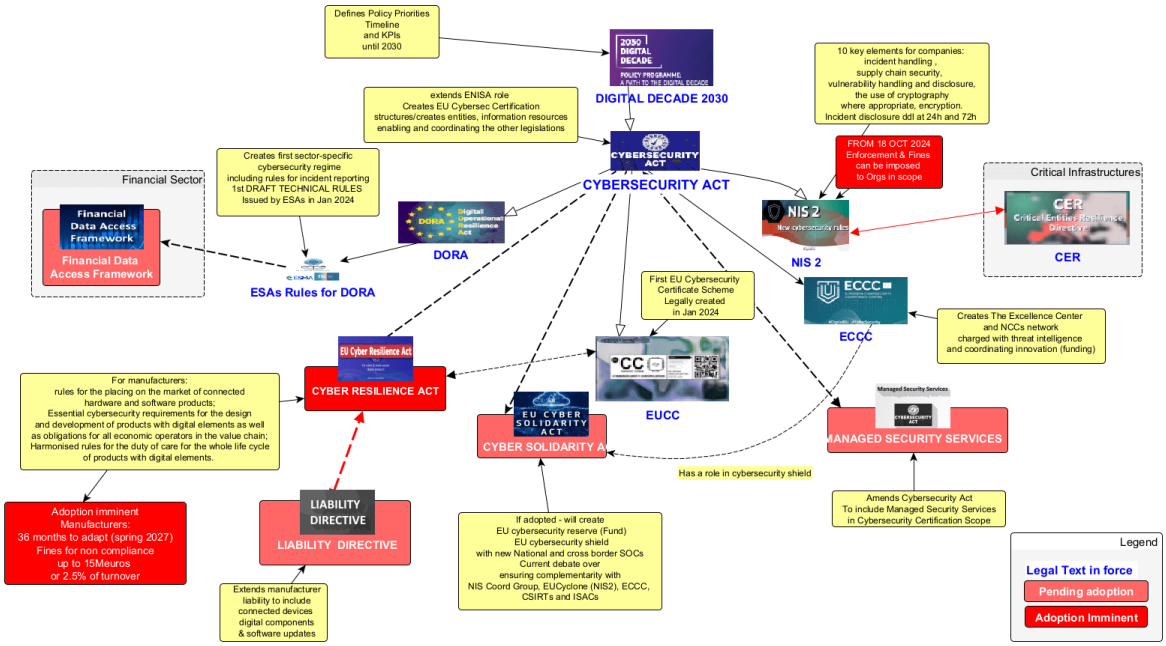
Špecifické požiadavky pre **identifikované finančné subjekty s dostatočnou IKT vyspelosťou**:

- **pokročilé testovanie digitálnej prevádzkovej odolnosti** (Threat-Led Penetration Testing – TLPT). Tieto testy sú náročnejšie a zamerané na odhaľovanie a riešenie potenciálnych zraniteľností. (16)

1.2.3 "Lex specialis" a porovnanie DORA vs. NIS2

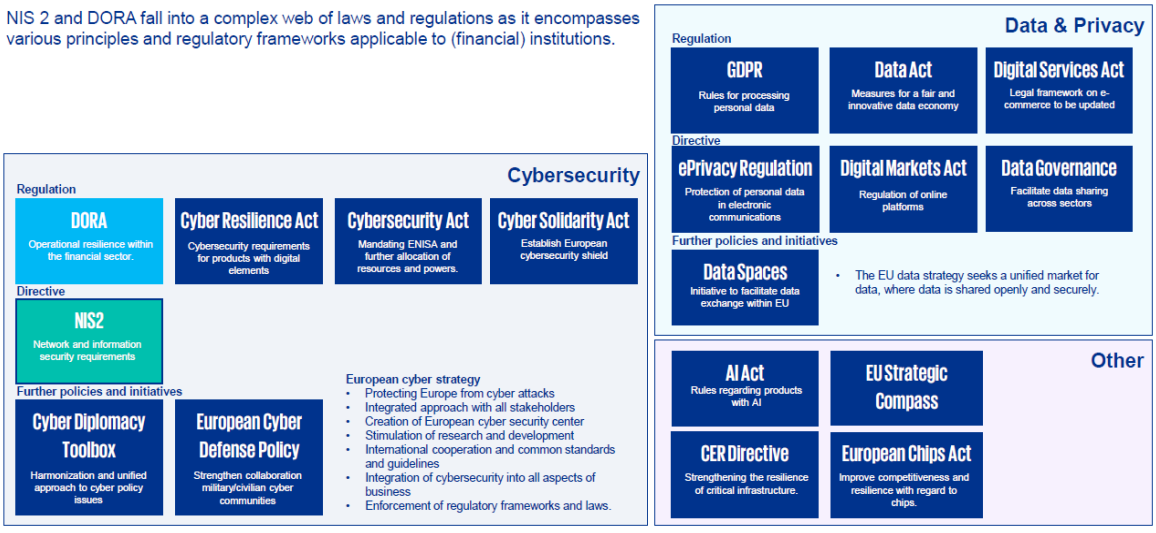
1.2.3.1 Lex specialis a komplementarita

Kľúčovým aspektom vzťahu medzi DORA a NIS2 je princíp **lex specialis derogat legi generali (špeciálny zákon ruší všeobecný zákon)**. Nariadenie DORA v odôvodnení č. 16 výslovne uvádza ako *lex specialis* vo vzťahu k smernici (EÚ) 2022/2555 (NIS2). Tento právny princíp znamená, že nariadenie DORA **má prednosť pred akýmikoľvek prekrývajúcimi sa regulačnými textami**, ako je smernica NIS2. To znamená, že finančné inštitúcie musia primárne dodržiavať požiadavky nariadenia DORA. (16) (26)



Obrázok č. 23 Prehľad hlavných legislatívnych iniciatív EÚ v oblasti kybernetickej bezpečnosti a ich prepojení (Zdroj: dossproject.eu/the-cra-and-the-new-eu-cybersecurity-architecture/)

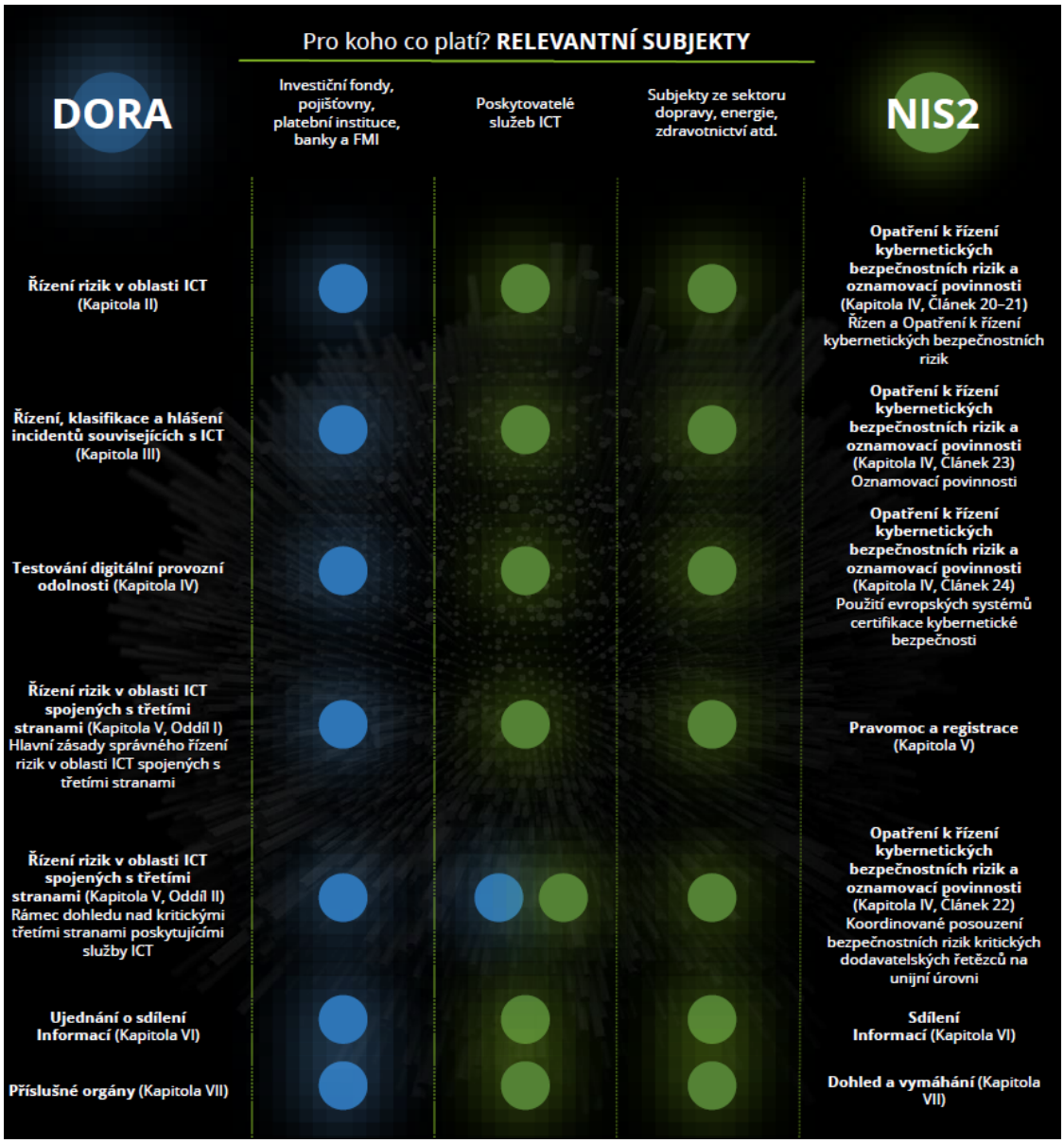
Článok 4 smernice NIS 2 (Smernica (EÚ) 2022/2555) stanovuje, že **požiadavky NIS 2 sa neuplatňujú na subjekty, ktoré patria pod sektorovo špecifické právne predpisy, ako je DORA**. To znamená, že finančné subjekty, na ktoré sa vzťahuje DORA, **nepodliehajú požiadavkám na kybernetickú bezpečnosť stanoveným v smernici NIS 2**, s výnimkou prípadov výslovne uvedených v nariadení DORA. (18) (21)



Obrázok č. 24 Európsky regulačný rámec pre finančné inštitúcie v oblasti kyberbezpečnosti a ochrany údajov (Zdroj: pvib.nl/cms/public/files/2024-07/presentatie-ronald-heil-en-ali-alam-kpmg.pdf)

Napriek tomu, že DORA predstavuje pre finančný sektor "lex specialis", **zachováva sa silný vzťah s horizontálnym rámcom Únie v oblasti kybernetickej bezpečnosti, ktorým je NIS2**. Finančné subjekty by mali naďalej zostať súčasťou „ekosystému“ NIS2, napríklad účasťou v skupine pre spoluprácu a tímoch pre riešenie počítačových bezpečnostných incidentov (CSIRT). To umožňuje **medziodvetvové vzdelávanie a efektívne využívanie skúseností z iných sektorov** pri riešení kybernetických hrozieb. (16)

Európske orgány dohľadu a vnútroštátne príslušné orgány v rámci DORA majú možnosť **zúčastňovať sa na diskusiách o strategickej politike a na technických činnostiach skupiny pre spoluprácu podľa NIS2** a vymieňať si informácie s jednotnými kontaktnými miestami zriadenými podľa NIS2. Príslušné orgány podľa DORA by mali taktiež **konzultovať a spolupracovať s tímami CSIRT** a môžu žiadať o technické poradenstvo od orgánov určených podľa NIS2. (16)



Obrázok č. 25 Porovnanie pôsobnosti nariadenia DORA a smernice NIS2 na vybrané subjekty (Zdroj: č.26)

Táto komplementarita zabezpečuje **súlad so stratégiami kybernetickej bezpečnosti prijatými členskými štátmi** a umožňuje príslušným orgánom dohľadu nad finančnými subjektmi byť informované o kybernetických incidentoch týkajúcich sa iných sektorov, na ktoré sa vzťahuje NIS2. (16)

Princíp **komplementarity** sa prejavuje v tom, že hoci DORA stanovuje špecifické a prísnejšie požiadavky pre finančný sektor v oblasti digitálnej prevádzkovej odolnosti, **NIS2 naďalej platí pre subjekty finančného sektora v otázkach, ktoré nie sú pokryté nariadením DORA**, alebo v prípadoch, kde DORA odkazuje na NIS2. (16) (27)

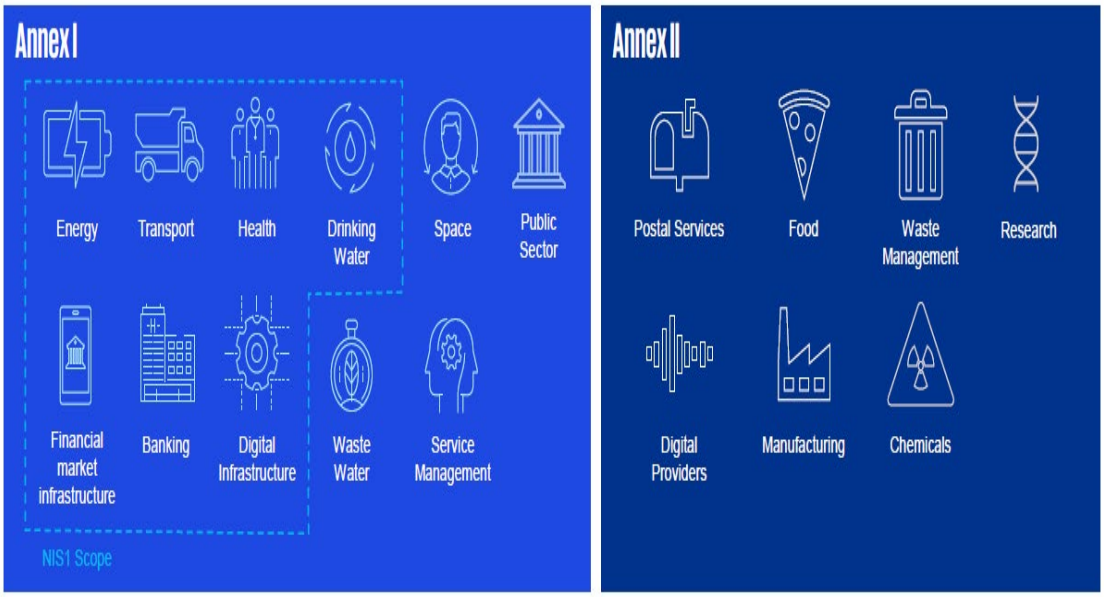
1.2.3.2 Porovnanie nariadenia DORA a smernice NIS2

1.2.3.2.1 Rozsah pôsobnosti a adresáti

Nariadenie DORA má **sektorovo špecifický rozsah pôsobnosti,** zameraný výlučne na subjekty pôsobiace v oblasti finančného sektora v EÚ. To zahŕňa široké spektrum inštitúcií, ako sú úverové inštitúcie, investičné fondy, poisťovne, platobné inštitúcie a banky. Cieľom je zabezpečiť prevádzkovú odolnosť týchto subjektov v digitálnom prostredí a tým chrániť stabilitu finančného systému EÚ. (20) (26) (27)

NIS2 má **širší, horizontálny charakter** a vzťahuje sa na **verejné a súkromné subjekty** označené ako **základné a dôležité subjekty** v rôznych sektoroch hospodárstva, ktoré sú kľúčové pre spoločenské a hospodárske činnosti na vnútornom trhu. Medzi tieto sektory patria napríklad doprava, energetika, zdravotníctvo a digitálna infraštruktúra.

NIS2 zavádza **pravidlo veľkostného obmedzenia**, pričom do pôsobnosti smernice spadajú všetky subjekty, ktoré sa považujú za stredné podniky alebo prekračujú stropy pre stredné podniky a pôsobia v určených odvetviach. Členské štáty môžu zahrnúť aj niektoré malé podniky a mikropodniky s kľúčovou úlohou. Cieľom je dosiahnuť vysokú spoločnú úroveň kybernetickej bezpečnosti v celej Únii a zlepšiť fungovanie vnútorného trhu. (26) (28)

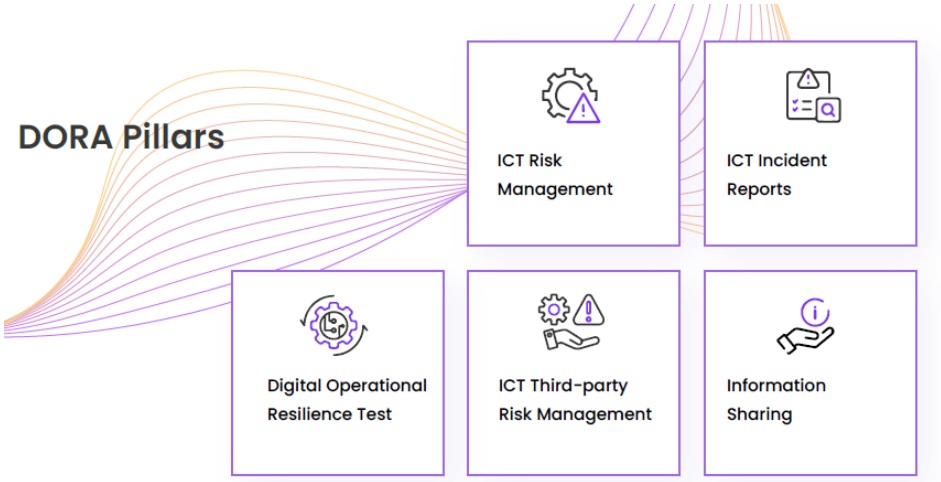


Obrázok č. 26 Sektory spadajúce pod smernicu NIS2 (Zdroj: pvib.nl/cms/public/files/2024-07/presentatie-ronald-heil-en-ali-alam-kpmg.pdf)

1.2.3.2.2 Kľúčové Povinnosti

DORA kladie dôraz na digitálnu prevádzkovú odolnosť finančných subjektov. Nariadenie stanovuje záväzné pravidlá pre:

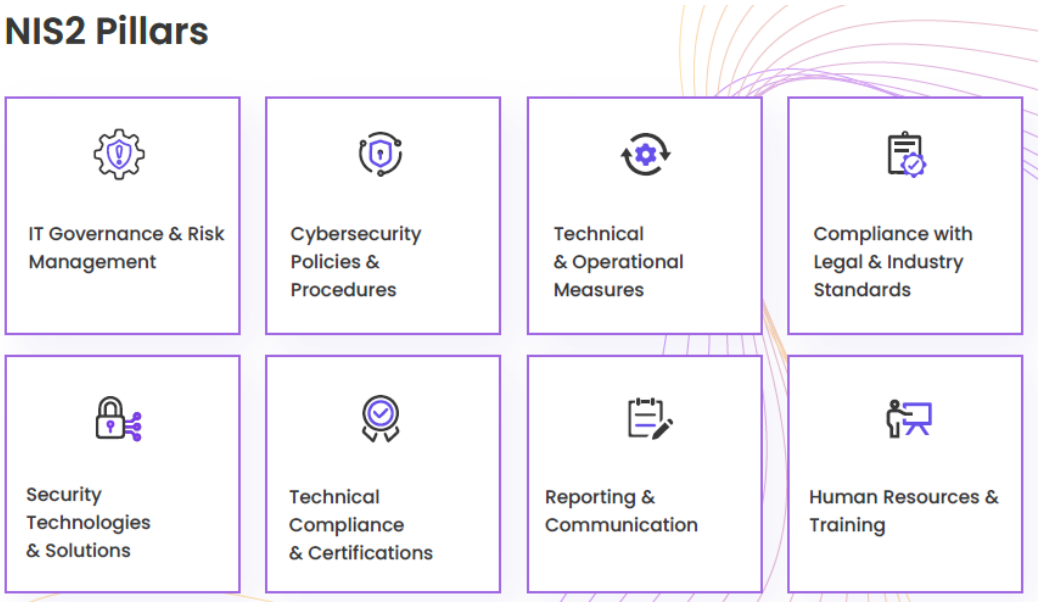
- **Riadenie IKT Rizika**
- **Hlásenie incidentov súvisiacich s IKT**
- **Testovanie digitálnej prevádzkovej odolnosti**
- **Riadenie rizika tretích strán v oblasti IKT**
- **Výmena informácií** (20)



Obrázok č. 27 Päť hlavných pilierov nariadenia DORA (Zdroj: č.27)

Finančné subjekty musia rozšíriť svoju obchodnú perspektívu aj na oblasť odolnosti a jasne stanoviť zodpovednosť na úrovni vrcholového vedenia. DORA vyžaduje zavedenie komplexnej politiky kontinuity činností v oblasti IKT a politík na testovanie IKT systémov, kontrol a procesov. (16) (20)

NIS2 sa zameriava na zavedenie **opatrení na riadenie kybernetických bezpečnostných rizík** a **oznamovacie povinnosti**. Základné a dôležité subjekty musia prijať primerané technické, prevádzkové a organizačné opatrenia na riadenie bezpečnostných rizík a minimalizáciu dopadov incidentov. Smernica stanovuje **viacfázový prístup k oznamovaniu významných incidentov**. NIS2 ukladá členským štátom povinnosť prijatia národných stratégií kybernetickej bezpečnosti a určenia príslušných orgánov a tímov CSIRT. (28)



Obrázok č. 28 Osem hlavných pilierov smernice NIS2 (Zdroj: č.27)

Konkrétne povinnosti podľa NIS2 zahŕňajú oblasti ako:

- **Opatrenia na riadenie kybernetických bezpečnostných rizík**: Implementácia politík na riešenie rizík, incidentov, kontinuity činností a bezpečnosti dodávateľského reťazca.
- **Hlásenie incidentov:** Oznamovanie incidentov, ktoré majú významný dopad na poskytovanie ich služieb. NIS2 zavádza viacfázový prístup k oznamovaniu incidentov.
- **Riešenie zraniteľností:** Stanovenie postupov na riešenie zistených zraniteľností.
- **Kybernetická hygiena a školenia:** Implementácia základných postupov kybernetickej hygieny a organizovanie školení pre zamestnancov. (16)

1.2.3.2.3 Výnimky

DORA zavádza **zjednodušený rámec riadenia IKT rizika** pre určité finančné subjekty, najmä **mikropodniky** a subjekty, na ktoré sa vzťahuje zjednodušený rámec. (16).

Z rámca dohľadu sú vyňaté finančné subjekty poskytujúce IKT služby iným finančným subjektom, ak už podliehajú dohľadu podľa iných právnych aktov Únie v oblasti finančných služieb, ako aj externí poskytovatelia IKT služieb poskytujúci služby prevažne subjektom svojej vlastnej skupiny alebo výlučne v jednom členskom štáte finančným subjektom pôsobiacim len v tomto štáte. (16)

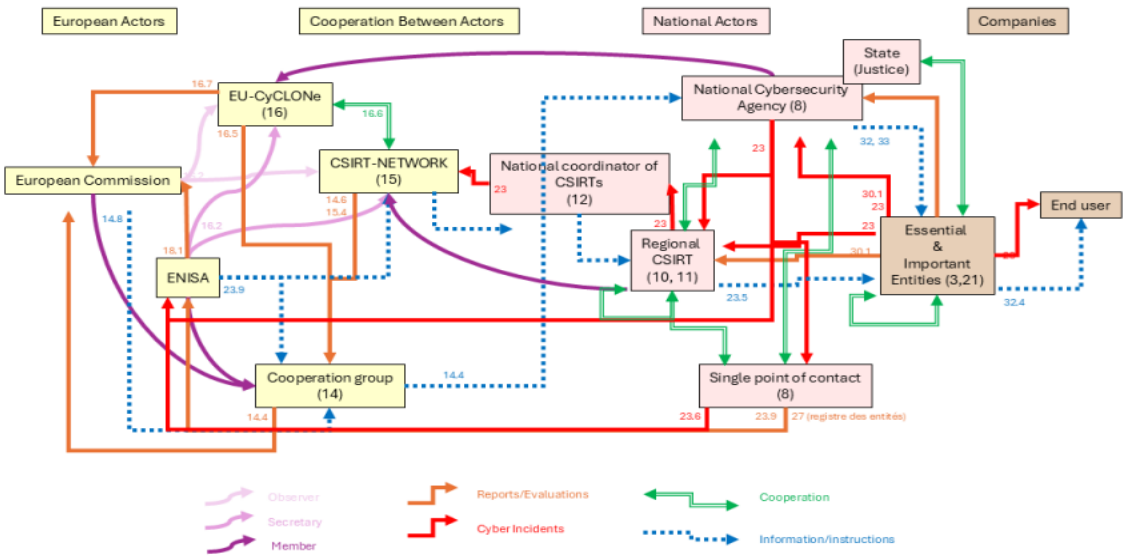
NIS2 vyčleňuje z rozsahu pôsobnosti subjekty vykonávajúce činnosť prevažne v oblasti **národnej bezpečnosti, verejnej bezpečnosti, obrany alebo vymáhania práva**. Výnimka sa týka aj diplomatických a konzulárnych misií členských štátov v tretích krajinách. (28)

1.2.3.2.4 Orgány dohľadu

DORA zavádza **rámec dohľadu na úrovni EÚ** pre **kritických externých poskytovateľov IKT služieb**. Za vykonávanie dohľadu nad týmito poskytovateľmi je určený jeden z troch európskych orgánov dohľadu (ESA) - EBA, EIOPA a ESMA, ktoré zohrávajú kľúčovú úlohu pri vývoji technických štandardov a zabezpečovaní konvergencie dohľadu. (16) (18)

Na úrovni členských štátov dohľad nad finančnými subjektmi vykonávajú **príslušné vnútroštátne orgány (NCA)** v rámci **Európskeho systému finančného dohľadu (ESFS)**. (16) (18)

NIS2 ponecháva výkon dohľadu na **príslušných orgánoch určených členskými štátmi**. Smernica rozlišuje medzi **základnými subjektmi**, ktoré podliehajú komplexnému dohľadu *ex ante* a *ex post*, a **dôležitými subjektmi**, ktoré podliehajú miernejšiemu dohľadu *ex post*. (28)



Obrázok č. 29 Orgány a väzby dohľadu podľa smernice NIS2 (Zdroj: cyberelements.io/complying-with-the-nis2-directive/)

1.2.3.2.5 Hlásenie incidentov

DORA zavádza **harmonizovaný režim nahlasovania incidentov súvisiacich s IKT**. Stanovuje trojstupňový prístup k hláseniu (počiatočné, priebežné a záverečné hlásenie) príslušným vnútroštátnym orgánom, ktoré následne tieto informácie odovzdávajú relevantným zainteresovaným stranám, vrátane ESA, ECB a tímov CSIRT. (16) (18)

NIS2 stanovuje **viacfázový prístup k oznamovaniu významných incidentov** príslušným vnútroštátnym orgánom a tímom CSIRT pre základné a dôležité subjekty. (18) (28)

1.2.3.2.6 Sankcie

DORA nešpecifikuje **konkrétne sumy administratívnych sankcií** pre finančné subjekty za porušenie nariadenia. Uvádza len, že príslušné orgány by mali mať právomoci na ukladanie sankcií. (16)

NIS2 stanovuje, že **každý príslušný orgán by mal mať právomoc ukladať správne pokuty** alebo požadovať uloženie správnych pokút základným a dôležitým subjektom. (28)

NIS2 umožňuje členským štátom stanoviť **pravidlá týkajúce sa trestných sankcií** za porušenie vnútroštátnych pravidiel implementujúcich túto smernicu. (28)

NIS2 zároveň stanovuje, že sankcie za porušenie smernice by mali byť účinné, primerané a odrádzajúce. (28)

Článok 34 ods. 4 a 5 smernice NIS2 uvádza **výšky správnych pokút** pre základné subjekty (najmenej **10 000 000 EUR alebo 2 % celkového celosvetového ročného obratu**) a dôležité subjekty (najmenej **7 000 000 EUR alebo 1,4 % celkového ročného obratu**). (28)

1.2.3.2.7 Technické štandardy

DORA poveruje európske orgány dohľadu (EBA, ESMA, EIOPA) vypracovaním **regulačných a vykonávacích technických predpisov (RTS - regulačné technické štandardy a ITS - implementačné technické štandardy)** na bližšie špecifikovanie

rôznych aspektov nariadenia, ako napríklad prvkov rámca riadenia IKT rizika, nahlasovania incidentov a testovania odolnosti. (16)

NIS2 podporuje **používanie európskych a medzinárodných noriem a technických špecifikácií** upravujúcich bezpečnosť sietí a informačných systémov. Agentúra ENISA v spolupráci s členskými štátmi vydáva odporúčania a pokyny v tejto oblasti. (28)

1.2.3.2.8 Úroveň harmonizácie

DORA prináša **vyššiu úroveň harmonizácie** v oblasti digitálnej prevádzkovej odolnosti pre finančný sektor v celej EÚ prostredníctvom priamo uplatniteľného nariadenia. (20)

NIS2 je **smernicou**, čo znamená, že členské štáty ju musia **transponovať** do svojho vnútroštátneho práva, čo môže viesť k určitým rozdielom v implementácii a úrovni harmonizácie. (28)

NIS2 ako smernica **stanovuje minimálne požiadavky**, ktoré musia členské štáty implementovať do svojich národných právnych predpisov. (29)

1.2.3.2.9 Sektorový vs. horizontálny prístup

DORA predstavuje **sektorovo špecifický prístup** zameraný na potreby a špecifiká finančného sektora. (26)

NIS2 uplatňuje **horizontálny prístup** a stanovuje rámec pre kybernetickú bezpečnosť pre širokú škálu odvetví. (28)

1.2.3.2.10 Zhodnotenie

„*DORA je zaujímavá svojím explicitným a implicitným prepojením s NIS2. Explicitné prepojenia vidíme v dôležitých článkoch, ako je* ***článok 3*** *(definície) a* ***článok 19*** *(hlásenie incidentov), ako aj v článkoch, týkajúcich sa spolupráce medzi regulačnými orgánmi, ako sú* ***články 15, 20 a 41****, ktoré sa zaoberajú harmonizáciou, alebo* ***články 22, 32 a 47****, ktoré sa zaoberajú vzájomnou spoluprácou. Implicitné prepojenie je dané rozsahom pôsobnosti, ktorý je uvedený v článku 1 ods. 2 DORA. Nariadenie má 2 zaujímavé prvky. Prvým je* ***dohľad nad dodávateľmi****, ktorý je opísaný v oddiele II (Rámec pre dohľad nad kritickými 3. stranami) v* ***článkoch 31 až 43****. Druhý prvok, súvisí so schopnosťou riadiť tretie strany -* ***požiadavky na zmluvy s dodávateľmi v článku 30****.*“ (30)

NIS 2 vs DORA
1.0, 27.03.2024

Topic	NIS 2 Directive	DORA
Code	**Directive** (EU) 2022/2555	**Regulation** (EU) 2022/2554
Summary	Cybersecurity of network and information systems (2022)	Digital operational resilience for the financial sector
Date of signature	14/12/2022	14/12/2022
Date of effect	16/01/2023 By 17 October 2024, Member States shall adopt and publish the measures necessary to comply with this Directive	17/01/2025
The aim	To achieve a **high common level of cybersecurity across the Union**, with a view to improving the functioning of the internal market	To achieve a **high common level of digital operational resilience**
Core terms	*'**Security of network and information systems**' means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems*	
	*'**Cybersecurity**' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats*	*'**Digital operational resilience**' means the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions*
Sectors	**Essential and important entities** (Banking and Financial market infrastructures are sectors of high criticality (essential entities))	**Financial entities** (DORA is a sector-specific Union legal act)
Main actors	European Union Agency on Cybersecurity (**ENISA**) National competent authorities [**NCSCs**] National Computer Security Incident Response Teams (**CSIRTs**) Cooperation Group European cyber crisis liaison organisation network (EU-CyCLONe)	**European Supervisory Authorities, ESAs** / Lead Overseer (for critical ICT third-party service providers): • European Banking Authority, EBA • European Insurance and Occupational Pensions Authority, EIOPA • European Securities and Markets Authority, ESMA European Union Agency on Cybersecurity (ENISA)
Core articles (for entities)	Article 20 Governance Article 21 Cybersecurity risk-management measures Article 22 Union level coordinated security risk assessments of critical supply chains Article 23 Reporting obligations Article 24 Use of European cybersecurity certification schemes **General Requirements**...	CHAPTER II. ICT risk management (Articles 5-16) CHAPTER III. ICT-related incident management, classification and reporting (Articles 17-23) CHAPTER IV. Digital operational resilience testing (Articles 24-27) CHAPTER V. Managing of ICT third-party risk (Articles 28-44) CHAPTER VI. Information-sharing arrangements (Article 45) Many **specific requirements**...

Obrázok č. 30 Základné rozdiely medzi reguláciami NIS2 a DORA z pohľadu cieľov, rozsahu a aktérov (Zdroj: linkedin.com/in/AndreyProzorov/)

Governance	The management bodies shall **approve the cybersecurity risk-management measures**, **oversee its implementation** and **can be held liable for infringements** by the entities. The members of the management bodies are required **to follow training**, and shall encourage to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity [From Art.20]	Financial entities shall have in place an **internal governance and control framework** that ensures an effective and prudent management of ICT risk in order to achieve a high level of digital operational resilience. The management body shall **define, approve, oversee and be responsible for the implementation of all arrangements** related to the **ICT risk management framework**. The management body shall: (a) **bear the ultimate responsibility** for managing the financial entity's ICT risk; (b) put in place **policies** that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality, of data; (c) set clear **roles and responsibilities** for all ICT-related functions and establish appropriate governance arrangements to ensure effective and timely communication, cooperation and coordination among those functions; (d) bear the overall responsibility for setting and approving the **digital operational resilience strategy**, including the determination of the appropriate **risk tolerance level** of ICT risk of the financial entity; (e) approve, oversee and periodically review the implementation of the financial entity's **ICT business continuity policy** and **ICT response and recovery plans**, which may be adopted as a dedicated specific policy forming an integral part of the financial entity's overall business continuity policy and response and recovery plan; (f) approve and periodically review the financial entity's ICT **internal audit** plans, ICT audits and material modifications to them; (g) allocate and periodically review the **appropriate budget** to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including relevant ICT security awareness programmes and digital operational resilience training, and ICT skills for all staff; (h) approve and periodically review the financial entity's policy on arrangements regarding the use of ICT services provided by ICT **third-party service providers**; (i) put in place, at corporate level, **reporting channels** enabling it to be duly informed of the following: (i) arrangements concluded with ICT third-party service providers on the use of ICT services, (ii) any relevant planned material changes regarding the ICT third-party service providers, (iii) the potential impact of such changes on the critical or important functions subject to those arrangements, including a risk analysis summary to assess the impact of those changes, and at least major ICT-related incidents and their impact, as well as response, recovery and corrective measures. Financial entities, other than microenterprises, shall establish a role in order to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services, or shall designate a member of senior management as responsible for **overseeing the related risk exposure and relevant documentation**. Members of the management body shall actively keep up to date with sufficient **knowledge and skills** to understand and assess ICT risk and its impact on the operations of the financial entity, including by following specific **training** on a regular basis, commensurate to the ICT risk being managed.

Obrázok č. 31 Požiadavky na správu a riadenie kybernetických rizík podľa NIS2 a DORA (Zdroj: linkedin.com/in/AndreyProzorov/)

Cybersecurity risk-management measures	(a) **policies on risk analysis and information system security**; (b) **incident handling**; (c) **business continuity**, such as backup management and disaster recovery, and crisis management; (d) **supply chain security**, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers; (e) **security in network and information systems acquisition, development and maintenance**, including vulnerability handling and disclosure; (f) policies and procedures to **assess the effectiveness** of cybersecurity risk-management measures; (g) **basic cyber hygiene practices and cybersecurity training**; (h) policies and procedures regarding the use of **cryptography** and, where appropriate, encryption; (i) **human resources security, access control policies and asset management**; (j) the **use of multi-factor authentication** or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate. [From Art.21.2]	**ICT risk management.** Financial entities, other than micro-enterprises, shall: • have in place internal governance and control measures that ensure effective and prudent management of ICT risk; • ensure that their management body defines, approves, oversees and is responsible for all the relevant arrangements; • have in place a sound, comprehensive and well-documented ICT risk management framework with the necessary strategies, policies, procedures, protocols and tools to respond quickly and efficiently; • use and maintain updated ICT systems, protocols and tools that are appropriate, reliable, technologically resilient and have sufficient capacity; • identify, classify and adequately document all ICT-supported business functions, roles and responsibilities and review risk scenarios; • continuously monitor the security and operation of ICT systems and tools to minimise the impact of any ICT risk; • promptly detect anomalies and identify potential failure points; • put in place a comprehensive ICT business continuity policy with appropriate plans, procedures and mechanisms; • develop and document backup policies and restoration and recovery procedures; • deploy resources and staff to assess vulnerabilities and cyber threats, ICT-related incidents, especially cyberattacks, and analyse their potential impact on the entity's digital operational resilience; • devise crisis communication plans to disclose at least major ICT-related incidents or vulnerabilities to clients, counterparts and the public. **ICT-related incident management, classification and reporting.** Financial entities shall: • define, establish and implement measures to detect, manage, record and notify ICT-related incidents; • classify incidents and determine their impact using criteria such as number of clients and counterparts affected, duration, geographical spread and data losses; • report major ICT-related incidents to their designated competent authority, which forwards it to a higher body such as the European Central Bank or the European Banking Authority. **Digital operational resilience testing.** Financial entities, other than micro-enterprises, shall: • establish, maintain and review a sound and comprehensive digital operational testing programme equipped with the necessary assessments, tests, methodologies, practices and tools; • carry out, at least every 3 years, threat level penetration testing based on their risk profile and taking account of operational circumstances – and only use testers that are certified, possess the necessary expertise and suitability and have professional indemnity insurance. **Managing ICT third-party risk.** Financial entities shall: • manage third-party risk as an integral component of their overall ICT risk; • have in place contractual arrangements for ICT services to run their business operations in full compliance with the relevant legislation; • take account of the nature, scale, complexity and importance of ICT-related dependencies and any potential risks; • weigh the benefits and costs of alternative solutions when identifying and assessing any risks involved; • include in the contract each party's rights and obligations and the service agreement.

Obrázok č. 32 Opatrenia kybernetickej bezpečnosti a testovanie digitálnej odolnosti v NIS2 a DORA

(Zdroj: linkedin.com/in/AndreyProzorov/)

		Information-sharing arrangements. Financial entities may exchange among themselves cyber threat information and intelligence, provided that this: • aims to strengthen their digital operational resilience; • occurs within their trusted communities; • protects business confidentiality and personal data, and respects competition policy rules. [From the official summary]
Incident Notification	Notification of the local NCSC/CSIRT and recipients of their services of any significant incidents. Early warning: 24 hours Notification: 72 hours Final report: not later than one month	Reporting of major ICT-related incidents and voluntary notification of significant cyber threats to the national competent authority Notification of clients without undue delay in case of major ICT-related incidents and impact on the financial interests of clients
Mentioned standards and guidelines	ISO/IEC 27000 series	G7 Fundamental Elements of Cybersecurity
Expected additional guidance	Guidance from the NCSCs ENISA's guidance	ESAs' draft regulatory technical standards ENISA's guidance

Obrázok č. 33 Oznamovacie povinnosti, normy a odporúčania v reguláciách NIS2 a DORA (Zdroj: linkedin.com/in/AndreyProzorov/)

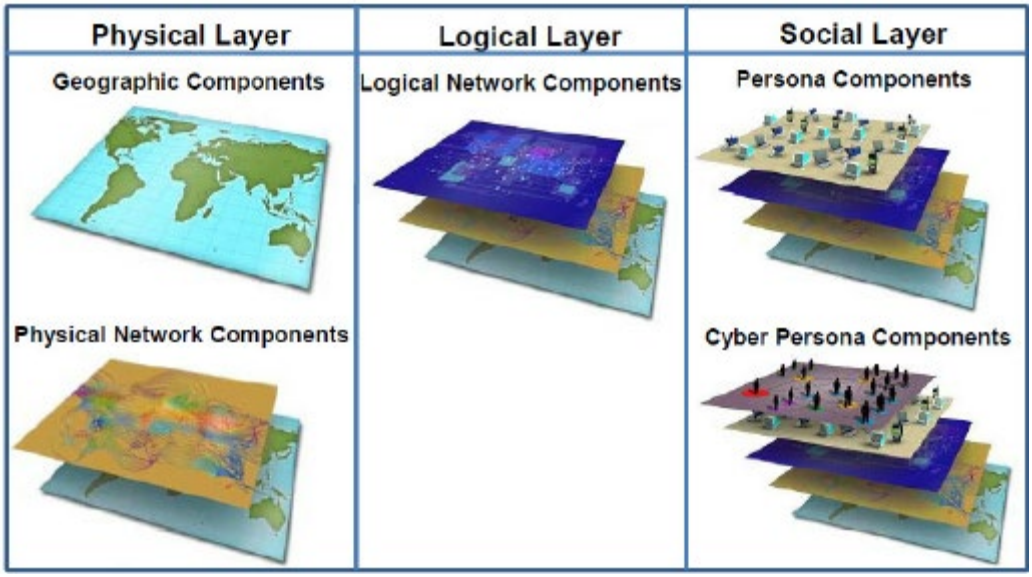
1.3 Kľúčové pojmy v oblasti kyberbezpečnosti

1.3.1 Kybernetický priestor, Kybernetická bezpečnosť a jej princípy

1.3.1.1 Kybernetický priestor

Kybernetický priestor predstavuje **digitálne prostredie** umožňujúce vznik, spracovanie a výmenu informácií prostredníctvom **informačných systémov, služieb a sietí elektronických komunikácií** využívajúcich protokol TCP/IP. Tento **dynamický systém**, hoci viazaný na hardvér, vytvára **nehmotné médium** charakterizované **decentralizovanosťou, globálnosťou a interaktívnosťou**. (31) (32)

Štruktúru kyberpriestoru tvoria **tri vrstvy**: **fyzická** (umiestnenie a hardvérové komponenty), **logická** (protokolové prepojenia) a **sociálna** (kyberosobnosť a osobnosti). Z hľadiska dostupnosti dát sa rozlišuje **Surface Web, Deep Web a Dark Web**, pričom kyberpriestor **zahŕňa všetky počítačové systémy, služby, používateľov a dáta**, nie len webové stránky. (31)



Obrázok č. 34 Vrstvový model kybernetického priestoru – fyzická, logická a sociálna vrstva (Zdroj: acqnotes.com/acqnote/careerfields/cyberspace)

1.3.1.2 Kybernetická bezpečnosť

Kybernetická bezpečnosť predstavuje **súhrn právnych, organizačných, technických a vzdelávacích prostriedkov** smerujúcich k **zabezpečeniu ochrany počítačových systémov a ďalších prvkov informačných a komunikačných technológií (IKT), aplikácií, dát a používateľov**. (31) (32)

Jej cieľom je **ochrana dôvernosti, integrity a dostupnosti informácií** počas ich spracovania, úschovy, distribúcie a prezentácie. (31)

Kybernetická bezpečnosť zahŕňa **schopnosť systémov reagovať na kybernetické hrozby a útoky** vrátane plánovania obnovy ich funkčnosti. Aplikuje sa v rámci **kyberpriestoru**, definovaného ako súbor väzieb a vzťahov medzi objektmi prístupnými prostredníctvom telekomunikačných sietí, ako aj mimo neho. (31)

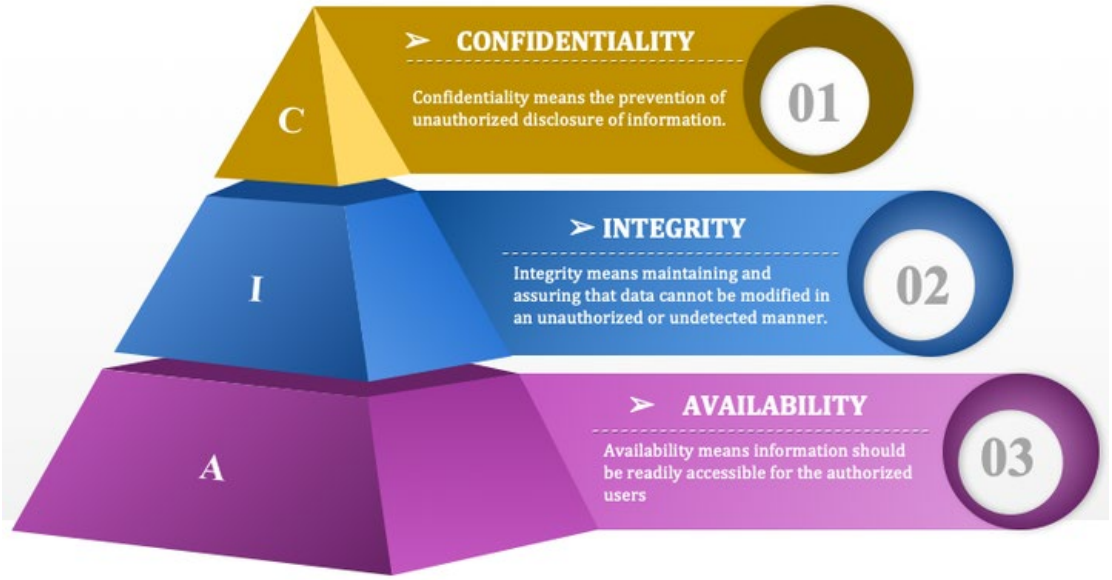
1.3.1.3 Princípy kybernetickej bezpečnosti

Princípy kybernetickej bezpečnosti sú implementované s cieľom ochrany ICT, dát a informácií. Základným rámcom týchto princípov je **triáda CIA**: **dôvernosť (Confidentiality)**, **celistvosť (Integrity)** a **dostupnosť (Availability)**. (31)

Dôvernosť zabezpečuje, že prístup k informáciám, dátam a ICT majú len autorizované subjekty, pričom sa odporúča zaviesť **klasifikáciu informácií** s ohľadom na ich hodnotu, právne požiadavky, citlivosť a kritickosť. (31)

Celistvosť predstavuje vlastnosť presnosti a úplnosti, zaisťujúcu nemožnosť neoprávneného zásahu do informácií, dát a počítačových systémov, čím garantuje ich neporušenosť. (31)

Dostupnosť definuje vlastnosť prístupnosti a použiteľnosti na žiadosť oprávnenej entity, čím zaručuje prístup k informáciám, dátam a systémom v okamihu potreby. Aplikácia triády CIA sa vzťahuje nielen na informácie, ale aj na dáta a samotné počítačové systémy. (31)



