

podpůrný materiál 4.2-4

Praktický návod ke katalogu rizik správy dat v Excelu

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	Katalog rizik správy dat (Excel) ve zkratce.....	3
1.1	Co je Excel katalog (a co není).....	3
1.2	Jak je katalog konstruován	3
2	Hlavní pracovní list „Katalog“ – integrovaný kauzální přehled	3
2.1	Úvod.....	3
2.2	Struktura sloupců a práce s nimi.....	4
2.3	Typový a konkrétní prvek v katalogu – jak je číst v jednom řádku	7
2.4	Doporučené způsoby filtrování a kombinace pohledů v hlavním pracovním listu	10
2.5	Výstupy práce s katalogem rizik správy dat.....	12
3	Typové seznamy v katalogu rizik správy dat – role a obecné principy.....	12
3.1	Zastřešující informace	12
3.2	Typový seznam kritických faktorů správy dat.....	14
3.3	Typový seznam příčin	15
3.4	Typový seznam zranitelností	16
3.5	Typový seznam hrozeb	17
3.6	Typový seznam rizik správy dat.....	19
3.7	Typový seznam dopadů (TD1–TD14)	20
3.8	Vztah katalogu rizik správy dat k typovým seznamům NÚKIB	22
4	Role a použití Excel katalogu rizik správy dat.....	22
4.1	Role Excel katalogu.....	22
5	Referenční „how-to“ scénáře práce v Excel katalogu	23
5.1	Scénář 1: Top-down analýza z pohledu oblasti správy dat.....	23
5.2	Scénář 2: Analýza konkrétního problému nebo incidentu	24
5.3	Scénář 3: Podpora auditu nebo přezkumu řízení rizik	24
6	Závěrečná poznámka	24

1 Katalog rizik správy dat (Excel) ve zkratce

1.1 Co je „Excel katalog“ (a co není)

- Excel katalog je analytický nástroj pro identifikaci souvislostí v rizicích správy dat (kauzální řetězce).
- Je vstupem pro hodnocení dopadu a prioritizaci rizik, sám o sobě prioritu neurčuje.
- Je kompatibilní s návaznostmi na kybernetickou bezpečnost (mapování na typové prvky, zejména zranitelnosti/hrozby).
- Excel katalog není: náhrada metodiky, výstup risk managementu ani seznamem přesně formulovaných opatření.

1.2 Jak je katalog konstruován

- Jeden hlavní pracovní list „Katalog“ = centrální místo práce (filtrace, vyhledávání, kombinace pohledů).
- Ostatní listy = typové seznamy (číselníky), běžně se needitují.
- Každý řádek hlavního listu reprezentuje jeden kauzální vztah: kritický faktor → příčina → zranitelnost → hrozba → riziko → dopad.
- Typové vazby a klasifikace jsou dostupné jako „rozbalitelné“ vrstvy sloupců v hlavním pracovním listu.

2 Hlavní pracovní list „Katalog“ – integrovaný kauzální přehled

2.1 Úvod

2.1.1 Účel listu

Tento list je **hlavním pracovním listem katalogu rizik správy dat**. Slouží k analytické práci s katalogem jako s **provázaným celkem**, který umožňuje identifikaci, vyhledávání a zkoumání souvislostí v oblasti správy dat z různých úhlů pohledu.

List obsahuje **kompletní soubor kauzálních vazeb** mezi kritickými faktory správy dat, jejich příčinami, zranitelnostmi, hrozbami, riziky a dopady. Je navržen tak, aby s ním bylo možné pracovat **flexibilně a nelineárně**, bez předepsaného pořadí kroků nebo privilegovaného vstupního bodu.

2.1.2 Jak s listem pracovat

Práce s tímto listem je založena na **kombinaci filtrování, vyhledávání a zpřesňování pohledu** podle aktuálního účelu využití katalogu. Uživatel může zahájit práci z libovolného prvku kauzálního řetězce nebo tematického pohledu, například:

- od konkrétního kritického faktoru správy dat,
- od vybrané oblasti nebo tématu správy dat,
- od typu nebo konkrétní zranitelnosti, hrozby nebo rizika,
- od typového nebo konkrétního dopadu,

- nebo na základě textového obsahu jednotlivých polí.

List umožňuje:

- současné použití více filtrů napříč různými sloupci,
- kombinaci strukturovaného filtrování a fulltextového vyhledávání,
- práci jak s typovými, tak s detailními prvky katalogu,
- opakované rozšiřování nebo zužování výběru podle potřeby.

Zvolený způsob práce vždy **závisí na účelu využití katalogu**, na roli osoby, která s katalogem pracuje, a na konkrétní situaci, ve které je katalog použit (např. analytická práce, workshop, podpora rozhodování, návaznost na kybernetickou bezpečnost).

2.1.3 Vztah ke scénářům využití katalogu

Způsob práce s hlavním pracovním listem není pevně daný a může se lišit podle scénářů využití katalogu popsaných v Metodice řízení rizik správy dat. Tyto scénáře ilustrují typické situace, ve kterých je katalog používán, nikoli jediný správný postup práce.

Hlavní pracovní list je navržen tak, aby **umožňoval všechny tyto scénáře podporovat**, aniž by bylo nutné měnit jeho strukturu nebo logiku práce s ním.

2.1.4 Vztah k ostatním listům

Ostatní listy v Excel souboru plní převážně roli **typových a referenčních číselníků**, které poskytují významový a klasifikační rámec. Tyto listy nejsou určeny k běžné analytické práci, jejich obsah je využíván prostřednictvím vazeb v hlavním pracovním listu.

Z pohledu uživatele je proto hlavní pracovní list **centrálním místem práce s katalogem**, zatímco ostatní listy tvoří stabilní podpůrnou strukturu katalogu.

2.1.5 Důležitá upozornění

- Neexistuje jeden „správný“ způsob práce s tímto listem; důležitá je **srozumitelnost zvoleného postupu a jeho účelnost**.
- Smyslem práce s listem není vyčerpání všech možností filtrování, ale **najít relevantní souvislosti a rizika** pro daný účel.
- List slouží jako **analytický podklad** pro další kroky (např. hodnocení dopadu a prioritizaci rizik), nikoli jako jejich náhrada.

