DORA

Riadenie IKT rizika (Kap. II)

Rámec riadenia IKT rizika

RTS/Delegované nariadenie

NATIONAL BANK OF SLOVAKIA
EUROSYSTEM

Branislav Machlica, OFI

19. jún 2024

DORA Čl. 4: Princíp proporcionality

Ods. 1.

„Finančné subjekty uplatňujú pravidlá stanovené v kapitole II (Riadenie IKT rizika) v súlade so zásadou proporcionality, pričom zohľadňujú svoju veľkosť a celkový rizikový profil, ako aj povahu, rozsah a zložitosť svojich služieb, činností a operácií.“

DORA: 4 základné funkcie

1) **funkcia zodpovedná za riadenie IKT rizika a dozor nad ním (Kap. II)**
2) **funkcia pre monitorovanie dojednaní o využívaní IKT služieb (Kap. V)**
3) **funkcia krízového riadenia (BC)**
4) **funkcia pre vykonávanie komunikačnej stratégie (incidenty)**

Pozn.: 1), 2), 3) ine ako mikropodniky

Riadenie IKT rizík v kontexte DORA

DORA Kap. II – Riadenie IKT rizika

DORA Kap. III – Riadenie, klasifikácia a nahlasovanie incidentov súvisiacich s IKT

DORA Kap. IV – Testovanie digitálnej prevádzkovej odolnosti

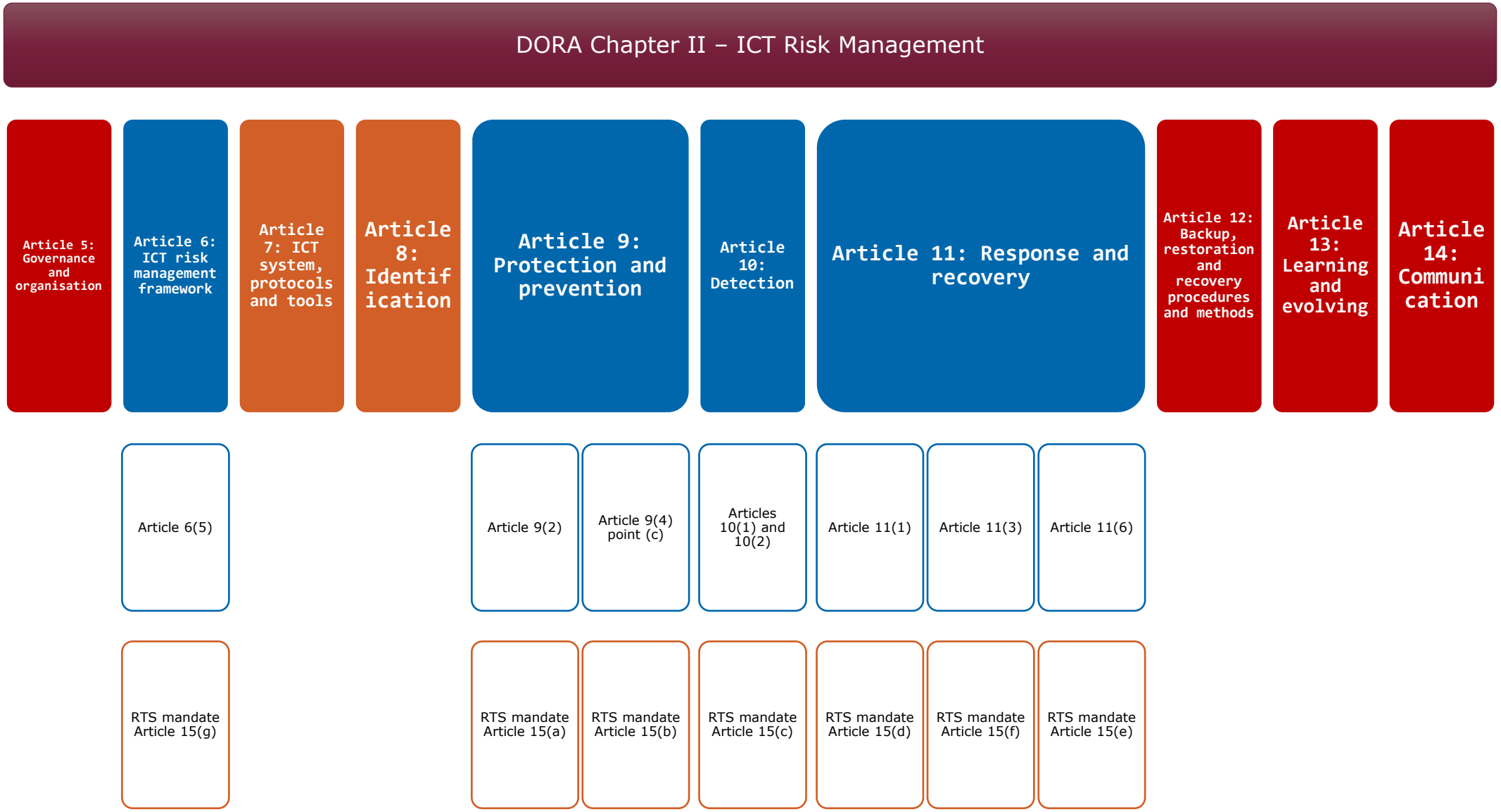
DORA Kap. V – Riadenie externého IKT rizika

