



KATEDRA
INFORMAČNÍCH
TECHNOLOGIÍ
PEF ČZU V PRAZE

Obec jako správce ISVS pod novými povinnostmi: co udělat hned zítra

Praktický postup pro starosty, tajemníky a úředníky: od evidence systémů po nástrojové řízení bezpečnosti.

Ing. Miroslav Pavelka | Katedra informačních technologií PEF ČZU v Praze

ISSS 2026 | Hradec Králové



Česká
zemědělská
univerzita
v Praze

Hned zítra: první porada na obci

Minimum, které lze zahájit bez velkého projektu a bez čekání na rozpočet.

- 1** Navrhnout garanta(y) ISVS / bezpečnosti
- 2** Ověřit zápisy v AIS RPP a smlouvách
- 3** Sepsat systémy, data, dodavatele a přístupy
- 4** Zkontrolovat zálohy a postup obnovy
- 5** Domluvit („pokusit se“) podporu s ORP, krajem a dodavateli

První schůzka má skončit zápisem: kdo má co zjistit do 14 dnů.



Prvních 180 dnů pro obec jako správce ISVS

Harmonogram pro obec, která začíná od nuly; cílem je prokazatelné řízení § 5b ZoISVS, ne „papír pro papír“.

0-30 dní odpovědnost a rozsah

- rozhodnutí vedení + odpovědná osoba
- seznam systémů a rolí
- AIS RPP / Katalog ISVS
- dodavatelé a nouzové kontakty
- rychlá kontrola záloh a účtů

31-60 dní evidence a závislosti

- evidence ISVS, dat, účtů a smluv
- závislosti: ICT, cloud, eSSL, ISDS
- kritické služby obce
- první C/I/A dopady podle § 5b
- rozdíly RPP vs. skutečnost

61-90 dní rizika a plán opatření

- základní analýza rizik
- priority a plán opatření
- MFA, přístupy, zálohy, incidentní karta
- smluvní mezery a plán oprav
- zápis vedení: kdo / co / kdy / náklady

91-180 dní provedení a důkaz

- realizace prioritních opatření
- test obnovy a revize oprávnění
- školení a poučení vedení
- provozní a bezpečnostní dokumentace
- cílový model ORP / kraj / eGC

Po 90 dnech obec nemusí být „hotová“.

Musí ale vědět, co je ISVS, kdo odpovídá, co je nejrizikovější a jaký plán je schválen.

Do 180 dnů mají být doloženy první výsledky.



Jdeme do hloubky...

*Toto téma a mnoho dalších bude detailně
řešeno v rámci specializovaného semináře
4. června 2026.*



1 | Jmenujte garanta ISVS / bezpečnosti

Někdo musí mít mandát ptát se na systémy, smlouvy, rizika a obnovu.

Garant není nutně „ajták“

Musí mít přístup k vedení obce, smlouvám, dodavatelům a interním uživatelům.

Co má garant dělat

- vést evidenci systémů
- koordinovat přístupy a role
- hlídat smluvní bezpečnost
- připravit obnovu po incidentu
- komunikovat s ORP/krajem/dodavateli

Formálně stačí jednoduché pověření a rozsah pravomocí.

2 | Najděte své ISVS a ověřte role

Evidence v AIS RPP je start, nikoli automaticky pravda. Je třeba ji porovnat se skutečností.



Pravidlo: pokud obec v praxi pouze využívá službu jiného správce, musí to být srozumitelně doložitelné.

3 | Evidence na jednu stránku

Jednoduchá evidence → pokud nejde udržovat, nebude fungovat.

Systém	Agenda/služba	Data (typy)	Role obce (správce / provozovatel / uživatel / žadatel)	Dodavatel (firma / hosting / ORP)	Záloha (ano/ne, frekvence, test?)	Dopad (nízký / střední / vysoký)	Priorita	Poznámky	Právní požadavky (GDPR/archivace)	Garant ISVS	Poslední aktualizace
Spisová služba	Výkon spisové služby	Dokumenty, metadata, osobní údaje	správce	ORP	ano, denně, test 1x ročně	vysoký	1	Vazba na datové schránky a podpisy	GDPR, archivnictví a spisová služba	pracovník spisové služby	18.5.2027
Ekonomika	Účetnictví, rozpočet, faktury	Účetní doklady, smlouvy, osobní a bankovní údaje	správce	firma	ano, denně, test 1x ročně	vysoký	1	Klíčové pro rozpočet, fakturaci a audit	GDPR, archivace dle spisového a skartačního plánu	účetní obce	18.05.2026
Web / portál	Informace občanům, formuláře, kontakty	Obsah, kontakty, formulářová data, statistiky	správce	hosting	ano, týdně, test 1x ročně	střední	2	Kontrola domény, CMS	GDPR, archivace zveřejňovaných dokumentů dle pravidel obce	tajemník	18.05.2026
...											

4 | Roztřídte systémy podle dopadu

Ne všechny systémy zaslouží stejnou pozornost ve stejný den. Prioritizace je jádro přiměřenosti.

Nízký dopad

krátký výpadek neohrozí službu; data nejsou citlivá

Střední dopad

výpadek omezí úřad, ale lze pracovat náhradním postupem

Vysoký dopad

výpadek nebo ztráta integrity zastaví klíčovou službu obce

Začněte systémy, bez kterých nemůžete přijímat podání, vyřizovat spisy, platit závazky nebo prokázat rozhodnutí.

5 | Přístupy a identity

Velká část incidentů začíná slabým nebo sdíleným přístupem.

