

23/9/2025

Nový Zákon (o kyberbezpečnosti)

Praktické zavedení krok za krokem

Nový zákon o kybernetické bezpečnosti.

Časová osa

- 26. června 2025 – zákon podepsán prezidentem.
- Poté předán do Sbírky zákonů (lhůta na zveřejnění max. 30 dní).
- Předpokládaná účinnost: 1. listopadu 2025.
- 60 dní na registraci
- 12 měsíců přechodné období na zavedení bezpečnostních opatření a hlášení incidentů od registrace.

Organizace spadají pod regulaci, pokud:

- Poskytují regulované služby (např. energetika, zdravotnictví, finance, doprava, veřejná správa apod.).
- Působí v regulovaném odvětví, i pokud nejsou přímo veřejnou institucí.
- Splňují vybraná kvantitativní kritéria, např. velikost (počet zaměstnanců, obrat).

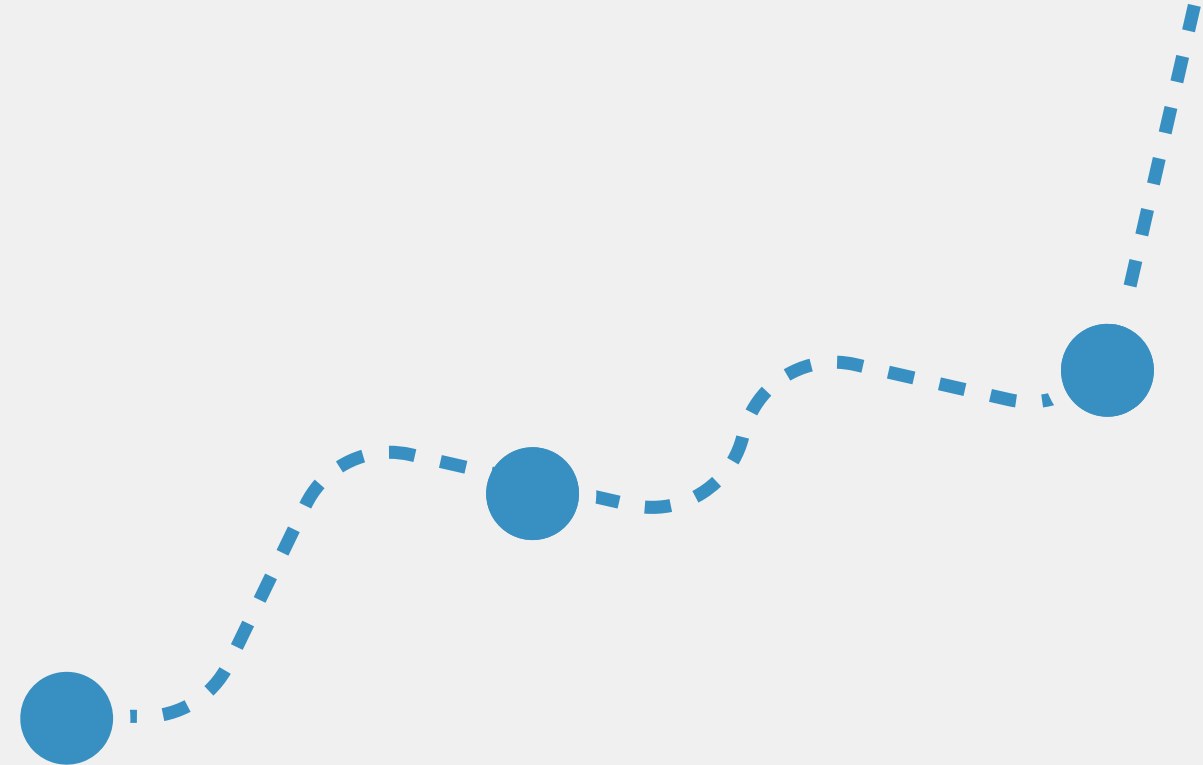
Režimy povinností podle nZKB

- **Vyšší režim:**
 - Rozšířené požadavky na bezpečnostní opatření, hlášení incidentů apod.
- **Nižší režim:**
 - Základní povinnosti – přiměřené rozsahu a typu služeb.

