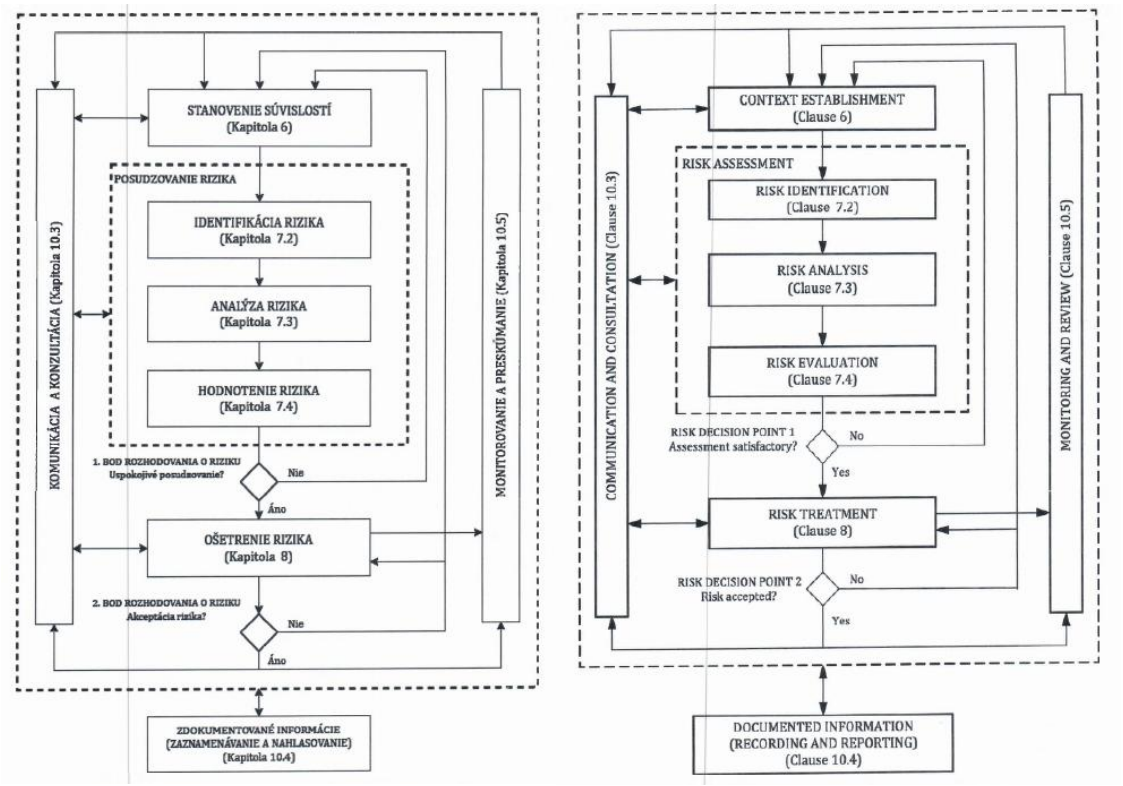
Aplikácia systému riadenia rizík vo vybranej organizácií verejnej správy s využitím softvérovej podpory



Proces riadenia rizík informačnej bezpečnosti

Metodický rámec:

1. Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti
2. Vyhláška NBÚ 227/2025 Z. z. o bezpečnostných opatreniach
3. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
4. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks
5. Metodika analýzy rizík a analýzy dopadov Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
6. Metodika analýzy rizík kybernetickej bezpečnosti Národného bezpečnostného úradu

Softvérová podpora:

Znalostná softvérová aplikácia ISIT software SK Cybersecurity (IS ISIT KB) s lokalizáciou v slovenskom a v českom jazyku. Modul Manažment výučby je učený pre výučbu riadenia procesov podľa jednotlivých modulov aplikácie.