- ✓ Každý uživatel má vlastní účet; sdílené účty zrušit nebo zdůvodnit.
- ✓ Administrátorské účty oddělit od běžných účtů.
- ✓ Vícefaktorové ověření nasadit alespoň u e-mailu, vzdálených přístupů a administrace.
- ✓ Při odchodu zaměstnance nebo dodavatele odebrat přístupy tentýž den.
- ✓ Jednou za půl roku udělat revizi účtů a oprávnění.

7 | Zálohy a obnova

Záloha, kterou nikdo nezkusil obnovit, je přání. Ne opatření.



Do plánu obnovy napište i náhradní papírový postup pro první den výpadku.

6 | Smlouvy a dodavatelé

Obec si může provoz objednat, ale odpovědnost správce tím sama nezmizí.

Data a umístění	kde jsou data, kdo je drží, jak se předají při ukončení
SLA a obnova	dostupnost, doba obnovy, test obnovy, zálohy
Incidenty	komu a do kdy dodavatel hlásí problém
Subdodavatelé	řetězení povinností na další subjekty
Kontrola	možnost ověřit plnění dohodnutých bezpečnostních pravidel

8 | Incident: první hodina

Kdo neví, komu zavolat, prohrává první hodinu incidentu.



Vytvořte jednu kartu: kontakty, první kroky, náhradní postup, místo pro zápis události.

9 | Informační koncepce a provozní dokumentace

Krátké, živé a použitelné dokumenty mají větší hodnotu než dokonalý šanon.

Informační koncepce OVS

kam se ICT obce vyvíjí a jak je řízeno

Provozní dokumentace ISVS

co systém dělá, jak funguje, kdo jej provozuje

Bezpečnostní dokumentace

dopady CIA, incidenty, bezpečnost sítí, povědomí, kontinuita

Záznamy a smlouvy

důkazy o školení, revizích, zálohách a dodavatelích

Zdroj: vyhláška č. 360/2023 Sb., zejména požadavky na informační koncepci a provozní dokumentaci.

ORP a kraj: co požadovat

Malé obce nemají nést celé bezpečnostní břemeno izolovaně.

- servisní kontakt pro incidenty a obnovu
- sdílené zálohování a základní monitoring
- doporučený standard spisové služby / hostingu
- podporu evidence ISVS a rolí v AIS RPP
- vzorové smluvní doložky pro dodavatele
- společný nástroj nebo portál pro řízení bezpečnosti

Sdílená služba je bezpečnější než tisíce lokálních improvizací.

10 | Bezpečnostní povědomí: tři scénáře

Nejrychlejší přínos má praktický nácvik situací, které se v obci opravdu stanou.

Phishing

podezřelý e-mail, příloha, odkaz,
přihlášení

Platba

změna účtu dodavatele, urgentní
faktura, telefonát

Datová schránka

příchozí dokument, formát,
podatelna, škodlivý kód

Každé školení musí skončit tím, že zaměstnanec ví, komu zavolat a co neudělat.

Vhodný nástroj pro řízení bezpečnosti

Excel je dobrý začátek. Trvalé řízení bezpečnosti ale potřebuje evidenci, úkoly a důkazy na jednom místě.



Aktiva a ISVS	co obec spravuje a používá
Rizika a dopady	co řešit jako první
Úkoly	kdo, co, termín, stav
Dodavatelé	smlouvy, SLA, kontakty, incidenty
Důkazy	školení, revize, testy obnovy, záznamy

Doporučení: pořídte nebo sdíleně využívejte nástroj, který vede obec krok za krokem a ukládá důkazy plnění.

Vhodný nástroj pro řízení bezpečnosti

Excel je dobrý začátek. Trvalé řízení bezpečnosti ale potřebuje evidenci, úkoly a důkazy na jednom místě.



Aktiva a ISVS

co obec spravuje a používá

Rizika a dopady

co řešit jako první

Úkoly

kdo, co, termín, stav

Dodavatelé

smlouvy, SLA, kontakty,
incidenty

Důkazy

školení, revize, testy
obnovy, záznamy

Doporučení: pořídte nebo sdíleně využívejte nástroj, který vede obec krok za krokem a ukládá důkazy plnění.

Kritéria nástroje pro obec / ORP / kraj

PODKLAD

Podklad pro následné rozhodnutí a případné zadání veřejné zakázky.

- ✓ evidence ISVS, služeb, dat, dodavatelů a smluvních vazeb
- ✓ jednoduché hodnocení dopadů a rizik podle C/I/A (důvěrnost / integrita / dostupnost)
- ✓ přehled bezpečnostních opatření a úkolů v čase
- ✓ vzory dokumentů a možnost jejich exportu pro kontrolu
- ✓ evidence školení, revizí přístupů, záloh a incidentů
- ✓ multitenantní provoz pro ORP/kraj a jejich obce
- ✓ jasné oddělení odpovědnosti správce, provozovatele a dodavatele
- ✓ nízká administrativní náročnost pro malé obce



Minimum dokumentů, které má smysl udržovat

PODKLAD

Dokumenty mají pomáhat v provozu a při kontrole; ne existovat samy pro sebe.

- 1 Evidence ISVS, dat a dodavatelů
- 2 Pověření garanta a popis rolí
- 3 Jednoduché hodnocení dopadů / rizik
- 4 Pravidla přístupů a revizí oprávnění
- 5 Plán záloh a obnovy
- 6 Incidentní karta a evidence událostí
- 7 Záznamy o školení a kontrolách
- 8 Smluvní doložky a kontakty dodavatelů



Zítřejší checklist

Osm úkolů, které lze začít bez čekání na nový projekt.