2.2 Struktura sloupců a práce s nimi

2.2.1 Logika struktury listu

Hlavní pracovní list je strukturován tak, aby **každý řádek reprezentoval jeden konkrétní kauzální vztah** v katalogu rizik správy dat. Řádek tedy nepopisuje izolovaný prvek (např. samotné riziko), ale **konkrétní vazbu** mezi prvky kauzálního řetězce.

Díky tomu je možné:

- sledovat celý kauzální řetězec v jednom řádku,
- filtrovat a kombinovat pohledy napříč různými částmi řetězce,
- pracovat s katalogem jako s **provázanou mapou rizik**, nikoli jako se seznamem položek.

2.2.2 Typy sloupců v hlavním pracovním listu

Sloupce v hlavním pracovním listu lze z hlediska práce s katalogem rozdělit do několika funkčních skupin. Toto rozdělení pomáhá pochopit, **jaký je význam jednotlivých sloupců a jak s nimi pracovat**.

1. Kauzální sloupce

Tyto sloupce popisují jednotlivé články (prvky) kauzálního řetězce:

- kritický faktor správy dat,
- příčina,
- zranitelnost,
- hrozba,
- riziko správy dat,
- dopad.

Kauzální sloupce tvoří **jádro katalogu** a jsou klíčové pro analytickou práci. Uživatel s nimi pracuje zejména pomocí:

- filtrování,
- vyhledávání,
- kombinování s dalšími sloupci.

Tyto sloupce se **neupravují**, slouží k orientaci a výběru relevantních vazeb.

2. Tematické a klasifikační sloupce

Tyto sloupce umožňují nahlížet na katalog z tematického nebo klasifikačního hlediska, například podle:

- oblasti správy dat,
- tematického okruhu,
- kategorie kritického faktoru.

Tematické sloupce jsou určeny zejména k:

- rychlé orientaci v katalogu,
 - omezení pohledu na konkrétní oblast,
 - kombinaci s kauzálními sloupci při analytické práci.
-

3. Integrační sloupce (vazby na typové seznamy)

Integrační sloupce zajišťují **propojení hlavního pracovního listu s typovými seznamy**, na kterých je katalog rizik správy dat založen. Tyto sloupce nepopisují nové skutečnosti, ale **odkazují na typové prvky**, které jsou udržovány v samostatných číselníkových listech.

Integrační sloupce se mohou vztahovat zejména k:

- typovým kritickým faktorům,

- typovým příčinám,
- typovým zranitelnostem,
- typovým hrozbám,
- typovým rizikům správy dat,
- typovým dopadům (TD1–TD14),
- typovým zranitelnostem a hrozbám podle NÚKIB,
- případně k dalším typovým klasifikacím používaným v katalogu.

Účelem integračních sloupců je:

- zajistit **jednoznačné a konzistentní propojení** jednotlivých záznamů s typovými seznamy,
- umožnit **filtrování a kombinování pohledů** napříč katalogem,
- podpořit **návaznosti na další oblasti řízení**, včetně (ale nikoli výhradně) řízení rizik kybernetické bezpečnosti.

Integrační sloupce jsou klíčové pro zachování integrity katalogu jako celku. Při běžné analytické práci se s nimi pracuje především prostřednictvím filtrování a čtení vazeb; **jejich obsah se neupravuje**.

4. Popisné a vysvětlující sloupce

Popisné sloupce obsahují doplňující textové informace, které:

- rozvádějí význam jednotlivých prvků,
- vysvětlují kontext kauzální vazby,
- pomáhají správné interpretaci záznamů.

Tyto sloupce jsou zvláště užitečné při:

- práci s katalogem v týmu,
- workshopech,
- předávání výstupů dalším osobám.

2.2.3 Základní a rozbalitelné vrstvy informací v hlavním pracovním listu

Hlavní pracovní list je navržen tak, aby **základní kauzální řetězec byl vždy plně viditelný**. Tento základní pohled obsahuje detailní prvky kauzality (např. konkrétní kritický faktor, příčinu, zranitelnost, hrozbu, riziko správy dat a dopad), se kterými uživatel pracuje při běžné orientaci v katalogu.

Na tyto detailní prvky jsou **navázány doplňující informace z typových seznamů**, tematické klasifikace a vysvětlující popisy. Tyto doplňující informace jsou v hlavním pracovním listu **seskupeny** a jsou dostupné až po jejich rozbalení.

Toto řešení umožňuje:

- pracovat s katalogem v jednoduchém a přehledném režimu,
- postupně si zobrazovat další vrstvy informací podle aktuální potřeby,
- zachovat čitelnost základního kauzálního řetězce i při práci s rozsáhlým katalogem.

Stejný princip seskupení je použit **konzistentně pro všechny typové seznamy**, na které je katalog navázán. Detailní prvek kauzálního řetězce je vždy součástí základního zobrazení, zatímco jeho typové a klasifikační vazby tvoří rozbalitelnou doplňující vrstvu.

2.2.4 Vizuální rozlišení sloupců v hlavním pracovním listu

Pro usnadnění práce jsou sloupce v hlavním pracovním listu **vizuálně rozlišeny podle jejich funkce**. Barevné podbarvení sloupců napovídá, jakým způsobem se se sloupcem pracuje:

Typ sloupců	Funkce	Barva podbarvení
Kauzální sloupce	Jádro kauzálního řetězce	Bez barvy / neutrální
Tematické a klasifikační	Pohledy, třídění, kontext	Světle modrá
Integrační (typové vazby)	Propojení na typové seznamy	Světle zelená
Popisné a vysvětlující	Kontext, interpretace	Světle šedá

(Barevné rozlišení má **orientační charakter** a nenahrazuje význam sloupců popsaný v tomto návodu.)

2.2.5 Jak číst jeden řádek v katalogu

Jeden řádek v hlavním pracovním listu představuje **konkrétní scénář vzniku rizika správy dat**, popsaný prostřednictvím kauzální vazby mezi jednotlivými prvky. Při čtení řádku je vhodné jej vnímat jako logický sled:

*Za určitých podmínek správy dat (kritický faktor),
z konkrétních příčin,
vzniká zranitelnost,
která může být zneužita hrozbou,
což vede k určitému riziku správy dat
s odpovídajícím dopadem.*

Tento způsob čtení pomáhá pochopit, **proč je dané riziko v katalogu obsaženo** a v jakých souvislostech se objevuje.

