DATRON
INFORMATION TECHNOLOGIES

# Rizika pod kontrolou

Jaromír Látal

# Co musí být pod kontrolou

## Hrozby

Evidovat a maximálně minimalizovat dopady možných hrozeb

## Aktiva

Detailní seznam všech aktiv a jejich vliv na základní procesy společnosti

## Zranitelnosti

Evidence a řešení známých zranitelností

## Uživatelé

Průběžné vzdělávání a testování uživatelů v oblasti KB

# Aktuální situace
# (NIS2 → Zákon o kybernetické bezpečnosti )….

# Aktuální situace vyhláška NIS 2
# a
# Zákon o kybernetické bezpečnosti

**2021–23**

## HW infrastruktura

Obnova a rozvoj

Realizace projektů

**2023**

## Legislativa

05/2023 – 09/2023 Připomínkové řízení

4Q Předložení návrhu ZKB Poslanecké sněmovně

Transpozice NIS 2 do 17.10.2024

**2023**

## Příprava

Lidské zdroje

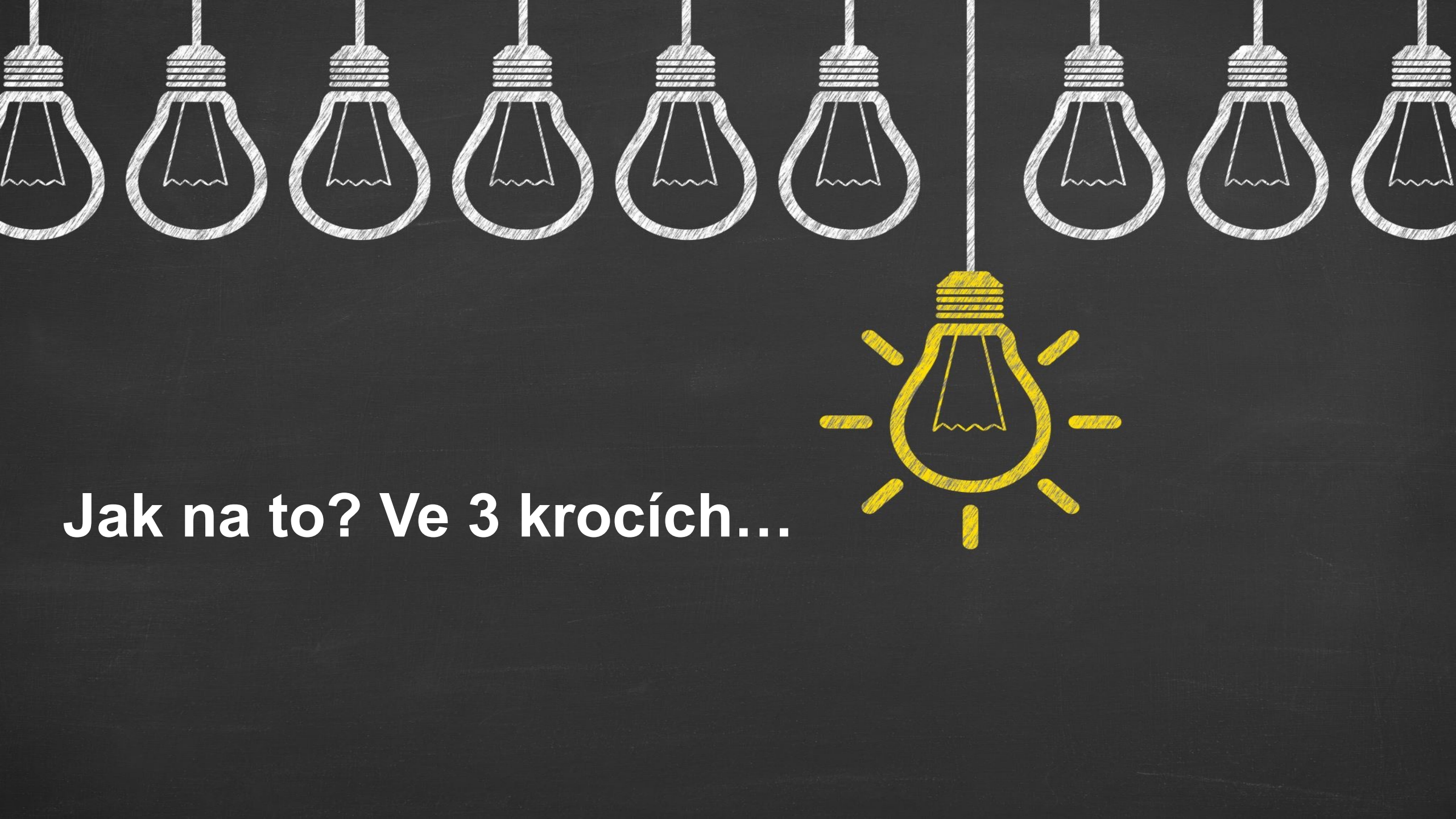
Procesní zpracování

Řešení rizik

**?**

## Realizace

Jak na to?