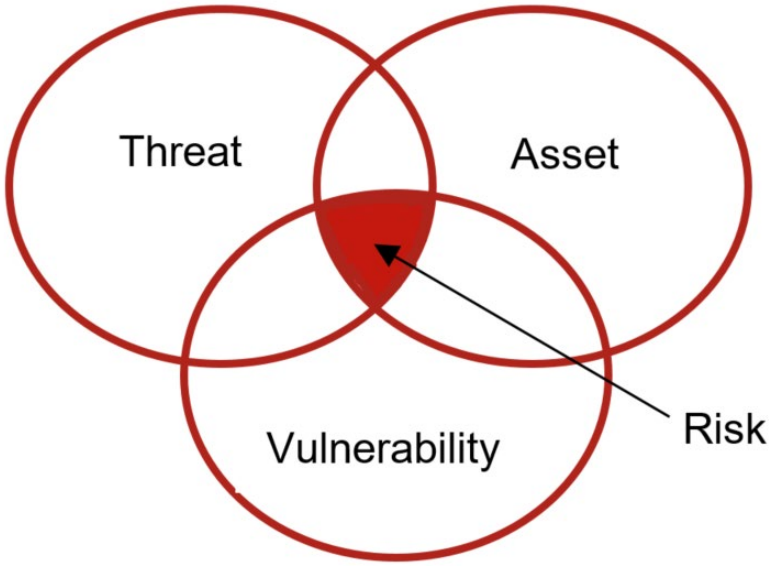
Obrázok č. 35 Tri piliere informačnej bezpečnosti – dôvernosť, integrita a dostupnosť (Zdroj: secureread ing.com/infobasics-basic-concept-information-security)

1.3.2 Kybernetické aktívum, zraniteľnosť, riziko

Aktívum je čokoľvek, čo má hodnotu pre organizáciu, štát alebo osobu. Môže byť hmotné (napr. počítačový systém) alebo nehmotné (napr. informácie), ale aj vlastnosť (napr. dostupnosť) či ľudia so svojimi znalosťami. Aktíva sa delia na primárne (informácie, služby) a podporné (technické aktíva, zamestnanci). (31) (32)

Zraniteľnosť označuje slabé miesto aktíva, softvéru alebo zabezpečenia, ktoré môže byť zneužité hrozbami. Zraniteľnosti sa klasifikujú ako známe (opravené alebo neopravené) a neznáme (skryté alebo neobjavené). Bezpečnostné zraniteľnosti sú potenciálnymi bezpečnostnými hrozbami a ich eliminácia je možná primárne, aktualizáciou softvéru. Príklady zraniteľností zahŕňajú nedostatočnú údržbu systémov, zastaranosť, slabú ochranu perimetra či nedostatočné bezpečnostné povedomie. (31) (32)

Riziko v kybernetickom priestore predstavuje potenciál, že hrozba využije zraniteľnosť aktíva alebo skupiny aktív a spôsobí organizácii škodu. Definuje sa aj ako účinok neistoty na dosiahnutie cieľov alebo ako akákoľvek primerane rozpoznateľná okolnosť či udalosť, ktorá by mohla mať negatívny dopad na bezpečnosť sietí a informačných systémov. Významnosť rizika sa stanovuje ako súčin dopadov rizika a pravdepodobnosti jeho výskytu. Pri hodnotení rizika sa zohľadňuje povaha rizika, zraniteľnosť aktíva a pravdepodobnosť premeny rizika na bezpečnostnú udalosť. (31)



Obrázok č. 36 Vizualizácia vzniku kybernetického rizika ako prieniku hrozby, zraniteľnosti a aktíva
(Zdroj: infoxchange.org/nz/au/news/2019/07/understanding-cyber-threat-landscape)

1.3.2.1 Procesy a pojmy riadenia kybernetických rizík

Riadenie rizík predstavuje súbor koordinovaných aktivít zameraných na efektívne usmerňovanie a kontrolovanie organizácie v súvislosti s potenciálnymi alebo existujúcimi rizikami. (33)

Hodnotenie rizík je definované ako systematický proces identifikácie, analýzy a následného posúdenia významnosti identifikovaných rizík. (33)

Analýza rizík zahŕňa metodické využívanie dostupných údajov a informácií s cieľom kvantifikovať úroveň rizika a identifikovať príčiny jeho vzniku a zdroje. (33)

Vyhodnotenie rizika je činnosť, pri ktorej sa výsledky analýzy rizík porovnávajú s vopred stanovenými kritériami na určenie ich relatívneho významu pre organizáciu. (33)

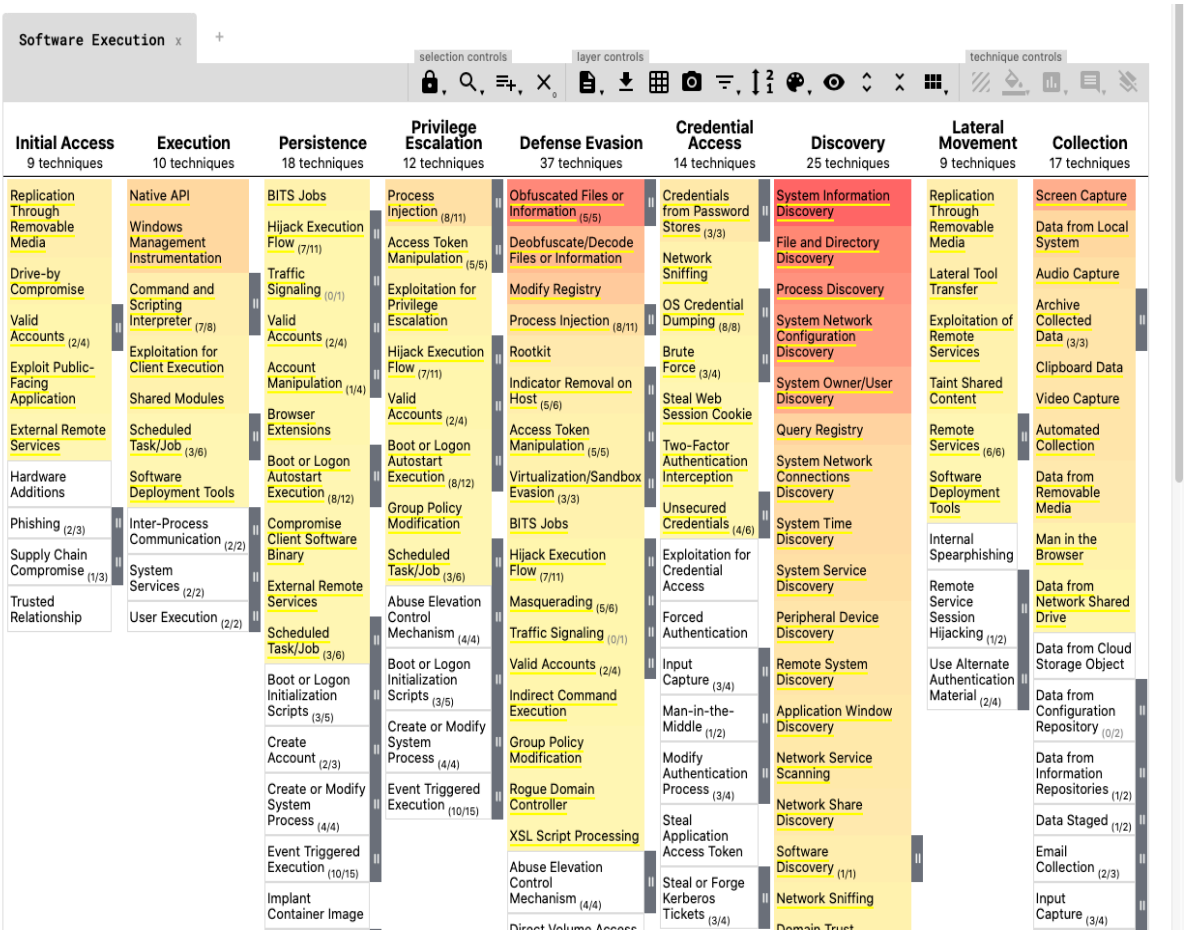
Zvládanie rizík sa týka procesu výberu vhodných opatrení a ich implementácie, ktorých účelom je redukovať úroveň rizika na akceptovateľnú hranicu alebo úplne eliminovať jeho potenciálny dopad. (33)

Akceptácia rizika predstavuje manažérske rozhodnutie o vedomom prijatí konkrétneho rizika bez vykonania ďalších opatrení na jeho minimalizáciu či elimináciu. (33)

1.3.2.1.1 Doporučený postup

1) Identifikácia aktív.
2) Zoskupovanie aktív (nástroje mapovanie siete a skenovanie zraniteľnosti, IDS s integráciou na CMDB, nástroje na zobrazenie toku dát).
3) Hodnotenie aktív (prioritizácia).
4) Využitie CTI technik k identifikácii relevantných skupín útočníkov.
5) Využitie MITRE ATT&CK.
    a. Identifikácia relevantnej domény.
    b. Identifikácia relevantných TTPs pri zohľadnení daných technológii v organizácii.
    c. Identifikácia relevantných skupín útočníkov a ich postupov.
6) Využitie nástroja ATT&CK Navigator k vizualizácii.
7) Vo vizualizácii sa zohľadní TTPs, ktoré sú pokryté bezpečnostnými nástrojmi a rovnako sa zohľadnia dáta z bezpečnostných nástrojov.

8) Prípadne je možné dáta pomocou dátových analytických nástrojov doplniť o vstupy z CVE, CWE a CAPEC.
9) Hodnotenie hrozieb a zraniteľností.
10) Stanovenie výšky rizík.
11) Realizácia opatrení k ošetreniu rizík.
12) Preskúmanie účinnosti opatrení a ošetrenie zbytkových rizík. (34)



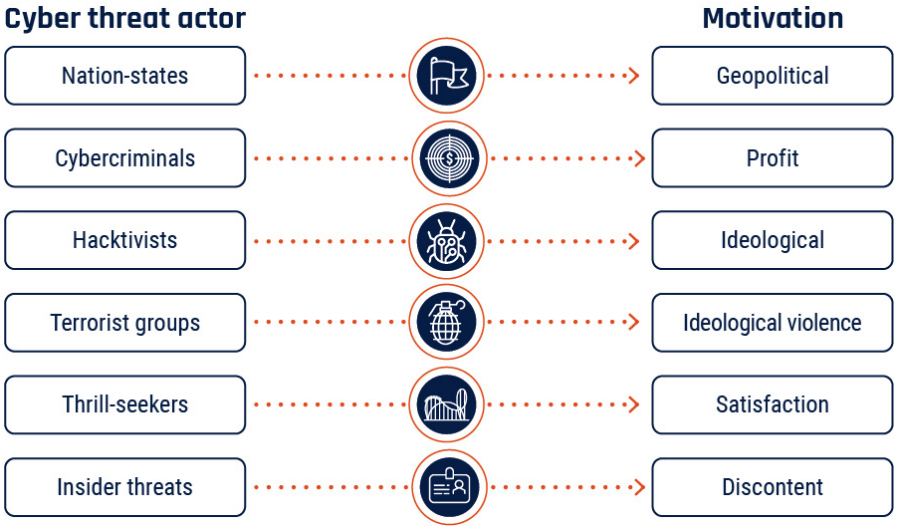
Obrázok č. 37 Prehľad kybernetických techník útočníkov podľa fáz kybernetického útoku podľa MITRE ATT&CK (Zdroj: attack.mitre.org/resources/attack-data-and-tools/)

1.3.3 Kybernetická hrozba, udalosť a incident

Kybernetická hrozba predstavuje potenciálnu príčinu nežiaduceho incidentu s možným následkom poškodenia systému alebo organizácie. Definuje sa ako čokoľvek schopné narušiť riadny stav a zasiahnuť do práv iných subjektov, pričom miera hrozby je daná veľkosťou možnej škody a pravdepodobnosťou jej uplatnenia. (31) (32)

Kybernetické hrozby sa členia podľa:

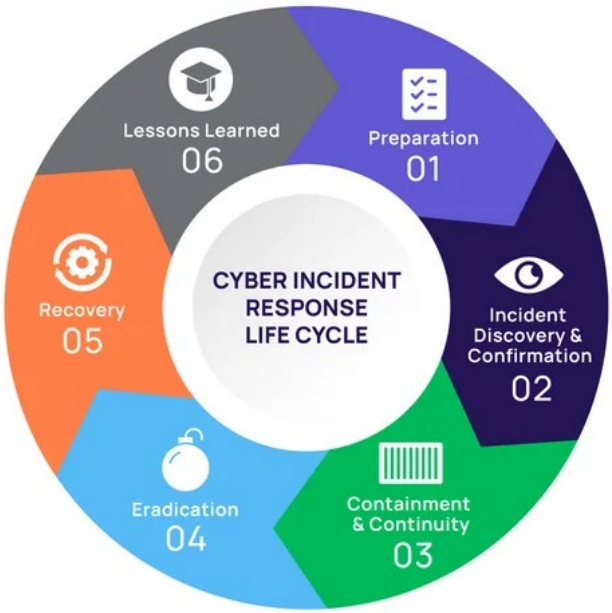
- **zdroja** (človekom úmyselne, z nedbalosti, technické chyby, vyššia moc), zdroja pôsobenia (vnútorné, vonkajšie)
- **cieľa** (útok na triádu CIA – dôvernosť, integritu, dostupnosť; útok na prvky kybernetickej bezpečnosti – ľudia, technológie, procesy)
- **motivácie** (finančný prospech, konkurenčná prevaha, atď.)
- **typu** (malware, phishing, DoS/DDoS útoky a iné). (31)



Obrázok č. 38 Klasifikácia aktérov kybernetických hrozieb podľa typu a zodpovedajúcej motivácie ich činnosti (Zdroj: cyber.gc.ca/en/guidance/introduction-cyber-threat-environment)

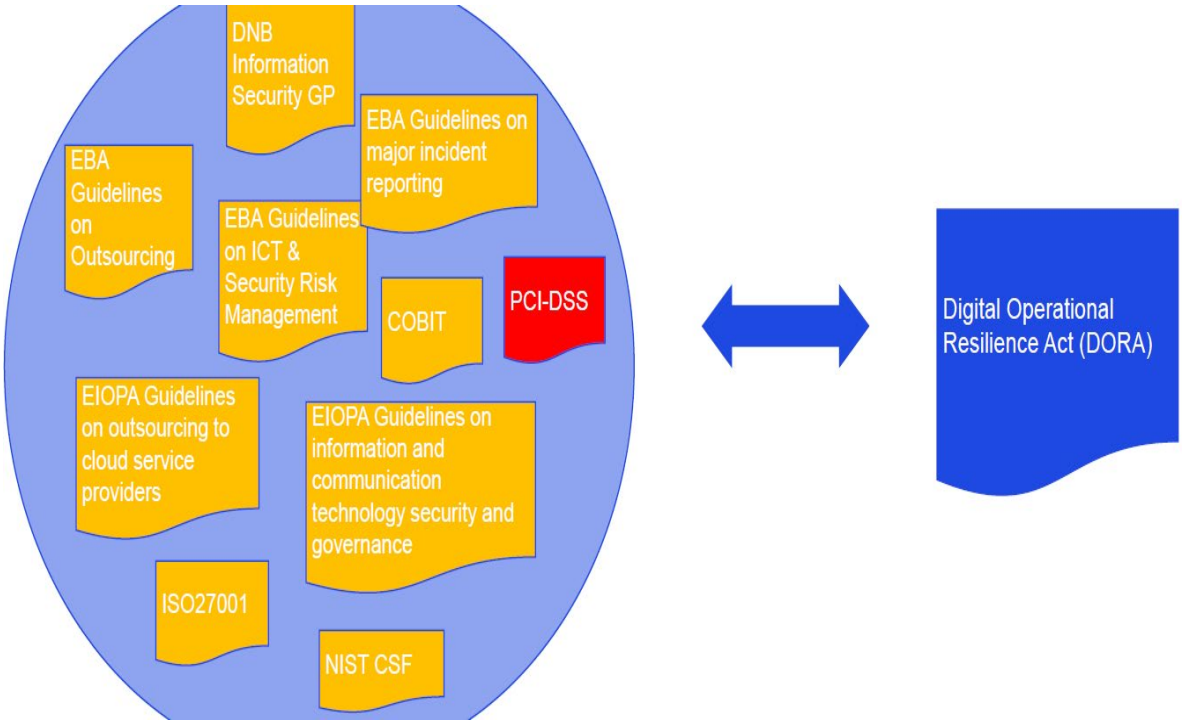
Kybernetická bezpečnostná udalosť je identifikovateľný stav systému, služby alebo siete indikujúci možné porušenie bezpečnostnej politiky alebo zlyhanie bezpečnostných opatrení. Predstavuje hrozbu bez reálneho negatívneho následku, avšak so schopnosťou narušiť bezpečnosť informácií v rámci informačných systémov. (31) (35)

Kybernetický bezpečnostný incident je narušenie alebo bezprostredná hrozba porušenia bezpečnostných politík, zásad alebo štandardných bezpečnostných pravidiel prevádzky informačných a komunikačných technológií. Ide o nežiaducu udalosť s vysokou pravdepodobnosťou kompromitácie činnosti organizácie a ohrozenia bezpečnosti informácií, vyplývajúcu z kybernetickej bezpečnostnej udalosti a majúcu negatívny dopad na informačné alebo komunikačné systémy. (31) (35)



Obrázok č. 39 Životný cyklus reakcie na kybernetický incident (Zdroj: delinea.com/blog/incident-response-lifecycle)

1.4 Metodiky, štandardy a rámce využívané pri implementácii kybernetickej bezpečnosti



Obrázok č. 40 Prepojenie DORA s existujúcimi bezpečnostnými rámcami a štandardmi (Zdroj: pvib.nl/cms/public/files/2024-07/presentatie-ronald-heil-en-ali-alam-kpmg.pdf)

1.4.1 Regulačné a implementačné technické štandardy RTS/ITS

Keďže samotné nariadenie DORA neobsahuje všetky špecifické detaily a technické požiadavky, poveruje Európske orgány dohľadu (ESAs) vypracovaním záväzných regulačných technických štandardov (**RTS**) a implementačných technických štandardov (**ITS**). Tieto technické štandardy sú kľúčové pre zabezpečenie jednotného uplatňovania a implementácie nariadenia DORA v celom finančnom sektore EÚ. (36) (37) (38)

Účelom regulačných technických štandardov (RTS) je ďalej špecifikovať regulačné požiadavky stanovené v samotnom nariadení DORA. RTS definujú technické kritériá, ktoré musia finančné subjekty spĺňať, a poskytujú presné inštrukcie o tom, ako dodržiavať všeobecné legislatívne požiadavky. (36)

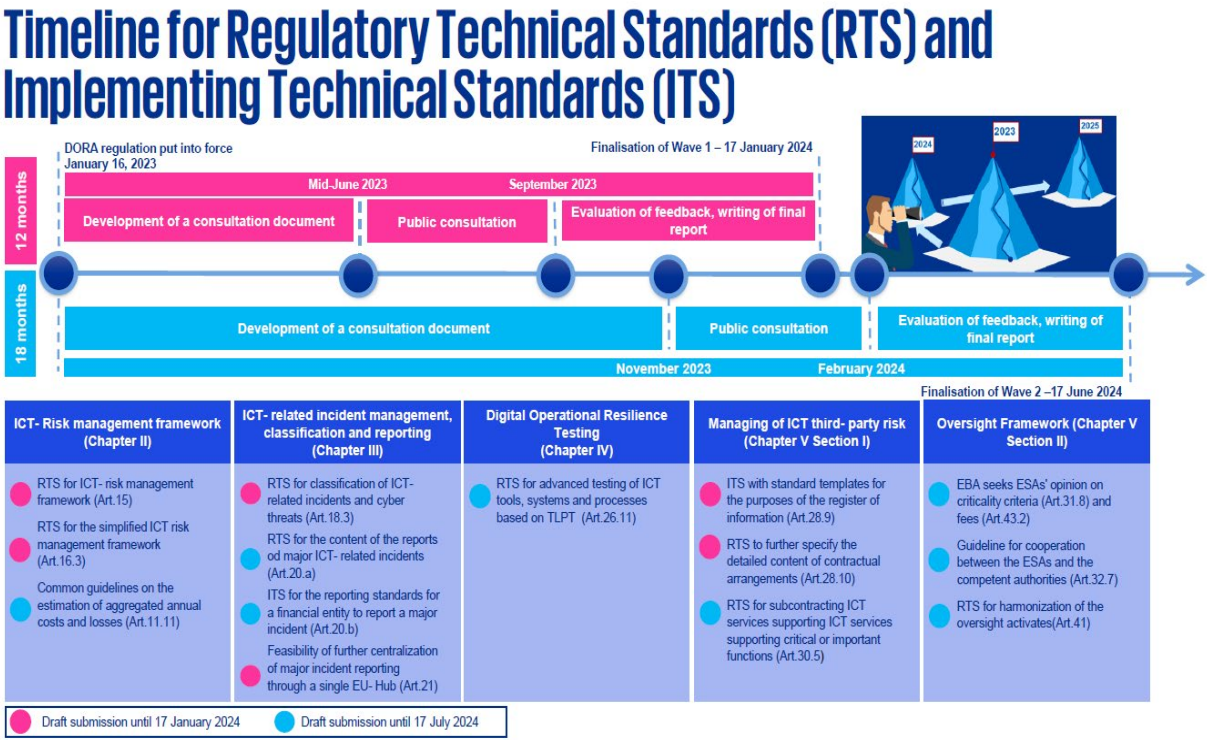
Na druhej strane, **implementačné technické štandardy (ITS)** slúžia na zabezpečenie jednotného uplatňovania právnych predpisov EÚ tým, že transformujú široké regulačné požiadavky na špecifické a vykonateľné usmernenia pre finančné subjekty a príslušné orgány. ITS obsahujú podrobné **pokyny na praktickú implementáciu, opisujú metódy výpočtu, formáty nahlasovania, prevádzkové postupy** a ďalšie technické detaily nevyhnutné pre súlad s predpismi. Stanovujú štandardné **formuláre, šablóny a postupy**. Sú teda **doplnkom k RTS**, špecifikujú podrobné implementačné pokyny a potrebné procesy na splnenie požiadaviek RTS. (36) (39)

	DORA policy work	Article	Public consultation	Finalise
	Call for advice on criticality criteria and fees	31.8 | 43.2	26 May - 23 June 23	30 Sept 2023
FIRST BATCH	RTS on ICT risk management framework	15		
	RTS on simplified ICT risk management framework	16		
	RTS on criteria for the classification of ICT-related incidents	18.3	19 June - 11 Sept 23	17 Jan 2024
	ITS to establish the templates for the Register of information	28.9		
	RTS to specify the policy on ICT services performed by 3rd party	28.1		
SECOND BATCH	RTS on specifying the reporting of major ICT-related incidents	20.a		
	ITS to establish the reporting details for major ICT-related incidents	20.b		
	Guidelines on the estimation of aggregated costs/losses caused by major ICTrelated incidents	11.11		
	RTS to specify threat led penetration testing aspects	26.11	Nov/Dec 23 - TBC	17 July 2024
	RTS to specify elements when sub-contracting critical or important functions	30.5		
	GL on cooperation between ESAs and CAs regarding the structure of the oversight	32.7		
	RTS to specify information on oversight conduct	41		
	Feasibility report on single EU Hub for major ICT-related events	21	TBC	17 January 2025

Obrázok č. 41 Časový harmonogram finalizácie RTS a ITS dokumentov podľa regulácie DORA (Zdroj: č.24)

Za vypracovanie RTS a ITS v rámci nariadenia DORA sú zodpovedné **Európske orgány dohľadu (ESAs)**, ktoré tvoria Európsky orgán pre bankovníctvo (**EBA**), Európsky orgán pre cenné papiere a trhy (**ESMA**) a Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov (**EIOPA**). (37) (40)

ESAs spoločne vyvíjajú tieto technické štandardy a po konzultácii s Európskou agentúrou pre kybernetickú bezpečnosť (ENISA) ich predkladajú Európskej komisii na prijatie vo forme delegovaných nariadení. Tieto delegované nariadenia sú potom priamo záväzné pre širokú škálu finančných subjektov v EÚ. (37) (40)



Obrázok č. 42 Časová os vývoja a finalizácie RTS a ITS štandardov podľa kapitol DORA (Zdroj: assets.kpmg.com/content/dam/kpmg/be/pdf/2023/DORA-webinar-SecOps-23-11.pdf)

Technické štandardy RTS a ITS pokrývajú rôzne kľúčové oblasti nariadenia DORA. Medzi tieto oblasti patrí napríklad stanovenie podrobných pravidiel pre **rámec riadenia rizík IKT**, vrátane bezpečnostných politík, postupov a nástrojov. Ďalšou dôležitou oblasťou je **klasifikácia a nahlasovanie závažných incidentov súvisiacich s IKT a významných kybernetických hrozieb**, kde RTS špecifikujú kritériá klasifikácie a ITS stanovujú štandardizované formuláre a postupy pre nahlasovanie. (40) (41) (42)

Okrem toho sa tieto štandardy zameriavajú na **riadenie rizík tretích strán v oblasti IKT**, vrátane vedenia **registra informácií o zmluvných dohodách s poskytovateľmi IKT služieb** a stanovenia politík pre tieto zmluvné vzťahy. Niektoré RTS sa venujú aj **testovaniu digitálnej prevádzkovej odolnosti**, vrátane požiadaviek na testovanie TLTP. (41) (43)

1.4.2 NIST Cybersecurity Framework

NIST Cybersecurity Framework (CSF) predstavuje rámec pozostávajúci z usmernení, štandardov a najlepších postupov, ktorý organizáciám pomáha lepšie porozumieť, riadiť a znižovať ich kybernetické riziká a chrániť ich siete a dáta. Bol vytvorený **Národným inštitútom pre štandardy a technológie (NIST)**, ktorý je súčasťou Ministerstva obchodu USA. (44) (45) (46)

Jeho vznik iniciovalo **výkonné nariadenie prezidenta Baracka Obamu v roku 2013**, ktoré požadovalo vytvorenie základného rámca na riešenie kybernetických rizík pre kritickú infraštruktúru. Následne bol jeho rozsah podporený a rozšírený **Zákonom o posilnení kybernetickej bezpečnosti z roku 2014**. (44) (45) (46)

NIST CSF je postavený na **šiestich základných funkciách**: **Govern (Riadiť)**, **Identify (Identifikovať)**, **Protect (Chrániť)**, **Detect (Detekovať)**, **Respond (Reagovať)** a **Recover (Obnoviť)**. Pôvodná verzia 1.1 obsahovala päť funkcií (Identify, Protect, Detect, Respond, Recover), pričom verzia 2.0 pridala funkciu Govern, čím zdôraznila význam **kybernetickej bezpečnosti riadenia** a **riadenia rizík dodávateľského reťazca**. (47)

Obrázok č. 43 Základné domény rámca kybernetickej bezpečnosti podľa NIST (Zdroj: orsys-lemag.com/en/glossary-2/nist-cybersecurity-framework-nist-csf/)

Každá z týchto funkcií obsahuje súbor kategórií a subkategórií, ktoré definujú špecifické kybernetické bezpečnostné výsledky/výstupy, ktorých dosiahnutie by organizácie mali zvážiť. Rámec nepredpisuje konkrétne technické riešenia, ale poskytuje **flexibilnú štruktúru** pre organizácie rôznych veľkostí, sektorov a úrovní zrelosti, aby si mohli prispôsobiť kybernetickú bezpečnosť svojim špecifickým potrebám a rizikám. (44)

NIST CSF bol pôvodne zameraný na zlepšenie kybernetickej bezpečnosti kritickej infraštruktúry, ale jeho **priemyselne neutrálny charakter** umožňuje jeho aplikáciu v akomkoľvek type organizácie. Využíva sa na **identifikáciu a stanovenie priorít** pre kritickú infraštruktúru a na **rozvoj stratégie riadenia rizík** pre tieto aktíva. (44) (46)

Rámec pomáha organizáciám **určiť aktuálny stav ich kybernetickej bezpečnosti** v porovnaní s cieľovým stavom, identifikovať **medzery a zraniteľnosti** a implementovať **akčný plán** na ich odstránenie. Dôraz sa kladie na **kontinuálny a cyklický charakter** týchto krokov. (44) (46)

Finančný sektor vyvinul špecifický profil založený na NIST CSF, známy ako **CRI Profile (Cyber Risk Institute Profile)**. Tento profil rozširuje rámec NIST CSF o dodatočné funkcie, kontrolné princípy a regulačné odkazy špecifické pre finančný sektor, pričom zdôrazňuje **riadenie kybernetickej bezpečnosti** a **riadenie rizík dodávateľského reťazca**. CRI Profile slúži ako nástroj na **sebahodnotenie**, **komunikáciu rizík** a **zosúladenie s regulačnými požiadavkami** vo finančnom sektore. (47) (48)

Table 1. CSF 2.0 Core Function and Category names and identifiers

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Obrázok č. 44 Kategórie a identifikátory funkcií rámca NIST CSF 2.0 (Zdroj: tevora.com/resource/exploring-the-enhanced-nist-cybersecurity-framework-20-empowering-organizations-to-strengthen-cyber-defenses/)

Prehľad kľúčových **implementačných štandardov** k NIST CSF:

- **NIST SP 800-53 Rev. 5** – Security and Privacy Controls for Information Systems and Organizations
- **NIST SP 800-37 Rev. 2** – Risk Management Framework for Information Systems and Organizations
- **NIST SP 800-30 Rev. 1** – Guide for Conducting Risk Assessments
- **NIST SP 800-39** – Managing Information Security Risk: Organization, Mission, and Information System View
- **NIST SP 800-61 Rev. 2** – Computer Security Incident Handling Guide
- **NIST SP 800-115** – Technical Guide to Information Security Testing and Assessment
- **NIST SP 800-84** – Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities (49)

1.4.3 ISO / IEC 27001

Norma **ISO/IEC 27001** predstavuje medzinárodný štandard zameraný na **informačnú bezpečnosť**, **kybernetickú bezpečnosť** a ochranu súkromia. Bola publikovaná Medzinárodnou organizáciou pre normalizáciu (ISO) v partnerstve s Medzinárodnou elektrotechnickou komisiou (IEC), ktoré sú poprednými medzinárodnými organizáciami vyvíjajúcimi medzinárodné štandardy. (51)

Norma ISO/IEC 27001 je kľúčovou súčasťou série noriem **ISO/IEC 27000**, ktorá sa zaoberá riadením informačnej bezpečnosti. Predstavuje najdôležitejšiu časť tejto skupiny noriem, pretože opisuje, ako riadiť všetky aspekty bezpečnosti. Jej úplný názov „ISO/IEC 27001 – Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia — Systémy riadenia informačnej bezpečnosti — Požiadavky“ podčiarkuje jej komplexný záber. (51)

Účelom rámca ISO/IEC 27001 je poskytnúť súbor požiadaviek na definovanie, implementáciu, prevádzkovanie a zlepšovanie **systému riadenia informačnej bezpečnosti (ISMS)**. Tento systém slúži na systematickú a nákladovo efektívnu ochranu informácií organizácie bez ohľadu na jej veľkosť či odvetvie. (51)

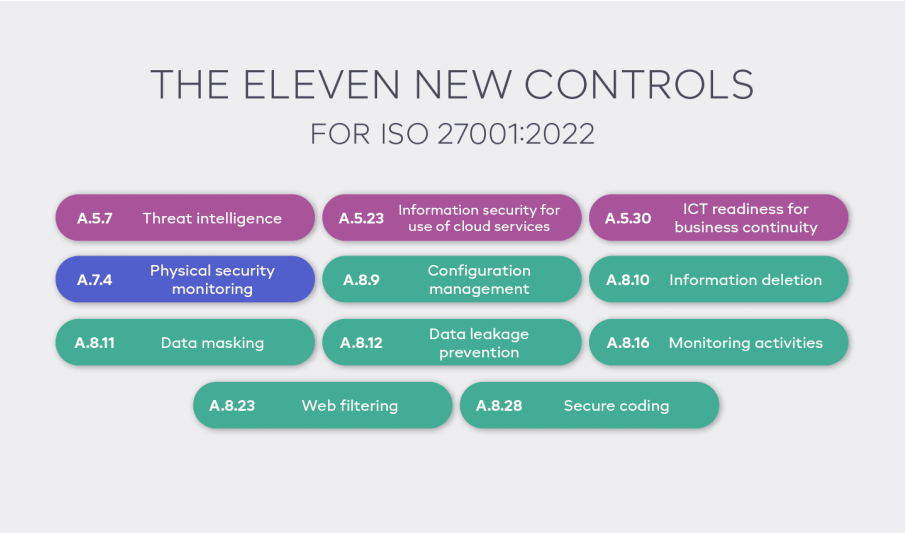
Obrázok č. 45 Oblasti pôsobnosti normy ISO 27001 (Zdroj: safetica.com/cs/zdroje/blogy/iso-iec-27001-rozsah-platnosti-ucel-a-zpusoby-plneni-pozadavku)

Základným cieľom ISMS podľa definície ISO/IEC 27001 je ochrana troch aspektov informácií: **dôvernosti** (prístup k informáciám majú len oprávnené osoby), **integrity** (informácie môžu meniť len oprávnené osoby) a **dostupnosti** (informácie musia byť prístupné oprávneným osobám, kedykoľvek sú potrebné). (52)

Základným princípom fungovania normy je **proces riadenia rizík**, identifikácia potenciálnych hrozieb a zraniteľností informačných aktív a následné zavedenie bezpečnostných opatrení (kontrol) na prevenciu, zmiernenie alebo iné ošetrenie týchto rizík (riziková mitigácia alebo ošetrenie rizík). Organizácia je povinná identifikovať a implementovať vhodné kontroly, ktoré sú zdokumentované v **Prehlásení o aplikovateľnosti.** (51) (53)

Norma ISO/IEC 27001 obsahuje rôznorodé **požiadavky**, ktoré možno všeobecne kategorizovať ako požiadavky na:

- **Stanovenie kontextu organizácie** a identifikáciu zainteresovaných strán a ich požiadaviek.
- **Preukázanie záväzku vedenia** k informačnej bezpečnosti, vrátane stanovenia politiky informačnej bezpečnosti a prideľovania rolí a zodpovedností.
- **Plánovanie ISMS**, ktoré zahŕňa posudzovanie rizík a príležitostí, stanovenie bezpečnostných cieľov a plánov na ich dosiahnutie.
- **Podporné procesy**, ktoré sa týkajú zabezpečenia potrebných zdrojov, kompetencií zamestnancov, povedomia o bezpečnosti a efektívnej komunikácie.
- **Operačné procesy** implementácie bezpečnostných opatrení a riadenia rizík v rámci každodenných činností organizácie.
- **Hodnotenie výkonnosti ISMS** prostredníctvom monitorovania, merania, analýzy, interných auditov a preskúmania manažmentom.
- **Neustále zlepšovanie ISMS** na základe výsledkov hodnotenia výkonnosti a reakcií na nezhody. (51)



Obrázok č. 46 Nové opatrenia v norme ISO/IEC 27001:2022 (Zdroj: č.50)

Prehľad vybraných kľúčových kontrolných opatrení ISO 27001:2022:

- **ISO 27001:2022 Annex A 5.1** – Information Security Policies
- **ISO 27001:2022 Annex A 5.2** – Information Security Roles and Responsibilities
- **ISO 27001:2022 Annex A 5.7** – Threat Intelligence
- **ISO 27001:2022 Annex A 5.9** – Inventory of Information and Other Associated Assets
- **ISO 27001:2022 Annex A 5.19** – Information Security in Supplier Relationships
- **ISO 27001:2022 Annex A 5.20** – Addressing Information Security Within Supplier Agreements
- **ISO 27001:2022 Annex A 5.21** – Managing Information Security in the ICT Supply Chain
- **ISO 27001:2022 Annex A 5.24** – Information Security Incident Management Planning and Preparation
- **ISO 27001:2022 Annex A 5.26** – Response to Information Security Incidents
- **ISO 27001:2022 Annex A 5.30** – ICT Readiness for Business Continuity
- **ISO 27001:2022 Annex A 8.8** – Management of Technical Vulnerabilities
- **ISO 27001:2022 Annex A 8.13** – Information Backup
- **ISO 27001:2022 Annex A 8.15** – Logging
- **ISO 27001:2022 Annex A 8.16** – Monitoring Activities (50)

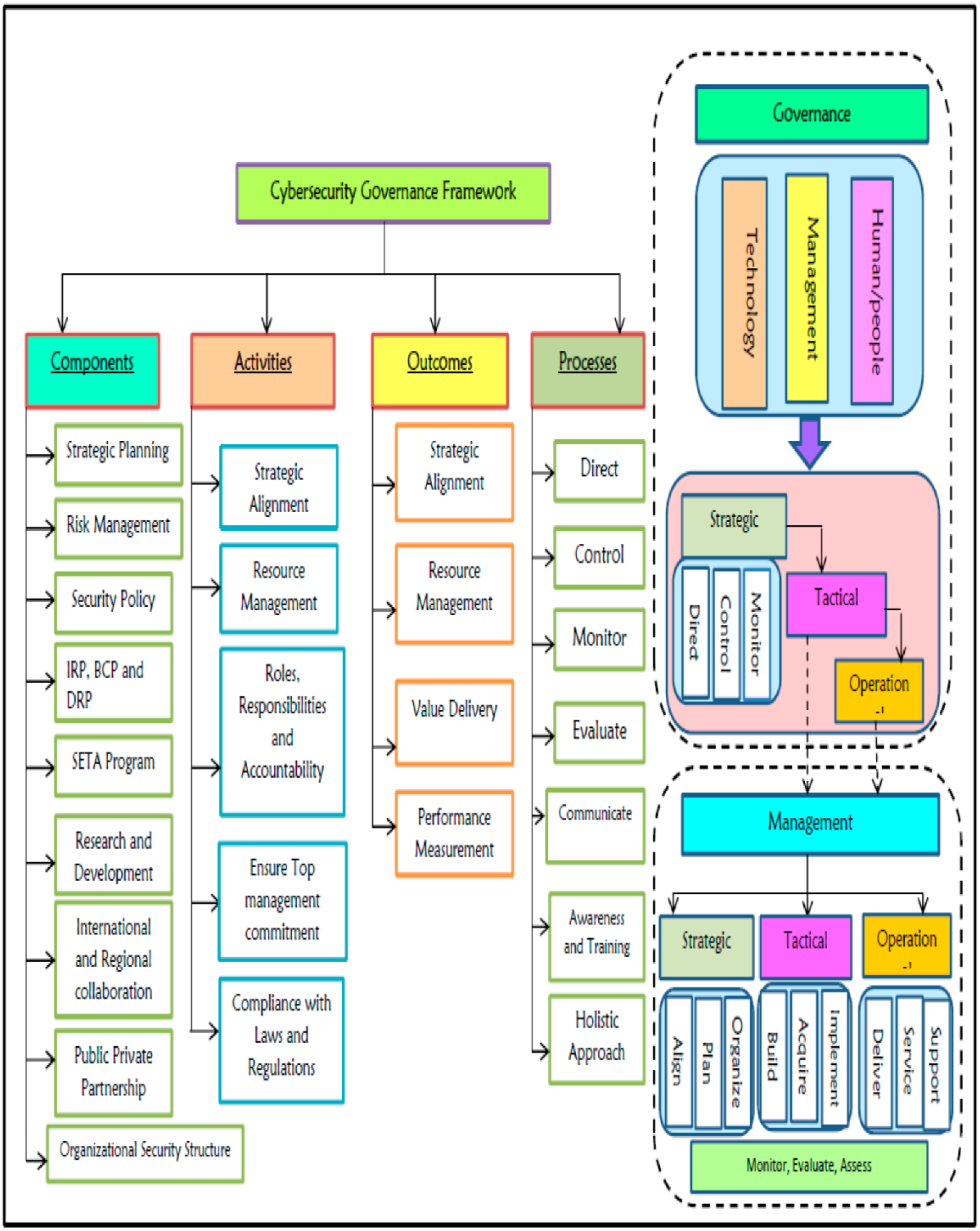
1.5 Regulačno-technické východiská implementačných aktivít podľa RTS/ITS

1.5.1 Rámec riadenia IKT rizík a organizačná úroveň zabezpečenia

1. **Zriadiť**, **dokumentovať** a **vykonávať rámec riadenia IKT rizika**.
2. **Zohľadniť** pri vypracúvaní a vykonávaní politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT **veľkosť** a **celkový rizikový profil** finančného subjektu, ako aj **povahu**, **rozsah** a **zložitosť** jeho služieb, činností a operácií.
3. **Zosúladiť politiky v oblasti bezpečnosti IKT** s **cieľmi informačnej bezpečnosti** finančného subjektu zahrnutými do **stratégie digitálnej prevádzkovej odolnosti**.
4. **Identifikovať** úlohy a **zodpovednosti** za **vypracovanie**, **vykonávanie** a **udržiavanie** politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT.
5. **Preskúmavať rámec riadenia IKT rizika** a predkladať správu o tomto preskúmaní **príslušnému orgánu** v **elektronickom formáte s možnosťou vyhľadávania**.
6. **Zahrnúť** do **správy o preskúmaní rámca riadenia IKT rizika identifikáciu finančného subjektu**, **opis kontextu správy** (povaha, rozsah, zložitosť služieb, kritické funkcie, stratégie, závislosti na IKT), **zhrnutie zistení**, **opis významných zmien**, **informácie o úrovni testovania** a prípadne **výsledky vnútorných auditov**, **posúdení súladu** a **testovania digitálnej prevádzkovej odolnosti**.
7. **Stanoviť** v rámci **zjednodušeného rámca jasné zodpovednosti**, **ciele informačnej bezpečnosti** a **požiadavky na IKT**.
8. **Schvaľovať**, **dohliadať** a **pravidelne preskúmavať klasifikáciu informačných aktív**, **zoznam identifikovaných hlavných rizík** a **analýzu vplyvu na podnikanie** a súvisiace **politiky**.
9. **Schvaľovať**, **dohliadať** a **pravidelne preskúmavať plány na zabezpečenie kontinuity činností** a **opatrenia reakcie a obnovy**.

10. **Prideliť** a **preskúmavať** aspoň raz ročne **rozpočet** potrebný na splnenie potrieb v oblasti **digitálnej prevádzkovej odolnosti**.
11. **Stanoviť** a **vykonávať politiky** a **opatrenia** na **identifikáciu**, **posudzovanie** a **riadenie IKT rizika**.
12. **Identifikovať** a **vykonávať postupy**, **IKT protokoly** a **nástroje** potrebné na **ochranu všetkých informačných aktív** a **IKT aktív**.
13. **Zabezpečiť**, aby si zamestnanci udržiavali **dostatočné znalosti a zručnosti** potrebné na pochopenie a posúdenie **IKT rizika**.
14. **Vypracovať**, **dokumentovať** a **vykonávať politiku v oblasti informačnej bezpečnosti** stanovujúcu **zásady a pravidlá na vysokej úrovni** na ochranu **dôvernosti**, **integrity**, **dostupnosti** a **pravosti údajov a služieb**.
15. **Stanoviť** a **vykonávať** na základe **politiky informačnej bezpečnosti bezpečnostné opatrenia v oblasti IKT** na **zmiernenie miery vystavenia IKT riziku**, vrátane opatrení vykonávaných **externými poskytovateľmi IKT služieb**.
16. **Identifikovať**, **klasifikovať** a **dokumentovať** všetky **kritické** alebo **dôležité funkcie**, **informačné aktíva** a **IKT aktíva**, ktoré ich podporujú, a ich **vzájomné závislosti** a podľa potreby ich **preskúmavať**.
17. **Vykonávať** a **dokumentovať** pravidelné **posudzovanie IKT rizika** zodpovedajúce **profilu IKT rizika** finančného subjektu.
18. **Nepretržite monitorovať hrozby** a **zraniteľné miesta** dôležité pre **kritické** alebo **dôležité funkcie**, **informačné aktíva** a **IKT aktíva** a **pravidelne preskúmavať rizikové scenáre**.
19. **Stanoviť varovné prahové hodnoty** a **kritériá** na spustenie a iniciáciu **procesov reakcie na incidenty súvisiace s IKT**.
20. **Zabezpečiť včasné overenie a nápravu kritických zistení auditu IKT**.
21. **Pravidelne preskúmavať** politiky v oblasti bezpečnosti IKT
22. **Zohľadňovať** závažné zmeny týkajúce sa finančného subjektu (zmeny činností, kybernetické hrozby, právne povinnosti) pri preskúmavaní politík v oblasti bezpečnosti IKT.

