

## Partner konferencie KYBERNETICKÁ BEZPEČNOSŤ 2023



### KYBERNETICKÁ BEZPEČNOSŤ, OCHRANA OSOBNÝCH ÚDAJOV, WHISTLEBLOWING, eLEARNING, FYZICKÁ A OBJEKTOVÁ BEZPEČNOSŤ v rokoch 2023 - 2024

K riadeniu kybernetickej bezpečnosti v organizácii sa môže pristupovať formálnym spôsobom, ktorý predstavuje vytvorenie množstva rôznych dokumentov, tabuliek, podkladov, smerníc a statických analýz, alebo kontrahovať expertov pracujúcich prevažne s excelovskými tabuľkami vytvárajúcimi statické analýzy rizík, alebo – pracovať účelne, systémovo a efektívne prostredníctvom špeciálnych modulov softvérovej aplikácie a s pomocou nej riadiť on-line proces analýzy rizík v oblasti kybernetickej bezpečnosti v organizácii.



Automatizované riadenie | Dosiahnutie finančných úspor  
Legislatívny súlad | Moderné riešenie | Optimalizácia

# **STRUČNÁ ANOTÁCIA MODULOV APLIKÁCIE ISIT SOFTWARE SK/CZ PRE SAMOSTATNÉ RIADENIE PROCESOV BEZPEČNOSTI V ORGANIZÁCII**

## **Modul KBO**



Komplexný nástroj pre riadenie kybernetickej bezpečnosti, ochrana kľúčových aktív definovanými opatreniami s riadením rizík, priama komunikácia NBU/NUKIB.

## **Modul GDPR s väzbami posúdenia DPIA**



Komplexné detailné riadenie bezpečnosti osobných údajov súladné so zmenami v legislatíve, interným auditom, personálnou bezpečnosťou ai.

## **Modul Whistleblowing s riadením korupčných rizík**



Bezpečnosť dát a garantovaná dôvernosť - ochrana identity Oznamovateľa s riadeným procesom vyšetrenia oznamenia.

## **Modul Fyzická a objektová bezpečnosť**



Prierezové riadenie fyzickej a objektovej bezpečnosti naprieč procesmi v organizácii (personálna bezpečnosť, riadenie 3 strán, opatrenia FOB - kamerové systémy, kľúčový poriadok, riadenie aktív FOB atď. – vhodné pre odbory bezpečnosti a kríz. riadenia, obecné polície, SBS ai.).

## **Modul E-learning**



Vzdelávací nástroj na budovanie a udržiavanie bezpečnostného povedomia v organizácii vrátane testovania užívateľov a generovania osvedčenia o úspešnom absolvovaní.

## **BEZPEČNOSTNÝ PORTÁL ISIT**



Web aplikáčna časť pre nahlasovanie bezpečnostných udalostí s manažmentom bezpečnostných incidentov (GDPR, KBO) a ďalších informácií prístupná len pre oprávnené osoby a vlastníkov aktív organizácie. Umiestnenie na webovom sídle organizácie s riadeným prístupom.



## MODUL KYBERNETICKÁ BEZPEČNOSŤ - KBO

### 3 hlavné dôvody prečo riadiť kybernetickú bezpečnosť softvérom:

1. Softvér predstavuje výkonný nástroj pre riadenie kybernetickej a informačnej bezpečnosti informačných systémov prevádzkujúcich základnú službu v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, ako aj informačných systémov verejnej správy v zmysle zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov.
2. Softvér zabezpečuje on-line riadenie procesu analýzy rizík, automaticky prispôsobuje analýzu rizík na realizáciu jednotlivých opatrení, ktoré sú zavádzané priebežne v zmysle plánu implementácie navrhovaných bezpečnostných opatrení.
3. Softvér pomáha v prípade budovania nových informačných systémov alebo ich častí analyzovať vo fáze návrhu jednotlivé prvky pripravovanej architektúry z hľadiska bežných kybernetických a informačných hrozieb a navrhovať potrebné eliminačné bezpečnostné opatrenia

### FUNKCIONALITA MODULU KBO :

- Komplexné riadenie procesov, vedenie evidencií a generovanie tlačových výstupov
- Obsahuje Automatizovanú analýzu rizík s možnosťou výberu zo 4 bezpečnostných modelov s namapovanými kolekciami opatrení ku konkrétnym hrozbám pre jednotlivé aktíva/skupiny aktív (best practices, podľa zákona č. 69/2018 o kybernetickej bezpečnosti, podľa zákona č. 95/2019 o ITVS a vyhlášky č. 362/2018 Z. o obsahu bezpečnostných opatrení, obsahu a štruktúre bezpečnostnej dokumentácie, podľa ISO/IEC 27xxx)
- Kolekcie aktív, resp. skupiny aktív obsahujú nielen aktíva informačných technológií, ale aj aktíva tzv. OT systémov (operational technologies, v odbornej terminológii označované aj ako ICS – Industrial Control System alebo IACS – Industrial Automation and Control Systems).
- Komplexný incident manažment s generovaním hlásenia o bezp. incidente
- Samostatné riadenie personálnej bezpečnosti.
- Riadenie tretích strán pristupujúce k informačno-komunikačným technológiám organizácie
- Aplikácia je škálovateľná ako konzola pre manažéra KB, ale zároveň je pripravená na komplexné riadenie KB so zapojením všetkých vlastníkov aktív, rizík až po riadiace zložky (admin/klient). Eliminuje potrebu trvalej prítomnosti externých poradcov na bezpečnosť, čím znižuje náklady a zároveň udržiava súlad riadenia KB s platnou legislatívou.
- Evidencia a riadenie aktív informačno-komunikačných technológií, resp. v rozsahu potrebnom pre ISMS (Systém riadenia bezpečnosti informácií - Information Security Management System - ISMS) v organizácii

## VÝHODY MODULU KBO:

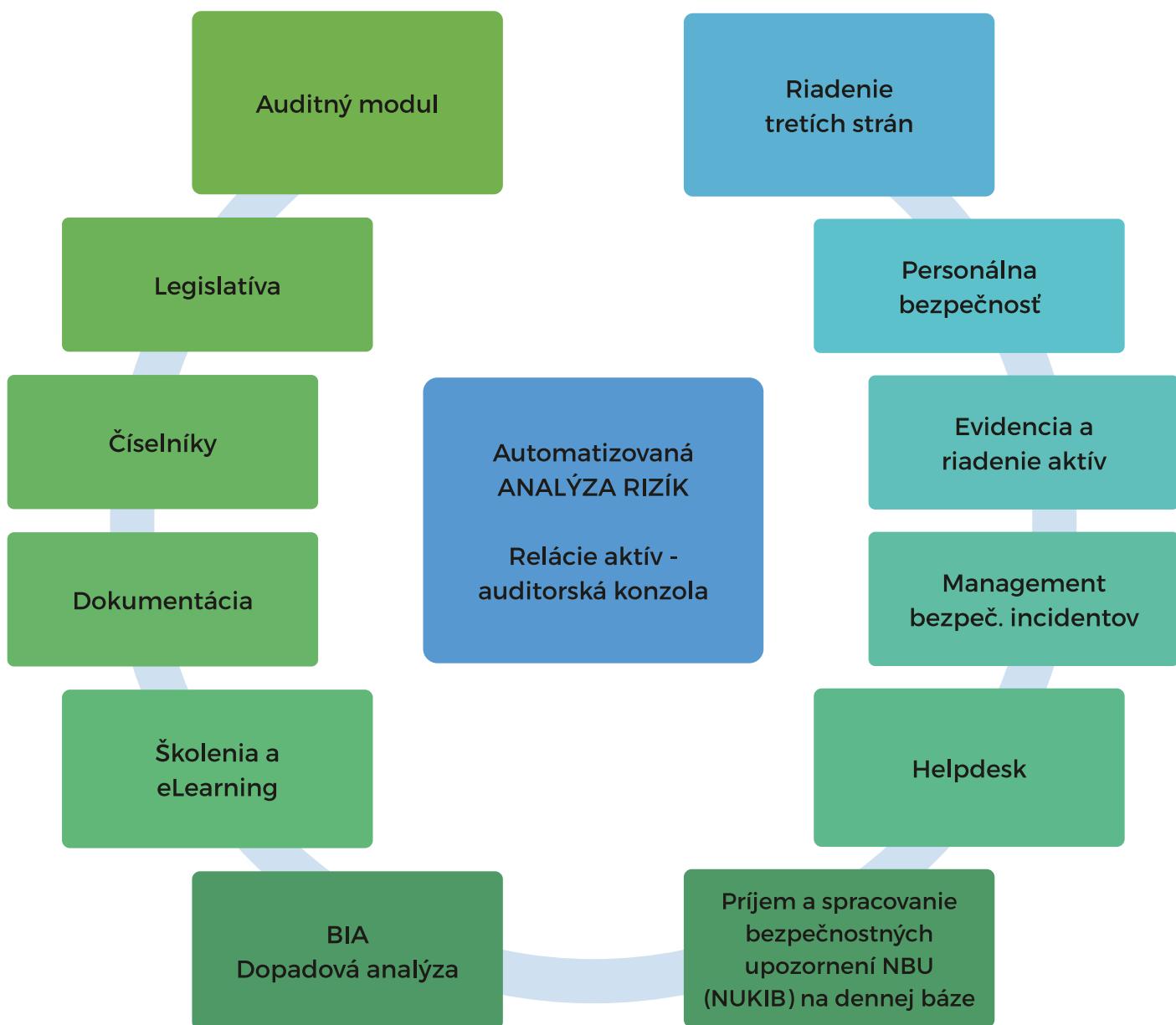
### Softvér ako znalostné riešenie v module KBO :

- Je dôležitým nástrojom a pomôckou pre manažéra informačnej a kybernetickej bezpečnosti rovnakého funkčného významu, ako je napr. účtovný softvér pre účtovníka.
- Je poistený na 1 mil. eur (všeobecná zodpovednosť za škodu) pre územie EU
- Získal Osvedčenie o súlade s platnou legislatívou v oblasti kyberbezpečnosti
- Stal sa súčasťou odbornej literatúry Kybernetická (ne)bezpečnosť – Problematika bezpečnosti v kyberprostoru, autor Petr Sedlák a kol. 10-2021 vydavatelství CERM ako implementačné riešenie KYBE pre KII a Z
- Môže slúžiť ako individuálne riešenie pre samotnú organizáciu, tak aj na riadenie sektorových procesov KB pre riadiace / ústredné orgány v rámci sektoru resp. na riadenie prístupu tretích strán a ich dodávateľov

### Modul KBO disponuje:

- Intuitívnym ovládaním, ktoré zvládne nielen expert ale aj informovaný laik
- Predvyplnenými číselníkmi v moduloch, nepotrebuje dopĺňať množstvo dát a súvislostí
- Zrozumiteľnými a prehľadnými výstupmi v elektronickej alebo tlačenej forme vrátane Záverečnej správy
- Aktuálne naprogramovanými cca 50 tisíc väzbami medzi aktívmi, hrozbami, zraniteľnosťami a ochr. opatreniami, čo výrazne zjednodušuje Vašu prácu v automatizovanej Analýze rizík
- Konzolou relácií aktív, kde Manažér IB/KB môže aktívne vykonávať zmeny v Analýze rizík
- Auditným modulom ciel'ov a opatrení podľa prílohy A a maticou RASCI
- Univerzálnosťou použitia, nie je potrebná customizácia softvéru pre zákazníka
- Príjemnou cenou pri širokom využití, s plnou podporou autorov softvéru

# GRAFICKÉ ZNÁZORNENIE MODULARITY MODULU KYBERNETICKÁ BEZPEČNOSŤ ORGANIZÁCIE



## **PERSONÁLNA BEZPEČNOSŤ**

Vedie evidenciu prístupov k informačným a komunikačným systémom organizácie, prístupových rolí a prenos oprávnení, vedie evidenciu zverených aktív, kontroluje rozvoj bezpečnostného povedomia.

## **RIADENIE TRETÍCH STRÁN**

Vedie evidenciu tretích strán, povolených prístupov k informačno-komunikačným technológiám organizácie, špecifikuje rozsah činností apod.

## **RIADENIE AKTÍV**

Vedie evidenciu aktív, opis ich vlastností, vedie evidenciu ich vlastníkov a správcov, osôb.

## **IMPORT AKTÍV A VYBRANÝCH ČÍSELNÍKOV**

Umožňuje načítanie zoznamu aktív a naplnenie vybraných číselníkov z externého súboru v podporovanom štandardnom formáte pre výmenu dát (xml, csv, xls).

## **ANALÝZA RIZÍK**

Výnimočný nástroj na realizáciu Analýzy rizík, ako účinného prostriedku na objektívnu identifikáciu slabých miest organizácie.

## **GAP Analýza**

Nástroj umožňuje v úvode procesu, resp. pred procesom analýzy rizík vykonať GAP analýzu.

## **Relácie aktív**

Slúži ako špeciálna manažérská konzola zameraná na Analýzu rizík, umožňuje aktívny vstup do modifikačného režimu Analýzy rizík, modifikuje prednastavenú paletu atribútov.

## **MANAŽMENT BEZPEČNOSTNÝCH INCIDENTOV**

Vedie súhrnnú evidenciu o životnom cykle incidentu, komplexne riadi bezpečnostné incidenty, generuje hlásenia o bezpečnostnom incidente SK-CERT-u ai.

## **MANAŽMENT AUDITOV, MATICA RASCI, CIELE RIADENIA A OPATRENIA**

Obsahuje funkčný manažment auditov, kompetenčnú maticu RASCI ako auditný nástroj pre identifikáciu rolí a zodpovednosti v rámci procesu.

## **ŠKOLENIA**

Systematicky riadi zvyšovanie povedomia používateľov v oblasti KB prostredníctvom interných školení alebo e-Learningových kurzov.

## **DOKUMENTÁCIA**

Vedie evidenciu povinných dokumentov a informácií, politík a metodík.

## **PRÍJEM A SPRACOVANIE BEZPEČNOSTNÝCH VAROVANÍ NBÚ / MANAŽMENT BEZPEČNOSTNÝCH VAROVANÍ**

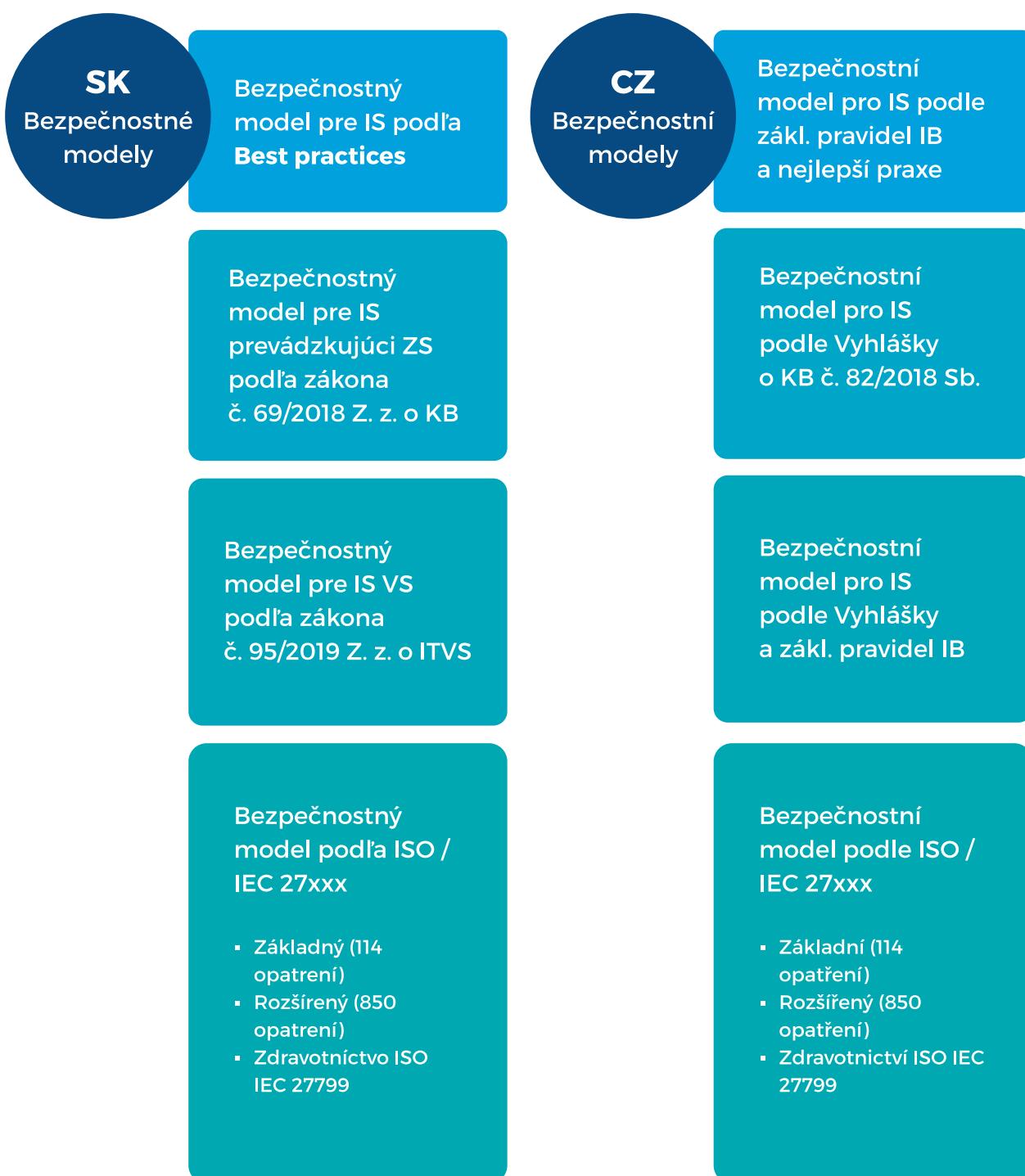
Umožňuje príjem a následné spracovanie bezpečnostných varovaní zverejňovaných a poskytovaných SK-CERT s automatizovaným upozornením pre vlastníkov/správcov relevantných aktív, ktorých sa bezpečnostné varovanie týka.

# ANALÝZA RIZÍK

Pred spustením Automatizovanej AR zadávate nasledovné informácie:

Základné informácie o IKS, primárne a podporné aktíva s vlastníkmi, voľbu bezpečnostného modelu, klasifikáciu a kategorizáciu informácií.

Vytvárate si Vstupnú AR, Priebežné AR a Testovacie AR.



# ANALÝZA RIZÍK

Práca s Automatizovanou analýzou rizík obsahuje:



# ANALÝZA RIZÍK - GRUPY AKTÍV

Novinkou od roku 2023 je jedinečná funkcia pre prácu s informačnými aktívami, ktorá umožňuje používateľmi zoskupovať a kombinovať informačné aktíva priradené k jednotlivým bezpečnostným modelom do používateľmi vytvorených a definovaných grúp a tieto následne využiť v procese analýzy rizík kybernetickej bezpečnosti.



**1 - Bezpečnostný model Best Practices**

**2 - Bezpečnostný model podľa zákona č.69/2018 Z. z. alebo č.95/2019 Z. z.**

**3 - Priradenie aktív do používateľmi definovaných grúp**

**4 - Bezpečnostný model Best Practices s vybranými používateľkými grupami**

**5- Bezpečnostný model podľa zákona č.69/2018 Z. z. s vybranými používateľkými grupami**

# ZÁVEREČNÁ SPRÁVA

Záverečná správa obsahuje vygenerované informácie obsiahnuté v aplikácii, pričom užívateľ si volí z jednotlivých parciálnych častí záverečnej správy:

- Správa kybernetickej bezpečnosti IS
- Závery z analýzy rizík skúmaného IS
- Aktíva
- Analýza rizík - výstup
- Záver
- Vyhlásenie o aplikovateľnosti
- Legislatívne východiská Kb
- Použitá metodika
- Označenie používané na zabezpečenie zdieľania citlivých informácií
- Podporné služby

Záverečná správa obsahuje ako textovú časť, tak aj grafické a číselné znázornenie vybraných informačných blokov:



# VÝŇATOK ZO ZÁVEREČNEJ SPRÁVY

Správa: Stav kybernetickej bezpečnosti informačného systému  
informačný systém verejnej správy / Všeobecný informačný systém

K zabezpečeniu využívajúceho stavu kybernetickej bezpečnosti hodnoteného informačného systému je potrebné implementovať opatrenia vychádzajúce z pravidiel dobrej praxe (Best practice).

## ZÁVER

POČET K ZAVEDENIU

OPATRENIA	POČET K ZAVEDENIU
Opatrenia typu FYZICKÁ REALIZÁCIA (A)	54
Opatrenia typu PROCES (P)	203
Opatrenia typu DOKUMENT (D)	50
Opatrenia typu ŠKOLENIE (S)	25

Zoznam opatrení pravidiel dobrej praxe (Best practice) typu FYZICKÁ REALIZÁCIA

Typ aktiva	Zoznam opatrení typu FYZICKÁ REALIZÁCIA potrebných k zavedeniu	MIERA RIZIKA / TYP	Zodpovedná osoba za riadenie rizika	Prihovávaný termín riešenia
Active Directory / AD Server - služba	Zoznam opatrení typu FYZICKÁ REALIZÁCIA potrebných k zavedeniu: Dvojfaktorová autentifikácia	64-A/A	Jozef IT Specialista 2. Daišbor Manager bezpečnosť (IKT).	25.10.2021
Detectia udalostí súvisiacich s bezpečnosťou	Centrálna detekcia a kontrola správ udalostí v reálnom čase - Na výhodnocovanie udalostí súvisiacich s bezpečnosťou je potrebné použiť centrálné komponenty vyukonávajúce automatizovanú analýzu týchto udalostí. <del>Automatizované nástrojmi sú použité na zaznamenávanie, korelovanie a vizualizovanie všetkých udalostí vystupujúcich sa v systémovom prostredí. Musia sa definovať prenové hodnoty potenciálne nebezpečných udalostí pri ktorých sa spláňa automaticky alarm.</del> Je potrebné, aby personál bol kvalifikovaný a schopný okamžite iniciovat kvalifikovanú a otvorenú reakciu. Je potrebné pravidelne kontrolovať parametre analýzy a v prípade potreby by sa mali upraviť. (násťor <del>Bezpečnosť informácií</del> a <del>externé manažmentu - SIEM</del> ) Použíte systémovú detekciu prieiniek - IDS alebo systémumu prevencie - IPS.	64-A/A	Silvester IT Specialista 1. Jozef IT Specialista 2.	15.09.2022
Detectia udalostí súvisiacich s bezpečnosťou	Použíte systémovú detekciu prieiniek - IDS alebo systémumu prevencie - IPS.	64-A/A	Peter Viedúci technológ ICS. Jozef IT.	01.10.2022

Zoznam vygenerovaný dňa: 14.01.2022

Na súčin záväznosti možného dopadu (D), potrebného času (T) a rizika (R) je závislosť (Z) určená bezpečností informačného systému verejnej správy / Všeobecný informačný systém

### záväznosť (Z)

Právdepodobnosť realizacie určené aktívum (je potrebné napojiť)

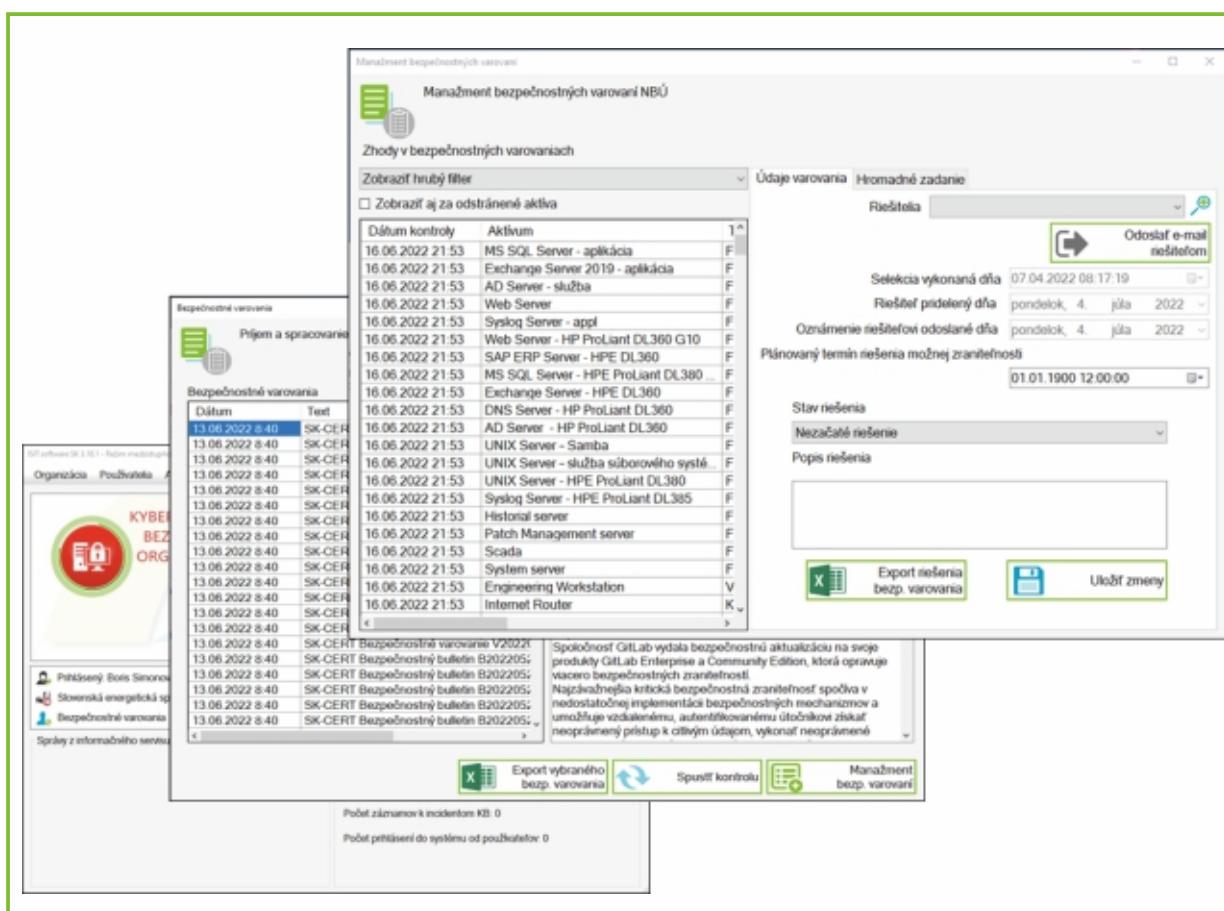
# MANAŽMENT BEZPEČNOSTNÝCH VAROVANÍ z SK CERT NBÚ SR

V module KBO je integrovaná dôležitá funkcia vo forme nástroja umožňujúceho účinné predchádzanie negatívnym dopadom kybernetických hrozien na informačné systémy, resp. informačno-komunikačné technológie, pomocou semi-automatického príjmu a spracovania bezpečnostných varovaní emitovaných SK-CERT NBÚ SR. Nástroj v polo-aktívnom režime vykoná vyhľadávanie v registri aktív prevádzkovateľa tie aktíva, ktoré majú vysokú relevanciu ku kritickým zraniteľnostiam uvedených v bezpečnostných varovaniach SK-CERT NBÚ SR. V prípade pozitívneho výsledku vyhľadávacieho procesu nástroj ponúka možnosť upovedomenia vlastníka/správcu aktíva na nutnosť kontroly a zavedenia nápravných opatrení na elimináciu kritickej zraniteľnosti spravidla informačného technického aktíva v jeho zodpovednosti.

S prihľadnutím na dôležitosť riadenia bezpečnostných varovaní ku konkrétnym aktívam organizácie, sme tento proces zvolili ako semi-automatický, teda s nevyhnutnosťou kontroly/zásahu manažéra KB.

## Tri základné kroky:

- Príjem, publikácia a archivácia bezpečnostných varovaní;
- Kontrola potenciálne ohrozených informačných aktív kritickými zraniteľnosťami a emitovanie upozornení pre ich vlastníkov / správcov;
- Správa / manažment varovaní a nápravných opatrení.



# VYBRANÉ UKÁŽKY Z MODULU KBO

## Riadenie rizík

The screenshot displays a software interface for managing risks. At the top, there are tabs for 'Analýza rizík' (Risk Analysis), 'Vývoj nové AR' (Development of new AR), 'Analýza rizík' (Risk Analysis), 'Riadenie rizík' (Risk Management), 'Vyhodnotenie rizík' (Risk Assessment), 'Pripája zostačkových rizík IB' (Associates remaining risks IB), 'Vzťahosť vlastníka' (Owner relationship), 'Monitorovanie rizík' (Risk monitoring), and 'Exporty AR' (AR exports). Below the tabs, there are several filters: 'Prehľad', 'Katalóg rizík', 'Identifikácia následkov' (Impact identification), 'Analýza rizík', 'Riadenie rizík', 'Vyhodnotenie rizík', 'Pripája zostačkových rizík IB', 'Vzťahosť vlastníka', 'Monitorovanie rizík', and 'Exporty AR'. A search bar and a 'Zoznam zmluvnosť + hrozob + opatrení' (List of contracts + threats + measures) button are also present.

ID Rizík	Aktívum / skupina aktív	Názov hrozby	Názov opatrenia	Úroveň rizikovosti	Mera rizika	Typ zavedenia	Dátum zák. zavedenia opatrení	Pôsobivý termín rešenia	Osoba zodpovedná za rešenie rizíka
R 4.1200	Active Directory	Chýbajúce plánovanie alebo chybáciu úprava implementačného metódu bezpečnej správy pre službu A...	Implementačná metóda bezpečnej správy pre službu A...	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Chýbajúce plánovanie alebo chybáciu úprava monitorovania infraštruktúry Active Directory	Monitorovanie infraštruktúry Active Directory	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Chýbajúce plánovanie alebo chybáciu úprava plánovanie skupinových politik v systéme Windows	Plánovanie skupinových politik v systéme Windows	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Chýbajúce plánovanie alebo chybáciu úprava plánovanie služby Active Directory	Plánovanie služby Active Directory	48	A	Zavedené			
R 4.1200	Active Directory	Chýbajúce plánovanie alebo chybáciu úprava plánovanie správky Active Directory	Plánovanie správky Active Directory	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Chýbajúce plánovanie alebo chybáciu úprava skolenie Active Directory Administration Training	Skolenie Active Directory Administration Training	27	B	Zavedené	13.1.2020		
R 4.1200	Active Directory	Importovanie správ	Bezpečné používanie DNS pre Active Directory	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Importovanie správ	Implementačná metóda bezpečnej správy pre službu A...	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Importovanie správ	Konfigurácia bezpečného kanálu pod operačným syst...	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Importovanie správ	Ochrana autentifikácie pri používaní Active Directory	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Importovanie správ	Ochrana služby Active Directory (vyznačené účty rizíka)	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Importovanie správ	Ochrana služby Active Directory (vyznačené účty rizíka)	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Importovanie správ	Plánovanie skupinových politik v systéme Windows	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Importovanie správ	Plánovanie správky Active Directory	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Importovanie správ	Zachovanie prevádzkovovej bezpečnosti služby Active...	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Informácie zo Splošnovania (spoločnosť)	Implementačná metóda bezpečnej správy pre službu A...	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Informácie zo Splošnovania (spoločnosť)	Konfigurácia bezpečného kanálu pod operačným syst...	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Informácie zo Splošnovania (spoločnosť)	Odsenie administratívneho a produkčného prostredia	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Informácie zo Splošnovania (spoločnosť)	Ochrana autentifikácie pri používaní Active Directory	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Informácie zo Splošnovania (spoločnosť)	Ochrana služby Active Directory (vyznačené účty rizíka)	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Informácie zo Splošnovania (spoločnosť)	Plánovanie skupinových politik v systéme Windows	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Informácie zo Splošnovania (spoločnosť)	Plánovanie správky Active Directory	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Informácie zo Splošnovania (spoločnosť)	Zachovanie prevádzkovovej bezpečnosti služby Active...	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Informácie zo Splošnovania (spoločnosť)	Implementačná metóda bezpečnej správy pre službu A...	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Informácie zo Splošnovania (spoločnosť)	Konfigurácia bezpečného kanálu pod operačným syst...	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Informácie zo Splošnovania (spoločnosť)	Odsenie administratívneho a produkčného prostredia	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Informácie zo Splošnovania (spoločnosť)	Ochrana autentifikácie pri používaní Active Directory	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Informácie zo Splošnovania (spoločnosť)	Ochrana služby Active Directory (vyznačené účty rizíka)	16	CS	Zavedené	13.1.2020		
R 4.1200	Active Directory	Informácie zo Splošnovania (spoločnosť)	Plánovanie skupinových politik v systéme Windows	16	CS	Zavedené	13.1.2020		

Below the table, there is a section titled 'RIADENIE RIZÍK' (Risk Management) with fields for 'Osoba zodpovedná za zavedenie opatrenia' (Person responsible for implementing measures), 'Plánovaný termín zavedenia opatrenia' (Planned date for implementing measures), 'Dátum zavedenia opatrenia' (Date of measure implementation), 'Dátum kontroly vykonania' (Date of control execution), and 'Kontrolu vykonal' (Controlled by). On the right, there is a preview of completed control status reports and buttons for 'Uložiť zadanie' (Save task) and 'Export údaje do excelu' (Export data to Excel).

## Riadenie prístupov tretích strán

The screenshot shows a software interface for managing third-party access. At the top, there are tabs for 'Riadenie tretích strán' (Management of third parties), 'Zoznam priradených tretích strán' (List of assigned third parties), 'Specifikácia a rozsah bezp. opatrení' (Specification and scope of security measures), 'Rozsah činností' (Scope of activities), 'Personálne tretej strany' (Personal of the third party), 'Riadenie prístupov' (Access management), 'Kontrolné činnosti' (Control activities), and 'Ohlásiť' (Report). Below the tabs, there is a search bar and a 'Export záznamu tretích strán' (Export third-party record) button.

ID	Meno	Osobné číslo	Zamestnanie	Dátum zav.
19	Tibor Bučovan			
25	Stanislav Borec			
27	Slavomír Mokrý			

On the left, there is a table titled 'Zoznam priradených tretích strán' (List of assigned third parties) showing a list of companies. On the right, there is a section for 'Detail prístupov daného zamestnanca' (Details of the employee's access) with fields for 'Názov skupiny podporovného aktíva' (Name of supporting asset group), 'Názov vybraného aktíva' (Name of selected asset), 'Stupeň dôležitosti' (Importance level), 'Dátum zák. podporovného oprávnenia aktíva' (Date of support asset authorization), and a dropdown for 'Internal Switch'. Below this, there is a link 'Prístupy k aktivám >>' (Accesses to assets >>). At the bottom, there are buttons for 'Login zamestnanca' (Employee login), 'Dátum zriadenia prístupu / oprávnenia' (Date of access creation / authorization), 'Dátum zrušenia prístupu / oprávnenia' (Date of access cancellation / authorization), 'Vymazat' (Delete), 'Pridať nový detail prístupu' (Add new access detail), and 'Upraviť detail prístupu' (Edit access detail).

# PRIPRAVENOSŤ MODULU KBO NA ROZŠÍRENIE REGULOVANÝCH ODVETVÍ O NOVÉ REGULOVANÉ SLUŽBY V ZMYSLE SMERNICE NIS2



Modul KBO aplikácie ISIT SOFTWARE SK/CZ obsahuje základné komponenty – aktíva OT/ICS systémov zraniteľné kybernetickými útokmi, tie to sú priebežne doplňované a rozširované o nové komponenty v zmysle odporúčaní medzinárodných profesne zameraných noriem.

Modul KBO splňa parametre riadenia procesov kybernetickej bezpečnosti ako podľa národnej tak aj európskej legislatívy a medzinárodných noriem, teda je pripravený na prácu pre každého manažéra KB resp. povinný subjekt v oblasti kybernetickej bezpečnosti.

**Bližšie informácie:** [www.analyza-rizik.eu](http://www.analyza-rizik.eu)



## Modul HELPDESK pre riadenie bezpečnosti

- Samostatný modul, ktorý slúži ako účinný nástroj k predchádzaniu vzniku bezpečnostných incidentov
  
- Zaznamenáva životný cyklus udalosti od jeho vzniku, cez hlásenie, realizáciu až po vyriešenie vrátane personálneho obsadenia a kontroly
  
- Užívateľ vyberá z databázy o aký typ problému ide, upresní záznam k problému, aké dátá boli zasiahnuté, popis možnej škody, dopad a odhad závažnosti, zasiahnuté aktíva, riešenie problému a nápravné opatrenia
  
- Výstupom je súhrnná evidencia a prehľad riešenia udalosti / problému s postúpením správcovi systému a možnosti
  
- V prípade detekcie udalosti, ktorá je incidentom, prechádza komplettná informácia do manažmentu bezpečnostných incidentov

### Ukážka z Helpdesku – Proces riešenia

The screenshot shows the Helpdesk application interface. The main window has two panes. The left pane lists tasks with columns for Date, Name, and Author. The right pane shows a detailed view of a selected task. The task details include:

- Type of problem: Technical problem (technical problems with applications or hardware)
- Responsible for problem: Jozef Bandrovč
- Name of the problem: Network PC
- Description of the problem: Computer is connected, but after turning it on, it does not boot and there is no control.

Below the main window, there is a sidebar with the following buttons:

- Vložit dokument (Insert document)
- Odešriť (Delete)
- Pridať nový (Create new)
- Upraviť (Update)



# Modul GDPR (eGDPR, GDPR s DPIA)

Samostatný modul na riadenie procesov ochrany osobných údajov vrátane väzieb posúdenia vplyvu (DPIA)

## EVIDENCIE INFORMAČNÝCH SYSTÉMOV (AGEND, SPRACOVATEĽSKÝCH ČINNOSTÍ)

- Povinné info – názov, účel, právny základ, lehota spracúvania, rozsah OU, OD, spracovateľské operácie, príjemcovia, tretie strany, oprávnené osoby atď

## ZOZNAMY A TLAČOVÉ ZOSTAVY

- Zamestnancov, oprávnených osôb, sprostredkovateľov, zodpovedných osôb, dotknutých osôb s archívom súhlásov, množstvo tlačových zostáv

## MANAŽMENT BEZPEČNOSTNÝCH INCIDENTOV

- Komplexné riadenie incidentov s tlačovou zostavou ku každému incidentu a generovaním hlásenia pre dozorný orgán

## BEZPEČNOSTNÁ DOKUMENTÁCIA

- Z údajov v softvéri sa generuje dokumentácia – záznam o spracovateľských činnostiach, smernice, kľúčový poriadok, poučenia oprávnených osôb ku konkrétnym účelom, odpovede dotknutých osobám, informácie o likvidácii, informačná povinnosť a i.

## AUTOMATIZOVANÝ AUDITNÝ MODUL

- Kontrolný nástroj na zistenie nezhôd v riadení ochrany OÚ v organizácii s generovaním správy z interného auditu s grafickým percentuálnym znázornením aktuálneho stavu nastavenia ochrany OÚ v organizácii.

## VÄZBY POSÚDENIA VPLYVU (DPIA)

- Obsahuje jednak evidenčnú časť aktív, cez hrozby, zraniteľnosti, hodnotu rizika až po ochranné opatrenia s generovaním výstupu

## TEST PROPORCIONALITY

- Podrobne spracovaný test proporcionality pri oprávnenom záujme špeciálne pre kamerové monitorovacie systémy

## KAMEROVÝ MONITOROVACÍ SYSTÉM

- Podľa nového usmernenia EDPB platného od 29.1.2020 s možnosťou generovania tabuľky označenia 1. vrstvy

## eLearning

- Obsahuje prístup k okruhom školení so skúškou a osvedčením pre absolventa pre jednotlivé okruhy tém ochrany citlivých dát

# KAMEROVÉ MONITOROVACIE SYSTÉMY

Samostatný podmodul v Module GDPR je v súlade s hlavným usmernením EDPB č. 3/2019 zo dňa 9.1.2020 ku kamerovým monitorovacím systémom.

Obsahuje:

- Evidencie účelov, právnych základov spracúvania, spôsobu a perimetra monitorovania, evidencie jednotlivých kamier, umiestnenia a popis kamier, lehôt uchovávania, prístupov pre oprávnené osoby, sprostredkovateľov, práv dotknutých osôb
- Eviduje dokumentáciu pre KMS (napr. architektúra KMS, perimeter monitorovania – polohy kamier a iné)
- Obsahuje pripravené testy proporcionality s generovaním výsledku
- Automatické upozornenia na lehoty pri pravidelnom prehodnocovaní testov proporcionality
- Generovanie kompletnej informačnej povinnosti pre kamerové systémy (2. vrstva)
- Generovanie 1. vrstvy tabuľky s povinnými náležitostami (viď obrázok)
- Výstupom môže byť samolepka alebo podklad pre inú formu grafického výstupu

Označenie 1. vrstvy - Dôležité !! Kompletný popis prvej vrstvy - nestačí len piktogram kamery !



## Evidencie KMS – Generovanie Informačnej povinnosti

The screenshot shows the 'Kamerový monitorovací systém' application window. On the left, there's a sidebar with 'Označenie KMS' containing items like 'KMS1', 'KMS2', and 'KMS3'. The main area has tabs for 'Účel spracúvania' (Purpose of processing) and 'Právny základ' (Legal basis). Under 'Účel spracúvania', 'Ochrana majetku života a zdravia osôb' (Protection of life and health of individuals) is selected. The 'Právny základ' section includes fields for 'V Názor' (In accordance with), 'Súhlas dotknutej osoby v zmysle článku 6 o...' (Consent of the data subject in accordance with Article 6(1)(a)), 'Lehotla uchovávania' (Retention period), 'Spôsob uchovávania dát' (Method of data storage), 'Funkcionalita' (Functionality), 'S uchovávaním dát (identifikačný záznamový kód)' (With data storage (identification code)), 'Perimeter monitoring' (Monitoring perimeter), 'Kombinované' (Combined), and 'Umiestnenie označenia (1 vrstva tabuľky)' (Location of marking (1 layer of table)). Buttons at the bottom include 'Počet umiestnených označení' (Number of placed markings) set to 5, and 'Vymazat účel' (Delete purpose), 'Nový účel' (New purpose), and 'Uložit zmeny' (Save changes). On the right, there's a panel titled 'Kamery KMS' with a list of cameras and their locations, and a 'Generovanie informačnej povinnosti' (Generate informational document) button.

**Test proporcionality - Dôležité !! Test je nevyhnutný pri každom Účele/agende, kde je určený právny základ Oprávnený záujem prevádzkovateľa**

The screenshot shows the 'Test proporcionality' feature. On the left, there's a sidebar with 'Označenie' (Identification) and 'Účely spracúvania procesovagendy (IS, sprac. činnost, primárne aktívum)' (Purposes of processing process agenda (IS, processing activity, primary active item)). The main area has tabs for 'Základné údaje' (Basic data), 'Doplňujúce údaje' (Supplementary data), 'Osobné údaje' (Personal data), 'Osobné doklady' (Personal documents), 'Oprávnené osoby' (Authorized persons), 'Súhlas dotknutých osôb' (Consent of data subjects), 'Test proporcionality' (Proportionality test), 'Správca' (Administrator), and 'Správca systému' (System administrator). The 'Test proporcionality' tab is active. It contains sections for 'Vykúška sa pri plnom základe oprávnený záujem' (Testing the right to privacy under full basic data), 'Na som orgán verejnej moci' (I am a public authority), 'Potvrdenie voľby oprávneného zákumu prevádzkovateľa ako orgán verejnej moci' (Confirmation of the elected representative's right to privacy as a public authority), 'Dátum testu' (Test date) set to '2.4.2020 15:21', 'Identifikácia-OZ: Test nevyhnutnosti: Test vhodnosti: Test výhľadnosti: Bezpečnostná kontrola: Rozhodnutie: Doplňujúce informácie: Test výhľadnosti' (Identification-OZ: Test of necessity: Test of appropriateness: Test of foresight: Safety check: Decision: Supplementary information: Test of foresight), and a large table with questions and answers related to the proportionality test. Buttons at the bottom include 'Predať účel spracúvania', 'Vymazat účel spracúvania', 'Generovať / uložiť dokumenty', 'Vymazat test proporcionality', 'Predať nový test proporcionality', and 'Upraviť test proporcionality'.

# VYBRANÉ UKÁŽKY Z MODULU GDPR

## Evidencie agend/procesov – Väzby posúdenia DPIA



## Prínos používania softvérového modulu GDPR pre prevádzkovateľa:

- Absolútny prehľad o všetkých agendách, účeloch a procesoch s generovaním povinných výstupov – dokumentácia je aktuálna v danom čase, „nedegraduje v čase“
- Plný manažment poučení oprávnených osôb ku konkrétnym úcelom podľa funkčných miest
- Súčasťou sú školenia pre oprávnené osoby a návštevy (tretie strany)
- Garancia legislatívneho súladu riadenia ochrany OU pre Zodpovednú osobu, štatutára a pri výkone kontroly dozorným orgánom, plná podpora autorov aplikácie
- Široká funkcionálita s prechodom do kybernetickej bezpečnosti
- Bohato naplnené číselníky so vzormi podľa zamerania prevádzkovateľov (verejná správa, školy, komerčné spoločnosti - obchod, výroba, eshop, ekonomika, služby a ī)

Viac informácií získate na [www.isitslovakia.sk](http://www.isitslovakia.sk)



## Modul WHISTLEBLOWING s riadením korupčných rizík

- Klúčové zmeny podľa Smernice EP a Rady EU č. 2019/1937 zo dňa 23. 10. 2019 o ochrane osôb, ktoré oznamujú porušenia práva Unie (smernica o whistleblowingu)

- Zmena z formálneho riadenia protikorupcie na funkčný systém whistleblowingu

- Dôraz na dôvernosť a bezpečnosť podania oznamovateľa, ochrana jeho totožnosti, dôvernosť spracovania a vyhodnotenia oznámení spolu s požiadavkami na organizáciu a riešiteľa/auditora

- Účinná ochrana pred odvetnými opatreniami

- Elektronická časť oznamovacieho procesu musí byť riešená dôverným spôsobom, čo nedokáže garantovať emailové oznamovanie, ale výhradne softvérová aplikácia s web nahlasovacím formulárom a manažérskou konzolou pre riadený proces spracovania Oznámení.

### Riešenie VOS WB v module ISIT software SK/CZ:

Povinný subjekt má umiestnený odkaz na VOS WB na svojej web stránke, prostredníctvom ktorej ľubovoľný Oznamovateľ môže bezpečne s garanciou dôvernosti nahlásiť svoj Podnet s voľbou anonymného alebo chráneného oznámenia. Každé oznámenie má pridelený jedinečný ID, prostredníctvom ktorého sa môže dobrovoľne zidentifikovať aj anonymný oznamovateľ pre prechod do pozície chráneného oznamovateľa.

Aplikačnú časť softvérového modulu má inštalovanú Audítor / skupina Audítorov, ktorá prijíma, procesuje a vyhodnocuje všetky Oznámenia.

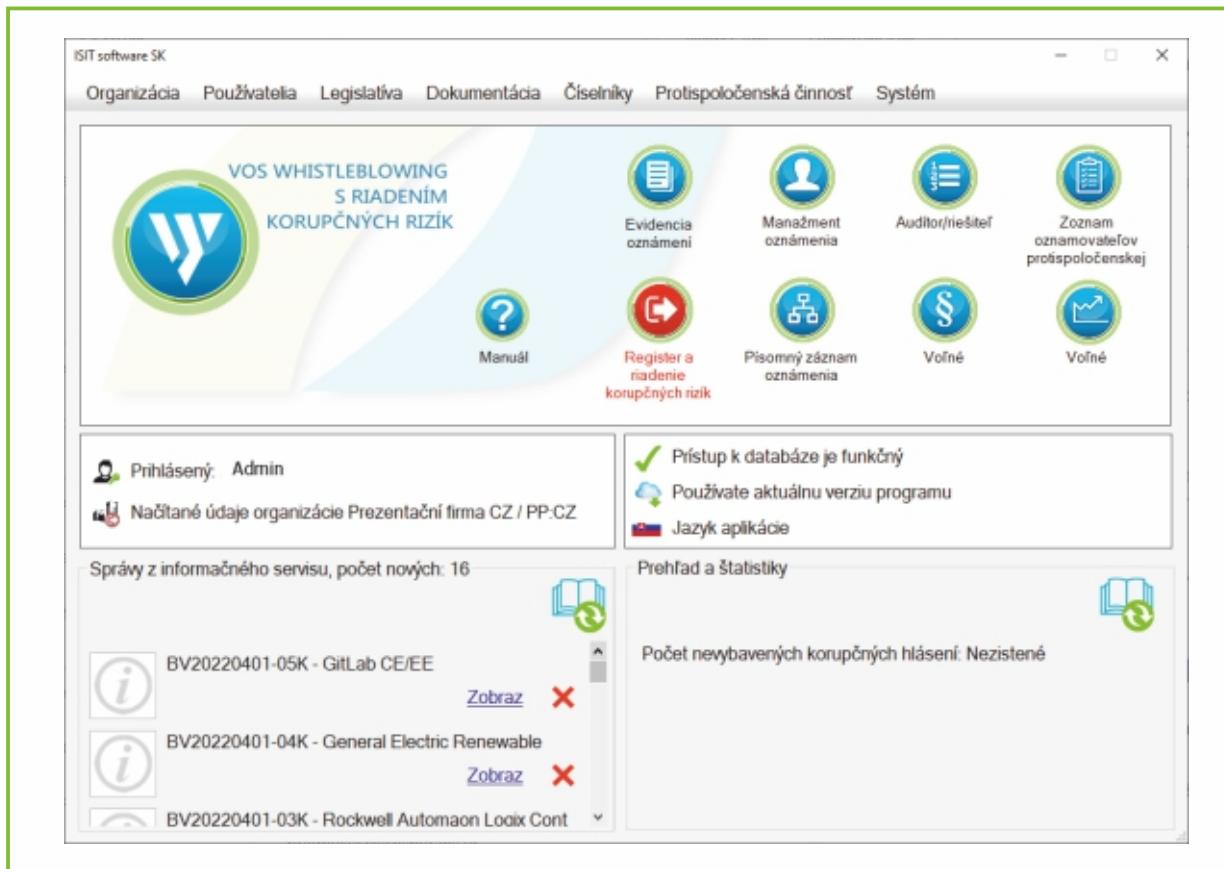
Dôvernosť pri spracúvaní je garantovaná administráciou portálu so zabezpečeným uchovávaním dát.

Riešenie je postavené ako na multiadmin platforme, kde jeden Audítor / právnická kancelária môže realizovať činnosť Whistleblowingu pre viacerých klientov pri dodržaní všetkých bezpečnostných parametrov tak aj na individuálnom riešení pre 1 konkrétnu organizáciu.

Viac informácií získate na [www.whistleblowing-software.eu](http://www.whistleblowing-software.eu)

# VYBRANÉ UKÁŽKY Z MODULU VOS WB

## Úvodné okno modulu VOS WB (manažérská konzola)



## Ukážka formuláru hlásenia (webklient)

The screenshot shows the internal reporting system's web client interface. The title bar reads "Vnútorný oznamovací systém WHISTLEBLOWING". Below the title, there's a welcome message: "Vitajte v internom oznamovacom systéme" and some instructions about reporting procedures. There are several buttons for different reporting categories: "Čo môžete nahlásiť cez VOS" (ZOBRAZIT), "Práca alebo iná obdobná činnosť" (ZOBRAZIT), "Odvetné opatrenia" (ZOBRAZIT), "Práva oznamovateľa" (ZOBRAZIT), "Ochrana oznamovateľa" (ZOBRAZIT), and "Použenie pre oznamovateľa" (ZOBRAZIT). Below these, there's a note about reporting requirements and a link to "Súhlas s polohou". At the bottom, there's a section for "Vyplniť formulár oznamenia:" with two options: "CHRÁNENÉ OZNAMENIE" and "ANONYMné OZNAMENIE".



## E-LEARNING

E-learning ako webová služba v licencii ISIT software SK/CZ predstavuje moderný spôsob pre efektívne zodelávanie zamestnancov, konkrétnie v oblasti ochrany osobných údajov/GDPR, Kyberbezpečnosti, riadení korupčných rizík a whistleblowingu. Prostredníctvom kurzov je možné jednoduchým spôsobom poskytnúť zamestnancom všetky potrebné informácie a overiť ich znalosti skúškou. Tvorcovia kurzov sú držitelia certifikátov interný audítork, lead auditor v príslušnej oblasti s dlhoročnou praxou. Lekcie v kurzoch vieme doplniť podľa interných riadiacich aktov zákazníka.

### E-learningové kurzy poskytujú:

logickú postupnosť školenia po kapitolách  
obsah podľa platnej legislatívy  
príbežné overovanie vedomostí  
záverečné overenie vedomostí testom (výber náhodných 5 otázok, 3 odpovede musia byť správne, ak sú nesprávne, ešte sú 2 opakovania testu)  
generovanie osvedčenia o úspešnom absolvovaní školenia

### E-learning ako služba v blokoch GDPR, KBO, Whistleblowing:

vzdelávanie administruje ISIT Slovakia s.r.o.  
zákazník získava vygenerované klientske prístupy pre všetkých účastníkov na prístup do webslužby (email účastníka + vstupné heslo)  
platená služba; doplnkovo možnosť naprogramovať lekcie podľa interných smerníc zákazníka  
doplňujúci bonus – pri objednaní elearningovej služby zákazník získava 10% zľavu na každé ďalšie služby a produkty našej spoločnosti (audit, školenia, ISIT software SK)

### Ukážka z Elearningu – Kurz KB

The screenshot shows a web browser window with the title 'E-learning ISIT software SK'. The main content area displays the course 'KB - Kurz 2 Praktické aspekty kybernetickej bezpečnosti'. Below the title, there's a navigation bar with links to 'Domov', 'Moje kurzy', and 'KB - Kurz 2 Praktické aspekty kybernetickej bezpečnosti'. A sidebar on the right shows a progress bar labeled 'Váš pokrok' with a value of 100%. The main content area contains text about course requirements and a checklist at the bottom.

**Informácie o podmienkach absolvovania kurzu**

Pre splnenie podmienok kurzu a získanie certifikátu je nutné absolvoovať prednášku spoločne s úspešným absolvovaním testu.

Test pozostáva z 5 náhodne vybraných otázok.

Minimálny počet bodov nutných na úspešné vykonanie testu sú 3 body.

Každá správna odpoveď má hodnotu 1 bodu.

Časový limit určený na odpovede je 5 minút.

V prípade úspešného absolvovania testu bude používateľovi v závere udelený certifikát.

V prípade neúspešného absolvovania testu a vyčerpania oboch pokusov bude používateľovi prístup zablokovaný.

**Praktické aspekty kybernetickej bezpečnosti**

KURZ Praktické aspekty kybernetickej bezpečnosti

TEST Praktické aspekty kybernetickej bezpečnosti

Certifikát

# BEZPEČNOSTNÝ PORTÁL ISIT

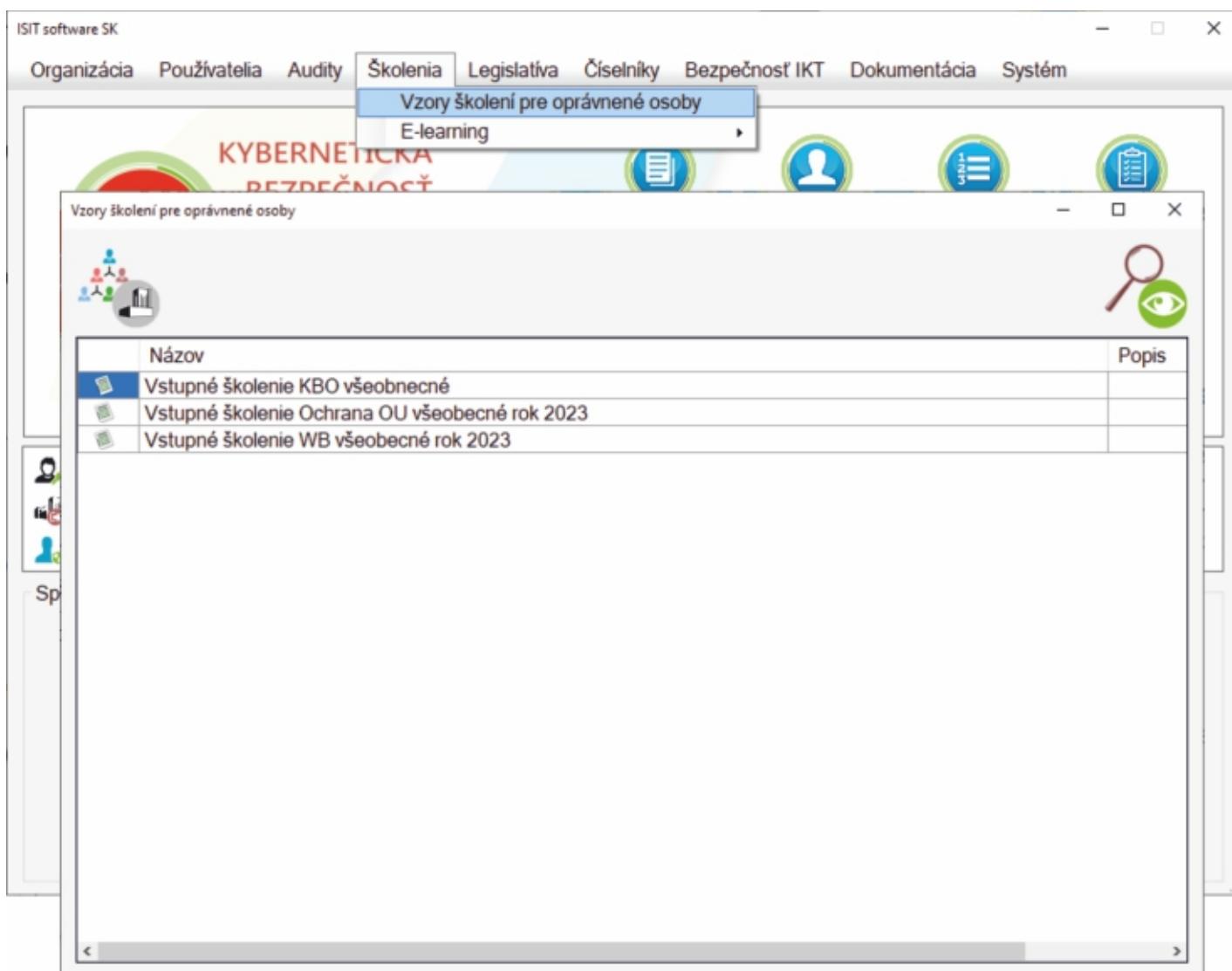
Bezpečnostný portál

VLADIMÍR TOMEK ÚVOD ODHĽAŠIŤ

The screenshot shows the homepage of the ISIT Slovakia security portal. At the top left is the company logo 'ISIT Slovakia s.r.o.' with the tagline 'Informačné systémy Informačné technológie'. To the right is a large banner featuring a blue-toned collage of various digital and security-related icons, such as a padlock, a hand interacting with a screen, and a camera. Overlaid on this banner is the text 'BEZPEČNOSTNÝ PORTÁL' in white. Below the banner are two smaller images: one showing a close-up of a padlock on a digital interface with binary code, and another showing a surveillance camera integrated into a modern building facade. At the top right of the page, there are three small green navigation icons. The main content area has a light gray background. On the right side, there is a section titled 'Použitie bezpečnostného portálu' (Usage of the security portal) which lists several functions with checkmarks. Below this is a green button labeled 'Zadať údaje do portálu' (Enter data into the portal) and another green button labeled 'Zobrazíť administráciu portálu' (View portal administration). At the bottom right of the content area is a small green icon with an upward arrow.

Bezpečnostný portál ISIT je samostatnou web aplikáciou, ktorá môže byť súčasťou web stránky povinného subjektu alebo jeho intranetu a je určená pre zamestnancov a zamestnancov dodávateľov povinného subjektu. Portál je prístupný aj na stránke [www.isitslovakia.sk](http://www.isitslovakia.sk) pre našich registrovaných zákazníkov, ktorým poskytujeme odborné služby (externá Zodpovedná osoba, externý manažér KB). Slúži na okamžité a zároveň personalizované nahlásenie udalostí súvisiacich s téhou GDPR a KYBE pre internú alebo externú Zodpovednú osobu, manažéra KB, bezpečnostný výbor a iné určené osoby dôverným spôsobom. Z tohto portálu je možné špecialistom GDPR/KYBE buď spracovať parciálne všetky oznámené informácie, alebo využiť prepojenie na jednotlivé časti konkrétnych modulov aplikácie ISIT SOFTWARE SK/CZ na automatizáciu všetkých činností pri dodržaní termínov riešenia a zároveň o konkrétnie naplnenie požiadaviek na personálne, technické a organizačné opatrenia pre zabezpečenie parametrov dôvernosti, dostupnosti a integrity.

# ODBORNÉ ŠKOLENIA



## Školenia pre zamestnancov organizácie:

- V každom module aplikácie ISIT SOFTWARE SK/CZ je preklik na vypracované školiace materiály GDPR, KYBE, WB
- Možnosť pripraviť video prezentácie ako vstupné školenia pre nových zamestnancov
- Elearningové vzdelávanie (popísané v samostatnej časti katalógu)
- školenia v moduloch GDPR, KYBE a WB sú pre držiteľov licencie bezplatne k dispozícii
- prezenčné školenia priamo pre zamestnancov (vedenie organizácie, stredný manažment) „na mieru“ procesov a riadiacich aktov organizácie. Ide o absolvovanie povinných preškolení v jedno alebo dvojročných intervaloch so zhrnutím noviniek v danej téme a zavedených pravidiel aj s vystavením osvedčení o absolvovaní školenia, pričom hlavným účelom je budovanie a udržiavanie bezpečnostného povedomia v organizácii. Cielene školenia akceptujú dozorné orgány ako účinné ochranné opatrenie.

Blížsie informácie: [www.vaclav.sr](http://www.vaclav.sr)



## Modul FYZICKÁ A OBJEKTOVÁ BEZPEČNOSŤ

Pre rok 2022 pripravujeme nový modul procesnej aplikácie ISIT software SK/CZ zameraný na komplexné riadenie ochrany fyzickej a objektovej bezpečnosti (FOB). Používateľmi modulu sú najmä bezpečnostný riaditeľ s pracovníkmi vrátane štatutára organizácie, veliteľ a výkonná časť obecnej polície alebo SBS, odbory bezpečnosti a krízového riadenia a pod.

V jednotlivých segmentoch Personálna bezpečnosť, Riadenie tretích strán, Manažment bezpečnostných udalostí, Špecifikácia opatrení FOB, Vymedzenie okolia IS organizácie, Riadenie Aktív FOB poskytuje plnohodnotný support pre povinné osoby s podrobnými podkapitolami určenými pre kamerové a monitorovacie systémy s výstupmi pre kontrolné, dozorné orgány a súčinnosť s policajným zborom, riadením prístupov vrátane kľúčového poriadku, zabezpečením chránených priestorov (objektov a okolia), evidenčných častí aktív bezpečnosti atď.

Tento modul je prierezovým zjednocujúcim riešením pre každú organizáciu so zameraním na všeobecné riadenie FOB, teda bez legislatívnych vymedzení podľa GDPR alebo KBO.

Modul FOB možno považovať za procesný model riadenia obecnej FOB v organizácii ako predstupňa riadenia FOB podľa zákona o utajovaných skutočnostiach podľa príslušnej národnej legislatívy.

The screenshot displays the main window of the ISIT software SK application. At the top, there is a navigation bar with tabs: Prevádzkovateľ, Používateľia, Školenia, Legislatíva, Číselníky, Evidencie a záznamy, Bezpečnosť a procesy, and Systém. Below the navigation bar, there is a large header section titled "FYZICKÁ A OBJEKTOVÁ BEZPEČNOSŤ" with a "FOB" icon. This section includes links for "Manuál", "Špecifikácia opatrení FOB", "Personálna bezpečnosť", "Manažment bezpečnostných udalostí", "Riadenie tretích strán", "Kamerové a monitorovacie systémy", "Riadenie aktiv FOB", "Vymedzenie okolia IS organizácie", and "Zodpovednosť". On the left side, there is a sidebar with user information: "Prihlásený: Admin" and "Načítané údaje prevádzkovateľa VZOR Moja firma / PP.SK". Below this, there is a section for "Správy z informačného servisu, počet nových: 16" with two items: "BV20220401-05K - GitLab CE/EE" and "BV20220401-04K - General Electric Renewable". To the right of the sidebar, there is a "Prehľad a štatistiky" section with various metrics: "Počet incidentov / nenahlásené: 4 / 1", "Počet nových záznamov k incidentom: 5", "Počet nevybavených žiadostí: 1", and "Počet prihlásení do systému od používateľov: 10".

	<b>RIEŠI TÉMU</b>	<b>KYBERNETICKÁ BEZPEČNOSŤ</b> (Protispoločenská činnosť pri porušovaní práv Unie)	<b>WHISTLEBLOWING</b> (Protispoločenská činnosť pri porušovaní práv Unie)	<b>GDPR – OCHRANA OSOBNÝCH ÚDAJOV</b>	<b>E-LEARNING</b>	<b>HELPDESK</b>
	<b>STRUČNÁ ANOTÁCIA MODULOV</b>	Samostatný modul na riadenie procesov KB, generovanie výstupov, dokumentácie, smerníc – záverečnej správy s prehlásením o aplikovateľnosti (Statement of Applicability - SOA), vrátane evidencí Pracovný nástroj manažéra KB s presahom na vlastníkov aktív	Vnútorný oznamovací systém na bezpečné nahlásование порушенí прав Únie a ochrane oznamovateľov a manažérská konzola na procesovanie udalostí Pracovný nástroj pre audítora / pověřenú osobu	Modul na riadenie procesov ochrany osobných údajov Elektronický záznam o sprac. činnostiach Generovanie povinnej dokumentácie Pracovný nástroj pre Zodpovednú osobu / DPO / Pověřenca	Vzdelávací nástroj na budovanie a udržiavanie bezpečnostného povedomia k jednotlivým modulom Testovanie užívateľov vrátane generovania osvedčenia o úspešnom absolvovaní	Modul na riadenie bezpečnostných udalostí v organizácii
	<b>VÝNIMOKOČNOSŤ</b>	Komplexný proces riadenia kybernetických a informačných rizík, Automatizovaná Analýza rizík, Riadenie a prístup k aktivam, Systémové riadenie tretích strán, BIA – dopadová analýza	Bezpečné a dôverné nahlásование udalostí s ochranou oznamovateľov a systémovým bezpečným riadením procesu whistleblowingu	Procesné komplexné riadenie ochrany OÚ s množstvom výstupov do povinnej dokumentácie s udržiavaním v aktuálnom stave	Plná podpora e-vzdelenia v oblasti KB, GDPR, Whistleblowingu a ďalších oblastí	Samostatná platforma na riadenie akýchkoľvek bezp. udalostí s výstupmi na management BI
	<b>PRIDANÁ HODNOTA</b>	Manažment bezpečnostných incidentov (MBI) Implementovaný Infoservis – príjem a spracovanie bezpečnostných varovani poskytovaných Národným centrom	Podmodul riadenia korupčných rizík podľa ISO 37001	Interný auditný modul, Väzby posúdenia vplivu (DPIA), Testy proporcionality, kamerové IS s generovaním I. vrstvy	Vypracované lekcie s kolekciami testových otázok kompetentnými autormi / auditormi z jednotlivých oblastí	Praktický manažment ľubovoľných bezpečnostných udalostí / udalostí v organizácii s členením na MBI GDPR a MBI KBO
						





Pomôcka pre zodpovedné osoby, štatutárov organizácií, personalistov, manažérov KYBE, pracovníkov IT.



Softvér vede evidencie, zoznamy, generuje dokumenty, obsahuje vzory dokumentov, archivuje verzie, zaznamenáva logy.



Pravidelná aktualizácia a upgrade od autorov v súlade s platnou legislatívou. Dôležité upozornenia.



Poradenstvo a podpora špecialistov - audítorov IB. Individuálne riešenia. Služby na kľúč.



Technická a zákaznícka podpora. Zaškolenie k obslužnosti. Návody a používateľské príručky.



Nepretržitý vývoj aplikácie s dôrazom na bezpečnosť.

- V súčasnosti cca **2500 zákazníkov** pre oblasť GDPR vrátane základných a stredných škôl, miest a obcí v SR a desiatky zákazníkov pre oblasť KYBE a Whistleblowingu
- **Referenční zákazníci:** Finančná správa SR, Štatistický úrad SR, Úrad na ochranu os. údajov SR, Úrad pre reg. sieťových odvetví, Úrad komisára pre deti SR, Duslo Šaľa a.s., SEPS a.s., UP CZ a.s., Elektárny Opatovice, a.s., Český hydrometeorologický ústav, a i. Na VUT Brno fakulta podnikatelská vo verzii Edukit slúži softvér ako výučbový nástroj pre študentov, manažérov kybernetickej bezpečnosti, ŠVPS SR + 40 RVPS, Min. dopravy SR, MPSVaR SR, Slovenská pošta a i.
- Aktuálne ceny a možnosti prenájmu licencií nájdete na [www.isitslovakia.sk](http://www.isitslovakia.sk)



QR kód k produktovému katalógu modulu KBO

Viac informácií o softvéri nájdete na našich web stránkach:

[www.isitslovakia.sk](http://www.isitslovakia.sk)  
[www.analyza-rizik.eu](http://www.analyza-rizik.eu)  
[www.whistleblowing-software.eu](http://www.whistleblowing-software.eu)

**Kontakt:** [info@isitslovakia.sk](mailto:info@isitslovakia.sk) | 0910 905 154



Analýza Rizík ISIT Software Sk Cybersecurity