- ✓ Jmenovat garanta ISVS / bezpečnosti.
- ✓ Stáhnout přehled ISVS z AIS RPP a porovnat se skutečností.
- ✓ Založit evidenci systémů, dat, dodavatelů a kontaktů.
- ✓ Vybrat systémy s nejvyšším dopadem na chod obce.
- ✓ Prověřit účty, administrátory a odebrání starých přístupů.
- ✓ Ověřit, že existuje použitelná záloha a kdo ji obnoví.
- ✓ Doplnit incidentní kartu: první hodina, kontakty, náhradní provoz.
- ✓ Zahájit jednání s ORP/krajem o sdíleném nástroji a službách.

Cílem prvního dne je zahájit řízení. Ne vyřešit celou kybernetickou bezpečnost.

Zdroje a doporučené materiály

PODKLAD

Pro následné čtení a praktickou implementaci.

Pavelka, M.; Jarolímek, J.: Nové povinnosti tisíců obcí v oblasti bezpečnosti po novele ZoISVS. Sborník ISSS 2026.
DIA: Metodický pokyn k aplikaci § 5b zákona č. 365/2000 Sb.
NÚKIB: Manuál pro poskytovatele regulovaných služeb v režimu nižších povinností; podpůrné materiály pro obce.
Vyhláška č. 410/2025 Sb. — bezpečnostní opatření v režimu nižších povinností.
Vyhláška č. 360/2023 Sb. — dlouhodobé řízení ISVS; Národní architektonický plán.

Podklady pro právní a metodický kontext prezentace.

Pavelka, M.; Jarolímek, J.: Nové povinnosti tisíců obcí v oblasti bezpečnosti po novele ZoISVS. Sborník ISSS 2026.
Zákon č. 264/2025 Sb., o kybernetické bezpečnosti; zákon č. 265/2025 Sb.; zákon č. 365/2000 Sb.
Vyhlášky č. 408/2025 Sb., 410/2025 Sb., 411/2025 Sb., 412/2025 Sb.; vyhláška č. 360/2023 Sb.
DIA: Metodický pokyn k aplikaci § 5b ZoISVS. NÚKIB: podpůrné materiály a manuál pro nižší režim.
AIS RPP Působnostní / Katalog ISVS.
Národní architektonický plán a archi.gov.cz.



Zabezpečení organizace je jako cibule.

Má spoustu vrstev a když se dostanete až doprostřed, chce se vám brečet.



Bezpečnost je celek.

Každá vrstva má svůj význam.
Společně chrání to nejcennější – naši organizaci.



Řízení kybernetické bezpečnosti

OAD Open Apps
Development

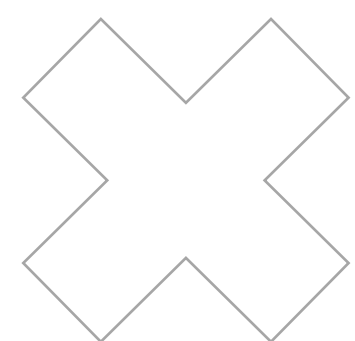
Kybernetická bezpečnost \neq IT

HW, SW a správa IT jen pomáhají zvýšit KB



- Manažerské řízení procesů
- Osoby znalé konkrétní oblasti (garanti)
- IT je část celku
- Odpovědnost vedení organizace
- **Nástroje pro komplexní řízení**
- **Lidské zdroje**

Aktuální stav řízení KB



Excel vs. nástroj

The image shows three overlapping Excel spreadsheets, each with a green 'X' icon. The top spreadsheet is an 'Aspect Identification Register' with columns for Aspect Category, Aspect Description, Risk Significance, and Compliance. The middle spreadsheet is a 'Portfolio return and risk' sheet with columns for TSLA, AMZN, and NFLX, showing weights and returns. The bottom spreadsheet is an 'IT RISK ANALYSIS TEMPLATE' with columns for Category/Threat, Risk or Hazard Description, Vulnerability, Assets and Consequences, Risk, IT Solution, Business Impacted, Existing Control Measures, Risk Probability, Risk Impact, Risk Rating, and Prevention Measures.

The image shows a screenshot of a risk management dashboard. On the left is a navigation menu with items like 'Přehled', 'Aktiva', 'Seznam aktiv', 'Mapa aktiv', 'Rizika', 'Seznam rizik', 'Mapa rizik', 'Zvládní rizik', 'Organizační struktura', 'Dodavatelé', 'Úkoly a události', 'Seznam událostí', 'Kalendář', 'Výstupy', 'Zjištění', 'BU / BI', 'Dokumentace', and 'Audit'. The main content area includes a calendar for 'září 2025', a 'Díleč zvládní rizik' pie chart, a 'Rizika' pie chart, a table of 'Primární aktiva s největším rizikem', and two 'Opatření' pie charts. The table lists assets with IDs, names, and risk levels.