23. **Vypracovať**, **zdokumentovať** a **vykonávať postupy riadenia IKT rizika** obsahujúce ustanovenia o **identifikácii aktív**, **ochranných opatreniach**, **detekcii**, **reakcii a obnove**, **poučení sa a vývoji**, **komunikácii**, **monitorovaní zmien hrozieb a zraniteľností**, **monitorovaní IKT rizika**, a **postupe na zohľadnenie zmien obchodnej stratégie**.
24. **Stanoviť** v **politike riadenia IKT aktív monitorovanie** a **riadenie životného cyklu** identifikovaných a klasifikovaných **IKT aktív**.
25. Pre finančné subjekty iné ako mikropodniky, **viesť záznamy** o informáciách potrebných na **osobitné posudzovanie IKT rizika všetkých pôvodných IKT systémov**.
26. **Vypracovať**, **zdokumentovať** a **vykonávať postup riadenia IKT aktív**.
27. **Určiť interné zodpovednosti** za **schvaľovanie**, **riadenie**, **kontrolu** a **dokumentáciu zmluvných dojednaní** o využívaní **IKT služieb podporujúcich kritické alebo dôležité funkcie** poskytovaných **externými poskytovateľmi IKT služieb**.
28. **Zabezpečiť**, aby **politika** týkajúca sa **zmluvných dojednaní** zahŕňala všetky kroky každej hlavnej fázy **životného cyklu zmluvných dojednaní** s **externými poskytovateľmi**.
29. **Špecifikovať plánovanie zmluvných dojednaní** vrátane **posúdenia rizík**, **náležitej starostlivosti** a **procesu schvaľovania nových alebo závažných zmien** týchto dojednaní.
30. **Stanoviť vhodný a primeraný postup výberu a posudzovania vhodnosti potenciálnych externých poskytovateľov IKT služieb** s ohľadom na demonštratívny zoznam prvkov (dobré meno, zdroje, bezpečnosť, organizácia, kontroly). (54)

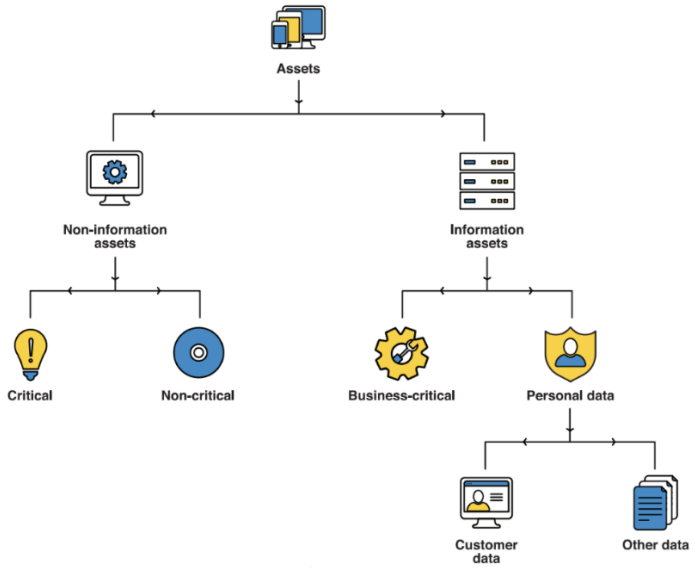


Obrázok č. 47 Rámec riadenia kybernetickej bezpečnosti a jeho komponenty, procesy a výstupy (Zdroj: mdpi.com/2624-800X/3/3/17)

1.5.2 Identifikácia a evidencia informačných a IKT aktív

1. **Identifikovať** všetky **kritické alebo dôležité funkcie** finančného subjektu.
2. **Identifikovať IKT služby alebo sieť a informačné systémy**, ktoré podporujú **kritické alebo dôležité funkcie** finančného subjektu.
3. **Identifikovať finančné služby**, ktoré poskytuje finančný subjekt a ktoré si vyžadujú povolenie, registráciu alebo ktoré podliehajú dohľadu príslušných orgánov.
4. **Klasifikovať** všetky **kritické alebo dôležité funkcie**, **informačné aktíva** a **IKT aktíva**, ktoré ich podporujú.
5. **Dokumentovať klasifikáciu** všetkých **kritických alebo dôležitých funkcií**, **informačných aktív** a **IKT aktív**.
6. **Preskúmať identifikáciu a klasifikáciu kritických alebo dôležitých funkcií, informačných aktív a IKT aktív** podľa potreby.
7. **Vytvoriť** a **udržiavať register** všetkých **IKT aktív**.
8. **Zaznamenať** pre každé **IKT aktívum jedinečný identifikátor**.
9. **Zaznamenať informácie o umiestnení** (**fyzickom alebo logickom**) všetkých **IKT aktív**.
10. **Zaznamenať klasifikáciu** všetkých **IKT aktív**.
11. **Zaznamenať** v prípade **IKT aktív** podporujúcich **kritické alebo dôležité funkcie** informácie o ich vlastníkovi.
12. **Zaznamenať** v prípade **IKT aktív** podporujúcich **kritické alebo dôležité funkcie** informácie o ich zmluvnom dojednaní s externým poskytovateľom IKT služieb, ak existuje.
13. **Zaznamenať závislosti** medzi **kritickými alebo dôležitými funkciami** a podporujúcimi **informačnými aktívami** alebo **IKT aktívami** v rámci posúdenia kritickosti.

14. **Zaznamenať** potenciálny vplyv straty **dôvernosti**, **integrity** a **dostupnosti informačných aktív** a **IKT aktív** na obchodné procesy a činnosti finančného subjektu v rámci posúdenia kritickosti.
15. **Viesť záznamy** o informáciách potrebných na vykonávanie osobitného posudzovania **IKT rizika** všetkých **pôvodných IKT systémov** (ak sa nevzťahuje zjednodušený rámec).
16. **Stanoviť** kritériá na vykonávanie posudzovania kritickosti **informačných aktív** a **IKT aktív** podporujúcich obchodné funkcie.
17. **Zohľadniť** pri posudzovaní kritickosti **IKT riziko** súvisiace s obchodnými funkciami a ich závislosťami od **informačných aktív** alebo **IKT aktív**.
18. **Zohľadniť** pri posudzovaní kritickosti potenciálny vplyv straty **dôvernosti**, **integrity** a **dostupnosti** takýchto **informačných aktív** a **IKT aktív** na obchodné procesy a činnosti finančného subjektu.
19. **Pravidelne vykonávať** a **dokumentovať** posudzovanie **IKT rizika**, ktoré zodpovedá profilu **IKT rizika** finančných subjektov so zjednodušeným rámcom.
20. **Nepretržite monitorovať** hrozby a zraniteľné miesta, ktoré sú dôležité pre **kritické alebo dôležité funkcie**, **informačné aktíva** a **IKT aktíva** finančných subjektov so zjednodušeným rámcom.
21. **Pravidelne preskúmavať** rizikové scenáre, ktoré majú vplyv na **kritické alebo dôležité funkcie** finančných subjektov so zjednodušeným rámcom. (54) (55)



Obrázok č. 48 Klasifikácia aktív v rámci informačnej bezpečnosti (Zdroj: manageengine.com/academy/asset-handling.html)

1.5.3 Hodnotenie rizík, klasifikácia funkcií a plánovanie zvládania rizík

1. **Vypracovať, zdokumentovať a vykonávať politiky a postupy riadenia IKT rizika**, ktoré obsahujú ustanovenia o **monitorovaní všetkých zmien panorámy hrozieb IKT rizika a kybernetických hrozieb**.
2. **Vypracovať, zdokumentovať a vykonávať politiky a postupy riadenia IKT rizika**, ktoré obsahujú ustanovenia o **monitorovaní vnútorných a vonkajších zraniteľných miest a hrozieb**.
3. **Vypracovať, zdokumentovať a vykonávať politiky a postupy riadenia IKT rizika**, ktoré obsahujú ustanovenia o **monitorovaní IKT rizika finančného subjektu**, ktoré umožňuje **rýchle odhalenie zmien**, ktoré by mohli ovplyvniť jeho profil IKT rizika.
4. **Vypracovať, zdokumentovať a vykonávať politiky a postupy riadenia IKT rizika**, ktoré obsahujú ustanovenia o postupe na zabezpečenie toho, aby sa **zohľadnili všetky zmeny obchodnej stratégie a stratégie digitálnej prevádzkovej odolnosti finančného subjektu**.
5. **Zohľadniť IKT riziko súvisiace s obchodnými funkciami a ich závislosti od informačných aktív alebo IKT aktív** pri posudzovaní kritickosti aktív.

6. **Nepretržite monitorovať hrozby a zraniteľné miesta**, ktoré sú dôležité pre **kritické alebo dôležité funkcie**, informačné aktíva a IKT aktíva finančných subjektov so zjednodušeným rámcom riadenia IKT rizika.
7. **Pravidelne vykonávať a zdokumentovať posudzovanie IKT rizika**, ktoré musí zodpovedať profilu IKT rizika finančných subjektov so zjednodušeným rámcom riadenia IKT rizika.
8. **Vypracovať, zdokumentovať a vykonávať postupy riadenia zraniteľnosti** v rámci politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT.
9. **Identifikovať a odstraňovať zraniteľné miesta** vo svojom IKT prostredí.
10. **Monitorovať zraniteľné miesta** v oblasti IKT využívaním spoľahlivých zdrojov a automatizovaných nástrojov.
11. **Uprednostniť zavedenie bezpečnostných záplat a iných zmierňujúcich opatrení** na riešenie identifikovaných zraniteľných miest.
12. **Zaznamenávať všetky odhalené zraniteľné miesta ovplyvňujúce IKT systémy** a **monitorovať ich riešenia**.
13. **Vykonávať automatizované skenovanie a posudzovanie zraniteľnosti IKT aktív** podporujúcich **kritické alebo dôležité funkcie** aspoň raz týždenne.
14. **Vypracovať, zdokumentovať a vykonávať postupy riadenia bezpečnostných záplat** v rámci politík, postupov, protokolov a nástrojov v oblasti bezpečnosti IKT.
15. **Identifikovať a vyhodnocovať dostupné softvérové a hardvérové bezpečnostné záplaty a aktualizácie** prostredníctvom používania **automatizovaných nástrojov** v čo najväčšej možnej miere.
16. **Stanoviť lehoty na inštaláciu softvérových a hardvérových bezpečnostných záplat a aktualizácií** a **eskalačné postupy**, ak tieto lehoty nemožno dodržať.
17. **Vypracovať politiku kontinuity činností v oblasti IKT**, pričom sa zohľadnia **základné zložky riadenia IKT rizika** vrátane **riadenia incidentov súvisiacich s IKT** a komunikačných stratégií, **procesu riadenia zmien IKT** a **riziká spojené s externými poskytovateľmi IKT služieb**.

18. **Vypracovať súbor scenárov**, ktoré by sa mali zohľadňovať pri vykonávaní **plánov reakcie a obnovy v oblasti IKT**, ako aj pri **testovaní plánov na zabezpečenie kontinuity činností v oblasti IKT**.

19. **Analyzovať relevantnosť a vierohodnosť každého scenára** pre plány kontinuity činností v oblasti IKT a plány reakcie a obnovy v oblasti IKT, ako aj potrebu vypracovať alternatívne scenáre.

20. **Testovať prepnutie medzi primárnou infraštruktúrou IKT a akoukoľvek redundantnou kapacitou, zálohami a redundantnými zariadeniami** s cieľom posúdiť ich účinnosť a zabezpečiť obnovenie normálneho fungovania primárnej infraštruktúry IKT v súlade s cieľmi obnovy.

21. **Pravidelne preskúmavať rizikové scenáre**, ktoré majú vplyv na **kritické alebo dôležité funkcie** finančných subjektov so zjednodušeným rámcom riadenia IKT rizika.

22. **Zohľadniť**, pri určení kritickosti zasiahnutých služieb, či incident **ovplyvňuje alebo ovplyvnil IKT služby alebo sieť a informačné systémy**, ktoré podporujú **kritické alebo dôležité funkcie** finančného subjektu.

23. **Stanoviť varovné prahové hodnoty a kritériá na spustenie a iniciáciu procesov reakcie na incidenty súvisiace s IKT** pre finančné subjekty so zjednodušeným rámcom riadenia IKT rizika.

24. **Vypracovať, zdokumentovať a vykonávať plány reakcie a obnovy v oblasti IKT**, pričom sa zohľadnia výsledky **analýzy vplyvu na činnosti (BIA)**.

25. **Zahrnúť do plánov reakcie a obnovy v oblasti IKT podmienky, ktoré vedú k ich aktivácii alebo deaktivácii**, a všetky výnimky pre takúto aktiváciu alebo deaktiváciu.

26. **Zahrnúť do plánov reakcie a obnovy v oblasti IKT opis opatrení**, ktoré sa majú prijať na zabezpečenie **dostupnosti, integrity, kontinuity a obnovy** aspoň **IKT systémov a služieb podporujúcich kritické alebo dôležité funkcie** finančného subjektu.

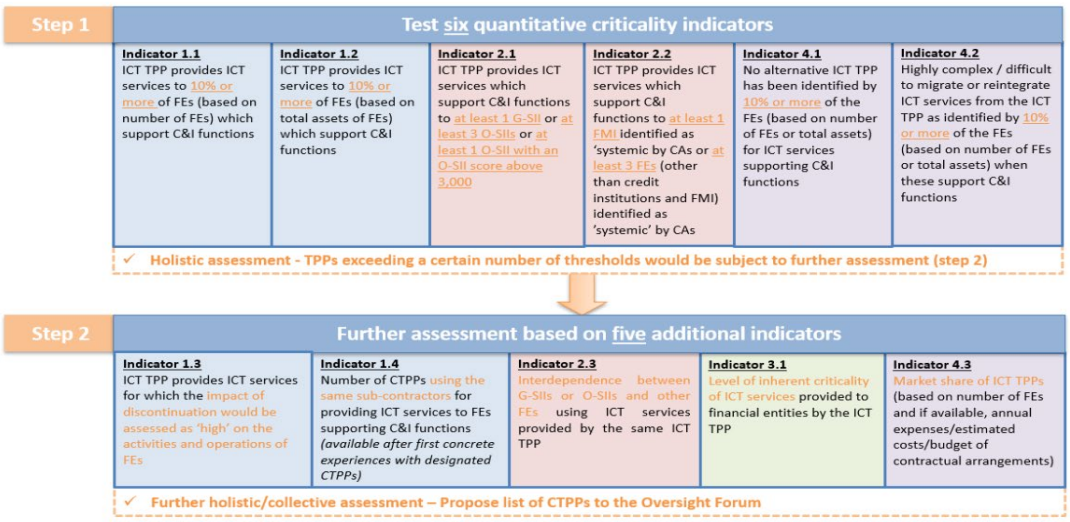
27. **Monitorovať a vyhodnocovať výsledky bezpečnostných testov** a bez zbytočného odkladu príslušným spôsobom **aktualizovať svoje bezpečnostné opatrenia** v prípade **IKT systémov podporujúcich kritické alebo dôležité funkcie** pre finančné subjekty so zjednodušeným rámcom riadenia IKT rizika.

28. **Vypracovať, zdokumentovať a vykonávať postup riadenia IKT zmien** s cieľom zabezpečiť, aby sa všetky **zmeny IKT systémov zaznamenávali, testovali, posudzovali, schválili, vykonávali a overovali kontrolovane a s primeranými zárukami na zachovanie digitálnej prevádzkovej odolnosti** finančného subjektu so zjednodušeným rámcom riadenia IKT rizika.

29. **Vypracovať plány kontinuity činnosti v oblasti IKT**, ktoré budú schválené riadiacim orgánom, zdokumentované, ľahko prístupné, s vyčlenenými dostatočnými zdrojmi a ktoré stanovia **plánované úrovne obnovy a časové rámce na obnovu funkcií a kľúčových závislostí**.

30. **Identifikovať podmienky**, ktoré môžu viesť k aktivácii plánov kontinuity činností v oblasti IKT, a opatrenia na zabezpečenie **dostupnosti, kontinuity a obnovy IKT aktív podporujúcich kritické alebo dôležité funkcie** pre finančné subjekty so zjednodušeným rámcom riadenia IKT rizika.

31. **Zdokumentovať výsledky testovania plánov kontinuity činností**, analyzovať a riešiť všetky zistené nedostatky a nahlásiť ich riadiacemu orgánu. (54)



Obrázok č. 49 Postup hodnotenia kritickosti externých poskytovateľov IKT služieb (Zdroj: itsecuritylocksmith.co.uk/critical-ict-third-party-providers/)

1.5.4 Riadenie rizík tretích strán a outsourcing IKT služieb

1. **Vypracovať**, **zdokumentovať** a **vykonávať politiku** týkajúcu sa zmluvných dojednaní o využívaní **IKT služieb** podporujúcich **kritické alebo dôležité funkcie**, ktoré poskytujú **externí poskytovatelia IKT služieb**.
2. **Zabezpečiť**, aby **politika** jasne stanovovala interné zodpovednosti za schvaľovanie, riadenie, kontrolu a dokumentáciu **zmluvných dojednaní**.
3. **Špecifikovať** v **politike** plánovanie **zmluvných dojednaní** vrátane posúdenia rizík, **náležitej starostlivosti** a procesu schvaľovania nových alebo závažných zmien týchto dojednaní.
4. **Stanoviť** v **politike** vhodný a primeraný postup výberu a posudzovania vhodnosti potenciálnych **externých poskytovateľov IKT služieb**.
5. **Zahrnúť** do **politiky** informácie o vykonávaní, monitorovaní a riadení **zmluvných dojednaní**, vrátane požiadaviek na **zmluvné doložky** o vzájomných záväzkoch.
6. **Bližšie určiť** v **politike stratégie ukončenia angažovanosti** a **postupy ukončenia zmluvných dojednaní**.
7. **Posúdiť**, či **externý poskytovateľ IKT služieb** využíva alebo má v úmysle využívať **subdodávateľov** pre **IKT služby** podporujúce **kritické alebo dôležité funkcie**.
8. **Posúdiť** v rámci **náležitej starostlivosti** existenciu opatrení na zmiernenie rizika a opatrení na zabezpečenie **kontinuity činností** u **externého poskytovateľa IKT služieb**.
9. **Vykonávať audity externých poskytovateľov IKT služieb**, a to aj v ich priestoroch, alebo zabezpečiť ich vykonávanie vymenovanými tretími stranami.
10. **Stanoviť** v **zmluvných dojednaniach** opatrenia a **kľúčové ukazovatele** pre priebežné **monitorovanie výkonnosti externých poskytovateľov** vrátane dodržiavania požiadaviek na dôvernosť, dostupnosť, integritu a pravosť údajov.
11. **Bližšie určiť** v **politike** opatrenia uplatňované v prípade nesplnenia **dohôd o úrovni poskytovaných služieb (SLA)**.

12. **Dokumentovať posúdenie výkonnosti externého poskytovateľa** a použiť jeho výsledky na aktualizáciu posúdenia rizika finančného subjektu.
13. **Viesť register informácií** v súvislosti so všetkými **zmluvnými dojednaniami** o využívaní **IKT služieb** poskytovaných **externými poskytovateľmi IKT**.
14. **Používať** v **registri informácií** štyri kľúče na prepájanie údajov: **referenčné číslo zmluvného dojednania**, identifikátor finančných subjektov a **externých poskytovateľov**, identifikátor funkcie a typ **IKT služieb**.
15. **Uvádzať** vo vzore **registra informácií** (B_02.02) podrobnosti o **IKT službách** zahrnutých do **zmluvného dojednania** a o podporovaných funkciách finančných subjektov.
16. **Zahrnúť** do **registra informácií** (B_05.01) podrobnosti o každom **externom poskytovateľovi IKT služieb**, vrátane identifikačných údajov a kontaktných informácií.
17. **Zahrnúť** do **registra informácií** informácie o **posudzovaní IKT služieb** poskytovaných **externými poskytovateľmi** podporujúcich **kritické alebo dôležité funkcie** (vzor B_07.01).
18. **Zabezpečiť** v prípade **zmluvných dojednaní** s **externými poskytovateľmi IKT služieb** ustanovenia o **práve na audit** finančného subjektu alebo vymenovanej tretej strany.
19. **Zabezpečiť** v **zmluvných dojednaniach** účinný **prístup k údajom** a do objektov **externého poskytovateľa**, ktoré súvisia s využívaním **IKT služieb** podporujúcich **kritické alebo dôležité funkcie**.
20. **Stanoviť** v **zmluvných dojednaniach opatrenia na prenosnosť IKT služieb** podporujúcich **kritické alebo dôležité funkcie** na iného **externého poskytovateľa**, a to aj v dôsledku technologických špecifík.
21. **Stanoviť** v **zmluvných dojednaniach** potenciálny vplyv narušení poskytovania **IKT služieb** podporujúcich **kritické alebo dôležité funkcie** na **kontinuitu činností** finančného subjektu.
22. **Zahrnúť** do **zmluvných dojednaní stratégie ukončenia** a súvisiace záväzky.

23. **Zabezpečiť**, aby **stratégie ukončenia** zohľadňovali potenciálne riziká, ktoré môžu vzniknúť pre **kontinuitu činností** finančného subjektu.

24. **Stanoviť** v **stratégiách ukončenia** plány na **prechod** na iného **externého poskytovateľa** alebo na návrat k internému poskytovaniu **IKT služieb**.

25. **Monitorovať subdodávateľské reťazce IKT služieb** poskytovaných **externými poskytovateľmi**.

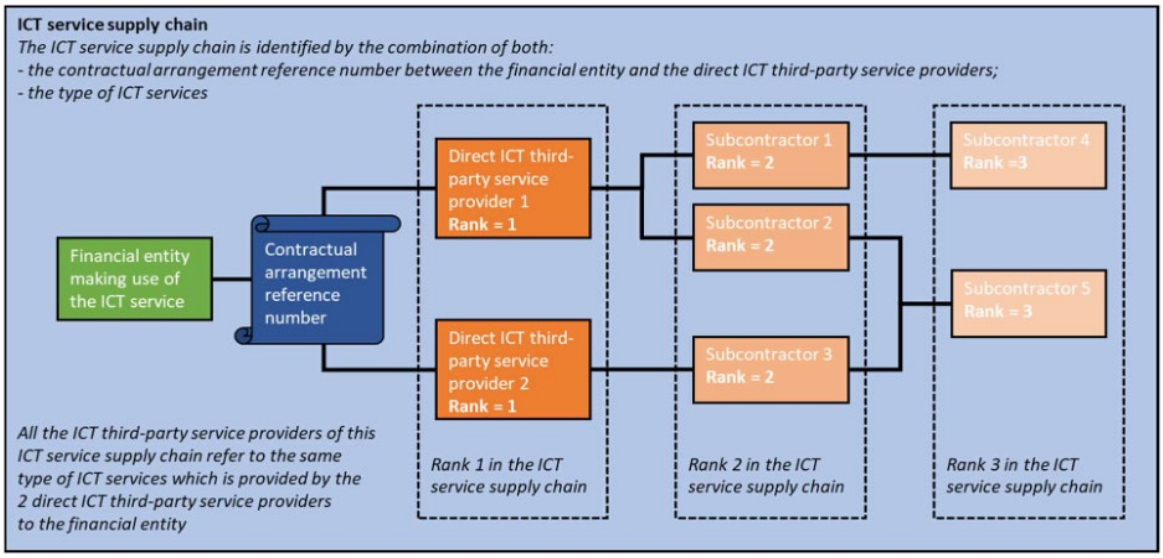
26. **Posudzovať** riziká súvisiace so **subdodávateľmi**, ktorí podporujú **kritické alebo dôležité funkcie**.

27. **Zaznamenávať** v **registri informácií** len **subdodávateľov**, ktorých narušenie by znížilo bezpečnosť alebo kontinuitu poskytovania služieb podporujúcich **kritické alebo dôležité funkcie**.

28. **Uvádzať** vo vzore **registra informácií** (B_05.02) podrobnosti o **subdodávateľoch IKT služieb**.

29. **Zabezpečiť**, aby **zmluvné dojednania** s **externými poskytovateľmi IKT služieb** obsahovali záväzky týkajúce sa ich **subdodávateľov**, najmä v oblasti bezpečnosti a **kontinuity činností**.

30. **Vyžadovať** od **externých poskytovateľov IKT služieb** informácie o ich **subdodávateľoch** relevantné pre posúdenie rizík. (56) (57)



Obrázok č. 50 Reťazec poskytovateľov IKT služieb a ich subdodávateľov (Zdroj: EBA, Final report on draft ITS on Register of Information, JC 2023 85)

1.5.5 Klasifikácia, hlásenie a manažment IKT incidentov

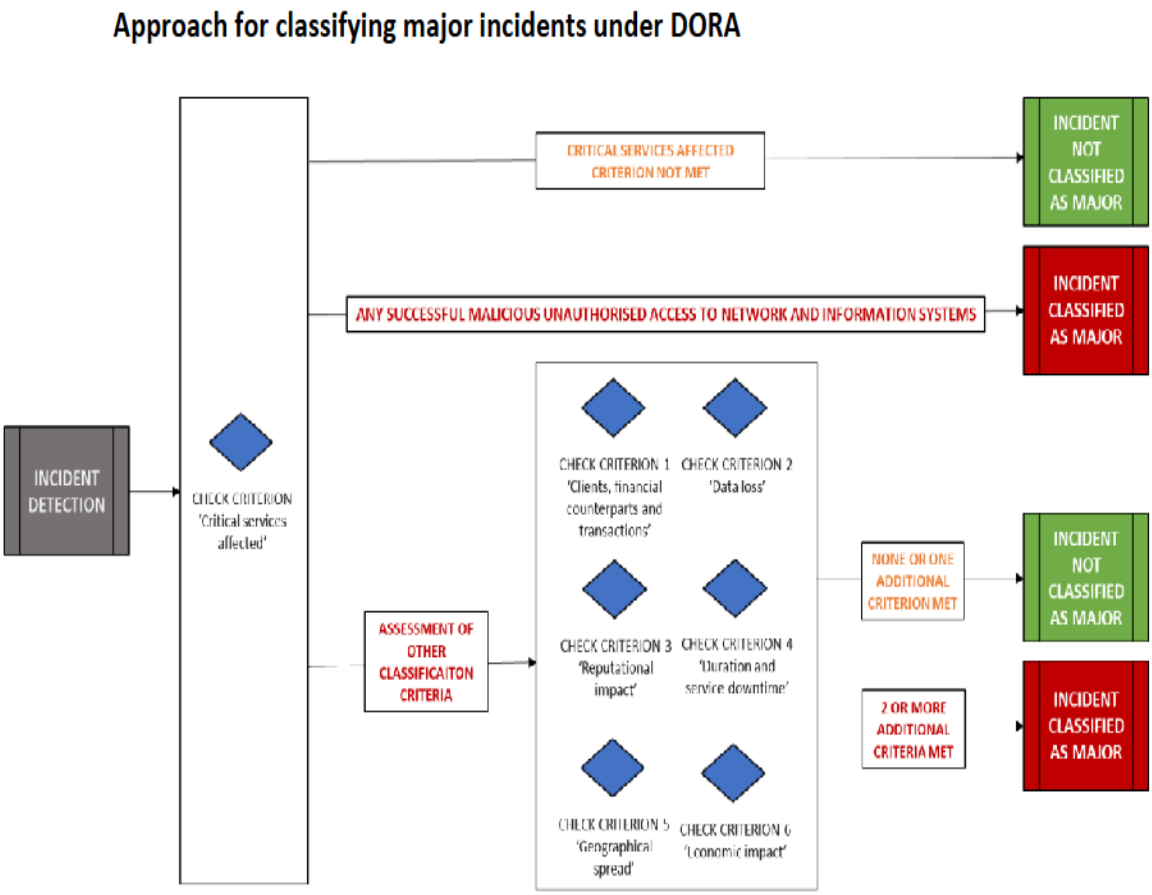
1. **Vytvoriť** a **udržiavať politiku incidentov súvisiacich s IKT**, ktorá zahŕňa všetky zložky **procesu riadenia incidentov súvisiacich s IKT**.
2. **Identifikovať** všetky relevantné **kontaktné osoby** v rámci organizácie aj mimo nej pre správnu koordináciu a vykonávanie fáz **procesu riadenia incidentov súvisiacich s IKT**.
3. **Analyzovať** podrobne **incidenty súvisiace s IKT**, ktoré považuje za najvýznamnejšie, okrem iného z dôvodu ich pravidelného opakovania, s cieľom identifikovať trendy a základné príčiny.
4. **Uchovávať dôkazy o incidentoch súvisiacich s IKT** po dobu určenú vzhľadom na **kritickosť údajov** a s ohľadom na požiadavky na **uchovávanie údajov** vyplývajúce z právnych predpisov Únie.
5. **Zohľadňovať** pri **klasifikácii kritickosť zasiahnutých služieb**, a to posúdením, či incident ovplyvňuje **IKT služby** alebo **sieťové** a **informačné systémy** podporujúce **kritické** alebo **dôležité funkcie** finančného subjektu, alebo finančné služby vyžadujúce povolenie, registráciu alebo dohľad.
6. **Zaviesť varovné prahové hodnoty a kritériá** na spustenie a iniciáciu **procesov reakcie na incidenty súvisiace s IKT**.
7. **Zaviesť** nástroje vytvárajúce **varovania** v prípade **anomálnych činností a správania**, a to aspoň v prípade **IKT aktív a informačných aktív podporujúcich kritické alebo dôležité funkcie** .
8. **Určiť priority** v prípade generovaných **varovaní** s cieľom umožniť riadenie zistených **incidentov súvisiacich s IKT** v rámci očakávaného času riešenia .
9. **Posudzovať kolektívnu závažnosť opakujúcich sa incidentov**, ktoré jednotlivo nie sú závažné, ak sú prepojené podobnou hlavnou príčinou a vyskytujú sa opakovane počas určitého obdobia.
10. **Viesť záznamy** o všetkých relevantných informáciách o každej odhalenej **anomálnej činnosti**, ktoré umožňujú identifikáciu dátumu a času výskytu a odhalenia, ako aj typu **anomálnej činnosti**.

11. **Implementovať** technické, organizačné a prevádzkové mechanizmy na podporu **procesu riadenia incidentov súvisiacich s IKT**, vrátane mechanizmov umožňujúcich urýchlené odhalenie **anomálnych činností a správania** .
12. **Uchovávať** všetky **dôkazy** týkajúce sa **incidentov súvisiacich s IKT** počas obdobia, ktoré zodpovedá **kritickosti ovplyvnených obchodných funkcií**, **podporných procesov**, **IKT aktív** a **informačných aktív**.
13. **Zabezpečiť**, aby **vzor nahlasovania** závažných incidentov súvisiacich s IKT umožňoval aktualizáciu predtým predložených informácií a prípadnú zmenu klasifikácie incidentu.
14. **Poskytovať** v hláseniach **právnu identifikáciu** ovplyvnených finančných subjektov v súlade s vykonávacími technickými predpismi,
15. Pri zmene klasifikácie incidentu na menej závažný, **oznámiť** túto zmenu príslušnému orgánu prostredníctvom **vzoru** s uvedením typu správy a ďalších informácií.
16. Poskytnúť **opis** najdôležitejších aspektov **závažného incidentu súvisiaceho s IKT**, vrátane možných príčin, bezprostredných vplyvov a ovplyvnených systémov.
17. Uviesť v hlásení **trvanie výpadku služby** merané od nedostupnosti do obnovenia činností.
18. **Uviesť** informácie o priamych a nepriamych nákladoch a stratách vyplývajúcich z incidentu a o potenciálnom vplyve na platobnú schopnosť, likviditu a prevádzkovú kontinuitu.
19. Klasifikovať **typ hlavnej príčiny incidentu** (napr. zlyhanie procesu, poruchy systému, chyba spôsobená človekom, externá udalosť).
20. V prípade **zlomyseľného konania**, opísať spôsob jeho vykonania vrátane použitých taktík, techník a postupov a vstupného vektora.

21. Uviesť vplyv **závažného incidentu súvisiaceho s IKT** na **platobnú schopnosť alebo likviditu**, **prevádzkovú kontinuitu**, **možnosť riešenia krízových situácií**, **dodatočné náklady a straty**, a spoľahlivosť **zmluvných dojednaní o využívaní IKT služieb**.

22. Predložiť **počiatočné oznámenie** o **závažnom incidente súvisiacom s IKT** čo najskôr, najneskôr však do štyroch hodín od jeho klasifikácie ako závažného a do 24 hodín od zistenia .

23. Predkladať **priebežné** a **záverečné správy** o **závažnom incidente súvisiacom s IKT** v stanovených lehotách . (54) (55) (58) (59)

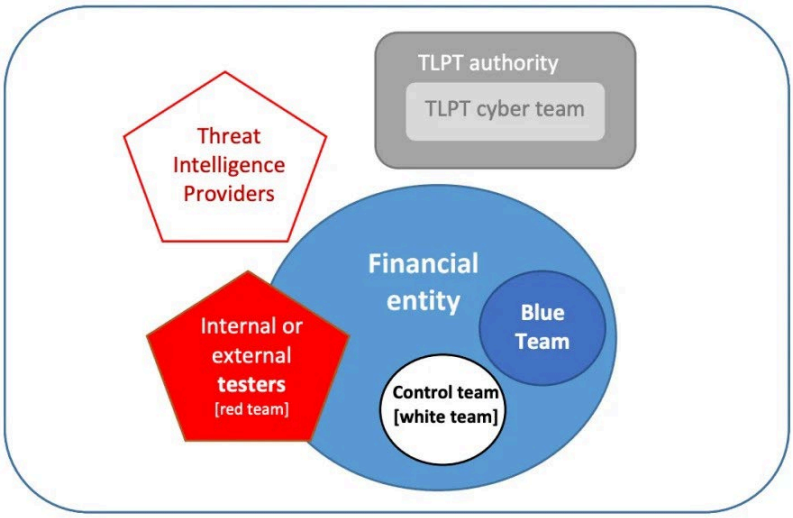


Obrázok č. 51 Klasifikácia závažných incidentov podľa metodiky DORA (Zdroj: EBA, Final Report on draft RTS on classification of major incidents and significant cyber threats, JC 2023 83)

1.5.6 Kontinuita činností a testovanie digitálnej prevádzkovej odolnosti

1. **Vypracovať** a **udržiavať** politiku kontinuity činností v oblasti IKT.
2. **Vypracovať** súbor **scenárov**, ktoré sa majú zohľadňovať pri vykonávaní **plánov reakcie a obnovy v oblasti IKT**, ako aj pri **testovaní plánov na zabezpečenie kontinuity činností v oblasti IKT**.
3. **Analyzovať** relevantnosť a vierohodnosť každého **scenára** a potrebu vypracovať alternatívne **scenáre**.
4. **Posúdiť** účinnosť **redundantnej kapacity**, **záloh** a **redundantných zariadení** prostredníctvom **testovania prepnutia** medzi primárnou infraštruktúrou IKT a týmito prvkami počas dostatočne dlhého obdobia.
5. **Zohľadňovať** výsledky **analýzy vplyvu na činnosti (BIA)** pri vypracúvaní **plánov reakcie a obnovy v oblasti IKT**.
6. **Zahrnúť** do **plánov reakcie a obnovy v oblasti IKT** podmienky, ktoré vedú k ich **aktivácii** alebo **deaktivácii**, a všetky výnimky pre takúto aktiváciu alebo deaktiváciu.
7. **Obsiahnuť** do **plánov reakcie a obnovy v oblasti IKT** opis opatrení na zabezpečenie **dostupnosti**, **integrity**, **kontinuity** a **obnovy** aspoň **IKT systémov** a **služieb podporujúcich kritické alebo dôležité funkcie finančného subjektu**.
8. **Zvážiť** a **vykonať** opatrenia na zabezpečenie **kontinuity** s cieľom zmierniť zlyhania **externých poskytovateľov IKT služieb** podporujúcich **kritické alebo dôležité funkcie finančného subjektu** v rámci **plánov reakcie a obnovy v oblasti IKT**.
9. **Stanoviť** plánované úrovne obnovy a časové rámce na obnovu a obnovenie funkcií a kľúčových interných a externých závislostí, vrátane externých poskytovateľov **IKT služieb**, v plánoch **kontinuity činnosti v oblasti IKT.**
10. **Vypracovať** súbor scenárov pre **testovanie plánov kontinuity činností**, ktoré zohľadňujú potenciálne zlyhania **IKT systémov** a **IKT infraštruktúry**.
11. **Zahrnúť** do **testovania** scenáre týkajúce sa prerušenia alebo narušenia prevádzky, straty integrity údajov a **incidentov kybernetickej bezpečnosti**.

12. **Zahrnúť** do **testovania** scenáre, ktoré spochybňujú predpoklady, na ktorých sú založené **plány na zabezpečenie kontinuity činností** vrátane mechanizmov správy a riadenia a **plánov krízovej komunikácie**.
13. **Zdokumentovať** výsledky **testovania plánov kontinuity činností**.
14. **Vykonávať testovanie plánov kontinuity činností** aspoň raz ročne.
15. **Dodržiavať** požiadavky týkajúce sa rozsahu testov, metodiky testovania a výsledkov **TLPT** podľa rámca TIBER-EÚ.
16. **Dodržiavať** požiadavky a normy, ktorými sa riadi využívanie **interných testovacích subjektov** pre **TLPT**.
17. **Zabezpečiť**, aby **poskytovatelia TLPT** mali potrebné zručnosti na vykonanie testov červeného tímu na základe spravodajských informácií, ktoré simulujú úplný scenár cieleného útoku.
18. **Zohľadňovať** pri výbere **poskytovateľov TLPT** ich schopnosť vykonávať testy červeného tímu, ktoré idú nad rámec bežných penetračných testov a zahŕňajú ľudí, procesy a technológie.
19. **Zabezpečiť**, aby si modrý tím a testovacie subjekty po **TLPT** prešli útok a preskúmali prijaté kroky s cieľom poučiť sa zo skúseností. (54) (56) (60)



Obrázok č. 52 Organizačná schéma účastníkov testovania odolnosti typu TLPT (Zdroj: yogosha.com/blog/tlpt-threat-led-penetration-testing/)

1.6 Praktický rámec implementácie nariadenia DORA

Implementácia nariadenia DORA vyžaduje štruktúrovaný a komplexný prístup, ktorý zahŕňa viacero fáz a krokov zameraných na posilnenie digitálnej prevádzkovej odolnosti finančných inštitúcií. Nasledujúci zoznam predstavuje praktický rámec činností, ktoré by mali finančné inštitúcie podniknúť v procese implementácie DORA, s cieľom dosiahnuť súlad s požiadavkami nariadenia.

1. **Vykonanie úvodnej GAP analýzy.** Východiskovým krokom je detailné posúdenie aktuálneho stavu digitálnej prevádzkovej odolnosti inštitúcie v porovnaní s elementárnymi požiadavkami DORA. Táto analýza identifikuje existujúce medzery a oblasti, ktoré si vyžadujú úpravy alebo zavedenie nových opatrení. Výstupom je **zaznamenaná GAP analýza**, často vytvorená pomocou **šablón pre GAP analýzu**, prípadne s využitím **nástrojov pre riadenie rizík a compliance (GRC)**, ako napríklad **Servicenow IRM**. (61)
2. **Získanie podpory vrcholového manažmentu.** Pre úspešnú implementáciu je nevyhnutné získať formálny súhlas a aktívnu podporu vrcholového manažmentu. To zahŕňa zabezpečenie adekvátnych časových, personálnych a finančných zdrojov pre realizáciu implementačného projektu. Výstupom je **formálne schválenie projektu implementácie DORA** vrcholovým manažmentom, zdokumentované napríklad v **projektovej charte**, a **pridelenie potrebných zdrojov** zaznamenané v **rozpočte projektu**. (61)
3. **Zostavenie projektového tímu DORA.** Je potrebné vytvoriť špecializovaný a multidisciplinárny tím, ktorý bude zodpovedný za riadenie a koordináciu implementačných aktivít. Tím by mal zahŕňať zástupcov relevantných oddelení, ako sú IT, riadenie rizík, compliance a právne oddelenie. Výstupom je **zriadený projektový tím DORA** s jasne definovanými rolami a zodpovednosťami, často zdokumentovanými v **organizačnej štruktúre projektu** a **matici zodpovedností (RACI matica)**. (61) (62) (63)

4. **Detailná revízia nariadenia DORA a súvisiacich štandardov.** Projektový tím a relevantní odborníci musia vykonať podrobnú analýzu požiadaviek DORA a súvisiacich regulačných a implementačných technických štandardov (RTS/ITS). Výstupom je **dokument preukazujúci porozumenie požiadaviek DORA** a ich dopadu na súčasné politiky, formou **prehľadu kľúčových článkov a ich interpretácie**.(61) (62)

5. **Mapovanie súčasného stavu voči požiadavkám DORA.** Na základe detailnej revízie je potrebné vytvoriť podrobné mapovanie existujúcich politík, postupov, ICT systémov a kontrolných mechanizmov voči konkrétnym článkom a požiadavkám DORA. Toto mapovanie pomáha vizualizovať mieru súladu a identifikovať špecifické oblasti s nedostatkami. Výstupom je **matica mapovania súladu**, ktorá prehľadne zobrazuje pokrytie požiadaviek DORA existujúcimi opatreniami a identifikované **medzery (tzv. "compliance gaps")**. (62)

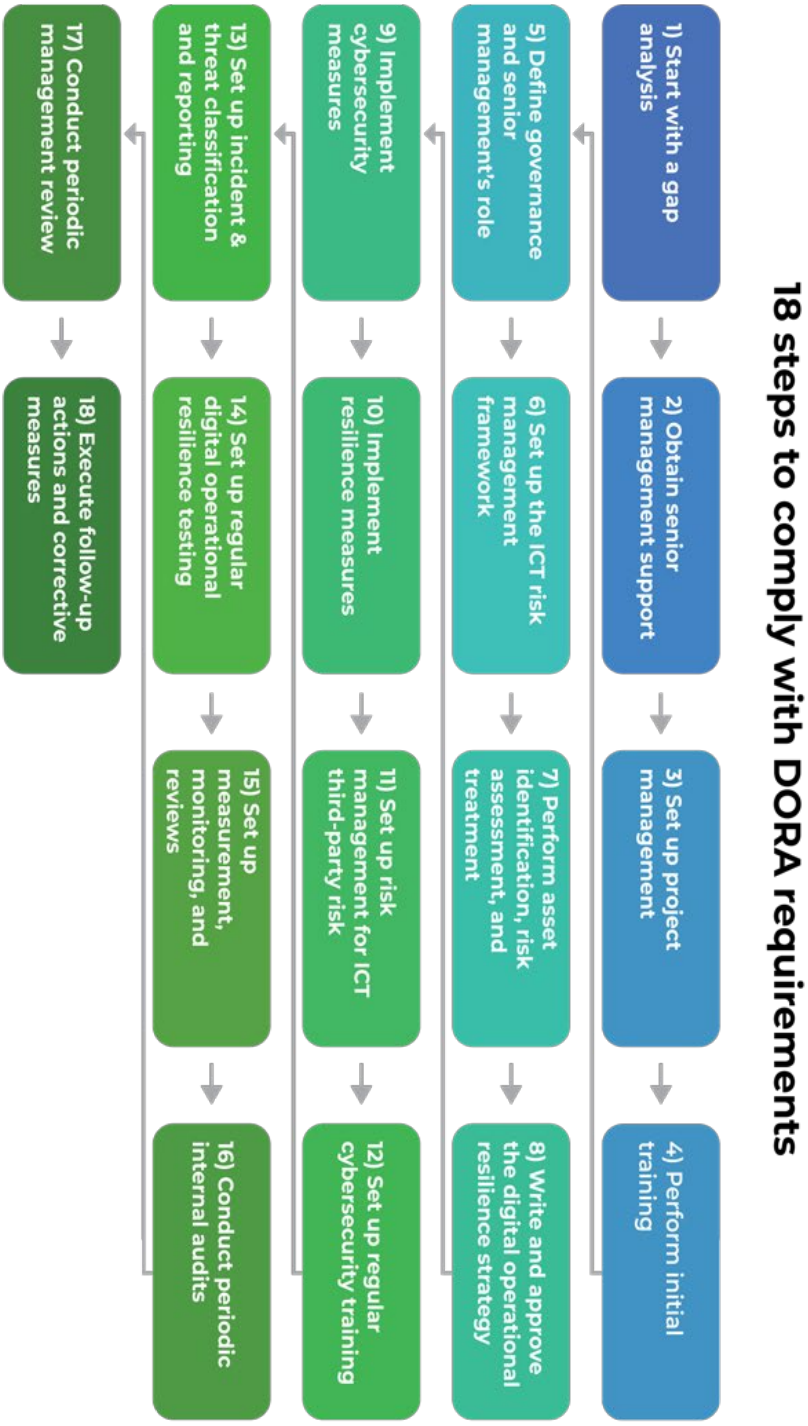
6. **Analýza možností riešenia zistených nedostatkov.** Pre každú identifikovanú medzeru je potrebné zvážiť rôzne možnosti jej odstránenia, s ohľadom na náklady, časovú náročnosť, súvisiace riziká a dopad na prevádzku. To zahŕňa analýzu potrebných zmien v politikách, postupoch, technológiách a organizačnej štruktúre. Výstupom je **dokument analyzujúci rôzne prístupy k odstráneniu zistených nedostatkov** s odporúčanými riešeniami, často obsahujúci **analýzu nákladov a prínosov (CBA - Cost benefit analysis)**. (62)

7. **Vytvorenie a schválenie plánu nápravných opatrení.** Na základe analýzy možností je potrebné vypracovať detailný plán implementácie nápravných opatrení s konkrétnymi úlohami, zodpovednosťami, termínmi a potrebnými zdrojmi. Tento plán musí byť schválený vrcholovým manažmentom a efektívne riadený. Výstupom je **schválený plán implementácie DORA** s **harmonogramom projektu** (napr. vytvoreným v nástrojoch ako **Microsoft Project** alebo **Asana**) a pridelenými zodpovednosťami. (62) (64)

8. **Implementácia plánu a priebežné monitorovanie.** Po schválení plánu nasleduje samotná realizácia naplánovaných opatrení. Počas implementácie je kľúčové priebežne monitorovať pokrok, identifikovať prípadné odchýlky a zabezpečiť ich promptné riešenie. Výstupom je **implementovaný plán DORA** s pravidelnými **správami o stave implementácie** a aktualizovanými záznamami v **nástrojoch pre riadenie projektov**. (62) (63)
9. **Realizácia úvodného školenia.** V skorých fázach implementácie je dôležité zabezpečiť školenie projektového tímu a relevantných zamestnancov o nariadení DORA, jeho požiadavkách a súvisiacich štandardoch. Cieľom je zabezpečiť informovaný a kompetentný tím zamestnancov. Výstupom sú **uskutočnené úvodné školenia o DORA** pre relevantné skupiny zamestnancov, s **prezenčnými listami** a **materiálmi zo školení**. Môžu sa využiť **e-learningové platformy** alebo interné **systémy pre riadenie vzdelávania (LMS)**. (61) (64)
10. **Definovanie riadenia a úlohy vrcholového manažmentu v oblasti ICT rizík.** V súlade s DORA je potrebné jasne definovať organizačnú štruktúru riadenia ICT rizík, vrátane politík, rolí a zodpovedností vrcholového manažmentu. To zahŕňa schvaľovanie stratégie, plánov auditu a rozpočtu. Výstupom je **definovaný rámec riadenia ICT rizík** zdokumentovaný v **organizačných smerniciach** a **popisoch pracovných pozícií**, a jasne stanovené úlohy a zodpovednosti vrcholového manažmentu v **zápisniciach zo zasadnutí vedenia**. (61)
11. **Zavedenie rámca riadenia ICT rizík.** Na základe definovaného riadenia je potrebné implementovať komplexný rámec riadenia ICT rizík, ktorý zahŕňa stratégie, politiky, postupy, ICT protokoly a nástroje na ochranu informačných a ICT aktív. Dôležitou súčasťou je dokumentácia tohto rámca v **súbore politík a smerníc ICT bezpečnosti a prevádzkovej odolnosti**. Výstupom je **dokumentovaný rámec riadenia ICT rizík** s implementovanými politikami a postupmi, uložený v **systéme pre riadenie dokumentov**. (61) (62)

12. **Identifikácia aktív, posúdenie rizík a ich manažment.** V súlade s DORA je potrebné identifikovať a zdokumentovať všetky ICT podporované obchodné funkcie, aktíva a ich vzájomné závislosti. Následne sa vykoná posúdenie hrozieb, zraniteľností a rizík a implementujú sa opatrenia na ich riadenie a zmiernenie. Výstupom je **register ICT aktív a rizík**, často spravovaný v **databázach aktív (CMDB)** a **nástrojoch pre riadenie rizík**, s implementovanými opatreniami na ich manažment zaznamenanými v **plánoch riadenia rizík**. (61) (65)
13. **Implementácia opatrení kybernetickej bezpečnosti a kontinuity činností.** Na základe posúdenia rizík je potrebné zaviesť adekvátne technické a organizačné opatrenia na zabezpečenie kybernetickej bezpečnosti a kontinuity činností. To zahŕňa implementáciu **bezpečnostných kontrol (napr. firewall, IDS/IPS)**, **zálohovacích a obnovovacích postupov** zdokumentovaných v **plánoch obnovy po havárii (DRP)** a **plánoch kontinuity činností (BCP)**. Výstupom sú **implementované opatrenia kybernetickej bezpečnosti** (doložené konfiguráciami systémov a záznamami o implementácii) a **plány kontinuity činností**, pravidelne testované a aktualizované. (61) (62) (66)
14. **Definovanie stratégie digitálnej prevádzkovej odolnosti.** Na základe vykonaných analýz a implementovaných opatrení je potrebné formalizovať stratégiu digitálnej prevádzkovej odolnosti, ktorá zohľadňuje všetky aspekty DORA. Táto stratégia by mala byť pravidelne prehodnocovaná a aktualizovaná. Výstupom je **dokument stratégie digitálnej prevádzkovej odolnosti**, schválený vrcholovým manažmentom. (61) (67)
15. **Zavedenie procesov riadenia a nahlasovania ICT incidentov.** Je potrebné implementovať jasné postupy pre detekciu, klasifikáciu, manažment a nahlasovanie významných ICT incidentov príslušným orgánom. To zahŕňa aj vykonávanie analýzy príčin incidentov. Výstupom sú **implementované procesy riadenia a nahlasovania ICT incidentov** zdokumentované v **pláne reakcie na incidenty**, používanie **systémov pre správu incidentov** a **šablóny pre nahlasovanie incidentov**. (62) (65)

16. **Zavedenie programu testovania digitálnej prevádzkovej odolnosti.** Inštitúcie musia zaviesť a vykonávať pravidelné testovanie svojich ICT systémov a procesov s cieľom overiť ich odolnosť voči rôznym scenárom narušenia. Väčšie inštitúcie sú povinné vykonávať aj pokročilé testovanie na základe hrozieb (TLPT) s využitím **špecializovaných nástrojov pre penetračné testovanie** a zapojením **akreditovaných tretích strán**. Výstupom je **implementovaný program testovania digitálnej prevádzkovej odolnosti** s **plánom testov**, **scenármi testov** a **záznamami o výsledkoch testov**. (64) (66)
17. **Riadenie rizík tretích strán.** Je potrebné implementovať procesy na identifikáciu, posúdenie, monitorovanie a riadenie rizík spojených s využívaním služieb tretích strán v oblasti ICT. To zahŕňa aj zmluvné požiadavky a stratégie ukončenia spolupráce. Môžu sa využiť **platformy pre riadenie rizík tretích strán** ako napríklad *ServiceNow Vendor Risk Management*. Výstupom je **implementovaný rámec riadenia rizík tretích strán** s vykonanými **hodnoteniami rizík dodávateľov**, **zmluvnými dodatkami** a **registrom tretích strán**. (62) (64) (66)
18. **Zavedenie mechanizmov zdieľania informácií.** V súlade s DORA je potrebné, zavedenie mechanizmov zdieľania informácií o kybernetických hrozbách a spravodajských informácií s inými finančnými inštitúciami. Výstupom sú **zavedené mechanizmy pre zdieľanie informácií o kybernetických hrozbách**, ak je to relevantné a vhodné, napríklad formou členstva v **platformách pre zdieľanie informácií (napr. FS-ISAC)** a používania zabezpečených komunikačných kanálov. (62)



Obrázok č. 53 Postupný plán implementácie rámca digitálnej prevádzkovej odolnosti DORA (Zdroj: č.51)

2 POPIS SÚČASNÉHO STAVU

2.1 Predstavenie spoločnosti Finsys, s.r.o.

2.1.1 Základné informácie, história a predmet podnikania

Analyzovaná spoločnosť, pre účely tejto práce označovaná ako **Finsys s.r.o.** (ďalej len „Finsys“ alebo „spoločnosť“), predstavuje dynamicky sa rozvíjajúci technologický subjekt pôsobiaci v oblasti finančných technológií (FinTech) so sídlom v Slovenskej Republike. Spoločnosť operuje vo forme spoločnosti s ručením obmedzeným (s.r.o.) a profiluje sa ako malý až stredný podnik (SME). Disponuje tímom 15 až 20 zamestnancov.