2.3 Typový a konkrétní prvek v katalogu – jak je číst v jednom řádku

2.3.1 Základní rozlišení

Hlavní pracovní list katalogu pracuje současně se dvěma rovinami popisu rizik správy dat:

- **konkrétní (detailní) rovina** – popisuje skutečný, věcný projev problému ve správě dat,
- **typová rovina** – zařazuje tento konkrétní projev do předem definovaného typového rámce.

Obě roviny jsou v katalogu **úmyslně propojeny v jednom řádku**, ale jsou odděleny **strukturou sloupců a jejich seskupením**.

2.3.2 Konkrétní (detailní) prvek

Konkrétní prvek představuje **věcný popis situace nebo jevu**, se kterým uživatel při práci s katalogem fakticky pracuje. V hlavním pracovním listu je konkrétní prvek vždy součástí **základního, plně viditelného kauzálního řetězce**.

Typickými příklady konkrétních prvků jsou:

- detailní kritický faktor správy dat,
- konkrétní příčina nedostatku ve správě dat,
- konkrétní zranitelnost,
- konkrétní hrozba,
- konkrétní riziko správy dat,
- konkrétní dopad.

Tyto sloupce:

- jsou **vždy viditelné**,
- tvoří **pevné jádro řádku**,
- a slouží jako hlavní opěrný bod pro analytickou práci (filtrování, vyhledávání, kombinování pohledů).

2.3.3 Typový prvek

Typový prvek slouží k **zařazení konkrétního projevu do typového rámce**, který umožňuje:

- srovnatelnost napříč katalogem,
- systematickou práci s velkým množstvím záznamů,
- vazby na další typové seznamy a rámce.

Typové prvky jsou v hlavním pracovním listu:

- **navázány na konkrétní prvky**,
- umístěny ve **sloupcích seskupených jako doplňující vrstva**,
- dostupné až po rozbalení příslušného seskupení.

Příklady typových prvků:

- typový kritický faktor,
- typová příčina,
- typová zranitelnost,
- typová hrozba,
- typové riziko,
- typový dopad (TD1–TD14).

2.3.4 Incident, následek a opatření v kauzálním řetězci

Součástí kauzální logiky katalogu rizik správy dat jsou rovněž prvky, které popisují **realizaci rizika a reakci organizace**, zejména:

- incident,
- následek,
- preventivní opatření,
- reaktivní opatření.

Tyto prvky jsou v hlavním pracovním listu **zahrnuty jako součást kauzálního řetězce**, aby bylo možné zachytit logickou návaznost od vzniku rizika až po jeho dopady a reakci organizace.

Na rozdíl od ostatních článků kauzálního řetězce však tyto prvky:

- **nemají typové protějšky**,
- **nejsou mapovány na typové seznamy**,

- a nejsou tedy součástí „typového katalogu rizik správy dat“.

Důvodem je skutečnost, že incidenty, následky a opatření jsou **vždy silně kontextové** a jejich konkrétní podoba závisí na prostředí, procesech a rozhodnutích konkrétní organizace. V katalogu proto plní především **ilustrační a podpůrnou roli**.

Při běžné práci s katalogem slouží tyto sloupce zejména k:

- lepšímu pochopení významu rizika a jeho možných důsledků,
- vazbě na řízení a případné směřování opatření v oblasti správy dat,
- propojení s praktickými scénáři řešení rizik.

2.3.5 Jak spolu konkrétní a typový prvek souvisejí

Vztah mezi konkrétním a typovým prvkem je **vztah přiřazení**, nikoli záměny:

- konkrétní prvek popisuje *co se děje*,
- typový prvek říká *do jaké kategorie tento jev patří*.

Typový prvek:

- **nenahrazuje** konkrétní popis,
- **nezjednodušuje** realitu,
- ale poskytuje **společný jazyk a strukturu** pro další práci s katalogem.

V jednom řádku katalogu tak uživatel vždy vidí:

- konkrétní kauzální scénář,
- a jeho typové zařazení jako doplňující informaci.

2.3.6 Praktický příklad čtení řádku

Při práci s jedním řádkem katalogu je vhodné postupovat takto:

1. nejprve se orientovat v **konkrétních prvcích kauzálního řetězce** (viditelný základ),
2. následně – podle potřeby – rozbalit příslušné seskupení a ověřit:
 - typové zařazení,
 - související klasifikace,
 - integrační vazby.

Tento postup umožňuje:

- rychlou orientaci v katalogu,
- a současně zachování detailu tam, kde je potřeba.

2.3.7 Důležitá upozornění

- Typové prvky **nejsou určeny k úpravám při běžné práci s katalogem**.
- Změna typového zařazení má význam pro celý katalog a patří do správy katalogu, nikoli do jeho běžného používání.
- Pokud konkrétní prvek neodpovídá žádnému existujícímu typovému prvku, je to informace **pro rozvoj katalogu**, nikoli chyba uživatele.

2.4 Doporučené způsoby filtrování a kombinace pohledů v hlavním pracovním listu

2.4.1 Obecný princip práce s filtry

Hlavní pracovní list je navržen tak, aby umožňoval **kombinované a nelineární filtrování** napříč celým kauzálním řetězcem. Neexistuje jeden správný způsob filtrování; zvolený postup vždy závisí na:

- účelu využití katalogu,
- roli uživatele,
- a konkrétní situaci, ve které je katalog používán.

Filtrování lze:

- zahájit v libovolném sloupci,
- postupně kombinovat napříč více sloupci,
- průběžně měnit a zpřesňovat podle potřeby.

2.4.2 Filtrování podle kauzálních prvků

Jedním z nejčastějších způsobů práce je filtrování podle jednotlivých článků kauzálního řetězce, například:

- podle konkrétního kritického faktoru správy dat,
- podle zranitelnosti nebo hrozby,
- podle rizika správy dat,
- podle incidentu nebo následku.

Tento přístup je vhodný zejména tehdy, když:

- uživatel vychází z konkrétního problému nebo zkušenosti,
- řeší se známá slabina ve správě dat,
- nebo se analyzuje již realizovaný incident.

