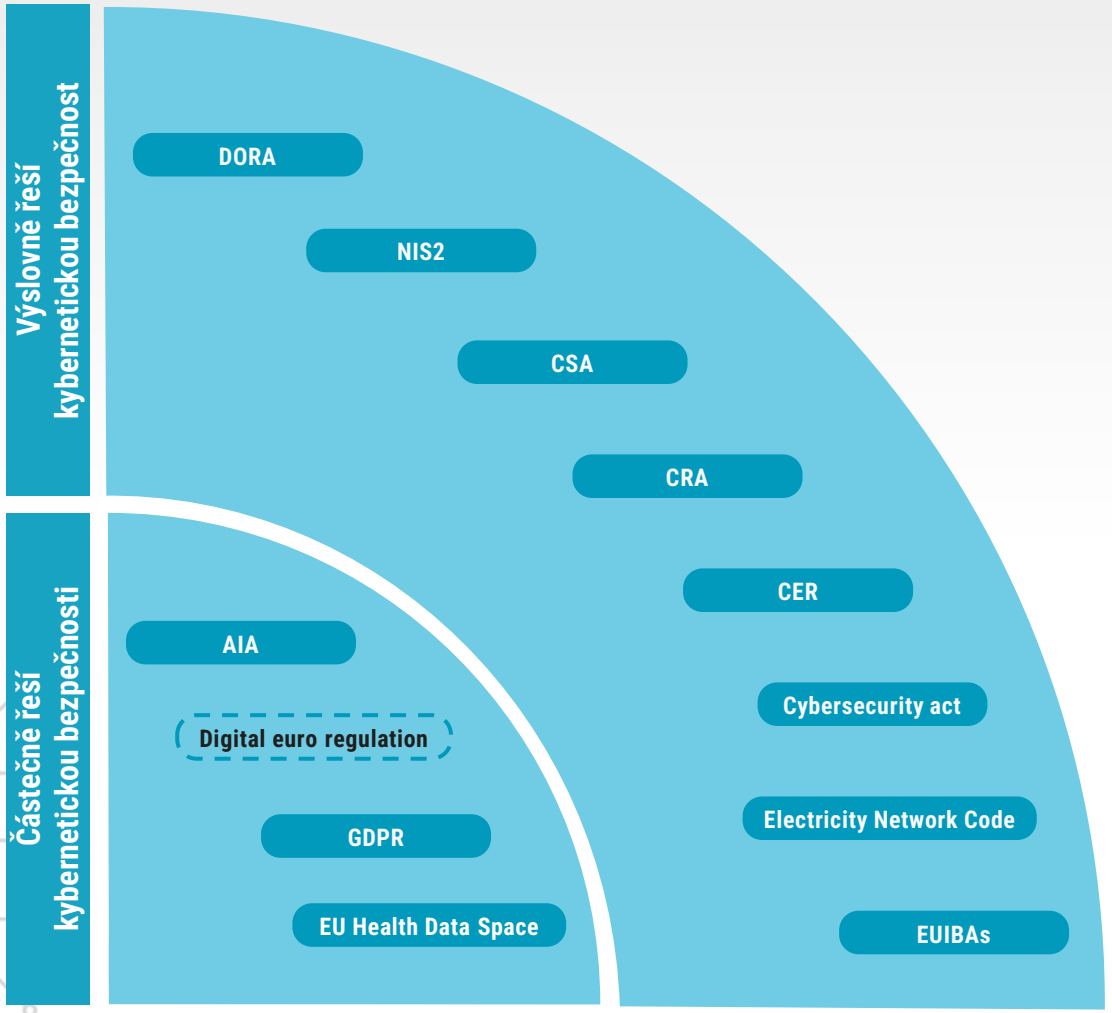
Kybernetická bezpečnost a personalistika.

