Představení Průvodce řízení aktiv a rizik podle vyhlášky o kybernetické bezpečnosti

Ing. Hana Kroupová a Ing. Jan Hraňo

Národní úřad pro kybernetickou a informační bezpečnost

a Ministerstvo vnitra

NÚKIB

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Program

- Projekt Řízen rizik v oblasti kybernetické bezpečnosti.
  - Představení projektu, jehož výsledkem je Průvodce.
  - Členové projektu a jeho cíle.
  - Fiktivní modelová organizace.
- Průvodce řízení aktiv a rizik podle vyhlášky o kybernetické bezpečnosti.
  - Kde Průvodce naleznete?
  - Co Průvodce a jeho přílohy obsahují?
  - Proces řízení aktiv a rizik podle Průvodce.
  - Výhody a nevýhody popsané metody v Průvodci.
  - Kdy je nutné provádět hodnocení rizik?

Projekt Řízení rizik v oblasti kybernetické bezpečnosti

- Průvodce je výsledkem projektu Řízení rizik v oblasti kybernetické bezpečnosti.
- Projekt byl zaměřen na problematiku řízení aktiv a rizik.
- První myšlenky o projektu byly již v roce 2019. Společně s NÚKIB jsme se shodli, že problematika řízení aktiv a rizik není dostatečně popsána, chybí názorné a odzkoušené postupy a vzory.
- Projekt byl oficiálně spuštěn v roce 2020 a ukončen v Q2 2022.
- Projekt se zabýval problematikou řízení aktiv a rizik opravdu komplexně a vyjadřovala se k němu řada organizací, proto nemohl být hotov za pár dní. Vždy bylo nutné najít shodu a co nejvhodnější řešení.
- Projekt byl také zakomponován jako jeden z úkolů v Akčním plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025.

Kód	Úkol	Gestor	Spolupracující	Časový rámec
44.	Porovnat vybrané v současnosti užívané metody analýzy rizik s cílem ověřit, zda jsou v souladu s požadavky VKB a zda jsou současně efektivně použitelné pro různé organizace. Výstup tohoto projektu bude v obecné rovině nabídnut orgánům a osobám povinným dle ZKB i široké veřejnosti.	NÚKIB	MV	Q2 2022

Členové projektu

Hlavní cíl projektu

- Vytvoření a zveřejnění podpůrného materiálu, vzorů a metodiky na základě výběru toho nejlepšího z metodik využívaných MV, NÚKIB a dalších organizací zapojených do projektu.