2.1.1.1 História a vývoj

Spoločnosť Finsys bola založená na začiatku druhej dekády 21. storočia s cieľom vyvíjať a prevádzkovať inovatívne softvérové riešenia pre finančný sektor. Kľúčovým medzníkom v histórii spoločnosti bolo spustenie jej prvého významného produktu okolo roku 2017, platformy **FinSecure Exchange**.

V reakcii na rastúci dopyt po pokročilejších nástrojoch pre obchodovanie s digitálnymi aktívami a s cieľom osloviť skúsenejších investorov, spoločnosť Finsys rozšírila svoje portfólio a začiatkom roka 2021 uviedla na trh platformu **FinSecure Trader.**

Táto platforma funguje na princípe kryptomenovej burzy (exchange), ktorá umožňuje klientom priamo zadávať nákupné a predajné pokyny (limitné a trhové príkazy) a obchodovať tak za aktuálne trhové ceny, pričom platforma poskytuje vizualizáciu aktuálneho dopytu a ponuky na rôznych cenových úrovniach. Spustenie FinSecure Trader predstavovalo významný krok v profilácii spoločnosti ako komplexného poskytovateľa služieb v oblasti obchodovania s kryptomenami na slovenskom a českom trhu.

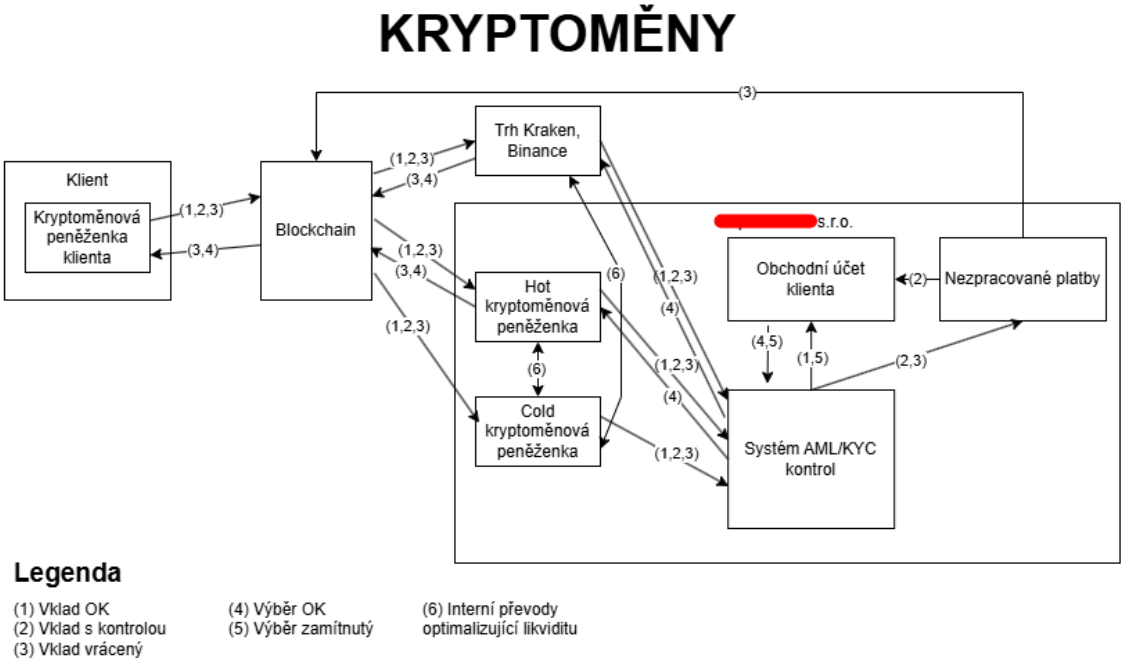
2.1.1.2 Predmet podnikania a hlavné činnosti

Predmet podnikania spoločnosti Finsys je primárne zameraný na **vývoj softvéru a poskytovanie služieb informačných a komunikačných technológií (IKT)**, špecificky v kontexte digitálnych finančných služieb. Hlavné činnosti spoločnosti zahŕňajú:

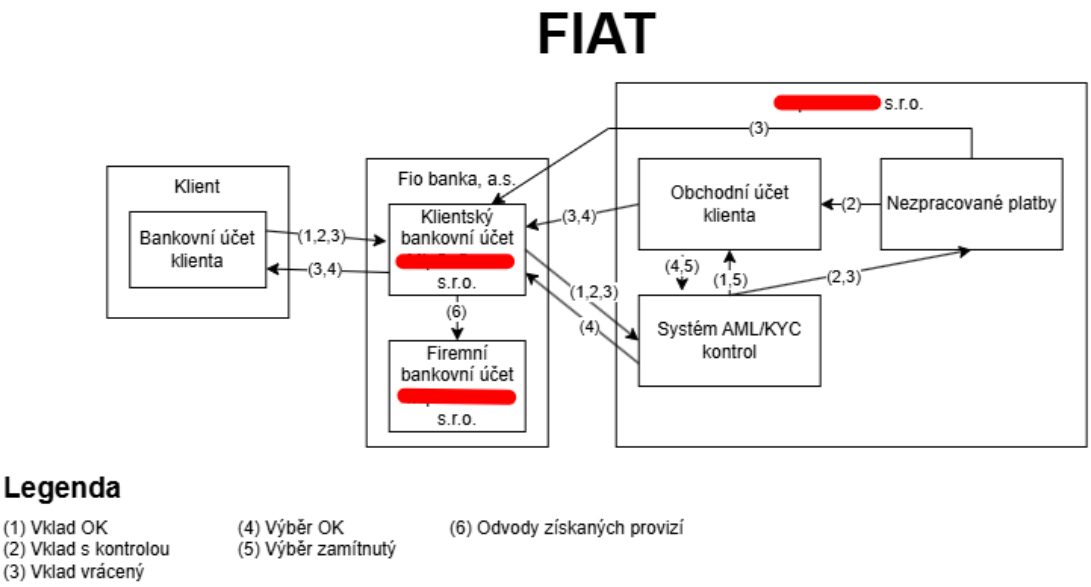
- Vývoj, správa a prevádzka digitálnych platforiem.
- Poskytovanie služieb súvisiacich s obchodovaním s digitálnymi aktívami.
- Vývoj softvéru na zákazku .
- Aplikácia komplexných opatrení proti legalizácii výnosov z trestnej činnosti a financovaniu terorizmu (AML/CFT).

2.1.1.3 Pozícia na trhu a kľúčové obchodné aktivity

Na slovenskom trhu si Finsys vybudovala pozíciu **významného lokálneho hráča** v segmente platforiem pre obchodovanie s kryptomenami. Jej konkurenčnú výhodu možno vidieť v **kombinácii technologickej expertízy s orientáciou na potreby slovenského a českého trhu** (jazyková podpora, EUR/CZK transakcie, lokálna zákaznícka podpora, integrácia s miestnymi bankami). Kľúčové obchodné aktivity sú neoddeliteľne spojené s prevádzkou platforiem, pričom hlavné zdroje príjmov pochádzajú z **transakčných poplatkov a spreadov** pri zmenárenských operáciách.



Obrázok č. 54: Schéma toku kryptomien v rámci systému klient – blockchain (Zdroj: Vlastné spracovanie)



Obrázok č. 55: Schéma toku fiat mien v rámci bankového účtu klienta (Zdroj: Vlastné spracovanie)

Zhrnutie:

Aktivity spoločnosti Finsys, najmä poskytovanie platformy pre obchodovanie s digitálnymi aktívami, spracovanie finančných transakcií a správa citlivých zákazníckych dát, ju priamo stavajú do pozície subjektu, ktorého prevádzková odolnosť a kybernetická bezpečnosť sú esenciálne. Tieto činnosti zároveň implikujú relevanciu požiadaviek vyplývajúcich z nových regulačných rámcov, akým je napríklad nariadenie DORA (Digital Operational Resilience Act). Povaha podnikania spoločnosti si vyžaduje robustné riadenie rizík IKT a zabezpečenie vysokej úrovne digitálnej prevádzkovej odolnosti. (68)

2.1.2 Organizačná štruktúra a kompetencie v oblasti kybernetickej bezpečnosti

Organizačná štruktúra spoločnosti Finsys s.r.o. **efektívne podporuje** jej kľúčové činnosti: vývoj, prevádzku a zabezpečenie digitálnych finančných platforiem. Štruktúra je relatívne plochá, funkčne orientovaná a kladie dôraz na priamu komunikáciu a spoluprácu medzi jednotlivými tímami a vedením spoločnosti.

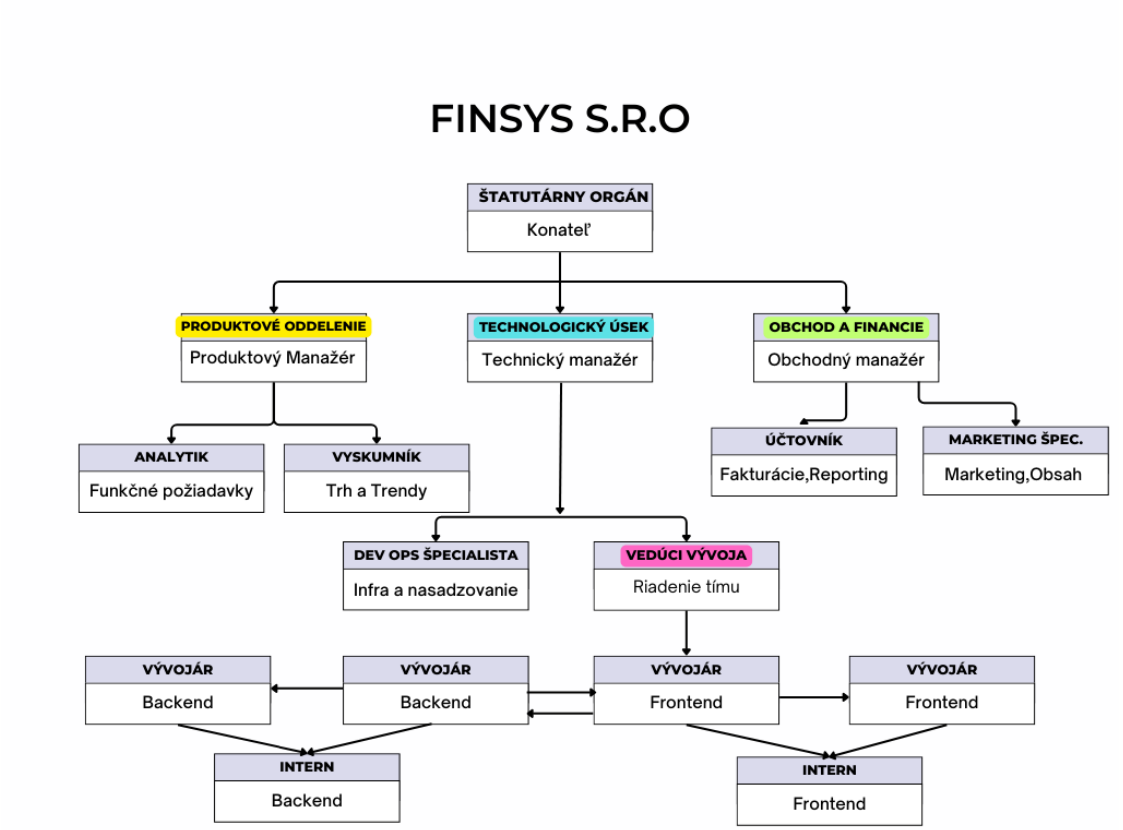
2.1.2.1 Riadenie a strategické rozhodovanie

Formálnu zodpovednosť za celkové smerovanie spoločnosti a schvaľovanie kľúčových rozhodnutí **prináleží vedeniu spoločnosti (konateľovi)**. Avšak, v praxi sa **rozhodovanie týkajúce sa IKT** zameriava primárne na vývoj produktov, zabezpečenie **nepretržitej prevádzky (dostupnosti) služieb** a na **rozvoj produktov podľa potrieb trhu**, zatiaľ čo systematické riadenie rizík IKT a formálne definovanie bezpečnostnej stratégie neboli doteraz prioritou. Rozhodovanie o bezpečnostných opatreniach má prevažne reaktívny charakter, iniciované ad-hoc technickými potrebami alebo incidentmi, absentuje proaktívny, rizikovo-orientovaný prístup.

2.1.2.2 Organizačné členenie spoločnosti

Fungovanie spoločnosti zabezpečujú tieto funkčné celky:

- **Technologický úsek (Vývoj a Prevádzka):** Predstavuje jadro spoločnosti, zodpovedné za kompletný životný cyklus softvérových produktov (FinSecure Exchange, FinSecure Trader) a súvisiacej IKT infraštruktúry. Tento kľúčový tím, zložený z približne 8-10 zamestnancov, operuje pod priamym vedením vedúceho technologického úseku, ktorý reportuje priamo konateľovi spoločnosti.
- **Produktový manažér:** Zodpovedá za stratégiu produktov (FinSecure Exchange, FinSecure Trader), definovanie požiadaviek na nové funkcionality a sledovanie trhových trendov v oblasti FinTech a kryptomien.
- **Obchod a Financie:** Zastrešujú aktivity spojené s obchodom, marketingom, finančným riadením, účtovníctvom, reportingom, kontrolou nákladov a všeobecnou administratívou



Obrázok č. 56: Organizačná schéma spoločnosti Finsys s.r.o. (stav k roku 2025) (Zdroj: Vlastné spracovanie)

2.1.2.3 Rozdelenie kompetencií a zodpovedností v oblasti kybernetickej bezpečnosti

V spoločnosti Finsys **neexistuje formalizovaný systém riadenia kybernetickej bezpečnosti a ani dedikovaná bezpečnostná rola,** čo je v priamom rozpore s požiadavkami nariadenia DORA na zavedenie komplexného rámca riadenia rizík IKT a jasne definovaných zodpovedností. Zodpovednosti sú rozdelené implicitne, čo so sebou prináša riziká nedostatočného pokrytia bezpečnostných oblastí, nejasnej zodpovednosti v prípade incidentov a komplikácií pri preukazovaní zhody, a zameriavajú sa skôr na operatívne a technické aspekty než na strategické riadenie rizík:

- **Najvyššie vedenie / Štatutárny orgán (konateľ):** Má najvyššiu formálnu zodpovednosť za fungovanie spoločnosti a jej IKT systémov. Schvaľuje rozpočty a kľúčové výdavky na IKT, vrátane investícií do zabezpečenia systémov a nesie konečnú zodpovednosť za plnenie legislatívnych povinností.

- **Vedúci technologického úseku:** Zodpovedá za chod technologického úseku a zabezpečenie funkčnosti a stability IKT systémov. Dohliada na implementáciu základných technických bezpečnostných opatrení (zálohovanie a obnova dát, riadenie prístupov a identít, zabezpečenie sieťovej infraštruktúry, logovanie, zabezpečenie koncových bodov). Rieši predovšetkým operatívne technické problémy a požiadavky. Nevykonáva systematické hodnotenie rizík ani neudržiava komplexnú bezpečnostnú dokumentáciu.
- **Technologický úsek (Tím):** Zabezpečuje praktickú implementáciu a funkčnosť technických a bezpečnostných opatrení, pod dohľadom vedúceho technologického úseku. Typické činnosti zahŕňajú:
    - Správa základnej IKT infraštruktúry.
    - Zriaďovanie, úprava a mazanie používateľských účtov a prístupových oprávnení k systémom.
    - Zabezpečenie aplikácie bezpečnostných aktualizácií (patch management) a základných konfigurácií systémov (hardening OS), ako aj správa a konfigurácia základných bezpečnostných nástrojov (firewall, antivírus, monitoring sieťovej prevádzky a logovanie – adaptovaná kombinácia open-source nástrojov).
    - Reakcia na vzniknuté technické problémy a incidenty (výpadok služieb).
- **Všetci ostatní zamestnanci: K základným zodpovednostiam všetkých zamestnancov patrí dodržiavanie základnej** IT hygieny (bezpečné heslá). Neexistuje však program pravidelného bezpečnostného školenia a povedomie o aktuálnych hrozbách a postupoch je na nízkej úrovni. Hlásenie bezpečnostných podozrení nie je formalizované.

Zhrnutie:

Tento stav, charakteristický pre mnohé SME v technologickom sektore, ukazuje existenciu základných technických opatrení, avšak bez zastrešujúceho rámca riadenia kybernetickej bezpečnosti. Analyzovaná organizačná štruktúra, hoci funkčná pre bežnú prevádzku, postráda formálne ukotvenie riadenia kybernetickej bezpečnosti. Absencia dedikovanej bezpečnostnej roly a explicitne definovaných, formalizovaných zodpovedností naprieč organizačnými úrovňami predstavuje významnú medzeru, najmä vo vzťahu k požiadavkám nariadenia DORA na riadiace a kontrolné funkcie. (68)

2.1.3 Legislatívny a normatívny kontext

Činnosť spoločnosti Finsys s.r.o., ako subjektu pôsobiaceho v dynamickom sektore finančných technológií (FinTech) so zameraním na služby súvisiace s kryptoaktívami, je ovplyvnená viacerými kľúčovými legislatívnymi rámcami. Okrem už existujúcich povinností vyplývajúcich napríklad zo zákona č. 297/2008 Z. z. o niektorých opatreniach proti legalizácii výnosov z trestnej činnosti a financovaniu terorizmu (AML zákon), sú pre oblasť digitálnej prevádzkovej odolnosti a kybernetickej bezpečnosti kľúčové najmä nové európske predpisy: Nariadenie (EÚ) 2023/1114 o trhoch s kryptoaktívami (MiCA) a Nariadenie (EÚ) 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora (DORA).

2.1.3.1 Zaradenie podľa Nariadení MiCA a DORA

Nariadenie **MiCA** harmonizuje pravidlá pre vydávanie, verejné ponúkanie a prijímanie kryptoaktív na obchodovanie a pre poskytovateľov služieb týkajúcich sa kryptoaktív (Crypto-Asset Service Providers – CASP) v EÚ. Spoločnosť Finsys, prevádzkujúca platformy FinSecure Exchange a FinSecure Trader, poskytuje služby ako „prevádzka obchodnej platformy pre kryptoaktíva“ a „zmena kryptoaktív za fiat menu, ktorá je zákonným platidlom“ (Článok 3(1) body 16 a 10 Nariadenia MiCA). Na legálne poskytovanie týchto služieb na území EÚ po nadobudnutí plnej účinnosti príslušných ustanovení musí spoločnosť Finsys disponovať povolením ako CASP, udeleným príslušným vnútroštátnym orgánom – v Slovenskej republike – Národnou bankou Slovenska.

Nariadenie DORA, zamerané na posilnenie digitálnej prevádzkovej odolnosti finančného sektora, vo svojej vecnej pôsobnosti (Článok 2(1)(h)) explicitne uvádza „poskytovateľov služieb týkajúcich sa kryptoaktív, ktorí majú povolenie podľa nariadenia MiCA“. Tým, že Finsys poskytuje **služby vyžadujúce autorizáciu podľa MiCA**, stáva sa **jednoznačne finančným subjektom spadajúcim pod reguláciu DORA**.

Veľkostné kritériá ďalej potvrdzujú **plnú aplikovateľnosť DORA**. S počtom zamestnancov 15 až 20, spoločnosť Finsys **nespĺňa definíciu mikropodniku**. Preto sa na ňu v plnom rozsahu vzťahujú všetky relevantné požiadavky nariadenia DORA, bez možnosti uplatnenia zjednodušení alebo výnimiek pre mikropodniky (ako umožňuje Článok 2(3) DORA pre vybrané povinnosti).

2.1.3.2 NIS2

Hoci existuje aj všeobecný rámec kybernetickej bezpečnosti v podobe Smernice NIS2 (EÚ) 2022/2556, pre finančné subjekty ako Finsys má Nariadenie DORA prednosť ako *lex specialis* v oblasti digitálnej prevádzkovej odolnosti a riadenia rizík IKT.

Zhrnutie:

Prístup spoločnosti Finsys k novým regulačným rámcom (DORA, MiCA) bol charakterizovaný skôr reaktívnosťou než proaktívnou prípravou. Interné aktivity zamerané na systematickú analýzu dopadov a dosiahnutie súladu boli iniciované až začiatkom roka 2025.

Pre účely tejto diplomovej práce, ktorá sa zameriava na implementáciu opatrení na posilnenie digitálnej prevádzkovej odolnosti, je teda Nariadenie (EÚ) 2022/2554 (DORA) **primárnym a najrelevantnejším legislatívnym rámcom**, ktorý definuje konkrétne povinnosti pre spoločnosť Finsys. (16) (68) (69)

2.1.4 Strategický prístup manažmentu k IKT a bezpečnosti

2.1.4.1 Význam IKT pre hlavné činnosti

Pre spoločnosť Finsys s.r.o., ktorej celý obchodný model je postavený na vývoji a prevádzke digitálnych platforiem (FinSecure Exchange, FinSecure Trader), predstavujú informačné a komunikačné technológie (IKT) absolútne jadro podnikania. IKT tu nie sú len podporným nástrojom, ale priamo esenciálnym prvkom tvorby hodnoty a poskytovania služieb klientom.

Funkčnosť, dostupnosť, výkonnosť a integrita týchto platforiem sú priamo úmerné obchodnému úspechu a reputácii spoločnosti. Akákoľvek významnejšia nedostupnosť alebo bezpečnostný incident v oblasti IKT by mal bezprostredný a závažný dopad na kontinuitu hlavných činností a dôveru zákazníkov.

2.1.4.2 Vízia/misia vo vzťahu k IKT a bezpečnosti

Spoločnosť Finsys nemá explicitne formulovanú a zdokumentovanú víziu alebo misiu, ktorá by strategicky integrovala kybernetickú bezpečnosť a digitálnu prevádzkovú odolnosť ako kľúčové piliere popri technologickej inovácii a raste. Neformálna vízia manažmentu (konateľa) sa historicky sústredila na etablovanie spoločnosti ako popredného lokálneho poskytovateľa užívateľsky prívetivých a funkčne bohatých platforiem pre obchodovanie s kryptoaktívami na slovenskom a českom trhu. Dôraz bol kladený na spoľahlivosť a dostupnosť služieb z pohľadu zákazníka a na rýchly vývoj nových funkcionalít podľa požiadaviek trhu.

2.1.4.3 Všeobecná úroveň povedomia a priority manažmentu

Manažment spoločnosti si bol vždy vedomý kritickej závislosti podnikania na IKT, najmä z pohľadu zabezpečenia nepretržitej prevádzky (dostupnosti) služieb pre klientov. Táto priorita sa odrážala v zameraní technologického úseku na stabilitu infraštruktúry a riešenie operatívnych problémov.

Avšak, strategické riadenie rizík IKT a kybernetická bezpečnosť ako samostatná disciplína neboli vnímané ako strategická priorita najvyššieho vedenia. Prevládalo skôr technokratické a operatívne vnímanie bezpečnosti – ako súbor technických opatrení

(firewall, antivírus, zálohovanie), ktorých implementácia a správa boli delegované na technologický úsek bez systematického strategického dohľadu, formálneho rámca riadenia rizík alebo definovanej bezpečnostnej stratégie schválenej vedením.

Investície do bezpečnosti boli schvaľované prevažne reaktívne, ako odpoveď na konkrétne technické potreby alebo ako súčasť nevyhnutných nákladov na prevádzku. Povedomie manažmentu o širších strategických implikáciách kybernetických rizík (finančné straty, poškodenie reputácie, regulačné sankcie) bolo pred rokom 2025 relatívne nízke.

Zaujímavým momentom vo vývoji interného vnímania rizík bolo **spustenie komplexnejšej platformy FinSecure Trader v roku 2021**. Hoci tento krok neviedol k okamžitej zmene strategického prístupu, interné diskusie v rámci technologického tímu a čiastočne aj na úrovni vedúceho daného tímu, poukázali na rastúcu zložitosť systémov a potenciálne zvýšenú expozíciu voči sofistikovanejším hrozbám.

Táto skúsenosť vytvorila isté podhubie pre neskoršie (v roku 2025) akceptovanie nevyhnutnosti zásadnejších zmien v prístupe k bezpečnosti, iniciovaných najmä externým tlakom nových regulácií ako DORA.

Zhrnutie:

Tento východiskový stav – silný dôraz na operatívnu funkčnosť IKT, avšak bez zodpovedajúceho strategického rámca riadenia kybernetickej bezpečnosti a rizík IKT na úrovni manažmentu – predstavuje kľúčový kontext pre implementáciu požiadaviek Nariadenia DORA, ktoré kladie zásadný dôraz práve na zodpovednosť riadiaceho orgánu za digitálnu prevádzkovú odolnosť. (68)

2.2 Východiskový stav kybernetickej bezpečnosti

2.2.1 Prehľad kľúčových informačných technológií a systémov

Technologická infraštruktúra a informačné systémy spoločnosti Finsys s.r.o. tvoria základ pre poskytovanie jej hlavných služieb – platforiem FinSecure Exchange a FinSecure Trader. Analýza súčasného stavu týchto systémov je nevyhnutná pre posúdenie digitálnej prevádzkovej odolnosti v kontexte nariadenia DORA.

2.2.1.1 Všeobecný opis technologickej infraštruktúry

Infraštruktúra spoločnosti Finsys kombinuje využitie externých poskytovateľov cloudových služieb s internými zdrojmi.

- **Servery a Hosting:** Produkčné prostredia pre kľúčové aplikácie FinSecure Exchange a FinSecure Trader sú prevádzkované primárne na **virtuálnych serveroch v rámci infraštruktúry ako služby (IaaS)** poskytovanej renomovaným externým dodávateľom dátového centra v EÚ. Toto riešenie poskytuje potrebnú škálovateľnosť a fyzickú bezpečnosť. Pre interné účely (vývoj, testovanie, administratíva) spoločnosť využíva aj menší počet vlastných fyzických serverov umiestnených v sídle spoločnosti.
- **Operačné systémy:** Serverové prostredie je dominantne založené na operačných systémoch **Linux** (Ubuntu Server alebo CentOS), ktoré sú využívané pre webové servery, aplikačné servery a databázové systémy. Pre internú správu používateľských účtov a niektoré administratívne funkcie sa využíva **Windows Server** s Active Directory. Na klientskych staniciach zamestnancov prevažuje OS Windows, doplnený o macOS u časti vývojárskeho tímu.
- **Sieťová infraštruktúra:** Interná sieť LAN v sídle spoločnosti je postavená na štandardných komponentoch (switche, routery) a zabezpečená centrálnym firewallom. Pre zamestnancov je k dispozícii zabezpečená Wi-Fi sieť. Segmentácia siete existuje, avšak jej granularita a komplexnosť sú základné. Pre zabezpečený vzdialený prístup sa využíva VPN.

2.2.1.2 Kľúčové informačné systémy

Identifikácia a pochopenie kľúčových systémov je esenciálna, nakoľko práve tieto systémy sú najrelevantnejšie z pohľadu dopadov prípadných incidentov a požiadaviek DORA.

- **Core Aplikácie (FinSecure Exchange a FinSecure Trader):** Tieto dve webové aplikácie predstavujú kritické informačné systémy spoločnosti. Sú vyvinuté interne s využitím moderných webových technológií (PHP/Node.js backend, JavaScript frontend framework – React). Využívajú relačné databázy

(PostgreSQL) pre uchovávanie transakčných dát a údajov klientov, a sú integrované s rôznymi externými API (pre získavanie trhových dát, napojenie na platobné brány). Zabezpečujú kompletný proces registrácie klientov, vkladov/výberov prostriedkov, zadávania a párovania obchodných pokynov a správu klientskych portfólií. Ich dostupnosť a integrita sú životne dôležité.

- **Interné podporné systémy:** Spoločnosť nevyužíva komplexný integrovaný ERP systém. Pre podporu interných procesov slúžia samostatné systémy:
    - **Účtovný softvér:** Štandardný komerčný účtovný systém využívaný pre finančné účtovníctvo a reporting (Pohoda).
    - **Nástroje pre vývoj a spoluprácu:** Systém pre správu verzií (Git), nástroje pre riadenie projektov a úloh (Jira), interná e-mailová komunikácia a úložisko dokumentov.
    - **Monitorovacie a logovacie nástroje:** Ako bolo uvedené v kapitole *2.1.2.3*, technologický tím spravuje interne adaptovanú kombináciu open-source nástrojov pre monitoring sieťovej prevádzky, výkonu systémov a zber logov (Prometheus, Grafana).

2.2.1.3 Stratégia zálohovania

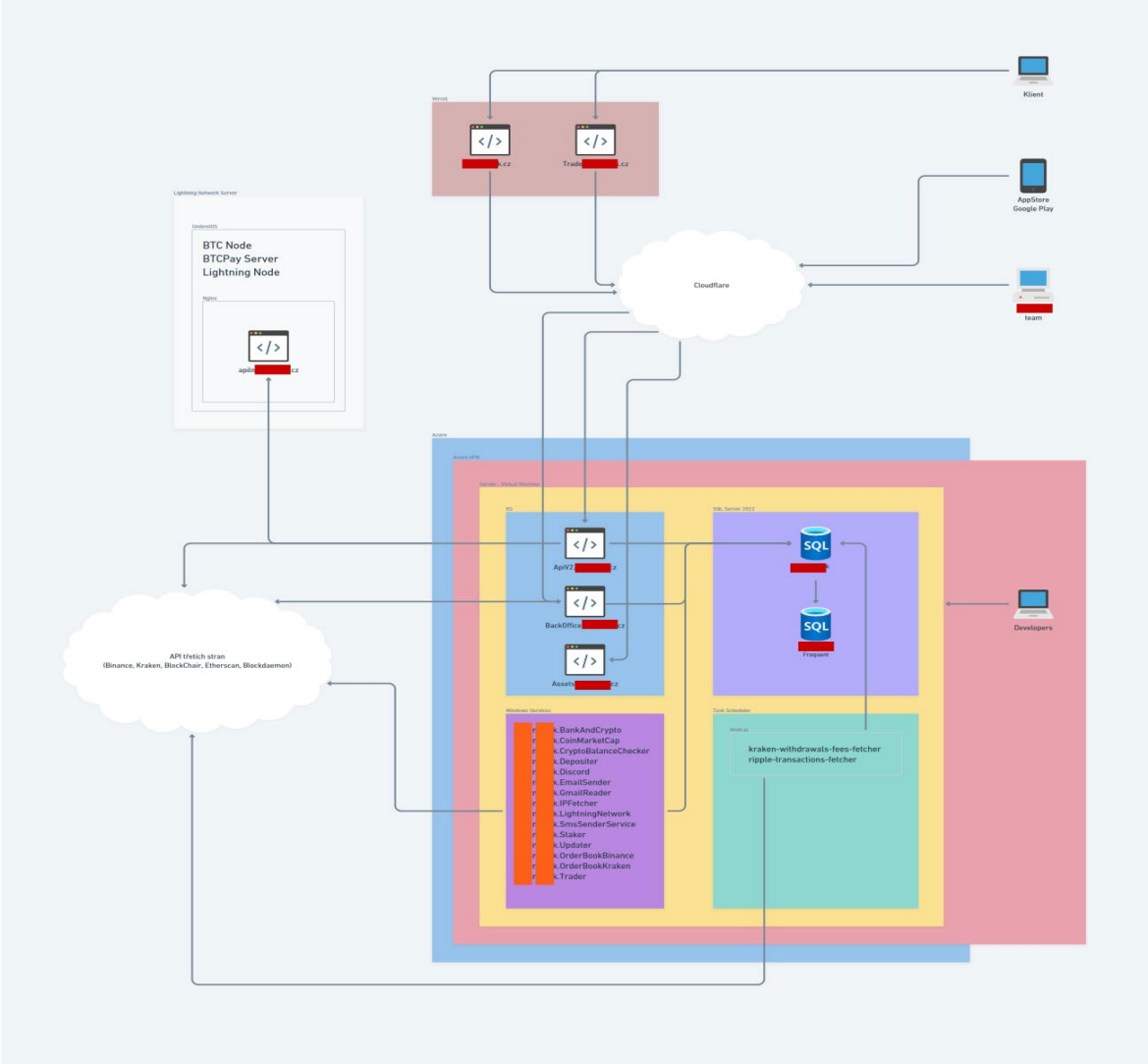
Základná stratégia zálohovania dát je implementovaná a spravovaná technologickým úsekom. Zameriava sa na ochranu dát kritických systémov:

- Pravidelné (typicky denné) zálohy databáz a konfiguračných súborov kľúčových aplikácií a serverov.
- Využívanie externého cloudového úložiska pre geograficky oddelené uloženie záloh (off-site backup).
- Definovaná základná retenčná politika záloh (uchovávanie denných záloh po dobu 14 dní, týždenných 2 mesiace, mesačných 2 roky).
- Proces obnovy dát je čiastočne zdokumentovaný, pričom pravidelné a komplexné testovanie obnovy zo záloh sa vykonáva skôr sporadicky.

Kľúčové **kryptografické materiály** (šifrovacie kľúče, certifikáty, seed phrases a recovery kódy, HMAC tajomstvá) sú **ukladané na fyzické médium v šifrovanej podobe**. Toto médium je následne v pravidelných intervaloch (týždenne) odovzdávané priamo konateľovi spoločnosti, ktorý zabezpečuje jeho uloženie na bezpečnom mieste mimo sídla firmy. Tento prístup, hoci neštandardný, reflektuje snahu o dodatočnú ochranu pred rizikami ako ransomware alebo kompromitácia cloudových účtov.

Zhrnutie:

Prehľad týchto technológií a systémov tvorí základ pre detailnejšiu analýzu rizík a hodnotenie súladu s požiadavkami Nariadenia DORA v nasledujúcich kapitolách. (68)



Obrázok č. 57: Architektúra a prepojenia kľúčových IT systémov a infraštruktúry spoločnosti Finsys s.r.o. (Zdroj: Vlastné spracovanie)

2.2.2 Základný prehľad stavu kybernetickej bezpečnosti

Táto podkapitola poskytuje súhrnný prehľad východiskového stavu kybernetickej bezpečnosti v spoločnosti Finsys s.r.o. pred implementáciou opatrení vyplývajúcich z Nariadenia DORA. Identifikuje existujúce organizačné zabezpečenie, implementované opatrenia a zaužívané prístupy v kľúčových oblastiach bezpečnosti.

2.2.1.4 Existujúce organizačné zabezpečenie

Ako bolo detailne opísané v kapitole 2.1.2, spoločnosť Finsys nemá formalizovanú funkciu riadenia kybernetickej bezpečnosti ani dedikovanú bezpečnostnú rolu (napr. CISO, manažér kybernetickej bezpečnosti). Zodpovednosti sú primárne implicitne delegované na technologický úsek:

- **Vedúci technologického úseku:** Zastrešuje dohľad nad základnými technickými bezpečnostnými opatreniami a operatívnym riešením problémov.
- **Technologický úsek (Tím):** Zodpovedá za praktickú implementáciu a správu technických opatrení (správa sietí, serverov, účtov, nasadzovanie nástrojov).
- **Najvyššie vedenie (Konateľ):** Nesie konečnú zodpovednosť, avšak bez hlbšieho strategického zapojenia do riadenia bezpečnostných rizík.

Tento model vedie k reaktívnemu prístupu a absencii proaktívneho, rizikami riadeného bezpečnostného programu.

2.2.1.5 Stručný prehľad implementovaných bezpečnostných opatrení

Napriek absencii formálneho rámca sú v spoločnosti implementované niektoré základné bezpečnostné opatrenia:

- **Fyzická bezpečnosť:** Kancelárske priestory spoločnosti sú zabezpečené štandardnými prostriedkami (uzamykateľné dvere, alarm). Fyzická bezpečnosť on-premise serverov je riešená ich umiestnením v uzamknutej miestnosti s kontrolovaným prístupom. Bezpečnosť produkčnej infraštruktúry hostovanej externe závisí od bezpečnostných štandardov a certifikácií poskytovateľa IaaS.

- **Riadenie prístupov a identít (IAM):** Existuje proces pre zriaďovanie, úpravu a rušenie používateľských účtov spravovaný technologickým tímom. Pre interných používateľov sa využíva Active Directory. Základné politiky pre heslá sú vynucované. Prístupové oprávnenia sú prideľované na základe pracovnej roly, avšak proces revízie oprávnení nie je formalizovaný. Pre prístup klientov k platformám je implementovaná dvojfaktorová autentifikácia (2FA), čo predstavuje dôležité bezpečnostné opatrenie. Využívanie 2FA pre interné systémy alebo administrátorské prístupy nie je plošne zavedené.
- **Základné bezpečnostné nástroje:** Spoločnosť využíva štandardné technológie ako centrálny sieťový firewall na perimetri siete, antivírusové riešenie na koncových staniciach a serveroch, VPN pre zabezpečený vzdialený prístup a základné nástroje pre monitoring a logovanie (interne adaptovaná kombinácia open-source riešení). Pravidelná aplikácia bezpečnostných aktualizácií (patch management) je súčasťou činností technologického tímu.

2.2.1.6 Všeobecný prístup k riešeniu incidentov, kontinuite a dodávateľom

V oblastiach vyžadujúcich procesný prístup sú zjavné medzery:

- **Riešenie bezpečnostných incidentov:** Prístup je primárne reaktívny. Technologický tím rieši vzniknuté problémy a bezpečnostné alerty s cieľom čo najrýchlejšej obnovy služby. Neexistuje formalizovaný proces klasifikácie incidentov, eskalácie, koordinovanej reakcie, forenznej analýzy alebo dokumentácie získaných ponaučení (lessons learned).
- **Kontinuita činností (Business Continuity):** Okrem základného zálohovania dát (viď kap. 2.2.1.3) spoločnosť nemá vypracované formálne plány kontinuity činností (BCP) ani plány obnovy po havárii (DRP) pre kľúčové procesy a systémy. Spolieha sa na odolnosť infraštruktúry externého IaaS poskytovateľa a schopnosť technologického tímu obnoviť systémy zo záloh. Testovanie scenárov výpadku alebo havárie sa nevykonáva.

- **Riadenie dodávateľov :** Spoločnosť využíva kľúčových externých dodávateľov (IaaS provider, účtovný softvér). Bezpečnostné aspekty sú riešené najmä na úrovni štandardných zmluvných ustanovení. Systematický proces hodnotenia a riadenia rizík spojených s dodávateľmi IKT (third-party risk management) nie je implementovaný.

2.2.1.7 Súčasná úroveň bezpečnostného povedomia a školení

Ako bolo uvedené v kapitole 2.1.2.3, všeobecné povedomie zamestnancov o aktuálnych kybernetických hrozbách a bezpečných praktikách je na nízkej úrovni. Neexistuje program pravidelných bezpečnostných školení. Hlásenie bezpečnostných podozrení alebo incidentov zo strany bežných zamestnancov prebieha neformálne a ad-hoc. Výnimku z tohto stavu predstavuje **každoročná simulácia phishingového útoku pre všetkých zamestnancov, organizovanou externou firmou**, vrátane krátkeho následného vyhodnotenia a poučenia. Hoci ide o izolovanú aktivitu, predstavuje jediný formalizovaný prvok zvyšovania povedomia v spoločnosti.

Zhrnutie:

Tento celkový obraz ukazuje spoločnosť so zavedenými základnými technickými kontrolami, avšak s výraznými nedostatkami v oblasti bezpečnostného riadenia (governance), formalizovaných procesov a celkovej bezpečnostnej kultúry. (68)

2.3 Zhodnotenie súčasného stavu a identifikácia medzier

2.3.1 Identifikácia medzier voči požiadavkám (GAP Analýza)

Táto podkapitola predstavuje porovnanie súčasného stavu fungovania spoločnosti Finsys s.r.o., opísaného v predchádzajúcich častiach kapitoly 2, s kľúčovými požiadavkami Nariadenia (EÚ) 2022/2554 o digitálnej prevádzkovej odolnosti finančného sektora (DORA). Cieľom tejto GAP analýzy je identifikovať hlavné oblasti nesúladu a nedostatky, ktoré je potrebné adresovať na dosiahnutie zhody s touto reguláciou. Zistenia tvoria priamy podklad pre návrhovú časť tejto diplomovej práce. Porovnanie je štruktúrované podľa hlavných tematických oblastí DORA.

2.3.1.1 Riadenie (Governance) a Rámec riadenia rizík IKT

- **Požiadavka DORA:** Vyžaduje, aby riadiaci orgán (top management) niesol konečnú zodpovednosť za riadenie rizík IKT, definoval, schválil a dohliadal na implementáciu komplexného a zdokumentovaného rámca riadenia rizík IKT, vrátane stratégie digitálnej prevádzkovej odolnosti.
- **Súčasný stav Finsys:** Riadiaci orgán (konateľ) sa zameriava primárne na operatívu a produktový vývoj. Neexistuje formálne schválená stratégia digitálnej odolnosti ani komplexný rámec riadenia rizík IKT. Riadenie bezpečnosti je delegované na technologický úsek s reaktívnym prístupom, chýbajú formalizované bezpečnostné roly a zodpovednosti.
- **Identifikovaná medzera:** Zásadný nedostatok v oblasti strategického riadenia a zodpovednosti najvyššieho vedenia za riziká IKT. Absencia formálneho, zdokumentovaného a schváleného rámca riadenia rizík IKT.