PIERSTONE

3. dubna 2025

Dominik Vítek
PIERSTONE

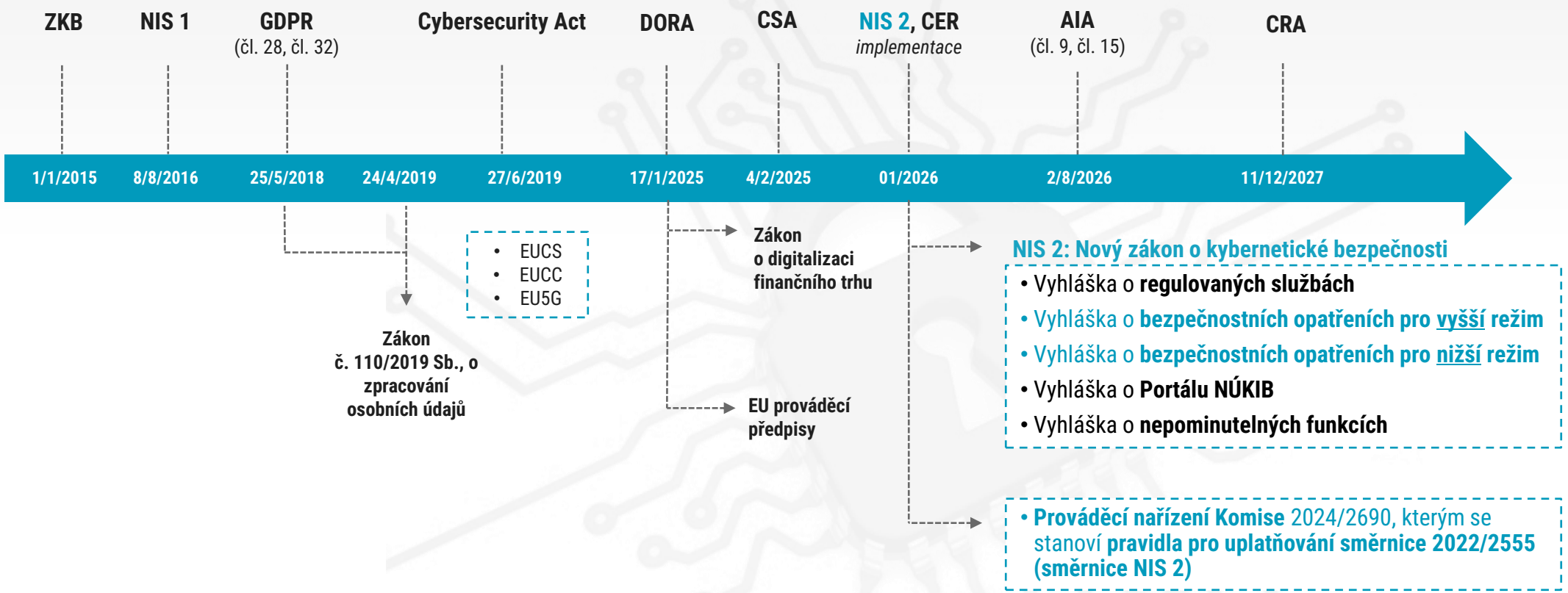
Unijní rámec kybernetické bezpečnosti.



Zdroj: Zpráva o stavu kybernetické bezpečnosti v Unii

PIERSTONE

Předpisy kybernetické bezpečnosti.



PIERSTONE

Nový zákon o kybernetické bezpečnosti.

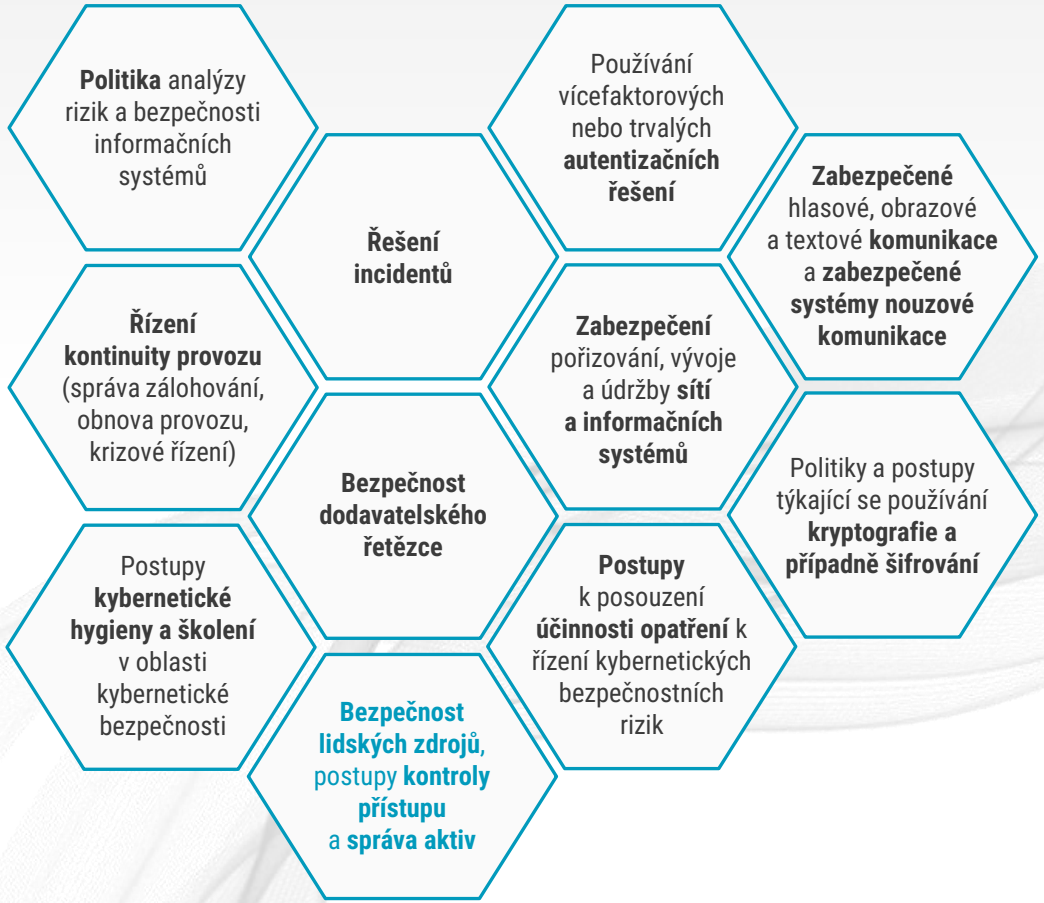
PIERSTONE

Vyhláška o regulovaných službách

Režim nižších povinností	Režim vyšších povinností	Strategicky významná služba
Zpravidla střední podnik • Min. 50 zaměstnanců* **nebo** roční obrat min. 10 mil. EUR	Zpravidla velký podnik • Min. 250 zaměstnanců* **nebo** roční obrat min. 50 mil. EUR	Regulovaná služba, jejíž narušení by mohlo způsobit závažný dopad na bezpečnost ČR nebo vnitřní či veřejný pořádek v odvětvích: • Veřejná správa • Energetika • Doprava • Digitální infrastruktura a služby Kritéria v § 5 Vyhlášky

* Vyhodnocení kritérií pro celý podnik

Nařízení (EU) 2024/2690.