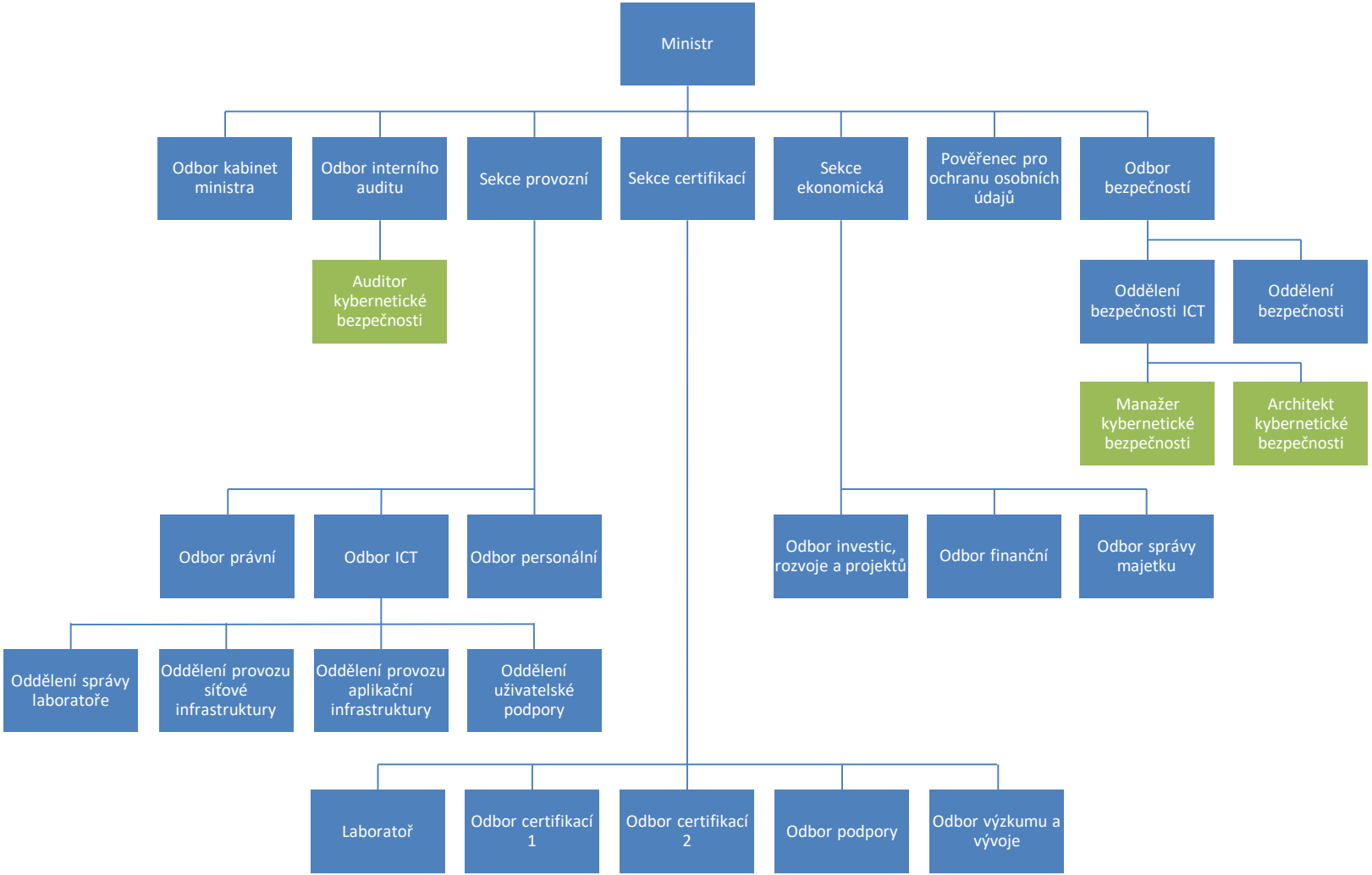
Dílčí cíl projektu

- Ověření funkčnosti navrženého způsobu provádění hodnocení rizik dle vytvořených materiálů na určených reálných systémech.

Fiktivní modelová organizace

- Přestože byly postupy ověřovány na reálných systémech, data z reálných systémů se v podpůrných materiálech samozřejmě objevit nemohla.
- Pro zachování názornosti byla v rámci projektu vytvořena fiktivní modelová organizace – **Ministerstvo pro certifikaci senzorů**.
- Toto fiktivní ministerstvo provádí kontrolu zařízení a v případě splnění podmínek uděluje certifikaci. Ministerstvo je jediným orgánem provádějící tuto certifikaci na území státu a subjekty spadající pod Ministerstvo certifikací mají povinnost používat certifikovaná zařízení.
- Ministerstvo využívá **fiktivní systémy,** nejvýznamnější je systém pro evidenci a zpracování procesu certifikace senzorů (agendový systém), který je informačním systémem kritické informační infrastruktury.
- Mimo jiné bylo nutné pro tuto fiktivní organizaci vymyslet **náplň činnosti, počet uživatelů, proces provádění certifikace, organizační strukturu, rozdělení odpovědností v rámci zajišťování kybernetické bezpečnosti této organizace a mnoho dalšího**.