2.4.3 Filtrování podle tematických a klasifikačních pohledů

Tematické a klasifikační sloupce umožňují **rychle zúžit pohled na katalog** bez nutnosti detailní znalosti všech kauzálních vazeb. Typicky se využívají k:

- omezení katalogu na konkrétní oblast správy dat,
- práci s vybraným tematickým okruhem,
- orientaci v katalogu při úvodní analýze nebo workshopu.

Tento způsob filtrování je vhodný zejména v počáteční fázi práce, kdy je cílem:

- získat přehled,
- identifikovat relevantní části katalogu,
- nebo připravit podklad pro další analýzu.

2.4.4 Filtrování podle typových vazeb

Rozbalením seskupených sloupců lze pracovat i s **typovými prvky**, například:

- typovým kritickým faktorem,

- typovou zranitelností nebo hrozbou,
- typovým dopadem.

Tento přístup je užitečný zejména tehdy, když je cílem:

- srovnání více konkrétních případů,
- systematická práce napříč katalogem,
- nebo vazba na další rámce a metodiky.

Filtrování podle typových prvků se obvykle kombinuje s filtrováním podle konkrétních prvků kauzálního řetězce.

2.4.5 Textové vyhledávání a kombinace filtrů

Vedle strukturovaného filtrování lze katalog efektivně používat také pomocí:

- vyhledávání podle textu v buňkách,
- kombinace více filtrů současně,
- postupného rozšiřování a zužování výběru.

Tento způsob práce je typický zejména při:

- explorativní analýze,
- hledání souvislostí,
- práci s katalogem bez předem dané hypotézy.

2.4.6 Iterativní práce s katalogem

Práce s hlavním pracovním listem je ze své podstaty **iterativní**. Uživatel může:

- začít s hrubým filtrem,
- postupně přidávat další kritéria,
- vracet se zpět a filtry upravovat.

Tento způsob práce podporuje:

- hlubší pochopení souvislostí,
- objevování nepřímých vazeb,
- a lepší orientaci v komplexním katalogu.

2.4.7 Upozornění k používání filtrů

- Kombinace více filtrů může vést k velmi úzkému výběru; to není chyba, ale výsledek zvoleného pohledu.
 - Při práci s rozbalenými seskupeními je vhodné průběžně kontrolovat, které filtry jsou aktivní.
 - Smyslem filtrování není „najít jeden správný řádek“, ale **porozumět souvislostem a vzorcům v katalogu**.
-

2.5 Výstupy práce s katalogem rizik správy dat

2.5.1 Smysl výstupů z katalogu

Hlavním smyslem práce s katalogem rizik správy dat není vytvořit nový seznam nebo dokument, ale **porozumět relevantním souvislostem a identifikovat rizika**, která jsou významná z hlediska konkrétní organizace nebo situace.

Katalog slouží jako **analytický podklad** pro další činnosti v oblasti řízení rizik správy dat. Výstupy z katalogu mají podpůrný charakter a nejsou samy o sobě výsledkem procesu řízení rizik.

2.5.2 Co je typickým výstupem práce s katalogem

Typickými výstupy práce s katalogem jsou zejména:

- výběr relevantních rizik správy dat,
- identifikace souvisejících kauzálních vazeb (od kritického faktoru po dopad),
- přehled možných následků realizace rizika,
- identifikace vazeb na další oblasti řízení (např. kybernetickou bezpečnost),
- podklady pro odbornou diskusi a rozhodování.

Tyto výstupy mohou mít podobu:

- vyfiltrovaného pohledu v hlavním pracovním listu,
- exportu vybraných řádků,
- nebo sdíleného pracovního výstupu z workshopu.

2.5.3 Co výstupem práce s katalogem není

Práce s katalogem sama o sobě:

- **nenahrazuje hodnocení dopadu ani prioritizaci rizik,**
- **neurčuje opatření, která mají být přijata,**
- **nevede automaticky k rozhodnutí, které riziko je „nejdůležitější“.**

Tyto kroky jsou řešeny v navazujících částech metodiky a v samostatném návodu k hodnocení rizik správy dat „Návod pro prioritizaci rizik správy dat“.

3 Typové seznamy v katalogu rizik správy dat – role a obecné principy

3.1 Zastřešující informace

3.1.1 Úloha typových seznamů v katalogu

Typové seznamy tvoří **stabilní významový a klasifikační základ** katalogu rizik správy dat. Jejich účelem je zajistit jednotné chápání pojmů, srovnatelnost jednotlivých záznamů a konzistenci katalogu jako celku.

Typové seznamy:

- nepopisují konkrétní situace v organizaci,
- ale poskytují **referenční rámec**, do kterého jsou konkrétní projevy rizik zařazovány.

Díky tomu je možné s katalogem pracovat systematicky i v prostředí, kde se konkrétní projevy rizik liší napříč organizacemi.

3.1.2 Vztah typových seznamů k hlavnímu pracovnímu listu

Typové seznamy nejsou určeny k samostatné analytické práci. Jejich obsah je využíván **nepřímo**, prostřednictvím vazeb v hlavním pracovním listu.

V hlavním pracovním listu jsou typové prvky:

- navázány na konkrétní (detailní) prvky kauzálního řetězce,
- zpřístupněny jako **rozbalitelné doplňující vrstvy informací**,
- používány především k filtrování, třídění a systematickému pohledu na katalog.

Z pohledu běžného uživatele tak typové seznamy fungují jako „**neviditelná infrastruktura**“, která podporuje práci s katalogem, aniž by ji komplikovala.

Poznámka k vícenásobným vazbám v typových seznamech

Typové seznamy v katalogu rizik správy dat umožňují vícenásobné vazby, například přiřazení více typových kritických faktorů, hrozeb nebo dopadů k jednomu kauzálnímu řetězci. Stejně tak může být u rizik nebo dopadů rozlišován primární a sekundární význam.

Tyto vícenásobné vazby nejsou chybou katalogu, ale odrazem složitosti reálných situací ve správě dat. Katalog je navržen tak, aby tuto složitost zachytil, nikoli ji uměle zjednodušoval.

Konkrétní způsob práce s těmito vazbami (např. určení primárního dopadu pro účely hodnocení) je řešen v metodice řízení rizik správy dat a v navazujícím návodu k hodnocení rizik „Návod pro prioritizaci rizik správy datů“.

