Financováno Evropskou unií
NextGenerationEU
NÁRODNÍ PLÁN OBNOVY
DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

podpůrný materiál 4.2-6

# Příklady využití Katalogu hrozeb a rizik správy dat

(Simulace práce s katalogem – ukázky využití katalogu rizik).

verze 1.0

vytvořeno v rámci projektu

*Zajištění podmínek pro kvalitní správu datového fondu a zajištění řízeného přístupu k datům*

*Reg.č.: CZ.31.1.01/MV/23_62/000006*

# Obsah

# 1 Úvodem – kategorie rizik správy dat a jejich chování v praxi

*(Jedná se pouze o úvodní praktickou pomůcku, jak se v rizicích neztratit).*

## 1.1 Rizika, která „náhle eskalují“

Jak se projevují?

- Dlouho vypadají jako drobný problém, najednou vznikne právní spor, auditní nález, tlak zvenčí.

Typická otázka vedení:

***„Jak je možné, že se tohle stalo?“***

Jak s katalogem pracovat:

- začněte konkrétním problémem, použijte vyhledávání, sledujte, jaké má riziko dopady.

Co je důležité:

- tato rizika často zasahují vedení, někdy mají dopad i na kybernetickou bezpečnost, i když nejsou technická.

---

## 1.2 Rizika, která „pomalu rozežírají organizaci“

Jak se projevují?

- Postupně klesá kvalita dat, rostou náklady, spolupráce je složitější, nikdo neřekne „tohle je ten problém“.

Typická věta:

***„My to tak děláme už roky.“***

Jak s katalogem pracovat:

- použijte systematický přehled (top-down), dívejte se po absenci pravidel, nestandardních postupech, nekonzistenci.

Co je důležité:

- tato rizika nevytvářejí incident, ale dlouhodobě brzdí rozvoj a digitalizaci.

---

## 1.3 Rizika, která se projeví incidentem

Jak se projevují?

- Dojde ke konkrétní chybě nebo selhání, data nejsou dostupná, správná nebo aktuální.

Typická otázka:

***„Kde se to vzalo a proč se to stalo?“***

Jak s katalogem pracovat:

- začněte incidentem, katalog použijte k vysvětlení příčin, pochopení souvislostí, identifikaci skutečného rizika.

Co je důležité:

- katalog nenahrazuje řešení incidentu, pomáhá pochopit, co bylo špatně systémově.

---

## 1.4 Rizika, která souvisí s lidmi a kulturou

Jak se projevují?

- Pravidla existují, ale nedodržují se, odpovědnost za data je nejasná, „nějak se to udělá“.

Typická věta:

***„Tohle nikdo nemá na starosti.“***

Jak s katalogem pracovat

- pouze systematicky a shora, porovnávat, jak by to mělo fungovat a jak to funguje ve skutečnosti.

Co je důležité

- tato rizika jsou nejméně viditelná, ale často velmi nebezpečná.

---

## 1.5 Jak tuto pomůcku používat

- Nepřemýšlejte, *do jaké kategorie riziko patří*.
- Ptejte se:
    - Jak se problém projevuje?
    - Je náhlý, nebo dlouhodobý?
    - Má incident, nebo se „rozpouští v provozu“?

Podle toho:

- zvolte správný způsob práce s katalogem, a vyhnete se chybným očekáváním.

**Shrnutí jednou větou:**

Katalog rizik správy dat pomáhá pochopit problémy – tato kapitola pomáhá pochopit, jak se tyto problémy v praxi chovají.

# 2 Příklad 1 - Řešení konkrétního problému / incidentu

*Modelový příklad scénáře 2 uvedeného v „Metodice řízení rizik správy dat“ založený na záznamu ID225 katalogu*.

## 2.1 Výchozí situace (impuls k použití katalogu)

Organizace veřejné správy řeší konkrétní problém:

- Došlo k (právnímu) sporu s jinou organizací ohledně sdílení dat. Spor vznikl v souvislosti s rozdílným výkladem legislativních požadavků a vedl k omezení výměny dat mezi agendami.

Vedení organizace požaduje:

- vysvětlení příčin problému,
- posouzení závažnosti vzniklého rizika,
- stanovení priority dalšího řešení.

Datový / bezpečnostní analytik proto otevírá Excel katalog rizik správy dat.

---

## 2.2 Vstupní bod: hledání kontextu problému

Cílem uživatele není najít konkrétní ID, ale porozumět kontextu, ve kterém se problém objevil.

Katalog umožňuje více rovnocenných vstupních cest; uživatel volí tu, která odpovídá míře znalosti problému:

- protože problém není popsán jednou přesnou formulací,
- ale je znám pouze obecně („právní spor“, „nejistota ohledně sdílení dat“),

➡️ uživatel začíná fulltextovým vyhledáváním (např. výrazy „legislativa“, „sdílení dat“, „právní“).

Následně:

- zpřesňuje výběr pomocí filtrů (oblast správy dat, téma, kritický faktor),
- a identifikuje záznamy:
  - ID 221 - Nedostatečná koordinace mezi úřady při sdílení dat.
  - ID 225 - Nejasnosti v legislativních požadavcích na sdílení dat.
  - ID 228 - Rezistence vůči sdílení dat mezi agendami.

Záznam ID 225 odpovídá popisu řešené situace Tím je nalezen relevantní kontext, nikoli náhodný řádek.

---

## 2.3 Základní kontext záznamu ID225

Uživatel čte levý kontext řádku:

- Oblast správy dat: Realizace datových řešení.
- Téma: Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady).
- Kategorie faktoru: Právní a regulatorní faktor.

- Kritický faktor: Nejasnosti v legislativních požadavcích na sdílení dat.

Již v této fázi je zřejmé, že:

- nejde o technický problém,
- ale o řízení právního významu dat a odpovědnosti za výklad.

---

## 2.4 Analýza kritického faktoru (detailní × typový pohled)

**Detailní úroveň**

- Kritický faktor popisuje konkrétní problém organizace:
  - Nejasnosti v legislativních požadavcích na sdílení dat.

**Typová úroveň (referenční rámec)**

Záznam je přiřazen k:

- TKF8.2 – Soulad s právními předpisy
- TKF1.4 – Jasná odpovědnost za rozhodování

Typové kritické faktory zde nenahrazují analýzu, ale potvrzují, že:

- jde o opakující se systémový vzorec,
- typicky řešitelný pouze jasným rozhodováním a výkladem.

➡️ Analýza je vedena na detailním prvku, typový prvek slouží k orientaci.

---

## 2.5 Kauzální řetězec: příčina → zranitelnost → hrozba

**Příčina**

- **detailní prvek**
  - Legislativa neobsahuje dostatečně konkrétní pokyny pro sdílení dat mezi organizacemi.
- **typový prvek**
  - PR12 – Nedostatečné legislativní ukotvení a aplikační praxe

**Zranitelnost**

- **detailní prvek**
  - Nejasné legislativní rámce vedou k různým výkladům a nesprávným implementacím procesů.
- **typový prvek**
  - ZR7 – Nezohlednění legislativních požadavků v procesech správy dat

**Hrozba (detailní prvek)**

- **detailní prvek**
  - Organizace nejsou schopny plně dodržovat právní předpisy, což zvyšuje riziko pokut a sankcí.
- **typový prvek**

- HR7 – Rizika z neefektivní správy vztahů s dodavateli.
- HR16 – Ztráta důvěry a reputační rizika.

➡️ Kauzální řetězec jasně ukazuje, že:

- riziko se realizuje manažersko-právním selháním, nikoli útokem.