2.3.1.2 Riadenie rizík IKT (Procesy a Opatrenia)

- **Požiadavka DORA:** Vyžaduje zavedenie procesov pre identifikáciu, klasifikáciu a hodnotenie rizík IKT, implementáciu primeraných bezpečnostných politík a opatrení na ochranu, detekciu, reakciu a obnovu, vrátane zálohovania a obnovy, riadenia zmien a bezpečnostného povedomia.
- **Súčasný stav Finsys:** Systematické hodnotenie rizík IKT sa nevykonáva. Bezpečnostné politiky sú neúplné a neformalizované. Existujú základné technické opatrenia (firewall, AV, zálohovanie, 2FA, patch management), ale chýba komplexný a integrovaný prístup. Detekcia je založená na základných nástrojoch, procesy reakcie a obnovy (okrem základného zálohovania) nie sú formalizované.
- **Identifikovaná medzera:** Chýbajúci systematický proces riadenia rizík IKT. Nedostatočne definované alebo chýbajúce bezpečnostné politiky a procedúry. Potreba posilnenia a formalizácie opatrení v oblasti ochrany, detekcie, reakcie a obnovy. Špecifický prístup k *air-gapped zálohám* spravovaným priamo konateľom, hoci predstavuje zaujímavú dodatočnú ochranu, podčiarkuje absenciu komplexného, zdokumentovaného a testovaného plánu kontinuity činností a

obnovy po havárii (BCP/DRP), ktorý by sa nemal spoliehať na jednotlivca a neštandardizované postupy.

2.3.1.3 Riadenie, klasifikácia a oznamovanie incidentov súvisiacich s IKT

- **Požiadavka DORA:** Vyžaduje zavedenie procesu riadenia incidentov IKT, vrátane ich detekcie, riadenia, zaznamenávania, klasifikácie (najmä identifikácie závažných incidentov) a oznamovania závažných incidentov príslušným orgánom.
- **Súčasný stav Finsys:** Prístup k riešeniu incidentov je reaktívny, zameraný na rýchlu obnovu. Chýba formalizovaný proces, systém klasifikácie incidentov podľa ich dopadu a mechanizmus pre včasné oznamovanie regulačným orgánom.
- **Identifikovaná medzera:** Absencia komplexného a zdokumentovaného procesu riadenia incidentov IKT vrátane klasifikácie a oznamovania v súlade s požiadavkami DORA.

2.3.1.4 Testovanie digitálnej prevádzkovej odolnosti

- **Požiadavka DORA:** Vyžaduje zavedenie programu testovania digitálnej prevádzkovej odolnosti primeraného veľkosti a rizikovému profilu, ktorý zahŕňa aspoň ročné vykonávanie základných testov.
- **Súčasný stav Finsys:** Spoločnosť nevykonáva pravidelné hodnotenia zraniteľností ani nevykonáva pravidelné penetračné testy. Neexistuje formalizovaný program testovania odolnosti. Testovanie sa obmedzuje na sporadické pokusy o obnovu zo záloh.
- **Identifikovaná medzera:** Chýbajúci program testovania digitálnej prevádzkovej odolnosti vrátane pravidelného vykonávania relevantných testov.

2.3.1.5 Riadenie rizika tretích strán v oblasti IKT

- **Požiadavka DORA:** Vyžaduje, aby finančné subjekty riadili riziko IKT spojené s využívaním tretích strán (dodávateľov IKT služieb), vrátane stratégie riadenia tohto rizika, vedenia registra informácií o zmluvách, hodnotenia rizík dodávateľov a zahrnutia špecifických zmluvných ustanovení.

- **Súčasný stav Finsys :** Spoločnosť využíva kľúčových dodávateľov IKT (najmä IaaS providera). Neexistuje však formalizovaná stratégia ani proces pre riadenie rizika tretích strán. Chýba centrálny register informácií a systematické hodnotenie dodávateľov či revízia zmlúv z pohľadu požiadaviek DORA.
- **Identifikovaná medzera:** Absencia komplexného prístupu k riadeniu rizika IKT tretích strán v súlade s DORA.

Záver GAP analýzy

Porovnanie súčasného stavu spoločnosti Finsys s požiadavkami nariadenia DORA odhalilo **významné medzery prakticky vo všetkých kľúčových oblastiach** regulácie. Najzávažnejšie nedostatky sa týkajú:

- **Strategického riadenia a governance:** Chýbajúce zapojenie vedenia, formálny rámec riadenia rizík IKT a definované zodpovednosti.
- **Systematických procesov:** Absencia formalizovaných a zdokumentovaných procesov pre riadenie rizík, incidentov, kontinuity činností, testovania odolnosti a riadenia rizika tretích strán.
- **Dokumentácie:** Nedostatočná alebo chýbajúca dokumentácia politík, procedúr, výsledkov hodnotení a testov.

Hoci spoločnosť disponuje základnými technickými opatreniami a funkčnou infraštruktúrou, súčasný prístup k riadeniu digitálnej prevádzkovej odolnosti je nedostatočný a vyžaduje si zásadnú transformáciu na dosiahnutie súladu s nariadením DORA. Tieto identifikované medzery predstavujú východiská pre návrh konkrétnych odporúčaní a riešení v nasledujúcej kapitole tejto práce. (16) (68)

DORA Gap Assessment

Chapter	Article	Requirement ID	Requirement	Compliance
CHAPTER I: General provisions	Article 4: Proportionality principle	1	1. Financial entities shall implement the rules laid down in Chapter II in accordance with the principle of proportionality, taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations.	Partially Compliant
CHAPTER I: General provisions	Article 4: Proportionality principle	2	2. In addition, the application by financial entities of Chapters III, IV and V, Section I, shall be proportionate to their size and overall risk profile, and to the nature, scale and complexity of their services, activities and operations, as specifically provided for in the relevant rules of those Chapters.	Not Compliant
CHAPTER I: General provisions	Article 4: Proportionality principle	3	3. The competent authorities shall consider the application of the proportionality principle by financial entities when reviewing the consistency of the ICT risk management framework on the basis of the reports submitted upon the request of competent authorities pursuant to Article 6(5) and Article 16(2).	Not Applicable
CHAPTER II: ICT risk management	Article 5: Governance and organisation	4	1. Financial entities shall have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk, in accordance with Article 6(4), in order to achieve a high level of digital operational resilience.	Not Compliant
CHAPTER II: ICT risk management	Article 5: Governance and organisation	5	2. The management body of the financial entity shall define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework referred to in Article 6(1).	Not Compliant
CHAPTER II: ICT risk management	Article 5: Governance and organisation	6	For the purposes of the first subparagraph, the management body shall: (a) bear the ultimate responsibility for managing the financial entity's ICT risk;	Partially Compliant
CHAPTER II: ICT risk management	Article 5: Governance and organisation	7	For the purposes of the first subparagraph, the management body shall: (b) put in place policies that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality, of data;	Partially Compliant
CHAPTER II: ICT risk management	Article 5: Governance and organisation	8	For the purposes of the first subparagraph, the management body shall: (c) set clear roles and responsibilities for all ICT-related functions and establish appropriate	Not Compliant

Obrázok č. 58: Výňatok z DORA Gap Assessment (Zdroj: Vlastné spracovanie)

2.3.2 SWOT analýza

2.3.2.1 Silné stránky (Strengths – Interné, Pozitívne)

- **Funkčné a zavedené produkty:** Prevádzka dvoch kľúčových platforiem (FinSecure Exchange, FinSecure Trader) s vybudovanou klientskou základňou na lokálnom trhu.
- **Technologická expertíza tímu:** Interný technologický tím, schopný vyvíjať, spravovať a prevádzkovať komplexné FinTech platformy.
- **Znalosť lokálneho trhu:** Dobrá orientácia na potreby slovenského a českého trhu (jazyk, EUR/CZK transakcie, lokálna podpora, integrácia s bankami).
- **Fungujúce základné bezpečnostné prvky:** Existencia základných bezpečnostných opatrení ako sieťový firewall, antivírusová ochrana, patch management a základné zálohovanie.

- **Špecifické bezpečnostné opatrenia:** Existencia unikátnych opatrení ako každoročný phishingový test pre zamestnancov a air-gapped záloha najkritickejších dát pod dohľadom konateľa.
- **Využívanie open-source nástrojov:** Flexibilné a nákladovo efektívne riešenia pre monitoring a logovanie (hoci vyžadujúce internú expertízu a údržbu).

2.3.2.2 Slabé stránky (Weaknesses – Interné, Negatívne)

- **Absencia strategického riadenia bezpečnosti:** Nedostatočné zapojenie a nízke povedomie manažmentu (konateľa) o rizikách IKT.
- **Chýbajúci rámec riadenia IKT rizík:** Neexistencia komplexného, zdokumentovaného a schváleného bezpečnostného rámca podľa požiadaviek DORA.
- **Deficit v bezpečnostnej governance:** Absencia dedikovanej bezpečnostnej roly a formálne definovaných zodpovedností za kybernetickú bezpečnosť.
- **Absencia formálnych procesov:** Chýbajúce alebo neformalizované kľúčové procesy riadenia rizík, incidentov, kontinuity činností (BCP/DRP), testovania odolnosti a riadenia rizika tretích strán.
- **Nedostatočná dokumentácia:** Chýbajúca alebo neúplná dokumentácia politík, procedúr, konfigurácií, výsledkov testov a analýz.
- **Absencia programu bezpečnostných školení:** Absencia systematického školenia zamestnancov a nízka úroveň všeobecného bezpečnostného povedomia (okrem phishing testu).

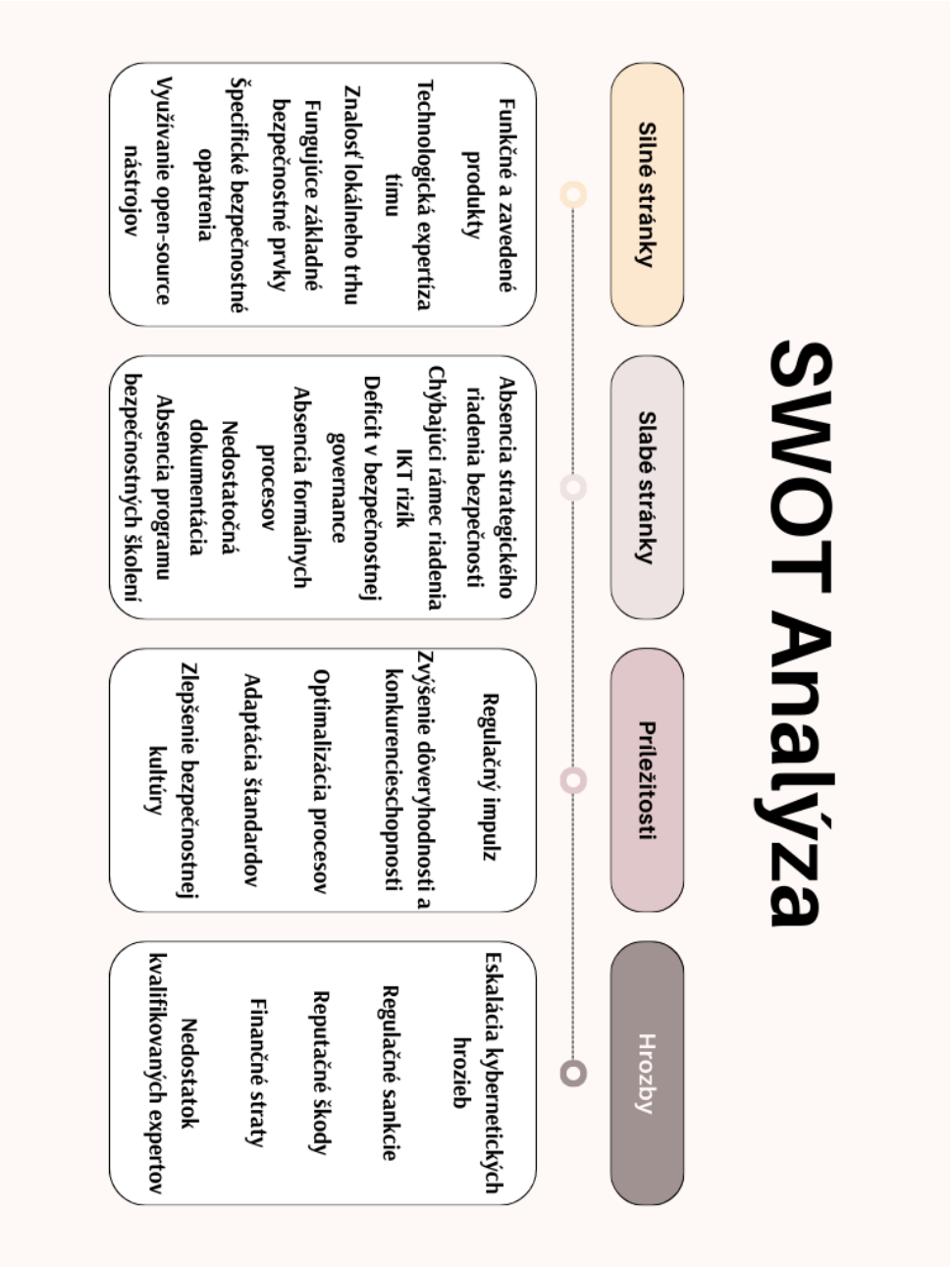
2.3.2.3 Príležitosti (Opportunities – Externé, Pozitívne)

- **Regulačný impulz (DORA/MiCA):** Vnímanie nových regulácií ako príležitosti na zásadné zlepšenie digitálnej odolnosti, bezpečnosti a interných procesov, nielen ako nákladovú položku.
- **Zvýšenie dôveryhodnosti a konkurencieschopnosti:** Dosiahnutie súladu s DORA môže posilniť dôveru klientov a partnerov a stať sa konkurenčnou výhodou voči menej pripraveným subjektom.

- **Optimalizácia procesov:** Implementácia DORA požiadaviek môže viesť k zefektívneniu prevádzky a zníženiu rizík.
- **Adaptácia štandardov:** Príležitosť implementovať a zaviesť využívanie medzinárodne uznávaných štandardov (ISO 27001, NIST CSF) ako súčasť dosahovania súladu s DORA.
- **Zlepšenie bezpečnostnej kultúry:** Využitie implementácie DORA ako katalyzátora pre budovanie silnejšej bezpečnostnej kultúry v celej spoločnosti.

2.3.2.4 Hrozby (Threats – Externé, Negatívne)

- **Eskalácia kybernetických hrozieb:** Neustále sa vyvíjajúce a čoraz sofistikovanejšie kybernetické útoky cielené na FinTech a krypto sektor (ransomware, phishing, útoky na platformy).
- **Regulačné sankcie:** Riziko finančných pokút, nápravných opatrení alebo až odobratia licencie (podľa MiCA) v prípade nedodržania požiadaviek DORA a MiCA.
- **Reputačné škody:** Významné poškodenie dobrého mena a strata dôvery klientov v prípade úspešného kybernetického útoku alebo dlhodobého výpadku služieb.
- **Finančné straty:** Priame finančné straty spôsobené únikom dát, krádežou aktív, nákladmi na obnovu systémov, právnymi spormi alebo pokutami.
- **Nedostatok kvalifikovaných expertov:** Problém nájsť a udržať si kvalifikovaných odborníkov na kybernetickú bezpečnosť a DORA compliance na trhu práce.



Obrázok č. 59: SWOT analýza kybernetickej bezpečnosti spoločnosti Finsys s.r.o. – silné a slabé stránky, príležitosti a hrozby (Zdroj: Vlastné spracovanie)

Táto SWOT analýza poskytuje strategický prehľad východiskovej pozície spoločnosti Finsys a identifikuje kľúčové interné a externé faktory, ktoré je potrebné zohľadniť pri návrhu riešení na dosiahnutie súladu s Nariadením DORA a celkové posilnenie kybernetickej odolnosti. (68)

3 NÁVRH RIEŠENIA

3.1 Návrh stratégie a bezpečnostného rámca digitálnej prevádzkovej odolnosti

3.1.1 Návrh stratégie digitálnej prevádzkovej odolnosti

Vedenie spoločnosti Finsys prijalo v súlade s požiadavkami nariadenia DORA formálnu **Stratégiu digitálnej prevádzkovej odolnosti**, ktorej cieľom je zabezpečiť nepretržité a spoľahlivé poskytovanie finančných a softvérových služieb aj počas významných prevádzkových narušení v oblasti IKT.

Stratégia je zosúladená s obchodnými cieľmi spoločnosti a nadväzuje na jej strategické priority v oblasti digitalizácie a kybernetickej bezpečnosti.

Tento strategický dokument bol vytvorený autorom tejto práce a **schválený vedúcim orgánom**.

Stratégia je členená do šiestich základných častí:

I. Úvod a účel stratégie

Úvodná časť definuje záväznosť dokumentu, jeho strategickú úlohu v rámci rámca riadenia IKT rizík a jeho prepojenie na požiadavky nariadenia DORA.

II. Štruktúra vnútorných predpisov

Táto časť sumarizuje súbor nadväzujúcich interných dokumentov upravujúcich riadenie rizík, kontinuitu prevádzky, bezpečnostné politiky, incident manažment a správu tretích strán v oblasti IKT.

III. Ciele IKT

Zavedenie stratégie má za cieľ podporiť obchodné a technologické ciele spoločnosti, vrátane zvýšenia stability a efektivity technologických procesov, minimalizácie výpadkov IKT systémov, zvyšovania dôvery klientov, ako aj zabezpečenia súladu s regulačnými požiadavkami a kybernetickej gramotnosti zamestnancov.

IV. Architektúra IKT

Architektúra je vizualizovaná prostredníctvom schémy siete, ktorá je súčasťou *Bezpečnostnej smernice*. Táto schéma znázorňuje logické rozdelenie systémov, segmentáciu infraštruktúry a umiestnenie bezpečnostných komponentov.

V. Zavedené mechanizmy a opatrenia

Súčasťou stratégie sú aj technické a organizačné opatrenia, ako je viacúrovňová autentifikácia, šifrovanie, segmentácia siete, pravidelné školenia, plánovanie obnovy a prevencia proti incidentom. Tieto opatrenia slúžia na posilnenie odolnosti systémov voči narušeniam.

VI. Rozvoj IKT

Dokument definuje aj smerovanie rozvoja digitálnej infraštruktúry, vrátane zavádzania nových technológií, automatizácie bezpečnostných procesov, optimalizácie pracovných postupov a zvyšovania interoperability medzi systémami.

Stratégia digitálnej prevádzkovej odolnosti tak predstavuje kľúčový nástroj riadenia IKT rizík v spoločnosti Finsys a tvorí základ pre ďalšie rozpracovanie súvisiacich politík a procesov.

3.1.2 Návrh bezpečnostnej smernice

Spoločnosť Finsys prijala v súlade s požiadavkami nariadenia DORA formálnu **Bezpečnostnú smernicu**, ktorá tvorí základný dokument rámca informačnej a kybernetickej bezpečnosti. Tento dokument systematizuje kľúčové pravidlá a princípy, ktoré upravujú bezpečnostné správanie a procesy v rámci celej organizácie.

Bezpečnostná smernica bola vytvorená autorom tejto práce a schválená vedúcim orgánom spoločnosti a je záväzná pre všetkých zamestnancov a externých partnerov. Je úzko previazaná so *Stratégiou digitálnej prevádzkovej odolnosti* a tvorí jej operatívne rozšírenie.

Dokument je členený do ôsmich základných oblastí:

I. Politika v oblasti ľudských zdrojov

Definuje bezpečnostné požiadavky na zamestnancov a tretie strany, zohľadňuje ich roly, zodpovednosti, ako aj pravidlá nástupu, zmeny a ukončenia prístupu.

II. Komunikačná stratégia

Špecifikuje pravidlá pre internú a externú komunikáciu počas incidentov a krízových situácií, vrátane zloženia krízového tímu a spôsobov komunikácie s klientmi, orgánmi dohľadu a verejnosťou.

III. Politika správy identít a riadenia prístupu

Upravuje procesy správy účtov, prideľovania prístupových práv, zásady tvorby hesiel a používania viacfaktorovej autentifikácie.

IV. Politika šifrovania

Stanovuje pravidlá pre šifrovanie dát v normálnom stave a pri prenose, s cieľom zabezpečiť dôvernosť a integritu informácií.

V. Bezpečnosť operácií IKT

Zameriava sa na oddelenie produkčných a testovacích prostredí, riadenie kapacity a výkonu, manažment zraniteľností, bezpečnosť systémov a uchovávanie protokolov.

VI. Bezpečnosť sietí

Rieši pravidlá a technické opatrenia na ochranu sieťovej infraštruktúry, vrátane segmentácie, monitorovania a kontroly prístupu.

VII. Riadenie projektov

Zahŕňa pravidlá pre vývoj a údržbu systémov, procesy schvaľovania zmien a zabezpečenie bezpečnosti v rámci životného cyklu projektov.

VIII. Politika fyzickej a environmentálnej bezpečnosti

Zahŕňa pravidlá pre fyzickú ochranu priestorov, implementáciu zásady "čistého stola" a environmentálne opatrenia na ochranu technológie.

Bezpečnostná smernica tak predstavuje komplementárny dokument k stratégii DPO, pričom zabezpečuje každodennú aplikáciu princípov bezpečnosti v technickej a organizačnej rovine. Slúži ako základ pre tvorbu špecializovaných postupov a nástrojov na zaistenie dôvernosti, integrity a dostupnosti informácií.

3.2 Návrh rámca riadenia rizík v oblasti IKT

3.2.1 Návrh procesu identifikácie, klasifikácie a hodnotenia aktív a funkcií

V rámci implementácie rámca riadenia IKT rizík spoločnosť Finsys zaviedla **systematizovaný proces identifikácie, evidencie, klasifikácie a hodnotenia všetkých relevantných aktív a kritických funkcií**. Cieľom tohto procesu je zabezpečiť úplnú znalosť o informačných aktívach, úrovni citlivosti, a závislostiach od IKT systémov. Tento proces bol zavedený autorom tejto práce.

Identifikácia a evidencia aktív a funkcií

Proces začína komplexnou identifikáciou všetkých relevantných aktív, ktoré sú rozdelené do dvoch kategórií:

- **Informačné aktíva** (napr. dáta, databázy, dokumentácia)
- **Podporné aktíva** (napr. servery, pracovné stanice, sieťové prvky, cloudové služby)

Pre každé podporné aktívum sa eviduje jedinečný identifikátor, fyzické alebo logické umiestnenie, väzby na IKT funkcie a prípadná expozícia voči externému prostrediu.

Rovnako sú identifikované všetky **kritické a dôležité funkcie**, ktoré priamo ovplyvňujú poskytovanie služieb alebo vnútorné prevádzkové procesy. Ku každej funkcii je priradená jej priorita obnovy, ktorá je stanovená na základe analýzy vplyvu výpadku na chod spoločnosti a jej reputáciu.

Klasifikácia aktív a funkcií

Každé identifikované informačné a podporné aktívum je klasifikované podľa nasledovných kritérií:

- **Dôvernosť** – potreba ochrany pred neoprávneným prístupom
- **Integrita** – požiadavka na presnosť a úplnosť údajov,
- **Dostupnosť** – potreba dostupnosti aktíva pre kritické procesy.

ID	Informačné aktívum	Špecifikácia	Dostupnosť	Dôvernosť	Integrita
A1	Klientské dáta	Všetky klientske dáta (dokumenty KYC, transakcie, ...)	3	3	3
A2	Finančné aktíva - transakčné data	Zostatky fiat a kryptomien klientov	3	4	4
A3	Finančné aktíva - prístupy	Privátne kľúče	4	4	4
A4	Finančné aktíva - prístupy	API kľúče bánk alebo búrz	4	4	4
A5	Provozné dáta	Databáza klientov, transakcií	3	3	3
A6	Interné projekty a vývojové dáta	Repozitáre kódov, backlogy, testovacie scenáre	3	3	4
A7	Regulatórne a bezpečnostné dáta	Záznamy auditov, interné smernice, AML/CFT hlásenia	2	3	3
A8	Webová platforma - verejná časť	Verejné API, trhové údaje	3	1	2
A9	Webová platforma - klienstká časť	Prístup klientov, zadávanie pokynov, dashboard	4	3	3
A10	Účtovné údaje	Faktury,výkazy, nákladové záznamy	3	3	3

Obrázok č.60 Hodnotenie informačných aktív podľa dostupnosti, dôvernosti a integrity (Zdroj: Vlastné spracovanie)

ID	Podporné aktívum	Kategória	Dostupnosť	Dôvernosť	Integrita	Aké funkcie sú aktívom podporované?	Poskytovateľ služieb IKT	Vlastník aktíva	Fyzické alebo logické umiestnenie aktíva	Je alebo môže byť aktívum vystavené sieťam (vrátane internetu)?
P1	Cloud Azure	Cloud - HW	3	4	4	F2,F3,F5,F6,F7,F8,F9,F10,F20,F23,F34,F41,F42,F43,F45,F46,F47,F48,F49,F51,F52,F53,F54,F55,F60,F64,F70,F73,F74,F75,F76,F77,F79,F80,F102,F103,F105,F106,F107,F110,F120,F121,F122,F130	Microsoft	Finsys	Logické	Ano
P2	Azure VPN	Cloud - HW	2	1	4	F74,F75	Microsoft	Finsys	Logické	Ano
P3	Azure WEB server	Cloud - HW	3	2	4	F1,F2,F3,F4,F5,F6,F7,F8,F9,F10,F20,F21,F22,F23,F24,F34,F36,F37,F38,F39,F40,F42,F43,F44,F45,F46,F47,F49,F50,F51,F52,F54,F55,F63,F73,F101,F102,F103,F104,F105,F107,F108,F121,F130	Microsoft	Finsys	Logické	Ano
P4	Azure SQL server	Cloud - HW	3	4	4	F1,F2,F3,F4,F5,F6,F7,F8,F9,F10,F20,F21,F22,F23,F24,F34,F36,F37,F38,F39,F40,F42,F43,F44,F45,F46,F47,F49,F50,F51,F52,F54,F55,F63,F73,F101,F102,F103,F104,F105,F107,F108,F121,F130	Microsoft	Finsys	Logické	Ano
P6	Azure Storage	Cloud - HW	2	3	3	F70,F71,F54,F105	Microsoft	Finsys	Logické	Ano
P7	Azure Monitor Application Insights	Cloud - HW	1	1	1	F76,F80	Microsoft	Finsys	Logické	Ano
P8	Confluence	Cloud - HW	1	2	2	F30,F31,F32,F33,F47,F48,F50,F53,F54,F60,F61,F62,F63,F64,F79,F122	Atlassian	Finsys	Logické	Ano
P9	Azure DevOps	Cloud - HW	1	4	2	F30,F31,F32,F33,F54,F60,F61,F62,F63,F64,F79	Microsoft	Finsys	Logické	Ano
P10	Google Workspace	Cloud - HW	1	4	2	F30,F31,F32,F33,F35,F36,F37,F38,F39,F40,F41,F44,F45,F47,F53	Google	Finsys	Logické	Ano
P11	Google Gmail	Cloud - HW	2	4	2	F30,F33,F40,F100,F103	Google	Finsys	Logické	Ano
P12	Dátová schránka	Cloud - HW	1	3	1	F35,F40	MIRRI SR	Finsys	Logické	Ano

Obrázok č.61 Klasifikácia podporných aktív podľa CIA triády a ich prepojenie na kľúčové funkcie časť 1. (Zdroj: Vlastné spracovanie)

P12	Dátová schránka	**Cloud - HW**	1	3	1	F35,F40	MIRRI SR	Finsys	Logické	Áno
P13	Vývojové prostredie	**Cloud - HW**	1	1	1	F62,F63	Microsoft	Finsys	Logické	Áno
P14	DevOps GIT	**Cloud - HW**	1	2	4	F62,F64	Microsoft	Finsys	Logické	Áno
P15	Vercel	**Cloud - HW**	3	1	3	F74,F75	Vercel	Finsys	Logické	Áno
P16	Cloudflare	**Cloud - HW**	3	1	4	F75,F80	Cloudflare	Finsys	Logické	Áno
P20	FinSecure.BankAndCrypto	**IS - Windows services - API 3.stran**	3	1	4	F1,F2,F3,F5,F7	Finsys	Finsys	Logické	Áno
P21	FinSecure.CryptoBalanceChecker	**IS - Windows services - API 3.stran**	3	1	4	F4,F6,F7,F9,F10,F21,F22	Finsys	Finsys	Logické	Áno
P22	FinSecure.Depositer	**IS - Windows services - API 3.stran**	3	1	4	F6,F7	Finsys	Finsys	Logické	Áno
P23	FinSecure.Discord	**IS - Windows services - API 3.stran**	1	1	1	F3,F4,F8,F9,F10	Finsys	Finsys	Logické	Áno
P24	FinSecure.EmailSenderService	**IS - Windows services - API 3.stran**	2	1	2	F1,F2,F3,F102,F103,F123	Finsys	Finsys	Logické	Áno
P25	FinSecure.LightningNetwork	**IS - Windows services - API 3.stran**	1	1	4	F4	Finsys	Finsys	Logické	Áno
P26	Finsecure.OrderBookBinance	**IS - Windows services - API 3.stran**	3	1	4	F120,F121	Finsys	Finsys	Logické	Áno
P27	Finsecure.OrderBookKraken	**IS - Windows services - API 3.stran**	3	1	4	F120,F121	Finsys	Finsys	Logické	Áno
P28	Finsecure.SmsSenderService	**IS - Windows services - API 3.stran**	3	1	2	F123	Finsys	Finsys	Logické	Áno
P29	Finsecure.Staker	**IS - Windows services - API 3.stran**	2	1	1	F6,F7,F8	Finsys	Finsys	Logické	Áno
P30	Finsecure.Trader	**IS - Windows services - API 3.stran**	3	1	4	F120,F121	Finsys	Finsys	Logické	Áno
P31	Finsecure.Updater	**IS - Windows services - API 3.stran**	3	1	3	F4,F6,F7	Finsys	Finsys	Logické	Áno
P32	PEP, SanctionList Downloader	**IS - Windows services - API 3.stran**	1	1	1	F46	Finsys	Finsys	Logické	Áno
P33	Finsecure.CoinMarketCap	**IS - Windows services - API 3.stran**	1	1	1	F122	Finsys	Finsys	Logické	Áno
P34	Finsecure.GmailReader	**IS - Windows services - API 3.stran**	2	1	1	F100,F107,F103	Finsys	Finsys	Logické	Áno
P35	Finsecure.IPFetcher	**IS - Windows services - API 3.stran**	1	1	1	F42,F43,F45	Finsys	Finsys	Logické	Áno
P40	SQL Validation System		3	1	2	F1,F2,F3,F4,F20,F21,F40,F4	Finsys	Finsys	Logické	Áno
P41	SQL AML Antifraud system		3	1	2	F1,F2,F3,F4,F20,F21,F40,F4	Finsys	Finsys	Logické	Áno
P50	Fio webové rozhranie	**Záložné systémy**	2	3	1	F1,F3,F5,F7	Fio banka	Finsys	Logické	Áno
P54	Vyhodnotenie prichádzajúcich platieb	**Automatické schvaľovacie systémy**	3	3	4	F1,F4	Finsys	Finsys	Logické	Áno
P60	Klientská webová aplikácia finsecure.cz	**Informačné systémy a aplikácie - klientské**	3	1	2	F1,F3,F4	Finsys	Finsys	Logické	Áno
P61	Klientská webová aplikácia trader.finsecure.cz	**Informačné systémy a aplikácie - klientské**	3	1	2	F1,F3,F4	Finsys	Finsys	Logické	Áno
P62	Obchodný systém backoffice.finsys.cz	**Informačné systémy a aplikácie - interné**	3	4	4	F1,F2,F3,F4,F5,F6,F7,F8,F9,F10,F20,F21,F23,F24,F34,F35,F40,F43,F47,F49,F51,F52,F54,F101,F105,F108	Finsys	Finsys	Logické	Áno
P63	Mobilná aplikácia aplikace iOS	**Informačné systémy a aplikácie - klientské**	2	1	2	F1,F3,F4	Finsys	Finsys	Logické	Áno
P64	Mobilná aplikácia Android	**Informačné systémy a aplikácie - klientské**	2	1	2	F1,F3,F4	Finsys	Finsys	Logické	Áno
P65	Ticket systém	**Informačné systémy a aplikácie - interné**	2	2	1	F42,F43,F45,F46,F47,F60,F	Finsys	Finsys	Logické	Áno

Obrázok č.62 Klasifikácia podporných aktív podľa CIA triády a ich prepojenie na kľúčové funkcie časť 2. (Zdroj: Vlastné spracovanie)

P65	Ticket systém	**Informačné systémy a aplikácie - interné**	2	2	1	F42,F43,F45,F46,F47,F60,F	Finsys	Finsys	Logické	Ano
P70	API Kľúče bankového rozhrania	**Kryptografické prostriedky**	3	4	3	F1,F2,F3,F5,F7	Fio banka	Finsys	Logické	Ano
P71	Hardvarové kľúče	**Kryptografické prostriedky**	2	4	4	F11,F22	Finsys	Finsys	Logické	Ano
P72	Certifikáty šifrovania záloh	**Kryptografické prostriedky**	3	4	4	F70,F71,F72	Finsys	Finsys	Logické	Ano
P75	BackOffice	**Ľudské zdroje**	2	2	3	F1,F2,F3,F4,F5,F6,F7,F9,F1 0,F11,F20,F21,F22,F24,F60, F63,F122	Finsys	Finsys	Fyzické	Ne
P76	Compliance	**Ľudské zdroje**	2	2	2	F30,F31,F32,F34,F35,F36,F 37,F38,F39,F40,F41,F42,F4 3,F44,F45,F46,F47,F48,F49, F50,F51,F52,F53,F54,F55,F 60,F63,F82,F105,F107	Finsys	Finsys	Fyzické	Ne
P77	Klientské oddelenie	**Ľudské zdroje**	2	2	2	F60,F63,F100,F101,F102,F1 03,F104,F105,F106,F107,F 108	Finsys	Finsys	Fyzické	Ne
P78	FrontOffice	**Ľudské zdroje**	2	1	2	F60,F63,F120,F121,F122	Finsys	Finsys	Fyzické	Ne
P79	Risk	**Ľudské zdroje**	2	2	2	F5,F6,F7,F30,F31,F32,F48,F	Finsys	Finsys	Fyzické	Ne
P80	Účtovné oddelenie	**Ľudské zdroje**	1	1	3	F60,F63,F130	Finsys	Finsys	Fyzické	Ne
P81	Kybernetická bezpečnosť	**Ľudské zdroje**	2	1	4	F1,F3,F4,F20,F21,F22,F60,F 63,F72	Finsys	Finsys	Fyzické	Ne
P82	Vedenie	**Ľudské zdroje**	1	3	3	F11,F22,F60,F61,F63	Finsys	Finsys	Fyzické	Ne
P83	ICT	**Ľudské zdroje**	2	3	4	F46,F54,F55,F60,F63,F70,F 71,F72,F73,F75,F77,F78,F7 9,F80,F81,F82,F130	Finsys	Finsys	Fyzické	Ne
P84	Vývoj	**Ľudské zdroje**	1	1	1	F62,F63,F64,F65,F74	Finsys	Finsys	Fyzické	Ne
P85	Marketing	**Ľudské zdroje**	1	1	1	F90,F91	Finsys	Finsys	Fyzické	Ne
P88	Fio Banka	**Tretie strany**	2	1	2	F1,F2,F3,F5,F7,F33	Fio banka	Fio banka	Fyzické	Ne
P89	Trh Kraken	**Tretie strany**	2	1	2	F8,F33,F120	Payward	Payward	Fyzické	Ne
P90	Trh Binance	**Tretie strany**	2	1	2	F33,F120	Binance	Binance	Fyzické	Ne
P91	Nástroj na BlockChain kryptomien	**Tretie strany**	2	1	4	F4,F6,F7,F9,F10,F21,F22,F2 3	Blockdeamon	Blockdeamon	Fyzické	Ne
P92	Právna Kancelária	**Tretie strany**	1	1	1	F30,F31,F32	FinLex Legal	FinLex Legal	Fyzické	Ne

Obrázok č.63 Klasifikácia podporných aktív podľa CIA triády a ich prepojenie na kľúčové funkcie časť 3. (Zdroj: Vlastné spracovanie)

P92	Právna Kancelária	Tretie strany	1	1	1	F30,F31,F32	FinLex Legal	FinLex Legal	Fyzické	Ne
P93	AML poradcovia	Tretie strany	1	1	1	F30,F31,F32,F33,F35,F36,F37,F38,F39,F40	AML Systems	AML Systems	Fyzické	Ne
P94	Sociálne siete, Kurzy.cz	Tretie strany	1	1	1	F90,F91	Meta, Aliaveb	Meta, Aliaveb	Fyzické	Ne
P95	Zdroje PEP, Sakčných zoznamov	Tretie strany	1	1	1	F46	OpenSanctions	OpenSanctions	Fyzické	Ne
P96	NBS,PSR,Finančná správa SR a další..,	Tretie strany	2	1	1	F55	-	-	Fyzické	Ne
P98	Google Meet, Discord	Externý - komunikačné nástroje	1	2	1	F76,F80	Google, Discord	Finsys	Logické	Ano
P99	Zabbix	Monitoring systém	2	1	1	F76,F78,F80	Zabbix	Finsys	Logické	Ano
P100	Stav systému	Monitoring systém	2	1	2	F1,F2,F3,F4,F5,F6,F7,F8,F9,F10,F76,F77,F80	Finsys	Finsys	Logické	Ano
P101	Generátor pravidelných činností	Monitoring systém	2	1	1	F6,F7,F9,F10,F11,F30,F78	Finsys	Finsys	Logické	Ano
P102	Discord Logs notifications	Monitoring systém	1	1	1	F76	Finsys	Finsys	Logické	Ano
P103	Discord BackOffice Notifications	Monitoring systém	1	1	1	F3,F4,F8,F9,F10	Finsys	Finsys	Logické	Ano
P104	Discord HelpDesk Notifications	Monitoring systém	1	1	1	F102, F107	Finsys	Finsys	Logické	Ano
P105	Discord Compliance Notifications	Monitoring systém	1	1	1	F42,F46	Finsys	Finsys	Logické	Ano
P118	Hardvarové peňaženky	HW - sídlo	2	4	4	F4,F6,F7,F9,F10,F22	Satoshi Labs, Ledger	Finsys	Fyzické	Ne
P119	Trezory	HW - sídlo	2	4	4		Kovona	Finsys	Fyzické	Ne
P120	Notebooky	HW - sídlo	2	3	4		Lenovo	Finsys	Fyzické	Ano
P121	Telefóny, mobily a pevná linka	HW - sídlo	2	2	2	F24,F33,F40,F104	Apple	Finsys	Fyzické	Ano
P122	USB sietové konektory	HW - sídlo	2	1	2		Lenovo	Finsys	Fyzické	Ano
P123	Tiskárny	HW - sídlo	1	1	1		Canon	Finsys	Fyzické	Ano
P130	Kancelária Sídla	Objekt	1	2	1		BH Securities	Finsys	Fyzické	Ano
P140	HotWallet	Kryptoprostriedky	2	4	4	F4,F6,F7,F9,F11	Electrum	Finsys	Logické	Ano
P141	ColdWalet	Kryptoprostriedky	2	4	4	F6,F7,F10,F11,F22	Satoshi Labs, Ledger	Finsys	Logické	Ano
P142	Trhy	Kryptoprostriedky	2	4	4	F6,F7,F8	Payward, Binance	Finsys	Logické	Ano

Obrázok č.64 Klasifikácia podporných aktív podľa CIA triády a ich prepojenie na kľúčové funkcie časť 4. (Zdroj: Vlastné spracovanie)

Funkcia	Špecifikácia	Dopad v prípade zlyhania funkcie						Priorita pre obnovenie	Poznámka
		Zásadná alebo dôležitá funkcia	Kategória osobných údajov	Kategória povinností	Kategória chodu finančného subjektu	Kategória image finančného subjektu	Kategória core business		
Prijímanie bezhotovostných platieb	BackOffice	Áno	1	2	3	2	3	3	Zabezpečenie prijatia platieb v EUR alebo CZK z tuzemských účtov klientov na účet zmenárne.
Vrátenie chybných bezhotovostných platieb	BackOffice	Áno	1	1	2	1	1	1	Vrátenie finančných prostriedkov klientom pri chybne zadanej čiastke alebo nesprávne uvedenom variabilnom symbole.
Odosielanie bezhotovostných platieb	BackOffice	Áno	1	2	3	2	3	3	Odosielanie EUR alebo CZK prostriedkov klientom na ich bankové účty na základe žiadosti o výber.
Prijímanie kryptomenových platieb	BackOffice	Áno	1	2	3	2	3	3	Zabezpečenie prijímania kryptomien do peňaženky klienta po zadaní správnej adresy a potvrdení prevodu.
Kontrola stavu fiat prostriedkov	BackOffice	Áno	1	1	1	1	1	1	Denná kontrola zostatkov fiat mien na bankových účtoch pre správne vykazanie likvidity spoločnosti.
Kontrola stavu krypto prostriedkov	BackOffice	Áno	1	1	1	1	1	1	Sledovanie aktuálnych zostatkov kryptomien v hot a cold peňaženkách a porovnanie s internou evidenciou.
Vykonávanie rekonciliácie	BackOffice	Áno	1	2	3	1	1	1	Vykonanie rekonciliácie.
Administratíva týkajúca sa Staking služieb	BackOffice	Ne	1	1	1	1	1	1	Spracovanie dát o stakovaných prostriedkoch, prípadných odmenách a modifikácia klientov v zmenách.
Aktualizácia zostatkov Hot wallet	BackOffice	Áno	1	1	1	1	1	1	Zálohovanie aktuálnych dát z hot wallet peňaženiek a ich zobrazenie klientovi v užívateľskom rozhraní.
Aktualizácia zostatkov Cold wallet	BackOffice	Áno	1	1	1	1	1	1	Pravidelné zaznamenávanie zostatkov cold wallet peňaženiek a ich premietnutie do celkovej bilancie klientov.
Overenie funkčnosti prevodov Cold, Hot wallet	BackOffice	Ne	1	1	1	1	1	1	Testovanie odosielania prijatia kryptomien medzi internými peňaženkami zmenárne pre overenie funkčnosti systému.
Analýza kryptovýberov	BackOffice - Oddelenie výberov	Áno	1	2	1	1	1	1	Prevzatie opráv mnohosti kryptovýberu, súlad s internou evidenciou a dostatočná rezerva v hot wallet.
Odosielanie kryptomenových prostriedkov	BackOffice - Oddelenie výberov	Áno	1	2	2	2	3	3	Odosielanie kryptomenových aktív klientom po schválení výberu a overení správnosti adresy peňaženky.
Prevody z Cold wallet	BackOffice - Oddelenie výberov	Áno	1	1	2	2	2	2	Vykonávanie presunu väčších objemov kryptomien z cold wallet do hot wallet pre zabezpečenie likvidity.
Analýza zle zaslaných kryptoaktív	BackOffice - Oddelenie výberov	Áno	1	1	1	1	1	1	Vykonávanie nesprávne zaslaných kryptoaktív, identifikácia klienta a snaha o ich navrátenie.
Telefonické overovanie rizikových výberov	BackOffice - Oddelenie výberov	Áno	1	1	1	1	1	1	Telefonické overenie identity klienta a dôvodu výberu pri podozrivých alebo nesúvislostných transakciách.
Sledovanie regulačných zmien	Compliance	Áno	1	2	1	1	1	1	Sledovanie a vyhodnocovanie zmien v európskej a slovenskej legislatíve, ktoré môžu ovplyvniť fungovanie zmenárne.
Periodické AML audity a revízie vnútorných predpisov	Compliance	Áno	1	2	1	1	1	1	Pravidelné preverovanie súladu AML procesov, revízia interných predpisov a dokumentácie podľa platnej legislatívy.
Aktualizácia a testovanie systému vnútorných zásad AML/CFT	Compliance	Áno	1	2	1	1	1	1	Testovanie funkčnosti a aktuálnosti AML politík, vrátane aktualizácie na základe legislatívnych zmien.
Odpovede na AML/KYC due diligence dotazníky od partnerov	Compliance	Áno	1	2	1	1	1	1	Zodpovedanie dotazníkov zameraných na AML/KYC politiku partnerov, burz a bankových inštitúcií.
Kontrola investičných dotazníkov	Compliance	Ne	1	1	1	1	1	1	Kontrola správneho vyplnenia investičných dotazníkov klientov vrátane validácie zadaných údajov a výsledkov.
Zabezpečenie komunikácie prostredníctvom dátovej schránky	Compliance	Áno	2	2	1	1	1	1	riprimanie a odosielanie dokumentov cez dátovú schránku voči štátnym inštitúciám a regulátorom.
Spolupráca s políciou SR	Compliance	Áno	2	2	1	1	1	1	Reakcia na žiadosti Polície SR o súčinnosť v rámci trestných konaní týkajúcich sa klientských transakcií.
Spolupráca s Národnou Bankou Slovenska (NBS)	Compliance	Áno	2	2	1	1	1	1	Komunikácia a spolupráca s NBS pri žiadostiach o informácie, kontrole alebo udelení licencie.
Spolupráca s ďalšími štátnymi orgánmi a inštitúciami	Compliance	Áno	2	2	1	1	1	1	Odpovedanie na žiadosti a podnety od ďalších orgánov verejnej správy v súvislosti s činnosťou zmenárne.
Zabezpečenie AML komunikácie s FSJ prostredníctvom kontaktnej osoby	Compliance	Áno	2	2	1	1	1	1	Zabezpečenie komunikácie s FSJ cez poverenú kontaktnú osobu pre portály AML hlásenia a dotazov.
Spracovanie podozrivého obchodu (OPO) a hlásenie na FSJ (Finančná spravodajská jednotka)	Compliance	Áno	3	2	1	1	1	1	Identifikácia a vyhodnotenie podozrivých obchodov a ich následné nahlásenie FSJ podľa zákonnej povinnosti.
Evidencia interných AML posúdení bez podania OPO	Compliance	Áno	2	2	1	1	1	1	Evidovanie a archivácia prípadov interného AML posúdenia, kde nedošlo k podaniu hlásenia OPO.
Vyhodnotenie geografického rizika klienta (mimo SR)	Compliance	Áno	1	1	1	1	1	1	Vyhodnotenie miery rizika klienta na základe jeho geografického pôvodu a pôsobnosti mimo SR.
Vyhodnotenie PEP a sankčných osôb	Compliance	Áno	2	2	1	1	1	1	Overovanie, či klient nepatrí alebo politicky exponovaná osoba PEP alebo na medzinárodných sankčných zoznamoch.
Kontrola vlastníckej a riadiacej štruktúry právnických osôb	Compliance	Áno	3	2	1	1	1	1	Analýza vlastníckej a riadiacej štruktúry právnických osôb za účelom identifikácie skutočného majiteľa.
Vyhodnotenie rizikovosti klienta a vykonanie zosilnenej kontroly	Compliance	Áno	2	2	1	1	1	1	Stanovenie úrovne rizikovosti klienta a prípadné vykonanie zosilneného overenia identity a zdroja prostriedkov.
Vedenie zoznamu rizikových a sankčných klientov	Compliance	Áno	2	2	1	1	1	1	Udržiavanie interného zoznamu klientov s vyšším AML rizikom alebo zaradených na sankčné zoznamy.
Pravidelná kontrola klientov podľa miery rizikovosti (priebežný monitoring)	Compliance	Áno	2	2	1	1	1	1	Pravidelný monitoring existujúcich klientov podľa rizikového profilu a prehodnocovanie ich aktivít.
Nastavenie a správa parametrov AML kontroly a klientskeho scoringu (podľa rizikovosti sa prideľuje skóre)	Compliance	Áno	2	2	1	1	1	1	Správa pravidiel AML scoringu, vrátane aktualizácie parametrov a priebežného hodnotenia klientom.