RTS Kap. III:
Detekcia a reakcia na IKT incidenty

napr. RTS Kap. II, Oddiel VII:
Projekt. riadenie a riadenie zmien

napr. DORA Kap. II, Článok 5:
Správa a riadenie a organizácia

Kapitola II: Riadenie IKT rizika



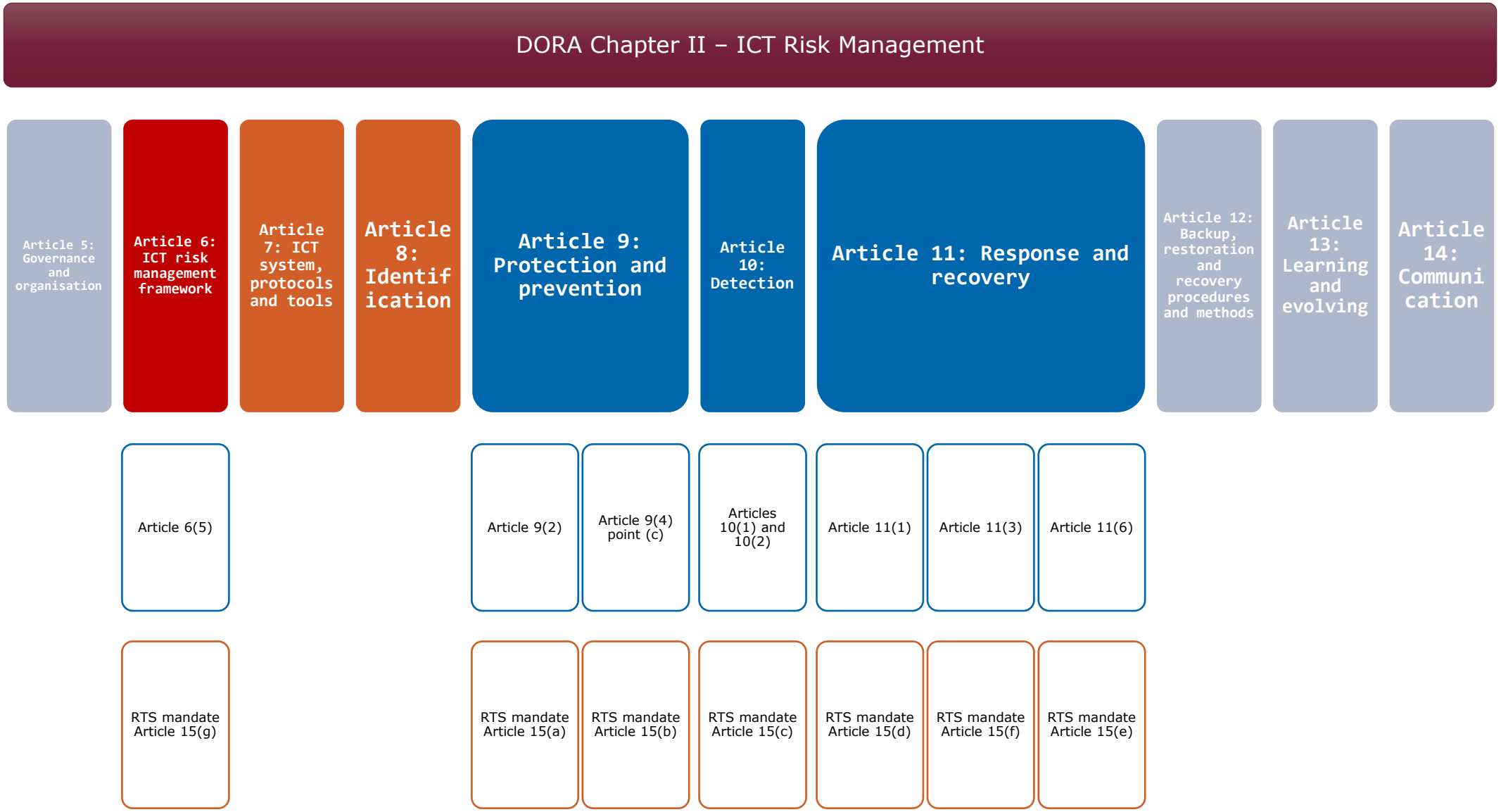
Články rozpracované do RTS v rámci článku 9

- **Článok 7 - Systémy, protokoly a nástroje IKT**:
  - podrobne RTS Kap. I - Bezp. politiky, postupy, protokoly a nástroje IKT
- **Článok 8 - Identifikácia**:
  - identifikovať, klasifikovať a dokumentovať všetky:
    - obchodné funkcie
    - úlohy a povinnosti podporované IKT
    - informačné aktíva a IKT aktíva podporujúce uvedené funkcie
    - viac RTS Kap. I, oddiel III - Správa IKT aktív
  - zmapovať konfiguráciu IA a IKT aktív, ako aj prepojenia a vzájomné závislosti medzi jednotlivými IA a IKT aktívami (fyzická architektúra)
  - identifikovať a dokumentovať procesy, ktoré sú závislé od externých poskytovateľov IKT služieb, a identifikovať vzájomné prepojenia s nimi