Uplatní se na:

- Provozovatele DNS
- Registry domén nejvyšší úrovně,
- Poskytovatele:
  - služeb cloud computingu,
  - služeb datových center,
  - sítí pro doručování obsahu,
  - řízených služeb,
  - řízených bezpečnostních služeb,
  - on-line tržišť,
  - internetových vyhledávačů
  - služeb platforem sociálních sítí
  - služeb vytvářejících důvěru

Obsah bezpečnostních opatření **vychází zejm. z mezinárodních standardů**, mj. řady ISO 27 000

Značná **shoda** s požadavky návrhu **vyhlášky o bezpečnostních opatřeních pro vyšší režim**

PIERSTONE

Relevantní povinnosti.

VYHLÁŠKA O BEZPEČNOSTNÍCH OPATŘENÍ PRO REŽIM NIŽŠÍCH POVINNOSTÍ	VYHLÁŠKA O BEZPEČNOSTNÍCH OPATŘENÍ PRO REŽIM VYŠŠÍCH POVINNOSTÍ	PROVÁDĚCÍ NAŘÍZENÍ (EU) 2024/2690
Povinnosti vrcholného vedení	Povinnosti vrcholného vedení	
Určení bezpečnostních rolí: • Osoba odpovědná za kyberbezpečnost	Určení bezpečnostních rolí: • Výbor pro řízení kybernetické bezpečnosti • Manažer kybernetické bezpečnosti • Architekt kybernetické bezpečnosti • Garant aktiva • Auditor kybernetické bezpečnosti	Povinnost rozdělení: • Úkolů • Odpovědností • Pravomocí
Bezpečnost lidských zdrojů	Bezpečnost lidských zdrojů	Oblasti bezpečnost lidských zdrojů (prescreening, disciplinární řízení, ukončení poměru)
Vstupní a pravidelná školení	Vstupní a pravidelná školení	Bezpečnostní školení, zvyšování povědomí kybernetické hygieny

PIERSTONE

Povinnosti vrcholného vedení.

PIERSTONE

Vrcholné vedení.

Vyhláška pro režim nižších/vyšších povinností

Osoba nebo skupina osob, které řídí povinnou osobu, nebo statutární orgán povinné osoby

Vyhláška pro režim vyšších povinností

§ 5
Povinnosti vrcholného vedení

(1) Vrcholné vedení s ohledem na systém řízení bezpečnosti informací
a) se prokazatelně účastní školení podle § 11 odst. 3 písm. a),
b) zajistí stanovení bezpečnostní politiky a cílů systému řízení bezpečnosti informací podle § 4, slučitelných se strategickým směřováním povinné osoby,
c) zajistí integraci systému řízení bezpečnosti informací do procesů povinné osoby,
d) zajistí dostupnost zdrojů potřebných pro systém řízení bezpečnosti informací,
e) informuje zaměstnance o významu systému řízení bezpečnosti informací a významu dosažení shody s jeho požadavky se všemi dotčenými stranami,
f) zajistí podporu k dosažení cílů systému řízení bezpečnosti informací,
g) vede zaměstnance k rozvíjení efektivity systému řízení bezpečnosti informací a podporuje je při tomto rozvíjení,
h) se podílí na vypracování analýzy dopadů podle § 16,
i) prosazuje neustálé zlepšování systému řízení bezpečnosti informací,
j) podporuje osoby zastávající bezpečnostní role při prosazování kybernetické bezpečnosti v oblastech jejich odpovědnosti,
k) zajistí stanovení pravidel pro určení administrátorů a osob, které budou zastávat bezpečnostní role,
l) zajistí, aby byla zachována mlčenlivost u všech relevantních osob (např. administrátorů, osob zastávajících bezpečnostní role, osob s přístupem k citlivým informacím, dodavatelů apod.)
m) pro osoby zastávající bezpečnostní role zajistí příslušné pravomoci a zdroje včetně rozpočtových prostředků k naplňování jejich rolí a plnění souvisejících úkolů a
n) zajistí testování plánů kontinuity činností, plánů obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů.

Vyhláška pro režim nižších povinností

§ 5
Povinnosti vrcholného vedení

Vrcholné vedení s ohledem na zajišťování kybernetické bezpečnosti
a) je prokazatelně poučeno o jeho povinnostech a rozsahu odpovědností,
b) zajistí dostupnost zdrojů potřebných pro zajišťování kybernetické bezpečnosti v souladu s přehledem bezpečnostních opatření,
c) se prokazatelně seznamuje s plněním přehledu bezpečnostních opatření dle § 4 odst. 2 písm. a).

