

NIS2: Osobní odpovědnost, rizika a jasná cesta k souladu.

Kompletní přehled povinností pro vedení firmy
i IT oddělení (zákon č. 264/2025 Sb.
a vyhláška č. 410/2025 Sb.)



[ÚČINNOST]:
1. 11. 2025



[LHŮTA NA OPATŘENÍ]:
12 měsíců



[KONTROLNÍCH
BODŮ]: **65**





Osobní odpovědnost nelze delegovat.



Zákon přenáší odpovědnost přímo na statutární orgán. Nelze ji plně převést na IT ani externího správce.

Pokuta až 250 mil. Kč
nebo 2 % celosvětového obrátu.

HROZÍ ZÁKAZ VÝKONU FUNKCE



Investice s nejvyšší návratností — ochrana před ztrátou zakázek a reputační škodou.

GAP Analýza:
50–100 tis. Kč

MÉNĚ NEŽ 0,04 % MAXIMÁLNÍ POKUTY





NIS2 ze dvou úhlů pohledu.



Dopad na Management (Boardroom)



Osobní ručení a zákaz činnosti.



Nutnost formálně akceptovat reziduální rizika.



Zajištění a schválení vyhrazeného rozpočtu.



Povinné školení statutárních orgánů (§4b).



Dopad na IT (Server Room)



Nová SLA na patch management a hlášení incidentů (24h).



Striktní MFA: Uživatel 12 znaků, Admin 17 znaků, Tech aktiva 22 znaků.



Nasazení EDR/XDR a segmentace sítě.



Offline a immutable zálohy proti ransomware.



Architektura souladu: Od 65 bodů ke 3 strategickým pilířům

Komplexní požadavky zákona rozdělené do srozumitelných celků

Lidé & Vedení

Governance, školení,
rozpočty, CISO

Mapuje 12 bodů

Procesy, Rizika & Reakce

ISMS, kontinuita, hlášení
incidentů

Mapuje 20 bodů

Technologie, Dodavatelé & Fyzická ochrana

MFA, síť, zálohy, SLA

Mapuje 33 bodů



Pilíř 1: Lidé & Vedení.

Zajištění governance a bezpečnostního povědomí.

Statutární orgán

CISO
(Manažer KB)

Formálně jmenován CISO (manažer KB) s přímým přístupem k vedení a dostatečnými pravomocemi.

[KRITICKÁ]

Schválena a fyzicky podepsána top-level bezpečnostní politika. Alokován vyhrazený rozpočet na příští rok.

[KRITICKÁ]

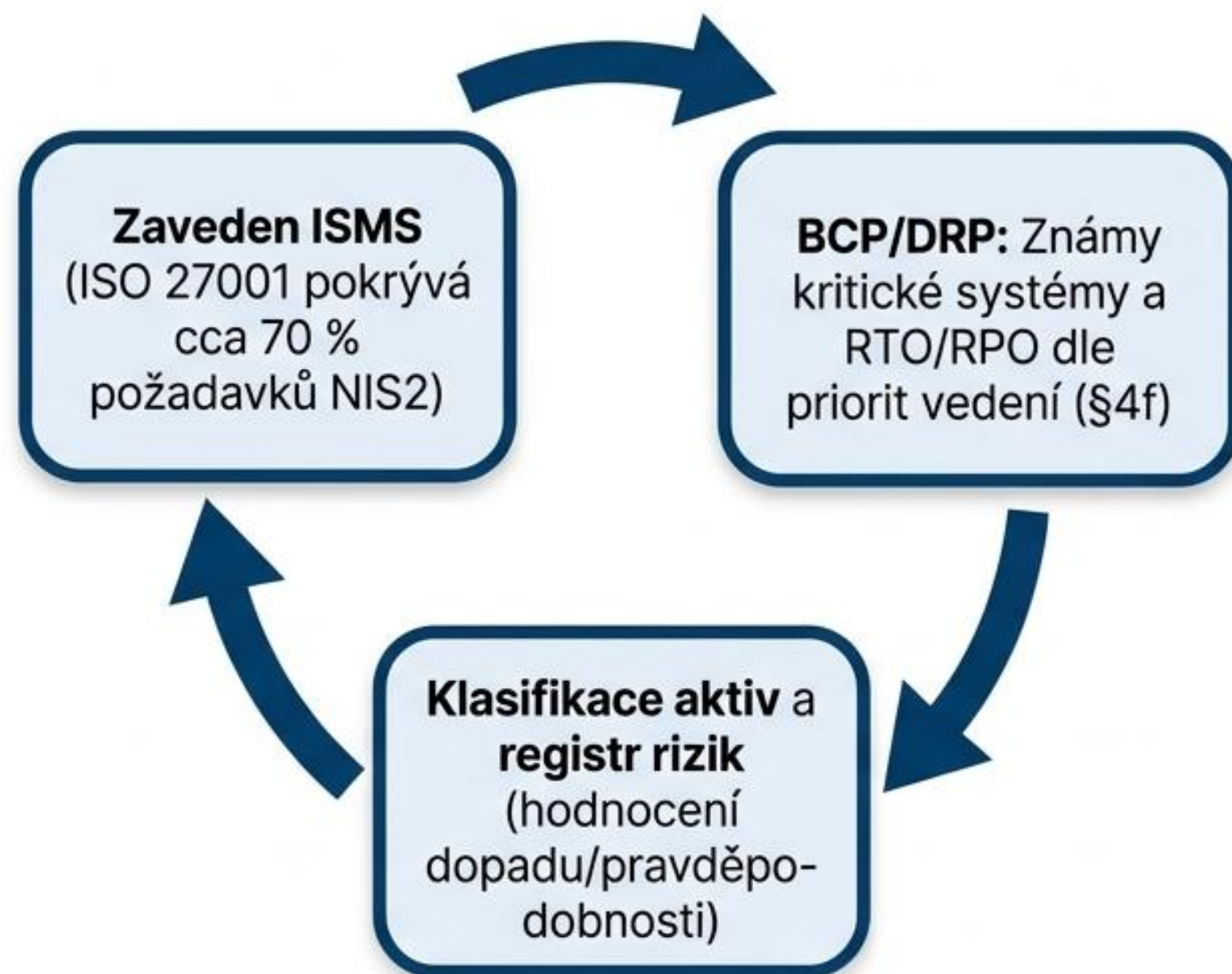
Povinná školení pro vedení. Pravidelná školení a simulace phishingových útoků pro zaměstnance.