Články nerozpracované do RTS

- **Článok 5 - Správa a riadenie a organizácia**:
  - povinnosť zaviesť rámec vnútornej správy a riadenia a kontroly,
  - zriadiť funkciu pre monitor. dojednaní o využívaní IKT služieb (non-micro)
  - absolvovanie osobitných školení členmi riadiaceho orgánu
- **Článok 12 - Politiky a postupy zálohovania, postupy a metódy obnovy**:
  - vypracovať politiky a postupy zálohovania + postupy a metódy obnovy dát
  - zriadiť záložné systémy pre prípad výpadku primárnych systémov
  - udržiavať redund. IKT kapacity vybavené adekvát. zdrojmi (non-micro)
- **Článok 13 - Učenie sa a vývoj**
  - povinné preskúmania po incidentoch súvisiacich s IKT + hlásenie NBS
  - vypracovať programy zvyšovania informovanosti o bezpečnosti v oblasti IKT a školenia o DPO ako povinné moduly vo svojich systémoch školenia
- **Článok 14 – Komunikácia**
  - komunikačné plány a politiky + zodpovedná osoba za komun. stratégiu

IKT RMF v kontexte riadenia IKT rizík



Rámec riadenia IKT rizík

- musí byť súčasť celkového systému riadenia rizík (nutnosť zladiť)
- **zahŕňa stratégiu DOR**, v ktorej sa stanoví spôsob jeho vykonávania
- zodpovednosť za riadenie IKT rizika a dozor nad ním priradený kontrolnej funkcii s primeranou úrovňou nezávislosti
- povinnosť **zdokumentovať a preskúmavať aspoň raz ročne**, ale aj pri výskyte závažného IKT incidentu
- **podlieha** pravidelnému **vnútornému auditu** vykonávanému audítormi (dostatočné zručnosti a odborné znalosti v oblasti IKT rizika)
- **overovanie súladu** s požiadavkami na riadenie IKT rizík **možno delegovať** na vnútroskupinový alebo externý podnik formou outsourcingu (zodpovednosť však zostáva na FE)

IKT RMF

RTS as mandated under Articles 15 and 16(3) of DORA

Title II Article 15

15(a)	15(b)	15(c)	15(d,e,f)	15(g)
Chapter I: ICT security policies, procedures, protocols, and tools	**Chapter II**: Human Resources Policy and Access control	**Chapter III**: ICT-related Incident Detection and Response	**Chapter IV**: ICT Business continuity management	**Chapter V**: Report on the ICT risk management framework review

Title III
Article 16 (3)

Chapter I: Simplified ICT Risk management framework

IKT RMF

- **HLAVA II** - ĎALŠIA HARMONIZÁCIA NÁSTROJOV, METÓD, PROCESOV A POLITÍK MANAŽMENTU IKT RIZÍK V SÚLADE S ČLÁNKOM 15

  - **KAP. I –** BEZP. **POLITIKY, POSTUPY, PROTOKOLY A NÁSTROJE IKT**
  - **KAP. II** - POLITIKA **ĽUDSKÝCH ZDROJOV** A KONTROLA PRÍSTUPU
  - **KAP. III** - DETEKCIA A REAKCIA NA **INCIDENTY** SÚVISIACE S IKT
  - **KAP. IV** - RIADENIE **BUSINESS CONTINUITY** IKT
  - **KAP. V** - **REPORT** O PRESKÚMANÍ RÁMCA RIADENIA RIZÍK IKT