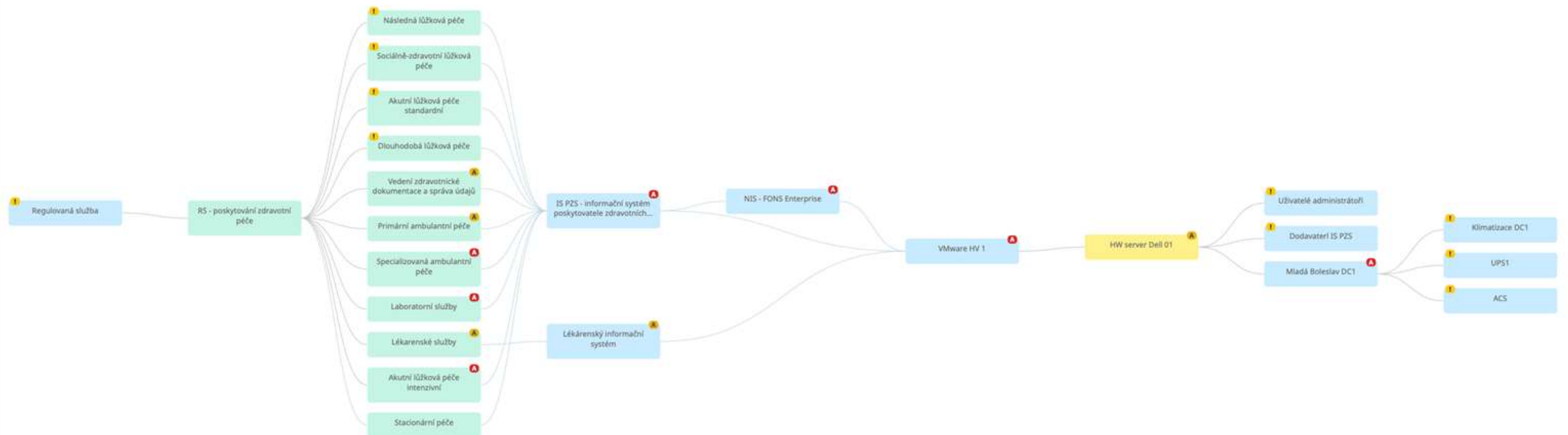
ID	NÁZEV	GARANT	RIZIKO
A-47	Synology (NAS)	Kamala Fešná (kfe@nmc.cz)	velké
A-19	Uživatelské vedoucí lékaři	Alena Bůčková (ab@nmc.cz)	střední
A-47	Synology (NAS)	Kamala Fešná (kfe@nmc.cz)	velké