Obrázok č.65 Hodnotenie kritickosti funkcií časť 1. (Zdroj: Vlastné spracovanie)

Evidencia rozhodnutí a zásahov Compliance/AML (napr. blokácie, zmena rizikového profilu atď.)	Compliance	Áno	2	2	1	1	1	1	Zaznamenávanie a vyhodnotenie zásahov no strany compliance, napr. blokácia účtu alebo zmena rizikovosti.
Školenie zamestnancov v oblasti AML/CFT a MiCA, vrátane vedenia záznamu	Compliance	Áno	1	1	1	1	1	1	Organizácia školení zamestnancov v oblasti AML, CFT a MiCA, vrátane vedenia dochádzky a výstupov.
Evidencia incidentov s dopadom na compliance alebo klientov (napr. záznam výpadku obchodovania)	Compliance	Áno	1	1	1	1	1	1	Záznam incidentov ovplyvňujúcich chod u compliance alebo dopad klientských operácií a systémov.
Záznam a rozhodnutie o ukončení obchodného vzťahu / zrušení klientskeho účtu	Compliance	Áno	3	1	1	1	1	1	Ukladanie rozhodnutí o ukončení obchodného vzťahu vrátane odvodnenia a informovania príslušných osôb.
Interné oznamovanie porušení AML/Compliance pravidiel pre zamestnancov (whistleblowing)	Compliance	Áno	1	1	1	1	1	1	Zabezpečenie interného oznamovania porušenia pravidiel AML/Compliance (tzv. whistleblowing) v súlade s GDPR.
Zabezpečenie súladu s GDPR pri spracovaní osobných údajov klientov	Compliance	Áno	3	1	1	1	1	1	Implementácia pravidiel GDPR pri spracovaní osobných údajov klientov a uchovávanie dokumentácie o súhlasoch.
Zabezpečenie hlásení a vyjadrení k výkazníctva voči NBS (reporting po získaní licencie)	Compliance	Áno	2	1	1	1	1	1	Zostavenie a odoslanie zákonných reportov a prehľadov pre NBS po získaní licencie.
Zber požiadaviek k úpravám systému	Vývoj	Áno	1	1	1	1	1	1	Zber technických a prevádzkových požiadaviek na zmeny informačných systémov od všetkých oddelení.
Vyhodnotenie požiadaviek a príprava zadania	Vývoj	Áno	1	1	1	1	1	1	Vyhodnotenie prijatých požiadaviek, posúdenie dopadov a príprava detailného zadania pre vývojárov.
Implementácia zmien	Vývoj	Áno	1	1	1	2	1	1	Programovanie a nasadenie nových funkcií podľa zadania a aktualizácia projektov.
Testovanie nových funkcií	Vývoj	Áno	2	1	1	1	1	1	Testovanie nasadených zmien vrátane kontroly funkčnosti a pripadného zabezpečenia opráv pred produktívou.
Code review	Vývoj	Áno	1	1	1	1	1	1	Kontrola kódu (code review) v rámci tímu, revízia zmien a zabezpečenie súladu so štandardmi vývoja.
Audit komponentov tretích strán	Vývoj	Áno	1	1	1	1	1	1	Prevedia kontrolu a komponentov tretích strán z hľadiska bezpečnosti a licenčných podmienok.
Zálohovanie systémov	ICT	Áno	2	2	2	1	1	1	Pravidelné zálohovanie systémov, databáz (DB) a konfiguračných súborov na bezpečné úložiská.
Kontrola záloh DB	ICT	Áno	2	1	1	1	1	1	Overenie správnosti a konzistencie záloh databáz (DB) vrátane schopnosti vykonať ich obnovu.
Overenie funkčnosti obnovy systému	ICT	Áno	1	1	1	1	1	1	Testovanie obnovy systému zo záloh, simulácia havárie a kontrola funkčnosti všetkých komponentov.
Zabezpečenie generovania tiketov pravidelných činností	ICT	Áno	1	1	1	1	1	1	Automatizácia pravidelných operácií pomocou tiketovacieho systému pre vyššiu prehľadnosť a zodpovednosť.
Prevádzka vývojového a testovacieho prostredia	ICT	Nie	2	1	1	1	1	1	Správa vývojového a testovacieho prostredia oddeleného od produkcie pre bezpečné nasadenie zmien.
Prevádzka produkčného prostredia	ICT	Áno	1	1	3	2	3	3	Zabezpečenie prevádzky produkčného systému a jeho dostupnosti pre klientov bez prerušenia služieb.
Vyhodnocovanie logov	ICT	Áno	1	1	1	1	1	1	Pravidelné vyhodnocovanie systémových logov pre detekciu chýb, výnimiek a bezpečnostných hrozieb.
Aktualizácia systémov	ICT	Áno	1	1	1	1	1	1	Nasadzovanie systémových a bezpečnostných aktualizácií na serveroch a klúčových službách.
Audit užívateľských staníc	ICT	Áno	1	1	1	1	1	1	Vykonávanie auditov pracovných staníc zamestnancov z hľadiska bezpečnosti a správnej konfigurácie.
Správa incidentov	ICT	Áno	1	1	1	1	1	1	Evidencia, klasifikácia a riešenie incidentov v rámci IT a prevádzky, vrátane sledovania závažnosti.
Sledovanie dostupnosti systémov	ICT	Áno	1	1	1	1	1	1	Sledovanie dostupnosti kľúčových systémov a ich reakčnej doby pomocou monitorovacích nástrojov.
Penetračné testovanie	ICT	Nie	1	1	1	1	1	1	Vykonávanie penetračných testov interne alebo externe za účelom odhalenia potenciálnych slabín.
Audit prístupových práv systému a užívateľov	ICT	Áno	1	1	1	1	1	1	Pravidelná kontrola a audit prístupových práv k systémom pre zamestnancov a externých užívateľov.
Články na Hlonline.sk, Trend.sk, Kurzy.cz	Marketing	Nie	1	1	1	1	1	1	Publikácia článkov s odborným obsahom na Hlonline.sk a iné externé vzdelávania klientov a PR zmeniarne.
Príspevky na sociálne siete	Marketing	Nie	1	2	1	1	1	1	Príprava a publikácia príspevkov na sociálnych sieťach o novinkách, vzdelávaní a bezpečnosti.
Kontrola emailovej komunikácie	Klientské oddelenie	Áno	2	1	1	1	1	1	Kontrola komunikácie so zákazníkmi e-mailom z hľadiska kvality, relevancie a rýchlosti odpovede.
Preverovanie nových klientov	Klientské oddelenie, Compliance	Áno	2	1	1	1	1	1	Preverenie identity a zázemia nových klientov pred povolením obchodovania, vrátane AML kontroly.
Odpovedanie klientskych tiketov	Klientské oddelenie	Áno	2	1	1	2	1	1	Odpovedanie na klientske dotazy prostredníctvom ticketovacieho systému v rámci SLA lehotách.
Odpovedanie emailových dotazov	Klientské oddelenie	Áno	2	1	1	2	1	1	Reaktívna odpoveď na dotazy klientov zaslané e-mailom, vrátane pripadného postúpenia odbornému oddeleniu.
Odpovedanie telefonických dotazov	Klientské oddelenie	Nie	2	1	1	1	1	1	Telefonická podpora klientov, overovanie údajov a poskytovanie informácií o stave transakcií.
Overovanie klientov na príslušné stupne overenia (identifikácia a kontrola)	Compliance, Klienstké oddelenie	Áno	2	1	1	1	1	1	Overenie identity klienta podľa zákona, vrátane vyžiadania dokumentov a overenia ich pravosti.
Posudzovanie a odovzdávanie rizikových prípadov klientov oddeleniu Compliance	Klientské oddelenie	Áno	2	1	1	1	1	1	Posúdenie podozrivých aktivít klienta a eskalácia prípadu na AML alebo Compliance oddelenie.
Vybavovanie reklamácií a sťažností klientov	Compliance, Klienstké oddelenie	Áno	3	2	2	2	1	1	Riešenie reklamácií klientov, zabezpečenie nápravy a zodpovedanej komunikácie podľa interných pravidiel.
Aktualizácia klientských údajov na základe zmien (napr. zmena adresy, občianstva, štruktúry právnickej	Compliance, Klienstké oddelenie	Áno	2	1	1	1	1	1	Aktualizácia údajov klientov v systéme na základe doložených zmien a ich archivácia.
Komunikácia s trhmi	Frontoffice	Áno	1	1	3	1	1	1	Komunikácia s burzami a externými trhmi ohľadne transakcií, zostatkov alebo nových funkcionalít.
Kontrola kurzov kryptomien	Frontoffice	Áno	1	1	1	1	1	1	Pravidelná kontrola kurzov kryptomien a ich aktualizácia v systéme zmeniarne.
Hodnotenie rizikovosti jednotlivých kryptomien	BackOffice	Nie	1	1	1	1	1	1	Analýza bezpečnostných, likvidných a reputačných rizík vybraných kryptomien v ponuke.
Preverovanie nových klientov	Klienstké oddelenie, Compliance	Áno	1	1	1	1	1	1	Preverovanie identity, zdrojov prostriedkov a histórie obchodovania nových klientov.
Zmena ponuky kryptomien (vyradenie a pridanie)	Compliance, BackOffice, FrontOffice	Nie	2	1	1	2	1	1	Rozhodovanie o pridaní alebo odstránení kryptomien z ponuky podľa obchodných a technických kritérií.
Prenos dát do účtovníctva	IT / Účtovníctvo	Nie	1	2	1	1	1	1	Zabezpečenie exportu dát o transakciách a zostatkoch do účtovného softvéru pre ďalšie spracovanie.

Obrázok č.66 Hodnotenie kritickosti funkcií časť 2. (Zdroj: Vlastné spracovanie)

3.2.2 Návrh procesu riadenia rizík IKT

Na základe požiadaviek nariadenia DORA a v nadväznosti na strategický rámec digitálnej prevádzkovej odolnosti bol v spoločnosti Finsys vypracovaný rámec riadenia rizík v podobe dokumentu **Smernica o riadení rizík v oblasti IKT**, ktorý predstavuje základný metodický rámec a proces, pre identifikáciu, hodnotenie a monitorovanie rizík vyplývajúcich z technických, procesných a organizačných aspektov IKT infraštruktúry. Smernica bola vytvorená autorom tejto práce.

Identifikácia rizík

Riziká sú identifikované na základe:

- **Zraniteľností a hrozieb** zistených pri hodnotení aktív a funkcií (vychádza sa z CIA klasifikácie a kritickosti).
- Výsledkov **penetračných testov**, **interných auditov**, **incidentov** a **testovania digitálnej odolnosti.**
- Sledovania zmien v regulačnom, technologickom alebo prevádzkovom prostredí.

Hodnotenie rizík

Každé identifikované riziko je hodnotené ako výsledok interakcie troch faktorov:

- **Hodnota dopadu** na činnosť spoločnosti (finančná, reputačná, právna).
- **Úroveň zraniteľnosti** príslušného aktíva alebo funkcie.
- **Hodnota / intenzita hrozby**, ktorá môže zraniteľnosť zneužiť.

Riziko je kvantifikované pomocou výpočtu:

Riziko = Dopad × Zraniteľnosť × Hrozba

Hodnoty vstupov sú priraďované na škále od 1 (nízka) po 4 (kritická), pričom výsledné rizikové skóre určuje zaradenie do jednej zo štyroch kategórií: nízke, stredné, vysoké alebo kritické. Výsledky hodnotenia sú evidované v **katalógu rizík**. Katalóg rizík je zostavený na základe hodnotenia konkrétnych aktív a funkcií a slúži ako východisko pre plánovanie bezpečnostných opatrení.

Spôsob zvládania rizík

Na základe vyhodnotenej hodnoty rizika je každému riziku priradený adekvátny spôsob zvládania, ktorý je súčasťou samotného procesu hodnotenia.

Príklady priradenia:

- **Redukcia rizika** je zvolená pri vysokých a kritických hodnotách (napr. riziko poškodenia technického vybavenia s hodnotou 36 alebo pôsobenie škodlivého kódu s hodnotou 48).
- **Sledovanie rizika** je uplatnené pri stredne vysokých rizikách, kde je potrebné priebežné monitorovanie bez nutnosti okamžitých opatrení (napr. neoprávnené používanie licencií).
- **Akceptácia rizika** sa týka nízkorizikových situácií, kde by implementácia protiopatrení nebola efektívna (napr. bežné pochybenia interných používateľov s hodnotou rizika 12).

Pravidelné preskúmanie a aktualizácia

Riadenie rizík je založené na princípe nepretržitého zlepšovania (cyklus PDCA – Plan, Do, Check, Act). Riziká a ich hodnotenia sa revidujú:

- Najmenej raz ročne.
- Po výskyte incidentu, zmene systému, zmene regulačných požiadaviek alebo aktualizácii infraštruktúry.

Integrácia do rámca digitálnej odolnosti

Riadenie rizík je priamo prepojené na:

- **Stratégiu digitálnej prevádzkovej odolnosti a Bezpečnostnej smernice**
- **Plánu obnovy a kontinuity činností**
- **Smernici o riadení incidentov súvisiacich s IKT**

Týmto spôsobom spoločnosť zabezpečuje, že riadenie IKT rizík nie je izolovanou činnosťou, ale integrálnou súčasťou celkového systému prevádzkovej bezpečnosti.

Hodnotenie rizík

ID	Aktívum / Funkcia	Hodnota dopadu	Zraniteľnosť	Hodnota zraniteľnosti	Hrozba	Hodnota hrozby	Hodnota rizika	Spôsob zvládania rizika
R1	P1: Aplikačný server (hardvér)	3	Zastaranosť aktív	4	Poškodenie alebo zlyhanie technického alebo programového vybavenia	3	36	Redukcia
R2	P10: Operačný systém (databázový server)	3	Nedostatočná údržba aktív	4	Pôsobenie škodlivého kódu (napríklad vírusy, spyware, trójske kone)	4	48	Redukcia
R3	P19: Aplikačný server (licencia)	3	Nedostatočné monitorovanie činnosti zamestnancov a neschopnosť odhaliť ich nevhodné alebo závadné spôsoby správania	3	Užívanie programového vybavenia v rozpore s licenčnými podmienkami	2	18	Sledovanie
R4	P28: Administrátor (interný)	3	Nedostatočné bezpečnostné povedomie užívateľov a administrátorov	2	Pochybenie zo strany zamestnancov a administrátorov	2	12	Akceptácia
R5	F22: Riadenie vzťahov s poskytovateľmi služieb IKT	4	Veľká časť zásadných alebo dôležitých funkcií je závislá na jednom poskytovateľovi služieb IKT z radov tretích strán.	4	Zlyhanie tohto poskytovateľa služieb IKT	2	32	Redukcia
R6	P61: Klientská webová aplikácia trader.finsecure.sk	4	Závislosť na externom autentifikačnom systéme	3	Nedostupnosť externého poskytovateľa SSO	2	24	Sledovanie
R7	P40: SQL Validation System	3	Absencia pravidelného monitorovania chýb	3	Zlyhanie kontroly vstupných dát a validácií	3	27	Redukcia
R8	P70: API Kľúče bankového rozhrania	4	Nedostatočné zabezpečenie API tokenov	3	Zneužitie autentifikačných údajov externou stranou	3	36	Redukcia
R9	P34: Finsecure.GmailReader	2	Zraniteľnosti v knižniciach pre parsing e-mailov	3	Spustenie škodlivého kódu pri spracovaní prijatého e-mailu	3	18	Sledovanie
R10	P99: Zabbix	3	Nedostatočná separácia monitorovacej vrstvy	3	Útočník získa prístup k sieťovým alebo systémovým štatistikám	2	18	Sledovanie

Obrázok č.67 Analýza rizík. (Zdroj: Vlastné spracovanie)

3.2.3 Návrh plánu zvládania rizík IKT

V súlade s nariadením DORA a v nadväznosti na zavedený proces identifikácie a hodnotenia rizík bol v spoločnosti Finsys implementovaný formálny **Plán zvládania rizík IKT**. Tento plán predstavuje kľúčový výstup celkového rámca riadenia rizík, ktorého cieľom je zabezpečiť, aby na každé významnejšie riziko boli aplikované primerané a zdokumentované opatrenia.

Plán zvládania rizík bol vytvorený autorom tejto práce a schválený vedúcim orgánom a je spravovaný ako živý dokument – **pravidelne sa aktualizuje** v závislosti od nových zistení z hodnotenia aktív, výsledkov testov, interných auditov a prevádzkových incidentov.

Obsah plánu zvládania rizík

Každé riziko identifikované v katalógu rizík je priradené k jednému alebo viacerým konkrétnym bezpečnostným opatreniam. Tieto opatrenia sú v pláne zaznamenané vrátane nasledujúcich atribútov:

- Popis opatrenia a jeho hlavný účel
- Priorita realizácie podľa závažnosti súvisiaceho rizika
- Väzba na konkrétne identifikované riziko
- Stav implementácie (zavedené, v priebehu zavádzania, plánované)
- Ciele a prínosy
- Termín zavedenia opatrenia
- Potrebné zdroje: technické, investičné, prevádzkové, ľudské a informačné
- Metrika na vyhodnotenie účinnosti (napr. audit, školenie, úspešné testovanie)

Ukotvenie v riadiacom rámci spoločnosti

Plán zvládania rizík nie je samostatným dokumentom, ale je plne integrovaný do riadiaceho systému spoločnosti. Vychádza z metodiky stanovenej v **Smernici o riadení rizík v oblasti IKT** a nadväzuje na výsledky z dokumentu **Hodnotenie aktív, funkcií a rizík**. Navyše, opatrenia sú koordinované s plánovaním bezpečnostných testov a auditov, čo zabezpečuje neustále zlepšovanie a uzatváranie zistených nedostatkov.

ID	Popis bezpečnostního opatření	Priorita	Naväznosť na riziká	Stav	Ciele a prínosy	Termín zavedenia opatrenia	Potrebné zdroje				Informačné	Metrika pre vyhodnotenie úspešnosti
							Technické (EUR)	Finančné - investičné (EUR)	Finančné - prevádzkové (EUR)	Ľudské		
B02	Zabezpečiť odmenu a aktualizáciu hardvérových komponentov aplikačných serverov.	3	R1	V priebehu zaväzania	Zvýšenie spoľahlivosti a odolnosti infraštruktúry voči technickým zlyhaniam.	30.6.2025	2500	5000	500	2 MD Technologický úsek (IT oddelenie)	-	Dokončenie hardvérovej výmeny
B03	Implementovať centralizovaný systém aktualizácie a antivírusovej ochrany serverov.	3	R2	V priebehu zaväzania	Zvýšenie odolnosti serverov voči škodlivému kódu.	30.5.2025	3000	300	500	3 MD Technologický úsek (IT oddelenie)	-	Kontrola aktualizačných logov
B04	Zaviesť pravidelné audity licenčného súladu softvéru.	2	R3	Čaká na schválenie vedúcim IT oddelenia	Zabezpečenie právneho súladu s licenčnými podmienkami.	31.8.2025	0	0	300	1 MD právneho (externého) a 1 MD IT oddelenia	Licenčné podmienky softvérov	Vyhotovenie auditnej správy
B05	Realizovať školenia zamerané na zvyšovanie bezpečnostného povedomia	2	R4	V priebehu zaväzania	Zníženie rizika pochybenia pri výkone oprávnení.	30.9.2025	0	100	500	1 MD Technický manažér + externý školiteľ	-	Uskutočnenie školenia
B06	Dvierenfilkovať poskytovateľov IKT služieb pre kľúčové funkcie.	3	R5	Čaká na schválenie vedúcim IT oddelenia	Zníženie prevádzkovej závislosti a zvýšenie kontinuity služieb.	31.12.2025	0	2000	1500	2 MD Technický manažér + právne oddelenie (externé)	Smernica o riadení vzťahov s tretími stranami	Podpis zmluvy s alternatívnym dodávateľom
B07	Nastaviť automatické monitorovanie vstupných dát a validačných kontrol.	3	R7	Zavedené	Zníženie rizika zlyhania spracovania dát.	19.5.2025	1500	1500	500	1 MD vývojový tím	-	Funkčné logy validačných pravidiel
B08	Zaviesť bezpečnostnú politiku pre správu API tokenov a revokácie.	3	R8	V priebehu zaväzania	Minimalizácia rizika kompromitácie API prístupov.	31.10.2025	2800	500	200	1 MD DevOps Špecialista + Backend vývojár	-	Implementácia politiky a jej revízia
B09	Aktualizovať knižnice používané na parsovanie e-mailov a zaviesť sandboxing mechanizmus.	2	R9	Čaká na schválenie vedúcim IT oddelenia	Zníženie rizika spustenia škodlivého obsahu.	30.9.2025	600	1200	300	1 MD vývojový tím + 1 MD bezpečnostný analytik (externý)	-	Úspešné testy na škodlivé e-maily
B010	Oddeliť monitorovaciu vrstvu (Zabbix) od produkčnej infraštruktúry.	2	R10	V priebehu zaväzania	Zamedzenie zneužitia prístupov k sieťovým štatistikám.	31.8.2025	1200	1800	400	2 MD DevOps Špecialista	-	Bezpečnostný audit topológie Zabbixu

Obrázok č.68 Plán zvládania rizík – Návrh bezpečnostných opatrení (Zdroj: Vlastné spracovanie)

3.3 Návrh riadenia incidentov súvisiacich s IKT

3.3.1 Návrh procesu riadenia incidentov a definovanie rolí

V súlade s požiadavkami nariadenia DORA spoločnosť Finsys zaviedla formalizovaný proces riadenia incidentov súvisiacich s informačnými a komunikačnými technológiami (IKT), ktorý pokrýva celý životný cyklus incidentu – od jeho identifikácie až po fázu poučenia sa. Tento proces je zakotvený v internom predpise **Smernica o riadení incidentov súvisiacich s IKT** a tvorí integrálnu súčasť rámca digitálnej prevádzkovej odolnosti. Smernica bola vytvorená autorom tejto práce.

Identifikácia a detekcia incidentu

Incidenty sú identifikované na základe **ukazovateľov včasného varovania**, ktoré zahŕňajú nezvyčajnú sieťovú aktivitu, opakované chyby autentifikácie, výpadky služieb či alarmy z bezpečnostných nástrojov. Finsys využíva kombináciu automatizovaných detekčných nástrojov a manuálnych kontrol prostredníctvom monitoringu systémových logov.

Analýza a klasifikácia

Po detekcii nasleduje fáza analýzy a klasifikácie incidentu. Incidenty sú kategorizované podľa vplyvu na dôvernosť, integritu a dostupnosť aktív, pričom sa posudzuje ich rozsah, závažnosť a pôvod. Významné incidenty sú klasifikované ako „závažné“ a podliehajú povinnosti hlásenia príslušným regulačným orgánom.

Reakcia, obmedzenie a odstránenie

V prípade potvrdeného incidentu sa aktivujú procesy obmedzenia jeho dopadu (napr. izolácia postihnutých systémov, blokovanie prístupov), následne nasleduje odstránenie príčiny (napr. odstránenie škodlivého kódu, aktualizácia zraniteľných komponentov). V prípade závažného narušenia je aktivovaný pohotovostný a obnovovací plán.

Obnova a post-incident review

Po odstránení dôsledkov incidentu sa vykoná komplexná obnova dotknutých systémov a služieb vrátane obnovy dát zo záloh. Obnova je koordinovaná podľa vopred definovaných plánov obnovy. Následne prebieha fáza „post-incident review“, ktorej cieľom je identifikovať príčiny incidentu, zhodnotiť účinnosť reakcie a navrhnúť preventívne opatrenia pre budúcnosť.

Definovanie rolí a zodpovedností

Proces riadenia incidentov je pod gesciou vymenovaného **Incident manažéra**, ktorý zodpovedá za koordináciu všetkých fáz incidentu a komunikáciu s vedením. V prípade závažného incidentu je zvolaný **krízový tím**, ktorého zloženie je definované v *Bezpečnostnej smernici*. Úlohy jednotlivých členov tímu, vrátane technickej podpory, právneho zástupcu a zástupcu pre komunikáciu, sú presne špecifikované.

Dokumentácia a evidencia

Vedie sa evidencia incidentov v elektronickej podobe, ktorá slúži ako vstup pre ďalšiu analýzu a reporting (podrobnejšie v 3.3.3).

ID	Typ incidentu	Popis incidentu	Dátum, čas výskytu	Dátum, čas detekcie	Dátum, čas nahlásenia	Kto incident nahlásil	Zodpovedná osoba za incident	Klasifikácia	Priorita	Dátum, čas klasifikácie	Význam dotknutých služieb	Splnené klasifikačné kritériá	Príslušné funkčné oblasti a obchodné procesy	Príslušné súčasti infraštruktúry podporujúce obchodné procesy	Posúdenie rizika pre zasiahnuté funkcie
INC-2025-001	Výpadok pripojenia	Krátkodobý výpadok internetového pripojenia v hlavnej kancelárii (20 minút).	10.3.2025 9:15	10.3.2025 9:16	10.3.2025 9:16	IT helpdesk	IT manager	NEZÁVAŽNÝ	3	10.3.2025 9:20	Nízky – len interná komunikácia a prístup k CRM	Nie	Podpora klientskeho servisu	Internetové pripojenie, router	Žiadne priame ohrozenie
INC-2025-002	Kybernetický útok (phishing)	Zamestnanec dostal podvodný e-mail a kliknul na odkaz, neočisto k úniku dát.	15.4.2025 14:20:00	15.4.2025 14:22:00	15.4.2025 14:22:00	Zamestnanec (interné hlásenie)	Vedúci IT oddelenia	NEZÁVAŽNÝ	2	15.4.2025 14:30:00	Stredný – potenciálne riziko pre e-mailové systémy a internú sieť	Nie	Bezpečnostný monitoring a školenia zamestnancov	E-mailové servery, antispam brány	Potenciálne riziko pri opakovanej nevedomosti používateľov
INC-2025-003	Výpadok služby poskytovateľa (cloud hosting)	Nedostupnosť hlavnej SaaS aplikácie po dobu 4 hodín kvôli výpadku u poskytovateľa Azure.	2.5.2025 8:30	2.5.2025 9:32	2.5.2025 8:35	Monitoring systému	DevOps špecialista	ZÁVAŽNÝ	1	2.5.2025 8:45	Vysoký – hlavnú SaaS aplikáciu používa viacero klientov na dennej báze	Áno	Poskytovanie SaaS služieb klientom	Cloud hosting, aplikačný backend	Zníženie dostupnosti kritických klientských služieb

Obrázok č.69 Evidencia a klasifikácia IKT incidentov – vzorové vyplnenie (Zdroj: Vlastné spracovanie)

3.3.2 Návrh klasifikácie incidentov a kybernetických hrozieb

S cieľom zabezpečiť efektívnu reakciu na narušenia v oblasti IKT implementovala spoločnosť Finsys metodiku **klasifikácie incidentov a kybernetických hrozieb**, ktorá je plne zosúladená s požiadavkami nariadenia DORA a súvisiacich regulačných technických štandardov (RTS/ITS). Klasifikácia je navrhnutá tak, aby umožňovala promptnú identifikáciu „závažných incidentov“ a významných hrozieb s vysokým potenciálom dopadu na obchodnú kontinuitu a bezpečnosť údajov. Metodika bola navrhnutá autorom tejto práce.

Klasifikácia incidentov súvisiacich s IKT

Incidenty sú klasifikované podľa ich závažnosti a dopadu na dôvernosť, integritu a dostupnosť spracovávaných údajov, ako aj podľa vplyvu na prevádzku služieb. Klasifikačné kritériá zahŕňajú:

- **Počet dotknutých klientov alebo protistrán** (napr. viac ako 10 % celkového počtu)
- **Územný rozsah dopadu** (napr. viac ako jeden štát)
- **Doba nedostupnosti služieb** (napr. viac ako 4 hodiny pre kritické služby)
- **Finančné škody** (napr. prekročenie stanovenej sumy v EUR)
- **Reputačný dopad alebo zasiahnutie médiami**

Incidenty, ktoré prekročia vopred definované prahové hodnoty v aspoň jednom z kritérií, sú označované ako závažné incidenty a podliehajú povinnostiam hlásenia orgánom dohľadu. Závažné incidenty a významné hrozby sú oznamované príslušným orgánom dohľadu podľa stanovených časových lehôt (do 4 hodín od klasifikácie incidentu).

Proces identifikácie a reakcie na kybernetické hrozby

Spoločnosť zaviedla aj samostatný proces pre identifikáciu a správu významných kybernetických hrozieb, ktoré ešte nevyústili do incidentu, ale majú potenciál spôsobiť vážne narušenia. Identifikácia hrozieb prebieha na základe:

- Výstupov z bezpečnostných nástrojov (napr. SIEM, IDS/IPS)
- Výstrah z externých informačných zdrojov (napr. CSIRT, ENISA)
- Interného monitoringu sietí a systémových logov

Po identifikácii hrozby je vypracované interné hodnotenie jej pravdepodobnosti a dopadu. Ak je hrozba vyhodnotená ako významná, je aktivovaný režim zvýšenej pripravenosti a spracované **Oznámenie o významnej kybernetickej hrozbe**. Tento formulár obsahuje základné identifikačné údaje, popis hrozby, možné dopady, ukazovatele kompromitácie, prijaté preventívne opatrenia a informácie o oznámení ďalším stranám.

Oznámenie o významnej kybernetickej hrozbe

1	**Názov subjektu, ktorý oznámenie podáva**	Finsys s.r.o.
2	**Identifikačný kód subjektu, ktorý oznámenie podáva**	IČO: 12345678
3	**Typ subjektu, ktorý oznámenie podáva**	Poskytovateľ digitálnych služieb (ICT)
4	**Názov dotknutého subjektu (ak je odlišný od subjektu podávajúceho oznámenie)**	-
5	**Kód LEI dotknutého subjektu (ak je odlišný od subjektu podávajúceho oznámenie)**	-
6	**Primárna kontaktná osoba (meno, email, telefón)**	Jan Novák, jan.novak@finsys.sk, +421 777 123 456
7	**Sekundárna kontaktná osoba, pokiaľ je k dispozícii (meno, email, telefón)**	Petra Hudaková, petra.hudakova@finsys.sk, +421 777 987 654
8	**Dátum a čas zistenia kybernetickej hrozby**	2025-05-02 08:32
9	**Popis významnej kybernetickej hrozby**	Došlo k náhlemu výpadku cloudovej služby XXX, ktorú organizácia využíva pre prevádzku hlavnej SaaS aplikácie. Incident bol detekovaný prostredníctvom automatizovaného monitoringu. Príčinou bol výpadok na strane poskytovateľa cloudovej infraštruktúry.
10	**Informácie o potenciálnom vplyve**	Dočasná nedostupnosť SaaS aplikácie mala priamy dopad na klientov, ktorí nemali prístup k službe po dobu 4 hodín. Incident mohol viesť k narušeniu obchodných činností a zníženiu dôvery zo strany zákazníkov
11	**Klasifikačné kritériá potenciálnych incidentov**	Význam dotknutých služieb, Dopad na dostupnosť služieb poskytovaných klientom, Ohrozenie kontinuity obchodných procesov
12	**Stav kybernetickej hrozby**	Uzavretá – incident bol ukončený, služba obnovená po ukončení výpadku u poskytovateľa
13	**Opatrenia prijaté na prevenciu realizácie hrozieb**	Presmerovanie komunikácie klientov na informačnú stránku s hlásením stavu. Spustenie revízie SLA zmluvy s poskytovateľom XXX. Príprava návrhu na zavedenie multicloudovej zálohy a geografickej redundancie. Interné informovanie klientov a registrácia incidentu v systéme riadenia rizík.
14	**Oznámenie ostatným zúčastneným stranám**	O incidente boli informovaní: IT oddelenie a vedenie spoločnosti. Incident bol zaznamenaný v internom registri kybernetických hrozieb.
15	**Indikátory kompromitácie**	Záznamy o nedostupnosti služby v monitorovacom nástroji (response time > 5s, error rate > 90 %). Chybové hlásenia HTTP 503 od cloudovej infraštruktúry. Hlásenia o zlyhaní pripojenia k aplikačným backend službám

Obrázok č.70 Vzor oznámenia o významnej kybernetickej hrozbe – vzorové vyplnenie – prvá tretina formulára (Zdroj: Vlastné spracovanie)

3.3.3 Návrh evidencie a nahlasovania závažných incidentov

S cieľom zabezpečiť transparentné, úplné a včasné riadenie incidentov spoločnosť Finsys zaviedla formalizovaný systém **evidencie a hlásenia incidentov súvisiacich s informačnými a komunikačnými technológiami (IKT)**. Tento systém je navrhnutý v súlade s požiadavkami nariadenia DORA a súvisiacich technických štandardov (RTS/ITS), ktoré upravujú oznamovanie „závažných incidentov“ príslušným regulačným orgánom (NBS).

Interná evidencia incidentov

Spoločnosť vedie centrálny elektronický register incidentov, ktorý umožňuje sledovať celý životný cyklus incidentu – od jeho vzniku až po uzavretie. Evidencia obsahuje tieto kľúčové údaje:

- Identifikátor incidentu
- Dátum a čas výskytu a detekcie
- Typ a klasifikácia incidentu (vrátane závažnosti)
- Dotknuté aktíva a funkcie
- Prijaté opatrenia a fáza riešenia
- Osoba zodpovedná za riešenie incidentu.

Na tento účel je využívaný formulár *Evidencia incidentov*, ktorý je spravovaný bezpečnostným tímom Finsys a pravidelne aktualizovaný. Evidencia zároveň slúži ako východisko pre reporting a analýzu trendov.

Hlásenie závažných incidentov

Pre incidenty, ktoré prekročia stanovené prahové hodnoty v súlade s klasifikačnými kritériami DORA (viď 3.3.2), je povinné vypracovanie a doručenie trojfázového hlásenia:

1. **Prvotné hlásenie** (do 4 hodín od klasifikácie ako závažný incident) – obsahuje základné fakty, predbežné zhodnotenie dopadu a plánované opatrenia.
2. **Priebežné hlásenie** sa podáva v prípade zmeny situácie alebo dodatočných zistení, ktoré majú významný vplyv na hodnotenie incidentu.
3. **Záverečné hlásenie** obsahuje kompletné vyhodnotenie príčin, prijatých opatrení a odporúčaní na zamedzenie opakovania.

Na formálne oznamovanie incidentov je používaný štruktúrovaný dokument **Hlásenie o incidente**, ktorý je súčasťou interných smerníc. Tento formulár bol prispôsobený tak, aby spĺňal obsahové náležitosti podľa RTS/ITS a požiadaviek národných orgánov dohľadu.

Riadenie a kontrola oznamovacieho procesu

Za vypracovanie a odoslanie hlásení je zodpovedný Incident manažér, ktorý zároveň zabezpečuje ich uloženie a archiváciu. Súčasťou procesu je aj interná kontrola kvality údajov a validácia správnosti klasifikácie. V prípade závažných incidentov sa aktivuje aj krízový tím, ktorý koordinuje komunikáciu s externými subjektmi.

Hlásenie závažného incidentu súvisiaceho s IKT

Všeobecné informácie o finančnom subjekte		
1.1	Typ správy	Prvotné oznámenie
1.2	Názov subjektu, ktorý správu podáva	Finsys s.r.o.
1.3	Identifikačný kód subjektu, ktorý správu podáva	IČO: 12345678
1.4	Typ dotknutého subjektu	Poskytovatel digitálních služeb (ICT)
1.5	Názov dotknutého subjektu (ak je odlišný od subjektu podávajúceho správu)	-
1.6	Kód LEI dotknutého subjektu (ak je odlišný od subjektu podávajúceho správu)	-
1.7	Primárna kontaktná osoba (meno, email, telefón)	Ing. Anna Nováková, ciso@finsys.sk, +421 721 555 441
1.8	Sekundárna kontaktná osoba (meno, email, telefón)	Tomáš Gregor, backend@finsys.sk, +421 778 312 145
1.9	Název mateřského podniku	-
1.10	Kód LEI mateřského podniku	-
1.11	Měna	EUR

Náležitosti prvotného oznámenia		
2.1	Referenčný kód incidentu poskytnutý finančným subjektom	INC-2025-004
2.2	Dátum a čas zistenia incidentu	2025-05-01 17:05
2.3	Dátum a čas klasifikácie incidentu ako závažného	2025-05-01 17:45
2.4	Popis incidentu	Externý aktér zneužil nezaplátanú zraniteľnosť v rozhraní REST API aplikácie *FinSecure Exchange*, čím získal administratívny prístup k časti systému bez autentifikácie. Išlo o „zero-day" zraniteľnosť odhalenú až po podozrivej zmene systémových logov. Dočasne bola obmedzená funkcionalita platformy, služby pre klientov boli deaktivované ako preventívne opatrenie.
2.5	Klasifikačné kritériá, na základe ktorých bolo podané hlásenie o incidente	Zasiahnutie viac ako 25 % klientov, narušenie dôvernosti a integrity systému, nedostupnosť služieb > 1 hodina
2.6	Prahová hodnota významnosti pre klasifikačné kritérium „územný rozsah"	Objekt v rámci SR
2.7	Informácie o tom, ako bol incident zistený	Log alerty z backend systému a SIEM upozornenie
2.8	Informácie o tom, či má incident pôvod od poskytovateľa z radov tretích strán alebo od iného finančného subjektu	Nie – vnútorná aplikačná zraniteľnosť
2.9	Údaj o tom, či bol aktivovaný plán kontinuity prevádzky	ANO
2.10	Ďalšie informácie, ak sú relevantné	Prebieha forenzná analýza. Dočasne obmedzený prístup do administrácie. Klientom boli poskytnuté informácie cez alternatívny kanál.

Náležitosti priebežnej správy		
3.1	Referenčný kód incidentu poskytnutý príslušným orgánom	Zatiaľ nepridelené
3.2	Dátum a čas vzniku incidentu	2025-05-01 16:40
3.3	Dátum a čas obnovenia služieb, činností a/alebo operácií	2025-05-01 19:30
3.4	Počet dotknutých klientov	2
3.5	Percento dotknutých klientov	50%
3.6	Počet dotknutých finančných protistrán	1
3.7	Percento dotknutých finančných protistrán	25%
3.8	Vplyv na príslušných klientov alebo finančné protistrany	ANO
3.9	Počet dotknutých transakcií	12
3.10	Percento dotknutých transakcií	9%
3.11	Hodnota dotknutých transakcií	42 360€
3.12	Informácie o tom, či ide o skutočné čísla alebo odhady, prípadne či nedošlo k žiadnemu vplyvu	Odhad – na základe porovnania dennej prevádzky a forenznej analýzy
3.13	Poškodenie dobrej povesti	Áno
3.14	Súvisiace informácie o poškodení dobrej povesti	Zaznamenaná diskusia na Twitteri, podanie na NBS
3.15	Trvanie incidentu	2 hodiny 50 minút
3.16	Doba odstávky služby	2 hodiny 30 minút
3.17	Informácie o tom, či sú údaje o dobe trvania incidentu a o	Skutočné – potvrdené SIEM systémom a manuálnym potvrdením z tímu DevOps

Obrázok č.71 Hlásenie závežného IKT incidentu – vzorové vyplnenie (Zdroj: Vlastné spracovanie)

3.4 Návrh testovania digitálnej prevádzkovej odolnosti a kontinuity činností

3.4.1 Návrh programu testovania digitálnej prevádzkovej odolnosti

Spoločnosť Finsys implementovala systematický program **Testovania digitálnej prevádzkovej odolnosti** (DPO) s cieľom overiť pripravenosť informačných systémov, procesov a tímov na zvládanie incidentov a narušení v oblasti IKT. Program vychádza z požiadaviek nariadenia DORA a zohľadňuje veľkosť, obchodný profil a rizikový kontext spoločnosti. Program bol navrhnutý autorom tejto práce.

Politika a procedúry testovania DPO

Testovanie digitálnej odolnosti je riadené formálnou politikou testovania DPO, ktorá definuje:

- **Záväznosť** a zodpovednosti za plánovanie a vykonávanie testov.
- **Rozsah a typy testov** podľa kritickosti systémov a funkcií.
- **Frekvenciu testovania** – minimálne ročne, pri významných zmenách systémov, po incidentoch a na základe výstupov z hodnotenia rizík.

Východiskovým dokumentom pre realizáciu testovania je **metodický rámec Testovanie digitálnej prevádzkovej odolnosti**. Tento dokument systematizuje hlavné zásady a požiadavky testovania a je rozčlenený do tematických častí, ktoré upravujú:

I. Obecné zásady – definujú základné princípy testovania vrátane periodicity, požiadaviek na nezávislosť testujúcich subjektov, dokumentovania a validácie výsledkov.

II. Testovacie prostredie – špecifikuje požiadavky na oddelené, realistické a bezpečné testovacie prostredie vrátane podmienok jeho prevádzky a aktualizácie.

III. Testovanie systémov IKT – opisuje metodiky pre funkčné a záťažové testy kľúčových aplikácií, infraštruktúry a systémových komponentov. Zároveň stanovuje požiadavky na realizáciu testovania zabezpečenia softvérového kódu prostredníctvom SAST (Static Application Security Testing) a DAST (Dynamic Application Security Testing), ktoré umožňujú identifikovať zraniteľnosti už počas vývoja a v bežnej prevádzke systémov.

IV. Testovanie detekčných mechanizmov – zameriava sa na overenie účinnosti bezpečnostných nástrojov ako SIEM, IDS/IPS a antivírusových riešení pri simulovaných scenároch hrozieb.

V. Testovanie plánov krízovej komunikácie – overuje pripravenosť komunikačných kanálov a tímov na efektívne zvládnutie komunikácie počas incidentov.

VI. Testovanie plánov ukončenia zmluvného vzťahu s poskytovateľom služieb IKT – hodnotí pripravenosť na plánovaný alebo núdzový prechod služieb medzi dodávateľmi, vrátane dostupnosti potrebnej dokumentácie a údajov.

VII. Zistené nedostatky – sumarizuje pravidlá pre evidenciu, vyhodnotenie a riešenie nedostatkov identifikovaných počas testovania. Stanovuje tiež spôsob ich sledovania, priradenie zodpovedností a kontrolu účinnosti prijatých nápravných opatrení.

Typy testov

Program testovania DPO zahŕňa široké spektrum testovacích aktivít:

- **Skenovanie zraniteľností** – pravidelné a *ad hoc* skeny systémov s cieľom identifikovať technické slabiny
- **Penetračné testovanie** – simulované útoky na vybrané komponenty infraštruktúry (externé aj interné)
- **Testy kontinuity činností a obnovy** – simulácie výpadkov a obnovy procesov podľa plánov obnovy
- **Testy fyzickej bezpečnosti** – overenie prístupu do zabezpečených priestorov, kontrola zásady „čistého stola“
- **Testy komunikačných plánov** – cvičenia zamerané na reakciu a koordináciu krízového tímu, vrátane internej a externej komunikácie

Každý typ testu je prispôsobený konkrétnemu prostrediu a rizikovému profilu, pričom sa dôsledne využívajú **izolované testovacie prostredia**, aby sa predišlo narušeniu produkčných systémov.

Program testovania a evidencia výsledkov

Na zabezpečenie systematického plánovania a riadenia testovacích aktivít bol zavedený centralizovaný evidenčný nástroj, ktorý slúži na zaznamenávanie všetkých plánovaných a realizovaných testov digitálnej prevádzkovej odolnosti. Tento nástroj obsahuje:

- identifikátor a názov testu
- plánovaný a posledný dátum vykonania testovania
- zistené nedostatky z predchádzajúcich testov a prijaté bezpečnostné opatrenia
- kategorizáciu potrebných zdrojov (technické, finančné, ľudské a informačné)
- metriku na vyhodnotenie úspešnosti testu

Evidencia slúži nielen ako plánovací a dokumentačný nástroj, ale aj ako základ pre analýzu trendov, sledovanie vývoja odolnosti a spätné začlenenie výsledkov do procesov riadenia rizík a obnovy. Údaje sú pravidelne aktualizované a vyhodnocované bezpečnostným tímom v spolupráci s vedením spoločnosti.

Vyhodnocovanie a nepretržité zlepšovanie

Výsledky testovania sú pravidelne vyhodnocované a prerokovávané vedením spoločnosti. Zistenia z testov sú implementované do plánov obnovy, bezpečnostných opatrení a školení. Testovanie je súčasťou **cyklu PDCA** a zabezpečuje spätnú väzbu pre ďalší rozvoj rámca digitálnej prevádzkovej odolnosti.