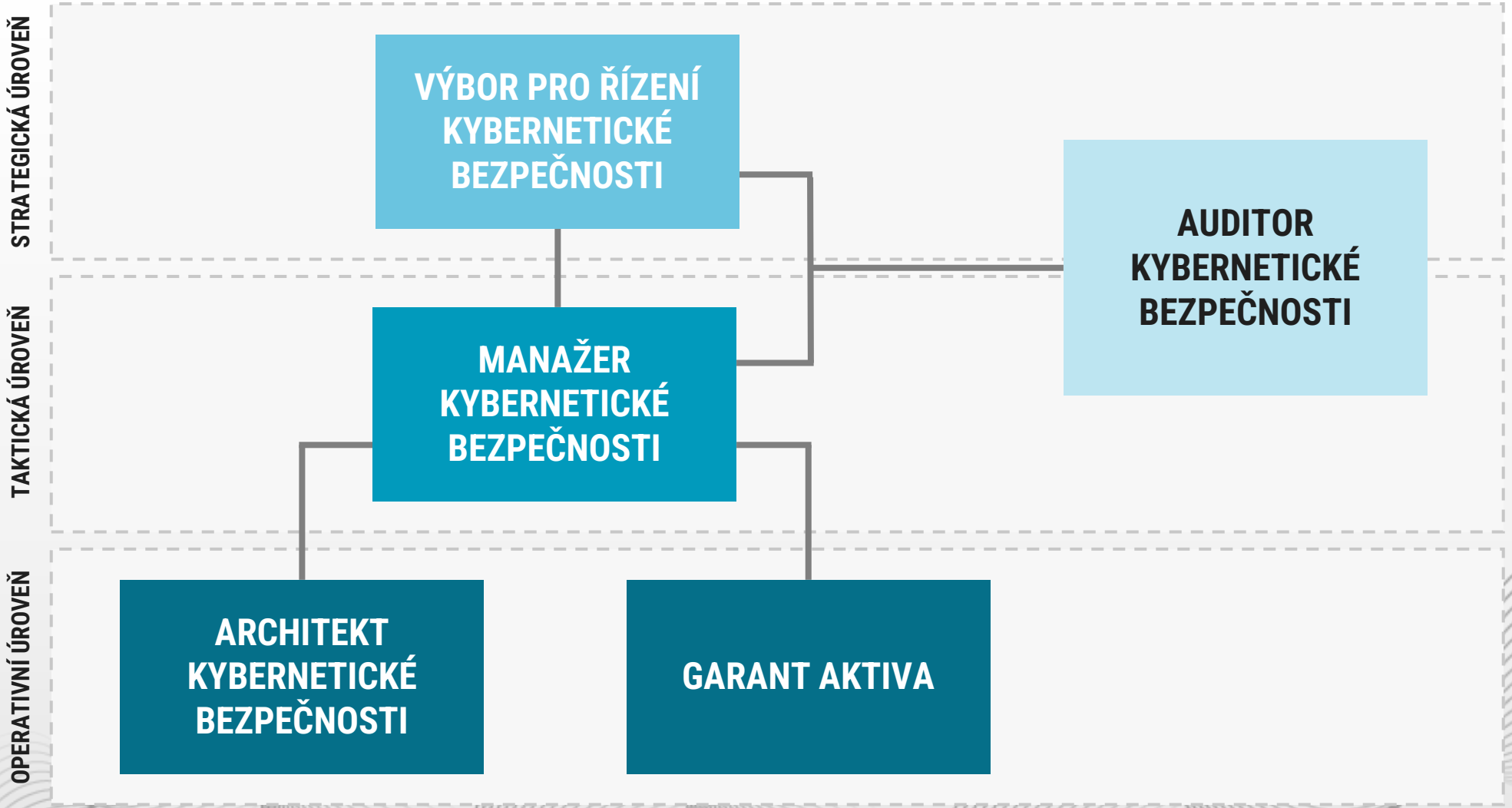
PIERSTONE

Bezpečnostní role.

PIERSTONE

Určení bezpečnostních rolí.

Vyhláška pro režim vyšších povinností



Zdroj: Národní úřad pro kybernetickou a informační bezpečnost

Výbor pro řízení kybernetické bezpečnosti.

Vyhláška pro režim vyšších povinností

Složení výboru pro řízení kybernetické bezpečnosti:

- Osoby s příslušnými pravomocemi a odbornou způsobilostí pro celkové řízení bezpečnosti informací
- Osoby významně se podílející na řízení a koordinaci činností spoj. s kybernetickou bezpečností
- Min. 1 zástupce vrcholného vedení / jím pověřená osoba
- Manažer kybernetické bezpečnosti

Požadavky:

Role:	Výbor pro řízení kybernetické bezpečnosti
Klíčové činnosti:	a) Odpovědnost za celkové řízení a rozvoj kybernetické bezpečnosti v rámci povinné osoby. b) Tvorba rámce kybernetické bezpečnosti, směrování a zásad kybernetické bezpečnosti povinné osoby (definování strategických cílů a směrování rozvoje v oblasti kybernetické bezpečnosti). c) Definice rolí a odpovědností v rámci systému řízení bezpečnosti informací. d) Definice požadavků na podávání zpráv a kontrolu systému řízení bezpečnosti informací. e) Kontrola aktuálního stavu kybernetické bezpečnosti v rámci povinné osoby a zjišťování, zda dochází k naplňování plánovaných cílů.
Další podmínky:	a) Člen výboru pro řízení kybernetické bezpečnosti musí být alespoň 1. zástupce vrcholného vedení nebo jím pověřená osoba, 2. manažer kybernetické bezpečnosti. b) Členové výboru pro řízení kybernetické bezpečnosti se pravidelně scházejí, přičemž průběh a výstupy z jednání jsou uchovávány v listinné nebo elektronické podobě.