- **HLAVA III –** ZJEDNODUŠENÝ IKT RMF

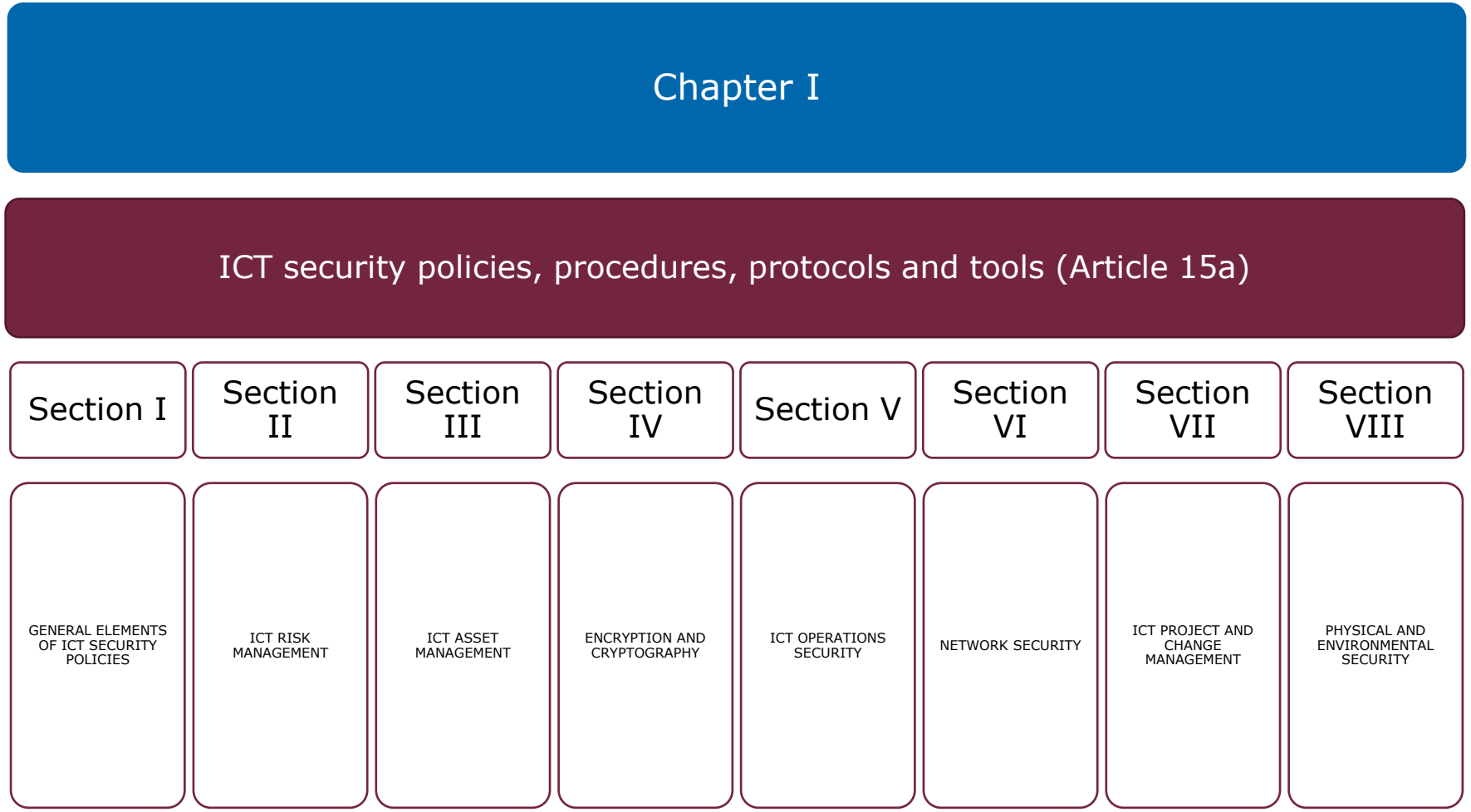
IKT RMF: Politiky a postupy

ONLY POLICIES	ONLY PROCEDURES	POLICIES AND PROCEDURES
• ICT asset management • Encryption & cryptographic controls • ICT project management • Acquisition, development and maintenance of ICT systems • Physical and environmental security • Human resources • Identity management • Access control • ICT-related incident management • ICT business continuity	• ICT asset management • Capacity and performance management • Vulnerability and patch management • Data and system security • Logging • Acquisition, development, and maintenance of ICT systems • ICT change management • Identity management	• ICT risk management • ICT operations • Network security management • Security information in transit

IKT RMF: Obsah

- **HLAVA II** - ĎALŠIA HARMONIZÁCIA NÁSTROJOV, METÓD, PROCESOV A POLITÍK MANAŽMENTU IKT RIZÍK V SÚLADE S ČLÁNKOM 15
  - **KAP. I –** BEZP. **POLITIKY, POSTUPY, PROTOKOLY A NÁSTROJE IKT**
  - **KAP. II** - POLITIKA **ĽUDSKÝCH ZDROJOV** A KONTROLA PRÍSTUPU
  - **KAP. III** - DETEKCIA A REAKCIA NA **INCIDENTY** SÚVISIACE S IKT
  - **KAP. IV** - RIADENIE **BUSINESS CONTINUITY** IKT
  - **KAP. V - REPORT** O PRESKÚMANÍ RÁMCA RIADENIA RIZÍK IKT
- **HLAVA III –** ZJEDNODUŠENÝ IKT RMF PRE SUBJEKTY

Kapitola I


Chapter I
ICT security policies, procedures, protocols and tools (Article 15a)
Section I
Section II
Section III
Section IV
Section V
Section VI
Section VII
Section VIII
GENERAL ELEMENTS OF ICT SECURITY POLICIES
ICT RISK MANAGEMENT
ICT ASSET MANAGEMENT
ENCRYPTION AND CRYPTOGRAPHY
ICT OPERATIONS SECURITY
NETWORK SECURITY
ICT PROJECT AND CHANGE MANAGEMENT
PHYSICAL AND ENVIRONMENTAL SECURITY

Oddiel I: VŠEOBECNÉ PRVKY BEZP. POLITÍK IKT

- Všetky **parciálne IKT politiky** treba začleniť do celkového IKT RMF
- Vo všetkých parciálnych politikách treba definovať napr.:
  - povinnosti a zodpovednosti zamestnancov
  - zoznam dokumentácie, ktorá sa má viesť
  - dátum schválenia
  - ukazovatele a opatrenia na monitorovanie vykonávania bezp. politík IKT
  - dôsledky nedodržiavania politík IKT bezpečnosti zo strany zamestnancov
  - opatrenia pre oddelenie povinností (predísť konfliktu záujmov)
  - úlohy a zodpovednosti za rozvoj, implementáciu a udržiavanie politík pre IKT bezpečnosť