Režim se určí podle významnosti poskytované služby a velikosti organizace.

Nový zákon o kybernetické bezpečnosti.

10 kroků k implementaci nZKB.



KROK 1:

**ZJISTĚTE, ZDA SE NA VÁS
ZÁKON VZTAHUJE.**

Vyhláška o regulovaných službách

- 22 odvětví
- Regulované služby
- Doplnující podmínky

Regulovaná služba:

- služba, jejíž narušení by mohlo mít významný dopad na zabezpečení důležitých společenských nebo ekonomických činností a k jejímuž poskytování jsou používána aktiva,

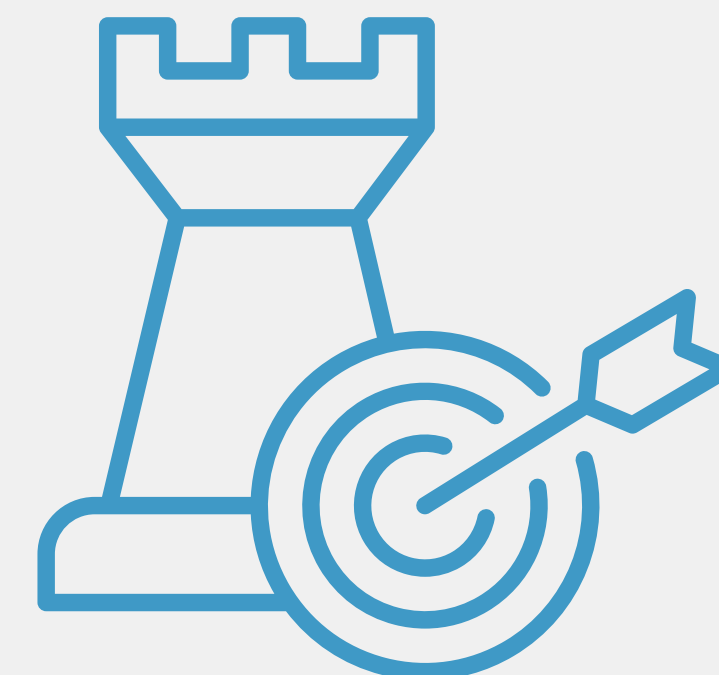
Poskytovatel regulované služby

- orgán nebo osoba, které poskytují jednu nebo více regulovaných služeb,

Pozor na “křížení” regulací

Jak to zjistíme?

KROK 2:
**PROVEĎTE SEBEHODNOCENÍ
A URČETE REŽIM
POVINNOSTÍ.**



Regulovaná služba

+

Kategorie podniku	Počet zaměstnanců: roční pracovní jednotka (RPJ)	Roční obrat	Bilanční suma roční rozvahy
Velký podnik	≥ 250	> 50 miliónů EUR	> 43 miliónů EUR
Střední podnik	< 250	≤ 50 miliónů EUR	≤ 43 miliónů EUR
Malý podnik	< 50	≤ 10 miliónů EUR	≤ 10 miliónů EUR
Mikro podnik	< 10	≤ 2 miliónů EUR	≤ 2 miliónů EUR

KROK 3:
**ZÍSKÁNÍ PODPORY
VRCHOLOVÉHO VEDENÍ.**



Jak se projevuje?