3.1.3 Proč se s typovými seznamy běžně nepracuje přímo (ve smyslu jejich úprav)

Typové seznamy jsou v katalogu rizik správy dat **běžně používány jako analytický nástroj**, zejména při práci typu *top-down*, kdy uživatel:

- vychází z typového kritického faktoru, zranitelnosti, hrozby nebo dopadu,
- a postupně zkoumá, jaké konkrétní projevy a kauzální vazby jsou s tímto typovým prvkem v katalogu spojeny.

V tomto smyslu jsou typové prvky **plnohodnotným výchozím bodem práce s katalogem** a jsou aktivně využívány při filtrování, třídění a kombinování pohledů v hlavním pracovním listu.

Přímá práce s typovými seznamy však **není běžná ve smyslu jejich úprav**. Typové seznamy:

- mají globální význam pro celý katalog,
- zajišťují jednotný význam pojmů napříč všemi záznamy,
- a jejich změna by měla dopad na velké množství vazeb.

Z tohoto důvodu:

- se typové položky při běžné práci **neupravují**,
- nové typové prvky se **nevytvářejí ad-hoc**,
- a změny typových seznamů patří do řízeného procesu správy katalogu.

Pokud při analytické práci vyjde najevo, že určitý konkrétní prvek nelze smysluplně zařadit do žádného existujícího typového prvku, nejde o chybu v použití katalogu, ale o **podnět k jeho dalšímu rozvoji**.

3.1.4 Typové seznamy jako nástroj konzistence a integrace

Jedním z hlavních přínosů typových seznamů je možnost:

- udržet konzistenci katalogu v čase,
- podporovat jednotný jazyk napříč organizacemi,
- a vytvářet vazby na další rámce a oblasti řízení.

Typové seznamy tak plní roli **dlouhodobě stabilního referenčního základu**, na kterém je katalog postaven, zatímco konkrétní projevy rizik mohou být variabilní a situačně podmíněné.

3.2 Typový seznam kritických faktorů správy dat

3.2.1 Úloha typového seznamu

Typový seznam kritických faktorů správy dat slouží k **systematickému zachycení oblastí správy dat**, ve kterých může docházet ke vzniku významných nedostatků. Kritické faktory představují **výchozí bod kauzálního řetězce** a umožňují nahlížet na rizika správy dat z hlediska jejich kořenových slabin.

Typové kritické faktory nejsou popisem konkrétní situace v organizaci, ale **obecnou charakteristikou typu problému**, který se může v různých podobách opakovat napříč organizacemi.

3.2.2 Typ informace, kterou seznam obsahuje

Typový seznam kritických faktorů obsahuje:

- vymezení jednotlivých typů kritických faktorů správy dat,
- jejich zařazení do tematických oblastí správy dat,
- případně doplňující vysvětlující informace k jejich významu.

Seznam nepopisuje konkrétní příčiny, zranitelnosti ani rizika, ale poskytuje **konceptuální rámec**, ze kterého tyto prvky v kauzálním řetězci vycházejí.

3.2.3 Použití v hlavním pracovním listu

V hlavním pracovním listu jsou typové kritické faktory:

- navázány na konkrétní (detailní) kritické faktory,
- dostupné jako rozbalitelná vrstva informací,
- využívány zejména při práci typu *top-down*.

Uživatel může typový kritický faktor použít jako:

- výchozí bod analýzy,
 - filtr pro omezení katalogu na vybrané oblasti správy dat,
 - nástroj pro systematické porovnání různých kauzálních řetězců.
-

3.2.4 Poznámka k interpretaci

Jeden konkrétní kauzální řetězec může být:

- navázán na více typových kritických faktorů,
- nebo může být relevantní z více pohledů současně.

Tato vícenásobnost není chybou, ale odrazem skutečnosti, že problémy ve správě dat často vznikají **kombinací více slabin**.

3.3 Typový seznam příčin

3.3.1 Úloha typového seznamu

Typový seznam příčin slouží k zachycení **typických mechanismů, kterými se kritické faktory správy dat promítají do konkrétních slabin**. Zatímco kritické faktory vymezují *oblast problému*, příčiny popisují, *jakým způsobem problém vzniká nebo se projevuje*.

Typové příčiny umožňují systematicky rozlišovat, zda rizika správy dat vznikají např. v důsledku chybného nastavení procesů, nedostatečných kompetencí, absence pravidel, technologických omezení nebo jiných opakujících se vzorců.

3.3.2 Typ informace, kterou seznam obsahuje

Typový seznam příčin obsahuje:

- obecně formulované typy příčin,
- které se mohou opakovaně vyskytovat napříč různými oblastmi správy dat,
- bez vazby na konkrétní organizaci nebo situaci.

Příčiny nejsou samy o sobě rizikem ani zranitelností, ale představují **mezistupeň** mezi kritickým faktorem a vznikem konkrétní zranitelnosti.

3.3.3 Použití v hlavním pracovním listu

V hlavním pracovním listu jsou typové příčiny:

- navázány na konkrétní (detailní) příčiny,
- dostupné jako rozbalitelná doplňující vrstva,
- využívány při analýze kauzální logiky rizik.

Uživatel může typové příčiny využít zejména:

- k pochopení, *proč* určitý kritický faktor vede ke konkrétnímu riziku,
- k porovnání různých kauzálních řetězců, které mají obdobný původ,
- jako podpůrný pohled při identifikaci opatření (bez jejich přímého návrhu).

3.3.4 Poznámka k interpretaci

Jednomu kritickému faktoru může odpovídat:

- více typových příčin,
- které se mohou vzájemně kombinovat nebo posilovat.

Typová příčina nevyjadřuje míru závažnosti ani pravděpodobnosti, slouží výhradně k **strukturaci a pochopení vzniku rizika** v rámci kauzálního řetězce.

3.4 Typový seznam zranitelností

3.4.1 Úloha typového seznamu

Typový seznam zranitelností slouží k zachycení **typických slabín**, které vznikají jako důsledek působení příčin v oblasti správy dat a které mohou být **zneužitelné hrozbou**. Zranitelnost představuje bod, ve kterém se nedostatek ve správě dat stává potenciálně využitelným a kde se kauzální řetězec přibližuje realizaci rizika.

V kontextu správy dat nejsou zranitelnosti chápány pouze technicky, ale **v širším smyslu**, zahrnujícím i organizační, procesní a koncepční slabiny.