Oddiel II: Riadenie rizík IKT

- **Politika** má obsahovať najmä:
  - schválenú úroveň tolerancie rizika
  - postup a metodiku pre hodnotenie IKT rizika, identifikáciu zraniteľností a hrozieb
  - postup pre identifikáciu, implementáciu a dokumentovanie opatrení pre riešenie posudzovaného IKT rizika
  - ustanovenia pre monitorovanie akýchkoľvek zmien v oblasti IKT rizík
  - **ustanovenia pre identifikáciu zvyškových IKT rizík**
    - vypracovanie zoznamu akceptovaných zvyškových IKT rizík
    - ustanovenia pre posudzovanie akceptovaných zvyškových IKT rizík (1y)
    - pridelenie úloh a zodpovedností, pokiaľ ide o akceptovanie zvyškových IKT rizík, ktoré presahujú úroveň tolerancie rizika

Oddiel III: Správa aktív IKT

- **Politika** vyžaduje najmä:
  - monitorovanie a riadenie životného cyklu aktív IKT
  - aby FE viedla záznamy v stanovenej štruktúre, napr.:
    - jedinečný identifikátor IKT aktíva
    - informácia o lokácii (fyzická, logická) pre všetky IKT aktíva
    - klasifikácia všetkých IKT aktív
    - identita vlastníkov IKT aktív
    - business funkcie alebo služby podporované IKT aktívami
    - požiadavky na BC IKT, vrátane RTO a RPO

- **Postup** má obsahovať kritériá na vykonanie hodnotenia kritickosti IKT aktív

Oddiel IV: Šifrovanie a kryptografia

- **Politika** má obsahovať napr.:
  - pravidlá pre šifrovanie údajov v pokoji a počas prenosu
  - pravidlá pre šifrovanie interných sieťových pripojení a spojení s ext. stran.
  - ustanovenia o správe kryptografických kľúčov (napr. PKI - public key infrastructure)
  - kritériá na výber kryptografických techník a **postupov** používania

- zaviesť **kontroly na ochranu kryptografických kľúčov** počas celého ich životného cyklu

- vytvoriť a udržiavať **register pre všetky certifikáty**

Oddiel V: Bezpečnosť prevádzky IKT

- **Polititky a postupy** na riadenie operácií IKT aktív:
  - opis majetku IKT
  - kontroly a monitorovanie systémov IKT
  - riešenie chýb týkajúcich sa systémov IKT
- **Postupy** riadenia kapacity a výkonnosti, napr.:
  - monitorovanie vyťaženosti/porúch diskových polí
- **Postupy** riadenia zraniteľností a záplat, napr.:
  - sledovanie zverejňovaných zraniteľností používaných SW knižníc
  - Pozn.: Kap. IV Testovanie DOR + povinnosť napr. pen. testov (raz ročne)
- **Postup** zabezpečenia údajov a systémov IKT (napr. bezpečn. konfigurácia)
- **Postupy, protokoly a nástroje** logovania (správa prístupu, riadenie kapacity, riadenie zmien, správa sietí, ...)

Oddiel VI: Bezpečnosť sieťe

- **Politiky, postupy, protokoly a nástroje** obsahujúce najmä:
  - dokumentáciu všetkých sieťových pripojení a dátových tokov
  - používanie samostatnej a vyhradenej siete na správu aktív IKT
  - identifikáciu a implementáciu kontrol prístupu do siete
  - vykonávania preskúmaní arch. siete a návrhu bezpečnosti siete raz ročne

- **Postupy, protokoly a nástroje** na ochranu informácií pri prenose
  - treba zabezpečiť dostupnosť, pravosť, integritu a dôvernosť dát počas sieťového prenosu
  - všetky majú zohľadňovať výsledky schválenej klasifikácie údajov a procesov hodnotenia rizika IKT

Oddiel VII: Projekt. man. IKT a man. zmien IKT

- **Politika** pre riadenie IKT projektov obsahujúcu najmä:
  - ciele projektu, dôležité miľníky, požiadavky na riadenie zmien
  - riadenie projektu, vrátane úloh a zodpovedností
  - plánovanie, časový rámec a kroky, posúdenie rizík projektu
- **Politika** pre získavanie, vývoj a údržbu IKT systémov, napr.:
  - testovanie všetkých IKT systémov pred ich použitím (Kap. IV)
  - vykonávanie revízií zdrojového kódu
- **Postup** pre riadenie zmien IKT
  - všetky zmeny SW, HW, komponentov firmvéru, systémov alebo bezpečnostných parametrov (ide napr.: o pridanie novej funkcionality)
  - CP a CDCP zapoja do navrhovania a vykonávania týchto testov ďalšie entity (napr. klientov, zúčtovacích členov, iné zainteresované strany)

Oddiel VIII: Fyzická a environ. bezpečnosť

- **Politika** má obsahovať najmä:
  - opatrenia na ochranu priestorov, dátových centier FE a citlivých oblastí
  - opatrenia na zabezpečenie IKT aktív v priestoroch FE aj mimo nich
  - opatrenia na zabezpečenie dostupnosti, pravosti, integrity a dôvernosti údajov informačných aktív a zariadení na kontrolu fyzického prístupu FE
  - opatrenia na zachovanie dostupnosti, autenticity, integrity a dôvernosti údajov vrátane "clear desk" politiky pre dokumenty a "clear screen" politiky pre zariadenia na spracovanie informacií.