- Oznámení budování ISMS
- Jmenování bezpečnostních rolí
- Schválení bezpečnostních cílů a projektů
- Vydání bezpečnostní politiky

Podpora nejvyššího vedení

Role podle nZKB

- **Vyšší režim:**
 - Manažer KB
 - Architekt KB
 - Auditor KB
 - Výbor KB
 - Garanti (vlastníci) aktiv
- **Nižší režim:**
 - Osoba pověřená kybernetickou bezpečností

KROK 4:
**STANOVENÍ ROZSAHU
KYBERNETICKÉ BEZPEČNOSTI
VE VAŠÍ ORGANIZACI.**

Rozsah kybernetické bezpečnosti

Co je součástí regulované:

- Technologie
- Software
- Lidé
- Budovy
- Data a informace
- Dodavatelé

Rozdíl oproti ISO 27001/TISAX atd.:

- Jsou přímo určené hranice ISMS
- Regulovaná služba nemusí souviset k “core” činností společnosti

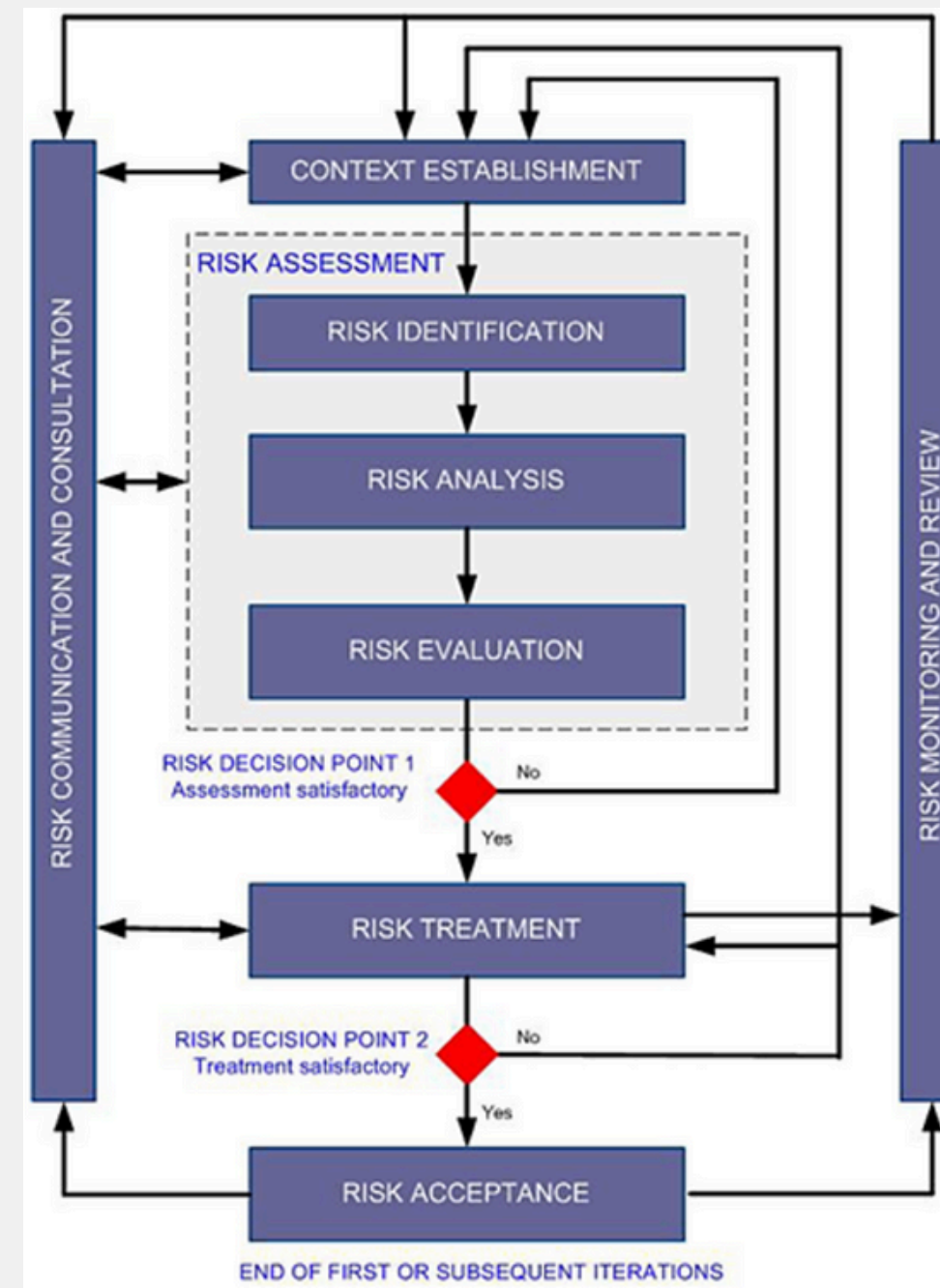
← Budeme potřebovat pro analýzu rizik

KROK 5:
**PROVEĎTE ANALÝZU A ŘÍZENÍ
RIZIK POKUD SPADÁTE DO