# Jak na to? Ve 3 krocích…

# 1. Lidé

# VZDĚLÁVÁNÍ A BEZPEČNOST

## 1 Vzdělávání/rozvoj dovedností

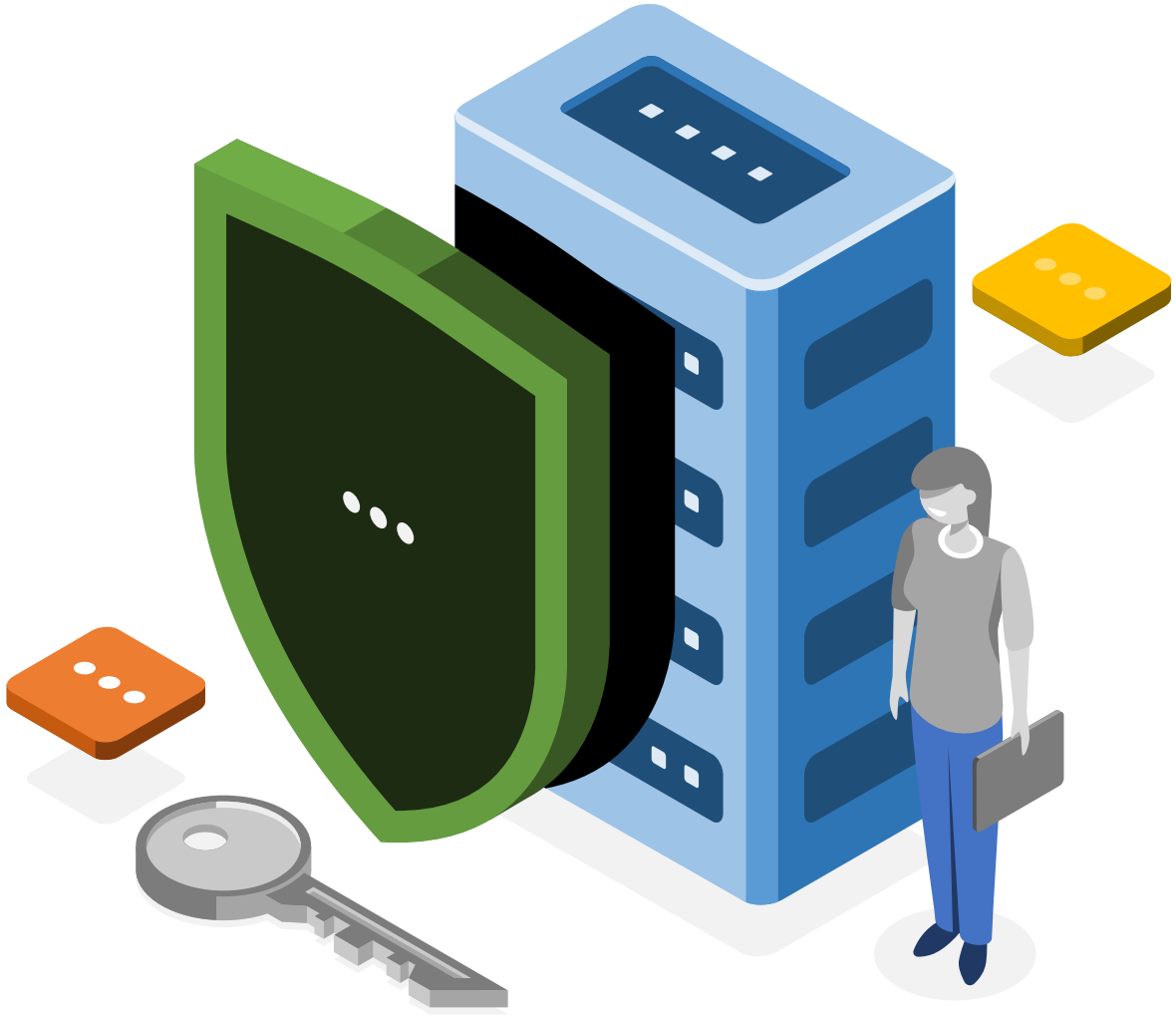
- Vzdělávání interních uživatelů
- Audit znalostí
- Online/prezenční kurzy dle potřeby

## 2 Konzultace/analýza

- Analýza procesů a přípravy na ZKB
- Konzultace řešení prioritních rizik organizace
- Definování nástrojů pro interní uživatele