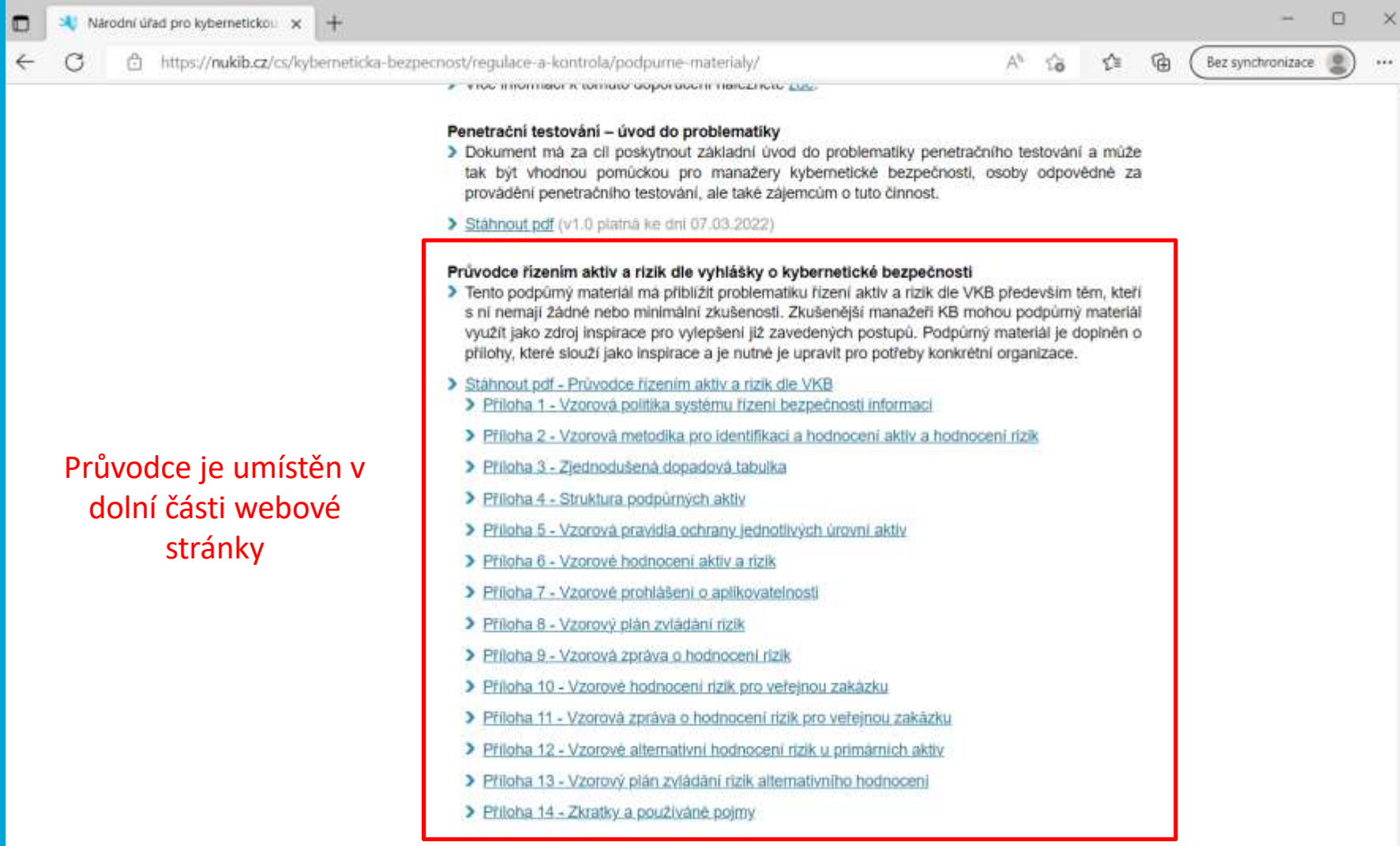
Fiktivní modelová organizace



Průvodce řízení aktiv a rizik podle vyhlášky o KB

Kde průvodce naleznete?

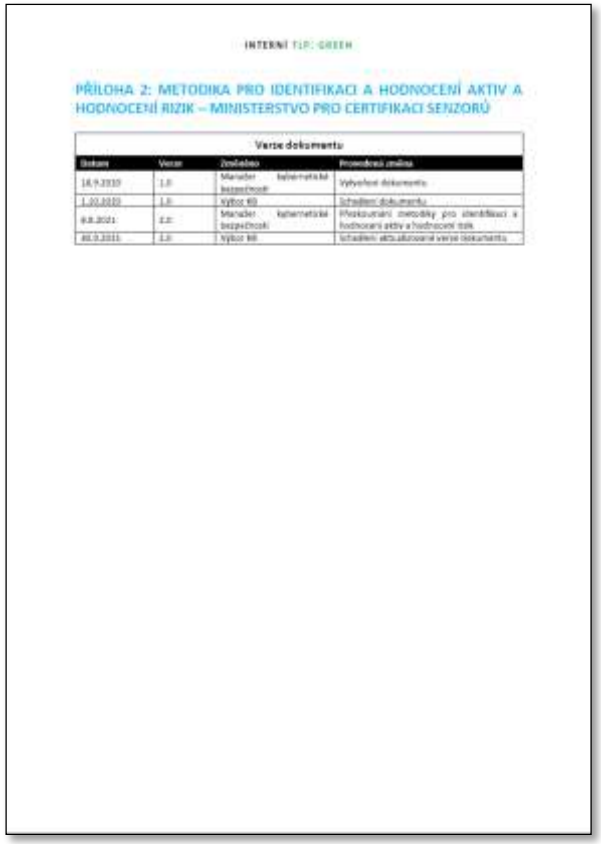
Průvodce je umístěn v dolní části webové stránky



Co Průvodce a jeho přílohy obsahují?