PIERSTONE

Manažer kybernetické bezpečnosti.

Vyhláška pro režim vyšších povinností

Náplň role:

Odpovědnost a kvalifikace:

- Odpovědnost za systém řízení bezpečnosti informací
- Osoba musí být vyškolená a splnit jednu z podmínek odborné způsobilosti:
  - 3 roky praxe v řízení kybernetické bezpečnosti nebo bezpečnosti informací, nebo
  - 1 rok praxe, pokud absolvovala studium na VŠ

Povinnosti:

- Pravidelné informování vrcholného vedení o:
  - činnostech v rozsahu své odpovědnosti a
  - stavu systému řízení bezpečnosti informací

Omezení:

- Nesmí být pověřena výkonem rolí odpovědných za provoz regulované služby.

Požadavky:

Role:	Manažer kybernetické bezpečnosti
Klíčové činnosti:	a) Odpovědnost za řízení systému řízení bezpečnosti informací. b) Pravidelný reporting pro vrcholné vedení povinné osoby. c) Pravidelná komunikace s vrcholným vedením povinné osoby. d) Koordinace a podílení se na procesu řízení aktiv a rizik. e) Předkládání zpráv o hodnocení aktiv a rizik, plánu zvládání rizik a prohlášení o aplikovatelnosti výboru pro řízení kybernetické bezpečnosti. f) Poskytování pokynů pro zajištění bezpečnosti informací při vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů. g) Komunikace s Vládním nebo Národním CERT. h) Koordinace řízení incidentů. i) Vyhodnocování vhodnosti a účinnosti bezpečnostních opatření.
Znalosti:	a) Normy řady ISO/IEC 27000 a obdobné normy z oblasti bezpečnosti a ICT. b) Přehled v oblasti ICT (operační systémy, databáze, aplikace, datové sítě) s důrazem na bezpečnost. c) Řízení rizik. d) Řízení kontinuity činností. e) Relevantní právní a regulatorní požadavky, zejména zákon. f) Kontext povinné osoby
Zkušenosti:	a) Prosazování systému řízení bezpečnosti informací. b) Porozumění definicím rizik a rizikovým scénářům. c) Řízení rizik v rámci povinné osoby. d) Schopnost interpretovat výsledky řízení rizik a koordinovat zvládání rizik.
Vzdělání a praxe:	a) Alespoň 3 roky praxe v oboru informační nebo kybernetické bezpečnosti, nebo b) absolvování studia na vysoké škole a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti.
Relevantní certifikace*:	Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional (CISSP), Manažer BI (akreditační schéma ČIA).
Další podmínky:	a) Role není slučitelná s rolemi odpovědnými za provoz ICT a s dalšími provozními či řídicími rolemi. b) Pro správný výkon této role je zapotřebí zajistit potřebné pravomoci, odpovědnost a rozpočet

PIERSTONE

Architekt kybernetické bezpečnosti.

Vyhláška pro režim vyšších povinností

Náplň role:

Odpovědnost a kvalifikace:

- Odpovědnost za návrh implementace bezpečnostních opatření s cílem zajištění bezpečné architektury regulované služby.
- Osoba musí být vyškolená a splnit jednu z podmínek odborné způsobilosti praxí s navrhováním implementace bezpečnostních opatření a zajišťováním architektury bezpečnosti v délce:
  - 3 roky, nebo
  - 1 rok, pokud absolvovala studium na vysoké škole.

Požadavky:

Role:	**Architekt kybernetické bezpečnosti**
Klíčové činnosti:	a) Odpovědnost za návrh implementace bezpečnostních opatření. b) Odpovědnost za stanovení, dokumentování, údržbu a neustálý rozvoj vhodné bezpečné architektury regulované služby podle aktuální dobré praxe.
Znalosti:	a) Architektura informačních a komunikačních systémů a její navrhování. b) Hardwarové komponenty, nástroje a architektury. c) Operační systémy a software. d) Podnikové procesy a jejich integrace a závislost na ICT. e) Řízení bezpečnosti a rizik. f) Bezpečnost komunikací a sítí. g) Řízení identit a přístupů. h) Hodnocení a testování bezpečnosti. i) Bezpečnost provozu. j) Základní principy bezpečného vývoje softwaru. k) Integrace a závislosti ICT a obchodních procesů.
Zkušenosti:	a) Navrhování a implementace bezpečnostních opatření. b) Navrhování bezpečné architektury. c) Bezpečnost vývoje softwaru.
Vzdělání a praxe:	a) Alespoň 3 roky praxe v oboru informační nebo kybernetické bezpečnosti, nebo b) absolvování studia na vysoké škole a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti.
Relevantní certifikace*:	Certified Ethical Hacker (CEH), CompTIA Security +, Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional (CISSP), Manažer BI (akreditační schéma ČIA).
Další podmínky:	Role není slučitelná s rolemi odpovědnými za provoz ICT.

PIERSTONE

Auditor kybernetické bezpečnosti.