3.4.2 Typ informace, kterou seznam obsahuje

Typový seznam zranitelností obsahuje:

- obecně formulované typy zranitelností,
- které se mohou opakovat napříč různými oblastmi správy dat,
- bez vazby na konkrétní technologii, systém nebo organizaci.

Typové zranitelnosti nepopisují konkrétní bezpečnostní incidenty ani hrozby, ale vymezují **stav nebo vlastnost**, která umožňuje, aby se hrozba uplatnila.

U některých typových zranitelností je uvedena také informace o potenciálním ovlivnění důvěrnosti, integrity nebo dostupnosti aktiv. Tato informace má orientační charakter a vyjadřuje **potenciál ovlivnění** těchto vlastností v případě realizace zranitelnosti.

Nejedná se o hodnocení dopadu, klasifikaci aktiv ani o výsledek analýzy kybernetické bezpečnosti. Účelem této informace je usnadnit porozumění možným vazbám mezi riziky správy dat a oblastí kybernetické bezpečnosti.

3.4.3 Použití v hlavním pracovním listu

V hlavním pracovním listu jsou typové zranitelnosti:

- navázány na konkrétní (detailní) zranitelnosti,
- dostupné jako rozbalitelná doplňující vrstva informací,
- využívány k pochopení vazby mezi příčinami a hrozbami.

Uživatel může typové zranitelnosti využít zejména:

- při analýze, jakým způsobem nedostatky ve správě dat vytvářejí prostor pro realizaci hrozeb,
 - při systematickém porovnání různých kauzálních řetězců,
 - jako podklad pro posouzení, zda se daný problém může projevit i v oblasti kybernetické bezpečnosti.
-

3.4.4 Vztah ke kybernetické bezpečnosti

Některé zranitelnosti správy dat mohou mít význam i z pohledu kybernetické bezpečnosti, jiné jsou relevantní primárně v kontextu správy dat. Tato skutečnost odráží rozdílné zaměření obou oblastí.

Katalog rizik správy dat proto pracuje s typovými zranitelnostmi tak, aby zachytil i ty slabiny, které nejsou v rámci kybernetické bezpečnosti explicitně popsány, ale mohou vést k významným dopadům. Vazby na oblast kybernetické bezpečnosti jsou v katalogu uplatňovány prostřednictvím konkrétních kauzálních prvků, tedy na úrovni konkrétních zranitelností, hrozeb nebo rizik, nikoli přímým mapováním typových seznamů mezi sebou.

3.4.5 Poznámka k interpretaci

Jednomu kauzálnímu řetězci může odpovídat:

- více typových zranitelností,
- případně kombinace zranitelností různého charakteru (např. procesní a technické).

Typová zranitelnost sama o sobě nevyjadřuje pravděpodobnost ani závažnost rizika; slouží k **pochopení mechanismu, kterým se riziko může realizovat.**

3.5 Typový seznam hrozeb

3.5.1 Úloha typového seznamu

Typový seznam hrozeb slouží k zachycení **typických způsobů, jakými mohou být zranitelnosti ve správě dat zneužity nebo realizovány.** Hrozba představuje aktivní prvek kauzálního řetězce, který působí na existující zranitelnost a může vést ke vzniku konkrétního rizika správy dat.

Typové hrozby nepopisují konkrétní incidenty ani aktéry v konkrétní organizaci, ale **obecné vzorce působení**, které se mohou opakovat v různých kontextech.

3.5.2 Typ informace, kterou seznam obsahuje

Typový seznam hrozeb obsahuje:

- obecně formulované typy hrozeb,
- které mohou působit na zranitelnosti v oblasti správy dat,
- bez vazby na konkrétní technologii, systém nebo organizační prostředí.

Hrozby mohou mít:

- vnitřní nebo vnější původ,
- úmyslný nebo neúmyslný charakter,
- technickou, organizační nebo procesní povahu.

Typová hrozba sama o sobě nevyjadřuje pravděpodobnost ani závažnost dopadu, slouží k **pojmenování způsobu, jakým může být slabina ve správě dat realizována.**

3.5.3 Použití v hlavním pracovním listu

V hlavním pracovním listu jsou typové hrozby:

- navázány na konkrétní (detailní) hrozby,
- dostupné jako rozbalitelná doplňující vrstva informací,
- využívány při analýze vazby mezi zranitelností a vznikem rizika správy dat.

Uživatel může typové hrozby využít zejména:

- při systematickém porovnání různých kauzálních řetězců,
 - při práci typu *top-down* (např. vycházet z určitého typu hrozby),
 - jako podpůrný prvek při posuzování, zda se daný problém může projevit i mimo oblast správy dat.
-

3.5.4 Poznámka k informaci o CIA

U některých typových hrozeb je uvedena také informace o potenciálním ovlivnění důvěrnosti, integrity nebo dostupnosti aktiv. Tato informace má **orientační charakter** a vyjadřuje potenciál ovlivnění těchto vlastností v případě realizace hrozby.

Nejedná se o hodnocení dopadu, klasifikaci aktiv ani o výsledek analýzy kybernetické bezpečnosti. Účelem této informace je usnadnit porozumění možným vazbám mezi riziky správy dat a oblastí kybernetické bezpečnosti.

3.5.5 Vztah ke kybernetické bezpečnosti

Některé hrozby relevantní pro správu dat mohou mít význam i z pohledu kybernetické bezpečnosti, jiné jsou relevantní primárně v kontextu správy dat. Tato skutečnost odráží rozdílné zaměření obou oblastí.

Vazby na oblast kybernetické bezpečnosti jsou v katalogu uplatňovány **prostřednictvím konkrétních kauzálních prvků**, tedy na úrovni konkrétních hrozeb nebo rizik, nikoli přímým mapováním typových seznamů mezi sebou.

3.5.6 Poznámka k interpretaci

Jednomu kauzálnímu řetězci může odpovídat:

- více typových hrozeb,
- případně kombinace hrozeb různého charakteru.

Tato vícenásobnost není chybou, ale odrazem skutečnosti, že realizace rizik správy dat je často výsledkem **souběhu více působících faktorů**.

3.6 Typový seznam rizik správy dat

3.6.1 Úloha typového seznamu

Typový seznam rizik správy dat slouží k zachycení **typických rizik**, která vznikají kombinací zranitelnosti a působících hrozeb v oblasti správy dat. Riziko představuje **syntézu kauzálního řetězce** a vyjadřuje, jaký nežádoucí stav nebo situace může v důsledku nedostatků ve správě dat nastat.