Východí hodnocení rizik ve stávajícím prostředí v případě výsotěžemi prvky společnosti uvedených ve varování NUKIB														Varianta A: Hodnocení rizik ve stávajícím prostředí v případě výsotěžemi prvky společnosti uvedených ve varování NUKIB a dodatečnými opatřeními						Varianta B: Hodnocení rizik ve stávajícím prostředí v případě, že budou vyloučeny prvky společnosti uvedených ve varování NUKIB																		
ID	Aktivum	Hodnota dopadu - dostupnost	Hodnota dopadu - důvěrnost	Hodnota dopadu - integrita	Zranitelnost	Hodnota zranitelnosti	Hroba	Hodnota hroby	Hodnota rizika - dostupnost	Hodnota rizika - důvěrnost	Hodnota rizika - integrita	Hodnota rizika - dostupnost	Úroveň zvládnutí rizika	Komentář	Opatření	A	Hodnota dopadu - dostupnost (A)	Hodnota dopadu - důvěrnost (A)	Hodnota dopadu - integrita (A)	Hodnota zranitelnosti (A)	Hodnota rizika - dostupnost (A)	Hodnota rizika - důvěrnost (A)	Hodnota rizika - integrita (A)	B	Hodnota dopadu - dostupnost (B)	Hodnota dopadu - důvěrnost (B)	Hodnota dopadu - integrita (B)	Zranitelnost (B)	Hodnota rizika - dostupnost (B)	Hodnota rizika - důvěrnost (B)	Hodnota rizika - integrita (B)	Úroveň zvládnutí rizika (B)	Komentář (B)					
R1	POI: Switch (přepínač)	3	2	3	Z1: Nedostatečná údržba aktiv	3	H1: Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany	2	18	12	18	Sledování	-	-	-	3	2	3	3	2	18	12	18	Sledování	-	-	-	3	2	3	3	2	18	12	18	Sledování	-	
R2	POI: Switch (přepínač)	3	Nerelevantní	3	Z1: Nedostatečná údržba aktiv	3	H2: Poškození nebo selhání technického nebo programového vybavení	4	36	Nerelevantní	36	Redukce	-	Varianta A - OP2; OP4 Varianta B - OP1	-	3	Nerelevantní	3	3	4	36	Nerelevantní	36	Redukce	-	V rámci VZ nelze snížit toto riziko dalšími bezpečnostními opatřeními.	3	Nerelevantní	3	3	2	18	Nerelevantní	18	Sledování	-		
R3	POI: Switch (přepínač)	3	2	3	Z1: Nedostatečná údržba aktiv	3	H3: Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých	4	36	24	36	Redukce	-	-	-	3	2	3	3	4	36	24	36	Redukce	-	V rámci VZ nelze snížit toto riziko dalšími bezpečnostními opatřeními.	3	2	3	3	2	18	12	18	Sledování	-		
R4	POI: Switch (přepínač)	3	2	3	Z1: Nedostatečná údržba aktiv	3	H5: Působení škodlivého kódu (například viny, spyware, trojské koně)	4	36	24	36	Redukce	-	-	Varianta A - OP3; OP4 Varianta B - OP1	-	3	2	3	3	4	36	24	36	Redukce	-	V rámci VZ nelze snížit toto riziko dalšími bezpečnostními opatřeními.	3	2	3	3	2	18	12	18	Sledování	-	
R5	POI: Switch (přepínač)	3	Nerelevantní	3	Z1: Nedostatečná údržba aktiv	3	H7: Přerušení poskytování služeb elektronických komunikací nebo	2	18	Nerelevantní	18	Sledování	-	-	-	3	Nerelevantní	3	3	2	18	Nerelevantní	18	Sledování	-	-	-	3	Nerelevantní	3	3	2	18	Nerelevantní	18	Sledování	-	
R6	POI: Switch (přepínač)	3	Nerelevantní	3	Z1: Nedostatečná údržba aktiv	3	H8: Zneužití nebo neoprávněná modifikace údajů	4	36	24	36	Redukce	-	-	Varianta A - OP3; OP4; OP5 Varianta B - OP1	-	3	2	3	3	4	36	24	36	Redukce	-	V rámci VZ nelze snížit toto riziko dalšími bezpečnostními opatřeními.	3	2	3	3	2	18	12	18	Sledování	-	
R7	POI: Switch (přepínač)	3	2	3	Z1: Nedostatečná údržba aktiv	3	H9: Ztráta, odcizení nebo poškození aktiva	4	36	24	Nerelevantní	Redukce	-	-	Varianta A - OP2; OP3; OP4; OP5 Varianta B - OP1	-	3	2	Nerelevantní	3	4	36	24	Nerelevantní	Redukce	-	V rámci VZ nelze snížit toto riziko dalšími bezpečnostními opatřeními.	3	2	Nerelevantní	3	2	18	12	Nerelevantní	Sledování	-	
R8	POI: Switch (přepínač)	3	2	3	Z1: Nedostatečná údržba aktiv	3	H11: Pochybení ze strany	2	18	12	18	Sledování	-	-	-	3	2	3	3	2	18	12	18	Sledování	-	-	-	3	2	3	3	2	18	12	18	Sledování	-	
R9	POI: Switch (přepínač)	3	2	3	Z1: Nedostatečná údržba aktiv	3	H12: Zneužití vnitřních prostředků, sabotáž	4	36	24	36	Redukce	-	-	Varianta A - OP3; OP4 Varianta B - OP1	-	3	2	3	3	4	36	24	36	Redukce	-	V rámci VZ nelze snížit toto riziko dalšími bezpečnostními opatřeními.	3	2	3	3	2	18	12	18	Sledování	-	
R10	POI: Switch (přepínač)	3	2	3	Z1: Nedostatečná údržba aktiv	3	H13: Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých	4	36	Nerelevantní	Nerelevantní	Redukce	-	-	Varianta A - OP2; OP4 Varianta B - OP1	-	3	Nerelevantní	Nerelevantní	3	4	36	Nerelevantní	Nerelevantní	Redukce	-	V rámci VZ nelze snížit toto riziko dalšími bezpečnostními opatřeními.	3	Nerelevantní	Nerelevantní	3	2	18	Nerelevantní	Nerelevantní	Sledování	-	
R11	POI: Switch (přepínač)	3	2	3	Z1: Nedostatečná údržba aktiv	3	H14: Členy kybernetický útok pomocí sociálního inženýrství, použití špiónských technik	4	36	24	36	Redukce	-	-	Varianta A - OP2; OP3; OP4; OP5 Varianta B - OP1	-	3	2	3	3	4	36	24	36	Redukce	-	V rámci VZ nelze snížit toto riziko dalšími bezpečnostními opatřeními.	3	2	3	3	2	18	12	18	Sledování	-	
R12	POI: Switch (přepínač)	Nerelevantní	2	Nerelevantní	Z1: Nedostatečná údržba aktiv	3	H15: Zneužití výměnitelných	4	Nerelevantní	24	Nerelevantní	Redukce	-	-	Varianta A - OP5; OP6 Varianta B - OP1	-	Nerelevantní	2	Nerelevantní	3	4	Nerelevantní	24	Nerelevantní	Sledování	-	-	-	Nerelevantní	2	Nerelevantní	3	2	Nerelevantní	12	Nerelevantní	Akceptace	-
R13	POI: Switch (přepínač)	Nerelevantní	2	3	Z1: Nedostatečná údržba aktiv	3	H16: Napadení elektronické komunikace (odposlech, modifikace)	4	Nerelevantní	24	36	Redukce	-	-	Varianta A - OP2; OP3; OP4; OP5 Varianta B - OP1	-	Nerelevantní	2	3	3	4	Nerelevantní	24	36	Redukce	-	V rámci VZ nelze snížit toto riziko dalšími bezpečnostními opatřeními.	Nerelevantní	2	3	3	2	Nerelevantní	12	18	Sledování	-	
R14	POI: Switch (přepínač)	3	2	3	Z2: Zastaralost aktiv	2	H1: Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany	2	12	8	12	Akceptace	-	-	-	3	2	3	2	2	12	8	12	Akceptace	-	-	-	3	2	3	2	2	12	8	12	Akceptace	-	