VYŠŠÍHO REŽIMU (A I KDYŽ NE) .**

Řízení rizik

Fáze:

- **1:** Stavenovení souvilostí (primární a podpůrná aktiv, hrozby a zranitelnosti, metodika)
- **2:** Analýza rizik
- **3:** Hodnocení rizik
- **4:** Ošetření rizik



Řízení rizik

Na co pamatovat?

- Vedení schvaluje celkové řešení rizik
- Vlastník rizika schvaluje plánovanou hodnotu zbytkového rizika
- Revidovat účinnost nasazených opatření
- Pravidelná činnost - nekončí po prvním cyklu

Základní pravdy:

- Papír snese všechno... a excel taky
- Kdo zná své prostředí, tak ví, jaká rizika mu hrozí
- Pravidlem starý server nezabezpečím

KROK 6:
**POLOŽTE STAVEBNÍ
KAMENY KYBERNETICKÉ
BEZPEČNOSTI (ISMS).**



ISMS

Bezpečnostní politika

Kontext (co je důležité)



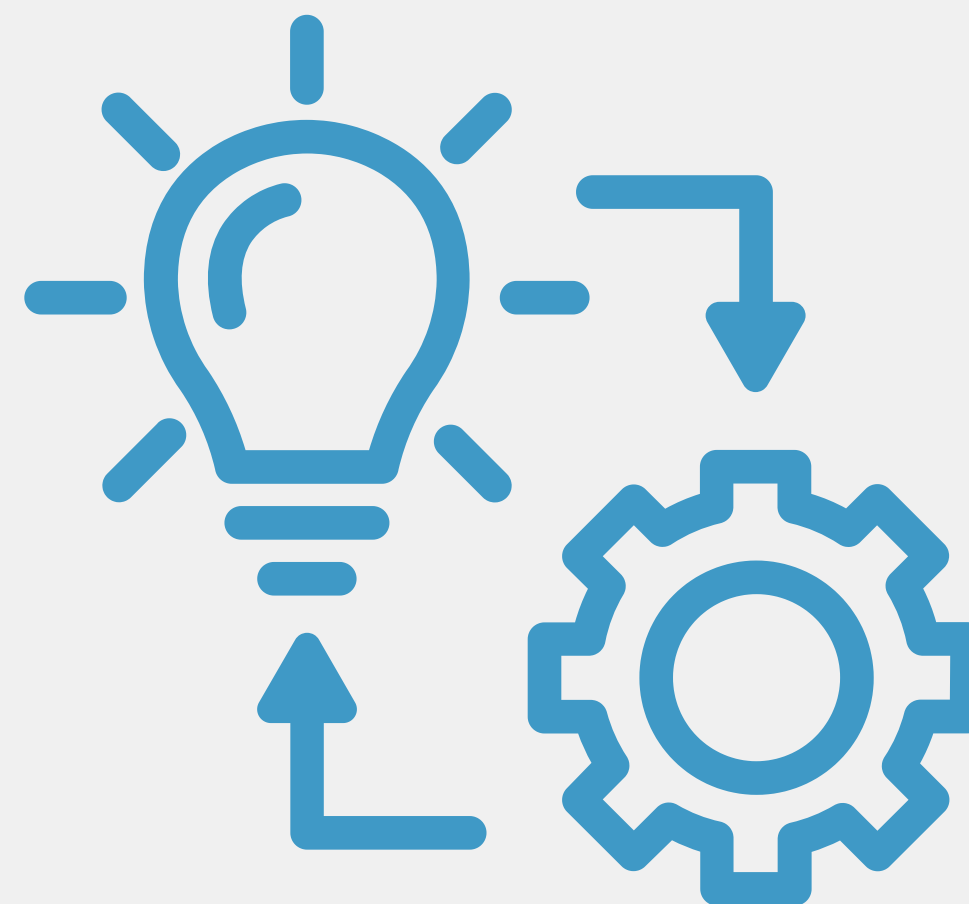
Kde leží rizika (co chráním)