Typová rizika nejsou popisem konkrétní události v organizaci, ale **obecně formulovanými rizikovými scénáři**, které se mohou opakovat napříč různými organizacemi a kontexty.

3.6.2 Typ informace, kterou seznam obsahuje

Typový seznam rizik správy dat obsahuje:

- obecně formulované typy rizik,
- které popisují možné negativní důsledky působení hrozeb na zranitelnosti,
- bez vazby na konkrétní systém, proces nebo organizační uspořádání.

Typové riziko nevyjadřuje:

- pravděpodobnost jeho realizace,
- ani závažnost dopadu.

Jeho účelem je **pojmenovat rizikovou situaci** tak, aby byla srozumitelná a srovnatelná napříč katalogem.

3.6.3 Použití v hlavním pracovním listu

V hlavním pracovním listu jsou typová rizika:

- navázána na konkrétní (detailní) rizika správy dat,
- dostupná jako rozbalitelná doplňující vrstva informací,
- využívána jako jeden z hlavních orientačních bodů při práci s katalogem.

Uživatel může typová rizika využít zejména:

- jako výchozí bod práce typu *top-down*,
 - k systematickému porovnání různých kauzálních řetězců,
 - k přípravě podkladů pro hodnocení dopadů a stanovení priority rizik.
-

3.6.4 Poznámka k informaci o CIA

U některých typových rizik je uvedena také informace o potenciálním ovlivnění důvěrnosti, integrity nebo dostupnosti aktiv. Tato informace má **orientační charakter** a vyjadřuje potenciál ovlivnění těchto vlastností v případě realizace rizika.

Nejedná se o hodnocení dopadu, klasifikaci aktiv ani o výsledek analýzy kybernetické bezpečnosti. Účelem této informace je usnadnit porozumění možným vazbám mezi riziky správy dat a oblastí kybernetické bezpečnosti.

3.6.5 Vztah ke kybernetické bezpečnosti

Typová rizika správy dat nemají přímý ekvivalent v rámci kybernetické bezpečnosti. V oblasti kybernetické bezpečnosti nejsou používány typové seznamy rizik; riziko je zde vždy posuzováno v konkrétním kontextu na základě kombinace hrozby, zranitelnosti a dopadu.

Rizika správy dat mohou mít význam z pohledu kybernetické bezpečnosti **nepřímo**, zejména tehdy, pokud jejich realizace souvisí s konkrétními zranitelnostmi nebo hrozbami, které jsou relevantní i v kontextu kybernetické bezpečnosti. Tyto vazby jsou v katalogu uplatňovány prostřednictvím konkrétních kauzálních prvků, nikoli přímým mapováním typových seznamů rizik.

3.6.6 Poznámka k interpretaci

Jednomu konkrétnímu riziku správy dat může odpovídat:

- více typových rizik,
- případně různé typové formulace téhož problému z odlišných pohledů.

Tato vícenásobnost umožňuje:

- zachytit komplexní povahu rizik správy dat,
- a pracovat s nimi flexibilně podle účelu analýzy.

3.7 Typový seznam dopadů (TD1–TD14)

3.7.1 Úloha typového seznamu

Typový seznam dopadů slouží k **systematickému zachycení možných následků realizace rizik správy dat**. Dopady představují **poslední článek kauzálního řetězce** a vyjadřují, jaký negativní efekt může mít realizované riziko na organizaci, její činnosti nebo plnění jejích povinností.

Typové dopady jsou formulovány tak, aby:

- byly srozumitelné napříč organizacemi,
- pokrývaly různé oblasti působení (provozní, právní, reputační, strategické apod.),
- a umožňovaly následné hodnocení dopadu jednotným způsobem.

3.7.2 Typ informace, kterou seznam obsahuje

Typový seznam dopadů obsahuje:

- omezený a stabilní soubor typových dopadů (TD1–TD14),
- které reprezentují **základní kategorie negativních následků** v oblasti správy dat,
- bez vazby na konkrétní aktiva, systémy nebo organizační kontext.

Typové dopady:

- nejsou hodnocením závažnosti,
- nevyjadřují finanční ani jiný kvantifikovaný rozsah,
- slouží výhradně k **pojmenování typu následku**.

3.7.3 Použití v hlavním pracovním listu

V hlavním pracovním listu jsou typové dopady:

- navázány na konkrétní (detailní) dopady,
- dostupné jako rozbalitelná referenční vrstva,
- využívány jako **výchozí bod pro hodnocení dopadu rizika**.

Uživatel může typové dopady využít zejména:

- k určení **primárního dopadu** daného rizika,
- k identifikaci **sekundárních dopadů**, které mohou riziko dále doprovázet,
- jako společný jazyk pro diskusi o následcích rizik napříč rolemi a útvary.

3.7.4 Primární a sekundární dopady

Jedno riziko správy dat může vést k:

- jednomu primárnímu dopadu,
- a jednomu nebo více sekundárním dopadům.

Primární dopad je ten, který:

- nejlépe vystihuje **hlavní povahu škody**,
- a na jehož základě je riziko **hodnoceno a prioritizováno**.

Sekundární dopady:

- poskytují širší kontext,
- pomáhají pochopit celkový rozsah následků,
- ale **nejsou samostatně hodnoceny** v rámci prioritizace.

Konkrétní způsob práce s primárními a sekundárními dopady je řešen v navazujícím návodu k hodnocení rizik správy dat.

3.7.5 Vztah ke kybernetické bezpečnosti

Některé typové dopady správy dat mohou být relevantní i z pohledu kybernetické bezpečnosti, zejména pokud se týkají:

- narušení dostupnosti,
- integrity informací,
- nebo důvěryhodnosti činností organizace.

Typový seznam dopadů však:

- neslouží ke klasifikaci aktiv,
- nenahrazuje hodnocení dopadu v řízení kybernetické bezpečnosti,
- a není mapován na žádný typový seznam dopadů v rámci NÚKIB.

Vazby na oblast kybernetické bezpečnosti jsou uplatňovány **na úrovni konkrétních kauzálních prvků a jejich hodnocení**, nikoli prostřednictvím typového seznamu dopadů jako takového.