---

## 2.6 Riziko – syntéza kauzálního řetězce

- **detailní prvek**
  - Nesprávná interpretace legislativy vede k právním nesouladům a omezením sdílení dat.
- **typový prvek**
  - RI2 – Nesoulad s legislativními a metodickými požadavky.
  - RI21 – Riziko právních a finančních dopadů.

➡️ Riziko je:

- srozumitelně pojmenováno,
- komunikovatelné vedení,
- a přímo navázané na reálný problém.

---

## 2.7 Dopady: primární a sekundární

- **detailní prvek**
  - Pokuty, právní spory a poškození reputace organizace.
- **typový prvek**
  - Primární dopad: TD6 – Právní a regulační důsledky.
  - Sekundární dopad: TD5 – Reputační škody.

➡️ Podle metodiky:

- hodnocení a prioritizace se provádí výhradně na základě primárního dopadu,
- sekundární dopady poskytují kontext, ale nejsou samostatně hodnoceny.

---

## 2.8 Stanovení priority rizika (ilustrační „výpočet“)

Uživatel přechází k „Návodu pro prioritizaci rizik správy dat“ a provádí hodnocení.

**Ilustrační hodnocení:**

- primární dopad TD6,
  - právní spor, potenciální sankce,
  - zásah do zákonných povinností organizace.
- Dle pětiúrovňové škály (v souladu s Metodikou a návodem Hodnocení rizik správy dat) vychází:
  - ➡️ Výsledná priorita rizika: vysoká

Podpůrné otázky uvedené v „Příloze – hodnotící otázky dopadů“ k hodnocení dopadu „TD6:

- K1 – Rozsah dopadu
  - Týká se dopad více povinností nebo více zákonů?
  - Zasahuje dopad do více procesů s právními závazky?
- K2 – Intenzita dopadu
  - Může dojít k nesplnění právních povinností?
  - Hrozí opakované právní nedostatky (audit, kontrola)?
- K3 – Náklady/úsilí na nápravu
  - Vyžaduje náprava právní analýzu nebo přepracování dokumentace?
  - Vznikají náklady z nesouladu (pokuty, nápravná opatření)?
- K4 – Reputační / právní / strategický dopad
  - Hrozí přímý právní postih?
  - Může dojít k pozastavení projektu/služby kvůli právnímu riziku?

***Poznámka**:* Jedná se o ukázkový výpočet dle publikované metodiky. Organizace může použít vlastní způsob hodnocení.

---

## 2.9 Vazba na kybernetickou bezpečnost

Záznam ID225 v Katalogu uvádí:

- Žádnou typovou zranitelnost NÚKIB (legislativní neurčitost není kybernetická zranitelnost).
- Hrozbu NÚKIB H1 odvozenou:
  - z detailní hrozby správy dat: Organizace nejsou schopny plně dodržovat právní předpisy, což zvyšuje riziko pokut a sankcí.
  - z detailního dopadu správy dat: Pokuty, právní spory a poškození reputace organizace.
- Hrozba NÚKIB: H1 – Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů.

➡️ Kybernetická bezpečnost se zde aktivuje na úrovni hrozby a dopadu, ne na úrovni zranitelnosti správy dat.

---

## 2.10 Incident, následek a opatření (případná návazná reflexe)

**Incident**

- Nedodržení legislativy vedlo k (právnímu) sporu s jinou organizací o sdílení dat.

**Následek**

- Zvýšené náklady na právní služby a ztráta důvěry v procesy sdílení dat.

**Preventivní opatření**

- Zajistit konzultace s právními odborníky a vytvořit jasné metodiky pro dodržování legislativy.

**Reaktivní opatření**

- Provést revizi procesů a implementovat nápravná opatření na základě zjištěných nedostatků.

➡️ Tyto prvky:

- nejsou vstupem do analýzy rizika,
- ale dokládají situaci, kdy se riziko již realizovalo,
- a ukazují, jak na něj organizace může reagovat.

---

## 2.11 Závěrečná metodická reflexe

Tato simulace ukazuje, že:

- katalog nevytváří rizika,
- ale strukturuje porozumění reálnému problému,
- umožňuje dohledatelnost, auditovatelnost a opakovatelnost práce.

Katalog:

- nekonkuruje řízení kybernetické bezpečnosti,
- ale vytváří most mezi správou dat, právem a bezpečností.

**Shrnutí jednou větou:**

Katalog rizik správy dat pomáhá pochopit, proč problém vznikl, jak závažný je a kam patří – nikoli rozhodnout za organizaci.

---

# 3 Příklad 2 - Systematický (top-down) přístup

*Modelový příklad scénáře 1 uvedeného v „Metodice řízení rizik správy dat“ založený na záznamu ID225 katalogu.*

## 3.1 Výchozí situace (odlišná od bottom-up)

Role uživatele:
Vlastník / věcný správce dat / garant správy dat / auditor.

**Impuls k použití katalogu:**
Neexistuje konkrétní incident. Organizace:

- provádí systematický přezkum rizik správy dat souvisejících se sdílením dat,
- nebo se připravuje na:
  - audit,
  - významnou změnu,
  - zavádění správy dat.

Cílem není řešit jeden problém, ale získat přehled o rizicích v určité oblasti správy dat.

---

## 3.2 Vstupní bod: typový prvek jako navigace (top-down logika)

Uživatel vědomě nezačíná konkrétním rizikem, ale:

- oblastí a tématem správy dat,
- typovým kritickým faktorem,
- případně typovým rizikem.

V tomto scénáři zvolí vstup přes:

- oblast správy dat: Realizace datových řešení
- téma: Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady)

➡️ Jde o vědomou analytickou volbu:
„Chci vědět, jaká rizika jsou typická pro tuto oblast.“

---

Výsledek výběru je uveden na další stránce.