ID	Názov testu	Termín plánovaného testovania	Dátum posledného testovania	Zistené nedostatky z posledného testovania	Zavedené bezpečnostné opatrenia z posledného testovania	Potrebné zdroje				Metrika pre vyhodnotenie úspešnosti
						Technické	Finančné	Ľudské	Informačné	
T1	Plán ukončenia zmluvného vzťahu (č. 005022024)	15.6.2026	-	-	-	0	200 €	2 MD vedúci tech. oddelenia + externé právne oddelenie	-	Zmluva bola formálne ukončená potvrdením o výpovedi, prenesené boli všetky dohodnuté údaje a služby do alternatívneho prostredia v termíne do 5 pracovných dní bez výpadku služieb
T2	Test validačných pravidiel pre vstupné dáta	15.7.2025	-	-	-	1 500 €	1 500 €	1 MD vývojový tím	-	Validačné logy potvrdzujú, že 100 % vstupov so zámerným porušením dátovej štruktúry bolo správne odmietnutých systémom
T3	Plán obnovy č. 2 (kybernetický útok)	5.7.2025	15.3.2025	Potrebné doplniť postup izolácie cloudových prostredí	Zavedené nové zálohovacie skripty a autentizačné mechanizmy	3 000 €	800 €	3 MD technologický tím	-	Úspešná simulácia obnovy systémov po kybernetickom útoku
T4	Test API autentizácie a revokácií	5.11.2025	-	-	-	2 800 €	500 €	1 MD DevOps + vývojár	-	100 % úspešná autentizácia a okamžitá deaktivácia tokenov po revokácii
T5	Simulácia zlyhania poskytovateľa IKT	12.12.2025	10.12.2024	Závislosť na jedinom dodávateľovi	Uzavreté partnerstvo s alternatívnym poskytovateľom	0 €	2 000 €	2 MD právnici (externí) + IT vedenie	Smernica o dodávateľoch	Plne funkčný prechod služieb do 30 minút bez prerušenia SLA a so zachovaním dostupnosti nad 99,9 %
T6	Test bezpečnostného povedomia zamestnancov	10.10.2025	3.4.2025	Nízka úroveň povedomia zamestnancov v oblasti rozpoznávania phishingových e-mailov	-	0 €	100 €	1 MD všetci zamestnanci + externý školiteľ	-	Účasť min. 90 % zamestnancov na školení a úspešné zvládnutie simulovaného phishingového útoku 2 mesiace po školení
T7	Test detekčného mechanizmu SIEM	16.1.2026	-	-	-	1 500 €	1 500 €	1 MD vývojový tím	-	SIEM systém správne detegoval 100 % simulovaných bezpečnostných udalostí, do 5 minút od ich vzniku a vytvoril relevantné výstrahy podľa nastavených pravidiel korelácie
T8	Test krízovej komunikácie	18.9.2025	10.3.2024	Neúplné kontaktné údaje v krízovom pláne a oneskorená aktivácia komunikačného tímu	Aktualizácia kontaktných údajov, zavedenie rotačných kontro	0 €	400 €	1 MD krízový tím + vedenie	Interná smernica pre krízovú komunikáciu	Úspešná aktivácia komunikačného tímu do 5 min. a doručenie všetkých správ určeným adresátom

Obrázok č.72 Program testovania DPO (Zdroj: Vlastné spracovanie)

3.4.2 Návrh politiky kontinuity činností a obnovy po havárii (BCDR)

V rámci posilňovania digitálnej prevádzkovej odolnosti a v súlade s požiadavkami nariadenia DORA spoločnosť Finsys vypracovala a prijala formálny **rámec pre riadenie kontinuity činností a obnovy po havárii (BCDR)**.

Tento rámec bol vytvorený autorom tejto práce a je zakotvený v dokumente **Politika zachovania prevádzky IKT**, ktorý definuje strategické princípy zabezpečenia nepretržitého fungovania kritických systémov. Na operatívnej úrovni je táto politika doplnená o **Pohotovostný plán**, ktorý špecifikuje konkrétne pohotovostné scenáre a reakčné postupy.

V nadväznosti na tieto kľúčové dokumenty bolo vypracovaných **osem samostatných plánov obnovy**, pokrývajúcich najzásadnejšie rizikové situácie. Ako príklad možno uviesť **Plán obnovy č. 2 (kybernetický útok)**, ktorý stanovuje konkrétne kroky reakcie a obnovy v prípade kybernetického incidentu s dopadom na infraštruktúru a služby.

Základné komponenty politiky BCDR:

I. Stratégia zálohovania dát a systémov

Politika definuje viacúrovňový prístup k zálohovaniu, založený na pravidle 3-2-1, so zabezpečením záloh na viacerých médiách a lokalitách. Zálohovanie sa vykonáva v pravidelných intervaloch (denne, týždenne, mesačne) s dôrazom na systémy spracúvajúce kritické alebo citlivé dáta. Všetky zálohy sú šifrované a testované na obnoviteľnosť.

II. Definovanie RTO a RPO

Pre každú kľúčovú IKT funkciu, bol stanovený cieľový čas obnovy (RTO) a cieľový bod obnovy dát (RPO). Tieto parametre vychádzajú z analýzy kritickosti funkcií vykonanej v predchádzajúcich etapách (pozri kap. 3.2.1) a z analýzy vplyvu na podnikanie (BIA). Tieto parametre reflektujú prípustné limity výpadku pre zachovanie integrity služieb.

III. Plány obnovy podľa scenárov

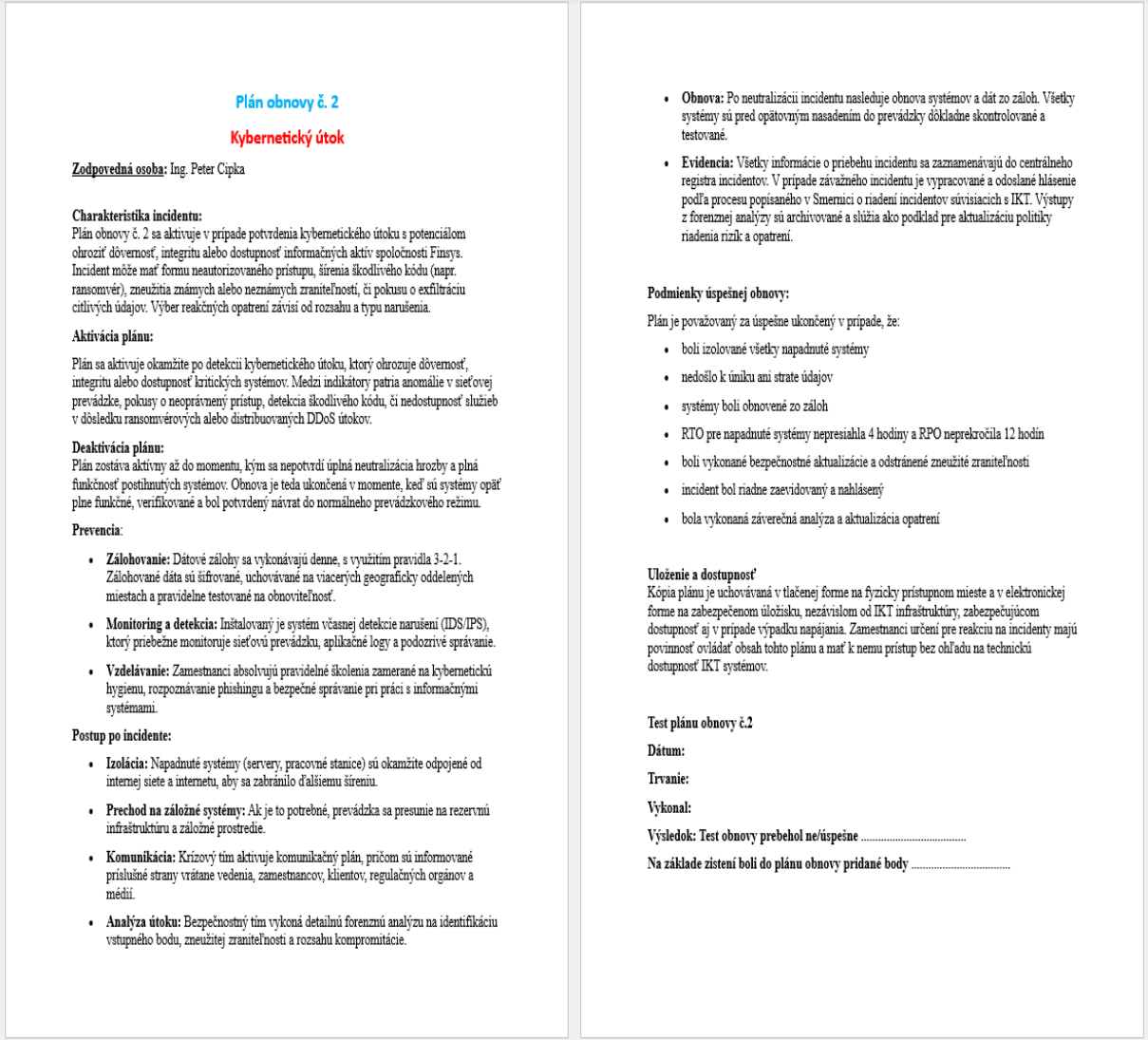
V rámci politiky boli vypracované konkrétne obnovovacie plány pre najpravdepodobnejšie a najzávažnejšie typy incidentov. Plán obnovy č. 2, zameraný na kybernetický útok, definuje okamžité kroky izolácie infikovaných systémov, aktiváciu rezervnej infraštruktúry a komunikačné postupy v rámci krízového tímu. Pre ostatné scenáre (napr. výpadok napájania, fyzické poškodenie serverovne) sú pripravené ďalšie čiastkové plány vychádzajúce z pohotovostného plánu.

IV. Pohotovostné a eskalačné postupy

Pohotovostný plán tvorí operatívnu nadstavbu politiky BCDR. Stanovuje detailné kroky pre zvládanie rôznych typov narušení – od kybernetických útokov cez prírodné katastrofy až po nedostupnosť zamestnancov. Súčasťou sú aj eskalačné matice, kontaktné osoby a rozpis kompetencií v rámci krízového riadenia.

V. Testovanie a revízia politiky

Politika BCDR podlieha pravidelnému testovaniu prostredníctvom simulačných cvičení a záťažových testov, ktoré overujú efektívnosť pohotovostných plánov, pripravenosť tímov a funkčnosť zálohovacích mechanizmov. Na základe zistení sa vykonávajú revízie politiky minimálne raz ročne, prípadne po každom významnom incidente.



Plán obnovy č. 2

Kybernetický útok

Zodpovedná osoba: Ing. Peter Cipka

Charakteristika incidentu:
Plán obnovy č. 2 sa aktivuje v prípade potvrdenia kybernetického útoku s potenciálom ohroziť dôvernosť, integritu alebo dostupnosť informačných aktív spoločnosti Finsys. Incident môže mať formu neautorizovaného prístupu, šírenia škodlivého kódu (napr. ransomvér), zneužitia známych alebo neznámych zraniteľností, či pokusu o exfiltráciu citlivých údajov. Výber reakčných opatrení závisí od rozsahu a typu narušenia.

Aktivácia plánu:

Plán sa aktivuje okamžite po detekcii kybernetického útoku, ktorý ohrozuje dôvernosť, integritu alebo dostupnosť kritických systémov. Medzi indikátory patria anomálie v sieťovej prevádzke, pokusy o neoprávnený prístup, detekcia škodlivého kódu, či nedostupnosť služieb v dôsledku ransomvérových alebo distribuovaných DDoS útokov.

Deaktivácia plánu:
Plán zostáva aktívny až do momentu, kým sa nepotvrdí úplná neutralizácia hrozby a plná funkčnosť postihnutých systémov. Obnova je teda ukončená v momente, keď sú systémy opäť plne funkčné, verifikované a bol potvrdený návrat do normálneho prevádzkového režimu.

Prevencia:

- **Zálohovanie:** Dátové zálohy sa vykonávajú denne, s využitím pravidla 3-2-1. Zálohované dáta sú šifrované, uchovávané na viacerých geograficky oddelených miestach a pravidelne testované na obnoviteľnosť.
- **Monitoring a detekcia:** Inštalovaný je systém včasnej detekcie narušení (IDS/IPS), ktorý priebežne monitoruje sieťovú prevádzku, aplikačné logy a podozrivé správanie.
- **Vzdelávanie:** Zamestnanci absolvujú pravidelné školenia zamerané na kybernetickú hygienu, rozpoznávanie phishingu a bezpečné správanie pri práci s informačnými systémami.

Postup po incidente:

- **Izolácia:** Napadnuté systémy (servery, pracovné stanice) sú okamžite odpojené od internej siete a internetu, aby sa zabránilo ďalšiemu šíreniu.
- **Prechod na záložné systémy:** Ak je to potrebné, prevádzka sa presunie na rezervnú infraštruktúru a záložné prostredie.
- **Komunikácia:** Krízový tím aktivuje komunikačný plán, pričom sú informované príslušné strany vrátane vedenia, zamestnancov, klientov, regulačných orgánov a médií.
- **Analýza útoku:** Bezpečnostný tím vykoná detailnú forenznú analýzu na identifikáciu vstupného bodu, zneužitej zraniteľnosti a rozsahu kompromitácie.

- **Obnova:** Po neutralizácii incidentu nasleduje obnova systémov a dát zo záloh. Všetky systémy sú pred opätovným nasadením do prevádzky dôkladne skontrolované a testované.
- **Evidencia:** Všetky informácie o priebehu incidentu sa zaznamenávajú do centrálneho registra incidentov. V prípade závažného incidentu je vypracované a odoslané hlásenie podľa procesu popísaného v Smernici o riadení incidentov súvisiacich s IKT. Výstupy z forenznej analýzy sú archivované a slúžia ako podklad pre aktualizáciu politiky riadenia rizík a opatrení.

Podmienky úspešnej obnovy:

Plán je považovaný za úspešne ukončený v prípade, že:

- boli izolované všetky napadnuté systémy
- nedošlo k úniku ani strate údajov
- systémy boli obnovené zo záloh
- RTO pre napadnuté systémy nepresiahla 4 hodiny a RPO neprekročila 12 hodín
- boli vykonané bezpečnostné aktualizácie a odstránené zneužité zraniteľnosti
- incident bol riadne zaevidovaný a nahlásený
- bola vykonaná záverečná analýza a aktualizácia opatrení

Uloženie a dostupnosť
Kópia plánu je uchovávaná v tlačenej forme na fyzicky prístupnom mieste a v elektronickej forme na zabezpečenom úložisku, nezávislom od IKT infraštruktúry, zabezpečujúcom dostupnosť aj v prípade výpadku napájania. Zamestnanci určení pre reakciu na incidenty majú povinnosť ovládať obsah tohto plánu a mať k nemu prístup bez ohľadu na technickú dostupnosť IKT systémov.

Test plánu obnovy č.2

Dátum:

Trvanie:

Vykonal:

Výsledok: Test obnovy prebehol ne/úspešne .....

Na základe zistení boli do plánu obnovy pridané body .....

Obrázok č.73 Plán obnovy č.2 - kybernetický útok (Zdroj: Vlastné spracovanie)

3.5 Návrh riadenia rizík IKT spojených s tretími stranami

3.5.1 Návrh politiky riadenia rizík tretích strán

V súlade s požiadavkami nariadenia DORA a v nadväznosti na rámec riadenia rizík IKT, spoločnosť Finsys implementovala samostatnú **Politiku riadenia rizík v oblasti IKT spojeného s tretími stranami**. Táto politika predstavuje špecializovaný interný predpis, ktorého cieľom je systematicky riadiť riziká vyplývajúce zo vzťahov s externými poskytovateľmi IKT služieb **počas celého životného cyklu týchto vzťahov** – od predzmluvnej fázy, cez uzatváranie a správu zmlúv, až po ich ukončenie a prechod na nového poskytovateľa.

Politika bola vytvorená autorom tejto práce a zahŕňa tieto základné oblasti.

I. Predzmluvná fáza a výber poskytovateľov

Každá spolupráca s tretími stranami podlieha vopred stanovenému procesu due diligence, ktorý zahŕňa posúdenie finančnej stability, technickej a prevádzkovej spôsobilosti, ako aj hodnotenie miery IKT rizika vrátane rizika koncentrácie. Dôležitou súčasťou predzmluvnej analýzy je aj posúdenie úrovne kybernetickej odolnosti potenciálneho poskytovateľa a jeho schopnosti zabezpečiť kontinuitu služieb a riadne reagovať na incidenty.

II. Hodnotenie rizík a prevencia konfliktu záujmov

Každý externý vzťah je podrobený systematickému hodnoteniu rizík vrátane identifikácie potenciálnych konfliktov záujmov. Hodnotenie zahŕňa aj analýzu dopadov na dôvernosť, integritu a dostupnosť údajov a služieb, ako aj schopnosť dodávateľa reagovať na incidenty.

III. Zmluvné ujednania

Zmluvy s poskytovateľmi musia obsahovať povinné bezpečnostné doložky, ako napríklad požiadavky na dostupnosť služieb, auditovateľnosť, subdodávky, právo na ukončenie zmluvy a plán prechodného obdobia.

IV. Monitorovanie a kontrola počas trvania zmluvy

Počas celej doby trvania spolupráce je vykonávané priebežné monitorovanie plnenia zmluvných požiadaviek. Zahŕňa:

- **Pravidelné hodnotenie SLA parametrov a výkonnosti služieb**
- **Overenie pripravenosti na incidenty a zmeny v zabezpečení** – bezpečnostné hodnotenia
- **Aktualizáciu rizikového profilu dodávateľa** – rizikový monitoring

Tieto aktivity sú zaznamenávané a slúžia ako vstup pre prípadnú úpravu zmluvných opatrení, ako aj pre aktualizáciu rizikového profilu dodávateľa v rámci evidencie tretích strán.

V. Riadenie subdodávateľov

V prípade zapojenia ďalších subdodávateľov je nevyhnutné vykonať dodatočné hodnotenie rizík a zabezpečiť zmluvné záruky, že subdodávateľ bude dodržiavať rovnaké požiadavky ako hlavný dodávateľ. Zvláštna pozornosť sa venuje sledovaniu zmien v reťazci subdodávateľov.

VI. Ukončenie zmluvného vzťahu a prechod

Politika obsahuje štandardizovaný **Plán ukončenia a prechodu**, ktorý zabezpečuje riadený prechod služieb na iného poskytovateľa alebo do interného prostredia. Plán definuje podmienky ukončenia, výpovedné lehoty, identifikáciu ovplyvnených funkcií a povinnosť zabezpečiť integritu a dostupnosť údajov počas celej prechodnej fázy.

VII. Registrácia a evidencia informácií

Všetky vzťahy s tretími stranami, vrátane identifikácie poskytovateľa, zmluvného rámca, hodnotenia rizík a výsledkov monitorovania, sú evidované v centrálnom **Registri informácií**.

3.5.2 Návrh vytvorenia a údržby registra informácií o využívaní tretích strán

V súlade s nariadením DORA zaviedla spoločnosť Finsys centralizovaný **Register informácií o využívaní tretích strán**, ktorý systematizuje a sprístupňuje všetky kľúčové údaje o externých poskytovateľoch IKT služieb. Tento register tvorí základný nástroj pre zabezpečenie transparentnosti, riadenia rizík a preukázateľnosti voči regulačným orgánom.

Štruktúra a obsah registra

Register je vedený v elektronickej forme a je tvorený viacerými navzájom prepojenými modulmi. Register zahŕňa najmä tieto oblasti:

- **Zoznam poskytovateľov IKT služieb** – meno poskytovateľa, IČO, kontaktná osoba, status (aktívny/neaktívny), kategória (kritický/dôležitý/štandardný), úroveň certifikácie.
- **Zoznam poskytovaných služieb a ich klasifikácia** – popis služby, jej zaradenie podľa typu (napr. hosting, cloud, softvérové riešenie), a prepojenie na funkcie definované v rámci Finsys.

- **Zmluvné ujednania** – údaje o uzatvorených zmluvách, typ zmlúv, ich platnosť, dátum uzatvorenia, trvanie, výpovedné lehoty, existencia SLA, doložky o audite, nahlasovaní incidentov a subdodávkach.
- **Subdodávatelia** – identifikácia a schválenie zapojených subdodávateľov, rozsah ich plnenia, vzájomné väzby, kontrolné mechanizmy.
- **Geografická lokalizácia dát** – krajina alebo jurisdikcia spracovania, miesto uloženia hlavných údajov (umiestnenie dátových centier), prípadné prenosy mimo EÚ.
- **Kritickosť služby** – hodnotenie služby na základe jej obchodného významu a vplyvu na prevádzku spoločnosti – či ide o službu podporujúcu kritické, dôležité alebo štandardné funkcie, hodnotenie úrovne závislosti.

Proces správy a aktualizácie

Register je spravovaný vedúcim technologického oddelenia v spolupráci s externým právnym oddelením. Pravidlá aktualizácie zahŕňajú:

- **Povinnosť aktualizácie pri zmene zmluvných podmienok, poskytovateľa, typu služby** a pri identifikovaní nového rizika.
- **Štvrťročná kontrola správnosti údajov** na základe výstupov z monitorovania poskytovateľov.
- **Auditná stopa všetkých zmien** vrátane identifikácie osoby, ktorá zmenu vykonala.

Hodnotenie služieb IKT												
Referenčné číslo zmluvnej dohody	ID poskytovateľa služieb IKT	Nekódovaný typ IKT služby	Nahraditeľnosť poskytovateľa služieb IKT	Dôvod, ak je poskytovateľ služieb IKT považovaný za nenahraditeľného alebo vysoko ťažko nahraditeľného	Dátum posledného auditu poskytovateľa služieb IKT	Plán ukončenia zmluvného vzťahu	Možnosť reintegrácie zazmluvnenej služby IKT	Vplyv ukončenia služby IKT	Sú určení alternatívni poskytovatelia služieb IKT?	Identifikácia alternatívneho poskytovateľa služieb IKT
ZML-001	P1	Azure IaaS	Náročná - Vysoko ťažko nahraditeľný	Vysoká integrácia do IKT infraštruktúry	15.3.2024	Áno	Obtiažne	Vysoký	Áno	Amazon Web Services
ZML-002	P2	Azure VPN Gateway	Náročná - Vysoko ťažko nahraditeľný	Bezpečnostné prepojenie celej siete	10.12.2023	Áno	Jednoduché	Stredný	Áno	Fortinet VPN Cloud
ZML-003	P3	Azure Web Server	Náročná - Vysoko ťažko nahraditeľný	Prevádzka hlavných aplikácií	1.2.2024	Áno	Vysoko obtiažne	Vysoký	Áno	Google Cloud App Engine
ZML-004	P4	M365	Jednoduchá - Jednoducho nahraditeľný	-	22.11.2023	Áno	Jednoduché	Hodnotenie nebolo vykonané	Nie	-
ZML-005	P5	CRM softvér	Stredná - Stredne ťažko nahraditeľný	-	20.1.2024	Áno	Obtiažne	Stredný	Áno	Salesforce
FNS-01	SK-DOMREG-01	DNS / Domény	Stredná - Stredne ťažko nahraditeľný	-	7.4.2024	Čiastočný	Jednoduché	Hodnotenie nebolo vykonané	Nie	-
FNS-02	SK-BANKA-INT	Banking API služby	Náročná - Vysoko ťažko nahraditeľný	Integrácia s platbami, AML	-	Nie	Vysoko obtiažne	Kritický	Nie	-
FNS-03	PROXY-LOG	Monitoring logov	Jednoduchá - Jednoducho nahraditeľný	-	9.2.2025	Áno	Obtiažne	Stredný	Nie	-

Obrázok č.74 Hodnotenie služieb IKT – vzorové vyplnenie (anonymita) (Zdroj: Vlastné spracovanie)

3.5.3 Návrh stratégie ukončenia spolupráce (Exit Strategy)

V súlade s požiadavkami nariadenia DORA, ktoré kladú dôraz na zabezpečenie kontinuity kritických a dôležitých IKT funkcií aj v prípade ukončenia zmluvného vzťahu s externým poskytovateľom, prijala spoločnosť Finsys **formálnu stratégiu ukončenia spolupráce**, označovanú ako *Exit Strategy*.

Táto stratégia predstavuje **systematický súbor plánovacích a vykonávacích krokov, ktorých cieľom je zabezpečiť riadený prechod služieb bez ohrozenia prevádzkovej kontinuity**, integrity údajov alebo kybernetickej bezpečnosti.

Účel a uplatnenie stratégie

Stratégia sa uplatňuje pri všetkých zmluvných vzťahoch týkajúcich sa **kritických alebo dôležitých IKT funkcií**. Jej účelom je:

- minimalizovať riziká spojené s náhlym alebo plánovaným ukončením spolupráce
- zabezpečiť dostupnosť alternatívneho riešenia (náhradného poskytovateľa alebo interného zabezpečenia služieb)
- zaistiť riadny prenos aktív, dát a kompetencií
- ochrániť citlivé údaje a ukončiť všetky prístupy poskytovateľa

Plán ukončenia a prechodu

Zo stratégie ukončenia vychádzajú individuálne **plány ukončenia**, ktoré sú vypracované osobitne pre každého **kritického alebo dôležitého poskytovateľa IKT služieb.** Tieto plány definujú štruktúrovaný postup pre každé ukončenie zmluvného vzťahu

Plán ukončenia a prechodu - základné prvky

Analýza závislosti a vplyvu

Pre každý zmluvný vzťah je vyhodnotená miera závislosti spoločnosti Finsys na poskytovanej službe, jej prepojenie na kritické funkcie a potenciálny dopad ukončenia.

Výber alternatívneho riešenia

Identifikujú sa možné alternatívy – buď náhradní poskytovatelia s rovnocennou službou, alebo možnosť presunu služieb do interného prostredia (in-house). Zohľadňujú sa pri tom technické, právne a finančné aspekty.

Identifikácia dôvodov ukončenia

Medzi typické dôvody patria neplnenie SLA, bezpečnostné incidenty, strategické rozhodnutie či fúzia alebo akvizícia partnera.

Identifikácia ovplyvnených funkcií a služieb

Podrobný výpis všetkých služieb a IKT funkcií, ktoré sú predmetom poskytovania, vrátane ich klasifikácie z pohľadu kritickosti.

Plán prechodu (Transition Plan)

Obsahuje harmonogram a organizačné kroky na zabezpečenie kontinuity služieb, vrátane:

- časového rámca ukončenia
- zodpovedných osôb
- definície cieľového stavu po prechode
- požiadaviek na poskytovateľa pri odovzdaní služieb.

Zachovanie prevádzkovej kontinuity

Identifikácia kritických medzier a návrh dočasných opatrení na zabezpečenie nepretržitého fungovania služieb počas prechodného obdobia.

Prenos a zabezpečenie dát

Stanovuje pravidlá pre bezpečný prenos dát od poskytovateľa vrátane formátu, šifrovania, kontrol integrity a verifikácie úplnosti údajov. Súčasťou je aj povinnosť poskytovateľa zmazať všetky kópie údajov po ukončení spolupráce.

Ukončenie prístupov a technická dekonekcia (odpojenie)

Určuje postup pri deaktivácii všetkých technických prístupov, účtov, API prepojení a oprávnení pridelených tretej strane v informačných systémoch spoločnosti. Tieto kroky sa vykonávajú v koordinácii s interným bezpečnostným tímom, ktorý je pre túto potrebu zriadený.

Zmluvné ustanovenia a výpovedné lehoty

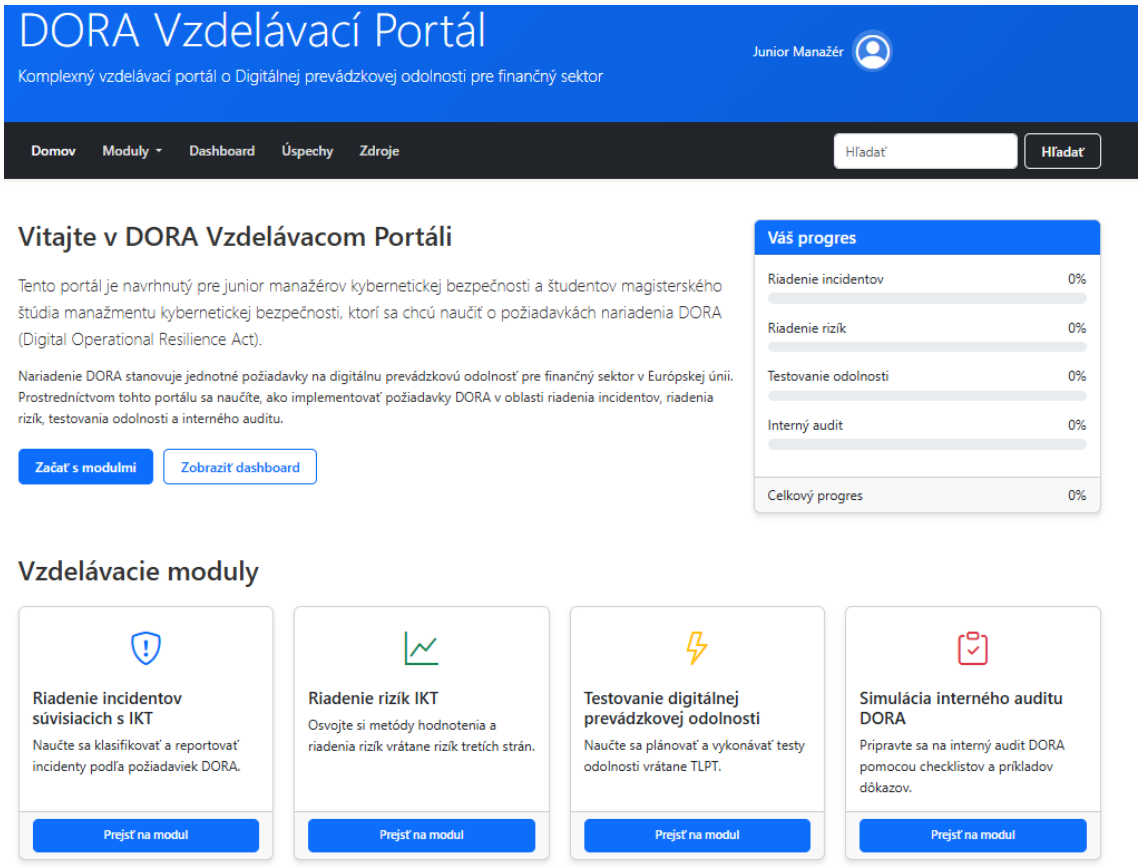
Plán zohľadňuje právne záväzky, výpovedné lehoty, doložky o asistencii pri prechode a súčinnosti poskytovateľa. V prípade potreby sa dojednávajú rozšírené prechodné obdobia.

Post-exit hodnotenie a aktualizácia registra

Po dokončení procesu prechodu sa vykonáva zhodnotenie priebehu a prípadné aktualizácie registra informácií, rizikového profilu a interných kontrol.

3.6 Proaktívne iniciatívy a nadstavbové opatrenia

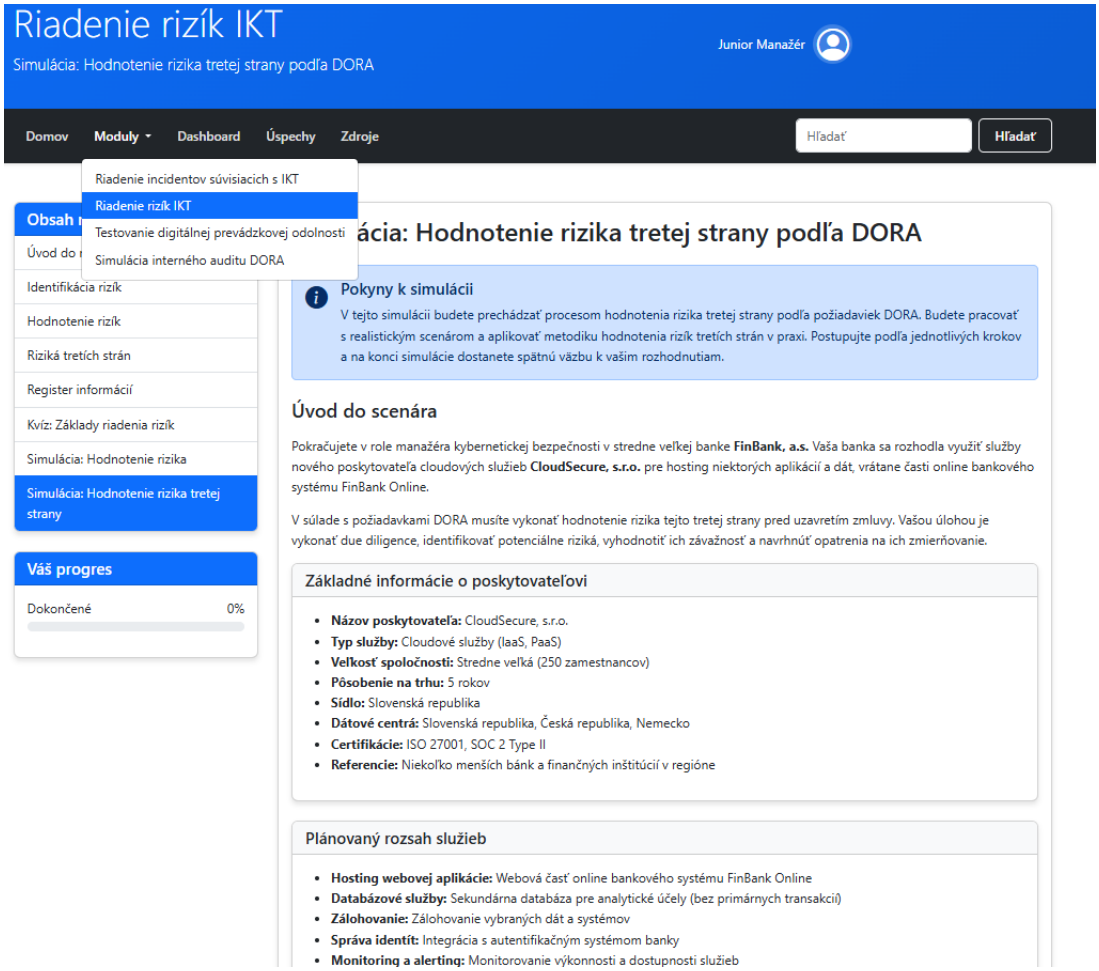
Okrem štandardnej implementácie opatrení vyplývajúcich z nariadenia DORA sa spoločnosť Finsys s.r.o., aj vďaka iniciatíve autora tejto práce, rozhodla realizovať niekoľko proaktívnych aktivít nad rámec regulačných požiadaviek. Tieto iniciatívy boli navrhnuté s cieľom posilniť kultúru bezpečnosti, zvýšiť digitálnu odolnosť a pripraviť sa na očakávané legislatívne zmeny. Zohľadňovali pritom aktuálny stav kybernetickej bezpečnosti spoločnosti ako aj rizikový profil spätý s poskytovaním finančno-technologických služieb vrátane obchodovania s kryptoaktívami.



Obrázok č.75 Vzdelávací portál – úvodná stránka (Zdroj: Vlastné spracovanie)

3.6.1 Vytvorenie vzdelávacieho portálu DORA

Najvýznamnejším nadstavbovým opatrením bolo navrhnutie a kompletná implementácia **interaktívneho vzdelávacieho portálu DORA**, ktorý bol vyvinutý autorom tejto práce ako interný nástroj pre štúdium a praktické osvojenie si požiadaviek nariadenia. Vzhľadom na chýbajúce centrálne vzdelávacie procesy a nízku úroveň povedomia o DORA medzi zamestnancami, portál predstavoval kľúčový nástroj na systematickú edukáciu.



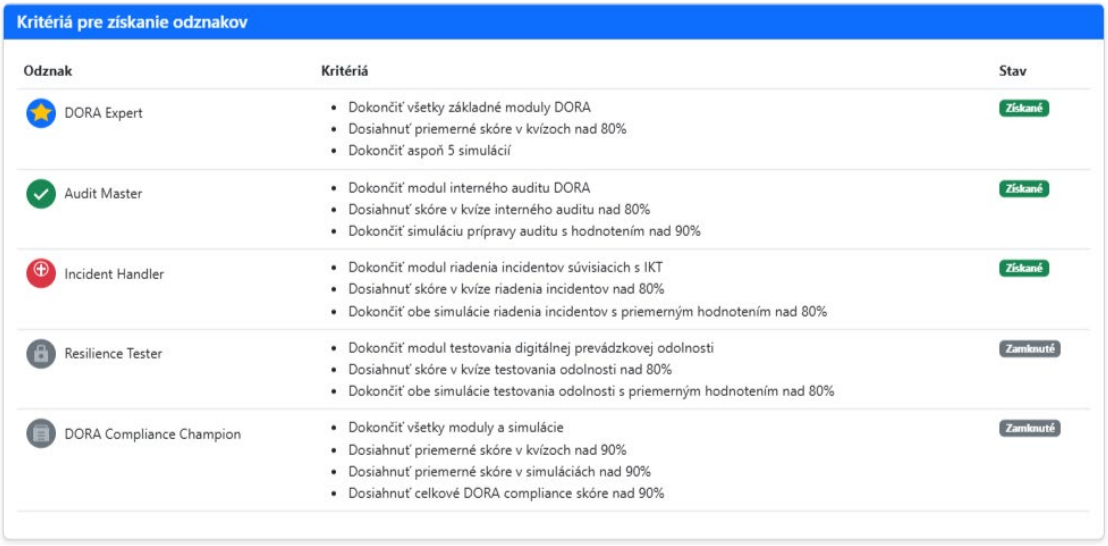
Obrázok č.76 Vzdelávací portál – Moduly (Zdroj: Vlastné spracovanie)

Portál, naprogramovaný v JavaScripte, ponúka 4 prehľadne spracované moduly: *Riadenie incidentov, Riadenie rizík IKT, Testovanie odolnosti a Interný audit*. Každý modul obsahuje teoretické časti, kvízy, simulácie a prepojenia na aktuálne šablóny dokumentácie. Personalizované dashboardy poskytujú zamestnancom prehľad o ich študijnom pokroku a odporúčania na doplnenie znalostí, zatiaľ čo vedeniu umožňujú rýchlo identifikovať slabé miesta zamestnancov v povedomí o DORA a cielene plánovať ďalšie vzdelávacie aktivity.

```
script.js ×

function updateProgressBars() {
    const progressData = getUserProgressData();
    const progressBars = document.querySelectorAll('.progress-bar');
    const progressTexts = document.querySelectorAll('.progress-item .justify-content-between span:last-child');

    if (progressBars.length > 0 && progressTexts.length > 0) {
        for (let i = 0; i < Math.min(progressBars.length, progressData.modules.length); i++) {
            const progress = progressData.modules[i].progress;
            progressBars[i].style.width = `${progress}%`;
            progressTexts[i].textContent = `${progress}%`;
        }

        const footerProgress = document.querySelector('.card-footer .justify-content-between span:last-child');
        if (footerProgress) {
            footerProgress.textContent = `${progressData.overall}%`;
        }
    }
}

function getUserProgressData() {
        return {
        modules: [
            { id: 'incident_management', name: 'Riadenie incidentov', progress: 0 },
            { id: 'risk_management', name: 'Riadenie rizík', progress: 0 },
            { id: 'resilience_testing', name: 'Testovanie odolnosti', progress: 0 },
            { id: 'internal_audit', name: 'Interný audit', progress: 0 }
        ],
        overall: 0
    };
}
function setupInteractiveElements() {
    setupQuizzes();
    setupSimulations();
    setupDecisionTrees();
}
```

Obrázok č.77 Vzdelávací portál – Javascript ukážka kódu (Zdroj: Vlastné spracovanie)

Motivujúcim prvkom portálu je aj systém odznakov, ktorý podporuje súťaživosť a angažovanosť zamestnancov tým, že oceňuje dosiahnuté výsledky v moduloch, kvízoch a simuláciách.

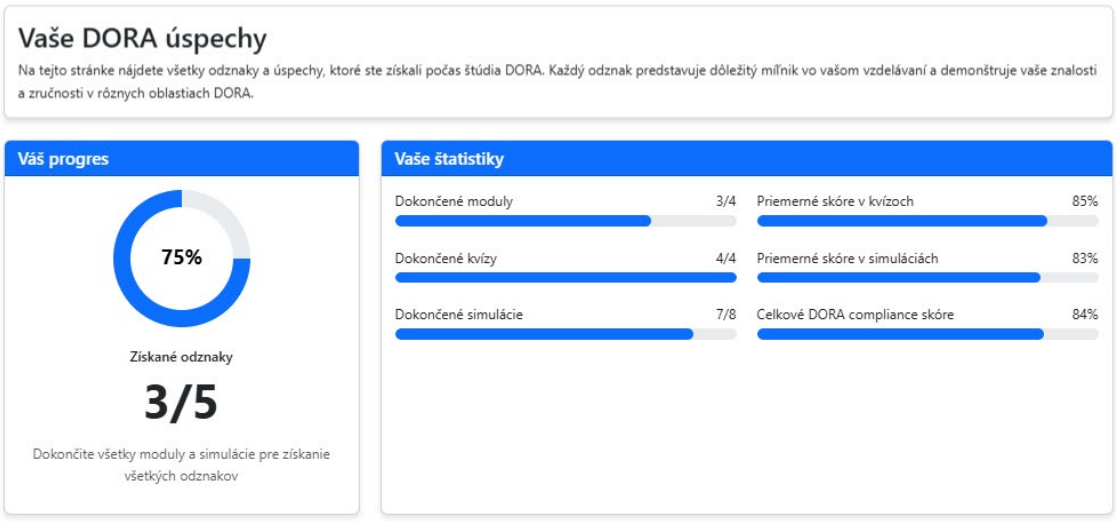


Kritériá pre získanie odznakov

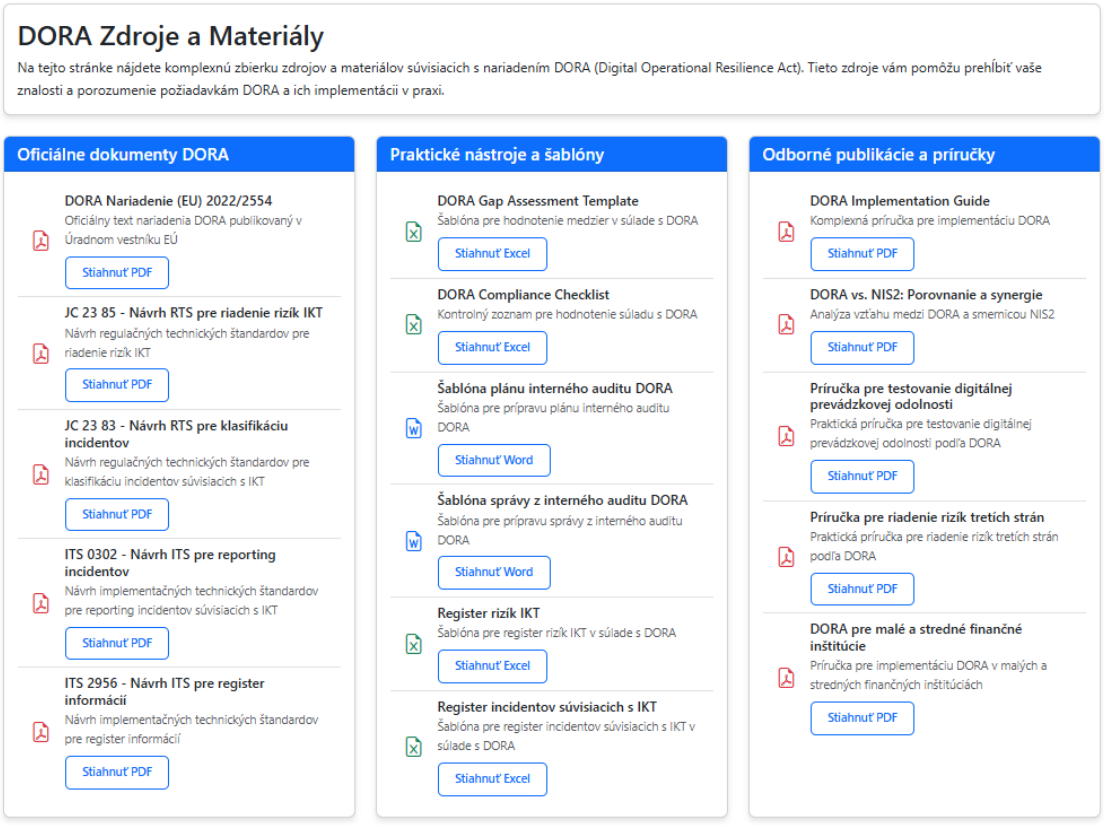
Odznak	Kritériá	Stav
DORA Expert	• Dokončiť všetky základné moduly DORA • Dosiahnuť priemerné skóre v kvízoch nad 80% • Dokončiť aspoň 5 simulácií	Získané
Audit Master	• Dokončiť modul interného auditu DORA • Dosiahnuť skóre v kvíze interného auditu nad 80% • Dokončiť simuláciu prípravy auditu s hodnotením nad 90%	Získané
Incident Handler	• Dokončiť modul riadenia incidentov súvisiacich s IKT • Dosiahnuť skóre v kvíze riadenia incidentov nad 80% • Dokončiť obe simulácie riadenia incidentov s priemerným hodnotením nad 80%	Získané
Resilience Tester	• Dokončiť modul testovania digitálnej prevádzkovej odolnosti • Dosiahnuť skóre v kvíze testovania odolnosti nad 80% • Dokončiť obe simulácie testovania odolnosti s priemerným hodnotením nad 80%	Zamknuté
DORA Compliance Champion	• Dokončiť všetky moduly a simulácie • Dosiahnuť priemerné skóre v kvízoch nad 90% • Dosiahnuť priemerné skóre v simuláciách nad 90% • Dosiahnuť celkové DORA compliance skóre nad 90%	Zamknuté

Obrázok č.78 Vzdelávací portál – Odznaky (Zdroj: Vlastné spracovanie)

Portál zároveň podporuje systematické budovanie bezpečnostného povedomia (security awareness) a posilňuje kultúru kybernetickej bezpečnosti, čo je obzvlášť dôležité pre spoločnosť ako Finsys, kde pred jeho zavedením absentoval formálny rámec pre riadenie bezpečnosti.



Obrázok č.79 Vzdelávací portál – Dashboard (Zdroj: Vlastné spracovanie)



Obrázok č.80 Vzdelávací portál – Zdroje a materiály (Zdroj: Vlastné spracovanie)

3.6.2 Licenčné riadenie MiCA

Vzhľadom na predmet podnikania spoločnosti Finsys s.r.o., ktorý je úzko spätý s poskytovaním služieb týkajúcich sa kryptoaktív, boli v spolupráci s externým právnym oddelením spoločnosti, za iniciatívy autora tejto práce, podniknuté proaktívne kroky smerujúce k dosiahnutiu súladu s požiadavkami *Nariadenia o trhoch s kryptoaktívami* (MiCA, Nariadenie (EÚ) 2023/1114). Konkrétne bolo iniciované licenčné konanie s Národnou bankou Slovenska (NBS), ako príslušným vnútroštátnym orgánom pre udeľovanie povolení poskytovateľom služieb súvisiacich s kryptoaktívami (CASP).

3.6.3 Implementácia pokročilých SIEM / SORA technológií

Ďalším nadstavbovým opatrením bolo nasadenie moderných systémov typu SIEM a SOAR (konkrétne Elastic a IBM QRadar), ktoré umožňujú pokročilý zber, koreláciu a analýzu bezpečnostných logov. Hoci spoločnosť predtým využívala open-source riešenie postavené na platformách Grafana a Prometheus, rozhodnutie prejsť na komerčné nástroje bolo motivované potrebou centralizovanej správy incidentov, automatizovaného vyhodnocovania korelačných pravidiel z rôznych zdrojov, vyššej úrovne integrácie s ostatnými systémami, automatizovanej reakcie a garancie technickej podpory v prípade výpadku. Nasadením týchto systémov sa predpokladá výrazne zlepšenie schopnosti spoločnosti včasne detekovať anomálie a reagovať na bezpečnostné incidenty v reálnom čase.