Moduly IS ISIT KB

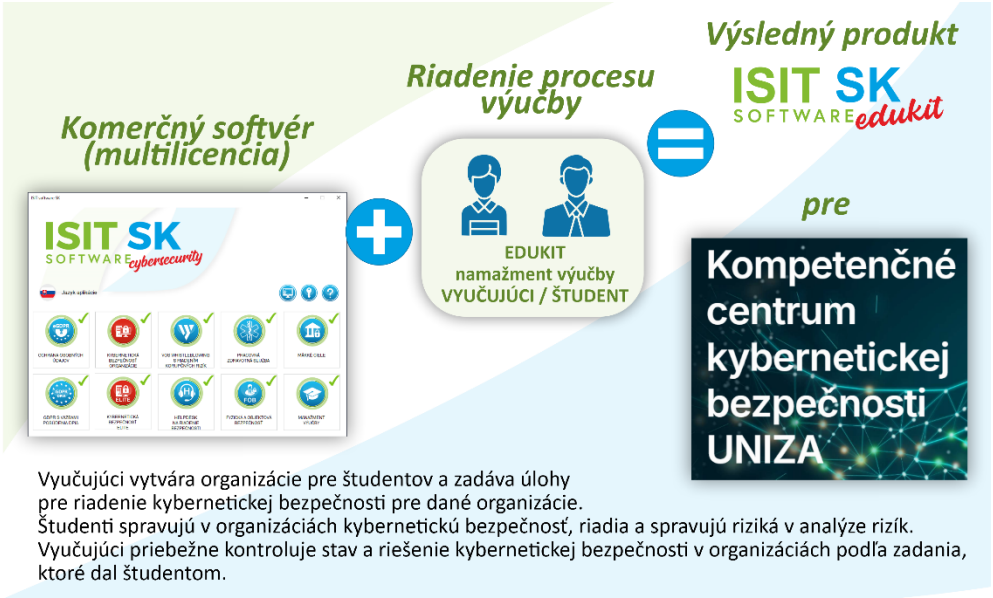
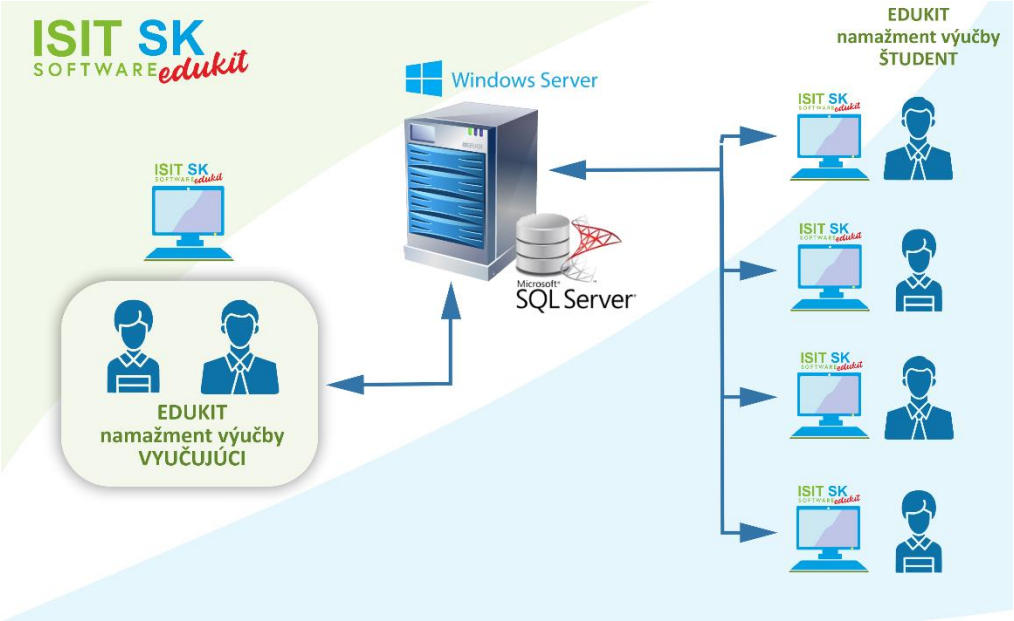


Schéma riešenia IS ISIT KB



Bloková schéma zapojenia IS ISIT KB

Tutoriál: https://www.youtube.com/watch?v=gom_TDEKJa8

Zadania pre študentov zamerané na kapitoly

4. Editácia údajov

Zadanie: Naučte sa, ako efektívne spravovať údaje v ISIT software SK.
Kroky:

- Prečítajte si kapitolu „Editácia údajov“ a oboznámte sa s jej obsahom.

- Diskutujte o dôležitosti správneho spravovania údajov v kontexte kybernetickej bezpečnosti.

4.1 Pridanie záznamov

Zadanie: Naučte sa, ako pridať nové záznamy do systému.
Kroky:

- Otvorte ISIT software SK a prihláste sa do svojho účtu.

- Prejdite do sekcie, kde sa spravujú záznamy (napr. „Riadenie aktív“ alebo „Dokumentácia“).

- Kliknite na tlačidlo „Pridať...“.
- Vyplňte nasledujúce polia:
    - Názov záznamu: [Zadajte názov]
    - Typ záznamu: [Vyberte z rozbaľovacieho zoznamu]
    - Popis: [Zadajte popis záznamu]
    - Ďalšie relevantné údaje: [Vyplňte podľa potreby]
- Kliknite na „Uložiť“ a overte, že sa nový záznam zobrazuje v zozname.
- Napíšte krátku správu o tom, aké údaje ste pridali a prečo sú dôležité.

4.2 Úprava záznamov

Zadanie: Naučte sa, ako upraviť existujúce záznamy.
Kroky:

- Prejdite do sekcie, kde sa nachádzajú existujúce záznamy.
- Vyberte záznam, ktorý chcete upraviť, a kliknite na „Upraviť“.
- Zmeňte nasledujúce údaje:
    - Názov: [Zmeňte názov, ak je to potrebné]
    - Popis: [Upravte popis podľa aktuálnych informácií]
    - Ďalšie relevantné údaje: [Upravte podľa potreby]
- Kliknite na „Uložiť“ a skontrolujte, či sa aktualizované údaje zobrazujú správne.
- Napíšte krátku správu o tom, aké zmeny ste vykonali a prečo boli potrebné.

4.3 Odstránenie záznamov

Zadanie: Naučte sa, ako odstrániť záznamy zo systému.
Kroky:

- Prejdite do sekcie, kde sa nachádzajú záznamy, ktoré chcete odstrániť.
- Vyberte záznam, ktorý chcete odstrániť, a kliknite na „Vymazať...“.
- Systém vás vyzve na potvrdenie akcie. Potvrďte, že chcete záznam skutočne odstrániť.
- Skontrolujte, či záznam už nie je v zozname.

- Napíšte krátku správu o tom, prečo ste sa rozhodli záznam odstrániť a aké to môže mať dôsledky pre systém.

