

Příloha č. 1 – Specifikace předmětu plnění

### Předmět dodávky

#### Funkční požadavky:

Požadavky na funkcionalitu systému:

- Vytvoření číselníku auditních jednotek
  - Synchronizace číselníku pracovišť FNUSA (zdroj MSSQL) min 1x denně
  - interní auditoři včetně rozdělení dle specifikace
  - procesy
  - kontrolní otázky k ISO normám (9001, 13485, 15189, 27000)
  - kontrolní otázky dle legislativních požadavků (zákony, vyhlášky, nařízení, pokyny SÚKLu příp. jiných subjektů)
  - kontrolní otázky dle celonemocničních požadavků (viz směrnice, pracovní postupy...)
- tvorba harmonogramu interních auditů v tříletých cyklech
  - tvorba více harmonogramů interních auditů dle skupin
- příprava plánu a vlastního auditu
  - tvorba dotazníku — výběrem otázek z číselníku — možnost kombinovat z různých norem a požadavků
  - zpracování
  - připomínkování (auditory, auditovaným pracovištěm)z
  - vyhodnocení
  - uzavření auditu
  - rozeslání výsledků na oprávněné osoby
- evidence, sledování a kontrola nápravných opatření
- zadání konkrétní osobě úkolu vyplývajícího ze zjištění interního auditu
- Roční souhrnné vyhodnocení jednotlivých pracovišť a celkově za FNUSA
- Dle procesu daného pracoviště vyhledávání i v historii, sumarizace dle vydefinovaných kritérií (pracoviště, kapitola normy apod.)
- Fulltxtové vyhledávání
- Český jazyk
- Ochrana — kyberbezpečnost, GDPR (dle legislativy a interních požadavků FNUSA)

Řešení musí splňovat požadavky metodik a doporučení Českého institutu interních auditorů

#### Nefunkční požadavky:

Požadavky na bezpečnost:

##### Obecné —

Nabízený systém musí splňovat požadavky na řízení bezpečnosti informací v souladu s platnou legislativou, standardy v oblasti řízení bezpečnosti informací. Požadavky jsou rozděleny dle oblastí, které požaduje zákon

č. 181/2014 Sb., o kybernetické bezpečnosti, v platném znění (ZoKB). Vzhledem k tomu, že poptávaný systém není určen jako VIS (KII), nejsou zahrnuty všechny požadavky tohoto zákona. Systém nebude obsahovat údaje klasifikované dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Předložené bezpečnostní požadavky lze chápat jako nutné minimum a zároveň je přihlédnuto k povaze informačního nástroje, který bude předmětem veřejné zakázky.

##### Řízení přístupů —

Cílem řízení přístupů je přidělit jedinečné identifikátory jednotlivým uživatelům a administrátorům přistupujícím k softwaru (aplikaci). Tyto identifikátory musí být řízeny a evidovány, stejně jako přístupová práva a oprávnění aplikací a technických účtů.

- Řízení přístupu musí být založeno na základě skupin a rolí.
- Musí probíhat ověřování proti záznamům v LDAP, později možná integrace na AD.
- Pravidla pro nastavení hesel musí vycházet z požadavků ZoKB.
- Další pravidla pro řízení přístupů musí být v souladu s těmito požadavky:

- o Všem uživatelům a administrátorům budou přidělena pouze nezbytná přístupová práva.

Musí být zajištěno oddělení neslučitelných rolí (např. zadavatel, schvalovatel apod.) V případě servisních účtů musí být zajištěna změna implicitního hesla.

#### **Ochrana před škodlivým kódem —**

V rámci softwaru (aplikace) musí být umožněno implementovat způsob řešení ochrany před škodlivým kódem:

- o Umožnit nainstalovat agenta pro detekci a odstranění škodlivých programů, který bude nejméně jednou denně aktualizován.
- o Software (aplikace) musí být pravidelně aktualizována.
- o Software (aplikace) musí být prověřitelná z hlediska možných zranitelností.
- o Software (aplikace) nesmí obsahovat žádné známé kritické zranitelnosti, vysoké zranitelnosti a střední zranitelnosti (dle CVE score).
- o V prostředí softwaru (aplikace) musí být zakázáno vzdálené spouštění kódu ze zdroje mimo jeho prostředí.

Odolnost proti zranitelnostem může být v rámci zakázky ověřena zadavatelem prostřednictvím penetračních testů i opakovaných po celou dobu poskytování plnění.

#### **Důvěrnost a integrita —**

Software (aplikace) musí umožňovat zajištění důvěrnosti a integrity dat na úrovni databáze, a to i před správci provozního prostředí (vyjma administrátorů DB).

Software (aplikace) musí zajistit důvěrnost a integritu dat na celé cestě mezi databázovým serverem a klientem, tedy je požadováno zabezpečené propojení mezi všemi architektonickými vrstvami systému vyjma zásahů a úprav realizovaných administrátory DB.

Důvěrnost a integrita dat musí být zachována i při zálohování a archivaci, a to jak při vlastním procesu, tak i následně vzhledem k médiím, na nichž jsou zálohy a archivní data uloženy vyjma zásahů a úprav realizovaných administrátory DB.

#### **Auditovatelnost a nepopíratelnost —**

Software (aplikace) musí zajišťovat auditovatelnost dat i procesů. Jedná se zejména o přístupy a změny v datech pro jednotlivé objekty (princip zajištění nepopíratelnosti). Auditovatelný musí být také proces řízení identit uživatelů.

Logy softwaru (aplikace) musí být integrovatelné do centrálního řešení pro vyhodnocování provozních a bezpečnostních logů (LOG management).

Zaznamenávání událostí zohledňuje technické možnosti softwaru (aplikace) a pro sběr záznamů ukládá minimálně tyto typy událostí:

- a) přihlášení a odhlášení uživatelů a administrátorů, a to včetně neúspěšných pokusů
- b) činnosti provedené administrátory, o použití privilegovaných účtů, např. účtu supervisor, administrátora,
- c) spuštění a ukončení softwaru (aplikace)
- d) změny konfigurací,
- e) úspěšné i neúspěšné činnosti vedoucí ke změně přístupových oprávnění,
- f) zahájení a ukončení činností zařízení a aplikací
- g) automatická varovná nebo chybová hlášení zařízení a aplikací
- h) přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností

i) použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.  
Všechny záznamy o činnosti v systému musí být zabezpečeny proti:

- a) neoprávněnému přístupu k datům (zachování důvěrnosti);
- b) neoprávněné manipulaci (zachování integrity a prokazatelnosti, resp. principu nepopiratelnosti)
- c) ztrátě uložených informací v požadované době dostupnosti záznamů (zálohování a archivace).

Přístup k záznamům o činnosti musí být umožněn pouze oprávněným osobám (nemusí být administrátoři daného provozního prostředí).

#### **Kryptografické prostředky —**

Data a informace zpracovávaná v rámci softwaru (aplikace) musí být chráněna proti zneužití vhodnými kryptografickými metodami, které zajistí pouze autorizovaný přístup k těmto datům a informacím. Šifrování uložených dat NÚKIB pouze doporučuje, a to v návaznosti na typ a charakter dat a v návaznosti na možné technologické řešení.