[VYSOKÁ]



Pilíř 2: Procesy, Rizika a Reakce

Zavedení ISMS a striktních pravidel pro kontinuitu





Pilíř 3: Technologie, Dodavatelé a Obrana.

Specifické technické parametry a ochrana dodavatelského řetězce.



Přístup

Přístup

Least privilege & MFA.
(Specifikace: Uživatel 12 zn., Admin 17 zn.,
Technická aktiva 22 zn.)



Obrana

Obrana

Segmentace sítě.
EDR/XDR na serverech
i stanicích. TLS 1.2+.



Zálohování

Zálohování

Strategie 3-2-1.
Offline a immutable
(ransomware-proof)
kopie. Testy obnovy
min. 1× za 6 měsíců.



Dodavatelé

Dodavatelé

Ve smlouvách bezp.
požadavky (Příloha č. 2),
SLA, právo auditu a
ošetřený přístup (VPN).

Akční plán: 5 absolutních priorit pro start.



1 **Ověření rozsahu a registrace:** Klasifikace systémů a registrace u NÚKIB (do 30 dnů od splnění podmínek).

Action Required

2 **Jmenování CISO:** Definování role s přímou linkou na statutární orgán.

Action Required

3 **MFA a Segmentace:** Zabezpečení privilegovaných účtů a oddělení kritických systémů.

Action Required

4 **Immutable Zálohy:** Odstřižení záloh od sítě jako prevence proti ransomware.

Action Required

5 **Identifikace dodavatelů:** Vytvoření evidence klíčových IT dodavatelů a revize SLA.

Action Required

Architektura souladu: 10 sekcí a 65 bodů ve třech strategických pilířích



Compliance Radar

Strategie a Řízení 25 bodů celkem

1. Identifikace a rozsah (5 bodů)
2. Governance a odpovědnosti (7 bodů)
3. Řízení rizik (6 bodů)
4. Bezpečnostní politiky a ISMS (7 bodů)

Ochrana a Detekce 22 bodů celkem

5. Technická bezpečnostní opatření (10 bodů)
6. Řízení incidentů a hlášení NÚKIB (7 bodů)
10. Fyzická bezpečnost a komunikace (5 bodů)

Odolnost a Ekosystém 18 bodů celkem

7. Kontinuita provozu a zálohování (6 bodů)
8. Bezpečnost dodavatelského řetězce (6 bodů)
9. Školení a bezpečnostní povědomí (6 bodů)

Priorita opatření: ■ **KRITICKÁ** (Řešit okamžitě) ■ **VYSOKÁ** (1–3 měsíce) ■ **STŘEDNÍ** (Best practice)



Pilíř I: Strategie, odpovědnost a řízení rizik

Identifikace (5 bodů)

⑤

- Určení klasifikace (režim vyšších/nížších povinností).
- Registrace u NÚKIB (do 30 dnů od splnění podmínek).