Tieto zadania pomôžu študentom osvojiť si praktické zručnosti v oblasti správy údajov v ISIT software SK a pochopiť dôležitosť správneho spravovania záznamov v kontexte kybernetickej bezpečnosti.

Atlas

pridaj ku každej úlohe príklad pre Žilinská univerzita v Žiline

Tu sú detailné zadania pre študentov zamerané na kapitolu „Editácia údajov“ a jej podkapitoly v ISIT Software User Manual, vrátane príkladov pre Žilinskú univerzitu v Žiline:

4. Editácia údajov

Zadanie: Naučte sa, ako efektívne spravovať údaje v ISIT software SK.
Kroky:

- Prečítajte si kapitolu „Editácia údajov“ a oboznámte sa s jej obsahom.

- Diskutujte o dôležitosti správneho spravovania údajov v kontexte kybernetickej bezpečnosti.

4.1 Pridanie záznamov

Zadanie: Naučte sa, ako pridať nové záznamy do systému.
Kroky:

- Otvorte ISIT software SK a prihláste sa do svojho účtu.

- Prejdite do sekcie, kde sa spravujú záznamy (napr. „Riadenie aktív“ alebo „Dokumentácia“).

- Kliknite na tlačidlo „Pridať...“.

- Vyplňte nasledujúce polia:

  - Názov záznamu: **„Záznam o kybernetickej bezpečnosti pre Žilinskú univerzitu“**
  - Typ záznamu: **„Dokumentácia“**
  - Popis: **„Dokumentácia o opatreniach kybernetickej bezpečnosti na Žilinskej univerzite“**

- Ďalšie relevantné údaje: **„Zabezpečenie prístupu k citlivým údajom študentov“**

- Kliknite na „Uložiť“ a overte, že sa nový záznam zobrazuje v zozname.

- Napíšte krátku správu o tom, aké údaje ste pridali a prečo sú dôležité.
Príklad správy: „Pridali sme záznam o kybernetickej bezpečnosti, aby sme zabezpečili ochranu osobných údajov študentov a dodržiavali legislatívne požiadavky.“

4.2 Úprava záznamov

Zadanie: Naučte sa, ako upraviť existujúce záznamy.
Kroky:

- Prejdite do sekcie, kde sa nachádzajú existujúce záznamy.

- Vyberte záznam, ktorý chcete upraviť, a kliknite na „Upraviť“.

- Zmeňte nasledujúce údaje:

  - Názov: **„Záznam o kybernetickej bezpečnosti pre Žilinskú univerzitu - aktualizovaný“**
  - Popis: **„Aktualizovaná dokumentácia o opatreniach kybernetickej bezpečnosti na Žilinskej univerzite“**
  - Ďalšie relevantné údaje: **„Zabezpečenie prístupu k citlivým údajom študentov - revízia 2026“**

- Kliknite na „Uložiť“ a skontrolujte, či sa aktualizované údaje zobrazujú správne.

- Napíšte krátku správu o tom, aké zmeny ste vykonali a prečo boli potrebné.
Príklad správy: „Upravili sme záznam, aby sme odrážali najnovšie bezpečnostné opatrenia a revíziu dokumentácie, čím zabezpečujeme aktuálnosť informácií.“

4.3 Odstránenie záznamov

Zadanie: Naučte sa, ako odstrániť záznamy zo systému.
Kroky:

- Prejdite do sekcie, kde sa nachádzajú záznamy, ktoré chcete odstrániť.

- Vyberte záznam, ktorý chcete odstrániť, a kliknite na „Vymazať...“.

- Systém vás vyzve na potvrdenie akcie. Potvrďte, že chcete záznam skutočne odstrániť.

- Skontrolujte, či záznam už nie je v zozname.

- Napíšte krátku správu o tom, prečo ste sa rozhodli záznam odstrániť a aké to môže mať dôsledky pre systém.

Príklad správy: „Rozhodli sme sa odstrániť starý záznam o kybernetickej bezpečnosti, pretože obsahoval zastarané informácie, ktoré by mohli viesť k nedorozumeniam a ohrozeniu bezpečnosti údajov.“

Tieto zadania pomôžu študentom osvojiť si praktické zručnosti v oblasti správy údajov v ISIT software SK a pochopiť dôležitosť správneho spravovania záznamov v kontexte kybernetickej bezpečnosti, pričom príklady sú prispôsobené pre Žilinskú univerzitu v Žiline.

5.1 Hlavné menu

Zadanie: Naučte sa, ako používať hlavné menu v ISIT software SK.
Kroky:

- V hlavnom okne sa zamerajte na horné menu, ktoré obsahuje rôzne možnosti.
- Prejdite myšou nad jednotlivé položky menu a pozorujte, ako sa rozbalí zvislé menu.
- Vyberte si jednu z položiek, napríklad „Organizácia“, a kliknite na ňu.
- Preskúmajte, aké možnosti sú k dispozícii v tejto sekcii a aké úlohy môžete vykonávať.
- Napíšte krátku správu o tom, aké funkcie sú dostupné v hlavnom menu a ako môžu prispieť k efektívnemu riadeniu kybernetickej bezpečnosti na Žilinskej univerzite v Žiline.