IKT RMF

- **HLAVA II** - ĎALŠIA HARMONIZÁCIA NÁSTROJOV, METÓD, PROCESOV A POLITÍK MANAŽMENTU IKT RIZÍK V SÚLADE S ČLÁNKOM 15
  - **KAP. I – BEZP. POLITIKY, POSTUPY, PROTOKOLY A NÁSTROJE IKT**
  - **KAP. II** - POLITIKA **ĽUDSKÝCH ZDROJOV** A KONTROLA PRÍSTUPU
  - **KAP. III** - DETEKCIA A REAKCIA NA **INCIDENTY** SÚVISIACE S IKT
  - **KAP. IV** - RIADENIE **BUSINESS CONTINUITY** IKT
  - **KAP. V - REPORT** O PRESKÚMANÍ RÁMCA RIADENIA RIZÍK IKT
- **HLAVA III** – ZJEDNODUŠENÝ IKT RMF PRE SUBJEKTY

Politika ľudských zdrojov

- Do **politiky ĽZ** má FE pridať najmä tieto prvky IKT bezpečnosti:
  - určenie a pridelenie akýchkoľvek špecifických zodpovedností za IKT bezpečnosť
  - požiadavky na zamestnancov FE a TPP, ktorí používajú IKT aktíva FE
    - boli informovaní a dodržiavali politiky, postupy, protokoly pre IKT bezpečnosť FE
    - poznali reportovacie kanály zavedené zo strany FE na účely detekcie anomálneho správania
    - po ukončení zmluvného vzťahu vrátili FE všetky jej IKT aktíva

Správa identít

- **Politiky a postupy** pre riadenie identít obsahujú najmä tieto povinnosti:
  - pridelenie jedinečnej identity zodpovedajúcej jedinečnému používateľskému účtu každému zamestnancovi FE alebo zamestnancom TPP, ktorí majú prístup k informačným aktívam
  - vedenie záznamov o všetkých prideleniach takýchto používateľ. účtov
  - proces riadenia životného cyklu identít a účtov, ktorý riadi vytváranie, zmenu, kontrolu a aktualizáciu, dočasnú deaktiváciu a zrušenie všetkých účtov

Kontrola prístupu

- **Politika**, ktorá rieši prideľovanie prístupových práv k IKT, má obsahovať napr.:
  - ustanovenia o prideľovaní prístupových práv k IKT aktívam na základe zásad „need-to-know“, „need-to-use“ a least privilege principles, a to aj pre vzdialený a núdzový (pohotovostný) prístup
  - ustanovenie o zodpovednosti používateľov prostredníctvom maximálneho možného obmedzenia používania generických a zdieľaných používateľ. účtov
  - **postupy** pre správu účtov - prideľovanie, zmena a zrušenie prístupových práv pre používateľské a generické účty
  - rôzne metódy autentifikácie (podľa RP IA, napr. dvojf. autent. + tokeny)
  - prideľovanie privilegovaného, núdzového a admin prístupu
  - opatrenia na kontrolu fyzického prístupu (napr. čipové karty a zónovanie)

IKT RMF

- **HLAVA II** - ĎALŠIA HARMONIZÁCIA NÁSTROJOV, METÓD, PROCESOV A POLITÍK MANAŽMENTU IKT RIZÍK V SÚLADE S ČLÁNKOM 15
  - **KAP. I – BEZP. POLITIKY, POSTUPY, PROTOKOLY A NÁSTROJE IKT**
  - **KAP. II** - POLITIKA **ĽUDSKÝCH ZDROJOV** A KONTROLA PRÍSTUPU
  - **KAP. III** - DETEKCIA A REAKCIA NA **INCIDENTY** SÚVISIACE S IKT
  - **KAP. IV** - RIADENIE **BUSINESS CONTINUITY** IKT
  - **KAP. V - REPORT** O PRESKÚMANÍ RÁMCA RIADENIA RIZÍK IKT
- **HLAVA III** – ZJEDNODUŠENÝ IKT RMF PRE SUBJEKTY

Politika riadenia IKT incidentov

- **Politika** má obsahovať napr.:
  - zdokumentovaný proces riadenia IKT incidentov podľa čl. 17 DORA
  - zoznam relevantných kontaktov
  - ustanovenia pre zriadenie, implementovanie a prevádzkovanie technických a organizačných mechanizmov na podporu procesu riadenia IKT incidentov
  - povinnosť uchovávať všetky dôkazy týkajúce sa IKT incidentov
  - povinnosť vytvoriť a implementovať mechanizmy na analýzu IKT incidentov

- Pozn.: **Kapitola III** Riadenie, klasifikácia a nahlasovanie incidentov súvisiacich s IKT + RTS o klasifikácii incidentov

Detekcia anomálnych činností

FE je v tomto kontexte povinná:

- mať jasne stanovené role a zodpovednosti na efektívne detegovanie IKT incidentov a reakcií na ne
- **zaviesť detekčné mechanizmy**, ktoré umožnia najmä:
  - zhromažďovať, monitorovať a analyzovať najmä info o incid. a hrozbách
  - identifikovať anomálne aktivity a impl. nástroje na generovanie upozornení
- **zaznamenať všetky relevantné informácie** o každej zistenej anomálnej aktivite
- **zvážiť kritériá** pre spustenie procesov **na detekciu IKT incidentov**, napr.:
  - zistené straty dát
  - zistený nepriaznivý vplyv na transakcie a operácie
  - problémy nahlásené používateľmi FE