R15	POI: Switch (přepínač)	3	Nerelevantní	3	Z2: Zastaralost aktiv	2	H2: Poškození nebo selhání technického nebo programového vybavení	4	24	Nerelevantní	24	Sledování	-	-	-	3	Nerelevantní	3	2	4	24	Nerelevantní	24	Sledování	-	-	-	3	Nerelevantní	3	2	2	12	Nerelevantní	12	Akceptace	-	
R16	POI: Switch (přepínač)	3	2	3	Z2: Zastaralost aktiv	2	H5: Působení škodlivého kódu (například viny, spyware, trojské koně)	4	24	16	24	Sledování	-	-	-	3	2	3	2	4	24	16	24	Sledování	-	-	-	3	2	3	2	2	12	8	12	Akceptace	-	
R17	POI: Switch (přepínač)	3	2	3	Z2: Zastaralost aktiv	2	H7: Přerušení poskytování služeb elektronických komunikací nebo	2	12	Nerelevantní	12	Akceptace	-	-	-	3	Nerelevantní	3	2	2	12	Nerelevantní	12	Akceptace	-	-	-	3	Nerelevantní	3	2	2	12	Nerelevantní	12	Akceptace	-	
R18	POI: Switch (přepínač)	3	2	3	Z2: Zastaralost aktiv	2	H8: Zneužití nebo neoprávněná modifikace údajů	4	24	16	24	Sledování	-	-	-	3	2	3	2	4	24	16	24	Sledování	-	-	-	3	2	3	2	2	12	8	12	Akceptace	-	
R19	POI: Switch (přepínač)	3	2	3	Z2: Zastaralost aktiv	2	H9: Ztráta, odcizení nebo poškození aktiva	4	24	16	Nerelevantní	Sledování	-	-	-	3	2	Nerelevantní	2	4	24	16	Nerelevantní	Sledování	-	-	-	3	2	Nerelevantní	2	2	12	8	Nerelevantní	Akceptace	-	
R20	POI: Switch (přepínač)	3	2	3	Z2: Zastaralost aktiv	2	H11: Pochybení ze strany	2	12	8	12	Akceptace	-	-	-	3	2	3	2	2	12	8	12	Akceptace	-	-	-	3	2	3	2	2	12	8	12	Akceptace	-	
R21	POI: Switch (přepínač)	3	2	3	Z2: Zastaralost aktiv	2	H12: Zneužití vnitřních prostředků, sabotáž	4	24	16	24	Sledování	-	-	-	3	2	3	2	4	24	16	24	Sledování	-	-	-	3	2	3	2	2	12	8	12	Akceptace	-	
R22	POI: Switch (přepínač)	3	Nerelevantní	3	Z2: Zastaralost aktiv	2	H13: Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých	4	24	Nerelevantní	Nerelevantní	Sledování	-	-	-	3	Nerelevantní	Nerelevantní	2	4	24	Nerelevantní	Nerelevantní	Sledování	-	-	-	3	Nerelevantní	Nerelevantní	2	2	12	Nerelevantní	Nerelevantní	Akceptace	-	
R23	POI: Switch (přepínač)	3	2	3	Z2: Zastaralost aktiv	2	H14: Členy kybernetický útok pomocí sociálního inženýrství, použití špiónských technik	4	24	16	24	Sledování	-	-	-	3	2	3	2	4	24	16	24	Sledování	-	-	-	3	2	3	2	2	12	8	12	Akceptace	-	
R24	POI: Switch (přepínač)	Nerelevantní	2	3	Z2: Zastaralost aktiv	2	H15: Zneužití výměnitelných	4	Nerelevantní	16	Nerelevantní	Akceptace	-	-	-	Nerelevantní	2	Nerelevantní	2	4	Nerelevantní	16	Nerelevantní	Akceptace	-	-	-	Nerelevantní	2	Nerelevantní	2	2	2	Nerelevantní	8	Nerelevantní	Akceptace	-
R25	POI: Switch (přepínač)	Nerelevantní	2	3	Z2: Zastaralost aktiv	2	H16: Napadení elektronické komunikace (odposlech, modifikace)	4	Nerelevantní	16	24	Sledování	-	-	-	Nerelevantní	2	3	2	4	Nerelevantní	16	24	Sledování	-	-	-	Nerelevantní	2	3	2	2	2	Nerelevantní	8	12	Akceptace	-
R26	POI: Switch (přepínač)	3	2	3	Z3: Nedostatečná ochrana perimetru	2	H1: Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany	2	12	8	12	Akceptace	-	-	-	3	2	3	2	2	12	8	12	Akceptace	-	-	-	3	2	3	2	2	12	8	12	Akceptace	-	
R27	POI: Switch (přepínač)	3	Nerelevantní	3	Z3: Nedostatečná ochrana perimetru	4	H2: Poškození nebo selhání technického nebo programového vybavení	4	48	Nerelevantní	48	Redukce	-	-	Varianta A - OP2; OP4 Varianta B - OP1	-	3	Nerelevantní	3	1	4	12	Nerelevantní	12	Akceptace	-	-	-	3	Nerelevantní	3	2	2	12	Nerelevantní	12	Akceptace	-
R28	POI: Switch (přepínač)	3	2	3	Z3: Nedostatečná ochrana perimetru	4	H5: Působení škodlivého kódu (například viny, spyware, trojské koně)	4	48	32	48	Redukce	-	-	Varianta A - OP3; OP4 Varianta B - OP1	-	3	2	3	1	4	12	8	12	Akceptace	-	-	-	3	2	3	2	2	12	8	12	Akceptace	-
R29	POI: Switch (přepínač)	3	2	3	Z3: Nedostatečná ochrana perimetru	2	H7: Přerušení poskytování služeb elektronických komunikací nebo	2	12	Nerelevantní	12	Akceptace	-	-	-	3	Nerelevantní	3	2	2	12	Nerelevantní	12	Akceptace	-	-	-	3	Nerelevantní	3	2	2	12	Nerelevantní	12	Akceptace	-	
R30	POI: Switch (přepínač)	3	2	3	Z3: Nedostatečná ochrana perimetru	4	H8: Zneužití nebo neoprávněná modifikace údajů	4	48	32	48	Redukce	-	-	Varianta A - OP3; OP4; OP5 Varianta B - OP1	-	3	2	3	1	4	12	8	12	Akceptace	-	-	-	3	2	3	2	2	12	8	12	Akceptace	-
R31	POI: Switch (přepínač)	3	2	Nerelevantní	Z3: Nedostatečná ochrana perimetru	4	H9: Ztráta, odcizení nebo poškození aktiva	4	48	32	Nerelevantní	Redukce	-	-	Varianta A - OP2; OP3; OP4; OP5 Varianta B - OP1	-	3	2	Nerelevantní	1	4	12	8	Nerelevantní	Akceptace	-	-	-	3	2	Nerelevantní	2	2	12	8	Nerelevantní	Akceptace	-
R32	POI: Switch (přepínač)	3	2	3	Z3: Nedostatečná ochrana perimetru	2	H11: Pochybení ze strany	2	12	8	12	Akceptace	-	-	-	3	2	3	2	2	12	8	12	Akceptace	-	-	-	3	2	3	2	2	12	8	12	Akceptace	-	
R33	POI: Switch (přepínač)	3	2	3	Z3: Nedostatečná ochrana perimetru	4	H12: Zneužití vnitřních prostředků, sabotáž	4	48	32	48	Redukce	-	-	Varianta A - OP3; OP4 Varianta B - OP1	-	3	2	3	1	4	12	8	12	Akceptace	-	-	-	3	2	3	2	2	12	8	12	Akceptace	-
R34	POI: Switch (přepínač)	3	Nerelevantní	3	Z3: Nedostatečná ochrana perimetru	4	H13: Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých	4	48	Nerelevantní	Nerelevantní	Redukce	-	-	Varianta A - OP2; OP4 Varianta B - OP1	-	3	Nerelevantní	Nerelevantní	1	4	12	Nerelevantní	Nerelevantní	Akceptace	-	-	-	3	Nerelevantní	Nerelevantní	2	2	12	Nerelevantní	Nerelevantní	Akceptace	-
R35	POI: Switch (přepínač)	3	2	3	Z3: Nedostatečná ochrana perimetru	4	H14: Členy kybernetický útok pomocí sociálního inženýrství, použití špiónských technik	4	48	32	48	Redukce	-	-	Varianta A - OP2; OP3; OP4; OP5 Varianta B - OP1	-	3	2	3	1	4	12	8	12	Akceptace	-	-	-	3	2	3	2	2					