Príklad správy: „Hlavné menu ISIT software SK umožňuje prístup k rôznym funkciám, ako sú správa organizácie a používateľov, čo je kľúčové pre zabezpečenie efektívneho riadenia kybernetickej bezpečnosti na Žilinskej univerzite v Žiline.“

5.2 Organizácia

Zadanie: Naučte sa, ako spravovať údaje o organizácii v ISIT software SK.
Kroky:

- V hlavnom menu vyberte položku „Organizácia“.
- Preskúmajte, aké možnosti sú k dispozícii na pridanie, úpravu alebo odstránenie údajov o organizácii.
- Pridajte nový záznam pre Žilinskú univerzitu v Žiline, vrátane názvu, adresy a kontaktných údajov.
- Uložte záznam a skontrolujte, či sa zobrazuje v zozname organizácií.
- Napíšte krátku správu o tom, aké údaje ste pridali a prečo sú dôležité pre správu kybernetickej bezpečnosti.

Príklad správy: „Pridali sme záznam o Žilinskej univerzite v Žiline, aby sme zabezpečili správne riadenie a ochranu citlivých údajov študentov a zamestnancov.“

5.3 Používatelia

Zadanie: Naučte sa, ako spravovať používateľské účty v ISIT software SK.
Kroky:

- V hlavnom menu vyberte položku „Používatelia“.

- Preskúmajte, aké možnosti sú k dispozícii na pridanie, úpravu alebo odstránenie používateľských účtov.

- Pridajte nový používateľský účet pre zamestnanca Žilinskej univerzity v Žiline, vrátane mena, priezviska, e-mailu a rolí.

- Uložte záznam a skontrolujte, či sa zobrazuje v zozname používateľov.

- Napíšte krátku správu o tom, aké údaje ste pridali a akú úlohu má tento používateľ v rámci kybernetickej bezpečnosti.
Príklad správy: „Pridali sme používateľský účet pre zamestnanca, ktorý bude zodpovedný za správu kybernetickej bezpečnosti na Žilinskej univerzite v Žiline, čím zabezpečujeme efektívne riadenie bezpečnostných opatrení.“

5.4 Audity

Zadanie: Naučte sa, ako spravovať audity v ISIT software SK.
Kroky:

- V hlavnom menu vyberte položku „Audity“.

- Preskúmajte, aké možnosti sú k dispozícii na pridanie a správu auditov.

- Pridajte nový audit pre Žilinskú univerzitu v Žiline, vrátane názvu auditu, dátumu a popisu.

- Uložte záznam a skontrolujte, či sa zobrazuje v zozname auditov.

- Napíšte krátku správu o tom, aké údaje ste pridali a aký je význam auditu pre kybernetickú bezpečnosť.
Príklad správy: „Pridali sme nový audit, ktorý pomôže identifikovať a vyhodnotiť riziká v oblasti kybernetickej bezpečnosti na Žilinskej univerzite v Žiline.“

5.4.1 Manažment auditov

Zadanie: Naučte sa, ako spravovať záznamy o auditoch.
Kroky:

- V sekcii „Audity“ prejdite na podsekciu „Manažment auditov“.

- Preskúmajte, aké možnosti sú k dispozícii na správu existujúcich auditov.

- Upravte existujúci audit a pridajte nové informácie o jeho priebehu a výsledkoch.

- Uložte zmeny a skontrolujte, či sa aktualizované údaje zobrazujú správne.

- Napíšte krátku správu o tom, aké zmeny ste vykonali a aký je ich význam.
Príklad správy: „Upravili sme záznam o audite, aby sme zahrnuli najnovšie zistenia a odporúčania, čím zvyšujeme úroveň kybernetickej bezpečnosti na Žilinskej univerzite v Žiline.“

5.4.2 R A S C I

Zadanie: Naučte sa, ako používať maticu RASCI pre správu rolí a zodpovedností.
Kroky:

- V sekcii „Audity“ prejdite na podsekciu „R A S C I“.

- Preskúmajte, aké možnosti sú k dispozícii na definovanie rolí a zodpovedností.

- Vytvorte maticu RASCI pre projekt kybernetickej bezpečnosti na Žilinskej univerzite v Žiline.

- Uložte maticu a skontrolujte, či sa zobrazuje správne.

- Napíšte krátku správu o tom, aké úlohy a zodpovednosti ste definovali a prečo sú dôležité.
Príklad správy: „Vytvorili sme maticu RASCI, ktorá jasne definuje úlohy a zodpovednosti členov tímu pre projekt kybernetickej bezpečnosti, čím zabezpečujeme efektívnu spoluprácu a riadenie.“

5.4.3 Ciele riadenia a opatrenia

Zadanie: Naučte sa, ako spravovať ciele riadenia a opatrenia v ISIT software SK.
Kroky:

- V sekcii „Audity“ prejdite na podsekciu „Ciele riadenia a opatrenia“.

- Preskúmajte, aké možnosti sú k dispozícii na pridanie a správu cieľov a opatrení.

- Pridajte nový cieľ riadenia pre Žilinskú univerzitu v Žiline, vrátane popisu a očakávaných výsledkov.

- Uložte záznam a skontrolujte, či sa zobrazuje v zozname cieľov.

- Napíšte krátku správu o tom, aké ciele ste pridali a aký je ich význam pre kybernetickú bezpečnosť.
Príklad správy: „Pridali sme cieľ riadenia, ktorý sa zameriava na zlepšenie ochrany osobných údajov študentov, čím posilňujeme kybernetickú bezpečnosť na Žilinskej univerzite v Žiline.“

5.5 Školenia

Zadanie: Naučte sa, ako spravovať školenia v ISIT software SK.
Kroky:

- V hlavnom menu vyberte položku „Školenia“.