3.7.6 Poznámka k interpretaci

Vícenásobné dopady nejsou chybou katalogu, ale odrazem skutečnosti, že:

- realizace rizik správy dat má často **řetězový nebo kombinovaný efekt**,
- a může se projevit v různých oblastech současně.

Typový seznam dopadů poskytuje **strukturovaný rámec**, který umožňuje tuto komplexitu zachytit, aniž by byla ztracena přehlednost.

3.8 Vztah katalogu rizik správy dat k typovým seznamům NÚKIB

Katalog rizik správy dat je koncipován tak, aby byl **kompatibilní s přístupem k řízení rizik kybernetické bezpečnosti**, zejména v prostředí veřejné správy. V této souvislosti pracuje s vazbami na vybrané typové seznamy používané v rámci řízení kybernetické bezpečnosti podle metodik NÚKIB.

Specifika mapování na typové seznamy NÚKIB

Katalog rizik správy dat obsahuje vazby na typové seznamy kybernetické bezpečnosti používané v rámci metodik NÚKIB, které jsou vedeny na samostatných listech. Tato mapování jsou uplatňována **na úrovni konkrétních kauzálních prvků**, nikoli mezi typovými seznamy jako takovými.

Mapování může vycházet nejen z konkrétních zranitelností nebo hrozeb správy dat, ale také z **konkrétních dopadů rizik správy dat**. V těchto případech může dopad rizika správy dat představovat **hrozbu z pohledu kybernetické bezpečnosti**, a to i tehdy, pokud neexistuje přímé mapování mezi zranitelnostmi nebo hrozbami správy dat a typovými zranitelnostmi či hrozbami NÚKIB.

Tento přístup umožňuje:

- zachytit relevantní souvislosti mezi riziky správy dat a kybernetickou bezpečností,
- aniž by docházelo k míchání metodických rámců nebo duplikaci typových katalogů.

Podrobná práce s typovými seznamy NÚKIB, včetně hodnocení rizik kybernetické bezpečnosti, zůstává plně v gesci příslušných procesů řízení kybernetické bezpečnosti.

4 Role a použití Excel katalogu rizik správy dat

4.1 Role Excel katalogu

Excel katalog rizik správy dat slouží jako **praktický analytický nástroj**, který podporuje identifikaci, porozumění a systematickou práci s riziky správy dat. Umožňuje zachytit kauzální souvislosti mezi kritickými faktory, příčinami, zranitelnostmi, hrozbami, riziky a jejich dopady a vytváří společný referenční rámec pro odbornou diskusi.

Katalog:

- nepředstavuje samostatnou metodiku řízení rizik,
- ale je **nástrojem pro její praktickou aplikaci**,
- a podporuje propojení oblasti správy dat s řízením rizik kybernetické bezpečnosti.

4.1.1 Vymezení hranic katalogu

Excel katalog rizik správy dat:

- **nenahrazuje hodnocení dopadu ani prioritizaci rizik,**
- **nepředepisuje konkrétní opatření,**
- **neřeší řízení rizik kybernetické bezpečnosti jako celek.**

Katalog neposkytuje „správná rozhodnutí“, ale **strukturované podklady**, na jejichž základě mohou být rozhodnutí činěna v navazujících procesech.

Způsob práce s katalogem, míra detailu i forma dokumentace výstupů závisí na potřebách, zvyklostech a vyspělosti konkrétní organizace.

4.1.2 Vztah k navazujícím dokumentům

Práce s Excel katalogem je úzce provázána s dalšími dokumenty:

- **Metodika řízení rizik správy dat**, která vymezuje koncepční rámec a scénáře použití katalogu,
- **Návod pro prioritizaci rizik správy dat**, který stanovuje způsob hodnocení dopadů a určování priority rizik.

Excel katalog poskytuje vstupy pro tyto procesy, ale **nenahrazuje je**.

5 Referenční „how-to“ scénáře práce v Excel katalogu

Následující scénáře ilustrují typické způsoby práce s katalogem. Nejde o závazné postupy, ale o **referenční příklady**, které lze kombinovat a přizpůsobovat.

5.1 Scénář 1: Top-down analýza z pohledu oblasti správy dat

Cíl: Získat přehled o rizicích spojených s konkrétní oblastí správy dat.

Postup:

1. V hlavním pracovním listu vyberte typový kritický faktor nebo tematickou oblast.
2. Pomocí filtrace omezte zobrazení na relevantní kauzální řetězce.
3. Prohlédněte navázaná rizika a jejich dopady.
4. Identifikujte primární dopady jako vstup pro hodnocení rizik.

Vhodné zejména pro:

- úvodní analýzu,
- plánování rozvoje správy dat,
- systematický přehled rizik.

5.2 Scénář 2: Analýza konkrétního problému nebo incidentu

Cíl: Pochopit souvislosti konkrétního problému ve správě dat.

Postup:

1. Vyhledejte konkrétní zranitelnost, hrozbu nebo incident.
2. Sledujte kauzální vazby směrem ke kritickým faktorům i dopadům.
3. Identifikujte související rizika a případné vazby na oblast kybernetické bezpečnosti.
4. Použijte výstup jako podklad pro další řešení nebo eskalaci.

Vhodné zejména pro:

- řešení incidentů,
 - post-incidentní analýzu,
 - odbornou diskusi nad příčinami.
-

5.3 Scénář 3: Podpora auditu nebo přezkumu řízení rizik

Cíl: Ověřit, zda jsou relevantní rizika správy dat systematicky zohledněna.

Postup:

1. Filtrem vymezte vybranou oblast, systém nebo typ rizik.
2. Porovnejte existující kauzální řetězce s realitou v organizaci.
3. Identifikujte chybějící nebo nedostatečně pokryté oblasti.
4. Využijte katalog jako argumentační a referenční nástroj.

Vhodné zejména pro:

- interní audity,
 - přezkum řízení rizik,
 - komunikaci s vedením nebo kontrolními orgány.
-

6 Závěrečná poznámka

Excel katalog rizik správy dat je navržen jako **otevřený a flexibilní nástroj**, který umožňuje postupné zavádění správy dat a její integraci s existujícími procesy řízení rizik. Jeho přínos spočívá především ve **strukturování myšlení a diskuse**, nikoli v automatizaci rozhodování.