Vyhláška pro režim vyšších povinností

Náplň role:

Odpovědnost a kvalifikace:

- Odpovědnost za provádění auditu kybernetické bezpečnosti.
- Osoba musí být vyškolená a splnit jednu z podmínek odborné způsobilosti praxí s prováděním auditů kybernetické bezpečnosti nebo auditů systému řízení bezpečnosti informací v délce:
  - 3 roky, nebo
  - 1 rok praxe, pokud absolvovala studium na vysoké škole.

Povinnosti:

- Zaručuje nestrannost při provádění auditu kybernetické bezpečnosti.

Omezení:

- Nesmí být pověřena výkonem jiných bezpečnostních rolí.

Požadavky:

Role:	Auditor kybernetické bezpečnosti
Klíčové činnosti:	a) Provádění auditu kybernetické bezpečnosti. b) Hodnocení správnosti a účinnosti zavedených bezpečnostních opatření.
Znalosti:	a) Metodologie a rámce auditu informační bezpečnosti. b) Procesy a postupy interního auditu. c) Role a funkce interního auditu. d) Proces provádění auditu ICT bezpečnosti. e) Strategické a taktické řízení ICT. f) Akvizice, vývoj a nasazení ICT. g) Řízení provozu, údržby a služeb ICT. h) Ochrana aktiv. i) Hodnocení kybernetické bezpečnosti, metody testování a vzorkování. j) Relevantní právní předpisy. k) ICT bezpečnost.
Zkušenosti:	a) Plánování auditů informační nebo kybernetické bezpečnosti. b) Provádění auditů kybernetické bezpečnosti nebo auditů systému řízení bezpečnosti informací. c) Analyzování výsledků auditů. d) Psaní auditních závěrů, jejich prezentace a navrhování doporučení vedoucích k nápravě nálezů. e) Reporting stavu plnění zákonných požadavků. f) Provádění auditů se zaměřením na ICT a informační nebo kybernetickou bezpečnost.
Vzdělání a praxe:	a) Alespoň 3 roky praxe v oblasti auditu informační nebo kybernetické bezpečnosti, nebo b) absolvování studia na vysoké škole a alespoň 1 rok praxe v oblasti auditu informační nebo kybernetické bezpečnosti.
Relevantní certifikace*:	Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), Certified in Risk and Information Systems Control (CRISC), Lead Auditor Information Security Management Systém (Lead Auditor ISMS), Auditor BI (akreditační schéma ČIA).
Další podmínky:	a) Role není slučitelná s rolemi 1. výboru pro řízení kybernetické bezpečnosti, 2. manažera kybernetické bezpečnosti, 3. architekta kybernetické bezpečnosti, 4. garanta aktiva. b) Role není slučitelná s rolemi odpovědnými za provoz ICT.

PIERSTONE

Garant aktiva.

Vyhláška pro režim vyšších povinností

Náplň role:

Odpovědnost:
Odpovědnost za zajištění rozvoje, použití a bezpečnosti aktiva.

Požadavky:

Role:	Garant aktiva:
Klíčové činnosti:	a) Odpovědnost za zajištění rozvoje, použití a bezpečnosti aktiva. b) Spolupráce s ostatními osobami zastávajícími bezpečnostní role. c) Provádění identifikace a hodnocení aktiv a rizik.
Znalosti:	a) Dobrá znalost aktiva, jehož je garantem. b) Dobrá znalost interních bezpečnostních politik a metodik (například Metodika pro hodnocení aktiv a rizik).

PIERSTONE

Souběh rolí, outsourcing rolí.

Vyhláška pro režim vyšších povinností

TATÁŽ OSOBA

- Manažer kybernetické bezpečnosti
- Architekt kybernetické bezpečnosti
- Garant aktiv

Auditor

OUTSOURCING ROLÍ?

ANO
Pozice významného dodavatele

Řízení rizik nad dodavatelem

PIERSTONE

„Pověřená“ osoba.

Vyhláška pro režim nižších povinností

Role:

Obdoba manažera kybernetické bezpečnosti

Odpovědnost:

- Odpovědnost za řízení a rozvoj kybernetické bezpečnosti, dohled nad stavem kybernetické bezpečnosti a komunikaci v oblasti kybernetické bezpečnosti s vrcholným vedením.
- Osoba musí
  1. absolvovat odborné školení odborné školení, nebo
  2. prokázat odbornou způsobilost v oblasti kybernetické bezpečnosti.

Požadavky:

S ohledem na **nedostupnost osob** v oboru kybernetické bezpečnosti v ČR musí organizací určená osoba pověřená řízením kybernetické bezpečnosti pouze absolvovat **odborné školení**, nebo jinak **doložit odbornou způsobilost** v oblasti kybernetické bezpečnosti.

Zákon ani navazující vyhláška pro nižší režim **nestanovují žádné konkrétní doporučené znalosti, zkušenosti, vzdělání a praxi, relevantní certifikaci** či jiné požadavky. Je na zvážení poskytovatele regulované služby v režimu nižších povinností, aby vyhodnotil dostatečnou odbornou způsobilost pověřené osoby, případně zajistil další odborné školení této osoby.

PIERSTONE

Rozdělení úkolů, odpovědností a pravomocí.

Nařízení (EU) 2024/2690

1.2.1 přílohy nařízení

*Příslušné subjekty v rámci **politiky bezpečnosti sítí a informačních systémů** **stanoví odpovědnosti, přidělí je k úkolům, rozdělí je podle potřeb příslušných subjektů a sdělí je řídícím orgánům**.“*

1.2.3 přílohy nařízení

Řídícím orgánům je** v otázkách bezpečnosti sítí a informačních systémů **přímo podřízena alespoň jedna osoba.