# 2. Procesy

# PROCESY A NÁSTROJE



## 1 PROCESY

- Definice potřeb vlastní organizace
  - nižší vs. vyšší požadavky dle nového ZKB
- Definice rolí a potřeb uživatelů

## 2 Nástroje/agenda

- Přehledy a **evidence aktiv a rizik**
- Reporting, notifikace a vyhodnocení
- **Řízení rizik v reálném čase**

# AGENDA ISMS (analýza rizik)

## Hlavní vlastnosti

- Řízení/správa dat v oblasti kybernetické bezpečnosti
- Podpora norem:
  - Zákon o kybernetické bezpečnosti
  - ISO 27001
  - TISAX
- Kontrola rizik a jejich řízení
- Automatizace procesů (notifikace, reporting, vazby…)

# AGENDA ISMS (analýza rizik)

## „Moduly“ agendy ISMS

- Katalog **informačních aktiv**
- Katalog hrozeb
- Evidence rizik a jejich řízení

- Úkoly - Plán zvládání rizik

- Vzdělávání v rámci kybernetické bezpečnosti

- Úkoly, změnové požadavky…

- Evidence
    - audity
    - neshody/opatření
    - **bezpečnostních událostí/incidentů**

# AGENDA ISMS (analýza rizik)

## Katalog „hrozeb“ a „informačních aktiv“

- Katalog „hrozeb“:
  - definice a možnosti úpravy
  - implementace v rámci více organizací
  - vazba na katalog opatření dle norem (ZKB, ISO 27001, TISAX)

- Katalog „ informačních aktiv“:
  - seznam primárních aktiv
  - seznam podpůrných aktiv
  - N úrovní katalogu aktiv
  - definice jednotlivých aktiv

# AGENDA ISMS (analýza rizik)

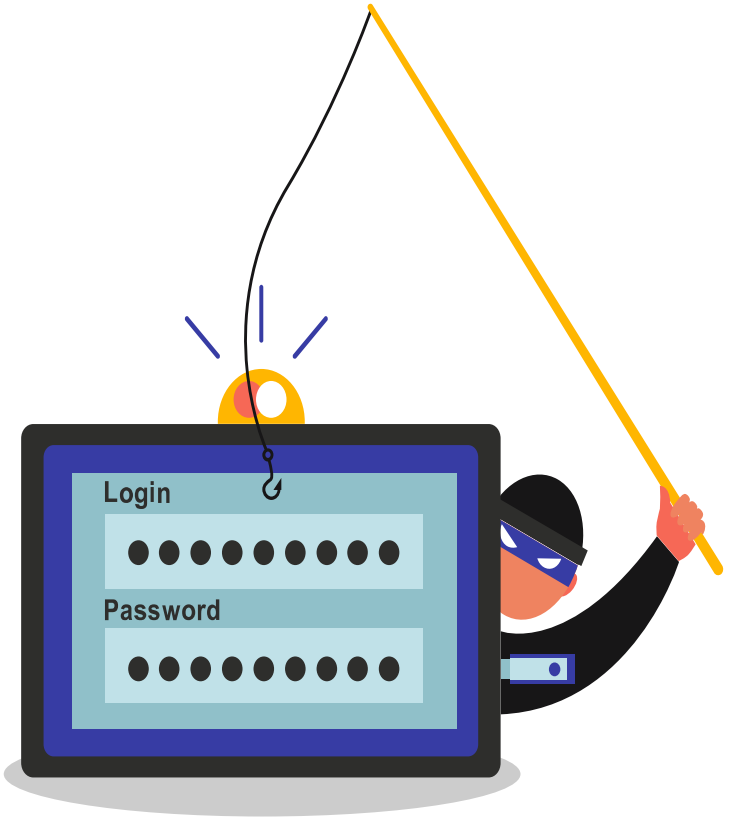
## Rizika

- Automatické generování rizik na základě hrozeb a informačních aktiv
- Kategorizace rizik dle metodiky a správa vlastníky rizik
- Aktualizace hodnocení rizik včetně historie změn
- Vazba na úkoly plánů zvládání rizik
- Automatizovaný výstup pro „Prohlášení o aplikovatelnosti“

# AGENDA ISMS (analýza rizik)

## Bezpečnostní události a incidenty

- Bezpečnostní události
    - Zobrazení vlivu BÚ na aktiva a rizika
    - Notifikace zodpovědných osob
    - Zavedené procesy pro řešení BÚ
- Bezpečnostní incidenty
    - evidence zpracování incidentů
    - výstup hlášení pro NÚKIB
    - evidence incidentů



# AGENDA ISMS (analýza rizik)

## Doplňkové evidence

- Dokumentace
  - Evidence potřebné dokumentace
    - externí
    - Interní – řízená dokumentace
- Audity/neshody
  - evidence auditů a neshod
- Opatření
  - seznam předpisů
  - zodpovědnost vlastníků rizik