Governance (7 bodů)

⑦

- Formální jmenování CISO (s přímým přístupem k vedení).
- Povinné školení kyberbezpečnosti pro statutární orgán (§4b).
- Vedením podepsaná bezpečnostní politika.

Řízení rizik (6 bodů)

⑥

- Zavedení formální metodiky řízení rizik.
- Klasifikace aktiv a aktuální registr rizik (dopad/pravděpodobnost).
- Plán zvládání rizik s konkrétními termíny.

ISMS a Politiky (7 bodů)

⑦

- Implementace ISMS (ISO 27001 pokrývá cca 70 % požadavků NIS2).
- Schválené politiky: řízení přístupu, klasifikace dat, dodavatelé.

Pilíř II: Technologická ochrana, detekce a incidenty



Technická opatření (10 bodů)

- **Řízení přístupu:** Vícefaktorové ověření (MFA) a princip nejmenších oprávnění.
- **Ochrana sítě:** Segmentace kritických systémů a firewall na perimetru.
- **Endpoint a servery:** Automatická ochrana (EDR/XDR) a bezodkladný patching.
- **Šifrování dat** v klidu i při přenosu.

Řízení incidentů (7 bodů)

- **Incident Response Plan:** Formální plán a eskalační postupy.

- **Hlášení NÚKIB:** Striktní časová osa:



Fyzická bezpečnost (5 bodů)

- **Zabezpečení:** Datové centrum/serverovna chráněna přístupovým systémem a kamerami.
- **Prostředí:** Ochrana proti požáru, vodě a výpadku proudu (UPS/diesel).



Pilíř III: Odolnost ekosystému, dodavatelé a lidé

Kontinuita a zálohování (6 bodů)

- **Plány obnovy:** Business Continuity Plan (BCP) a Disaster Recovery Plan (DRP) na základě BIA.
- **Zálohování (3-2-1):** Immutable (neměnné) / offline kopie chráněné proti ransomware.
- **Testování:** Pravidelné testy obnovitelnosti záloh (min. 1× za 6 měsíců).

Dodavatelé (6 bodů)

- **Evidence a audit:** Hodnocení rizik klíčových dodavatelů IT.
- **Smlouvy:** Zakotvené bezpečnostní požadavky (SLA) a právo na audit (Příloha č. 2).
- **Exit strategie:** Plán pro ukončení spolupráce.

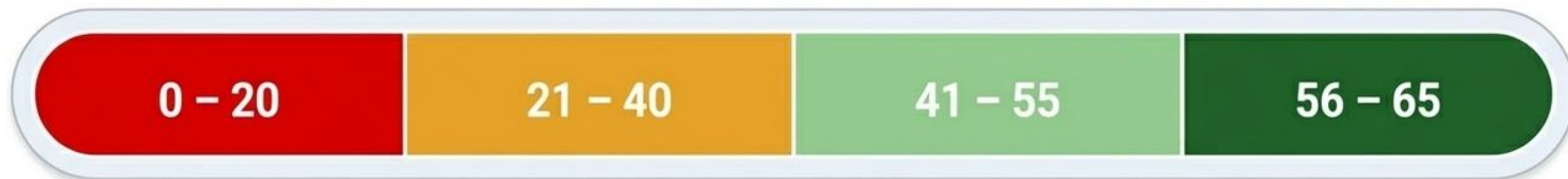
Školení zaměstnanců (6 bodů)

- **Plošné vzdělávání:** Vstupní a pravidelná roční školení s certifikátem.
- **Praktický trénink:** Simulace phishingových útoků a měření rizikových skupin.



Diagnostika připravenosti: Kde se nacházíte?

Zhodnocení stavu vůči 65 kontrolním bodům NIS2.



0 – 20 [Kritický stav]

Okamžitě zahájit GAP analýzu a implementaci.

21 – 40 [Částečná připravenost]

Základy jsou, chybí klíčové oblasti a procesní dokumentace.

41 – 55 [Dobrá připravenost]

Většina pokryta, zaměřte se na zbývající mezery a testování.

56 – 65 [Vysoká připravenost]

Dolad'te detaily, zajistěte průběžnou údržbu a audity.



Realistická časová osa implementace (3–6 měsíců)

Lhůta na opatření běží. Nečekejte na poslední chvíli.

Účinnost: 1. 11. 2025



Zajistěte klid pro vedení i IT oddělení.

Získejte přesnou GAP analýzu a konkrétní plán
nápravy s certifikovaným ISMS auditorem.



30min konzultace zdarma, bez závazků.
Kontaktujte Blue Partners.



+420 602 177 433



bluepartners.cz