1.2.4. přílohy nařízení

V závislosti na velikosti příslušných subjektů spadá bezpečnost sítí a informačních systémů pod specializované úkoly nebo povinnosti, které jsou vykonávány nad rámec stávajících úkolů.

1.2.5. přílohy nařízení

Kolidující povinnosti a protichůdné oblasti odpovědnosti budou v příslušných případech odděleny.

1.2.6. přílohy nařízení

*Řídící orgány **úkoly, odpovědnosti a pravomoci přezkoumávají** a v případě potřeby aktualizují **v plánovaných intervalech a při výskytu významných incidentů nebo významných změn operací či rizik**.*

PIERSTONE

Řízení lidských zdrojů.

PIERSTONE

Bezpečnost lidských zdrojů.

Vyhláška pro režim nižších/vyšších povinností

Požadavky bezpečnosti lidských zdrojů	Vyhláška pro režim nižších povinností	Vyhláška pro režim vyšších povinností
Povinná politika bezpečnosti lidských zdrojů?	*Politika bezpečného chování uživatelů*	*Plán rozvoje bezpečnostního povědomí*
Povinný plán rozvoje bezpečnostního povědomí?	*Pravidla rozvoje bezpečnostního povědomí*	*Plán rozvoje bezpečnostního povědomí*
Vstupní a pravidelná školení	✓ § 6 d)	✓ § 11(3)a)
Kontrola dodržování bezpečnostní politiky	✓ § 6 h)	✓ § 11(3)d)
Pravidla a postupy pro řešení případů porušení bezpečnostních pravidel	✓ § 6 i)	✓ § 11(3)e)
Hodnocení účinnosti plánu rozvoje bezpečnostního povědomí, poučení a školení	✗	✓ § 11(3)c)
Určení osoby odpovědné za realizaci jednotlivých činností v plánu rozvoje bezpečnostního povědomí	✗	✓ § 11(3)b)
Předání odpovědností v případě ukončení / změny smluvního vztahu s administrátory a osobami v bezpečnostních rolích	✗	✓ § 11(3)f)

PIERSTONE

Ověření spolehlivosti.

Nařízení (EU) 2024/2690

10.2. přílohy nařízení

*Příslušné subjekty v proveditelném rozsahu zajistí, aby se u jejich zaměstnanců provádělo **ověřování spolehlivosti**, pokud to vyžadují jejich úkoly, povinnosti a oprávnění.*

Příslušné subjekty zavádí kritéria, která stanoví, které úkoly, odpovědnosti a pravomoci mohou vykonávat pouze osoby, jejichž spolehlivost byla ověřena.

- *Ověření spolehlivosti těchto osob vezme v potaz **platné zákony, předpisy a etické zásady** úměrně k obchodním požadavkům, ke klasifikaci aktiv, k sítím a informačním systémům, k nimž mají mít přístup, a vnímaným rizikům.*
- *Ověření spolehlivosti musí být provedeno **před tím, než tyto osoby začnou vykonávat dané úkoly, odpovědnosti a pravomoci.***

Povinnost postupy pravidelně přezkoumávat a v případě potřeby aktualizovat.

PIERSTONE

Disciplinární řízení, ukončení pracovního poměru.

DISCIPLINÁRNÍ ŘÍZENÍ

Nařízení (EU) 2024/2690

*Příslušné subjekty **zavedou, sdělí a udržují disciplinární postup pro řešení porušení politik bezpečnosti sítí a informačních systémů**. Tento postup zohledňuje příslušné právní, zákonné, smluvní a obchodní požadavky.*

Vyhláška pro nižší/vyšší režim

N: *Pravidla a postupy pro řešení případů porušení bezpečnostní politiky.*

V: *Pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel **ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.***

UKONČENÍ PRACOVNÍHO POMĚRU

Nařízení (EU) 2024/2690

- *Příslušné subjekty zajistí, aby byly **smluvně vymezeny a vymáhány odpovědnosti a povinnosti** v oblasti bezpečnosti sítí a informačních systémů, **které zůstávají v platnosti i po ukončení nebo změně pracovního poměru jejich zaměstnanců**.*

- *Příslušné subjekty začlení do pracovních podmínek, smlouvy nebo dohody fyzické osoby odpovědnosti a povinnosti, které zůstávají v platnosti i po ukončení pracovního poměru nebo smlouvy, například ustanovení o důvěrnosti.*

Vyhláška pro režim vyšších povinností

- *V případě ukončení nebo změny smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role **zajistí předání odpovědností**.*

PIERSTONE

Zvyšování povědomí, školení.

PIERSTONE

Školení, rozvoj bezpečnostního povědomí.