- Preskúmajte, aké možnosti sú k dispozícii na pridanie a správu školení.

- Pridajte nové školenie pre zamestnancov Žilinskej univerzity v Žiline, vrátane názvu, dátumu a popisu.

- Uložte záznam a skontrolujte, či sa zobrazuje v zozname školení.

- Napíšte krátku správu o tom, aké školenie ste pridali a aký je jeho význam pre zvyšovanie povedomia o kybernetickej bezpečnosti.
Príklad správy: „Pridali sme školenie o kybernetickej bezpečnosti, ktoré pomôže zamestnancom lepšie chrániť citlivé údaje a dodržiavať legislatívne požiadavky.“

5.6 Legislatíva

Zadanie: Naučte sa, ako spravovať legislatívne dokumenty v ISIT software SK.
Kroky:

- V hlavnom menu vyberte položku „Legislatíva“.

- Preskúmajte, aké možnosti sú k dispozícii na pridanie a správu legislatívnych dokumentov.

- Pridajte nový legislatívny dokument, ktorý sa týka kybernetickej bezpečnosti, vrátane názvu a popisu.

- Uložte záznam a skontrolujte, či sa zobrazuje v zozname legislatívy.

- Napíšte krátku správu o tom, aký dokument ste pridali a aký je jeho význam pre dodržiavanie legislatívnych požiadaviek.
Príklad správy: „Pridali sme legislatívny dokument, ktorý upravuje ochranu osobných údajov, čím zabezpečujeme dodržiavanie zákonných požiadaviek na Žilinskej univerzite v Žiline.“

5.7 Číselníky

Zadanie: Naučte sa, ako spravovať číselníky v ISIT software SK. Číselníky sú dôležité pre správu údajov a zabezpečujú, že všetky informácie sú konzistentné a správne. V tejto úlohe sa zameriate na pridávanie, úpravu a správu rôznych číselníkov.

Tutoriál: https://www.youtube.com/watch?v=tHpPAOXObjI

5.7.1 Číselník zamestnancov

Kroky:

- V hlavnom menu vyberte položku „Číselníky“ a následne „Zamestnanci“.

- Preskúmajte existujúce záznamy zamestnancov.

- Pridajte nový záznam pre zamestnanca Žilinskej univerzity v Žiline, vrátane nasledujúcich údajov:

  - Meno
  - Priezvisko
  - Funkcia
  - Oddelenie
  - E-mail
  - Telefónne číslo

- Uložte záznam a skontrolujte, či sa zobrazuje v zozname zamestnancov.

- Napíšte krátku správu o tom, aké údaje ste pridali a aký je ich význam pre správu kybernetickej bezpečnosti.
Príklad správy: „Pridali sme záznam o zamestnancovi, ktorý bude zodpovedný za školenia v oblasti kybernetickej bezpečnosti, čím zabezpečujeme efektívne vzdelávanie zamestnancov na Žilinskej univerzite v Žiline.“

5.7.2 Číselník pracovných pozícií

Kroky:

- V sekcii „Číselníky“ vyberte „Pracovné pozície“.

- Preskúmajte existujúce pracovné pozície.

- Pridajte novú pracovnú pozíciu, napríklad „Špecialista na kybernetickú bezpečnosť“, vrátane nasledujúcich údajov:

  - Názov pozície
  - Popis pozície
  - Požiadavky na vzdelanie a skúsenosti

- Uložte záznam a skontrolujte, či sa zobrazuje v zozname pracovných pozícií.

- Napíšte krátku správu o tom, aké údaje ste pridali a aký je ich význam pre organizáciu.
Príklad správy: „Pridali sme pracovnú pozíciu pre špecialistu na kybernetickú bezpečnosť, aby sme posilnili tím zodpovedný za ochranu citlivých údajov na Žilinskej univerzite v Žiline.“

5.7.3 Číselník tretích strán

Kroky:

- V sekcii „Číselníky“ vyberte „Tretie strany“.

- Preskúmajte existujúce záznamy tretích strán.

- Pridajte nový záznam pre dodávateľa služieb, napríklad „IT Služby s.r.o.“, vrátane nasledujúcich údajov:

  - Názov firmy
  - IČO
  - DIČ
  - Adresa
  - Popis predmetu činnosti

- Uložte záznam a skontrolujte, či sa zobrazuje v zozname tretích strán.

- Napíšte krátku správu o tom, aké údaje ste pridali a aký je ich význam pre správu dodávateľských vzťahov.
Príklad správy: „Pridali sme záznam o dodávateľovi IT Služby s.r.o., ktorý poskytuje technickú podporu, čím zabezpečujeme efektívne riadenie našich IT služieb na Žilinskej univerzite v Žiline.“

5.7.4 Číselník školení

Kroky:

- V sekcii „Číselníky“ vyberte „Školenia“.

- Preskúmajte existujúce školenia.

- Pridajte nové školenie, napríklad „Základy kybernetickej bezpečnosti“, vrátane nasledujúcich údajov:

  - Názov školenia
  - Popis školenia

- Dátum konania
- Cieľová skupina

- Uložte záznam a skontrolujte, či sa zobrazuje v zozname školení.