| ID | Oblast správy dat | Téma | Kategorie faktoru | Kritický faktor | TKF SD (P,S) | Typový kritický faktor SD (P, S) |
|---|---|---|---|---|---|---|
| 210 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 1. Organizační faktor | Nedostatečná koordinace mezi organizačními útvary | TKF2.2, TKF9.3 | Koordinace útvarů a projektů. Podpora spolupráce |
| 211 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 1. Organizační faktor | Nedostatečná koordinace mezi úřady při sdílení dat | TKF2.2, TKF9.3 | Koordinace mezi organizačními útvary a projekty. Podpora otevřenosti, spolupráce a inovací |
| 212 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 1. Organizační faktor | Nedostatečná podpora vedení pro rozvoj datové integrace | TKF1.1, TKF5.3 | Aktivní podpora a angažovanost vedení. Interoperabilita a propojitelnost |
| 213 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 1. Organizační faktor | Nejasné odpovědnosti za správu datové integrace | TKF2.1, TKF1.4 | Vymezené datové role a odpovědnosti. Jasná odpovědnost za |
| 214 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 1. Organizační faktor | Nejasné vedení při správě otevřených dat | TKF1.4, TKF1.1 | Jasná odpovědnost za rozhodování. Aktivní podpora vedení |
| 215 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 2. Procesní faktor | Chybějící standardizace procesů datové integrace | TKF3.1, TKF5.3 | Standardizované a zdokumentované procesy. Interoperabilita |
| 216 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 2. Procesní faktor | Neefektivní procesy pro evidenci údajů v RPP | TKF3.1, TKF7.2 | Standardizované procesy správy dat. Řízení životního cyklu dat |
| 217 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 2. Procesní faktor | Nejednotné technické specifikace sdílených dat | TKF5.2, TKF5.3 | Používání jednotných datových standardů. Interoperabilita |
| 218 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 2. Procesní faktor | Slabá integrace mezi agendami jedné organizace | TKF5.3, TKF6.2 | Interoperabilita a propojitelnost systémů. Technologická kompatibilita |
| 219 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 3. Technický faktor | Nedostatečné napojení systémů na PPDF | TKF5.3, TKF6.1 | Interoperabilita a propojitelnost systémů. Nástroje pro správu dat |
| 220 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 3. Technický faktor | Nedostatek nástrojů pro interní integraci | TKF6.1, TKF6.2 | Dostupnost a funkčnost nástrojů. Technologická kompatibilita |
| 221 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 3. Technický faktor | Nekompatibilita agendových systémů s PPDF a VDF | TKF6.2, TKF5.3 | Technologická kompatibilita. Interoperabilita |
| 222 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 3. Technický faktor | Nízká kvalita technické podpory pro integraci dat | TKF6.1, TKF4.2 | Nástroje pro správu dat. Personální kapacity |
| 223 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 3. Technický faktor | Technologická zastaralost agendových systémů | TKF6.3, TKF6.2 | Pravidelná údržba a modernizace infrastruktury. Technologická kompatibilita |
| 224 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 4. Právní a regulatorní faktor | Nedostatečná ochrana osobních údajů při datové integraci | TKF8.1, TKF8.2 | Integrita, důvěrnost a dostupnost dat. Soulad s právními předpisy |
| 225 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 4. Právní a regulatorní faktor | Nejasnosti v legislativních požadavcích na sdílení dat | TKF8.2, TKF1.4 | Soulad s právními předpisy. Jasná odpovědnost za rozhodování |
| 226 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 5. Kulturní faktor | Nízké povědomí o významu integrace dat | TKF9.1, TKF9.3 | Datová kultura a povědomí. Podpora spolupráce |
| 227 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 5. Kulturní faktor | Podcenění využití otevřených dat | TKF9.1, TKF1.1 | Datová kultura. Aktivní podpora vedení |
| 228 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 5. Kulturní faktor | Rezistence vůči sdílení dat mezi agendami | TKF9.3, TKF2.2 | Podpora otevřenosti, spolupráce a inovací. Koordinace útvarů |
| 229 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 6. Bezpečnostní faktor | Riziko ztráty integrity dat během integrace | TKF8.1, TKF5.3 | Integrita, důvěrnost a dostupnost dat. Interoperabilita |
| 230 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 7. Ekonomický faktor | Omezené zdroje na školení a technickou podporu | TKF4.2, TKF4.1 | Personální a odborné kapacity. Finanční zajištění |
| 231 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 7. Ekonomický faktor | Vysoké náklady na modernizaci a integraci | TKF4.3, TKF6.3 | Efektivní alokace zdrojů. Modernizace infrastruktury |

Výsledek obsahuje rizika související se sdílením dat ve všech kategoriích kritických faktorů, zajímá ho ale především právní a regulatorní stránka sdílení dat, proto pro práci zúží výběr další filtrací dle kategorie faktoru na: „Právní a regulatorní faktor“.

| ID | Oblast správy dat | Téma | Kategorie faktoru | Kritický faktor | TKF SD (P,S) | Typový kritický faktor SD (P, S) |
|---|---|---|---|---|---|---|
| 224 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 4. Právní a regulatorní faktor | Nedostatečná ochrana osobních údajů při datové integraci | TKF8.1, TKF8.2 | Integrita, důvěrnost a dostupnost dat. Soulad s právními předpisy |
| 225 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 4. Právní a regulatorní faktor | Nejasnosti v legislativních požadavcích na sdílení dat | TKF8.2, TKF1.4 | Soulad s právními předpisy. Jasná odpovědnost za rozhodování |

## 3.3 Práce s typovými prvky (orientační fáze)

Ke stejnému výsledku je možné dojít využitím typových kritických faktorů.

Uživatel se nejprve podívá na typové kritické faktory na listu „Typové kritické faktory (SD)“ a vybere ty, které nejvíce odpovídají řešenému problému, např.:

- TKF8.2 – Soulad s právními předpisy
- TKF1.4 – Jasná odpovědnost za rozhodování

Typové prvky zde plní roli:

- mapy terénu,
- nikoli popisu reality konkrétní organizace.

➡️ V tuto chvíli:

- se neprovádí analýza rizika,
- pouze se vymezuje relevantní oblast.

---

## 3.4 Přechod z typového na detailní (klíčový moment top-down)

Uživatel nyní:

- filtruje hlavní pracovní list podle:
  - zvolených typových kritických faktorů,
  - oblasti a tématu.

Tím získá konkrétní detailní záznamy, které:

- typový vzorec naplňují,
- popisují reálné situace.

| ID | Oblast správy dat | Téma | Kategorie faktoru | Kritický faktor | TKF SD (P,S) | Typový kritický faktor SD (P, S) |
|---|---|---|---|---|---|---|
| 224 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 4. Právní a regulatorní faktor | Nedostatečná ochrana osobních údajů při datové integraci | TKF8.1, TKF8.2 | Integrita, důvěrnost a dostupnost dat. Soulad s právními předpisy |
| 225 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 4. Právní a regulatorní faktor | Nejasnosti v legislativních požadavcích na sdílení dat | TKF8.2, TKF1.4 | Soulad s právními předpisy. Jasná odpovědnost za rozhodování |

Nalezne:

- ID224 s kritickým faktorem: „Nedostatečná ochrana osobních údajů při datové integraci“.
- ID225 s kritickým faktorem: „Nejasnosti v legislativních požadavcích na sdílení dat“.

Mezi nimi identifikuje řádek ID225.

➡️ Tady dochází k přechodu z typového na detailní pohled.
Od tohoto okamžiku se analýza vede výhradně na detailních prvcích.

---

## 3.5 Analýza detailního záznamu ID225

Uživatel nyní postupuje stejně metodicky jako v bottom-up scénáři, ale s jiným kontextem:

**Kritický faktor:**

- Nejasnosti v legislativních požadavcích na sdílení dat

**Příčina:**

- Legislativa neobsahuje dostatečně konkrétní pokyny pro sdílení dat mezi organizacemi.

**Zranitelnost:**

- Nejasné legislativní rámce vedou k různým výkladům a nesprávným implementacím procesů.

**Hrozby:**

- Organizace nejsou schopny plně dodržovat právní předpisy, což zvyšuje riziko pokut a sankcí (HR7, HR16 – reputační a vztahová rizika).

**Riziko:**

- Nesprávná interpretace legislativy vede k právním nesouladům a omezením sdílení dat.

➡️ Rozdíl proti bottom-up:

- problém není impulsem,
- ale výsledkem systematického mapování.

---

## 3.6 Dopady a prioritizace

Stejně jako dříve:

- Primární dopad: TD6 – právní / regulatorní
- Sekundární dopad: TD5 – reputační

Uživatel:

- provede hodnocení dopadu TD6 dle návodu,
- stanoví prioritu rizika.

Důležité metodické sdělení:

I v top-down přístupu se priorita stanovuje na základě konkrétního detailního rizika, nikoli typového.

---

## 3.7 Vazba na kybernetickou bezpečnost (systematický pohled)

Uživatel si všímá, že:

- neexistuje typová zranitelnost NÚKIB,
- ale existuje typová hrozba NÚKIB H1 odvozená z hrozeb i dopadu.