Vyhláška pro režim nižších/vyšších povinností

- Plán rozvoje bezpečnostního povědomí (režim vyšších povinností)
- Pravidla rozvoje bezpečnostního povědomí (režim nižších povinností)

Příloha č. 3 vyhlášky pro nižší režim / Příloha č. 7 vyhlášky pro vyšší režim

Doporučená témata pro rozvoj bezpečnostního povědomí

a) Techniky zabezpečení zařízení.
b) Firewall, antivirový program a jejich omezení.
c) Škodlivé programy a jejich projevy.
d) Rizika stahování programů a aplikací.
e) Aktualizace softwaru.
f) Rizika povolení/zakázání spouštění maker.
g) Rizika spustitelných souborů.
h) Zásady zabezpečení uživatelských účtů.
i) Používání, tvorba a správa hesel.
j) Vícefaktorová autentizace.
k) Techniky sociálního inženýrství.
l) Online identita, digitální stopa a její minimalizace.
m) Zásady práce v počítačové síti.
n) Používání vzdáleného připojení (VPN).
o) Bezpečná elektronická komunikace.
p) Bezpečnost webových stránek.
q) Zálohování, ukládání a šifrování dat.
r) Bezpečné používání přenosných technických nosičů dat.
s) Využívání cloudových úložišť.
t) Pravidla a postupy pro oznamování neobvyklého chování technických aktiv a podezření na jakékoliv zranitelnosti.
u) Základní postup reakce na kybernetickou bezpečnostní událost nebo incident.
v) Zásady bezpečného používání pracovních zařízení pro soukromé účely.
w) Zásady bezpečného používání soukromých zařízení pro pracovní účely (tzv. BYOD).
x) Osobní odpovědnost zaměstnance při dodržování zásad kybernetické bezpečnosti.
y) Aktuální hrozby v kybernetické bezpečnosti.

PIERSTONE

Základní postupy v oblasti kybernetické hygieny.

Nařízení (EU) 2024/2690

> *Subjekty zajistí, aby si jejich zaměstnanci, včetně členů řídících orgánů, přímí dodavatelé a poskytovatelé služeb byli vědomi rizik, informování o významu kybernetické bezpečnosti a uplatňovali postupy v oblasti kybernetické hygieny.*

Program zvyšování povědomí / informovanosti (awareness raising programme)

- Plánován tak, aby se v něm opakovaly různé aktivity a zahrnoval nové zaměstnance.
- Vytvořen v souladu s Politikou bezpečnosti sítí a informací, technicky zaměřenými politikami a příslušnými postupy bezpečnosti sítí a informací.
- Zahrnuje relevantní kybernetické hrozby, opatření k řízení bezpečnostních rizik, nebo postupy v oblasti kybernetické hygieny.

Pravidelné testování a aktualizace

Program zvyšování povědomí / informovanosti se pravidelně testuje a aktualizuje s přihlédnutím ke změnám postupů v oblasti kybernetické hygieny aktuálním hrozbám a rizikům.

Bezpečnostní školení.

Nařízení (EU) 2024/2690

Pouze pro **zaměstnance**, jejichž **funkce a pozice vyžadují dovednosti a odborné znalosti v oblasti bezpečnosti.**

Školení v oblasti bezpečnosti sítí a informačních systémů (training on network and information system security)

- Pokyny týkající se bezpečné konfigurace a provozu sítí a informačních systémů, včetně mobilních zařízení.
- Informování o známých kybernetických hrozbách.
- Chování v případě výskytu bezpečnostních událostí.

Další požadavky na obsah školení

- Vytvořen v souladu s Politikou bezpečnosti sítí a informací, technicky zaměřenými politikami a příslušnými postupy bezpečnosti sítí a informací.
- Pravidelně aktualizován s přihlédnutím k interním politikám, rozdělení odpovědnosti, kybernetickým hrozbám a technologickému vývoji.

PIERSTONE

Vymáhání povinností.

PIERSTONE

Sankční mechanismy.

Dozorový orgán

Příslušným regulátorem je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).

Finanční postihy

NÚKIB může udělit pokutu do výše až **250 mil. Kč** nebo **2 % čistého celosvětového ročního obratu** podniku pro nezavedení/neprovádění stanovených bezpečnostních opatření.

NÚKIB může dále rozhodnout o uložení pořádkové pokuty 100 tis. Kč (i opakovaně) nebo donucovací pokuty až do výše **10 mil. Kč nebo 1 % z čistého obratu za poslední ukončené účetní období.**

Ostatní sankční mechanismy

Vedle pokut zahrnuje nový ZKB i jiné správní tresty, jako pozastavení certifikace či **dočasný zákaz výkonu funkce člena statutárního orgánu** do doby odstranění zjištěných nedostatků, nejméně však 6 měsíců. **Tyto sankce však platí pouze pro poskytovatele regulovaných služeb s vyšším režimem povinností.**

Odpovědnostní aspekty.

Porušení péče řádného hospodáře

- *Ručení za závazky společnosti (§ 159/3 OZ)*
- *Vyloučení člena statutárního orgánu (§ 63 ZOK)*
- *Povinnost uhradit újmu (§ 53/3 ZOK)*

Porušení zákonné povinnosti (§ 2910 OZ)

- *Subjektivní odpovědnost*
- *Zákonný standard pečlivosti (§ 2912)*

Porušení smluvní povinnosti (§ 2913 OZ)

- *Objektivní odpovědnost*
- *Smluvní omezení*
- *Možnost liberace (§ 2913 OZ)*

Obecná prevenční povinnost (§ 2900 OZ)

PIERSTONE

Děkujeme za Vaši pozornost.

Mgr. Dominik Vítek, Ph.D.
dominik.vitek@pierstone.com

PIERSTONE
Perlová 371/5, Praha
www.pierstone.com | in