Komunikace a spolupráce

Co nám zajišťují dodavatelé



KROK 7:
**IMPLEMENTUJTE
BEZPEČNOSTNÍ
OPATŘENÍ.**



Budujeme ISMS

Vyšší režim

- Řízení aktiv a rizik
- Řízení dodavatelů
- Bezpečnost lidských zdrojů
- Řízení změn
- Akvizice, vývoj a údržba
- Řízení přístupů
- Zvládání incidentů
- Řízení kontinuity činností
- Auditování
- Fyzická bezpečnost
- Bezpečnost sítí
- Přístupová práva a oprávnění
- Detekce událostí
- Zaznamenávání událostí
- Vyhodnocování událostí
- Aplikační bezpečnost
- Kryptografie
- Dostupnost reg. služby
- OT bezpečnost

Nižší režim

- Řízení kontinuity
- Řízení přístupů
- Řízení identit a oprávnění
- Detekce a zaznamenávání událostí
- Řešení incidentů
- Bezpečnost komunikačních sítí
- Aplikační bezpečnost
- Kryptografické algoritmy

Procesy - opatření - záznamy

KROK 8:
**NASTAVTE PROCES
ZVLÁDÁNÍ INCIDENTŮ
A HLÁŠENÍ.**

Řízení incidentů

Co je tady důležité:

- Připravte si jasný postup řízení incidentů
- Definujte konkrétní role (řešitele)
- Sestavte si plán reakce na incidenty
- Testujte, testujte, testujte!

Povinnosti pro vyšší režim:

- Prvotní hlášení do 24 hodin
- Průběžné hlášení (oznámení) do 72 hodin
- Závěrečné hlášení do 30 dnů

Povinnosti pro nižší režim:

- hlásit na CERT významné incidenty

<https://portal.nukib.gov.cz>



cert.incident@nukib.gov.cz

BESECURED

KROK 9:
**PROVEĎTE AUDIT A
PŘEZKUM SYSTÉMU.**

Audit ISMS

Co vše je auditem ISMS:

- Systémový audit auditorem
- Test BCP, IRP a DRP
- Penetrační test
- Test technických zranitelností
- a každá další kontrolní činnost

Co je cílem:

- Odhalit nedostatky a slabá místa
- Ověřit funkčnost bezpečnostních mechanismů a procesů

Kdo netestuje, ten neví, kudy pronikne útočník.

KROK 10:
**BUDUJTE KULTURU
KYBERNETICKÉ
BEZPEČNOSTI.**

Bezpečnostní kultura

Vedte příkladem, nestrašte trestem!

- Bezpečnostní školení
- Mail-learning kampaň
- Plakáty
- Videá a workshopy



Zůstaňme v kontaktu.



Radim Trávníček

+420731209891

info@besecured.online



Propojme se na
LinkedInu



www.besecured.online