# AGENDA ISMS (analýza rizik)

## Doplňkové evidence

- Evidence dodavatelů
    - Evidenční údaje
    - Kategorizace
    - Návaznost na Aktiva
    - Hodnocení bezpečnostních rizik dodavatelů
    - Kategorizace a evidence smluv

# NÁHLED AGENDY ISMS

## Bezpečnostní události

| + Úkol | Typ | Stav | Konec | Prodlení |
|---|---|---|---|---|
| | Bezpečnostní událost | Schváleno | 19.07.2022 10:... | |
| | Bezpečnostní událost | Zrušeno | | |
| | Bezpečnostní událost | Dokončeno | 16.07.2022 00:... | |
| | Bezpečnostní událost | Dokončeno | 09.06.2022 00:... | |
| | Bezpečnostní událost | Dokončeno | 31.08.2022 00:... | |
| | Bezpečnostní událost | Zrušeno | 05.05.2022 00:... | |

## Evidence auditů

| Číslo | Název | Termín od | Termín do |
|---|---|---|---|
| 2017/01 | EMS - Interní audit | | |
| 2017/02 | Vývoj a vydání nových verzí aplikací ... | | |
| 2018/01 | Implementace produktů | | |
| 2018/02 | EMS interní auditnový | | |
| 2020/01 | EMS interní audit | | |
| 2020/02 | Prodej vlastních výrobků a služeb (D... | | |
| 2021/01 | Vývoj d.kurzů | 04.03.2021 | 04.03.2021 |
| 2021/02 | Vývoj DAS | 07.04.2021 | 07.04.2021 |
| 2021/03 | Impementace ISMS | 14.10.2021 | 14.10.2021 |
| 2022/01 | Spuštění ISMS | 14.01.2022 | 14.01.2022 |

## Rizika ISMS

| Číslo hroz... | Název hrozby | Frekvence cíl | Dopad cíl | Zraniteln... | RPN cíl | RPN start | RPN skut... |
|---|---|---|---|---|---|---|---|
| TT03 | **Selhání aplikačního software** | | | | | | |
| TT04 | **Selhání komunikačních služeb** | | | | | | |
| TT06 | **Selhání dodávky el. energie** | | | | | | |
| TT09 | **Ztráta dat** | | | | | | |
| TM02 | **Kybernetický útok z vnější sítě** | | | | | | |
| TM03 | **Útok pomocí sociálního inženýrství nebo špionážních technik** | | | | | | |
| TM04 | **Trvale působící a pokročilé hrozby** | | | | | | |
| TM05 | **Neoprávněný přístup a manipulace s informačním aktivem** | | | | | | |
| TM07 | **Neoprávněné nakládání s osobními údaji** | | | | | | |
| TM09 | **Odposlech a manipulace komunikace** | | | | | | |
| TM10 | **Škodlivé a destruktivní programy** | | | | | | |
| TO01 | **Porušení legislativních požadavků** | | | | | | |
| TO02 | **Porušení smluvních požadavků** | | | | | | |
| TO03 | **Nevhodné nastavení přístupových oprávnění** | | | | | | |
| TO04 | **Nedostatky v nastavení a dokumentaci procesů,** | | | | | | |
| TO07 | **Závady v komunikaci (mezilidské)** | | | | | | |
| TO11 | **Selhání služeb dodavatele** | | | | | | |

# 3. Praxe

# PRAXE

1

## Školení a rozvoj dovedností

- Zajištěné vzdělávaní uživatelů => vyšší bezpečnost

2

## Nástroje a agendy pro KB

- Implementace agendy => fungující procesy v rámci KB

3

## Dokončení realizace a praxe

- Definování prioritních rizik => řízení jejich snižování

DATRON
INFORMATION TECHNOLOGIES

# Jak Vám v tom můžeme pomoci ???

# NAŠE SLUŽBY A ŘEŠENÍ

## Digitalizace úřadu

- Portál občana – online komunikace úřadu
- Formulářové řešení
- Portál úředníka
- Rada a zastupitelstvo (komise a výbory)
- Integrace

## IDM

- Řízený přístup uživatelů
- Licence, implementace a podpora

## Digitalizace procesů/agendy

- ISMS (analýza rizik) pro ZKB
- HelpDesk
- Rezervace aut a zdrojů
- Interní směrnice a další agendy

## Vzdělávání/bezpečnost

- Školení zaměstnanců (kyberbezpečnost)
- Online kurzy
- Evidence školení a jejich realizace

DATRON
INFORMATION TECHNOLOGIES

# Více informací…

jlatal@datron.cz