IKT RMF

- **HLAVA II** - ĎALŠIA HARMONIZÁCIA NÁSTROJOV, METÓD, PROCESOV A POLITÍK MANAŽMENTU IKT RIZÍK V SÚLADE S ČLÁNKOM 15
  - **KAP. I – BEZP. POLITIKY, POSTUPY, PROTOKOLY A NÁSTROJE IKT**
  - **KAP. II** - POLITIKA **ĽUDSKÝCH ZDROJOV** A KONTROLA PRÍSTUPU
  - **KAP. III** - DETEKCIA A REAKCIA NA **INCIDENTY** SÚVISIACE S IKT
  - **KAP. IV** - RIADENIE **BUSINESS CONTINUITY** IKT
  - **KAP. V - REPORT** O PRESKÚMANÍ RÁMCA RIADENIA RIZÍK IKT
- **HLAVA III** – ZJEDNODUŠENÝ IKT RMF PRE SUBJEKTY

Komponenty politiky BC IKT

- Do **politiky BC IKT** je FE povinná zahrnúť najmä:
  - určenie cieľov vrátane vzájomného vzťahu IKT a celkovej BCP
  - určenie rozsahu a časového rámca
  - kritériá na aktiváciu a deaktiváciu plánov
  - ustanovenia o riadení a organizácii vrátane úloh, zodp. a esk. postupov
  - ustanovenia o zosúladení plánov pre IKT BC a plánov pre BC

- Špeciálne ustanovenia pre **centrálne protistrany, CDCP, obchodné miesta,** napr. pevne stanovené časy obnovy ich obchodných funkcií **– 2h**

Testovanie plánov BC IKT

- Testovanie plánov BC IKT má napr.:
  - byť vykonávané na základe test. scenárov, ktoré simulujú poten. narušenia
  - zahŕňať testovanie IKT služieb poskytovaných TPP (DORA Kap. V)
  - zahŕňať scenáre prechodu z primárnej IKT infra. na redundantnú (≠Micro)
  - zahŕňať postupy na overenie schopnosti zamestnancov FE, TPP, IKT systémov a IKT služieb primerane reagovať

- Špeciálne ustanovenia pre **centrálne protistrany** a **CDCP,** napr. účasť používateľov na testovaní BC

Plány reakcie a obnovy IKT

- Plány majú napr.:
  - špecifikovať podmienky vedúce k ich aktivácii al. deaktivácii
  - popísať, aké opatrenia treba prijať na zabezpečenie dostupnosti, integrity, kontinuity a obnovy aspoň CIF
  - byť zdokum. a sprístupnené zamestnancom zapojeným do ich vykonávania

- Relevantné scenáre, ktoré treba v plánoch zvážiť:
  - **kybernetické útoky** a prepinania medzi prim. IKT infra. a redun. kapacitou
  - scenáre, v ktorých sa **kvalita CIF** zhorší na neprijateľnú úroveň alebo zlyhá
  - čiastočné alebo úplné **zlyhanie priestorov** (kanc., obch. priestorov al. DC)
  - závažné **zlyhanie IKT aktív** alebo komunikačnej infraštruktúry
  - **nedostupnosť** kritického počtu **zamestnancov**
  - **insider útoky** al. rozsiahle **výpadky elektriny**

IKT RMF

- **HLAVA II** - ĎALŠIA HARMONIZÁCIA NÁSTROJOV, METÓD, PROCESOV A POLITÍK MANAŽMENTU IKT RIZÍK V SÚLADE S ČLÁNKOM 15
  - **KAP. I** - BEZPEČNOSTNÉ **POLIT., POSTUPY, PROTOK. A NÁSTR. IKT**
  - **KAP. II** - POLITIKA **ĽUDSKÝCH ZDROJOV** A KONTROLA PRÍSTUPU
  - **KAP. III** - DETEKCIA A REAKCIA NA **INCIDENTY** SÚVISIACE S IKT
  - **KAP. IV** - RIADENIE **BUSINESS CONTINUITY** IKT
  - **KAP. V - REPORT** O PRESKÚMANÍ RÁMCA RIADENIA RIZÍK IKT
- **HLAVA III** – ZJEDNODUŠENÝ IKT RMF PRE SUBJEKTY

Report o preskúmaní IKT RMF

- **Elektronická forma** s možnosťou vyhľadávania
- **Riadne raz ročne vypracovať** a poskytnúť NBS na jej žiadosť
- Mimoriadne **vypracovať aj po závažnom incidente** a odoslať NBS
- Report má obsahovať najmä:
  - definovanie FE a predmetu správy
  - zhrnutie súčasného a krátkodobého budúceho rizikového profilu IKT
  - dôvod preskúmania IKT RMF a dátumy začiatku a konca obdobia preskúm.
  - označenie funkcie zodpovednej za preskúmanie
  - opis hlavných zmien a zlepšení IKT RMF od predchádzajúceho preskúmania
  - zhrnutie zistení preskúmania a posúdenie závažnosti nedostatkov
  - opis opatrení na riešenie zistených nedostatkov
  - informácie o ďalšom plánovanom vývoji
  - prílohy (napr. auditné správy, výsledky testovania)