3.6.4 Špecializované školenie a red teaming

Autor tejto práce navrhol a organizačne zastrešil **cieľovo orientované školenia**, ktorých cieľom bolo zvýšiť praktickú pripravenosť zamestnancov na kybernetické incidenty. Školenie absolvovalo viac ako 75 % zamestnancov, pričom jednotlivé moduly boli prispôsobené ich rolám a zodpovednostiam. Osobitná pozornosť bola venovaná rizikám špecifickým pre fintech sektor – ako sú útoky na kryptopeňaženky, spear phishing voči vývojárom a zneužitie API rozhraní.

Inovatívnym prvkom bola realizácia **simulovaných útokov typu red teaming**, ktoré preverili pripravenosť spoločnosti na reálne incidenty. Tieto testy preukázali zlepšenie v schopnosti detekcie, aktivácie incident response tímu a dokumentovania zásahov. Zároveň poskytli cenné dáta pre zlepšenie existujúcich smerníc a plánov obnovy.

4 EKONOMICKÉ ZHODNOTENIE

4.1 Výpočet pomocou ROSI

Ekonomické zhodnotenie investícií do kybernetickej bezpečnosti je kľúčové pre efektívne rozhodovanie a alokáciu zdrojov v každej organizácii. Metodika *Návratnosti investícií do kybernetickej bezpečnosti* (Return on Security Investment - ROSI) poskytuje kvantitatívny prístup na posúdenie finančnej efektívnosti implementovaných bezpečnostných opatrení prostredníctvom **porovnania nákladov na opatrenie s redukciou očakávaných strát z kybernetických incidentov**. Tento prístup umožňuje spoločnosti Finsys prioritizovať investície, ktoré prinášajú najväčší prínos k zníženiu rizika v pomere k ich nákladom.

Vybrané bezpečnostné opatrenia a vstupné údaje

Pre výpočet ROSI boli na základe "Plánu zvládánia rizik" a analýzy súčasného stavu spoločnosti Finsys vybrané štyri kľúčové bezpečnostné opatrenia, ktoré sú v stave "V priebehu zavádzania".

Vybrané opatrenia sú:

BO2: Zabezpečiť obmenu a aktualizáciu hardvérových komponentov aplikačných serverov.

BO3: Implementovať centralizovaný systém aktualizácie a antivírusovej ochrany serverov.

BO5: Realizovať školenia zamerané na zvyšovanie bezpečnostného povedomia.

BO8: Zaviesť bezpečnostnú politiku pre správu API tokenov a revokácie.

Tabuľka vstupných údajov pre výpočet ROSI

ID Opatrenia	Popis Opatrenia	Celkové Náklady (C) (EUR)	Súvisiace Riziko (ID)	Odhadovaná Ročná Miera výskytu - ARO	Odhadovaná Jednorázová Strata - SLE (EUR)
BO2	Obmena a aktualizácia HW aplikačných serverov	8 000,00 €	R1	0.5 (1x za 2 roky)	50 000,00 €
BO3	Centralizovaný systém aktualizácií a AV ochrany serverov	3 800,00 €	R2	1.0 (1x ročne)	50 000,00 €
BO5	Školenia bezpečnostného povedomia	600,00 €	R4	0.25 (1x za 4 roky)	20 000,00 €
BO8	Bezpečnostná politika pre správu API tokenov	3 500,00 €	R8	0.5 (1x za 2 roky)	150 000,00 €

Obrázok č. 81 Parametre pre výpočet ROSI (Zdroj: Vlastné spracovanie)

Výpočty pre jednotlivé opatrenia

BO2: Obmena a aktualizácia HW aplikačných serverov

ALE = 50,000 EUR * 0.5 = 25,000 EUR

MLR = 25,000 EUR * 0.70 = 17,500 EUR

Celkové Náklady (C) = 2,500 + 5,000 + 500 = 8,000 EUR

ROSI = (17,500 EUR - 8,000 EUR) / 8,000 EUR = 118.75%

BO3: Centralizovaný systém aktualizácií a AV ochrany serverov

ALE = 50,000 EUR * 1.0 = 50,000 EUR

MLR = 50,000 EUR * 0.80 = 40,000 EUR

Celkové Náklady (C) = 3,000 + 300 + 500 = 3,800 EUR

ROSI = (40,000 EUR - 3,800 EUR) / 3,800 EUR = 952.63%

BO5: Školenia bezpečnostného povedomia

ALE = 20,000 EUR * 0.25 = 5,000 EUR

MLR = 5,000 EUR * 0.60 = 3,000 EUR

Celkové Náklady (C) = 0 + 100 + 500 = 600 EUR

ROSI = (3,000 EUR - 600 EUR) / 600 EUR = 400.00%

BO8: Bezpečnostná politika pre správu API tokenov

ALE = 150,000 EUR * 0.5 = 75,000 EUR

MLR = 75,000 EUR * 0.75 = 56,250 EUR

Celkové Náklady (C) = 2,800 + 500 + 200 = 3,500 EUR

ROSI = (56,250 EUR - 3,500 EUR) / 3,500 EUR = 1507.14%

Obrázok č. 82 Vzorec ROSI (Zdroj: blog.netwrix.com/2018/08/07/how-to-calculate-return-on-security-investment/)

Výsledné hodnoty ROSI pre jednotlivé opatrenia

Nasledujúca tabuľka sumarizuje vypočítané hodnoty ALE, Ročného Prínosu - MLR (Benefit) a výslednej Návratnosti Investície do Bezpečnosti (ROSI) pre každé hodnotené opatrenie.

ID Opatrenia	Celkové Náklady (C) (EUR)	Odhadovaná Ročná strata - ALE	Odhadované Zníženie Rizika (%)	Ročný prínos - Benefit - MLR (EUR)	ROSI (%)
BO2	8 000,00 €	25 000,00 €	70%	17 500,00 €	118,75 %
BO3	3 800,00 €	50 000,00 €	80%	40 000,00 €	952,63 %
BO5	600,00 €	5 000,00 €	60%	3 000,00 €	400 %
BO8	3 500,00 €	75 000,00 €	75%	56 250,00 €	1507,14%

Obrázok č. 83 Výpočet ROSI (Zdroj: Vlastné spracovanie)

Agregované ROSI

Na zhodnotenie celkovej efektívnosti, zloženej z vyššie uvedených štyroch opatrení, je možné vypočítať agregované ROSI.

Celkový Ročný Prínos (Total Benefit): Suma ročných prínosov.

Total Benefit = 17,500 (BO2) + 40,000 (BO3) + 3,000 (BO5) + 56,250 (BO8) = **116,750 EUR**

Celkové Náklady (Total Cost): Suma celkových nákladov.

Total Cost = 8,000 (BO2) + 3,800 (BO3) + 600 (BO5) + 3,500 (BO8) = **15,900 EUR**

Celkový Efektívny ROSI (Aggregated ROSI):

Aggregated ROSI = (Total Benefit - Total Cost) / Total Cost

Aggregated ROSI = (116,750 EUR - 15,900 EUR) / 15,900 EUR

Aggregated ROSI (%) = 6.3428 * 100% = **634.28%**

Agregované ROSI dosahuje približne 634.28%. Táto hodnota naznačuje, že celkový očakávaný finančný prínos zo zníženia rizík výrazne prevyšuje celkové náklady na implementáciu týchto štyroch opatrení. Každé investované euro do tejto stratégie by tak mohlo priniesť viac ako 6.34 EUR v podobe ušetrených nákladov spojených s bezpečnostnými incidentmi.

4.2 Gordon-Loeb model

Model Gordon-Loeb poskytuje ekonomický rámec **pre stanovenie optimálnej úrovne investícií do kybernetickej bezpečnosti**, pričom naznačuje, že nie je vždy ekonomicky opodstatnené snažiť sa eliminovať všetky riziká.

Kľúčovým prínosom modelu je zistenie, že optimálna výška investície do zabezpečenia informačného aktíva by spravidla nemala presiahnuť približne **37%** (alebo presnejšie 1/e) očakávanej straty spojenej s narušením bezpečnosti daného aktíva.

Pre spoločnosť Finsys bola aplikácia *Gordon-Loeb modelu* zvážená pre nasledujúce vybrané podporné aktíva:

1. Podporné aktívum P4: Azure SQL server

Server Azure SQL (P4) je kritickým cloudovým aktívom pre Finsys, uchovávajúcim transakčné dáta a údaje o klientoch, nevyhnutné pre kľúčové finančné operácie (napr. F1, F3, F4). Jeho narušenie by malo závažné dôsledky.

Potenciálna ročná strata (L): *350 000 EUR*. Tento odhad je založený na vysokej dôvernosti (4) a integrite (4) dát.

Pravdepodobnosť narušenia (v): *0.35 (35%)*. Odhad vychádza z vysokej hodnoty zraniteľnosti (4) a hrozby (4) pre súvisiace riziko R2 (Pôsobenie škodlivého kódu na OS databázového servera) a zohľadňuje súčasný stav zabezpečenia popísaný v Kapitole 2.

Očakávaná ročná strata (v × L): 0.35×350 000 EUR = 122 500 EUR.

Optimálna investícia (z∗): ≈ 122 500 EUR×0.3678 ≈ **45 030 EUR**.

2. Podporné aktívum P70: API Kľúče bankového rozhrania

API kľúče k bankovému rozhraniu (P70) sú *extrémne kritickým aktívom*, umožňujúcim priame finančné operácie (F1, F2, F3, F5). Ich kompromitácia by znamenala okamžité finančné straty.

Potenciálna ročná strata (L): *250 000 EUR*. Tento odhad reflektuje vysokú hodnotu dopadu (4) spojenú s rizikom R8 (Zneužitie autentifikačných údajov) a možnosť priamych finančných krádeží.

Pravdepodobnosť narušenia (v): *0.25 (25%)*. Odhad je založený na stredne vysokej hodnote zraniteľnosti (3) a hrozby (3) pre riziko R8 a súčasnej absencii robustnej politiky pre správu API tokenov.

Očakávaná ročná strata (v × L): 0.25×250 000 EUR=62 500 EUR.

Optimálna investícia (z∗): ≈ 62 500 EUR×0.3678 ≈ **22 988 EUR**.

3. Podporné aktívum P62: Obchodný systém backoffice.finsys.cz

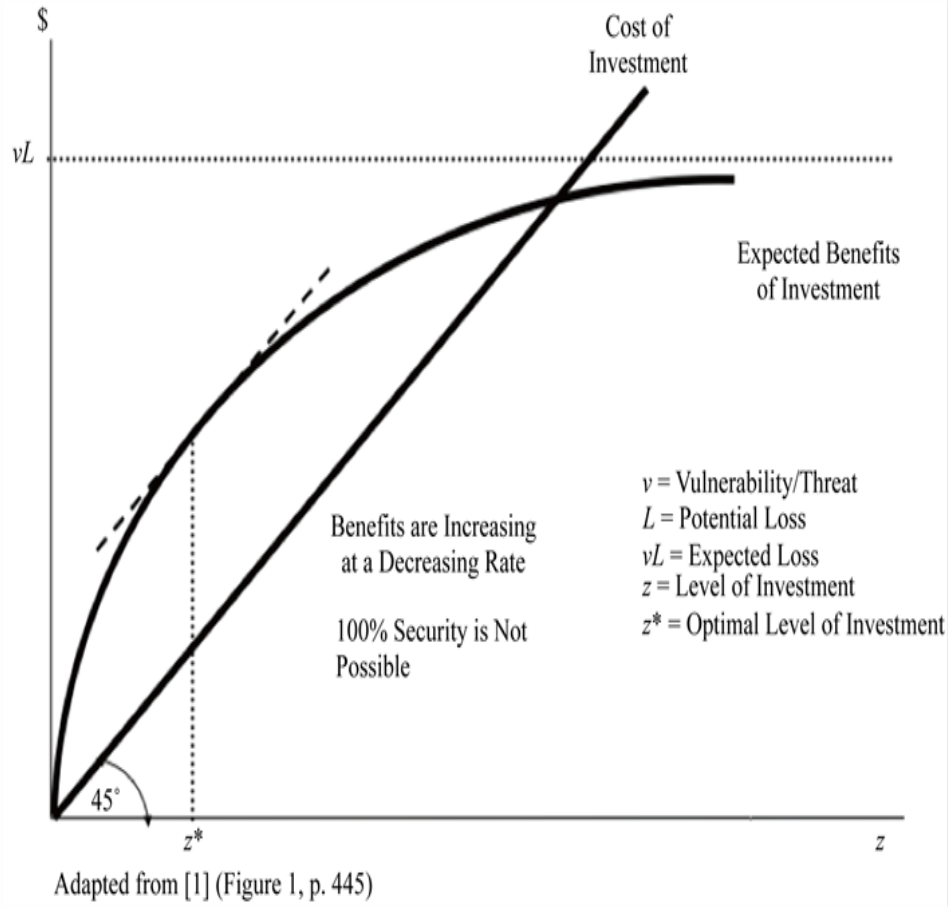
Interný obchodný systém backoffice.finsys.cz (P62) je kľúčový pre interné operatívne procesy spoločnosti Finsys, vrátane správy financií, klientov a AML (napr. F1-F7, F20, F40, F101). Jeho narušenie by spôsobilo rozsiahle prevádzkové problémy.

Potenciálna ročná strata (L): *180 000 EUR*. Odhad zohľadňuje náklady na obnovu, stratu produktivity a možné chyby v dôsledku narušenia integrity (4) a dôvernosti (4) dát tohto kritického interného systému.

Pravdepodobnosť narušenia (v): *0.20 (20%)*. Odhad zohľadňuje, že ide o interne vyvinutý systém, kde existujú základné bezpečnostné opatrenia.

Očakávaná ročná strata (v × L): 0.20×180 000 EUR= 36 000 EUR.

Optimálna investícia (z∗): ≈ 36 000 EUR×0.3678 ≈ **13 241 EUR**.



Obrázok č. 84 Optimalizácia úrovne investícií do kybernetickej bezpečnosti podľa modelu Gordon-Loeb (Zdroj: scirp.org/journal/paperinformation?paperid=64892)

4.3 Ekonomické náklady implementácie DORA

Implementácia komplexného regulačného rámca, akým je DORA, nevyhnutne predstavuje pre každý finančný subjekt, vrátane spoločnosti Finsys, ekonomickú záťaž.

Nasledujúca tabuľka poskytuje prehľad identifikovaných nákladov, pričom sa zameriava výlučne na výdavky priamo súvisiace s požiadavkami DORA, ako vyplývajú z návrhov riešení prezentovaných v tejto diplomovej práci.

Názov nákladu	Popis činnosti / účelu nákladu	Výpočet / Typ nákladu	Výsledná suma v EUR
Tvorba a aktualizácia internej dokumentácie	Vypracovanie interných politík, smerníc a procesných dokumentov	450 hod. × 50 EUR/hod	22 500 EUR
Právne a odborné konzultácie	Odborné právne poradenstvo k súladu s DORA	20 hod. × 200 EUR/hod	4000 EUR
Cestovné náklady	6 služobných ciest na pobočku Finsys	6 × 36 € (benzín za cestu tam a späť)	216 EUR
Úvodná konzultácia k DORA	Odborná konzultácia na začiatku projektu	4 hod. × 100 EUR	400 EUR
DMS - DocuWare	Licencia na systém pre správu interných smerníc, politík a plánov	Ročná licencia	1200 EUR
Penetračné testovanie – Remediata	Penetračné testovanie webových aplikácií a infraštruktúry	Externá služba	2500 EUR
Školenie k DORA	Celodenné školenie pre manažment a zamestnancov	6 hod. × 100 EUR	600 EUR
Súčet všetkých výdavkov na implementáciu DORA			31 416 EUR

Obrázok č. 85 Prehľad výdavkov na implementáciu požiadaviek nariadenia DORA (Zdroj: Vlastné spracovanie)

Celkové ekonomické náklady, ktoré sú priamo spojené s implementáciou požiadaviek nariadenia DORA v spoločnosti Finsys, predstavujú celkovú sumu **31 416 €**.

Je dôležité zdôrazniť, že ide o počiatočnú investíciu do dosiahnutia súladu a udržanie tohto stavu si bude vyžadovať ďalšie priebežné prevádzkové náklady v nasledujúcich obdobiach.

Tieto náklady však treba vnímať nielen ako povinný výdavok, ale aj ako investíciu do zvýšenia celkovej odolnosti a dôveryhodnosti spoločnosti Finsys na finančnom trhu.

5 ZÁVER

Diplomová práca sa zamerala na komplexnú analýzu a návrh opatrení na zvýšenie kybernetickej bezpečnosti vo vybranej fin-tech spoločnosti v kontexte požiadaviek nariadenia DORA. Hlavným cieľom bolo nielen identifikovať a odstrániť existujúce nedostatky v oblasti riadenia kybernetickej bezpečnosti, ale aj navrhnúť praktické a ekonomicky efektívne riešenia, ktoré umožnia spoločnosti dosiahnuť vyššiu úroveň digitálnej prevádzkovej odolnosti a zabezpečiť súlad s aktuálnou legislatívou. Hlavným prínosom práce je nielen splnenie stanovených cieľov, ale aj realizácia iniciatív nad rámec pôvodného zadania, ktoré výrazne posilnili praktickú relevantnosť a aplikovateľnosť výstupov.

V teoretickej časti práce bol poskytnutý ucelený prehľad problematiky kybernetickej bezpečnosti v dynamickom prostredí finančných inštitúcií, analyzované boli špecifiká kybernetických hrozieb typických pre tento sektor a detailne rozpracovaný legislatívny a rámec Nariadenia DORA, vrátane jeho kľúčových požiadaviek, subjektov podliehajúcich regulácii, vzťahu "lex specialis" k smernici NIS2 a relevantných technických a implementačných štandardov (RTS/ITS).

Na základe podrobnej analýzy súčasného stavu boli identifikované zásadné medzery v oblasti riadenia IKT rizík, správy incidentov, kontinuity činností a riadenia vzťahov s tretími stranami. Návrhová časť práce poskytla konkrétne riešenia v podobe interných politík, stratégií, plánov a procesov, ktoré reflektujú požiadavky nariadenia DORA a súčasne zohľadňujú špecifiká analyzovanej spoločnosti. Ekonomické zhodnotenie navrhovaných opatrení, realizované prostredníctvom metodík ROSI a Gordon-Loeb modelu, preukázalo, že investície do navrhovaných opatrení majú návratnosť 634 % v horizonte najbližšieho obdobia 12 mesiacov a súčasne potvrdilo, že investície do kybernetickej bezpečnosti sú nielen nevyhnutné, ale aj finančne opodstatnené z pohľadu návratnosti a dlhodobej stability spoločnosti.

Za hlavné obmedzenie možno označiť limitovaný prístup k niektorým citlivým údajom, čo ovplyvnilo rozsah kvantitatívnej analýzy. Okrem toho, časové a kapacitné limity práce neumožnili detailnejšie sledovať dlhodobý dopad implementovaných riešení na úroveň kybernetickej odolnosti organizácie.

Osobitne je potrebné vyzdvihnúť, že v rámci spracovania tejto diplomovej práce a v úzkej súčinnosti s analyzovanou spoločnosťou boli realizované viaceré aktivity, ktoré presahujú rámec pôvodne stanovených cieľov a zadania.

Vytvorenie vzdelávacieho portálu DORA. Najprácnejšou a zároveň kľúčovou aktivitou nad rámec zadania bolo navrhnutie a implementácia vzdelávacieho portálu zameraného na problematiku DORA. Tento portál poskytuje interaktívny obsah, aktuálne šablóny dokumentácie, prehľad legislatívnych zmien a praktické nástroje na samoštúdium pre zamestnancov aj manažment. Portál významne podporuje budovanie bezpečnostného povedomia.

Iniciatíva pre súlad s nariadením MiCA. V spolupráci s externým právnym oddelením bolo iniciované licenčné konanie s NBS.

Implementácia pokročilých monitorovacích systémov typu SIEM/SOAR. Spoločnosť taktiež pristúpila k implementácii modernejších systémov pre monitoring bezpečnostných udalostí a analýzu logov (Elastic, IBM QRadar).

Špecializované školenie pre zamestnancov**.** V spolupráci s vedením spoločnosti bolo vyškolených 75 % zamestnancov v oblasti riadenia incidentov a princípov DORA. Školenia boli doplnené simuláciami útoku typu *red teaming*, čím sa zvýšila praktická pripravenosť personálu.

Diplomová práca tak presahuje rámec teoretickej analýzy a návrhu opatrení – predstavuje ucelený a prakticky overený model, ktorý môže slúžiť ako inšpirácia pre ďalšie finančné inštitúcie čeliacim výzvam digitálnej transformácie a rastúcim regulačným požiadavkám.

Kombinácia legislatívnej analýzy, návrhu procesných a technických opatrení, ekonomického zhodnotenia a realizácie nadstavbových aktivít vytvára unikátny prístup k budovaniu digitálnej prevádzkovej odolnosti.

Záverom možno konštatovať, že **stanovené ciele práce boli naplnené** a výsledky práce významne prispievajú k rozvoju poznania a praxe v oblasti manažmentu kybernetickej bezpečnosti vo finančnom sektore.

6 ZOZNAM POUŽITEJ LITERATÚRY

[1] POLISHCHUK, Volodymyr. Analysis of the Impact of Cybersecurity on the Stability of Financial Institutions. In: *Economic Affairs* [online]. 2024, roč. 69, č. 1 [cit. 10.05.2025]. ISSN 04242513, 09764666. DOI: 10.46852/0424-2513.2.2024.30

[2] DOROSH, Iryna. Cyber security and its role in the financial sector: threats and protection measures. In: *Economics. Finances. Law* [online]. 2023, roč. 10, č. , s. 48-51. ISSN 2786-5517, 2409-1944. DOI: 10.37634/efp.2023.10.10

[3] BOITAN, Iustina Alina. Cyber Security Challenges through the Lens of Financial Industry. *International Journal of Applied Research in Management and Economics*. 2019. ISSN 2538-8053

[4] Kopp, E., Kaffenberger, L., Wilson, C., Danninger, S., & Jenkinson, N. (2017). *WP/17/185 Cyber Risk, Market Failures, and Financial Stability IMF Working Paper Western Hemisphere and Monetary and Capital Markets Departments Cyber Risk, Market Failures, and Financial Stability*. Dostupné z: www.elibrary.imf.org/downloadpdf/view/journals/001/2017/185/article-A001-en.pdf

[5] Cuomo, A. M., & Lawsky, B. M. (2014). *New York State Department of Financial Services Report on Cyber Security in the Banking Sector*. Dostupné z: home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf

[6] Department of the Treasury, U. (2024). *Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector*. Washington, D.C., USA: U.S. Department of the Treasury.

[7] *Global Financial Stability Report, April 2024: The Last Mile: Financial Vulnerabilities and Risks* [online]. Washington, D.C.: International Monetary Fund, 2024 [cit. 10.05.2025]. ISBN 979-8-4002-5770-4. DOI: 10.5089/9798400257704.082

[8] BOUVERET, Antoine (2018). *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment*. [IMF Working Paper, WP/18/143]. Washington, D.C.: International Monetary Fund. [online]. 2018 Dostupné z: www.imf.org/-/media/Files/Publications/WP/2018/wp18143.ashx

[9] JAVAHERI, Danial et al. Cybersecurity threats in FinTech: A systematic review. In: *Expert Systems with Applications* [online]. 2024, roč. 241, s. 122697. ISSN 09574174. DOI: 10.1016/j.eswa.2023.122697

[10] DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY, MULUNGUSHI UNIVERSITY, ZIMBA, Aaron. A Bayesian Attack-Network Modeling Approach to Mitigating Malware-Based Banking Cyberattacks. In: *International Journal of Computer Network and Information Security* [online]. 2021, roč. 14, č. 1, s. 25-39. ISSN 20749090, 20749104. DOI: 10.5815/ijcnis.2022.01.03

[11] MASTER OF SCIENCE IN MANAGEMENT INFORMATION SYSTEMS, COLLEGE OF BUSINESS, LAMAR UNIVERSITY, TEXAS, USA. et al. ASSESSING THE INFLUENCE OF CYBERSECURITY THREATS AND RISKS ON THE ADOPTION AND GROWTH OF DIGITAL BANKING: A SYSTEMATIC LITERATURE REVIEW. In: *American Journal of Advanced Technology and Engineering Solutions* [online]. 2025, roč. 1, č. 01, s. 226-257. ISSN 30670470. DOI: 10.63125/fh49gz18

[12] MAHESWARI S, Dr Uma. Cybersecurity Challenges In Fintech: Assessing Threats And Mitigation Strategies For Financial Institutions. In: *Educational Administration: Theory and Practice* [online]. 2024, s. 1063-1071. DOI: 10.53555/kuey.v30i5.3010

[13] *REGIONAL CYBER DEFENCE CENTRE & SNRD CYBER SECURITY (2022). Study on cybersecurity threat landscape in energy and financial sector in Lithuania. Vilnius, Lithuania.*

[14] OFFICE OF THE COMPTROLLER OF THE CURRENCY (2024). *Cybersecurity and Financial System Resilience Report*. Washington, D.C.: Office of the Comptroller of the Currency.

[15] NOVAES NETO, Nelson et al. A Case Study of the Capital One Data Breach. In: *SSRN Electronic Journal* [online]. 2020 [cit. 10.05.2025]. ISSN 1556-5068. DOI: 10.2139/ssrn.3542567

[16] European Commission (2022). Digital Operational Resilience Act (DORA): Regulatory Framework for Financial Services. Official Journal of the European Union. In: *Úradný vestník Európskej únie. ELI: data.europa.eu/eli/reg/2022/2554/oj*

[17] Esma. (n.d.). *Securities and Markets Stakeholder Group Advice to ESMA SMSG advice to ESMA on potential practical challenges regarding the implementation of the Digital Operational Resilience Act 1 Executive Summary*. Paris: European Securities and Markets Authority. [online] ESMA22-106-4405. Dostupné: www.esma.europa.eu/sites/default/files/library/ESMA22-106-405_SMSG_advice_on_DORA.pdf

[18] BUTTIGIEG, Christopher P., ZIMMERMANN, Beatriz Brunelli. The digital operational resilience act: challenges and some reflections on the adequacy of Europe's architecture for financial supervision. In: *ERA Forum* [online]. 2024, roč. 25, č. 1, s. 11-28. ISSN 1612-3093, 1863-9038. DOI: 10.1007/s12027-024-00793-w

[19] TRUCHET, Marc, 2021. Digital Operational Resilience Act (DORA): main proposals and pending issues. In: *EUROFI REGULATORY UPDATE SEPTEMBER 2021*, s. 44-46.

[20] Deloitte Česká republika**.** *Nařízení EU o digitální provozní odolnosti (DORA): Prezentace hlavních požadavků*. Praha: Deloitte Advisory s.r.o., 2023. Interní firemní prezentace. Dostupné z: www2.deloitte.com/cz

[21] Pattison, A. (2022). DORA: A Guide to the EU Digital Operational Resilience Act. ISBN 978-1787784512.

[22] European Central Bank. *TIBER-EU Framework: How to implement the European framework for Threat Intelligence-Based Ethical Red teaming*. Frankfurt am Main: European Central Bank, January 2025. Dostupné z: www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

[23] PRUSSEN, Elvinger Hoss. DORA (DIGITAL OPERATIONAL RESILIENCE ACT). 2024. [Brožúra]. Dostupné z: elvingerhoss.lu/sites/default/files/upload/media/document/2025-04/Brochure%20DORA.pdf

[24] URBÁNOVÁ CSAJKOVÁ, Alexandra (2023). Čo očakávať od regulácie digitálnej prevádzkovej odolnosti DORA? In: Slovenský finančný trh a inovácie 2023. Bratislava: Národná banka Slovenska. [online]. 2023-10-03 [cit. 2025-05-10]. Dostupné z: https://nbs.sk/dokument/49329c2f-8da6-4d9a-a717-c14fd24459e7/stiahnut/?force=true

[25] Deloitte Česká republika. *DORA: Seznamte se s nařízením o digitální provozní odolnosti. Jak by měly finanční instituce zohlednit nová pravidla ve svých strategiích?* Praha: Deloitte Advisory s.r.o., 2023. Interní prezentace. Dostupné z: www2.deloitte.com/cz

[26] Deloitte Česká republika. *DORA a NIS2: Dva legislativní nástroje EU. V čem se liší? Jaké požadavky přinášejí? Jaké výzvy představují? Pro koho jsou relevantní?* Praha: Deloitte Advisory s.r.o., 2023. Interní odborná prezentace. Dostupné z: www2.deloitte.com/cz.

[27] LETSBLOOM, 2024. *NIS2 & DORA: Are You Prepared for The Two EU Legislative Instruments? How can organizations be proactive and pragmatic in their adoption to become compliant?* [S. l.]: letsbloom.

[28] EVROPSKÝ PARLAMENT a RADA EVROPSKÉ UNIE, 2022. *Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2)*. In: *Úřední věstník Evropské unie* L 333, s. 80-150. ELI: data.europa.eu/eli/dir/2022/2555/oj

[29] PURSER, Steve, 2023. *NIS2 DORA: Are You Prepared for The Two EU Legislative Instruments? How can organizations be proactive and pragmatic in their adoption to become compliant?* [S. l.]: letsbloom. 2023. Dostupné z: www.letsbloom.io/themes/letsbloom/assets/Images/ebook-letsbloom-nis2-dora-are-you-prepared-for-two-eu-legislative-instruments.pdf

[30] NAGY, Viktor, 2024. *Řízení právních rizik v kybernetické bezpečnosti*. Vedoucí práce JUDr. Mgr. Jakub Harašta, Ph.D. Brno: Masarykova univerzita, Právnická fakulta, Ústav práva a technologií. Závěrečná práce LL.M..

[31] KOLOUCH, Jan, BAŠTA, Pavel, KROPÁČOVÁ, Andrea a KUNC, Martin, 2019. *Cybersecurity*. 1. vyd. Praha: CZ.NIC. Edice CZ.NIC. ISBN 978-80-88168-34-8.

[32] DOUCEK Petr, Martin KONEČNÝ a Luděk NOVÁK, Řízení kybernetické bezpečnosti a bezpečnosti informací, Praha: Professional Publishing, 2020. ISBN 978-80-88260-39-4.

[33] SEDLÁK Petr, Martin KONEČNÝ, Přeměna ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2023. ISBN 978-80-7623-110-8

[34] SEDLÁK Petr, Martin KONEČNÝ a kolektiv, Případové studie řízení kybernetické bezpečnosti. CERM, Akademické nakladatelství, 2024. ISBN 978-80-7623-126-9.

[35] SEDLÁK Petr, Martin KONEČNÝ a kolektiv, Kybernetická (ne)bezpečnost. CERM, Akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

[36] DEVLHON CONSULTING, [s. d.]. *What are ITS and RTS standards?* [S. l.]: Devlhon Consulting. Dostupné na: www.devlhon-consulting.com/en/normes-its-et-rts-de-lautorite-bancaire-europeenn/

[37] EMMANUEL, Jonathan, PUNIA, Gavin a RUIZ, Kuba, 2024. *DORA - what do in-house lawyers need to know about the recent Regulatory Technical Standards (supplementing DORA)?* [S. l.]: Bird & Bird. Dostupné na: www.twobirds.com/en/insights/2024/global/dora-what-do-inhouse-lawyers-need-to-know-about-the-recent-regulatory-technical-standards

[38] HØJ, Peter, 2024. *What is ITS, RTS, and ESA in DORA? Learn here how to decode the regulation.* [S. l.]: [s. n.]. Dostupné na: www.linkedin.com/pulse/what-its-rts-esa-dora-learn-here-how-decode-regulation-peter-h%C3%B8j-w7uzf/

[39] USD AG, 2024. *DORA Requirements Become More Concrete: Further RTS and ITS Published.* [S. l.]: usd AG. Dostupné na: www.usd.de/en/dora-new-batch-of-rts-and-its/

[40] ZAPPATERRA, Giulia a MENEGHETTI, Maria Chiara, 2023. *The new technical standards implementing the DORA Regulation.* [S. l.]: DLA Piper. Dostupné na: www.dlapiper.com/es-pr/insights/publications/law-in-tech/the-new-technical-standards-implementing-the-dora-regulation

[41] *THE NEW TECHNICAL STANDARDS IMPLEMENTING THE DORA REGULATION*, 2023. [S. l.]: A&L Goodbody LLP, 13. október 2023. Dostupné na: www.algoodbody.com/insights-publications/first-tranche-of-draft-rts-and-its-published-under-dora

[42] AKD. DORA update: Adoption of additional technical standards [online]. Amsterdam: AKD N.V., 2024-11-08 [cit. 2025-05-10]. Dostupné z: www.akd.eu/insights/dora-update-adoption-of-additional-technical-standards

[43] GRANT THORNTON. DORA RTS and ITS: Regulatory overview and timeline [online]. San Ġwann: Grant Thornton Malta, 2023-06-19 [cit. 2025-05-10]. Dostupné z: www.grantthornton.com.mt/insights/dora-RTS-and-ITS/

[44] AUDITBOARD. NIST Cybersecurity Framework (NIST CSF): Overview & Guide [online]. Los Angeles: AuditBoard, [2023] [cit. 2025-05-10]. Dostupné z: www.auditboard.com/blog/nist-cybersecurity-framework/

[45] BOWMAN, Keri. *NIST Cybersecurity Framework Executive Summary And Overview* [online]. Pathlock, 2022-06-05 [cit. 2025-05-10]. Dostupné z: pathlock.com/learn/nist-cybersecurity-framework-executive-summary-and-overview/

[46] FEDERAL TRADE COMMISSION. *NIST Cybersecurity Framework: A Guide for Small Businesses* [online]. Washington, D.C.: Federal Trade Commission, [s. d.] [cit. 2025-05-10]. Dostupné z: www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework

[47] OLAES, Terry. What is the NIST Cybersecurity (CSF) 2.0 Framework? [online]. San Jose: Balbix, 2025-01-17 [cit. 2025-05-10]. Dostupné z: www.balbix.com/insights/nist-cybersecurity-framework/

[48] CYBER RISK INSTITUTE. *The Cyber Risk Institute Profile: A Financial Sector Use Case of the NIST Cybersecurity Framework* [online]. Cyber Risk Institute, 2023-03 [cit. 2025-05-10]. Dostupné z: cyberriskinstitute.org/the-profile

[49] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Publications* [online]. In: *Computer Security Resource Center*. Gaithersburg, MD: National Institute of Standards and Technology, [cit. 2025-05-10]. Dostupné z: csrc.nist.gov/publications

[50] ISMS.ONLINE. *ISO 27001: The Complete Guide to ISO/IEC 27001 Information Security Standard* [online]. Brighton, United Kingdom: ISMS.online, [s. d.] [cit. 2025-05-10]. Dostupné z: www.isms.online/iso-27001/

[51] KOSUTIC, Dejan. *What does ISO 27001 mean?* [online]. Advisera, [s. d.] [cit. 2025-05-10]. Dostupné z: advisera.com/27001academy/what-is-iso-27001/

[52] ANWITA. ISO 27001 Compliance: Guide to Security Framework [online]. Bengaluru: Sprinto Technologies Pvt. Ltd., 2024-10-05 [cit. 2025-05-10]. Dostupné z: sprinto.com/blog/iso-27001-compliance/

[53] CYBERCX. What is ISO/IEC 27001 and why is ISO 27001 important to me? [online]. Sydney: CyberCX Pty Ltd., [s. d.] [cit. 2025-05-10]. Dostupné z: cybercx.com.au/resource/ten-things-you-should-know-about-iso-iec-27001/

[54] EURÓPSKA KOMISIA (2024). *Delegované nariadenie Komisie (EÚ) 2024/1774 z 13. marca 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa spresňujú nástroje, metódy, postupy a politiky riadenia IKT rizika a zjednodušený rámec riadenia IKT rizika*. In: *Úradný vestník Európskej únie*, 2024, L, č. 2024/1774. ELI: data.europa.eu/eli/reg_del/2024/1774/oj

[55] EURÓPSKA KOMISIA (2024). *Delegované nariadenie Komisie (EÚ) 2024/1772 z 13. marca 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa bližšie určujú klasifikačné kritériá incidentov súvisiacich s IKT a kybernetických hrozieb, stanovujú prahové hodnoty významnosti a spresňujú podrobnosti správ o závažných incidentoch*. In: *Úradný vestník Európskej únie*, 2024, L, č. 2024/1772. ELI: data.europa.eu/eli/reg_del/2024/1772/oj

[56] EURÓPSKA KOMISIA (2024). *Delegované nariadenie Komisie (EÚ) 2024/1773 z 13. marca 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, ktorými sa bližšie spresňuje podrobný obsah politiky v súvislosti so zmluvnými dojednaniami o využívaní IKT služieb podporujúcich kritické alebo dôležité funkcie a poskytovaných externými poskytovateľmi IKT služieb*. In: *Úradný vestník Európskej únie*, 2024, L, č. 2024/1773. ELI: data.europa.eu/eli/reg_del/2024/1773/oj

[57] I EURÓPSKA KOMISIA (2024). *Vykonávacie nariadenie Komisie (EÚ) 2024/2956 z 29. novembra 2024, ktorým sa stanovujú vykonávacie technické predpisy na uplatňovanie nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o štandardné vzory registra informácií*. In: *Úradný vestník Európskej únie*, 2024, L, č. 2024/2956. ELI: data.europa.eu/eli/reg_impl/2024/2956/oj

[58] EURÓPSKA KOMISIA (2025). *Delegované nariadenie Komisie (EÚ) 2025/301 z 23. októbra 2024, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa stanovuje obsah a lehoty na počiatočné oznámenie, a priebežnú a záverečnú správu o závažných incidentoch súvisiacich s IKT a obsah dobrovoľného oznamovania v prípade významných kybernetických hrozieb*. In: *Úradný vestník Európskej únie*, 2025, L, č. 2025/301. ELI: data.europa.eu/eli/reg_del/2025/301/oj

[59] EURÓPSKA KOMISIA (2025). *Vykonávacie nariadenie Komisie (EÚ) 2025/302 z 23. októbra 2024, ktorým sa stanovujú vykonávacie technické predpisy na uplatňovanie nariadenia Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o štandardné formuláre, vzory a postupy pre finančné subjekty na nahlasovanie závažných incidentov súvisiacich s IKT a na oznamovanie významných kybernetických hrozieb*. In: *Úradný vestník Európskej únie*, 2025, L, č. 2025/302. ELI: data.europa.eu/eli/reg_impl/2025/302/oj

[60] EURÓPSKA KOMISIA. *Delegované nariadenie Komisie (EÚ) …/… z 13. februára 2025, ktorým sa dopĺňa nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554, pokiaľ ide o regulačné technické predpisy, v ktorých sa bližšie špecifikujú kritériá používané na identifikáciu finančných subjektov povinných vykonať penetračné testovanie na základe konkrétnej hrozby....* C(2025) 885 final. Brusel: Európska komisia, 2025. Dostupné z: ec.europa.eu/transparency/documents-register/detail?ref=C(2025)885&lang=sk

[61] KOSUTIC, Dejan. *18 steps to comply with DORA requirements* [online]. Advisera, 2024-10-05 [cit. 2025-05-10]. Dostupné z: advisera.com/articles/dora-process-for-implementation/

[62] FS-ISAC'S DORA WORKING GROUP (2024). *Digital Operational Resilience Act (DORA) Implementation Guidance* [online]. FS-ISAC, Inc., 2024 [cit. 2025-05-10]. Dostupné z: www.fsisac.com/hubfs/Knowledge/DORA/FSISAC_DORA-ImplementationGuidance.pdf

[63] GREENFIELD, Martin; WILKES, Jason a GUPTA, Robert. *The Practical Steps to Implementing DORA*. [online]. London: Quod Orbis, Secon, 2024. Dostupné z: www.quodorbis.com/digital-operational-resilience-act

[64] VAN ZYL, Wesley. *DORA Compliance Checklist: From Preparation to Implementation* [online]. Scytale, [s. d.] [cit. 2025-05-10]. Dostupné z: scytale.ai/resources/dora-compliance-checklist/

[65] RSM BUSINESS INTELLIGENCE SERVICES (2024). *Get ready for DORA: A guide to help Financial Institutions with practical cyber governance implementation* [online]. Hoofddorp, Nederland: RSM Netherlands, 2024-12. Dostupné z: www.rsm.global/netherlands/en/insights/digital-operational-resilience-act-dora

[66] Naess, Kristine. *CSDM Implementation Guide for DORA ITS Reporting: How to align your data with the DORA ITS Reporting Framework Requirements using the ServiceNow Common Service Data Model.* v.07. Santa Clara: ServiceNow,Inc.,2024.Dostupné: ww.servicenow.com/community/s/cgfwn76974/attachments/cgfwn76974/common-service-data-model-forum/7043/2/CSDM%20Implementation%20guide%20for%20DORA%20ITS%20Reporting.pdf

[67] GUSIV, Pavel. *Development of a compliance gap analysis method for the Digital Operational Resilience Act (DORA)* [Master's thesis]. Rovaniemi: Lapin AMK, Master of Business Administration – Knowledge Management Expertise, 2023. 60 s. Vedúci práce: Milla Immonen.

[68] FINSYS S.R.O. (2025). *Rozhovory s predstaviteľmi a zamestnancami spoločnosti Finsys s.r.o.* [Osobné rozhovory]. Bratislava. Rozhovory uskutočnené autorom tejto diplomovej práce.

[69] EURÓPSKY PARLAMENT A RADA EÚ. 2023. Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1114 z 31. mája 2023 o trhoch s kryptoaktívami a o zmene nariadení (EÚ) č. 1093/2010 a (EÚ) č. 1095/2010 a smerníc 2013/36/EÚ a (EÚ) 2019/1937. Úradný vestník Európskej únie, L 150, 9. jún 2023, s. 40–204. Dostupné z: eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32023R1114

7 ZOZNAM OBRÁZKOV

8 SLOVNIK

2FA - Dvojfaktorová autentifikácia: Bezpečnostný proces, ktorý vyžaduje dva rôzne autentifikačné faktory.

Active Directory - Služba adresárovej štruktúry od Microsoftu na správu používateľov.

AI - Umelá inteligencia: Simulovanie inteligentného riešenia problémov PC programami.

ALE - Ročná očakávaná strata: Odhad finančnej straty z rizika za rok.

AML/CFT - Opatrenia proti legalizácii a financovaniu terorizmu.

API - Aplikačné programovacie rozhranie: Súbor pravidiel pre komunikáciu aplikácií.

BIA - Analýza vplyvu na činnosti: Hodnotenie dopadu narušenia na operácie.

BCDR - Plánovanie kontinuity a obnovy po havárii.

BCP - Plán kontinuity činností: Postup organizácie v reakcii na incident.

CaaS - Crimeware-as-a-service: Model, kde zločinci poskytujú malvér ako službu.

CAPEC - Spoločná enumerácia a klasifikácia útokov: Katalóg známych útočných vzorov

CASP - Poskytovatelia služieb týkajúcich sa kryptoaktív.

CentOS - Distribúcia Linuxu.

CIA - Triáda dôvernosti, integrity a dostupnosti: Základný model bezpečnosti.

CMDB - Konfiguračná databáza: Úložisko informácií o IKT komponentoch.

CSIRT - Tím pre reakcie na počítačové bezpečnostné incidenty.

CTI - Spravodajstvo o kybernetických hrozbách: Informácie o potenciálnych útokoch.

CVE - Bežné zraniteľnosti a expozície: Slovník bezpečnostných zraniteľností.

CWE - Bežná enumerácia slabín: Kategórie softvérových a hardvérových slabín

DDoS - Distribuovaný útok odmietnutia služby: Znefunkčenie služby zahltením prevádzky .

DeFi - Decentralizované financovanie: Finančné služby na blockchain technológiách .

DFS - Stratégia pre digitálne financie.

DLT - Technológia distribuovanej účtovnej knihy: Decentralizovaná digitálna databáza.

DORA - Nariadenie o digitálnej prevádzkovej odolnosti finančného sektora.

DPO - Digitálna prevádzková odolnosť.

DRP - Plán obnovy po havárii: Súbor postupov na obnovenie IT infraštruktúry.

ESA - Európske orgány dohľadu.

ESBA - Európsky orgán pre bankovníctvo.

ESFS - Európsky systém finančného dohľadu.

EIOPA - Európsky orgán pre poisťovníctvo a dôchodky.

ENISA - Agentúra EÚ pre kybernetickú bezpečnosť.

ESMA - Európsky orgán pre cenné papiere a trhy.

ETF - Fond obchodovaný na burze.

FinTech - Finančné technológie: Technológie pre finančné služby.

GAP analýza - Metóda na porovnanie aktuálneho a požadovaného stavu.

GoZ - GameOver Zeus: Typ finančného malvéru.

GRC - Správa, riziko a dodržiavanie predpisov: Stratégia riadenia rizík.

IaaS - Infraštruktúra ako služba: Cloudový model pre výpočtové zdroje.

IAM - Správa identít a prístupu: Rámec pre riadenie prístupových práv.

IKT - Informačné a komunikačné technológie.

ISO - Medzinárodná organizácia pre normalizáciu.

ITS - Implementačné technické štandardy.

JON - Spoločná sieť dohľadu.

LAN - Miestna počítačová sieť.

LR-DDoS - Nízkofrekvenčné DDoS útoky.

LMS - Systém pre riadenie vzdelávania.

MiCA - Nariadenie o trhoch s kryptoaktívami.

NCA - Príslušné vnútroštátne orgány.

NIS - Smernica o opatreniach na kybernetickú bezpečnosť.

NIST - Národný inštitút pre štandardy a technológie.

PKICPP - Podniky kolektívneho investovania do cenných papierov.

RACI matica - Matica zodpovednosti: Zobrazenie rolí a zodpovedností.

RTS - Regulačné technické štandardy.

ROSI - Návratnosť investícií do kybernetickej bezpečnosti.

SLA - Dohoda o úrovni služieb: Zmluva o očakávanej úrovni služieb.

SME - Malý a stredný podnik.

SWOT analýza - Analýza silných a slabých stránok, príležitostí a hrozieb.

TCP/IP - Sada protokolov pre prepojenie sieťových zariadení.

TLPT - Penetračné testovanie na základe hrozieb.

TPRM - Rámec riadenia rizík tretích strán.