(Ne)Přehlednost

Excel neumí reálně zachytit a zobrazit víceúrovňové vazby mezi aktivy

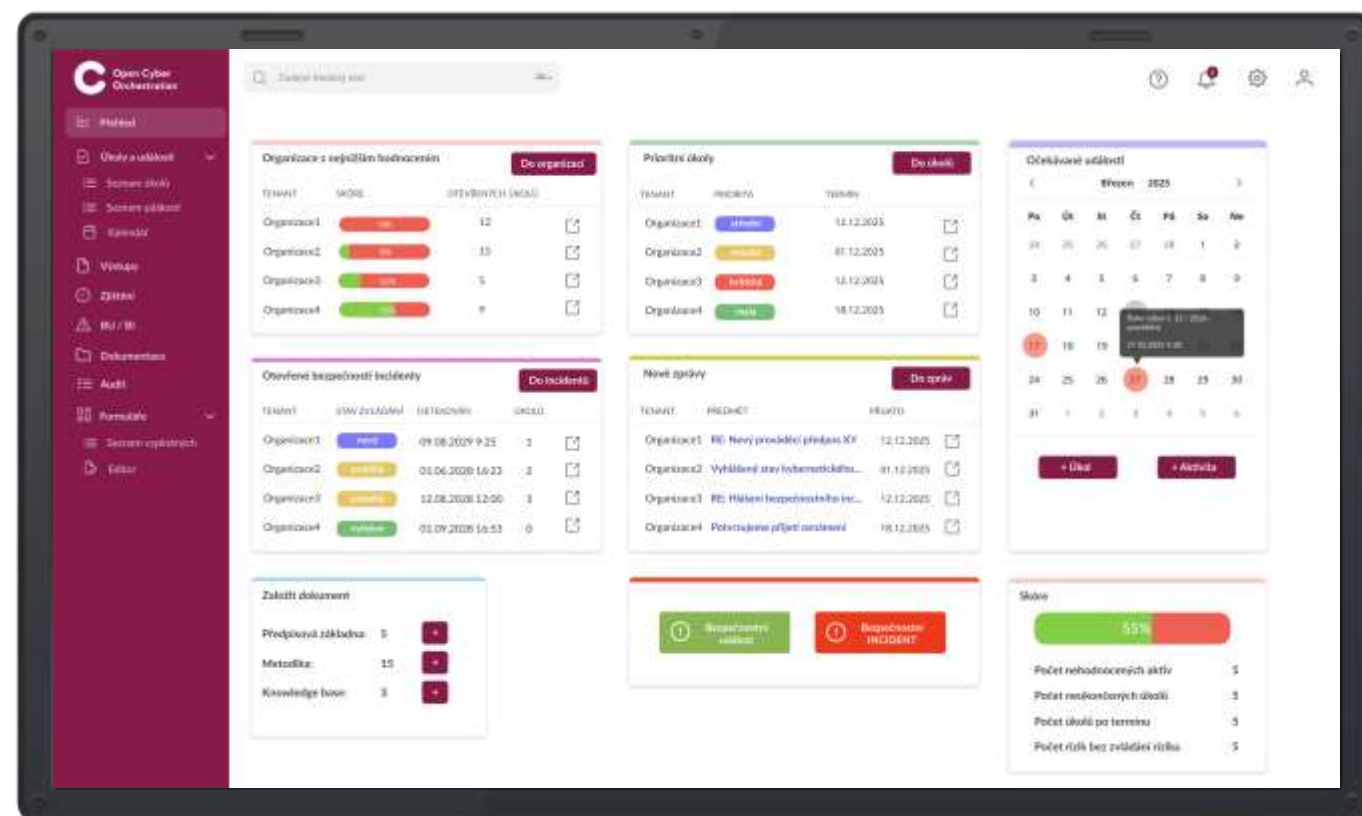
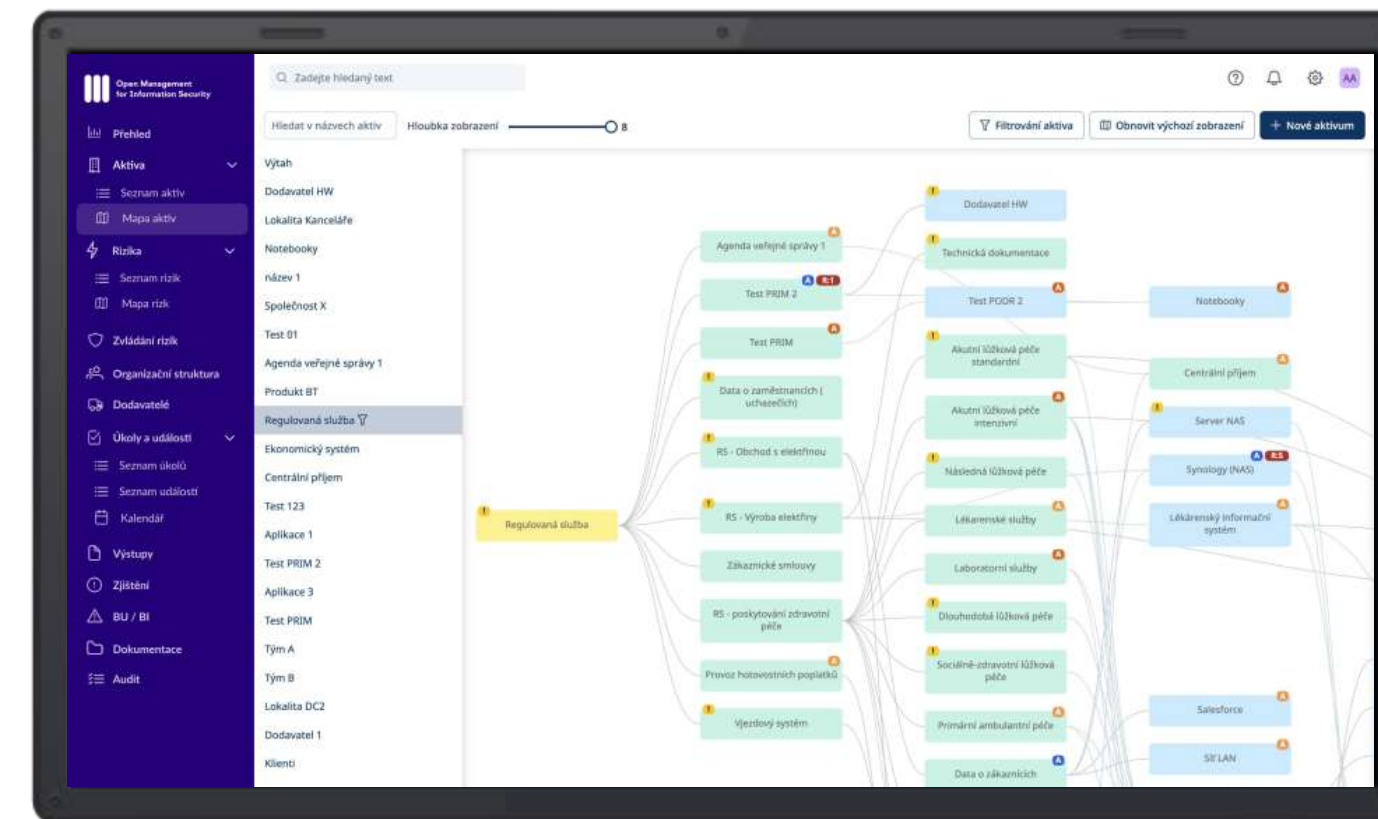
primární → podpůrná → podpůrná → podpůrná aktiva





Manažerské řízení KB

- Interaktivní mapa aktiv a rizik
- Bezpečnostní události a incidenty
- Generování dokumentů ZHR, POA, PZR
- Správa katalogů hrozeb, zranitelností, opatření, lokalit, dodavatelů
- Auditní záznam změn
- Komunikace s regulátorem



Komplexní řízení KB v rámci celé organizace

- Sledování úkolů napříč všemi OMIS tenanty
- Hlídání termínů a eskalační scénáře
- Automatické upozornění a notifikace
- Flexibilní řízení termínů a odpovědností osob a týmů
- Hlídání povinností dle legislativy – přezkumy, audity, analýzy
- Automatické vyplňování formulářů, hlášení, auditní stopa a výstupy (NÚKIB)



Málo času, hodně informací, potkejme se na stánku **č.6**

OCO

OMIS



Odborný seminář pořádaný ve spolupráci Českou zemědělskou univerzitou v Praze

Témata:

- Legislativa vyšších i nižších povinností
- Implementace směrnic a SW v rámci řízení kybernetické bezpečnosti – praktické ukázky
- Reálné zkušenosti po kybernetickém útoku a jak dále postupovat
- Řešení kybernetické bezpečnosti v organizaci od identifikace až po řízení
- Služby a nástroje vhodné pro řešení kybernetické bezpečnosti v organizaci

Program:

9:30 – 10:00	Příjezd, registrace, občerstvení
10:00 – 12:00	1. blok odborných přednášek vč. přestávky a občerstvení
12:00 – 13:00	Oběd
13:00 – 16:30	2. blok odborných přednášek vč. přestávek a občerstvení
16:30 – 17:00	Diskuze
18:00 -	Raut + neformální diskuze, bowling + vyhlášení vítězů

Před seminářem bude registrovaným účastníkům odeslán přesný program přednášek a jmenný seznam odborných řečníků z oblasti governmentu, legislativy a kybernetické bezpečnosti.

Termín: 4. června 2026

Místo: Hotel Akademie Naháč

Komorní Hrádek 277, 257 24 Chocerady (D1 exit 29)

www.hotelnahac.cz

Seminář je určený pro: obce, města, kraje, nemocnice, zřizované organizace

Omezená kapacita semináře, případné ubytování je zajištěno.

 **Registrační formulář**



Kontakt: Petr Danielovský, +420 602 790 136, petr.danielovsky@openapps.cz

Partneři semináře:





Děkujeme za pozornost

Vlasta Šejvlová – vlasta.sejvlova@openapps.cz

Miroslav Pavelka – pavelka@pef.czu.cz

www.openapps.cz



KATEDRA
INFORMAČNÍCH
TECHNOLOGIÍ
PEF ČZU V PRAZE