- Úvod.
- Kybernetická bezpečnost.
- Kontext organizace.
- Řízení aktiv v oblasti kybernetické bezpečnosti.
- Řízení rizik v oblasti kybernetické bezpečnosti.
- Kontinuální zlepšování.
- Opatření podle § 11 ZKB.
- Q&A.

- 14 příloh k samotnému Průvodci:
  - Politika systému řízení bezpečnosti informací.
  - Metodika pro identifikaci a hodnocení aktiv a hodnocení rizik.
  - Dopadová tabulka.
  - Struktura podpůrných aktiv.
  - Pravidla ochrany jednotlivých úrovní aktiv.
  - Hodnocení aktiv a rizik.
  - Prohlášení o aplikovatelnosti.
  - Plán zvládání rizik.
  - Zpráva o hodnocení rizik.
  - Hodnocení rizik pro veřejnou zakázku.
    - Zpráva o hodnocení rizik pro veřejnou zakázku.
  - Alternativní hodnocení rizik u primárních aktiv.
    - Plán zvládání rizik alternativního hodnocení.
  - Zkratky a používané pojmy.

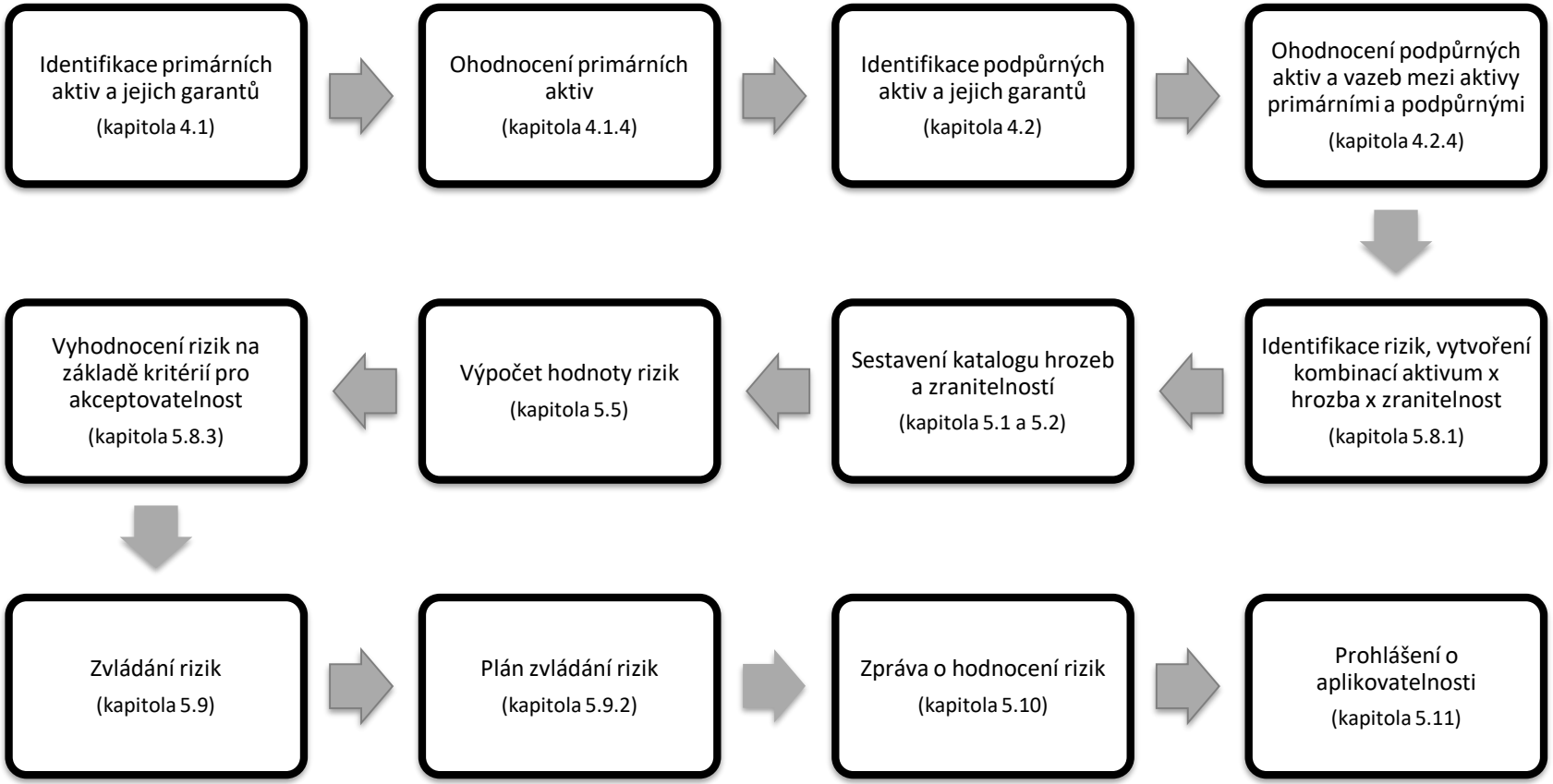

INTERNÍ TLP: GREEN

PŘÍLOHA 2: METODIKA PRO IDENTIFIKACI A HODNOCENÍ AKTIV A HODNOCENÍ RIZIK – MINISTERSTVO PRO CERTIFIKACI SENZORŮ

Verze dokumentu

Datum	Verze	Zpracoval(a)	Provedená změna
18.9.2020	1.0	Manažer kybernetické bezpečnosti	Vytvoření dokumentu
1.10.2020	1.0	Výbor KB	Schválení dokumentu
9.8.2021	2.0	Manažer kybernetické bezpečnosti	Provedení metodiky pro identifikaci a hodnocení aktiv a hodnocení rizik
30.9.2021	2.0	Výbor KB	Schválení aktualizované verze dokumentu

Proces řízení aktiv a rizik podle Průvodce



Výhody

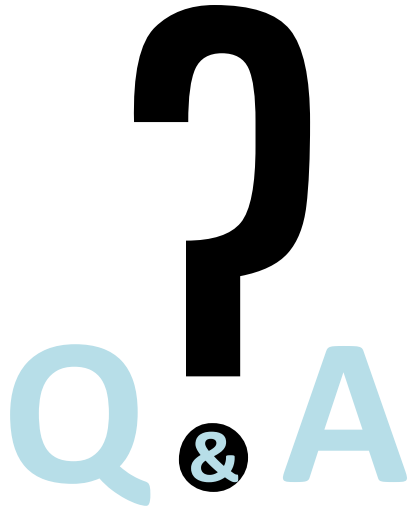
1. Univerzální metodika.
2. Nižší náklady při použití nástroje MS Excel pro provedení hodnocení rizik u malých organizací.
3. Soulad se ZKB a VKB.
4. Komplexnost.
5. Srozumitelnost a přehlednost.

Nevýhody

1. Nutnost upravit si dle požadavků organizace.
2. Vyšší náročnost při použití nástroje MS Excel pro provedení hodnocení rizik u větších organizací.
3. Časová náročnost provedení procesu a seznámení se s metodou.

Kdy je nutné provádět hodnocení rizik?

- Hodnocení rizik je nutné provádět:
  - V rámci § 3, § 4 a § 5 VKB:
    - KII a PZS **alespoň 1x ročně.**
    - VIS alespoň **1x za 3 roky.**
  - U významných změn dle § 11.
  - V souvislosti s plánovanou akvizicí, vývojem a údržbou dle § 13.
  - V rámci řízení dodavatelů dle § 8:
    - Řízení rizik spojených s dodavateli, významnými dodavateli a provozovateli.
    - U výběrového řízení a před uzavřením smlouvy povinná osoba provádí hodnocení rizik související s plněním předmětu výběrového řízení.


Q & A

NÚKIB

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Děkujeme za pozornost a Váš čas.

Ing. Hana Kroupová a Ing. Jan Hraňo

Národní úřad pro kybernetickou a informační bezpečnost
a Ministerstvo vnitra