- Napíšte krátku správu o tom, aké školenie ste pridali a aký je jeho význam pre zvyšovanie povedomia o kybernetickej bezpečnosti.
Príklad správy: „Pridali sme školenie o základoch kybernetickej bezpečnosti, ktoré pomôže zamestnancom lepšie chrániť citlivé údaje a dodržiavať legislatívne požiadavky na Žilinskej univerzite v Žiline.“

5.7.5 Číselník legislatívy

Kroky:

- V sekcii „Číselníky“ vyberte „Legislatíva“.

- Preskúmajte existujúce legislatívne dokumenty.

- Pridajte nový legislatívny dokument, ktorý sa týka ochrany osobných údajov, vrátane nasledujúcich údajov:

- Názov dokumentu
- Popis
- Dátum účinnosti

- Uložte záznam a skontrolujte, či sa zobrazuje v zozname legislatívy.

- Napíšte krátku správu o tom, aký dokument ste pridali a aký je jeho význam pre dodržiavanie legislatívnych požiadaviek.
Príklad správy: „Pridali sme legislatívny dokument o ochrane osobných údajov, čím zabezpečujeme dodržiavanie zákonných požiadaviek na Žilinskej univerzite v Žiline.“

5.8 Bezpečnosť IKT

Tutoriál: https://www.youtube.com/watch?v=amkhtLPkyjM

Zadanie: Naučte sa, ako spravovať a zabezpečovať informačné a komunikačné technológie (IKT) v ISIT software SK. V tejto úlohe sa zameriate na rôzne aspekty bezpečnosti IKT, ktoré sú kľúčové pre ochranu citlivých údajov a systémov na Žilinskej univerzite v Žiline.

5.8.1 Základné informácie

Kroky:

- Prejdite si základné informácie o bezpečnosti IKT v ISIT software SK.

- Zaznamenajte si kľúčové pojmy a definície, ktoré sú dôležité pre pochopenie bezpečnosti IKT.

- Napíšte krátku správu o tom, aké základné informácie sú dôležité pre zabezpečenie IKT na Žilinskej univerzite v Žiline.
Príklad správy: „Základné informácie o bezpečnosti IKT sú kľúčové pre ochranu citlivých údajov a systémov, čo je nevyhnutné pre zabezpečenie dôvery študentov a zamestnancov na Žilinskej univerzite v Žiline.“

5.8.2 Personálna bezpečnosť

Kroky:

- Preskúmajte, aké opatrenia sú zahrnuté v oblasti personálnej bezpečnosti.

- Zaznamenajte si, aké údaje sú potrebné na evidenciu zamestnancov a ich zodpovedností.

- Pridajte nový záznam pre zamestnanca, ktorý bude zodpovedný za personálnu bezpečnosť, vrátane nasledujúcich údajov:

  - Meno
  - Priezvisko
  - Funkcia
  - Zodpovednosti

- Uložte záznam a skontrolujte, či sa zobrazuje v zozname zamestnancov.

- Napíšte krátku správu o tom, aké opatrenia v oblasti personálnej bezpečnosti sú dôležité pre ochranu citlivých údajov.
Príklad správy: „Zabezpečenie personálnej bezpečnosti je kľúčové pre ochranu citlivých informácií, pretože zamestnanci musia byť riadne vyškolení a informovaní o svojich zodpovednostiach.“

5.8.3 Dopytovací formulár

Kroky:

- Preskúmajte, aké informácie sú potrebné na vyplnenie dopytovacieho formulára.

- Vyplňte dopytovací formulár pre Žilinskú univerzitu v Žiline, ktorý sa týka kybernetickej bezpečnosti.

- Uložte formulár a skontrolujte, či sa zobrazuje v zozname dopytovacích formulárov.

- Napíšte krátku správu o tom, aké informácie ste zahrnuli do formulára a aký je jeho význam.
Príklad správy: „Dopytovací formulár pomáha identifikovať potreby v oblasti kybernetickej bezpečnosti a zabezpečuje, že všetky aspekty sú riadne zohľadnené.“

5.8.4 Import aktív

Tutoriál: https://www.youtube.com/watch?v=C-Qzv1oR3Mo

Kroky:

- Preskúmajte, aké možnosti sú k dispozícii na import aktív do systému.

- Pripravte súbor s aktívami, ktoré sú potrebné pre Žilinskú univerzitu v Žiline.

- Importujte súbor do ISIT software SK a skontrolujte, či sa aktíva správne zobrazujú v zozname.

- Napíšte krátku správu o tom, aké aktíva ste importovali a aký je ich význam pre správu kybernetickej bezpečnosti.
Príklad správy: „Import aktív umožňuje efektívne spravovanie a evidenciu všetkých technických prostriedkov, čo je nevyhnutné pre zabezpečenie kybernetickej bezpečnosti na Žilinskej univerzite v Žiline.“

5.8.5 Zoznam aktív

Kroky:

- Preskúmajte existujúci zoznam aktív v ISIT software SK.

- Zaznamenajte si, aké typy aktív sú zahrnuté a aké informácie sú k nim priradené.

- Pridajte nové aktívum, napríklad „Server pre správu databáz“, vrátane nasledujúcich údajov:

  - Názov aktíva
  - Typ aktíva
  - Umístění
  - Zodpovedná osoba

- Uložte záznam a skontrolujte, či sa zobrazuje v zozname aktív.