Informační systém by měl být připraven využívat aktuálně odolné kryptografické algoritmy dle doporučení NÚKIB. Toto doporučení lze nalézt na:

<https://www.govcert.cz/cs/doporučení-v-oblasti-kryptografických-prostředků/>

V případě použití jiného, než doporučeného algoritmu by mělo být toto použití řádně odůvodněno.

#### **Zálohování a obnova —**

Software (aplikace) musí umožňovat průběžné i dávkové zálohování všech dat, která jsou dotčena užíváním, tedy nejen těch, která jsou uložena v databázi ale současně i dalších nastavení a konfigurací, která vznikají a jsou modifikována v průběhu užívání.

Zálohování a jeho dat bude řešeno centrálně Zadavatelem. Zálohována jsou pouze data uložená v primárních datových úložištích Zadavatele.

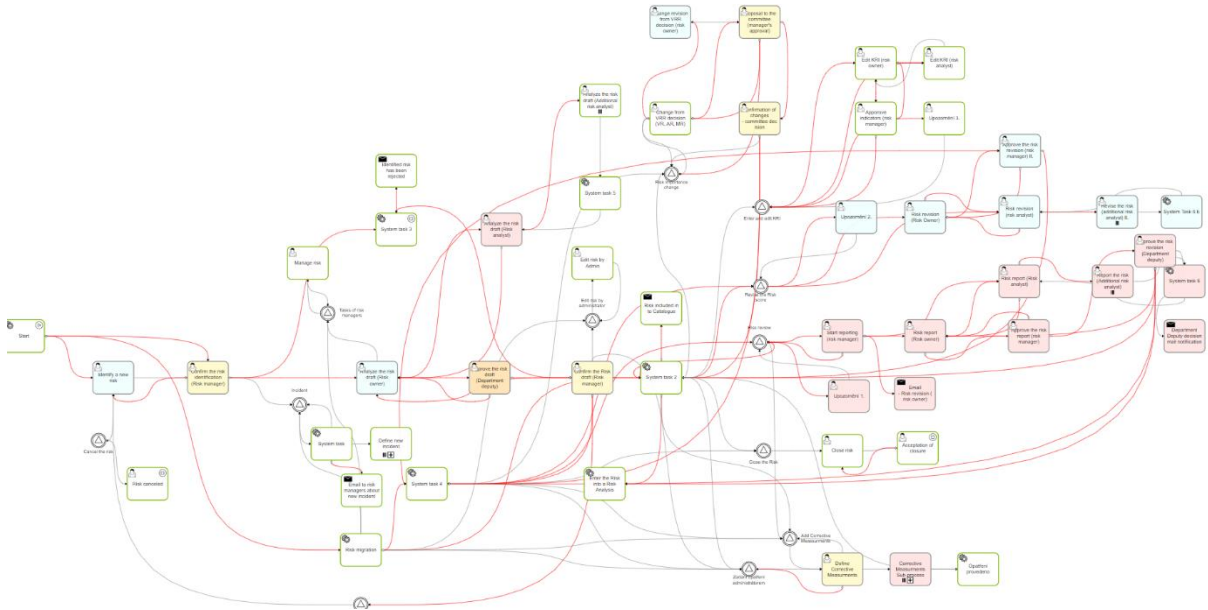
#### **Návrh řešení – obecná východiska**

SW pro řízení systému kvality ( dále jen QA) je postaveno na platformě Team assistant. Dílčí funkční vlastnosti aplikace budou v souladu s požadavky Zadavatele modifikovány tak, jak je to uvedeno v dalších kapitolách tohoto dokumentu.

Z technického hlediska se jedná o moderní třívrstvou aplikaci s daty uloženými v relační databázi, aplikační serverovou vrstvou s moderní objektovou architekturou SOA s úplným přístupem prostřednictvím rozhraní webových služeb a klientskou přístupovou vrstvou ve formě webového prohlížeče. Samozřejmostí je autentifikace pomocí LDAP serverů (podpora i pro MS Active Directory).

Součástí aplikace Team assistant je nástroj na vlastní modelování procesů, tvorbu tzv. **šablon** procesů, aplikačních formulářů, tabulkových reportů a tiskových sestav bez nutnosti programování a vlastní prostředí pro běh a správu jednotlivých úkolů konkrétních instancí procesů. V rámci dodávky máme připraveny standardní šablony procesů pokrývající zadání – např. plánování interního auditu, řízení rizik, ISMS, kybernetické bezpečnosti atd.

Příklad šablony – řízení rizik.

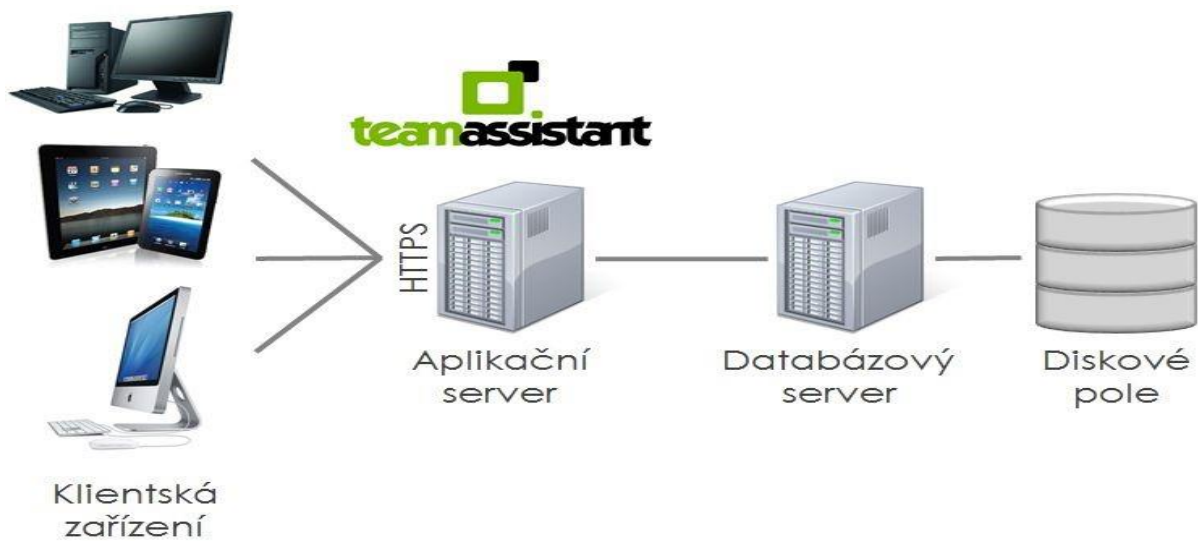


Napojení na jiné aplikace je možné prostřednictvím datové integrace (přímo jsou podporovány DB linky do obvyklých relačních databází a CSV souborové rozhraní) a prostřednictvím aplikační integrace (přímo je podporována integrace pomocí webových služeb, API).