V top-down režimu to znamená systémové upozornění, že určitý typ právních rizik správy dat může mít bezpečnostní implikace, i když nejde o kybernetickou slabinu.

➡️ To je důležité pro:

- koordinaci s KB,
- nikoli pro eskalaci každého jednotlivého případu.

---

## 3.8 Incident, následek a opatření v top-down scénáři

V tomto scénáři mají jinou roli než u bottom-up:

- incident slouží jako:
  - důkaz, že riziko není teoretické,
- opatření ukazují:
  - jaké typy reakcí organizace obvykle volí.

Nejsou:

- vstupem do analýzy,
- ani spouštěčem hodnocení.

---

## 3.9 Výstup top-down práce s katalogem

Uživatel získává:

- přehled, že v oblasti datové integrace existují právní rizika vysoké priority,
- identifikaci konkrétních rizik (např. ID225),
- podklad pro:
  - plánování,
  - řízení změn,
  - auditní závěry.

Bez nutnosti:

- řešit incident,
- okamžitě navrhovat opatření.

---

## 3.10 Závěrečná metodická reflexe (top-down)

Top-down přístup:

- začíná typovým pohledem,
- ale končí vždy u detailního rizika.

Katalog zde slouží jako:

- navigační nástroj,
- prostředek pro systematické pokrytí oblasti,
- nikoli jen reakční databáze incidentů.

---

## 3.11 Stručné srovnání bottom-up vs. top-down

| Aspekt | Bottom-up | Top-down |
|---|---|---|
| **Impuls** | Konkrétní problém / incident | Systematický přezkum |
| **Vstup** | Fulltext / symptomy | Typové prvky |
| **Role typových prvků** | Referenční | Navigační |
| **Přechod k detailu** | Okamžitý | Po vymezení oblasti |
| **Typický výstup** | Řešení konkrétního rizika | Přehled a priorizace |

**Shrnutí jednou větou**

Top-down přístup používá katalog k systematickému mapování rizik, bottom-up k pochopení konkrétního problému – oba se však vždy setkávají u detailního rizika.

# 4 Příklad 3 - Systematický (top-down) přístup

*Modelový příklad scénáře 1 uvedeném v „Metodice řízení rizik správy dat“ založený na záznamu ID33 katalogu.*

## 4.1 Výchozí situace (impuls k analýze)

Role uživatele:
Garant správy dat / datový architekt / interní auditor.

Impuls:
Organizace provádí systematický přezkum správy dat v rámci:

- zavádění správy dat,
- auditu,
- nebo přípravy na významnou změnu (digitalizace, sdílení dat).

Neexistuje konkrétní incident, ale objevují se opakované problémy s kvalitou dat, interoperabilitou a efektivitou.

Cílem je:

- identifikovat strukturální rizika,
- a stanovit jejich prioritu.

---

## 4.2 Vstupní bod: hledání kontextu (top-down)

Uživatel:

- začíná fulltextovým vyhledáním výrazu „kvalita“ v oblasti rizik,
- čímž získá širší množinu záznamů.
    - fulltextové vyhledání výrazu „kvalita“ lze samozřejmě využít i v dalších prvcích kauzálního řetězce,
    - pro srovnáni v případě vyhledávání v hrozbách je počet nalezených záznamů 73, v případě rizik 93, v případě dopadů 61,
    - volba výběru vyhledávání záleží na uživateli.

Pro zpřesnění:

- filtruje kategorii faktoru pomocí „Procesní faktor“,
- výběr se zúží na 16 řádků.

| ID | Oblast správy dat | Téma | Kategorie faktoru | Kritický faktor | TKF SD (P,S) | Typový kritický faktor SD (P, S) |
|---|---|---|---|---|---|---|
| 3 | 0. ŘÍZENÍ A ORGANIZACE SPRÁVY DAT | Organizace (role, jejich odpovědnosti a pravomoci v oblasti dat) | 2. Procesní faktor | Chybějící interní pravidla upravující správu dat, včetně jasné definice rolí a odpovědností za jednotlivé procesy | TKF3.1, TKF3.2 | Standardizované a zdokumentované procesy správy dat.<br>Používání jednotných metodik, šablon a nástrojů |
| 33 | 0. ŘÍZENÍ A ORGANIZACE SPRÁVY DAT | Standardizace (zakotvení rolí, odpovědností, procesů a pravidel pro práci s daty v řídících dokumentech úřadu) | 2. Procesní faktor | Neexistence publikovaných standardů pro správu dat ve veřejné správě | TKF5.2, | Používání jednotných datových standardů. |
| 72 | 1. STANOVENÍ DATOVÝCH POTŘEB | Řízení datových potřeb (identifikace a řízení požadavků na data / datové výstupy) | 2. Procesní faktor | Nedostatečná koordinace mezi odděleními | TKF2.2, TKF2.3 | Koordinace mezi útvary a projekty.<br>Centralizovaná koordinace |
| 130 | 2. POPIS DAT A DATOVÝCH ŘEŠENÍ | Evidence v RPP (evidence agendových údajů v Registru práv a povinností) | 2. Procesní faktor | Formální a nesystematický přístup k evidenci dat v RPP | TKF3.1, TKF11.2 | Standardizované procesy správy dat.<br>Kontrola a audit souladu |
| 146 | 2. POPIS DAT A DATOVÝCH ŘEŠENÍ | Kategorizace dat (používané kategorie dat, číselníky a jejich správa, sdílení dat napříč agendami) | 2. Procesní faktor | Chybějící standardizace procesů pro správu kategorií dat | TKF3.1, TKF5.2 | Standardizované procesy správy dat.<br>Jednotné datové standardy |
| 148 | 2. POPIS DAT A DATOVÝCH ŘEŠENÍ | Kategorizace dat (používané kategorie dat, číselníky a jejich správa, sdílení dat napříč agendami) | 2. Procesní faktor | Neefektivní koordinace mezi agendami při sdílení kategorií dat | TKF2.2, TKF9.3 | Koordinace útvarů a projektů.<br>Podpora spolupráce a inovací |
| 149 | 2. POPIS DAT A DATOVÝCH ŘEŠENÍ | Kategorizace dat (používané kategorie dat, číselníky a jejich správa, sdílení dat napříč agendami) | 2. Procesní faktor | Neefektivní validace a schvalování číselníků | TKF3.1, TKF1.4 | Standardizované procesy správy dat.<br>Jasná odpovědnost za rozhodování |
| 185 | 2. POPIS DAT A DATOVÝCH ŘEŠENÍ | Modelování dat a datových řešení (modely dat, datových toků a komponent využívaných při získávání, ukládání a zpracování dat) | 2. Procesní faktor | Nedostatečné procesy pro validaci a schválení modelů | TKF3.1, TKF1.4 | Standardizované procesy.<br>Jasná rozhodovací odpovědnost |
| 215 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady) | 2. Procesní faktor | Chybějící standardizace procesů datové integrace | TKF3.1, TKF5.3 | Standardizované a zdokumentované procesy.<br>Interoperabilita |
| 235 | 3. REALIZACE DATOVÝCH ŘEŠENÍ | Datové aspekty řešených změn informačních systémů (přepoužívání existujících dat, zpřístupňování dat v rámci propojeného nebo veřejného datového fondu jako součást rozvoje IS, požadavky na dodavatele IS související s daty a jejich dokumentací) | 2. Procesní faktor | Chybějící standardizace procesů pro řízení datových změn v IS | TKF3.1, TKF3.2 | Standardizované procesy správy dat.<br>Metodiky a šablony |
| 315 | 4. ZAJIŠTĚNÍ A VYUŽÍVÁNÍ DAT | Kvalita dat (evidence a řešení problémů s nedostatečnou kvalitou dat) | 2. Procesní faktor | Absence standardních procesů pro zajištění kvality dat | TKF7.1, TKF3.1 | Rámec řízení kvality.<br>Standardizované procesy |
| 316 | 4. ZAJIŠTĚNÍ A VYUŽÍVÁNÍ DAT | Kvalita dat (evidence a řešení problémů s nedostatečnou kvalitou dat) | 2. Procesní faktor | Chybějící procesy pro pravidelnou aktualizaci dat | TKF7.2, TKF3.1 | Řízení životního cyklu dat.<br>Standardizované procesy |
| 319 | 4. ZAJIŠTĚNÍ A VYUŽÍVÁNÍ DAT | Kvalita dat (evidence a řešení problémů s nedostatečnou kvalitou dat) | 2. Procesní faktor | Slabá integrace procesů kvality dat s ostatními oblastmi správy dat | TKF7.1, TKF2.3 | Rámec řízení kvality dat.<br>Centralizovaná koordinace |
| 359 | 4. ZAJIŠTĚNÍ A VYUŽÍVÁNÍ DAT | Provoz datových úložišť a řešení (správa datových úložišť a souvisejících komponent, využívání cloudových úložišť a nástrojů, efektivní řízení dostupnosti/výkonu datových úložišť a řešení) | 2. Procesní faktor | Nedostatečné procesy pro auditování externích úložišť | TKF11.2, TKF10.2 | Pravidelná kontrola a audit souladu.<br>Kontrola poskytovatelů |
| 417 | 4. ZAJIŠTĚNÍ A VYUŽÍVÁNÍ DAT | Využití dat (podmínky a nástroje pro analýzu dat / tvorbu analytických výstupů, podpora řízeného přístupu) | 2. Procesní faktor | Chybějící standardizace procesů analýzy dat | TKF3.1, TKF3.2 | Standardizované procesy.<br>Metodiky a šablony |
| 435 | Samostatná část zaměřená na implementaci správy dat | Implementace | 2. Procesní faktor | Zajištění kontinuálního zlepšování | TKF3.3, TKF11.3 | Pravidelná revize a zlepšování.<br>Mechanismy nápravy |

➡️ Cílem tohoto kroku není najít konkrétní riziko, ale vymezit kontext: standardizace procesů správy dat.

---

## 4.3 Typové prvky jako navigace (orientační fáze)

Typový kritický faktor TKF5.2 uživateli říká:

- jde o oblast, kde:
  - bez jednotných standardů vzniká nekonzistence,
  - každá organizace řeší správu dat jinak,
  - interoperabilita je systematicky narušena.

Typový prvek zde:

- nepopisuje realitu organizace,
- ale slouží jako mapa oblasti, kterou je třeba projít.

➡️ Analýza zatím není vedena na riziku, ale na strukturálním tématu.

---

## 4.4 Přechod z typového na detailní (klíčový bod)

Uživatel nyní:

- filtruje hlavní pracovní list podle:
  - oblasti: Řízení a organizace správy dat,
  - tématu: Standardizace,

- typového kritického faktoru: TKF5.2 – Používání jednotných datových standardů.

Tím získá konkrétní detailní záznamy, které tento typový problém naplňují.

| ID | Oblast správy dat | Téma | Kategorie faktoru | Kritický faktor | TKF SD (P,S) | Typový kritický faktor SD (P, S) |
|---|---|---|---|---|---|---|
| 33 | 0. ŘÍZENÍ A ORGANIZACE SPRÁVY DAT | Standardizace (zakotvení rolí, odpovědností, procesů a pravidel pro práci s daty v řídících dokumentech úřadu) | 2. Procesní faktor | Neexistence publikovaných standardů pro správu dat ve veřejné správě | TKF5.2, | Používání jednotných datových standardů. |
| 146 | 2. POPIS DAT A DATOVÝCH ŘEŠENÍ | Kategorizace dat (používané kategorie dat, číselníky a jejich správa, sdílení dat napříč agendami) | 2. Procesní faktor | Chybějící standardizace procesů pro správu kategorií dat | TKF3.1, TKF5.2 | Standardizované procesy správy dat. Jednotné datové standardy |

Jedním z nich je řádek ID33.

Řádek ID146 se týká standardizace procesů pro správu kategorií dat, což přímo neodpovídá řešenému problémy s kvalitou dat, interoperabilitou a efektivitou, ale to neznamená, že standardizace i tohoto procesu by neměla být řešena.

➡️ Zde dochází k přechodu z typového na detailní pohled.
Od této chvíle je analýza vedena výhradně na detailním záznamu.

---

## 4.5 Analýza detailního kritického faktoru (ID33)

**Detailní úroveň**

- Neexistence publikovaných standardů pro správu dat ve veřejné správě
  - nejde o selhání jednotlivé organizace,
  - ale o systémovou absenci rámce a metodického vedení.

**Typová úroveň (referenční rámec)**

- TKF5.2 - Používání jednotných datových standardů
  - kritický faktor přímo odpovídá TKF5.2,
  - potvrzuje, že:
    - bez standardů nelze očekávat konzistenci,
    - ani koordinaci mezi organizacemi.

---

## 4.6 Kauzální řetězec: příčina → zranitelnost → hrozby

**Příčina**

- **detailní prvek**
  - Chybí jednotný rámec a metodické vedení pro vytvoření a zavedení standardů; organizace neznají osvědčené postupy.
- **typový prvek**
  - PR8 – Nedostatečná standardizace a interoperabilita.
    - Organizace nemají společný rámec, vytvářejí vlastní pravidla.

**Zranitelnost**

- **detailní prvek**
  - Bez standardů je každá organizace nucena vytvářet vlastní pravidla, což vede k nekonzistenci a obtížné spolupráci mezi úřady.
- **typový prvek**

- ZR22 – Nekonzistentní a neefektivní přístupy ke správě dat.
  - Procesy se liší, nejsou kompatibilní, nejsou přenositelné.

➡️ Zranitelnost je procesní, nikoli technická.

**Hrozba (detailní prvek)**

- **detailní prvek**
  - Nekonzistentní procesy mohou vést k chybnému sdílení dat, jejich duplicitě nebo ztrátě při přenosu odpovědností.
- **typový prvek**
  - HR5 – Slabá koordinace při zavádění správy dat.
  - HR11 – Neefektivní procesy správy a sdílení dat.
  - HR14 – Nedostatečná koordinace a spolupráce mezi útvary.

➡️ Hrozby zde nejsou využity incidenty, ale jedná se o trvalé provozní tlaky.

---

## 4.7 Riziko – syntéza kauzálního řetězce

- **detailní prvek**
  - Nízká kvalita dat, nesoulad mezi organizacemi a neefektivní správa dat způsobující ztráty v efektivitě veřejné správy.
- **typový prvek**
  - RI5 – Nedostatečná kvalita dat a výstupů.
  - RI12 – Ztráta interoperability a konzistence systémů.

Riziko je:

- dlouhodobé,
- kumulativní,
- obtížně „viditelné“ bez systematické analýzy.

---

## 4.8 Dopady a prioritizace

- **detailní prvek**
  - Zvýšené náklady, reputační škody a neschopnost efektivně poskytovat veřejné služby.
- **typový prvek**
  - Primární dopad: TD1 – finanční dopad.
  - Sekundární dopad:
    - TD5 – reputace.
    - TD2 – efektivita.

Vysvětlení v katalogu:

- zvýšené náklady,
- reputační škody,
- neschopnost efektivně poskytovat veřejné služby.

---

## 4.9 Ukázkové stanovení priority rizika

Uživatel provede ilustrační hodnocení podle „Návodu pro prioritizaci rizik správy dat“:

- primární dopad TD1 (finanční),
  - dlouhodobé a plošné náklady,
  - dopad na více organizací a agend.

➡️ Výsledná priorita rizika: střední až vysoká
(v závislosti na rozsahu a míře standardizace v organizaci).

***Poznámka**:* Hodnocení je ilustrační, organizace může použít vlastní metodu.

Podpůrné otázky k hodnocení dopadu TD1:

- K1 – Rozsah dopadu
  - Způsobuje riziko zvýšené výdaje napříč více odbory nebo projekty?
  - Ovlivňuje dopad provozní nebo strategické výdaje organizace?
- K2 – Intenzita dopadu
  - Došlo nebo může dojít k neplánovaným výdajům převyšujícím běžné provozní odchylky?
  - Vyžaduje řešení dopadu zásah do rozpočtu (rozpočtové opatření)?
- K3 – Náklady/úsilí na nápravu
  - Vyžaduje náprava nákup externích služeb nebo SW/HW?
  - Jsou náklady na nápravu vyšší než náklady způsobené prevencí?
- K4 – Reputační / právní / strategický dopad
  - Může vzniknout reputační problém kvůli nadměrným nákladům?
  - Zvyšuje dopad riziko právního postihu za nehospodárnost?

---

## 4.10 Vazba na kybernetickou bezpečnost

Záznam ID33 v Katalogu uvádí:

- Žádnou typovou zranitelnost NÚKIB (nekonzistence pravidel není KB zranitelností).
- Typovou hrozbu NÚKIB H11 (sekundární) – pochybení zaměstnanců a administrátorů.
- Hrozba NÚKIB: H11 – Pochybení ze strany zaměstnanců a administrátorů.

➡️ To znamená:

- riziko správy dat není kybernetickým rizikem samo o sobě,
- ale zvyšuje pravděpodobnost lidských chyb, které mohou mít bezpečnostní dopady.

---

## Incident, následek a opatření (případná návazná reflexe)

**Incident**

- Data nejsou dostupná nebo spolehlivá, což způsobuje problémy při jejich využití např. v rozhodovacích procesech.

**Následek**

- Ztráta důvěry ve správu dat, omezená možnost zlepšování digitálních služeb veřejné správy.

**Preventivní opatření**

- Vytvoření a publikace jednotných standardů správy dat v souladu s mezinárodními osvědčenými postupy, zavedení povinnosti jejich používání na národní úrovni.

**Reaktivní opatření**

- Identifikace chyb způsobených absencí standardů, vytvoření krizového plánu pro jejich odstranění a sjednocení přístupu mezi organizacemi.

➡️ Tyto prvky:

- nejsou součástí analýzy rizika,
- ale dokládají jeho dlouhodobou realizaci.

---

## 4.11 Závěrečná metodická reflexe

Tento příklad ukazuje, že:

- top-down přístup je ideální pro:
  - identifikaci strukturálních a systémových rizik,
  - která se jinak „rozpouštějí v provozu“,
- typové prvky slouží jako:
  - navigace,
  - nikoli náhrada analýzy,
- konečná práce se vždy odehrává na detailním riziku.

**Shrnutí jednou větou**

Top-down práce s katalogem umožňuje odhalit dlouhodobá procesní rizika správy dat, která nemají jeden incident, ale systematicky snižují kvalitu a efektivitu veřejné správy.

# 5 Přehledové srovnání dvou rizik – právní × procesní (archetyp)

| Dimenze | ID225 – nesprávná interpretace legislativy | ID33 – absence datových standardů |
|---|---|---|
| **Kategorie faktoru** | Právní a regulatorní | Procesní |
| **Typ problému** | Výklad a odpovědnost | Standardizace a koordinace |
| **Povaha rizika** | Diskrétní, eskalovatelné | Strukturální, kumulativní |
| **Vstupní signál** | Právní spor / omezení sdílení | Nízká kvalita, neefektivita |
| **Vhodný scénář** | Bottom-up i top-down | Primárně top-down |
| **Typový kritický faktor** | TKF8.2, TKF1.4 | TKF5.2 |
| **Charakter zranitelnosti** | Řídicí / rozhodovací | Procesní |
| **Hrozby** | Reputační, právní | Koordinační, provozní |

| | | |
|---|---|---|
| **Primární dopad** | TD6 – právní/regulatorní | TD1 – finanční |
| **Sekundární dopady** | TD5 – reputace | TD5 – reputace, TD2 – efektivita |
| **Vazba na NÚKIB** | Ano – odvozeně z dopadu (H1) | Ano – sekundárně (H11) |
| **Typická eskalace** | Náhlá, tlakem zvenčí | Pozvolná, „rozpuštěná v provozu“ |
| **Typické opatření** | Výklad, rozhodnutí, metodika | Standardy, sjednocení, governance |

## 5.1 Klíčové metodické rozdíly (komentář)

#### *5.1.1.1 ID225 – „eskalační“ archetyp*

- riziko dlouho latentní,
- aktivuje se skokově (spor, sankce, audit),
- má:
  - jasný právní spouštěč,
  - rychlou eskalaci,
  - silnou vazbu na vedení.

➡️ Ideální pro ukázku:

- proč správa dat není jen technická,
- jak se sekundární dopad stává bezpečnostním tématem.

---

#### *5.1.1.2 ID33 – „erozní“ archetyp*

- riziko nevybuchne, ale:
  - systematicky snižuje kvalitu,
  - zvyšuje náklady,
  - brzdí digitalizaci,
- často:
  - není nikým vlastněno,
  - není řešeno, protože „se s tím žije“.

➡️ Ideální pro ukázku:

- proč je nutný top-down přístup,
- proč jsou typové prvky klíčové pro orientaci,
- a jak katalog pomáhá odhalit *„tichá rizika“*.

# 6 Použití katalogu rizik správy dat při přípravě rozhovorů s garanty aktiv

*(perspektiva řízení kybernetické bezpečnosti)*

## 6.1 Účel a kontext použití

Řízení kybernetické bezpečnosti v organizacích veřejné správy není omezeno pouze na technickou oblast. Po identifikaci regulovaných služeb a navazujících aktiv je běžnou součástí práce kybernetických manažerů identifikace zranitelností a hrozeb, která vyžaduje součinnost s garanty jednotlivých aktiv, zejména vlastníky a správci dat.

V praxi je tato součinnost nejčastěji realizována formou:

- strukturovaných dotazníků,
- nebo osobních rozhovorů a workshopů.

Právě při přípravě a vedení těchto rozhovorů může katalog rizik správy dat sloužit jako významná podpůrná pomůcka.

---

## 6.2 Role katalogu v tomto scénáři

V tomto scénáři katalog rizik správy dat:

- nenahrazuje analýzu rizik kybernetické bezpečnosti,
- nenahrazuje odpovědnost garantů aktiv,
- a nepředstavuje checklist zranitelností.

Jeho přínos spočívá v tom, že:

- poskytuje strukturovaný přehled typických slabých míst správy dat,
- umožňuje kybernetickému manažerovi lépe porozumět kontextu datových aktiv,
- a podporuje přípravu cílených a věcných otázek pro rozhovory s vlastníky a správci dat.

---

## 6.3 Typický postup práce s katalogem (přípravná fáze)

Kybernetický manažer v přípravné fázi:

1. Nevyhledává konkrétní kybernetické zranitelnosti, ale orientuje se na:
    - oblast správy dat relevantní k regulované službě,
    - procesní, právní nebo organizační faktory,
    - rizika související s významem, sdílením a odpovědností za data.
2. Pomocí katalogu si vytváří přehled možných problémových oblastí, například:
    - nejasnosti ve výkladu legislativních požadavků,
    - absence jasných rozhodovacích mechanismů,
    - nedostatečné zakotvení odpovědností,
    - procesní slabiny při sdílení dat.
3. Identifikované záznamy (např. konkrétní rizika nebo zranitelnosti správy dat) neslouží jako předem dané závěry, ale jako:

- hypotézy k ověření,
- a podklad pro strukturovaný rozhovor.

---

## 6.4 Využití katalogu při vedení rozhovorů

Při samotném rozhovoru s garanty aktiv katalog umožňuje kybernetickému manažerovi:

- klást konkrétní a kontextové otázky, nikoli obecné dotazy,
- zaměřit se na:
  - rozhodovací procesy,
  - skutečnou aplikační praxi,
  - a odchylky mezi formálními pravidly a reálným fungováním.

Typickým přínosem je, že rozhovor:

- nesklouzne pouze k technickým aspektům,
- ale zahrne i řízení významu dat, odpovědností a procesů,
- které mohou být zdrojem zranitelností a hrozeb relevantních pro kybernetickou bezpečnost.

---

## 6.5 Vazba na identifikaci zranitelností a hrozeb kybernetické bezpečnosti

Informace získané prostřednictvím rozhovorů, připravených s využitím katalogu rizik správy dat, mohou:

- upozornit na vnitřní slabiny organizace, které nejsou v typových seznamech kybernetické bezpečnosti explicitně uvedeny,
- pomoci lépe pochopit, zda a jak mohou mít problémy správy dat dopad na důvěrnost, integritu nebo dostupnost aktiv,
- a podpořit rozhodnutí, zda je vhodné některé zjištění eskalovat do řízení rizik kybernetické bezpečnosti.

Katalog v tomto smyslu funguje jako most mezi správou dat a kybernetickou bezpečností, nikoli jako jejich sloučení.

---

## 6.6 Metodická poznámka

Tento způsob použití katalogu:

- nepředepisuje konkrétní otázky ani strukturu rozhovorů,
- respektuje rozdílné postupy jednotlivých organizací,
- a je plně kompatibilní s procesy řízení rizik kybernetické bezpečnosti.

Jeho cílem je zvýšit kvalitu přípravy kybernetických manažerů na spolupráci s garanty dat a tím i kvalitu vstupů pro následnou analýzu rizik.

## 6.7 Ilustrační příklad přípravy kybernetického manažera na rozhovor s garantem dat

### 6.7.1 Výchozí situace (role a kontext)

Kybernetický manažer organizace veřejné správy realizuje analýzu rizik kybernetické bezpečnosti v návaznosti na identifikované regulované služby. Součástí této práce je také identifikace zranitelností a hrozeb, která vyžaduje součinnost s garanty jednotlivých aktiv, zejména vlastníky a správci dat souvisejících s regulovanou službou.

Kybernetický manažer:

- není odborníkem na správu dat,
- ale potřebuje porozumět:
  - možným slabým místům práce s daty,
  - jejich dopadům,
  - a jejich vazbě na kybernetickou bezpečnost.

Cílem této fáze není provést hodnocení rizika, ale připravit se na kvalifikovaný rozhovor s garantem dat.

### 6.7.2 Vstup do katalogu rizik správy dat – způsob nalezení relevantního záznamu

Kybernetický manažer vstupuje do katalogu rizik správy dat s obecnou otázkou:

*„Může mít způsob sdílení a práce s daty právní nebo bezpečnostní dopady na regulovanou službu?“*

Pro vyhledání relevantního kontextu využije:

- fulltextové vyhledávání (např. pojmy „legislativa“, „sdílení“, „nesoulad“),
- případně filtraci podle:
  - oblasti správy dat,
  - kategorie faktoru (právní a regulatorní).

Tímto postupem identifikuje záznam ID225.

### 6.7.3 Orientace v kontextu záznamu ID225 (shrnutí z katalogu)

Kybernetický manažer se nejprve nesoustředí na hodnocení, ale na pochopení souvislostí.

**Kontext záznamu**

- Oblast správy dat:
  - Realizace datových řešení – datová integrace a sdílení dat
- Téma správy dat:
  - Datová integrace (způsoby výměny dat interně mezi agendami a externě s jinými úřady).
- Kategorie faktoru:

    - Právní a regulatorní faktor
- Kritický faktor:
    - Nejasnosti v legislativních požadavcích na sdílení dat
- Příčina:
    - Legislativa neobsahuje dostatečně konkrétní pokyny pro sdílení dat mezi organizacemi.
- Zranitelnost:
    - Nejasné legislativní rámce vedou k různým výkladům a nesprávným implementacím procesů.
- Hrozba:
    - Organizace nejsou schopny plně dodržovat právní předpisy, což zvyšuje riziko pokut a sankcí
- Riziko:
    - Nesprávná interpretace legislativy vede k právním nesouladům a omezením sdílení dat
- Primární dopad:
    - Právní a regulatorní dopady (TD6)
- Sekundární dopad:
    - Reputační dopady (TD5)

Kybernetický manažer si tímto krokem vytváří mentální mapu problému, nikoli závěry.

---

### 6.7.4 Vztah ke kybernetické bezpečnosti (orientační)

Záznam ID225:

- není mapován na typovou zranitelnost NÚKIB, což je v katalogu výslovně uvedeno a metodicky správně vysvětleno.
- Přesto je v katalogu:
    - uvedena vazba na typovou hrozbu NÚKIB H1 (porušení bezpečnostní politiky / právních povinností),
    - a to prostřednictvím dopadu i zranitelnosti.

Kybernetický manažer si z toho odnáší důležitý poznatek:

*„Ne každé relevantní riziko pro kybernetickou bezpečnost má technickou nebo bezpečnostní zranitelnost – některá vznikají z procesních a právních nejasností.“*

---

### 6.7.5 Překlad katalogu do otázek pro rozhovor

Na základě záznamu ID225 si kybernetický manažer nepřipravuje odpovědi, ale otázky, které bude klást garantovi dat.

**Příklady otázek vycházejících z katalogu:**

K odpovědnostem a rozhodování

- Kdo je u nás odpovědný za výklad legislativních požadavků na sdílení těchto dat?
- Existuje formální rozhodnutí, nebo se rozhoduje ad hoc?

K procesům

- Jak je dnes v praxi rozhodováno, zda lze data sdílet s jinou organizací?
- Existují situace, kdy se sdílení raději vůbec nerealizuje z obavy před porušením předpisů?

K aplikační praxi

- Setkali jste se s rozdílnými výklady stejných legislativních požadavků?
- Došlo někdy ke sporu nebo právnímu řešení v souvislosti se sdílením dat?

K dopadům

- Jaké byly dopady těchto nejistot na fungování služby nebo spolupráci s jinými subjekty?
- Vnímáte reputační nebo provozní dopady?