- Napíšte krátku správu o tom, aké aktíva ste pridali a aký je ich význam pre správu kybernetickej bezpečnosti.
Príklad správy: „Pridali sme server pre správu databáz, ktorý je kľúčový pre uchovávanie a ochranu citlivých údajov na Žilinskej univerzite v Žiline.“

5.8.6 Riadenie aktív

Tutoriál: https://www.youtube.com/watch?v=J7DFTwtiCVQ

Kroky:

- Preskúmajte, aké možnosti sú k dispozícii na riadenie aktív v ISIT software SK.

- Zaznamenajte si, aké informácie sú potrebné na správu aktív.

- Upravte existujúce aktívum a pridajte nové informácie o jeho stave a zodpovednostiach.

- Uložte zmeny a skontrolujte, či sa aktualizované údaje zobrazujú správne.

- Napíšte krátku správu o tom, aké zmeny ste vykonali a aký je ich význam.
Príklad správy: „Upravili sme záznam o aktíve, aby sme zahrnuli aktuálny stav a zodpovednosti, čím zabezpečujeme efektívne riadenie a ochranu našich technických prostriedkov.“

5.8.7 Riadenie tretích strán

Kroky:

- Preskúmajte, aké opatrenia sú zahrnuté v oblasti riadenia tretích strán.

- Zaznamenajte si, aké informácie sú potrebné na evidenciu tretích strán, ktoré majú prístup k systémom Žilinskej univerzity v Žiline.

- Pridajte nový záznam pre tretiu stranu, napríklad „Dodávateľ IT služieb“, vrátane nasledujúcich údajov:

  - Názov firmy
  - Kontaktná osoba
  - Úroveň prístupu

- Uložte záznam a skontrolujte, či sa zobrazuje v zozname tretích strán.

- Napíšte krátku správu o tom, aké údaje ste pridali a aký je ich význam pre správu bezpečnosti.

Príklad správy: „Pridali sme dodávateľa IT služieb, aby sme zabezpečili, že všetky externé prístupy sú riadne monitorované a kontrolované.“

5.8.8 Analýza rizík

Tutoriály

Analýza rizík - úvod: https://youtu.be/7bk8PKuFDIY

Podrobná analýza rizík: https://www.youtube.com/watch?v=75ZY-Uub294

Prioritizácia rizík: https://www.youtube.com/watch?v=X8iXvXi0K04

Monitorovanie rizík a exportovanie reportov: https://www.youtube.com/watch?v=QxRuQ4-Ym5Q

Kroky:

- Preskúmajte, aké možnosti sú k dispozícii na vykonanie analýzy rizík v ISIT software SK.
- Zaznamenajte si, aké informácie sú potrebné na vykonanie analýzy rizík.
- Vykonajte analýzu rizík pre Žilinskú univerzitu v Žiline, vrátane identifikácie hrozieb a zraniteľností.
- Uložte výsledky analýzy a skontrolujte, či sa zobrazujú správne.
- Napíšte krátku správu o tom, aké riziká ste identifikovali a aké opatrenia navrhujete.

Príklad správy: „Vykonali sme analýzu rizík, ktorá identifikovala potenciálne hrozby pre naše systémy, a navrhli sme opatrenia na ich minimalizáciu.“

5.8.9 Relácie aktív

Tutoriál: https://www.youtube.com/watch?v=-QZOoohdi1I

Kroky:

- Preskúmajte, aké možnosti sú k dispozícii na správu relácií aktív.
- Zaznamenajte si, aké informácie sú potrebné na evidenciu relácií medzi aktívami.
- Pridajte novú reláciu medzi dvoma aktívami, napríklad medzi serverom a databázou.
- Uložte záznam a skontrolujte, či sa zobrazuje v zozname relácií aktív.

- Napíšte krátku správu o tom, aké relácie ste pridali a aký je ich význam pre správu aktív.
Príklad správy: „Pridali sme reláciu medzi serverom a databázou, aby sme zabezpečili, že všetky prístupy sú riadne monitorované a spravované.“

5.8.10 Registratúrny poriadok a registratúrny plán

Kroky:

- Preskúmajte, aké informácie sú zahrnuté v registratúrnom poriadku a pláne.

- Zaznamenajte si, aké dokumenty sú potrebné na dodržiavanie registratúrneho poriadku.

- Pripravte a pridajte nový registratúrny plán pre Žilinskú univerzitu v Žiline.

- Uložte plán a skontrolujte, či sa zobrazuje v zozname registratúrnych plánov.

- Napíšte krátku správu o tom, aké dokumenty ste zahrnuli a aký je ich význam pre správu dokumentácie.
Príklad správy: „Pripravili sme registratúrny plán, ktorý zabezpečuje, že všetky dokumenty sú riadne evidované a spravované v súlade s legislatívnymi požiadavkami.“

5.8.11 Manažér informačnej bezpečnosti

Kroky:

- Preskúmajte, aké úlohy a zodpovednosti má manažér informačnej bezpečnosti.

- Zaznamenajte si, aké informácie sú potrebné na evidenciu manažéra.

- Pridajte nový záznam pre manažéra informačnej bezpečnosti na Žilinskej univerzite v Žiline, vrátane nasledujúcich údajov:

  - Meno
  - Priezvisko
  - Funkcia
  - Zodpovednosti

- Uložte záznam a skontrolujte, či sa zobrazuje v zozname manažérov.