Pro grafický záznam workflow procesu je k dispozici modelovací nástroj s podporou BPMN 2.0. Klíčové vlastnosti řešení:

- Jednoduchost – důraz na jednoduché ovládání ve stylu moderních webových aplikací
- Flexibilita – změny procesů, karet, obrazovek - rychle a jednoduše
- Škálovatelnost – zvládne řádové nárůsty počtu projektů, sledovaných entit nebo uživatelů.  
Pokud je to z pohledu výkonu potřeba, stačí pouze posílit technickou HW infrastrukturu.
- Základem je ověřené fungující řešení
- Přesně na míru potřebám a požadavkům Zadavatele
- Ukládání dokumentů

## Technická architektura

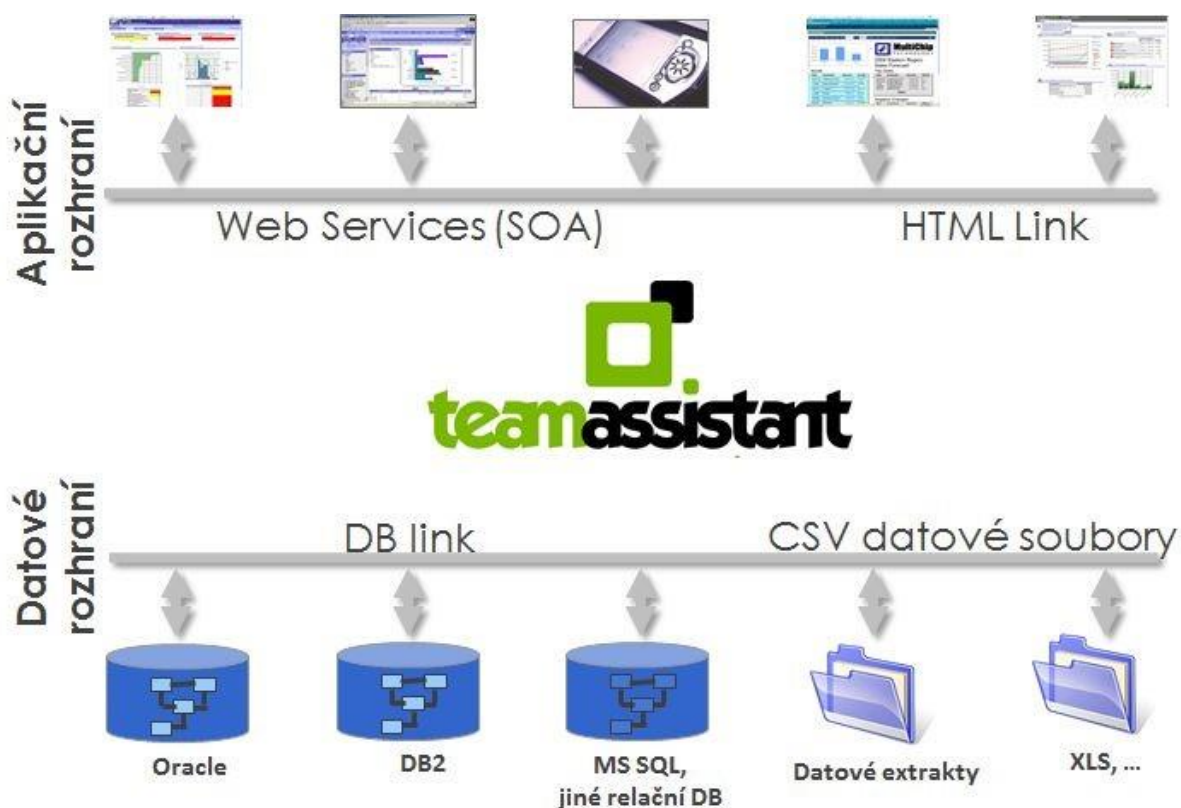


Z technického hlediska se jedná o moderní třívrstvou aplikaci s daty uloženými v relační databázi Oracle, MS SQL (příp. jiné), aplikační serverovou vrstvou s moderní objektovou architekturou SOA s úplným přístupem prostřednictvím rozhraní webových služeb a klientskou přístupovou vrstvou prostřednictvím webového prohlížeče z libovolné platformy (například: PC, MAC, IOS, Android). Na straně klientského zařízení není nutné provádět žádnou instalaci. Webový prohlížeč musí podporovat šifrovanou komunikaci podle standardu HTTPS a dále JavaScript. Žádné další požadavky nejsou na prohlížeč kladeny. V závislosti na typu prohlížeče se mírně mohou lišit jednotlivé ovládací prvky aplikace. Aplikace Team assistant je primárně testována pro tyto typy prohlížečů:

- Internet Explorer
- Edge
- Mozilla Firefox
- Google Chrome
- Opera
- Safari

Zabezpečení komunikace uživatele se serverem je provedeno pomocí běžných standardů používaných například pro elektronickou komunikaci s bankou. Samozřejmostí je autentifikace uživatelů pomocí LDAP serverů (například MS Active Directory).

## Integrační architektura



Pro snadné začlenění aplikace Team assistant do stávajícího IT prostředí Zadavatele slouží široké možnosti aplikační a datové integrace. Z pohledu aplikační integrace je primárně podporována integrace prostřednictvím webových služeb. Tato integrace může být obousměrná:

- Aplikace Team assistant volá webové služby integrované aplikace, prostřednictvím kterých může získávat informace nebo informace do dané aplikace zapisovat. Předpokladem je, že integrovaná aplikace disponuje dokumentovaným aplikačním rozhraním. V případě, že je nezbytné vytvořit aplikační rozhraní s aplikací, která webové služby nepodporuje, je nutné v součinnosti s dodavatelem této aplikace vytvořit integrační aplikační vrstvu, která s danou aplikací komunikuje prostřednictvím nativního aplikačního interface a s aplikací Team assistant prostřednictvím webových služeb. V tomto případě je vždy vhodné zvážit, zda není ekonomičtější využít datovou integraci.
- Integrovaná (externí) aplikace volá webové služby aplikace Team assistant. Team assistant obsahuje webové služby realizující komunikaci s klientskou aplikací (tzv. front-end vrstvu) a webové služby řídící běh procesů (tzv. back-end vrstvu). Integrovaná aplikace může využívat obě vrstvy.

Speciálním případem aplikační integrace je jednoduchá integrace pomocí HTML linků. Takto lze snadno a rychle začlenit aplikaci Team assistant a nebo její část do stávajícího řešení, které má stejnou koncepční architekturu klientské aplikace (např. do různých portálových aplikací nebo

aplikací, které jsou primárně obsluhovány webovým klientem). Z druhé strany Team assistant také podporuje propojení pomocí HTML linků. Pro ilustraci uvádíme scénáře:

- V případě, kdy je součástí IT infrastruktury zákazníka Document Management System (DMS) s podporou Deep Linking (každému uloženému dokumentu odpovídá unikátní HTML link), lze dokumenty ukládat v tomto DMS systému a v aplikaci team assistant místo ukládání fyzických souborů používat tyto linky – bez další aplikační integrace.
- Pokud je součástí plnění úkolu práce s jinou aplikací, lze tuto aplikaci nebo její část aktivovat prostřednictvím HTML linku a to včetně předání parametrů.