IKT RMF

- **HLAVA II** - ĎALŠIA HARMONIZÁCIA NÁSTROJOV, METÓD, PROCESOV A POLITÍK MANAŽMENTU IKT RIZÍK V SÚLADE S ČLÁNKOM 15
  - **KAP. I** - BEZPEČNOSTNÉ **POLIT., POSTUPY, PROTOK. A NÁSTR. IKT**
  - **KAP. II** - POLITIKA **ĽUDSKÝCH ZDROJOV** A KONTROLA PRÍSTUPU
  - **KAP. III** - DETEKCIA A REAKCIA NA **INCIDENTY** SÚVISIACE S IKT
  - **KAP. IV** - RIADENIE **BUSINESS CONTINUITY** IKT
  - **KAP. V** - **REPORT** O PRESKÚMANÍ RÁMCA RIADENIA RIZÍK IKT

- **HLAVA III –** ZJEDNODUŠENÝ IKT RMF

Zjednodušený IKT RMF

- **viac všeobecný** - väčšia miera abstrakcie

- **viac vecí vypustených**, najmä:
  - detekcia a reakcia na incidenty súvisiace s IKT (platí len DORA)
  - politika ľudských zdrojov (zostala len Kontrola prístupu)
  - zabezpečenie dát pri prenose
  - manažment kryptografických kľúčov
  - manažment zraniteľností a záplat
  - mnohé povinnosti ako predpísané štruktúry v akých má FE viesť určité záznamy (napr. riadenie aktív, projektový manažment)

- **zanedbateľné množstvo subjektov** na SK FT – rádovo v jednotkách (2 ocp)

NATIONAL BANK OF SLOVAKIA
EUROSYSTEM

Q&A

Kto bude vykonávať FE audit?

- **Interný audit**
  - Kap. II, čl. 6, ods. 6
  - *„**Rámec riadenia IKT rizika** finančných subjektov iných ako mikropodnikov **podlieha pravidelnému vnútornému auditu** vykonávanému audítormi v súlade s plánom auditu finančných subjektov. Títo audítori musia mať dostatočné znalosti, zručnosti a odborné znalosti v oblasti IKT rizika, ako aj primeranú nezávislosť. Frekvencia a zameranie auditov IKT musia zodpovedať IKT riziku daného finančného subjektu.“*

Kto bude vykonávať FE audit?

- **Externý audit:**
  - Kap. V, čl. 28, ods. 6
  - *„Pri vykonávaní práv na prístup, inšpekciu a audit, pokiaľ ide o externého poskytovateľa IKT služieb, **finančné subjekty** na základe prístupu založeného na riziku **vopred určia frekvenciu auditov a inšpekcií**, ako aj oblasti, v ktorých sa má audit vykonať dodržiavaním všeobecne akceptovaných audítorských štandardov v súlade s akýmikoľvek pokynmi orgánov dohľadu o používaní a začlenení týchto audítorských štandardov.“*

- Audítori by mali vlastniť certifikácie ako napr. Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), alebo Certified Information Systems Security Professional (CISSP).

Musí mať FE zamestnanca na RM a zvlášť na RM IKT?

- Podľa nariadenia DORA sú požiadavky na riadenie rizík a IKT rizík stanovené tak, aby zabezpečili primeranú úroveň digitálnej odolnosti finančných subjektov.
- Pre malé firmy môžu byť tieto požiadavky flexibilnejšie, aby sa prispôsobili ich kapacitám a zdrojom.
- Zamestnanci môžu byť na full-time, part-time pozíciách alebo môžu byť outsourcovaní, pokiaľ sú splnené požiadavky na kvalifikáciu, kontrolu a bezpečnosť.
- Dôležité je zabezpečiť, aby osoby alebo poskytovatelia služieb mali dostatočné odborné znalosti a schopnosti na efektívne riadenie rizík a IKT rizík v súlade s požiadavkami DORA a aby bola zabezpečená ich dostupnosť pre plný výkon svojej funkcie.

Budú pevne stanovené požiadavky na zamestnancov FE, ktorý budú riešiť problematiku IKT?

- Hoci DORA kladie dôraz na kvalifikácie a odborné znalosti zamestnancov v oblasti IKT, konkrétne požiadavky na vzdelanie nie sú striktne definované, čo umožňuje flexibilitu pri nábore.
- Dôležité je, aby zamestnanci mali primerané znalosti a schopnosti na efektívne riadenie IKT rizík a bezpečnosti.
- Spoločnosti môžu zamestnať osoby so stredoškolským vzdelaním a dostatočnou praxou, pokiaľ tieto osoby preukážu, že sú schopné splniť požiadavky stanovené v nariadení DORA.

Plánuje NBS zjednotiť RTS report a ECB ICT Risk Questionnaire?

- Report podľa článku V (RTS) má za cieľ poskytnúť NBS prehľad o rizikách v oblasti IKT a opatreniach, ktoré FE implementujú na ich riadenie.
- ECB ICT Risk Questionnaire je ročný dotazník, ktorý banky posielajú ECB a je zameraný na zhromažďovanie informácií o rizikách v oblasti IKT a bezpečnosti IT, ktoré môžu ovplyvniť finančnú stabilitu a operácie bánk.
- Napriek zjavným podobnostiam oboch reportov, nemá NBS v súčasnosti mandát ich akokoľvek zjednocovať, preto FE sú povinné splniť si obe reportovacie povinnosti nezávisle na sebe.

Ďakujem za pozornosť

slido

Join at
slido.com
#DORA