---

### 6.7.6 Přínos pro proces řízení kybernetické bezpečnosti

Díky přípravě s využitím katalogu rizik správy dat:

- rozhovor s garantem dat:
  - je věcný,
  - strukturovaný,
  - a zaměřený na skutečné slabiny,
- kybernetický manažer:
  - lépe porozumí vnitřním zranitelnostem organizace,
  - získá kvalitnější vstupy pro identifikaci hrozeb,
  - a dokáže rozhodnout, zda zjištění:
    - zůstane v rovině správy dat,
    - nebo má být eskalováno do řízení rizik kybernetické bezpečnosti.

---

### 6.7.7 Shrnutí příkladu

V tomto ilustračním příkladu katalog rizik správy dat:

- neslouží jako analytický nástroj,
- ale jako koncepční opora pro přípravu rozhovorů.

Umožňuje kybernetickému manažerovi:

- orientovat se v problematice správy dat,
- klást relevantní otázky,
- a identifikovat souvislosti, které by bez tohoto pohledu mohly zůstat skryté.

# 7 Příloha: Typové archetypy rizik správy dat

*(dynamika vzniku, projevu a řízení rizik)*

## 7.1 Účel přílohy

Tato příloha slouží jako doplňující didaktická pomůcka pro uživatele katalogu rizik správy dat. Jejím cílem je vysvětlit, že ačkoli jsou všechna rizika správy dat v katalogu popsána jednotnou strukturou kauzálního řetězce, v praxi se chovají rozdílně – zejména z hlediska:

- způsobu vzniku,
- rychlosti projevu,
- typických spouštěčů,
- a vhodného scénáře práce s katalogem.

Kapitola nezavádí nové typy rizik, nové kategorie ani nové prvky katalogu. Popisuje pouze opakující se vzorce chování rizik, které lze při práci s katalogem pozorovat napříč různými oblastmi správy dat.

---

## 7.2 Archetyp rizika versus kategorie faktoru

Je důležité rozlišovat mezi:

- kategorií faktoru (např. právní, procesní, technický),
- a archetypem rizika.

Kategorie faktoru popisuje věcnou povahu problému.
Archetyp rizika naproti tomu popisuje dynamiku rizika v čase a v řízení organizace.

Jeden a tentýž typ faktoru může vést k rizikům různých archetypů a naopak – stejný archetyp se může objevit u rizik vycházejících z odlišných kategorií faktorů.

Archetyp tedy není klasifikačním kritériem, ale pomůckou pro volbu vhodného způsobu práce s katalogem.

---

## 7.3 Archetyp 1 – eskalační rizika

### 7.3.1 Charakteristika

Eskalační rizika jsou rizika, která:

- mohou být dlouhou dobu latentní,
- ale aktivují se náhle v důsledku vnějšího nebo vnitřního tlaku,
- typicky vedou k okamžitému zapojení vedení organizace.

Jejich typickým rysem je skoková eskalace – problém, který byl dlouho tolerován nebo přehlížen, se náhle stává kritickým.

### 7.3.2 Typické spouštěče

- právní spor,
- audit nebo kontrola,

- formální stížnost,
- zásah do zákonných povinností organizace.

### 7.3.3 Typické faktory

Často (nikoli výlučně) souvisí s:

- právními a regulatorními faktory,
- organizačními a řídicími faktory,
- bezpečnostními povinnostmi.

### 7.3.4 Vhodný scénář práce s katalogem

- bottom-up (od konkrétního problému nebo incidentu),
- případně kombinace s top-down pro širší kontext.

### 7.3.5 Metodická poznámka

U eskalačních rizik se vazba na kybernetickou bezpečnost často objevuje až na úrovni dopadu, nikoli na úrovni zranitelnosti nebo hrozby správy dat.

---

## 7.4 Archetyp 2 – erozní rizika

### 7.4.1 Charakteristika

Erozní rizika:

- nepůsobí skokově,
- dlouhodobě a systematicky snižují kvalitu, efektivitu a důvěryhodnost správy dat,
- nemají jeden konkrétní incident, který by je „odhalil“.

Často se stávají součástí běžného provozu a jsou vnímána jako „normální stav“.

### 7.4.2 Typické projevy

- nekonzistentní data,
- zvyšující se provozní náklady,
- ztráta interoperability,
- pomalý nebo neefektivní rozvoj digitálních služeb.

### 7.4.3 Typické faktory

Často souvisí s:

- procesními faktory,
- organizačními a kulturními faktory,
- absencí standardizace nebo jasných pravidel.

### 7.4.4 Vhodný scénář práce s katalogem

- top-down (systematický přezkum oblasti),
- práce s typovými prvky jako navigací.

### 7.4.5 Metodická poznámka

Erozní rizika jsou často podhodnocována, protože nemají jasný spouštěč. Katalog pomáhá tato rizika zviditelnit a strukturovat.

---

## 7.5 Archetyp 3 – incidentní rizika

### 7.5.1 Charakteristika

Incidentní rizika:

- jsou spojena s konkrétní událostí nebo selháním,
- mají relativně jasný začátek i průběh,
- vyvolávají okamžitou reakci organizace.

Typicky jde o situace, kdy je problém již zřejmý, ale je třeba:

- pochopit jeho příčiny,
- a zasadit ho do širšího kontextu správy dat.

### 7.5.2 Typické faktory

Často souvisí s:

- technickými faktory,
- provozními faktory,
- bezpečnostními opatřeními nebo jejich selháním.

### 7.5.3 Vhodný scénář práce s katalogem

- bottom-up (od incidentu),
- katalog slouží k rekonstrukci kauzálního řetězce, nikoli k detekci incidentu.

### 7.5.4 Metodická poznámka

Katalog nenahrazuje incident management. Pomáhá ale pochopit, proč incident vznikl a jaké systémové slabiny odhalil.

---

## 7.6 Archetyp 4 – latentně-kulturní rizika

### 7.6.1 Charakteristika

Latentně-kulturní rizika:

- vycházejí z chování, zvyklostí a kompetencí lidí,
- nemají jasného vlastníka,
- bývají bagatelizována nebo racionalizována.

Jsou obtížně uchopitelná a často přežívají i při existenci formálních pravidel.

### 7.6.2 Typické projevy

- obcházení procesů,

- formální dodržování pravidel bez porozumění,
- nízká odpovědnost za data,
- slabá datová kultura.

### 7.6.3 Typické faktory

Často souvisí s:

- kulturními a kompetenčními faktory,
- organizačními nastaveními,
- způsobem řízení a komunikace.

### 7.6.4 Vhodný scénář práce s katalogem

- výhradně top-down,
- systematický přezkum napříč oblastmi.

### 7.6.5 Metodická poznámka

Tento archetyp je nejméně viditelný, ale dlouhodobě velmi nebezpečný. Bez koncepční práce s katalogem bývá prakticky neodhalitelný.

---

## 7.7 Praktický přínos archetypů pro uživatele katalogu

Pochopení archetypů rizik pomáhá uživateli:

- zvolit vhodný scénář práce s katalogem,
- nepřeceňovat absenci incidentu,
- správně interpretovat dynamiku rizika,
- a realisticky plánovat další kroky.

Archetypy:

- nenahrazují analýzu rizik,
- nenahrazují hodnocení dopadů,
- ale zvyšují srozumitelnost a použitelnost katalogu v praxi.

---

## 7.8 Závěrečné shrnutí

Katalog rizik správy dat pracuje s jednotnou strukturou popisu rizik.
Rizika samotná se však v praxi chovají rozdílně.

Typové archetypy rizik správy dat:

- pomáhají porozumět této rozdílnosti,
- podporují správné použití katalogu,
- a zvyšují kvalitu rozhodování bez zavádění nových metodických vrstev.