Z pohledu datové integrace jsou primárně podporovány tyto metody:

- Integrace pomocí databázových linků (DB link) – přímá komunikace s databází integrovaného systému. Na úrovni databáze Oracle se provede definice databázového linku do jiné relační databáze a aplikace Team assistant má v závislosti na oprávnění, které ji integrovaná databáze poskytne přímý přístup k tabulkovému datovému interface integrované databáze. Komunikace pomocí tohoto rozhraní může být obousměrná (zápis, čtení). Tímto způsobem lze připojit všechny běžně používané komerční i open-source relační databáze. Takto jsou podporovány například:
  - Oracle DB
  - Oracle TimesTen
  - MS SQL
  - IBM DB2
  - IBM Informix
  - Sybase IQ

### Typy dodávaných licencí

V této kapitole uvádíme základní roli používajících SW a mapování typů licencí.

Klíčoví uživatelé systému budou:

- **Interní auditor** – bude to pro ně hlavní nástroj pro jejich práci, plná licence. Např. Osoby tvořící auditní plány, dotazníky a protokoly
- **Auditor** - Omezení: pojmenovaný uživatel, který má přiřazenu roli "Auditor" a může v RMT/TASu vykonávat pouze úkoly, které jsou dedikované pro tuto roli. Např. vypracovávající audit, doplňování dat.
- **Vedoucí pracovník** - Omezení: pojmenovaný uživatel, který má přiřazenu roli "Analytik rizika" a může v RMT/TASu vykonávat pouze úkoly, které jsou dedikované pro tuto roli. např. pro náhled a schvalování vedoucími pracovníky.
- **Administrátor IS** - Omezení: pojmenovaný uživatel, který má přiřazenu roli "Administrátor" a může v RMT/TASu vykonávat pouze úkoly, které jsou dedikované pro tuto roli.

### Požadavky na HW – on premise

Základní HW požadavky - :

- OS: preferovaný linux CentOS v. 7, případně Win Server 2012 a vyšší
- CPU: 2 x CPU 4 jádra/vlákna

- RAM: 32 GB RAM
- HDD: 120 GB pro aplikaci a zbytek dle množství plánovaných dokumentů. Je vhodné mít možnost místo navýšit v průběhu užívání systému.

	LINUX	WINDOWS
Databáze	Oracle XE/SE/EE 11 nebo vyšší Doporučeno: Oracle XE 21c	MSSQL Express 2017 nebo vyšší Doporučeno: SQL Sever 2022
Minimální SW požadavky serveru pro TAS	CentOS/Red Hat EL/Oracle Linux 7 nebo Rocky Linux/Oracle Linux 8 (CentOS 8 není podporován!) Doporučeno: Red Hat 8	Windows Server 2016 nebo vyšší Doporučeno: Windows Server 2016

### Návrh řešení – popis aplikace - SW pro řízení systému kvality

V rámci projektu bude dodána aplikace - SW pro řízení systému kvality – dále jen „SW-QA“. Aplikace se bude skládat z jednotlivých šablon – které bude naplňovat funkční požadavky.

Pro zajištění provozování aplikace je nutné připraveny šablony – administrativy aplikace.

Administrativa aplikace bude obsahovat tyto šablony: jednotlivé případy se dále používat jako číselníky v dalších šablonách SW- QA.

### Dílčí evidence (případy):

## Definice používaných termínů

Pro práci s aplikací je vysvětlit několik základních pojmů, které popisují hlavní entity, se kterými aplikace pracuje. Tyto pojmy jsou:

- Šablona
- Příklad
- Úkol
- Přehled

Šablona je formalizovaná předloha procesu. Proces je jasně popsán a je jednoznačně řečeno, v jakém pořadí mají jednotlivé kroky následovat. Šablona má formát procesní mapy, která obsahuje všechny úkoly, vazby mezi nimi, podmínky, za jakých může daná situace nastat a určení, kdo má jednotlivé úkoly řešit a pravidla pro přístupová oprávnění.

Příklad je konkrétní spuštění procesu vytvořeného v šabloně. Každý případ má na sobě nezávislý obsah (kartu), strukturu odpovědných osob a jejich oprávnění, stupeň rozpracovanosti apod.

Úkol je dílčí úkon procesu, který je vždy přiřazen určitému uživateli.

Přehled je seznamové zobrazení skupiny úkolů či případů dle definovaných parametrů. Je to základní forma reportingu a umožňuje rychlý export do MS excelu, ale také spuštění vybraných akcí, přechod na kartu daného případu apod.

#### Příklad:

Evidence procesů (karet jednotlivých procesů) je šablonou, která určuje rozsah dat (položky karty procesu), tiskové výstupy, proces schvalování a oprav a rušení případu, obecná přístupová oprávnění, Karty jednotlivých procesů jsou případy. Každý případ má specifické řešitele, individuální viditelnost (danou pravidly stanoveným v rámci šablony).

Oprávněný uživatel například navrhne nový proces – vygeneruje úkol, kde vyplní data procesu, vlastník procesu (zpravidla přímý nadřízený), proces schválí nebo vrátí k opravě. Po schválení Vlastníkem se k procesu zpravidla ještě manažer procesů, po jehož schválení se proces zařadí do „katalogu“. Všechny činnosti uživatelů jsou detailně zaznamenány.

Přehled - Katalog procesů, ukazuje rychlá přehled na všechny platné procesy a jejich základní parametry.

Definovaná data „případů“ se mohou v systému sdílet, podle pravidel definovaných v šablonách. Lze tedy například definovat „podproces“, který zdědí z nadřízeného procesu vybraná data, seznam procesů může být aktivním číselníkem pro jiné typy případů, například auditní šetření.

Naopak data, která nejsou určena ke sdílení jsou uživatelům jiným případů nedostupná a to i u případů stejného typu. Např. Vlastník procesu vidí jen své procesy a nikoliv procesy ostatních vlastníků.

## Administrativa:

### Vytvoření číselníku auditních jednotek

#### Popis

Šablona Auditních jednotek nadefinuje novou auditní jednotku do katalogu a zavede všechny jejich požadované atributy dle interních metodik. Případy vytvořené v této šabloně budou používány i dalších šablonách.

- Nad otevřeným případem bude možné spouštět tyto události:
  - a) Editace
  - b) Storno
- Každý případ bude mít svoji kartu, kde budou uvedeny popisné a související informace –
- Katalog bude dostupný ve formě sdílené dynamické tabulky pro další typy případů
- Aktuální katalog bude dostupný v přehledech, které mohou sloužit pro reportování
- V rámci přehledu bude dostupné filtrování i uzavřených záznamů. Bude tak možné zobrazit hodnoty platné v minulém období (odfiltrování nových položek a zobrazení vyřazených)

#### Seznam proměnných:

- ID číslo auditní jednotky
- Název auditní jednotky
- A další....

#### Graf šablony - workflow

##### Činnosti:

- Zadání
  - o Provádí vlastník případu
    - Přidělí ID, Název procesu a případně nadřazený proces
- Editace
  - o Provádí vlastník případu
    - Vyplní všechny položky
- Storno
  - o Provádí Vlastní případu

### Synchronizace číselníku pracovišť FNUSA

#### Popis

Šablona se bude aktualizovat číselník pracovišť ze zdroje (zdroj MSSQL) min 1x denně. FNUSA připraví soubor csv ze MSSQL.Vstupní tabulka – csv – data z personálního systému.

Dynamická tabulka – DT – SWQA-Katalog útvarů pracovní dynamická tabulka s daty z MSSQL, používaná v celé aplikaci.

Případy budou spouštěny automaticky na pozadí, přičemž oprávněný uživatel bude mít možnost

- a) Zkontrolovat obsah – rozsah přenosu za daný den.
- b) V případě potřeby iniciovat přenos individuálně

#### Seznam proměnných:

- ID Procesu
- Název procesu – číselník
- Atd.

#### Graf šablony - workflow

##### Činnosti:

- Aktualizace nastavená v rámci plánování – min 1x denně v 01,00 hodin.

## Interní auditoři včetně rozdělení dle specifikace

### Popis

Šablona Interní auditoři je případem, který nadefinuje nový interní auditor do katalogu a zavede všechny jejich požadované atributy dle interních metodik. Případy vytvořené v této šabloně budou používány i dalších šablonách.

- Nad otevřeným případem bude možné spouštět tyto události:
  - c) Editace
  - d) Storno
- Každý případ bude mít svoji kartu, kde budou uvedeny popisné a související informace –
- Katalog bude dostupný ve formě sdílené dynamické tabulky pro další typy případů
- Aktuální katalog bude dostupný v přehledech, které mohou sloužit pro reportování
- V rámci přehledu bude dostupné filtrování i uzavřených záznamů. Bude tak možné zobrazit hodnoty platné v minulém období (odfiltrování nových položek a zobrazení vyřazených)

### Status případu:

- Nový – založen, do schválení
- Platný – schválen proces, zapsán do katalogu
- Zrušený – ukončena platnost

### Seznam proměnných:

- ID číslo interního auditora
- Jméno
- Příjmení
- Typ auditu
- A další....

### Graf šablony - workflow

#### Činnosti:

- Zadání
  - o Provádí vlastník případu
    - Přidělí ID, Název procesu a případně nadřazený proces
- Editace
  - o Provádí vlastník případu
    - Úpravy všech položek
- Storno
  - o Provádí Vlastník případu

## Procesy

### Popis

Šablona Procesu nadefinuje novou položku katalogu zavede všechny jejich požadované atributy dle interních metodik. Případy vytvořené v této šabloně budou používány i dalších šablonách.

- Nad otevřeným případem bude možné spouštět tyto události:
  - e) Editace procesu
  - f) Storno
  - g) Úkol zadání
- Každý proces bude mít svoji kartu, kde budou uvedeny související informace – včetně uvedení auditní stopy na kartě
- Po revizi se uloží karta případu ve tvaru PDF
- Katalog procesů bude dostupný ve formě sdílené dynamické tabulky pro další typy případů
- Aktuální katalog procesů bude dostupný v přehledech, které může sloužit pro reportování
- V rámci přehledu bude dostupné filtrování i uzavřených záznamů. Bude tak možné zobrazit hodnoty platné v minulém období (odfiltrování nových položek a zobrazení vyřazených)

### Status případu:

- Nový – založen, do schválení

- Platný – schválen proces, zapsán do katalogu
- Zrušení – ukončena platnost

## Seznam proměnných:

- ID Procesu
- Název procesu – číselník
- Útvar odpovědný za proces – číselník
- Nadřazený proces – číselník

*Každý proces může mít nadřazený jen jeden proces, v případě více nadřazených procesů se bude muset vytvořit nová karta*

- Podřazený proces/podřazené procesy – číselník
- Předpisy, zákony, normy, které řídí proces – číselník
- Popis procesu – txt
- Cíl procesu – txt
- Metrika, kterou se měří úspěšnost dosahování cíle – txt
- Předcházející proces(y) - číselník
- Navazující proces(y) - číselník
- Aktiva – číselník (kyber)
- Dodavatelé – číselník (SAP)
- Předpokládaný objem procesu, výstupu, činnosti – txt
- Minimální počet zdrojů pro zajištění provozu – txt (popř. číselník)

## Graf šablony - workflow

## Činnosti:

- Zadání
  - o Provádí vlastník případu
    - Přidělí ID, Název procesu a případně nadřazený proces
      - Přesun ke schválení??
- Editace
  - o Provádí vlastník případu
    - Vyplní všechny položky
- Storno
  - o Provádí vlastník případu
    - Vyplní poznámku ke zrušení

**Kontrolní otázky k ISO normám (9001, 13485, 15189, 27000)**

## Popis

Šablona nadefinuje nový případ katalogu otázek k normám ISO, zavede všechny jejich požadované atributy dle metodik. Případy vytvořené v této šabloně budou používány i dalších šablonách.

- Nad otevřeným případem bude možné spouštět tyto události:
  - a) Editace auditní otázky
  - b) Storno
  - c) Vyhodnocení
- Každý případ bude mít svoji kartu, kde budou uvedeny související informace – včetně uvedení auditní stopy na kartě
- Po revizi se uloží karta případu ve tvaru PDF
- Katalog bude dostupný ve formě sdílené dynamické tabulky pro další typy případů
- Aktuální katalog bude dostupný v přehledech, které může sloužit pro reportování
- V rámci přehledu bude dostupné filtrování i uzavřených záznamů. Bude tak možné zobrazit hodnoty platné v minulém období (odfiltrování nových položek a zobrazení vyřazených)
- V rámci vyhodnocení bude možné zpětně z dat auditů vyhodnotit otázku a případně ji upřesnit apod.

## Status případu:

- Nový – založen, do schválení
- Platný – schválený případ, zapsán do katalogu
- Zrušení – ukončena platnost

Seznam proměnných:

- ID
- Typ ISO – 9000,27000 atd
- Otázka –
- Platnost od
- Platnost do
- Score
- Související ISO

Graf šablony - workflow

Činnosti:

- Zadání
  - o Provádí vlastník případu
    - Doplní datové položky
      - Přesun ke schválení
- Editace
  - o Provádí vlastník případu
- Možnost opravy všech položek
- Storno
  - o Provádí vlastník případu
    - Vyplní poznámku ke zrušení

## **Kontrolní otázky dle legislativních požadavků (zákony, vyhlášky, nařízení, pokyny SÚKLu příp. jiných subjektů)**

Popis

Šablona nadefinuje novou položku katalogu otázek zavede všechny jejich požadované atributy dle legislativy. Případy vytvořené v této šabloně budou používány i dalších šablonách.

- Nad otevřeným případem bude možné spouštět tyto události:
  - h) Editace procesu
  - i) Storno
  - j) Vyhodnocení otázky
  - k) Úkol zadání
- Každý případ bude mít svoji kartu, kde budou uvedeny související informace – včetně uvedení auditní stopy na kartě
- Po revizi se uloží karta případu ve tvaru PDF
- Katalog případů bude dostupný ve formě sdílené dynamické tabulky pro další typy případů
- Aktuální katalog případů bude dostupný v přehledech, které může sloužit pro reportování
- V rámci přehledu bude dostupné filtrování i uzavřených záznamů. Bude tak možné zobrazit hodnoty platné v minulém období (odfiltrování nových položek a zobrazení vyřazených)

Status případu:

- Nový – založen, do schválení
- Platný – schválený případ
- Zrušení – ukončena platnost

Seznam proměnných:

- ID
- Typ ISO – 9000,27000 atd
- Otázka –
- Platnost od
- Platnost do
- Score
- Související ISO

Graf šablony - workflow

Činnosti:

- Zadání
  - o Provádí vlastník případu

- Doplní datové položky
  - Přesun ke schválení
- Editace
  - Provádí vlastník případu
- Možnost opravy všech položek
- Storno
  - Provádí vlastník případu
    - Vyplní poznámku ke zrušení

## Kontrolní otázky dle celonemocničních požadavků (viz směrnice, pracovní postupy...)

### Popis

Šablona nadefinuje novou položku katalogu otázek a zavede všechny jejich požadované atributy dle interních metodik. Případy vytvořené v této šabloně budou používány i dalších šablonách.

- Nad otevřeným případem bude možné spouštět tyto události:
  - a) Editace procesu
  - b) Storno
  - c) Vyhodnocení otázky
  - d) Úkol zadání
- Každý případ bude mít svoji kartu, kde budou uvedeny související informace – včetně uvedení auditní stopy na kartě
- Po revizi se uloží karta případu ve tvaru PDF
- Katalog případů bude dostupný ve formě sdílené dynamické tabulky pro další typy případů
- Aktuální katalog případů bude dostupný v přehledech, které může sloužit pro reportování
- V rámci přehledu bude dostupné filtrování i uzavřených záznamů. Bude tak možné zobrazit hodnoty platné v minulém období (odfiltrování nových položek a zobrazení vyřazených)

### Status případu:

- Nový – založen, do schválení
- Platný – schválený případ
- Zrušení – ukončena platnost

### Seznam proměnných:

- ID
- Typ ISO – směrnice, nařízení atd
- Otázka –
- Platnost od
- Platnost do
- Score
- Související ISO

### Graf šablony - workflow

#### Činnosti:

- Zadání
  - Provádí vlastník případu
    - Doplní datové položky
      - Přesun ke schválení
- Editace
  - Provádí vlastník případu
- Možnost opravy všech položek
- Storno
  - Provádí vlastník případu
    - Vyplní poznámku ke zrušení

## Tvorba harmonogramu interních auditů v tříletých cyklech

### Popis

Šablona je případem plánu harmonogramu auditních zakázek dle zadaných roků od: do. Bude možné zadat časové rozpětí výpisu auditních zakázek.

- Každý případ bude mít svoji kartu, kde budou uvedeny související informace – včetně uvedení auditní stopy na kartě
- Karta případu se uloží ve tvaru PDF
- Harmonogram se uloží ve tvaru PDF
- Report je možné libovolně x-krát generovat
- Název reportu: Harmonogram auditních zakázek: od: XXXX) např. 2022) do: YYYY( např. do 2025
- 

### Status případu:

- Založení nového plánu
- Příprava plánu
- Schválení plánu
- Vyhodnocení plánu

### Seznam proměnných:

- ID
- Auditní zakázka
- Název IA
- Popis
- Zahájení od:
- Ukončení do:

### Graf šablony - workflow

#### Činnosti:

- Zadání
  - o Založení nového plánu
  - o Příprava plánu
    - Provádí vlastník případu – vyplní datum – od: do:
      -
  - o Schválení plánu
  - o Vyhodnocení plánu

## Tvorba více harmonogramů interních auditů dle skupin

### Popis

Šablona vytvoří report harmonogramu auditních zakázek dle skupiny a zadaných roků od: do. Bude možné zadat časové rozpětí výpisu auditních zakázek.

- Každý případ bude mít svoji kartu, kde budou uvedeny související informace – včetně uvedení auditní stopy na kartě
- Karta případu se uloží ve tvaru PDF
- Harmonogram se uloží ve tvaru PDF
- Report je možné libovolně x-krát generovat
- Název reportu: Harmonogram auditních zakázek: skupiny : ..... a od: XXXX) např. 2022) do: YYYY( např. do 2025
- 

### Status případu:

- Vytvořený

### Seznam proměnných:

- ID
- Skupina
- Auditní zakázka
- Název IA

- Popis
- Zahájení od:
- Ukončení do:

Graf šablony - workflow

Činnosti:

- Zadání
  - o Provádí vlastník případu – vyplní datum – skupina:..... a od:..... do:.....

## Příprava plánu a vlastního auditu

### Popis

Šablona je případem, který vytvoří harmonogram konkrétního auditu - auditních zakázek dle skupiny a zadaných roků od: do. Bude možné zadat časové rozpětí výpisu auditních zakázek.

- Každý případ bude mít svoji kartu, kde budou uvedeny související informace – včetně uvedení auditní stopy na kartě
- Nad otevřeným případem bude možné spouštět tyto události:

- I. Příprava auditu
  - a. Plán auditu, auditní tým
  - b. Vygenerování auditní otázek (checklistu)
  - c. Oznámení o vykonání auditu
- II. Realizace audit
  - a. Rozeslání – sběr auditních dat a respondenty
- III. Uzavření auditu
  - a. Vyhodnocení auditu a příprava zprávy
  - b. Připomínkování oprávněnou osobou
  - c. Závěrečná zpráva a Nápravná opatření
- IV. Ostatní činnosti v rámci auditu
  - a. Storno auditu
  - b. Revize – oprava plánu auditu

- Každý případ bude mít svoji kartu, kde budou uvedeny související informace – včetně uvedení auditní stopy na kartě
- Po revizi se uloží karta případu ve tvaru PDF
- Katalog případů bude dostupný ve formě sdílené dynamické tabulky pro další typy případů
- Aktuální katalog případů bude dostupný v přehledech, které může sloužit pro reportování
- V rámci přehledu bude dostupné filtrování i uzavřených záznamů. Bude tak možné zobrazit hodnoty platné v minulém období (odfiltrování nových položek a zobrazení vyřazených)
- Přehledy:
  - o Roční souhrnné vyhodnocení jednotlivých pracovišť a celkově za FNUSA
  - o Dle procesu daného pracoviště vyhledávání i v historii, sumarizace dle vydefinovaných kritérií (pracoviště, kapitola normy apod.)

Status případu:

- Plánovaný – v horizontu 3 let – pro harmonogramy
- Vytvořený
- Vytvořený - editovaný
- Tvorba dotazníku
- Zpracování
- Připomínkování (auditory, auditovaným pracovištěm)z
- Vyhodnocení
- Uzavření auditu
- Rozeslání výsledků na oprávněné osoby
- Platný IA – zadaný úkol

Seznam proměnných:

- ID
- Číslo IA
- Název auditu
- Popis auditu
- Vedoucí IA
- Členové IA týmu
- Popis IA
- Dotčené útvary
- Skupina IA
- Zahájení od:
- Ukončení do:
- Auditní otázka ISO – (JSON – ISO otázky z administrativy)
- Auditní otázka LEG – (JSON – Legislativa otázky z administrativy)
- Auditní otázka INTERI– (JSON – Interní předpisy dle otázek z administrativy)
- 

Graf šablony - workflow

Činnosti:

- Zadání
  - o Provádí vlastník případu
- Editace
  - o Provádí vlastník případu
- Tvorba dotazníku — výběrem otázek z číselníku — možnost kombinovat z různých norem a požadavků
  - o Provádí vlastník případu
- Zpracování
  - o Provádí vlastník případu
- Připomínkování (auditory, auditovaným pracovištěm)z
  - o Provádí vlastník případu
- Vyhodnocení
  - o Provádí vlastník případu
- uzavření auditu
  - o Provádí vlastník případu
- rozeslání výsledků na oprávněné osoby
  - o Provádí vlastník případu
- zadání konkrétní osobě úkolu vyplývajícího ze zjištění interního auditu
  - o Provádí vlastník případu

## Evidence, sledování a kontrola nápravných opatření

### Popis

Šablona nadefinuje novou položku katalogu Opatření jako samostatný případ z daného auditu.

Nové nápravné opatření bude vznikat vždy jako samostatný případ a vazba na seznam Související audit.

Vlastní proces bude rozdělen na fázi přípravy/schvalování, fázi realizace a fázi kontroly účinnosti opatření, která bude realizována ve formě samostatného podprocesu nad dotčenými odpovědnými osobami.

- Nad otevřeným případem bude možné spouštět tyto události:
  - a) Editace -
  - b) Revize – změna statusu
    - a. Plán a příprava opatření
    - b. Realizace
    - c. Vyhodnocení a kontrola účinnosti
  - c) Storno
  - d) Úkol zadání
- Každý proces bude mít svoji kartu, kde budou uvedeny související informace – např. rizika atd., včetně uvedení auditní stopy na kartě

- Katalog procesů bude dostupný ve formě sdílené dynamické tabulky pro další typy případů
- Aktuální katalog procesů bude dostupný v přehledech, které může sloužit pro reportování
- V rámci přehledu bude dostupné filtrování i uzavřených záznamů. Bude tak možné zobrazit hodnoty platné v minulém období (odfiltrování nových položek a zobrazení vyřazených)

Pro každé nápravné opatření platí:

- bude mít svoji základní kartu s popisem a kategorizací,
- vlastník nápravného opatření je nezávislý na garantech aktiv nebo vlastnících rizika
  - o kontrolu účinnosti provádí vlastník rizika
- nápravné opatření ve fázi přípravy se nezapisuje do katalogu (nelze jej zohlednit v mitigačním plánu rizik
- nápravná opatření po realizaci přecházejí do fáze kontroly účinnosti
- kontrolu účinnosti nápravného opatření provádí vždy vlastník rizik
- k nápravnému opatření se evidují i opatření dle vyhlášky

-

Status případu:

- Nový – založen, do schválení
- Platný – schválen proces, zapsán do katalogu
- Změn statusu případu
- Zadán úkol
- Zrušení – ukončena platnost

Seznam proměnných:

- ID
- Číslo opatření
- Název opatření
- Popis opatření
- Zadavatel
- Datum zadání opatření
- Datum ukončení opatření
- Datum realizace opatření
- Datum kontroly realizace opatření
- Datum kontroly účinnosti
- A další
- 

Graf šablony - workflow

Činnosti:

Fáze realizace opatření:

- Návrh nápravného opatření
- Příprava nápravného opatření
- Realizace nápravného opatření
- Kontrola účinnosti (jako podproces)
- Uzavření nápravného opatření

Dopad do IA:

- Na co vázat na riziko – nebo jen zranitelnost – zatřídění dle ISO27000, zadání, realizace, kontrola až po kontrolu účinnost.
- Snížení

## Další požadavky

Další požadavky dodávané řešení splňuje:

- Fulltextové vyhledávání
- Český jazyk
- Ochrana — kyberbezpečnost, GDPR (dle legislativy a interních požadavků FNUSA)

**Nefunkční požadavky****Požadavky na bezpečnost:****Obecné —**

Nabízený systém musí splňovat požadavky na řízení bezpečnosti informací v souladu s platnou legislativou, standardy v oblasti řízení bezpečnosti informací. Požadavky jsou rozděleny dle oblastí, které požaduje zákon

č. 181/2014 Sb., o kybernetické bezpečnosti, v platném znění (ZoKB). Vzhledem k tomu, že poptávaný systém není určen jako VIS (KII), nejsou zahrnuty všechny požadavky tohoto zákona. Systém nebude obsahovat údaje klasifikované dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Předložené bezpečnostní požadavky lze chápat jako nutné minimum a zároveň je přihlédnuto k povaze informačního nástroje, který bude předmětem veřejné zakázky.

**Řízení přístupů —**

Cílem řízení přístupů je přidělit jedinečné identifikátory jednotlivým uživatelům a administrátorům přistupujícím k softwaru (aplikaci). Tyto identifikátory musí být řízeny a evidovány, stejně jako přístupová práva a oprávnění aplikací a technických účtů.

[Všechny entity v systému mají přidělený jedinečný identifikátor, díky kterému lze veškeré aktivity s danou entitou spárovat.](#)

- [Řízení přístupu musí být založeno na základě skupin a rolí. Na úrovni aplikace lze řídit oprávnění prostřednictvím organizačních jednotek, rolí a kompetencemi \(skupinami rolí\), případně lze do aplikace role importovat přímo z AD.](#)
- [Musí probíhat ověřování proti záznamům v LDAP, později možná integrace na AD. Aplikace TAS podporuje AD pro synchronizaci a autentizaci uživatelů.](#)
- [Pravidla pro nastavení hesel musí vycházet z požadavků ZoKB. Nastavení hesel se řídí nastavenými pravidly v AD, případně lze pravidla konfigurovat pro interní systém autentizace.](#)
- [Další pravidla pro řízení přístupů musí být v souladu s těmito požadavky:](#)

Všem uživatelům a administrátorům budou přidělena pouze nezbytná přístupová práva. Musí být zajištěno oddělení neslučitelných rolí (např. zadavatel, schvalovatel apod.) V případě servisních účtů musí být zajištěna změna implicitního hesla.

[Vše lze zajistit patřičnou konfigurací.](#)

**Ochrana před škodlivým kódem —**

V rámci softwaru (aplikace) musí být umožněno implementovat způsob řešení ochrany před škodlivým kódem:

- [Umožnit nainstalovat agenta pro detekci a odstranění škodlivých programů, který bude nejméně jednou denně aktualizován. Požadavek není v rozporu s provozuschopností aplikace.](#)
- [Software \(aplikace\) musí být pravidelně aktualizována. Standartní cyklus vydávání hlavních verzí je 3 měsíce. V případě kritických oprav jsou přednostně vydávány releasy v týdenním cyklu.](#)
- [Software \(aplikace\) musí být prověřitelná z hlediska možných zranitelností. Ano lze prověřovat.](#)
- [Software \(aplikace\) nesmí obsahovat žádné známé kritické zranitelnosti, vysoké zranitelnosti a střední zranitelnosti \(dle CVE score\). Všechny vysoké a kritické zranitelnosti přednostně řešíme.](#)
- [V prostředí softwaru \(aplikace\) musí být zakázáno vzdálené spuštění kódu ze zdroje mimo jeho prostředí. Vzdálené spuštění není možné.](#)

Odolnost proti zranitelnostem může být v rámci zakázky ověřena zadavatelem prostřednictvím penetračních testů i opakovaných po celou dobu poskytování plnění.

**Důvěrnost a integrita —**

Software (aplikace) musí umožňovat zajištění důvěrnosti a integrity dat na úrovni databáze, a to i před správcem provozního prostředí (vyjma administrátorů DB).

Databázovou vrstvu aplikace TAS zajišťuje MSSQL/DB ORACLE server, který nativně zajišťuje důvěryhodnost a integritu dat např. pomocí autentizace, autorizace, transakčnímu zpracování a šifrování.

Software (aplikace) musí zajistit důvěrnost a integritu dat na celé cestě mezi databázovým serverem a klientem, tedy je požadováno zabezpečené propojení mezi všemi architektonickými vrstvami systému vyjma zásahů a úprav realizovaných administrátory DB.

Aplikace TAS podporuje MSSQL/DB ORACLE s šifrovanou komunikací.

Důvěrnost a integrita dat musí být zachována i při zálohování a archivaci, a to jak při vlastním procesu, tak i následně vzhledem k médiím, na nichž jsou zálohy a archivní data uloženy vyjma zásahů a úprav realizovaných administrátory DB.

Řešeno na úrovni databázového serveru.

#### Auditovatelnost a nepopiratelnost —

Software (aplikace) musí zajišťovat auditovatelnost dat i procesů. Jedná se zejména o přístupy a změny v datech pro jednotlivé objekty (princip zajištění nepopiratelnosti). Auditovatelný musí být také proces řízení identit uživatelů.

Všechny změny v procesech a datech lze auditovat v rámci aplikační vrstvy.

Logy softwaru (aplikace) musí být integrovatelné do centrálního řešení pro vyhodnocování provozních a bezpečnostních logů (LOG management).

Aplikace obsahuje volitelnou automatizaci exportu logů do SIEM.

Zaznamenávání událostí zohledňuje technické možnosti softwaru (aplikace) a pro sběr záznamů ukládá minimálně tyto typy událostí:

- a) přihlášení a odhlášení uživatelů a administrátorů, a to včetně neúspěšných pokusů  
Na úrovni aplikace v základním rozsahu. Mělo by být ale logováno na straně MS AD.
- b) činnosti provedené administrátory, o použití privilegovaných účtů, např. účtu supervisora, administrátora,  
Jsou logovány pouze některé činnosti, jako smazání uživatele, nebo smazání či náhledu na dokument. U běžných činností uživatele není zvlášť logováno rozsah oprávnění uživatele tj. k uživateli, který zásah provedl je potřeba si dohledat rozsah oprávnění zvlášť. Není logováno zapnutí/vypnutí administrátorských oprávnění (uživatel v roli admina může přepínat mezi oběma režimy. Pro specifickou roli HR manažera jsou zásahy detailně logovány.
- c) spuštění a ukončení softwaru (aplikace)  
Ano, start aplikace a ukončení je logován na vícero úrovních (aplikační, OS log).
- d) změny konfigurací,  
Změny na úrovni jednotlivých případů jsou logovány detailně.
- e) úspěšné i neúspěšné činnosti vedoucí ke změně přístupových oprávnění, Vlastnictví evidence, přidělení úkolu je detailně logováno. Změny, které provede systémová role HR manager jsou detailně logovány. Řízení změn oprávnění na úrovni rolí je možné řídit z MS AD a tam je i logovat.
- f) zahájení a ukončení činností zařízení a aplikací  
Ano, vyjma logování otevření, nebo zavření prohlížeče, ve kterém je spuštěn systém.
- g) automatická varovná nebo chybová hlášení zařízení a aplikací  
Ano, chybová hlášení aplikace jsou zaznamenávány do warn a error logů.
- h) přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností  
V případě snahy podvrhu aplikace bez administrativních oprávnění systém loguje tyto požadavky jako neautorizované. Z pohledu administrátora nelogujeme pokusy o změnu aplikace.
- i) použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.  
Toto je část vyhodnocování MS AD.

Všechny záznamy o činnosti v systému musí být zabezpečeny proti:

- a) neoprávněnému přístupu k datům (zachování důvěrnosti);
- b) neoprávněné manipulaci (zachování integrity a prokazatelnosti, resp. principu nepopiratelnosti)

c) ztrátě uložených informací v požadované době dostupnosti záznamů (zálohování a archivace).

Přístup k záznamům o činnosti musí být umožněn pouze oprávněným osobám (nemusí být administrátoři daného provozního prostředí).

Záznamy o činnosti systému jsou řešeny na několika úrovních a každá vrstva řeší danou problematiku odlišně. Bohužel zajištění principů (integrita, prokazatelnost, nepopiratelnost) není stoprocentně naplněno na každé úrovni.

#### **Kryptografické prostředky —**

Data a informace zpracovávaná v rámci softwaru (aplikace) musí být chráněna proti zneužití vhodnými kryptografickými metodami, které zajistí pouze autorizovaný přístup k těmto datům a informacím. Šifrování uložených dat NÚKIB pouze doporučuje, a to v návaznosti na typ a charakter dat a v návaznosti na možné technologické řešení.

V současné době aplikace podporuje pouze kryptografickou metodou na úrovni přikládaných datových souborů uživateli systému, aplikace je fakticky nefunkční bez SSL zabezpečení, je podporováno šifrování na úrovni databáze. Šifrování neplatí obecně pro všechny zpracovávaná data.

Informační systém by měl být připraven využívat aktuálně odolné kryptografické algoritmy dle doporučení NÚKIB. Toto doporučení lze nalézt na:

<https://www.govcert.cz/cs/doporučení-v-oblasti-kryptografických-prostředků/>

V případě použití jiného, než doporučeného algoritmu by mělo být toto použití řádně odůvodněno