- Napíšte krátku správu o tom, aké úlohy má manažér informačnej bezpečnosti a aký je jeho význam pre organizáciu.
Príklad správy: „Manažér informačnej bezpečnosti je zodpovedný za ochranu citlivých

údajov a zabezpečenie dodržiavania legislatívnych požiadaviek na Žilinskej univerzite v Žiline."

5.8.12 Manažment bezpečnostných incidentov

Kroky:

- Preskúmajte, aké opatrenia sú zahrnuté v manažmente bezpečnostných incidentov.
- Zaznamenajte si, aké informácie sú potrebné na evidenciu incidentov.
- Pridajte nový záznam o bezpečnostnom incidente, vrátane nasledujúcich údajov:
    - Dátum incidentu
    - Popis incidentu
    - Zodpovedná osoba
- Uložte záznam a skontrolujte, či sa zobrazuje v zozname incidentov.
- Napíšte krátku správu o tom, aké incidenty ste evidovali a aké opatrenia ste prijali.

Príklad správy: „Evidovali sme bezpečnostný incident, ktorý bol promptne riešený, čím sme zabezpečili ochranu citlivých údajov na Žilinskej univerzite v Žiline."

5.8.13 Manažment kontrol dodržiavania bezpečnostnej politiky

Kroky:

- Preskúmajte, aké kontroly sú zahrnuté v manažmente dodržiavania bezpečnostnej politiky.
- Zaznamenajte si, aké informácie sú potrebné na evidenciu kontrol.
- Pridajte nový záznam o kontrole dodržiavania bezpečnostnej politiky, vrátane nasledujúcich údajov:
    - Dátum kontroly
    - Popis kontroly
    - Výsledok kontroly
- Uložte záznam a skontrolujte, či sa zobrazuje v zozname kontrol.
- Napíšte krátku správu o tom, aké kontroly ste vykonali a aké sú ich výsledky.

Príklad správy: „Vykonali sme kontrolu dodržiavania bezpečnostnej politiky, ktorá potvrdila, že všetky procesy sú v súlade s legislatívnymi požiadavkami."

5.8.14 Príjem a spracovanie bezpečnostných varovaní NBÚ

Kroky:

- Preskúmajte, aké postupy sú zahrnuté v príjme a spracovaní bezpečnostných varovaní.
- Zaznamenajte si, aké informácie sú potrebné na evidenciu varovaní.
- Pridajte nový záznam o bezpečnostnom varovaní, vrátane nasledujúcich údajov:
    - Dátum varovania
    - Popis varovania
    - Zodpovedná osoba
- Uložte záznam a skontrolujte, či sa zobrazuje v zozname varovaní.
- Napíšte krátku správu o tom, aké varovania ste prijali a aké opatrenia ste prijali.
Príklad správy: „Prijali sme bezpečnostné varovanie od NBÚ, ktoré sme promptne spracovali a prijali potrebné opatrenia na ochranu našich systémov.“

5.8.15 Manažment bezpečnostných varovaní NBÚ

Kroky:

- Preskúmajte, aké opatrenia sú zahrnuté v manažmente bezpečnostných varovaní.
- Zaznamenajte si, aké informácie sú potrebné na evidenciu varovaní.
- Pridajte nový záznam o manažmente bezpečnostného varovania, vrátane nasledujúcich údajov:
    - Dátum varovania
    - Popis varovania
    - Zodpovedná osoba
- Uložte záznam a skontrolujte, či sa zobrazuje v zozname varovaní.
- Napíšte krátku správu o tom, aké varovania ste spracovali a aké sú ich výsledky.
Príklad správy: „Spracovali sme bezpečnostné varovanie od NBÚ a prijali sme opatrenia na zabezpečenie našich systémov.“

5.8.16 Zoznam primárnych aktív – BIA

Tutoriál: https://youtu.be/yfkq3cC_LJM

Kroky:

- Preskúmajte, aké informácie sú zahrnuté v zozname primárnych aktív.

- Zaznamenajte si, aké aktíva sú považované za primárne a aké sú ich zodpovednosti.

- Pridajte nové primárne aktívum, napríklad „Hlavný server“, vrátane nasledujúcich údajov:

  - Názov aktíva
  - Typ aktíva
  - Zodpovedná osoba

- Uložte záznam a skontrolujte, či sa zobrazuje v zozname primárnych aktív.

- Napíšte krátku správu o tom, aké aktíva ste pridali a aký je ich význam pre správu kybernetickej bezpečnosti.
Príklad správy: „Pridali sme hlavný server ako primárne aktívum, ktoré je kľúčové pre uchovávanie a ochranu citlivých údajov na Žilinskej univerzite v Žiline.“

5.8.17 CMDB Konfiguračný manažment databázy

Kroky:

- Preskúmajte, aké informácie sú zahrnuté v konfiguračnej manažment databáze (CMDB).

- Zaznamenajte si, aké aktíva sú zahrnuté a aké informácie sú k nim priradené.

- Pridajte nové aktívum do CMDB, vrátane nasledujúcich údajov:

  - Názov aktíva
  - Typ aktíva
  - Verzia
  - Zodpovedná osoba

- Uložte záznam a skontrolujte, či sa zobrazuje v zozname aktív v CMDB.

- Napíšte krátku správu o tom, aké aktíva ste pridali a aký je ich význam pre správu IT infraštruktúry.
Príklad správy: „Pridali sme nové aktívum do CMDB, čím zabezpečujeme presnú evidenciu a správu našich IT systémov na Žilinskej univerzite v Žiline.


Financované
Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM
KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE