Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Příprava projektu a implementace požadavků metodiky ITIL pro interní audit ISO 27001

Diplomová práce

Autor: Bc. Karel Kavuljak
Studijní obor: Informační management

Vedoucí práce: doc. Ing. Pavel Čech, Ph. D.

Hradec Králové srpen 2023

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 7.8.2023 Karel Kavuljak

Poděkování:

Rád bych vyjádřil upřímné poděkování panu doc. Ing. Pavlu Čechovi, Ph.D., vedoucímu mé diplomové práce, za jeho cenné rady, odbornou pomoc a přátelské konzultace během celého procesu zpracování mé diplomové práce. Také bych chtěl vyjádřit vděčnost své firmě a kolegům, kteří mi umožnili provést tuto práci v navrhovaném rozsahu. Nemohu zapomenout ani na několik blízkých přátel, kteří mě při tvorbě této práce podporovali.

Tímto bych chtěl upřímně poděkovat všem výše zmíněným osobám za jejich přínos, který byl klíčový pro úspěšné dokončení mé diplomové práce.

Anotace

Diplomová práce se zabývá problematikou bezpečnosti informací a aplikací normy ČSN/EN ISO/IEC 27001 v softwarové firmě. Práce se zaměřuje na aktuální interní audit, který probíhá ve společnosti, a analyzuje implementaci a dodržování požadavků této normy v rámci konkrétního projektu. Norma ISO 27001 představuje mezinárodní standard pro systémy řízení bezpečnosti informací (ISMS) a je kombinována s ITIL praktikami pro správu ICT služeb.

V rámci práce budou provedeny detailní analýzy a zhodnocení implementace normy ISO 27001 ve zkoumané společnosti. Práce se bude zabývat nejen samotnými požadavky normy, ale také jejich aplikací v praxi a mírou dodržování v rámci projektového prostředí. Bude provedena srovnávací analýza mezi požadavky normy ISO 27001, ITIL metodikou a interními požadavky společnosti, a to s cílem posoudit míru adaptace a přizpůsobení těchto požadavků specifickým potřebám a požadavkům softwarové firmy.

Výsledkem práce bude komplexní zhodnocení bezpečnostní situace projektu a odpovídající dokumentace v rámci přípravy na interní ISO Audit 27001. Práce přispěje k lepšímu porozumění implementace a dodržování bezpečnostních standardů v softwarové firmě a poskytne doporučení pro zlepšení a optimalizaci bezpečnostních postupů a procesů.

Annotation

Title: Analysis and implementation of ITIL methodology requirements for ISO 27001 internal audit

The thesis focuses on the issue of information security and the application of the ČSN/EN ISO/IEC 27001 standard in the software company. The thesis examines the current internal audit taking place within the company and analyses the implementation and compliance with the requirements of this standard within a specific project. ISO 27001 is an international standard for Information Security Management Systems (ISMS) and is combined with ITIL practices for ICT service management.

The thesis will conduct detailed analysis and evaluation of the implementation of the ISO 27001 standard. It will address not only the requirements of the standard itself but also their practical application and the level of compliance within the project environment. A comparative analysis will be performed between the requirements of ISO 27001, ITIL methodology, and internal company requirements to assess the extent of adaptation and customization of these requirements to the specific needs of the software company.

The outcome of the thesis will be a comprehensive evaluation of the security situation of the project and the corresponding documentation in preparation for the internal ISO 27001 audit. The thesis will contribute to a better understanding of the implementation and compliance with security standards in a software company and provide recommendations for improving and optimizing security procedures and processes.

Obsah

1 Úvod

Tato diplomová práce se zaměřuje na řešení otázek spojených s pracovní zkušeností autora ve společnosti specializující se na tvorbu komerčního softwaru a přípravou na recertifikaci projektu. Jedná se o servisní projekt v oblasti energetiky. Z důvodu uchování důvěrnosti a ochrany citlivých informací vystupuje společnost v diplomové práci pouze pod označením „organizace“ nebo „společnost“. Na základě certifikačních doporučení a návodů pro neustálé zlepšování informační bezpečnosti bylo rozhodnuto, že projekt projde recertifikací dle standardu ISO 27001. Cílem práce je analyzovat teoretické základy ISO auditu, metodiky ITIL a jejich konkrétní implementaci v softwarové firmě. Praktická část práce se zaměřuje na popis konkrétních kroků při implementaci auditu, zkoumání výzev a příležitostí, které se během přípravy a následného auditu objevují.

Důkladné prozkoumání specifické implementace auditu ISO v softwarové firmě poskytne komplexní pochopení toho, jak jsou teoretické principy a požadavky normy upraveny a aplikovány v reálném pracovním prostředí. Práce se zaměřuje na poskytování znalostní báze, identifikaci nedostatků a poskytování řešení pro dosažení certifikace a zvýšení bezpečnosti projektů. Součástí a výstupem práce je také kompletní migrace a přestavba projektového portálu, který obsahuje všechny důležité body normy ISO 27001 a jejich implementaci. Společnost vyvinula projektový portál jako webovou platformu, která umožňuje centralizovanou správu projektu a efektivní sdílení dokumentace, reportování stavu a plánování projektu jak v rámci týmu, tak ve vztahu k vrcholovému vedení. Tento projektový portál bude podroben auditu.

2 Cíle a metodika zpracování práce

Cílem diplomové práce je provést analýzu požadavků a podrobně popsat přípravu a průběh interního ISO auditu. Pro zhodnocení procesu přípravy projektu a podkladů budou použity metodiky ITIL a požadavky auditora ISO 27001. Dále bude provedena analýza implementace standardních požadavků organizace během interního ISO auditu a také analýza samotného interního ISO auditu projektu.

Autor práce měl aktivní roli v přípravě projektu jako Team Leader, což zahrnovalo účast při tvorbě projektové dokumentace a účast ve všech fázích přípravy a hodnocení projektu. Taktéž měl přímý vliv na klíčová rozhodnutí týkající se implementace, nebo se spolupodílel na volbách ovlivňujících zákazníky.

Diplomová práce zahrnuje a rozvíjí značné množství témat a možností z oblasti projektového řízení, které by bylo možné dále rozpracovat do větších implementačních detailů. Pro zachycení klíčových aspektů byl nicméně zvolen přístup s vyšší úrovní abstrakce, který odpovídá také manažerské pozici autora. Tímto způsobem bude dosaženo nadhledu a komplexního zahrnutí tématu do uceleného díla.

Na základě této problematiky jsou formulovány následující výzkumné otázky:

1. Jaké jsou hlavní požadavky auditora ISO 27001 na přípravu projektu a projektového portálu v organizaci?
2. Jak je úroveň souladu přípravy projektu a projektového portálu s metodikou ITIL a požadavky auditora ISO 27001?
3. Jaká je míra implementace standardních požadavků organizace v rámci interního ISO auditu projektu?
4. Jaký je význam a přínos provedených změn během auditu a migrace na nový informační portál?

První metodou, pro získání odpovědí na tyto otázky v této diplomové práci, je provedení analýzy primárních požadavků ISO 27001 a relevantních aspektů

spojených s ITIL metodikou. Druhou metodou je na základě těchto poznatků je provedení analýzy míry adaptace a přizpůsobení v rámci interních požadavků v softwarové firmě. Třetí metodou je zhodnocení bezpečnostní situace projektu a příslušné dokumentace na základě provedené analýzy. Tyto metody umožní získat komplexní pohled na danou problematiku v kontextu přípravy na interní ISO Audit 27001.

V rámci literární rešerše budou studovány práce týkající se ITIL a jeho vztahu k přípravě projektu a podkladů, auditorství ISO 27001 a požadavků auditora, standardních požadavků organizace a jejich implementace v rámci interního ISO auditu. Také bude zkoumána doplňující literatura. V rámci diplomové práce budou upřesněny konkrétní rozsah a detaily metodiky vlastní přípravy a průběhu.

Čtením této práce může čtenář získat znalosti o požadavcích standardu ISO 27001 a pochopit, jak jsou tyto požadavky implementovány a upraveny v rámci softwarové firmy. Tímto se nabízí možnost pochopit konkrétní adaptace a implementační postupy, což může být užitečné pro čtenáře, kteří se zabývají implementací ISO 27001 v jiných organizacích a hledají inspiraci. Dále je v práci podrobně vysvětlena analýza bezpečnostní situace projektu a popisují se opatření, která byla provedena pro zlepšení. Tato informace může být přínosná pro čtenáře, kteří se zajímají o zvýšení bezpečnosti svých vlastních projektů a hledají osvědčené postupy.

Celkový přínos této práce spočívá v tom, že poskytuje cenné poznatky a osvědčené postupy, které lze aplikovat ve firmách po celém světě. To může přispět k celkovému zvýšení informační bezpečnosti a zlepšení řízení IT služeb ve firmách po celém světě.

3 ISO audit

Při přípravě na tvorbu této diplomové práce byla provedena studie problematiky z předchozích výzkumů. Mezi studie zaměřené na dané téma patří publikace od autorů Brennera a Schaafa z konference, která popisuje závislost poskytovatelů IT služeb na softwarových řešeních ITSM v souvislosti se stoupajícími požadavky na komplexní řízení IT služeb. Nicméně integrace ITSM softwaru od různých dodavatelů se potýká s nedostatkem standardizovaných informačních modelů. Článek představuje přístup k vytvoření informačního modelu pro ITSM procesy [1]. Většina publikací se soustředí na propojení metodiky COBIT a ISO 27001, například článek od autorů Mataracioglua a Ozkana. Tyto publikace popisují definice ISMS, výhody a implementaci ISO 27001 a COBITu a zkoumají jednotlivé prvky odděleně. [2]

Existuje několik článků, které dokazují a popisují kombinaci metodik ITIL a ISO 27001. Mezi ně patří článek od autora Orrega, který zkoumá vztah mezi COBITem, ITILem a ISO 27001 v souvislosti s informační bezpečností a způsob implementace ISMS a vylepšení systému [3]. Článek od autorů Elhasnaouiho, Medromiho, Farise, Iguera a Sayoutiho se zabývá sestavením multiagentového systému integrující hlavní IT rámce (COBIT, ITIL a ISO) tak, aby vytvořil robustní systém. V předložené architektuře je představen inovativní přístup k vývoji distribuovaného systému umožňující komunikaci mezi agenty prostřednictvím distribuovaných funkcionalit. Tato architektura také poskytuje přehled o implementaci prototypu navrhovaného řešení, který je momentálně omezen na nejčastěji používané integrační procesy v informačních systémech. [4]

Tyto články zkoumají vztahy mezi metodikami ITIL, COBIT a ISO 27k certifikacemi a zdůrazňují výhody spojení těchto rámců pro efektivní řízení IT služeb a praktiky informační bezpečnosti. Poskytují také pokyny, jak firmy mohou integrovat různé metodiky s ISO 27001 k lepšímu poskytování IT služeb a zajištění bezpečnostních opatření. Články zahrnují případové studie a příklady z reálného prostředí, které slouží k dosažení holistického řízení IT a řízení rizik. Z těchto příkladů je zřejmé, že každá metodika má své výhody i nevýhody a může být

posílena jinou metodikou. Nicméně omezením této práce je nutnost zohlednit nejen obecné globální možnosti, ale také firemní kulturu a požadavky projektu.

3.1 Přehled a význam normy ISO 27001

ISO audit neboli plným názvem ISO/IEC 27001:2022, je mezinárodně uznávaný standard pro řízení informační bezpečnosti. Jedná se o proces, během kterého se nezávisle ověří, zda organizace efektivně dodržuje a implementuje bezpečnostní politiku, postupy a opatření. V rámci této diplomové práce se zkoumá dodržení v rámci samostatného projektu. Během auditu auditor nebo tým auditorů provádí důkladné zhodnocení systému řízení informační bezpečnosti organizace. To zahrnuje sběr informací, vyhodnocování dokumentů, rozhovory s odpovědnými pracovníky a případně i fyzické prohlídky.

Přínosy certifikace systému managementu bezpečnosti informací podle ISO/IEC 27001:2022 [5]:

- **Zabezpečení informací** je nedílnou součástí celého řídicího systému organizace.
- **Klíčové faktory** ovlivňující podnikatelskou soutěž, informace a jejich zabezpečení jsou řádně řízeny.
- **Systémy zálohování** přispívají k vysoké spolehlivosti systému.
- **Zaměstnanci** mají zodpovědnost za zabezpečení informací na svých pracovištích i ve vztahu ke svým zákazníkům.
- Požadavek na **neustálé zlepšování** zajišťuje dlouhodobě efektivní řízení nákladů.

V roce 2022 došlo k vydání nové verze ISO standardu s názvem ISO/IEC 27001:2022. Oproti předchozí verzi z roku 2013 bylo představeno několik změn, které je nutné zohlednit. Předchozí ISO/IEC 27001:2013 se skládala z 11 hlavních kapitol zaměřených na různé aspekty řízení bezpečnosti informací. V rámci České republiky je dle Technické Normy ČSN stále tato verze ČSN EN ISO/IEC 27001 platná a poslední vydaná [6]. V této chvíli se nacházíme v přechodném období, které končí v říjnu 2025. Zde je přehled těchto kapitol:

- **Úvod**: Poskytuje úvodní informace o normě ISO/IEC 27001 a jejím účelu.
- **Rozsah**: Tato kapitola definuje rozsah a rozsah normy ISO/IEC 27001.
- **Normativní odkazy**: Zde jsou odkazy na další normy a dokumenty související s normou ISO/IEC 27001.
- **Termíny a definice**: Obsahuje definice důležitých termínů používaných v normě ISO/IEC 27001.
- **Organizační prostředí**: Zde se organizace zabývá analýzou svého prostředí, včetně vnitřních a vnějších faktorů, které ovlivňují její řízení bezpečnosti informací.
- **Plánování**: Tato kapitola se zaměřuje na plánování procesu řízení bezpečnosti informací, včetně identifikace rizik, cílů, zásad a zdrojů.
- **Podpora**: Zde jsou uvedeny požadavky na zajištění adekvátní podpory pro implementaci a provádění řízení informační bezpečnosti. Tato podpora zahrnuje dostatečné zdroje, kompetence a povědomí.
- **Provoz**: V této části se zabývá provozními aspekty řízení informační bezpečnosti, jako je plánování a realizace procesů a opatření pro dosažení stanovených cílů.
- **Vyhodnocování výkonu**: Zde jsou stanoveny požadavky na hodnocení výkonu řízení informační bezpečnosti, včetně monitorování, měření, hodnocení a interního auditu.
- **Vylepšování**: Zde se zaměřuje na proces vylepšování řízení informační bezpečnosti na základě získaných poznatků a výsledků hodnocení.
- **Integrovaný řídicí systém**: Diskuze o možnostech integrace normy ISO/IEC 27001 s jinými řídicími systémy v rámci organizace.

Vzhledem k technologickému pokroku, globalizaci, aktuálním potřebám uživatelů a zúčastněných stran bylo nevyhnutelné provést změny v normě ISO/IEC 27001:2022. Tyto změny nejsou zásadního rozsahu, především se týkají pravidelných kontrol ve společnostech. Jejich cílem je vylepšit procesy a systémy řízení informační bezpečnosti (ISMS). Počet opatření v normě ISO/IEC 27002:2022 se celkově snížil z 114 na 93. Z těchto opatření je 11 nových, 24 bylo sloučeno ze stávajících a 58 bylo aktualizováno. Mezi těmito změnami jsou například

opatření týkající se „informační bezpečnosti pro využívání cloudových služeb“, „monitorování fyzické bezpečnosti“, „správa konfigurace“, „prevence úniku dat“ a další. V současné době je v platnosti přechodné období, které končí v říjnu 2025. [7]

Revize nové normy pro rok 2022 se primárně zaměřila na aktualizace následujících bodů [8]:

- organizační opatření,
- personální opatření,
- fyzická opatření,
- technická opatření.

Tato práce bude zaměřena především na ISO 27001, které bude podléhat recertifikace projektu v rámci praktické části. Je ale důležité uvést, že ve výsledku rodina ISO 27k obsahuje více směrnic.

3.2 Definice pojmů

V rámci této práce se vyskytují termíny z oblasti informační bezpečnosti nebo bezpečnosti informací, které budou použity v následujících kapitolách. Nejprve je tedy nutné definovat jednotlivé pojmy, než se přistoupí k další analýze [9]:

- **Informací** se rozumí datové nebo zpracovávané informace, které mají význam a kontext. Informace mohou existovat v různé formě, od souborů, dokumentů, multimédií a dalších formátů sloužící pro uložení a záznam.
- **Aktivum** představuje cokoli, co má pro organizaci hodnotu. Identifikace aktivu je procesem, který předchází vytvoření seznamu aktiv a stanovení jejich vlastníka.
- **Ochrana informací** se zaměřuje na zajištění důvěrnosti, integrity a dostupnosti informací. Riziko je vyjádření možnosti, že určitá hrozba může způsobit škodu nebo ztrátu daného aktiva.
- **Hrozba** je možnou příčinou nežádoucího incidentu, který může mít za následek poškození systému nebo organizace.

- **Hodnocení rizik** je proces zahrnující posouzení pravděpodobnosti výskytu bezpečnostního selhání v důsledku působení hrozeb a zranitelností, ale také zhodnocení dopadu na konkrétní aktiva. Zranitelnost představuje slabé místo v aktivu nebo skupině aktiv, které může být využito jednou nebo více hrozbami.
- **Incident** je neplánovaná událost, která negativně ovlivňuje kvalitu nebo funkčnost poskytované IT služby. Představuje poruchu narušující běžný provoz a způsobuje přerušení nebo omezení dostupnosti poskytovaných IT služeb. Incidenty mohou zahrnovat různé situace, například výpadek systému, porucha hardwaru, chyba v aplikaci, nedostupnost služby, bezpečnostní incident a další problémy, které brání plnému fungování IT služeb. Pro řešení incidentů se v ITIL využívá proces Incident Managementu, který je odpovědný za co nejrychlejší řešení a obnovení normálního provozu s cílem minimalizovat negativní dopad incidentu na uživatele. Incident Management zahrnuje kroky, jako identifikace incidentu, sběr informací, diagnostika, přiřazení odpovědnosti, řešení problému a uzavření incidentu. Jeho hlavním cílem je co nejrychleji obnovit IT službu a minimalizovat vliv incidentů na uživatele v souladu s definovanými úrovněmi služby a cíli dohodnutými s uživateli v rámci SLA. [10]
- **Problém management** se zaměřuje na identifikaci a odstranění základních příčin s cílem zabránit opakování incidentů. Je zde důraz na systematické řešení problémů, zajištění stability IT infrastruktury a poskytovaných služeb v souladu s dohodnutými úrovněmi služby (SLA). Hlavním úkolem problém managementu je zajistit, aby se základní příčiny problémů byly vyřešeny, což přispívá ke zlepšení celkového stavu IT infrastruktury a snižování výskytu incidentů. [10]
- **SLA** je smluvní dohoda mezi poskytovatelem služeb a uživatelem, ve které jsou stanoveny parametry a očekávání týkající se poskytovaných IT služeb. Tento nástroj slouží k vydefinování, monitorování a zajištění dostupnosti a výkonu služeb.

- **TMS** zkratka je označení čas, materiál, služby. Jedná se o model fakturace a fakturačních postupů, který se využívá při poskytování IT služeb a pracovních projektů. Tento model se týká způsobu, jak jsou účtovány a fakturovány náklady spojené s poskytovanými službami. V rámci tohoto modelu mají poskytovatelé IT služeb a dodavatelé možnost fakturovat zákazníkům za vynaložené úsilí (čas), materiální zdroje a další poskytnuté služby. Tento přístup se uplatňuje jak při interním řízení nákladů, tak při fakturaci klientům nebo zákazníkům.
- **ISMS** zkratka označuje Information Security Management System, což je systém řízení informační bezpečnosti. ISMS je rámec procesů, politik, postupů a kontrol, který pomáhá organizaci chránit její informace a zajišťovat jejich bezpečnost. Hlavním cílem ISMS je zajistit, že informace jsou chráněny před riziky, jako jsou neoprávněný přístup, ztráta, poškození nebo zneužití, a to dle požadavků stanovených v rámci ISO/IEC 27001. [11]
- **Informační portál:** Projektový portál v ITSM je aplikace nebo internetová platforma sloužící k centralizovanému řízení a správě projektu v rámci IT služeb. Projektový portál v ITSM poskytuje týmu projektu, společnosti a dalším přihlášeným stranám přístup k svému virtuálnímu prostoru.
- **FLS**: První linka podpory se podle ITIL v IT zaměřuje na rychlou reakci na požadavky uživatelů v souladu s vydefinovanými SLA. Součástí její práce může být vyřešení jednoduchých problémů a dotazů. Helpdesk v rámci L1 předá záležitosti na vyšší úroveň podpory, konkrétně na SLS nebo TLS, které disponují dovednostmi pro řešení složitějších problémů. Důležitou složkou FLS je také komunikace se zákazníkem, aby byly jeho požadavky správně porozuměny. [10]
- **SLS**: Druhá úroveň podpory v rámci ITIL se zabývá řešením složitějších problémů, které první linka podpory nedokáže vyřešit. Jejím hlavním úkolem je poskytovat technickou podporu pomocí pokročilých nástrojů pro řešení problémů. Tým SLS disponuje znalostmi v konkrétních oblastech IT služeb. [10]

- **TLS**: Třetí úroveň podpory se dle ITIL zabývá především řešením složitých problémů a incidentů. Je ještě specializovanější a disponuje nejvyšší úrovní znalostí a dovedností. Tým TLS často disponuje nástroji a přístupem ke zdrojovému kódu aplikace. [10]

Znalost těchto termínů umožní porozumět různým aspektům informační bezpečnosti, IT služeb a projektového řízení v organizaci. Tyto pojmy budou použity při provádění analýz, konkrétních příkladů a postupů v těchto oblastech.

3.3 Cíl recertifikace IT projektu v rámci bezpečnostního řízení informací

Cílem recertifikace projektu v rámci bezpečnostního managementu informací je ověřit, zda zkoumaný projekt nadále splňuje požadavky na informační bezpečnost a je v souladu s příslušnými standardy a normami. Během recertifikačního procesu projektu je prováděno zhodnocení souladu, audit, identifikace nedostatků.

Tento standard stanovuje požadavky pro vytvoření, implementaci, monitorování, hodnocení a zlepšování systému řízení informační bezpečnosti (ISMS – Information Security Management System). Dle ISO standardu [11] má několik hlavních cílů, které jsou dále blíže vyspecifikované dle Eucertu [12] jako:

- **Ochrana informací:** Pomáhá organizacím identifikovat a řídit rizika spojená s důvěrností, integritou a dostupností informací. Jeho účelem je minimalizovat riziko ztráty, poškození nebo neoprávněného přístupu k informacím.
- **Dodržování předpisů**: Standard poskytuje organizacím rámcovou strukturu, aby splňovaly relevantní právní a regulační požadavky týkající se ochrany informací. To zahrnuje například ochranu osobních údajů a dodržování předpisů specifických pro danou oblast.
- **Vytváření důvěry**: ISO/IEC 27001:2022 organizacím poskytuje prostředky, jak prokázat svou schopnost účinně řídit informační bezpečnost. Certifikace

dle tohoto standardu může přispět k budování důvěry mezi zákazníky, partnery a dalšími zainteresovanými stranami.

- **Neustálé zlepšování**: Klade důraz na kontinuální zlepšování systému řízení informační bezpečnosti organizace. Jeho cílem je přizpůsobovat se novým hrozbám a rizikům, zvyšovat účinnost a dosahovat lepších výsledků v oblasti informační bezpečnosti.

Splnění a dodržování těchto bodů má klíčový dopad na zajištění bezpečnosti informací v projektu, a zároveň umožňuje organizaci plnit své závazky vůči zákazníkům a regulačním orgánům. Projekt, který je certifikován dle ISO/IEC 27001:2022, dokládá, že organizace má pevný základ v oblasti řízení informační bezpečnosti a je schopna neustále se zdokonalovat podle aktuálních i budoucích požadavků.

3.4 Klasifikace a hodnocení informačních aktiv a bezpečnosti

V nejširším slova smyslu se informace rozumí jako záznam o aktuálním prostředí, jeho stavu a probíhajících procesech. Informace slouží k redukci nebo odstranění nejistoty v systému, zejména u jejich příjemců. Množství informace je určeno rozdílem mezi původní nejistotou systému (entropií) a nejistotou, která je snížena díky přijaté informaci. Informace může být chápána jako vlastnost organizované hmoty odrážející její hloubkovou strukturu, nebo jako poznání zachycené ve znakové formě na nosičích informace. V oblasti informační vědy se informace zejména chápe jako sdělení nebo poznatek, který má význam pro příjemce nebo jako údaj usnadňující rozhodování mezi alternativami. [13]

ISO definuje klíčové pojmy týkající se informační bezpečnosti následovně [11]:

- **Informační aktivum**: Tento pojem označuje cenné prvky spojené s informacemi mající hodnotu pro organizaci. Informační aktiva zahrnují informace samotné, ale také systémy, infrastrukturu, zařízení, software, sítě, zaměstnance a další prvky, které jsou nezbytné pro činnost organizace.

- **Informační bezpečnost**: Jedná se o opatření zaměřená na ochranu informací před různými hrozbami, jako je neoprávněný přístup, poškození, ztráta nebo zneužití. Informační bezpečnost se snaží zajistit důvěrnost, integritu a dostupnost informací a souvisejících prostředků.

Tyto definice poskytují jasný rámec pro pochopení významu informací a důležitosti jejich bezpečného zpracování v rámci organizace. Klasifikace informačních aktiv je proces, který slouží k zařazení informací a dalších aktiv do různých kategorií na základě jejich důležitosti, hodnoty nebo citlivosti. Cílem je dosáhnout vhodné úrovně ochrany a přidělit odpovídající bezpečnostní opatření. [11]

Hodnocení informačních aktiv se zaměřuje na identifikaci rizik spojených s těmito aktivy a jejich důsledků a pravděpodobnosti. Jeho cílem je získat přehled o potenciálních nebezpečích a slabých místech, které ohrožují informační aktiva. Následně určit vhodná opatření k jejich ochraně. Hodnocení probíhá systematickým procesem, který zahrnuje identifikaci hrozeb, analýzu rizik a stanovení přijatelné úrovně rizika v rámci informačního systému řízení bezpečnosti (ISMS) v souladu s požadavky normy ISO. [11]

3.5 Hrozba a zranitelnost

Vyhláška č. 82/2018 Sb. O kybernetické bezpečnosti identifikuje několik rizik, kterým jsou organizace vystaveny [14]:

- Porušení bezpečnostní politiky, neoprávněné činnosti a zneužití oprávnění uživatelů a administrátorů.
- Mezi škodlivý kód patří viry, spyware a trojské koně.
- Porušení fyzické bezpečnosti.
- Přerušení elektronické komunikace nebo dodávek elektrické energie.
- Chyby a nedbalosti ze strany zaměstnanců.
- Nedostatek zaměstnanců s potřebnou odborností.
- Úmyslné kybernetické útoky, včetně využívání sociálního inženýrství a špionážních technik.

- Napadení elektronické komunikace, včetně odposlechu a modifikace.
- Při analýze kybernetické bezpečnosti je důležité přiřadit jednotlivým aktivům možné hrozby. Často se vyskytuje více hrozeb pro jedno aktivum. Avšak samotné přiřazení hrozby k aktivu není konečným krokem. Je také nezbytné hodnotit pravděpodobnost, kdy se daná hrozba může na aktivu projevit. Pro hodnocení hrozeb se obvykle doporučuje použít čtyřstupňovou klasifikaci (nízká – kritická), kterou lze najít i v nástroji CSA.

Zranitelnost je chápána jako slabé místo v aktivu nebo v bezpečnostním opatření, které může být zneužito jednou nebo více hrozbami. Zranitelnost tedy představuje nedostatek, který umožňuje, aby se hrozba stala skutečností.

Vyhláška o kybernetické bezpečnosti představuje několik příkladů zranitelností, které zahrnují [14]:

- zastaralé systémy pro informace a komunikaci,
- nedostatečné povědomí o bezpečnosti uživatelů a administrátorů,
- nedostatečné sledování aktivit uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo problematické chování,
- nedostatečnou ochranu cenných aktiv,
- neadekvátní bezpečnostní architekturu,
- nedostatečnou nezávislou kontrolu.

Dodržování bezpečnostních parametrů a identifikace a odstranění zranitelností pomáhá organizacím minimalizovat riziko kybernetických hrozeb a zajišťuje ochranu informací, infrastruktury a služeb. Tyto body jsou důležité pro udržení bezpečnosti a stability projektu i organizace.

4 ITIL 4 metodika

V této kapitole dochází k rozboru ITIL metodiky, která je jednou z výchozích metodik v rámci firmy. Ačkoliv primární zaměření a cíl je úspěšné provedení a zmapování ISO auditu, tato metodika je důležitá z několika důvodů. V kontextu daného krátkého textu je zřejmé, že ITIL metodika má významný vliv na proces provedení ISO auditu a je považována za jednu z hlavních určujících metodik v rámci firmy. Při implementaci ISO auditu je důležité mít vhodné procesy a postupy pro správu informační bezpečnosti a řízení IT služeb. ITIL metodika tedy umožňuje zajištění souladu s požadavky ISO 27001 a přizpůsobení interních procesů a postupů na základě osvědčených postupů. ITIL se zaměřuje na řízení služeb IT a zajištění kontinuity jejich poskytování. To je klíčové pro ISO audit, protože hodnotí efektivitu a bezpečnost poskytovaných IT služeb. Tímto způsobem přispívá k úspěšnému provedení ISO auditu a zvyšuje šance na dosažení souladu s požadavky informační bezpečnosti.

4.1 ITIL verze

Podle publikace ITIL je ITIL (Information Technology Infrastructure Library) definován jako uznávaný rámec pro správu IT služeb s celosvětovou platností. ITIL představuje soubor osvědčených postupů, konceptů a metodik, které organizacím pomáhají účinně řídit své IT služby a maximalizovat jejich hodnotu pro zákazníky i samotnou organizaci. [10]

Předchozí verzí byl ITIL 3, v této práci bude odkazováno na verzi z roku 2011. Mezi ITIL 4 a ITIL 3 existuje několik významných rozdílů, které byly provedeny s úmyslem aktualizovat a vylepšit celkový rámec ITIL. Mezi hlavní rozdíly lze uvést [15]:

- **Přístup**: ITIL 3 se zakládá na procesním přístupu, který klade důraz na definici a sledování procesů. Naproti tomu ITIL 4 přináší holistický přístup zaměřující se na hodnotu a výsledky poskytované IT službami.
- **Hodnota**: Zatímco ITIL 3 se zaměřuje na poskytování hodnoty IT službami pro zákazníka, ITIL 4 posouvá důraz na poskytování hodnoty dále

a zahrnuje koncept hodnotového systému, který zohledňuje i externí faktory, jako je spolupráce, kultura a technologie.

- **Životní cyklus služby**: ITIL 3 pracuje s životním cyklem služby, který se skládá ze čtyř fází: strategie, návrh, provoz a zlepšování. ITIL 4 tento životní cyklus služby nahrazuje konceptem služebního řetězce, který zahrnuje šest hlavních činností: plánování, vytváření, dodání, podpora, zajištění a zlepšování.

Celkově lze ITIL v ITIL 4 edition chápat jako rámec a soubor osvědčených postupů, které organizacím pomáhají dosáhnout lepší správy a poskytování IT služeb. Hlavním zaměřením ITIL 4 je maximalizace hodnoty IT služeb pro zákazníky a organizaci a poskytuje moderní a flexibilní přístup k řízení IT prostředí.

V rámci zkoumané problematiky důrazem na poskytování služeb (SLS), která bude dále blíže popsaná, je častější implementace ITIL 4. ITIL 4 je modernější verze, jež se více soustředí na hodnotu, výsledky a celkový přínos IT služeb pro organizaci. Poskytuje lepší rámec pro správu a provoz IT služeb a tím i zlepšuje kvalitu a efektivitu servisu zaměřeném na služby. Některé zmínky však budou odkazovat také na ITIL 3, jelikož je organizace stále využívá a v ITIL 4 byly vynechány.

4.2 Spojení mezi ITIL 4 and ISO 270001

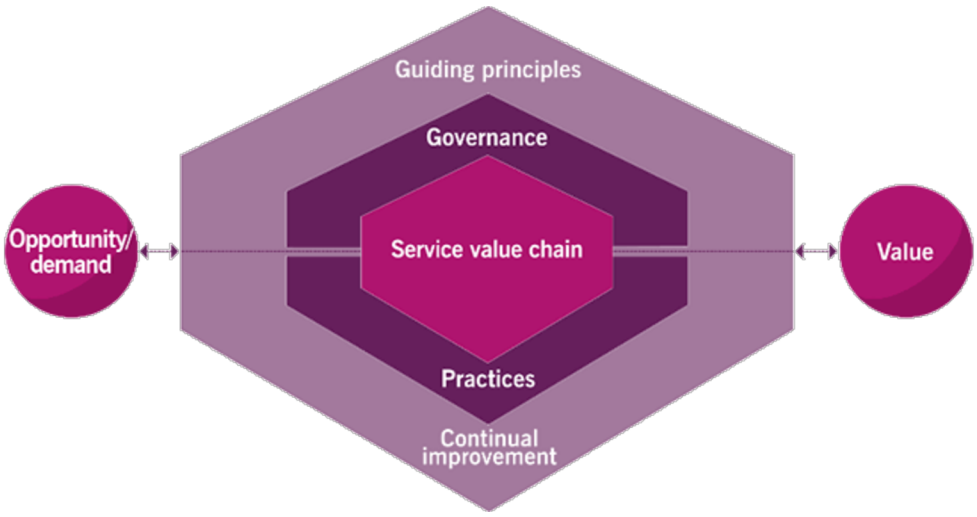
Podle porovnání ITIL 4 a ISO 27001 si navzájem doplňují a poskytují komplementární přístupy. ITIL 4 je rámec, který se zaměřuje na správu IT služeb a klade důraz na procesy, postupy a koncepty pro účinné poskytování IT služeb a maximalizaci jejich hodnoty pro organizaci a zákazníky. Na druhou stranu, ISO 27001 je mezinárodní standard pro řízení bezpečnosti informací, který stanovuje požadavky a směrnice pro správu a ochranu informací v organizaci. [16]

Při implementaci ITIL 4 může ISO 27001 sloužit jako referenční rámec pro informační bezpečnost. ISO 27001 nabízí ověřené postupy pro identifikaci, hodnocení a řízení rizik spojených s informační bezpečností. Podle ITIL 4 je

bezpečnost informací klíčovým faktorem, který je nutné zohlednit při návrhu a provozu IT služeb. Implementace ISO 27001 může organizacím pomoci dodržovat osvědčené postupy a mezinárodně uznávané standardy v oblasti bezpečnosti informací.

ITIL 4 a ISO 27001 mají společný cíl zlepšovat řízení a poskytování IT služeb. ITIL 4 se zaměřuje na celkovou správu služeb IT a zvyšování hodnoty pro zákazníky (Obrázek 1), zatímco ISO 27001 se soustředí na ochranu a zabezpečení informací. Tyto dva rámce mohou být vzájemně propojeny a integrovány, aby organizace dosáhla efektivního řízení IT služeb a zabezpečení informací dle mezinárodních standardů.

Spolupráce mezi ITIL 4 a ISO 27001 umožňuje organizacím získat komplexní přístup k řízení IT služeb, který zahrnuje aspekty správy služeb i informační bezpečnosti. Integrace těchto dvou rámů může přinést synergické výhody, které organizaci pomáhají dosáhnout efektivnějších a bezpečnějších IT procesů a služeb.

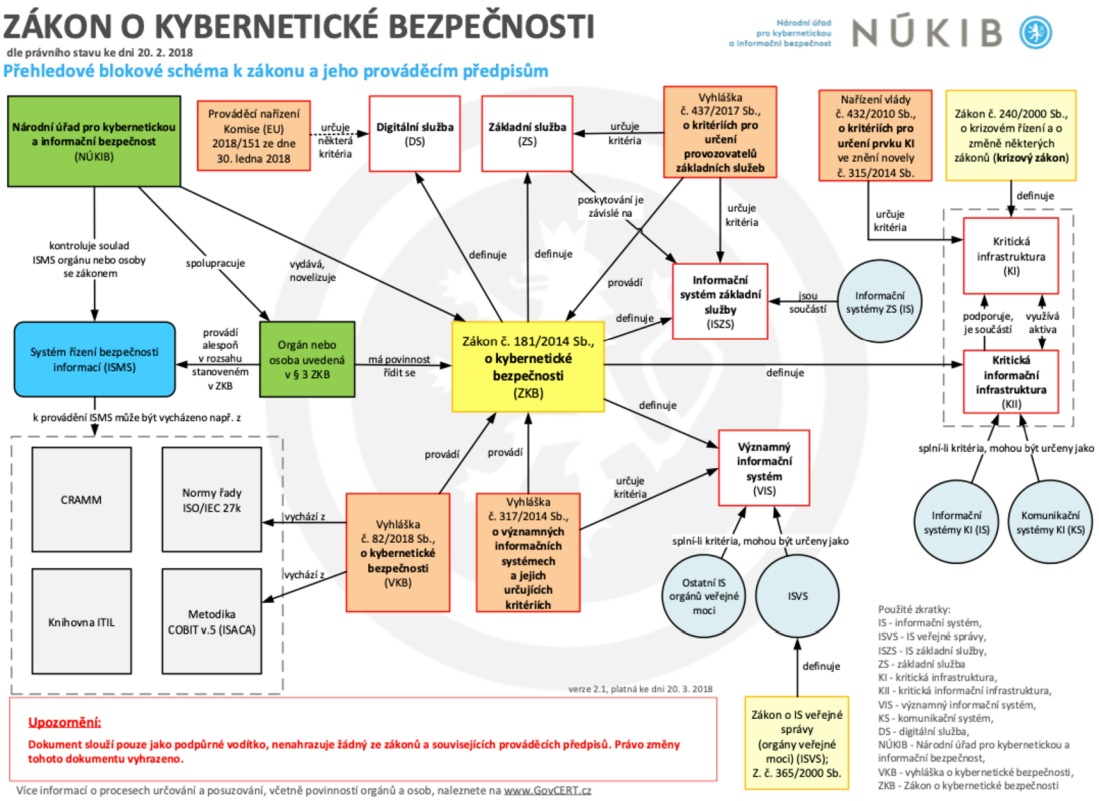


Obrázek 1: ITIL proces [17]

V rámci zákonu č. 181/2014 Sb [18], o kybernetické bezpečnosti, vzniklo blokové schéma (Obrázek 2), které vztahy mezi uváděnými normami, standardy a metodikami vysvětluje.

Toto blokové schéma kybernetické bezpečnosti je grafickým znázorněním struktur, prvků a vztahů definovaných v daném právním předpisu. Jedná se o vizualizační nástroj, který usnadňuje pochopení a výklad zákona o kybernetické bezpečnosti. Následující vývojový diagram má poskytnout strukturovaný a snadno čitelný přehled klíčových aspektů zákona o kybernetické bezpečnosti. Pomáhá identifikovat hlavní prvky zákona a jejich vzájemné vztahy, a tím usnadňuje jeho výklad a aplikaci.

Vývojový diagram zákona o kybernetické bezpečnosti je užitečným nástrojem pro právníky, odborníky na kybernetickou bezpečnost a další zúčastněné strany. Pomáhá jim získat komplexní pochopení právních požadavků, povinností a procesů v oblasti kybernetické bezpečnosti, usnadňuje jejich dodržování a vymáhání.



Obrázek 2: Zákon o kybernetické bezpečnosti [19]

4.3 ITSM systémy pro podporu ITIL procesů

Existuje několik důvodů, proč organizace potřebují nástroje pro správu, které zaručí to, že organizace dokáže zajistit normy a požadavky v rámci své správy. Nástroje pro sledování a správu incidentů umožňují organizacím sledovat, spravovat a řešit vzniklé incidenty. Jsou odpovědní za přidělování incidentů příslušným týmům, jejich sledování a řešení v pořadí podle priority a na dohodnutých úrovních služeb. Tyto nástroje nabízejí pohodlí centralizovaného monitorování a řízení IT procesů. Díky konsolidaci incidentů, problémů, změn a dalších úkolů správy IT služeb mohou organizace zefektivnit své operace. Poskytují způsoby, jak zautomatizovat a standardizovat IT procesy, což vede ke zvýšené konzistenci, rychlejším procesům a minimálním lidským chybám. Lze vytvořit pravidla a pracovní postupy pro různé typy požadavků, incidentů a vytvořit opakovaně použitelné šablony. Tento proces automatizace a standardizace pomáhá omezovat nekonzistence a ruční zásahy. Umožňují také vytváření reportů a analýz, které poskytují organizacím přehled o výkonnosti a

stavu IT procesů. Umožňují sledování klíčových ukazatelů výkonu (KPI), identifikaci trendů a problematických oblastí a usnadňují rozhodování na základě dat.

4.3.1 Softwarové nástroje pro evidenci chyb a problémů

Mezi nejdoporučovanější systémy pro zaznamenávání požadavků patří také následující platformy, které byly v rámci zvoleného IT projektu aktivně používané. [20]

- **ServiceNow**: Jedná se o velmi populární platformu pro správu služeb IT, která poskytuje širokou škálu funkcí pro sledování incidentů, problémů, změn, konfigurací a dalších aspektů ITIL. ServiceNow umožňuje centralizované sledování a správu IT procesů. ServiceNow proaktivně sleduje a implementuje bezpečnostní protokoly [21]:
    - ISO/IEC 27017:2015,
    - ISO/IEC 27001:2013,
    - ISO/IEC 27018:2019,
    - ISO/IEC 27701:2019.
- **Jira Service Management**: Tento systém, který je součástí širší platformy Jira, je široce využíván pro sledování incidentů, problémů a změn. Poskytuje také možnosti správy znalostní báze a reportingu, což je důležité pro řízení a analýzu dat. Podle Centra pro dodržování regulací Jira poskytuje, pro tuto práci důležité, následující předpisy [22]:
    - ISO/IEC 27001:2013,
    - GDPR.

- **Zendesk**: Tento systém je známý svým silným zaměřením na správu zákaznické podpory a sledování incidentů. Poskytuje také možnosti pro správu znalostní báze. Zendesk se ve svém prohlášení zavazuje dodržovat následující standardy [23]:
    - ISO 27001,
    - ISO 27018,
    - ISO 27701.

Volba systému se stala otazníkem během příprav na audit a bude více rozebrána v praktické části.

5 Energetika a vliv na bezpečnost

Bezpečnost v energetické oblasti je považována za velmi důležitou z několika důvodů. Fakt, že se softwarová firma specializuje právě na tuto oblast, naznačuje, že zkoumaný projekt se zaměřuje na energetické systémy a infrastrukturu. Projekt má rozsah napříč Evropou, což znamená, že se v bezpečnostních opatřeních musí zohlednit více než jeden stát, což přináší vyšší úroveň složitosti. Je zásadní, aby veškerá komunikace, přenos dat a operace byly zabezpečeny proti neoprávněnému přístupu, manipulaci a sabotáži. K tomuto účelu je třeba implementovat bezpečnostní prvky, jako je šifrování dat, autentizace uživatelů a monitorování síťového provozu a další opatření, která jsou nezbytná pro ochranu systému před hrozbami a útoky. Bezpečnost energetických systémů je kritická i z hlediska státu, protože tyto systémy představují strategickou infrastrukturu a mají významný vliv na národní bezpečnost a suverenitu. V reakci na kybernetické hrozby, teroristické útoky a další formy útoků projevují státy zvýšený zájem o ochranu energetických sítí. Bezpečnostní opatření v rámci energetických projektů jsou proto předmětem zvláštní pozornosti a dohledu ze strany vlád a regulátorů. Celkově lze tedy konstatovat, že bezpečnost v energetické oblasti je významným konceptem kvůli kritičnosti energetických systémů, jejich rozsahu přesahujícího jednotlivé státy a vlivu, který mají na státy a společnost jako celek.

5.1 Kritická infrastruktura státu

Existuje mnoho zákonů a předpisů upravujících kybernetickou bezpečnost pro energetické IT projekty. Tyto zákony se liší podle země a jurisdikce, kde je projekt realizován. Níže je uveden seznam několika mezinárodních a regionálních předpisů, které jsou obecně relevantní pro kybernetickou bezpečnost v energetickém sektoru:

- **Směrnice EU NIS** (Bezpečnost sítí a informací): Tato směrnice představuje součást legislativy Evropské unie, která stanovuje požadavky v oblasti kybernetické bezpečnosti a povinnost hlášení incidentů pro poskytovatele služeb digitální infrastruktury v energetickém sektoru.

V současné době dochází k přípravě novinek ve směrnici. Jak uvádí na svých stránkách NÚKIB [24], směrnice NIS2 vnáší řadu změn v prostoru kybernetické bezpečnosti, a to nejen pro organizace, které již mají povinnost chránit své systémy podle platného zákona o kybernetické bezpečnosti, ale také pro velké množství nových a regulovaných organizací, které dosud nemusely splňovat žádné závazky. V současné době nedochází ke konkrétní implementaci v rámci zkoumané problematiky.

- **ISO/IEC 27001**: Tato mezinárodní norma pro systémy managementu bezpečnosti informací poskytuje rámcový přístup pro identifikaci a řízení kybernetických rizik, a to i v energetickém sektoru. Mnoho energetických společností implementuje tento standard jako součást svých bezpečnostních postupů.
- **Zákony o kybernetické bezpečnosti**: Mnoho zemí má své vlastní zákony o kybernetické bezpečnosti pokrývající různá průmyslová odvětví včetně energetiky. Tyto zákony mohou vytvářet povinnosti, předpisy a standardy pro ochranu kybernetické bezpečnosti a hlášení incidentů. V této práci se jedná o klíčovou normu, podle které bude provedena recertifikace.

5.2 Požadavky na nakládání s informacemi

Zákony na ochranu dat, jako je obecné nařízení Evropské unie o ochraně osobních údajů (GDPR) a podobná legislativa v jiných zemích, stanovují pravidla pro ochranu osobních údajů. V energetickém sektoru mohou IT projekty podléhat těmto zákonům, pokud zpracovávají osobní údaje.

Společnost třídí všechny projekty do čtyř úrovní na základě zpracování osobních údajů:

- **Žádné osobní** údaje nejsou zpracovávány.
- Jsou zpracovávány pouze **základní osobní údaje** v malém rozsahu.
- Zpracovávají se **osobní údaje ve větším rozsahu** nebo se zpracovávají citlivé osobní údaje v prostředí klienta.

- Probíhá zpracování **velkého množství osobních údajů** a zpracování citlivých osobních údajů.

Klasifikace zabezpečení je interní proces přidělování úrovní zabezpečení různým projektům nebo systémům podle jejich požadavků a rizik. Jedná se o hierarchické rozdělení, které identifikuje a spravuje související zabezpečení a ochranu dat. Klasifikace zabezpečení určují ochranná opatření a úrovně nezbytné k ochraně informací a systémů před neoprávněným přístupem, zneužitím nebo ztrátou dat.

- **Standardní úroveň zabezpečení:** nákladově efektivní, efektivní zabezpečení.
- **Zvýšená úroveň zabezpečení:** výchozí úroveň, vyvážení vysokých požadavků na zabezpečení a náklady.
- **Vysoká úroveň zabezpečení:** velmi vysoká úroveň zabezpečení pro kritické systémy.

V rámci této práce zákony na ochranu osobních definují stupeň zabezpečení projektu, ačkoliv podléhají bezpečnostní klasifikaci, která určuje minimální stupeň projektu.

6 Praktická aplikace norem ve zkoumaném projektu

V této kapitole se provádí analýza konkrétních aplikací norem ve firmě. Tyto aplikace nejsou přímo součástí samotného ISO auditu, ale představují vyšší úroveň firemního prvku, který ovlivňuje samotné projekty, a tedy i následný zkoumaný audit. Proto je nezbytné provést důkladné zkoumání bezpečnostních standardů, které jdou nad rámec té nejvyšší úrovně.

- Cílem **právního a normativního souladu** ISO 27001 je pomoci splnit konkrétní legislativní požadavky jak v procesní, tak i v technické oblasti, ať už se jedná o nařízení EU (např. Network and Information Security Directive), mezinárodní zákon (např. Sarbanes-Oxley Act) či českou legislativu (zákon o kybernetické bezpečnosti). Nejde tak jen o to, nadefinovat procesy a procedury, nastavit technologická opatření, ale také poskytnout podporu i v rámci samotného auditu ISO 27001.
- **RedTeam** přesně simuluje reálný kybernetický útok na organizaci, což zahrnuje činnost motivované skupiny útočníků, kteří využívají různé techniky za účelem získání nejcennějších informací. Díky této operaci lze získat jasnou informaci o stavu zabezpečení.
- Při přezkoumání **bezpečnostní architektury** dochází k posouzení návrhu bezpečnostní architektury a zajištění souladu s aktuálními bezpečnostními standardy. Proběhne revize existující architektury a dojde k odhalení bezpečnostní chyby v návrhu, které mohou ohrozit dostupnost, důvěrnost a integritu dat. Cílem nastavení systému řízení informační bezpečnosti (ISMS) je zhodnotit existující úroveň systému řízení informační bezpečnosti a navrhnout opatření pro dosažení žádoucí, efektivní úrovně. Následně nastavit jednotlivé procesy a vytvořit nezbytnou dokumentaci pro jejich implementaci.
- Cílem **OWASP ASVS** auditu je posoudit shodu zabezpečení informačního systému oproti jeho standardům a tím poskytnout míru ujištění ohledně organizace, doporučení k nápravě chyb a současně prožít cílený kybernetický útok „nanečisto“.

- Smyslem **penetračních testů** je prověřit bezpečnost aplikace nebo infrastruktury a efektivně odhalit zranitelnosti informačních systémů, které by mohly být zneužity útočníkem a poškodit společnost. Penetrační testování představuje systematický a komplexní proces prověření bezpečnosti aplikace a /nebo infrastruktury, který identifikuje existující zranitelnosti informačních systémů a pomáhá předejít potenciálním problémům, které by mohly ohrozit firmu. Bezpečnost informací se zaměřuje na širokou škálu hrozeb s cílem zajistit kontinuitu činností organizace, minimalizovat obchodní ztráty a maximalizovat návratnost investic a podnikatelské příležitosti. ISMS představuje systematický, dokumentovaný a řízený systém správy informačních aktiv, který má za cíl eliminovat možnou ztrátu nebo poškození těchto aktiv.
- Cílem **SDLC – Secure Development Lifecycle** je úspěšná implementace metodiky bezpečného vývoje. Metodika SDLC přináší principy bezpečnosti a důvěrnosti po celý vývojový cyklus a pomáhá vývojářům vytvářet vysokou úroveň bezpečnosti software při snížení nákladů na vývoj. Bezpečnost vývoje, a tedy celého informačního systému, by měla být založena na základních principech, které se dodržují po celou dobu životního cyklu projektu – od návrhu IS, plánování, samotného kódování až po testování a provoz.
- **Forenzní analýza kybernetického útoku** probíhá post mortem. Jedná se o analýzu kybernetického útoku s cílem odpovědět na otázky: jak došlo k útoku, jak se infekce šířila, kam se útočník dostal, jaká data byla ztracena, jaká další rizika existují a často i kdo stojí za útokem. Součástí analýzy je navržení opatření k odstranění zranitelností, které umožnily provedení útoku, ať už se jednalo o hackování nebo neautorizovanou změnu firemních dat.

Tyto pravidla a standardy stanovují specifické bezpečnostní požadavky, které jsou navrženy tak, aby splňovaly interní požadavky a cíle organizace. Ačkoli tyto aplikace nejsou přímo součástí ISO auditu, mají klíčový vliv na celkovou úroveň bezpečnosti a řízení projektů. Důležitost rozboru těchto bezpečnostních

standardů spočívá v pochopení jejich významu a implementace ve firmě. Tímto způsobem je možné identifikovat klíčové oblasti, které ovlivňují projekty a mají značný dopad na informační bezpečnost a řízení rizik. Analyzování bezpečnostních standardů od nejvyšší úrovně je klíčové, neboť umožňuje hlubší porozumění jejich vztahu k celkovému bezpečnostnímu rámci firmy. Identifikace jejich vlivu na projekty umožňuje zavedení odpovídajících opatření a postupů, které jsou nezbytné pro dosažení požadované úrovně bezpečnosti.

6.1 Projekt a jeho aktuální stav, přístupy

V rámci informačního systému řízení bezpečnosti (ISMS) jsou jednoznačně definované funkce, povinnosti a pravomoci v organizaci v souvislosti s informační bezpečností. Tento prvek zahrnuje určení specifických rolí, přiřazení odpovědností a oprávnění jednotlivým členům organizace.

Organizační role se vztahují na konkrétní pozice nebo funkce, které mají zodpovědnost za správu informační bezpečnosti. Tímto způsobem se stanovují například role informačního bezpečnostního manažera, IT správce nebo vedoucích pracovníků.

Odpovědnosti se týkají specifických úkolů a povinností přiřazených jednotlivým rolím. Každá role má specifické odpovědnosti v oblasti ochrany informací a správy ISMS. Tyto odpovědnosti mohou zahrnovat například stanovení politiky informační bezpečnosti, hodnocení a řízení rizik, implementaci bezpečnostních opatření a školení zaměstnanců.

Pravomoci se týkají oprávnění a schopnosti jednotlivých členů organizace přijímat rozhodnutí, provádět opatření a vykonávat činnosti v rámci informační bezpečnosti.

Definice organizačních rolí, odpovědností a pravomocí jsou důležité pro jasnou strukturu a rozdělení úkolů v rámci ISMS. Tím se zajistí, že každý v organizaci ví, jaké jsou jeho povinnosti a oprávnění v souvislosti s ochranou informací a že odpovědnosti jsou správně přiděleny a vykonávány v souladu s požadavky na informační bezpečnost. [10]

V době před recertifikací se každý projekt řídí dvěma klasifikacemi – GDPR a Bezpečnostní klasifikací, které budou blíže popsané v následujících kapitolách. V rámci projektu jsou vydefinovány následující role:

- zaměstnanec,
- projektový manažer,
- bezpečnostní koordinátor.

Tyto role jsou pro nadcházející audit předělány v rámci migrace do nového projektového portálu takovým způsobem, aby umožnovaly jednoduchou správu a implicitní práva.

Kromě těchto univerzálních rolí lze také přiřazovat explicitní práva pro jednotlivé uživatele.

6.2 Certifikované normy společnosti

V rámci firemního prostředí a provádění auditu projektu se vyskytuje interakce s více než jedním standardem. Tato situace je důsledkem specifických požadavků a norem, které jsou aplikovány ve firmě a mají vliv na projektovou činnost. S ohledem na tuto skutečnost je v této kapitole představena kolekce norem, která zahrnuje soubor standardů a předpisů, jež jsou definovány na nejvyšší úrovni v rámci celé organizace. Cílem uvedení této kolekce certifikovaných norem je zdůraznit jejich význam a dopad na průběh samotného projektu. Tyto normy jsou navrženy tak, aby zabezpečily soulad s interními požadavky a zároveň usnadnily dosažení projektových cílů. Jsou také důležitým nástrojem pro zajištění dodržování předepsaných postupů a standardů v rámci celé organizace. Je nezbytné zhodnotit, jak tyto normy ovlivňují plánování, provádění a řízení projektu. Zahrnutí těchto normativních požadavků v projektových aktivitách je zásadní pro dosažení souladu s požadavky konkrétního auditní procesu.

ISO 9001 je norma Mezinárodní organizace pro normalizaci (ISO) s názvem „ISO 9001: Systémy managementu kvality“. Jde o standard managementu kvality,

který stanovuje požadavky na systém managementu pro řízení jakosti. QMS se zabývá procesy a postupy, které organizace používá k zajištění kvality svých produktů a služeb k dosažení spokojenosti zákazníků. [25]

ISO 14001 je norma Mezinárodní organizace pro normalizaci (ISO) s názvem „ISO 14001: Systémy environmentálního managementu – Požadavky a jejich aplikace“. Jedná se o standard pro systémy ochrany životního prostředí. Za tímto účelem byl vyvinut soubor norem systému environmentálního managementu, který poskytuje rámec pro zavádění, provozování a zlepšování systému environmentálního managementu (EMS) v organizaci. Účelem normy je umožnit organizacím minimalizovat negativní dopady jejich činností na životní prostředí a zároveň dosáhnout udržitelnosti a zachování přírodních zdrojů. [26]

Norma ISO/IEC 20000-1 je mezinárodním standardem, ve kterém jsou shrnuty základní postupy ITIL do standardizovaných kritérií, podle kterých lze úroveň služby zavádět, implementovat, udržovat a neustále se zlepšovat. Tato norma stanovuje požadavky na systém řízení služeb (Service Management System – SMS) pro organizaci poskytující IT služby s cílem zajistit kvalitu IT služeb, které společnost poskytuje. Stanovuje požadavky na vytvoření systému managementu a osvědčené postupy pro management firemních IT služeb. [27]

ISO/IEC 27001 – ISMS – Information Security Management System – Systém řízení informační bezpečnosti.

6.3 Důvody změn

Společnost a její projekty se zavazují plnit specifické legislativní požadavky v procesní a technické oblasti, ať už jde o nařízení EU (např. směrnice o kybernetické a informační bezpečnosti), mezinárodní právo (např. Sarbanes-Oxley) nebo českou legislativu (zákon o kybernetické bezpečnosti). V rámci zkoumaného projektu se často nejedná pouze o certifikaci samotného projektu, ale často se účastní také certifikace projektů klientů. To znamená, že organizace nejen připravuje a provádí certifikace svých vlastních projektů, ale také se podílí na certifikaci projektů svých klientů. Společnost poskytuje potřebnou znalostní

bázi, která je nezbytná pro úspěšné absolvování certifikačního procesu. Společnost je schopna identifikovat nedostatky a poskytnout doporučení a řešení, které vedou ke zvýšení bezpečnosti a dosažení požadovaného certifikátu. Účast na certifikacích klientů je pro organizaci přínosná z několika důvodů. Zaprvé, tímto způsobem společnost získává další zkušenosti a znalosti z různých projektů a odvětví, což ji posiluje jako odborného partnera v oblasti informační bezpečnosti. Za druhé, účast na certifikacích klientů rozšiřuje sítě společnosti a vytváří příležitosti pro nové obchodní kontakty a spolupráci. Tímto způsobem se organizace rozšiřuje na trhu a získává konkurenční výhodu.

V rámci certifikačních doporučení a návodů, které lze shrnout dle definice ustanovení „ISO 27001 pro Neustálé Zlepšování“. Standard ISO 27001 vymezuje ustanovení tak, že by organizace měla neustále zlepšovat vhodnost, dostatečnost a účinnost systému řízení informační bezpečnosti. Jak splnit požadavky na neustálé zlepšování dle normy ISO 27001, pak lze shrnout rámci certifikačních doporučení a návodů. [28]

6.3.1 Zavedení evidence incidentů a korektivních opatření

Vytvořením politiky pro řízení incidentů a korektivních opatření, stejně jako politiku pro neustálé zlepšování. Tyto politiky určují, jak se vypořádat s nesouladem. V rámci předcházení samotných incidentů je vytvořený takzvaný risk list, do kterého se na pravidelné bázi zapisují risky, které mohou vést k incidentům nebo jiným hrozbám. Hrozby jsou faktory, které představují potenciální riziko poškození zkoumaného systému a jeho majetku. Mohou mít nežádoucí dopady a negativní účinky. Hrozby se mohou vyskytovat přirozeně, nebo mohou být způsobeny lidským jednáním, také mohou být náhodné nebo úmyslné. Je důležité identifikovat zdroje náhodných i úmyslných hrozeb a odhadnout pravděpodobnost jejich výskytu.

Pro odhad hrozeb se používá vstup od vlastníků nebo uživatelů aktiv, zaměstnanců personálního oddělení, manažerů, odborníků a osob odpovědných za ochranu organizace.

Výsledkem posouzení hrozeb je seznam identifikovaných hrozeb, aktiv nebo skupin aktiv, který umožní správu incidentů a korektivních opatření. Tento evidenční systém je klíčovým nástrojem pro řízení nesouladů, které by mohly být těmito hrozbami ovlivněny a úroveň pravděpodobnosti, že k hrozbě dojde, je hodnocena jako nízká, střední nebo vysoká.

Ukázka současného risk listu (Tabulka 1), a jakým způsobem se nyní evidují v systému:

JMÉNO	DOPAD	POPIS	MITIGACE
KOMUNIKACE	Malý	Komunikace s externím týmem je nejasná.	Vydefinování zodpovědností, pravidelné mítinky.
ZOTAVENÍ PO INCIDENTU MODULU	Vysoký	Neexistuje automatický systém obnovy.	Vytvoření nové virtuální lokace, automatické přepnutí.
PRAVIDLA PRO UCHOVÁNÍ DAT	Střední	Nefungující procesy pro archivaci, nárůst na HW náročnost.	Dočasné skripty na manuální promazávání. Trvalé řešení v podobě implementace.

Tabulka 1: Risk list

6.3.2 Zavedení procesu řízení incidentů

Proces řízení incidentů určuje postupy pro zvládání incidentů. Tyto incidenty představují jednu z hlavních metod identifikace nesouladů.

V rámci řízení incidentu je zavedené pravidlo, které vyžaduje informování v rámci vydefinovaných SLA, a následně pravidelná aktualizace stavu až do vyřešení Incidentu, po kterém je možné dále v rámci problému.

V rámci auditu bylo kontrolováno, že bezpečnostní incident splňuje následující minimální požadavky:

- popis incidentu,
- datum vzniku incidentu,
- osobu, která incident identifikovala,
- kategorizaci incidentů,
- opatření, která byla bezprostředně přijata pro ukončení incidentu.

Následující interní pravidla v souladu s ITIL musí být dodržena [10]:

- **Definice incidentu**: Určení, jaké události se považují za incidenty v rámci informačního bezpečnostního řízení organizace.
- **Hlášení incidentu**: Stanovení postupů pro nahlášení incidentů, včetně instrukcí pro zaměstnance nebo uživatele, jak informovat o podezřelých aktivitách nebo bezpečnostních incidentech.
- **Klasifikace incidentů**: Rozdělení incidentů do kategorií nebo úrovní závažnosti, aby bylo možné přiřadit vhodnou reakci a určit prioritu jejich řešení.
- **Vyšetřování incidentů**: Provádění důkladného vyšetřování incidentů, včetně shromažďování důkazů, analýzy příčin, identifikace postižených systémů a posouzení dopadů.
- **Opatření a korektivní akce**: Implementace opatření a korektivních akcí zaměřených na řešení incidentů a prevenci jejich opakování v budoucnosti.
- **Komunikace a informování**: Zajištění efektivní komunikace a informování všech relevantních zainteresovaných stran, včetně interních týmů, vedení, zaměstnanců a případně i externích subjektů.
- **Dokumentace**: Zavedení dokumentace, která podrobně popisuje postupy, pravidla a odpovědnosti související s procesem řízení incidentů.

V rámci projektu se zavedl způsob hlášení, který tedy splňuje nejenom požadavky norem, ale také preference zákazníka. Ukázka řízení incidentu v rámci projektu dle vydefinovaných bodů (Obrázek 3):

Incident Start Time	22-04-2023 15:49 CEST	**Incident Number**	Jira-444
Incident Reported Time	22-04-2023 15:49 CEST	**Incident Priority**	High
Incident Resolution Time	22-04-2023 16:57 CEST, Final fix not available yet	**Assigned To / Resolved By**	SLS
Impacted Services	PROD client	Client-prod	
Impacted Customers	Operator		
Reported by	Incident identified by operators		
Impact Description	Delay in processing messages, connectivity test for Client returned disconnected status.		
Investigation Analysis	22.04. 15:49 – Operator reported the issue with connectivity status 22.04. 15:55 – SLS initiate investigation 22.04. 16:57 –SLS cleaned large logs. After logs clean-up, client was connected again. The large log size were already reported by SLS in Jira ticket. 22.04. 17:00 – Operator confirmed that connection was stable. 22.04. 18:08 – Operator reported unstable connection again. 22.04. 22:31 – SLS provided RCA – that reported issue is caused by heavy traffic. 23.04. 20:14 – SLS confirmed the root cause – when connectivity test is failing, there is queue of thousand messages waiting to be processed on Receiver side. 24.04. 16:20 – Ticket was created in order to validate possibilities for performance improvements on client side.		
Resolution	If Client is publishing or downloading large amount of data, this data has a priority before the connectivity test, so the connectivity test ACK is not delivered in time and client will look like disconnected even when files are being downloaded and uploaded properly. In peaks there are thousands of messages waiting to be consumed by client. These messages are being consumed, however it can take several minutes until all is processed. SLS will validate possibilities of performance improvements for the client in order to speed up processing of messages from Sender. SLS has created Jira-444 to validate possibilities for performance improvements. After configuration performance adjustments are defined and agreed, separate tickets for deployment to ACCE and PROD environments will be created. The large log size is probably not connected with the reported connectivity instability, this will be fixed within separate ticket Jira-444.		

Obrázek 3: Hlášení incidentu [Vlastní šetření]

V rámci vyřešení je následně nutné vyhodnotit incident a poučit se z incidentu, tzv. „Lessons learned“. Mezi opatření může patřit:

- Vytvoření nových nebo úprava stávajících technických opatření.
- Změna nebo úprava stávajícího procesu nebo úprava postupů.
    - Veškeré procesy jsou interně dokumentovány a dostupné zákazníkovi, proto je dochází ke kontrole z obou stran.
- Plány týkající se bezpečnostních politik a směrnic.
- Efektivní sdílení informací s kolegy a externími partnery.
    - K vyhodnocení dochází během pravidelných mítinků.

Hlavním přínosem řízení incidentů je zajištění rychlé a účinné reakce na zjištěné incidenty a odchylky. Pravidelné hlášení, klasifikace, vyšetřování a dokumentace incidentů umožňují sledovat průběh řešení, přijímat korektivní opatření a zabránit opakování problémů. Dále podporuje transparentní komunikaci a informování všech zúčastněných stran, umožňuje poučit se

z incidentů a implementovat opatření pro zlepšení budoucího řízení bezpečnosti a spolehlivosti projektu.

6.3.3 Reportování nesouladů a korektivních opatření týmu pro přezkoumání řízení

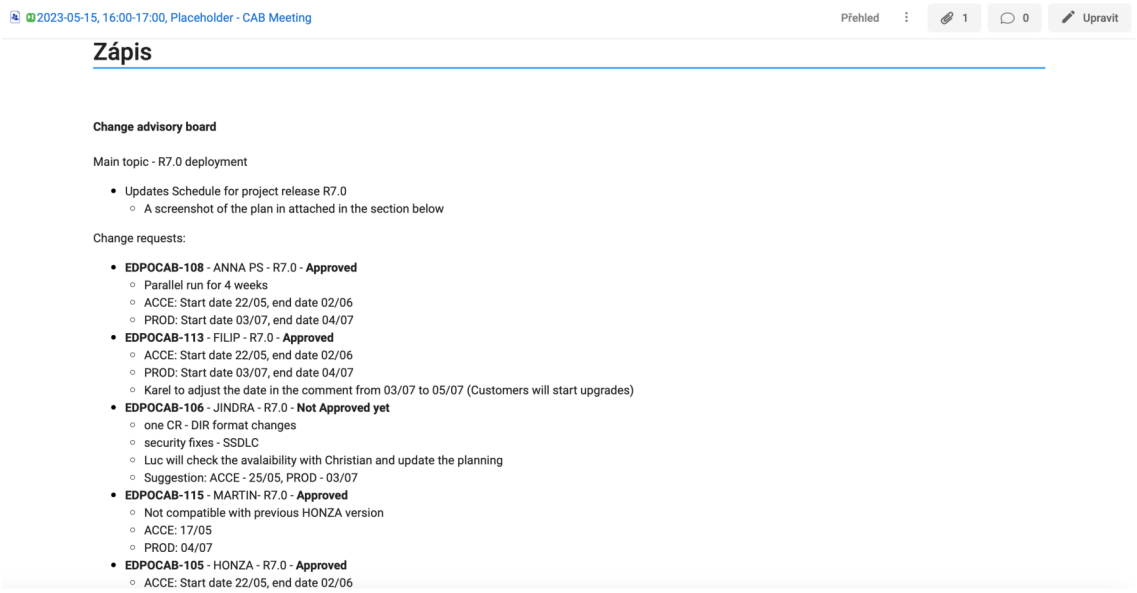
Tým pro přezkoumání řízení poskytuje dohled a rozhodovací orgán. Mezi povinnosti účastníků schůzek je to, že se provede report schůze do interního systému a také zápis z jednání. Každá schůzka je zaznamenána v systému na základě jeho zařazení:

- externí mítink,
- interní mítink (nemusí být posílán žádnému zákazníkovi ke schválení),
- pravidelné mítinky.

Každý mítink má několik interně definovaných pravidel, která jsou vyžadována:

- Poskytoval IT služeb i zákazník by měli být zastoupeni na schůzkách v počtu a v pozici, která umožnuje vyjednávání a učinění rozhodnutí dle komunikační matice.
- Schůzka se děli na dvě hlavní části, agenda a samotný zápis:
    - Pokud je mítink organizován společností, zasílá se jako tato část jako agenda v pozvánce.
    - Zápis musí mít jednotnou formu, která se následně sdílí pro námitky ze strany zákazníka.
- Dále schůzka obsahuje základní informace (název, datum, stav, místo), účastníky schůzky, vazby artefaktu (odkazy na jiné části v systému).

Ukázka zápisu z CAB (Obrázek 4) zobrazující témata a průběh dané schůzky. Na základě tohoto zápisu pak dochází k dalším krokům zdokumentovanými níže:



2023-05-15, 16:00-17:00, Placeholder - CAB Meeting

Přehled 1 0 Upravit

Zápis

Change advisory board

Main topic - R7.0 deployment

- Updates Schedule for project release R7.0
  - A screenshot of the plan in attached in the section below

Change requests:

- **EDPOCAB-108** - ANNA PS - R7.0 - **Approved**
  - Parallel run for 4 weeks
  - ACCE: Start date 22/05, end date 02/06
  - PROD: Start date 03/07, end date 04/07
- **EDPOCAB-113** - FILIP - R7.0 - **Approved**
  - ACCE: Start date 22/05, end date 02/06
  - PROD: Start date 03/07, end date 04/07
  - Karel to adjust the date in the comment from 03/07 to 05/07 (Customers will start upgrades)
- **EDPOCAB-106** - JINDRA - R7.0 - **Not Approved yet**
  - one CR - DIR format changes
  - security fixes - SSDLC
  - Luc will check the avalaibility with Christian and update the planning
  - Suggestion: ACCE - 25/05, PROD - 03/07
- **EDPOCAB-115** - MARTIN- R7.0 - **Approved**
  - Not compatible with previous HONZA version
  - ACCE: 17/05
  - PROD: 04/07
- **EDPOCAB-105** - HONZA - R7.0 - **Approved**
  - ACCE: Start date 22/05, end date 02/06

Obrázek 4: Zápis mítinku [Vlastní šetření]

- Po schůzce je založeno následné monitorování a implementace dohod a akcí v systému. Tím je zajištěno, že se zákazník a poskytovatel IT služeb řídí dohodnutými kroky. Součástí těchto kroků je také provádění průzkumů a zpětné vazby s cílem ověřit, zda jsou splněna očekávání zákazníka. Následné akce se lze založit nad schůzkou v systému:
  - úkol,
  - schůzka,
  - základní rozhodnutí,
  - informace,
  - upozornění,
  - milník,
  - událost,
  - vlastní rozhodnutí,
  - chat,
  - problém.

Dodržování těchto bodů má za hlavní cíl zabezpečit účinné a průhledné řízení projektu a komunikaci mezi týmem a zákazníkem. Pravidelné schůzky a záznamy důležitých informací do systému umožňují monitorovat průběh projektu, hodnotit dosažené výsledky, dělat rozhodnutí v souladu s komunikačními pravidly a implementovat dohodnuté kroky. To posiluje spolupráci mezi oběma stranami a umožňuje reagovat na potřeby a očekávání zákazníka. Ve výjimečných případech se také hodí pro zpětné dohledání rozhodnutí při sporných situacích v budoucnosti.

7 ISO recertifikace

V této kapitole bude popsána forma auditu, požadavky ISO 270001 a její hlavní kapitoly, které byly v rámci auditu připraveny a prezentovány.

7.1 Úvod do recertifikace

Recertifikace ISO představuje důležitý milník sledovaný v rámci IT projektu. Jedná se o proces, který slouží k ověření schopnosti poskytovat služby v souladu s mezinárodně uznávanými standardy a normami. Tato část diplomové práce poskytuje ucelený přehled o přístupu k recertifikaci ISO, zahrnující informace o cílech, postupech a závazku ke kvalitě a neustálému zlepšování. Recertifikace poskytuje příležitost k přezkoumání stávajících postupů a identifikaci oblastí pro další zlepšení a inovace. Úvod do této kapitoly slouží k seznámení čtenáře s obsahem a významem procesu recertifikace ISO v kontextu IT společnosti.

Samotná kapitola obsahuje podrobné informace o přípravě a průběhu ISO recertifikace v rámci zkoumané IT společnosti. Začíná kontextem organizace, který poskytuje bližší informace o samotné společnosti. Následuje kapitola o vedení, která se zaměřuje na aspekty managementu, včetně popisu rámce smluv, dlouhodobých cílů a zajištění právních požadavků. Kapitola plánování se pak soustředí na operativní prvky a zodpovědnost projektového manažera a týmových vedoucích, zejména v oblasti krátkodobého rozvoje a změn.

Následuje kapitola o podpoře, která se zaměřuje na zajištění potřebných zdrojů, komunikačních kanálů a podpory služeb poskytovaných IT projektem. Kapitola o provozu se zabývá přípravou dostatečných důkazů o řízení projektu, využívání klíčových bodů a projektových logů pro auditorské účely. Kapitola hodnocení výkonu se zaměřuje na hodnocení výkonnosti projektu. Poslední kapitola o zlepšování potvrzuje dlouhodobé zaměření projektu na zlepšování a inovace pro udržení konkurenční výhody.

Tímto úvodem do kapitoly je čtenář seznamován s obsahem a důležitostí recertifikačního procesu ISO v rámci IT společnosti.

7.2 Kontext organizace

Společnost je uznávanou evropskou firmou, která se specializuje na poskytování významných informačních systémů a IT řešení. Organizace vytvořila širokou škálu vynikajících a rozsáhlých řešení, která jsou využívána předními podniky z různých odvětví. Společnost také provozuje internetovou službu, která nabízí rozmanité portfolio služeb založených na robustních softwarových řešeních, primárně zaměřených na potřeby malých a středních podniků a samozřejmě na individuální potřeby uživatelů.

V oblasti energetiky a utilit se společnost zaměřuje na implementaci rozsáhlých informačních systémů v oblasti řízení energetických trhů na národní i mezinárodní úrovni a na související oblast energetického obchodu. Další prioritou společnosti je geoinformatika a řešení pro správu podnikových aktiv. Organizace přitom využívá jak své vlastní produkty, tak ověřené platformy svých partnerů.

Klíčovým prvek pro v rámci ISMS je rozdělení a definice kontextu organizace [29]:

- **Externí kontext**: Tento aspekt se zabývá faktory a podmínkami, které působí mimo organizaci a mohou ovlivnit ISMS. To může zahrnovat zákonné a regulační požadavky, obchodní prostředí, konkurenci a další externí zúčastněné strany.
- **Interní kontext**: Tento aspekt se zaměřuje na vnitřní prostředí organizace a faktory, které ovlivňují ISMS. Sem patří organizační struktura, cíle, politiky, procesy, firemní kultura, zdroje a další interní faktory, které mohou mít vliv na informační bezpečnost.
- **Zainteresované strany, jejich potřeby a očekávání**: Koncoví zákazníci, uživatelé, dodavatelé, obchodní partneři, konzultanti, certifikační autority.

V rámci zachování důvěrnosti, integrity a dostupnosti se základní bezpečnost soustředí na vybudování kompletního systému, a to nejen podle zkoumané části bezpečnosti dle ISO 27001. Nejdůležitější prvky bezpečnosti lze uvést následovně.

7.3 Vedení

V rámci této části kapitoly se provádí detailní popis připravených a sledovaných prvků z perspektivy projektového vedení. Tato část se zaměřuje zejména na body, které přímo navazují na komunikaci se zákazníkem a jsou v úzké interakci s ním.

Cílem je zajistit, že tyto body jsou pečlivě připraveny, sledovány a řízeny s cílem dosáhnout optimální spolupráce se zákazníkem a splnit jeho potřeby, očekávání, případně k bodům vedoucím k ještě lepší interakci se zákazníkem a dosažení vyšší úrovně spokojenosti.

7.3.1 NDA

V rámci auditu bylo kontrolováno, že projekt má jednoznačně stanovené NDA – dohodu o mlčenlivosti vůči zákazníkům. Jedná se o dohodu mezi dvěma nebo více stranami o ochraně důvěrných informací. NDA uvádí, že strany souhlasí s tím, že nebudou poskytovat, zveřejňovat ani používat důvěrné informace, které jim byly poskytnuty v rámci vztahu, jako je obchodní vztah, zaměstnání nebo vyjednávání potenciální transakce. NDA může obsahovat ustanovení týkající se povahy důvěrných informací, doby důvěrnosti, co dělat s těmito informacemi, omezení přenosu informací třetím stranám a důsledků porušení smlouvy, včetně jakýchkoli právních důsledků.

V rámci interního systému tak obsahuje artefakt informaci o tom, zda a do jaké míry podléhá informace každého artefaktu NDA.

7.3.2 Rámcové smlouvy

Zkoumaný projekt má samostatné smlouvy se zákazníkem, které musí být řádně vedeny a v rámci NDA ukládány.

Při kontrole rámcové smlouvy je smlouva přezkoumána a případně upravena tak, aby splňovala konkrétní podmínky a náležitosti konkrétního smluvního vztahu. Během kontroly tak dochází ke kontrole správného uložení, nakládání se smlouvou, právní platnost smlouvy, totožnost smluvních stran,

přesné vymezení předmětu smlouvy, důležité obchodní podmínky, rozsah smluvních povinností a odpovědnosti, ochranu důvěrných informací a sankce za případné porušení, které by měly vliv na celou společnost.

7.4 Plánování

Tato část kapitoly podrobně rozebírá operativní plánování, včetně návrhu služeb podle principů ITIL, předpokladů budoucího vývoje a procesu řízení změn v rámci CAB. Poskytuje komplexní přehled těchto klíčových prvků, které mají významný dopad na účinnost a úspěch systému řízení kvality.

Hlavním cílem této kapitoly je zdůraznit důležitost a přínos operativního plánování v rámci ISO recertifikace. Současně se zaměřuje na zajištění správného a efektivního návrhu služeb, předvídání budoucího vývoje a řízení změn s kontrolou v rámci CAB. Tímto přístupem organizace dosahuje vyšší úrovně kvality, inovace, udržitelnosti v oblasti IT služeb a procesů.

7.4.1 Návrh služeb

Design služeb v rámci ITIL [30] představuje jednu z fází životního cyklu, která se zaměřuje na plánování projektových služeb, jež jsou poskytovány organizacemi. V průběhu této fáze dochází k identifikaci a specifikaci požadavků na služby, návrhu architektury služeb, procesů a technologií a rovněž k definování dohodnutých úrovní služeb s cílem zajištění kvality a dodržování stanovených standardů. Návrh služeb zkoumá různé aspekty, včetně finančních, technických, organizačních a provozních, s cílem efektivně navrhnout služby, které splňují potřeby zákazníků a podporují strategické cíle a očekávání organizace. Tato identifikace zároveň poskytuje základ pro vytváření rámcových smluv a jednání se zákazníky.

7.4.2 Předpoklady budoucího rozvoje

V rámci přípravy na audit bylo nezbytné poskytnout předpovědi budoucích událostí a výsledků projektu. Tyto prognózy slouží k představení očekávaného vývoje projektu a předpovědi dosažených výsledků na základě dostupných

informací a analýz. Tato předpověď je založena na následujících aspektech, které jsou diskutovány v dalších částech:

- **Časový plán**: Odhady termínů dokončení stanovených milníků a klíčových cílů projektu. Tyto odhady vycházejí z předchozích zkušeností týmu a současného stavu projektu.
- **Rozpočet**: Vzhledem k tomu, že každý projekt je samostatnou entitou, je důležité předpovědět, jak se náklady budou vyvíjet v průběhu projektu a zda je nutné provést případné úpravy rozpočtu.
- **Kapacita týmu**: Informace a odhady potřebných lidských zdrojů v termínech lidských hodin, stejně jako potřebného softwaru nebo jiných prostředků.
- **Rizika a příležitosti**: Na základě očekávaných událostí a identifikovaných rizik je nutné provést prognózu, aby projekt mohl lépe plánovat a předvídat možné incidenty.

Hlavním přínosem je předkládání předpovědí budoucích událostí a výsledků, což usnadňuje lepší plánování projektu v časovém plánu, rozpočtu, potřebných zdrojích, identifikovaných rizikách a příležitostech. Tato prognóza má zásadní význam pro efektivní řízení projektu.

7.4.3 Změnové požadavky v rámci CAB

V rámci lepší dokumentaci a kontroly projektu se zavedl formát schvalování za pomocí mítinků CAB. CAB (Change Advisory Board) podle ITIL 3 je tým odborníků, který má odpovědnost za posuzování změn v IT prostředí [31]. V rámci ITIL verze 4 je upuštěno od tohoto formátu plánování, ale v rámci změn v projektu se stává novým standardem, který byl pro plánování a rozvoj nově zaveden ve spolupráci se zákazníkem. Jeho hlavním úkolem je provádět objektivní a souvislý proces posouzení změn a rozhodování o jejich implementaci. Tým CAB by měl zahrnovat zástupce z různých oblastí a funkcí IT, například správy služeb, technické podpory, vývoje, provozu a dalších relevantních oborů. [10]

CAB provádí posouzení změn na základě informací o rizicích, důsledcích, nákladech, časovém plánu a dalších faktorech, které by mohly ovlivnit úspěšnost provedení změn. Jeho cílem je zajistit transparentní a efektivní proces posuzování změn, který minimalizuje rizika a negativní vliv na IT služby. V rámci změnového požadavku v Jiře je třeba vydefinovat následující detaily:

- **Popis změny**: Podrobný popis toho, co se má změnit, včetně konkrétních komponent, systémů nebo procesů, které jsou dotčeny.
- **Priorita změny**: 3 stupně priority v souladu s řízením rizik.
- **Důvod změny**: Vysvětlení, proč je tato změna nezbytná, jaký problém nebo potřebu má řešit a jaké výhody přinese.
- **Očekávaný výsledek**: Specifikace očekávaných výsledků po provedení změny, včetně předpokládaných zlepšení výkonu, funkcionality nebo efektivity.
- **Důsledky změny z hlediska byznysu**: Identifikace možných dopadů změny na ostatní systémy, služby nebo procesy, včetně potenciálních rizik a negativních vlivů.
- **Plán změny**: Harmonogram a časový plán provedení změny, včetně navrhovaného data a času implementace.
- **Odhad nákladů**: Informace o předpokládaných nákladech na implementaci změny, včetně finančního rozpočtu a zdrojů potřebných k provedení.
- **Odhadovaný čas na implementaci**: Odhadovaný čas v člověkohodinách, který se bere jako nezávislý údaj na předchozím odhadu nákladů.
- **Odpovědné osoby**: Jmenování zodpovědných osob za provedení změny a jejich kontaktní údaje pro případné dotazy nebo další informace.
- **Rizika a zabezpečení**: Identifikace možných rizik spojených se změnou a navrhovaná opatření pro minimalizaci těchto rizik.
- **Související dokumentace**: Přiložení relevantní dokumentace nebo odkaz na současnou verzi dokumentací, jako jsou technické specifikace, testovací plány nebo další dokumenty, které podporují navrhovanou změnu.
- **Plán návratu**: Podrobný plán pro případ neúspěšné implementace navrhovaného řešení.

- **Schvalovatelé**: Identifikace osob nebo funkcí, které mají pověření k posouzení a schválení změny v rámci CAB.
- **Prostředí**: Jaké prostředí je afektované touto změnou.

Následně je tento změnový požadavek prezentován a po obhájení musí být schválen třemi hlavními manažery z oblasti bezpečnosti, komunity a kontinuálního vývoje.

7.5 Podpora

V této kapitole byly podrobně analyzovány a popsány různé aspekty týkající se komunikačních kanálů a schématu pro kontaktování zákazníka. To zahrnovalo vhodný výběr kanálů pro přenos informací, stanovení frekvence a formátu komunikace, také definici odpovědnosti za komunikaci ze strany projektu i zákazníka. Dále byla také řešena volba reportovacího nástroje pro projekt, která byla předem nastíněna v teoretické části. Všechny tyto prvky jsou klíčové pro efektivní řízení a kontrolu kvality projektu.

7.5.1 Organizační a komunikační schéma

V rámci ITIL je vydefinován organizační a komunikační diagram týkající se provozu služeb.

V kontextu ITIL se plánování organizace a komunikace zaměřuje na vytvoření jasné organizační struktury a efektivních komunikačních kanálů na podporu poskytování služeb. Zahrnuje následující klíčové prvky:

- **Role**: Definování rolí a přiřazení odpovědností jednotlivcům v týmu, aby byly jasně stanoveny jejich úkoly a oblasti zodpovědnosti.
- **Centrální kontakt**: Vytvoření centrálního bodu kontaktu, Helpdesku, který přijímá a spravuje žádosti o služby, incidenty a další dotazy od uživatelů na základě úrovně L1 podpory.
- **Eskalace**: Sestavení eskalačních postupů při řešení incidentů nebo požadavků na služby, které překračují dohodnuté časové limity stanovené v SLA.

- **Komunikační kanály**: Definování komunikačních kanálů a metod pro různé typy komunikace uvnitř IT organizace. Mezi povolené kanály patří e-mail, telefonní hovory, Jira a ServiceNow.
- **Reportování**: Vytvoření struktury pro reporting a řízení toku informací pro zachycení a sdělování relevantních dat a metrik příslušným zainteresovaným stranám. To podporuje rozhodovací proces a sledování výkonu služeb.

Dodržování těchto bodů v rámci ITIL přináší klíčový přínos v podobě zajištění efektivního a profesionálního provozu služeb prostřednictvím dobře koordinované reakce na požadavky uživatelů a rychlému řešení incidentů.

7.5.2 Volba reportovacího nástroje

Na studovaném projektu se v průběhu několika let používal nástroj Zendesk pro reportování a správu incidentů. Později však došlo k rozhodnutí přejít na platformu Jira, která nabízela širší možnosti přizpůsobení a umožňovala lepší správu incidentů a generování KPI reportů.

Nicméně vzhledem k potřebě dále zlepšovat správu změnových požadavků, incidentů a problémů byla znovu přezkoumána volba reportovacího nástroje. Proces volby nového nástroje zahrnoval setkání a následný workshop, na kterém byly diskutovány požadavky a potřeby projektu v souladu s ITIL požadavky.

Výsledkem mnoha mítinků a workshopů s experty z oblasti nástrojů došlo k rozhodnutí přejít na platformu ServiceNow, která byla vybrána jako nejvhodnější reportovací nástroj. ServiceNow nabízel rozšířené možnosti správy změnových požadavků, incidentů a problémů, které byly klíčové pro plnění požadavků ITIL a zajištění účinného řízení a sledování těchto procesů.

Tímto přechodem na platformu ServiceNow projekt získá v nejbližší době nástroj, který umožní lepší sledování, reportování a správu incidentů, změnových požadavků a problémů v souladu s ITIL metodikou. Tato volba byla založena na analýze, zhodnocení potřeb projektu a zároveň na schopnosti nástroje plnit

požadavky a standardy ITIL, které byly považovány za klíčové pro efektivní provoz a řízení projektu.

7.5.3 Rozdělení a podpora služeb L1, L2, L3

V rámci projektu je tým rozdělen do tří rolí – L1, L2 a L3, a je důležité jasně definovat přiřazení zodpovědností a řešení IT problémů a incidentů.

- **První úroveň podpory**:
  - L1 podpora je rozdělena mezi samostatný Helpdesk, který reaguje na vytvořené požadavky v Jiře, a projektový tým, který se zabývá známými a běžnými problémy.
  - Pokud problém nelze vyřešit na úrovni L1, je předán na úroveň L2.
- **Druhá úroveň podpory**:
  - L2 podpora se specializuje na správu a podporu centrálních prvků, které jsou definovány v rámcové smlouvě.
  - Zaměřuje se na složitější a technicky náročnější problémy a incidenty, které vyžadují více než pouhé použití znalostní databáze.
  - L2 má dostatek času a možnosti pro provedení detailnější diagnostiky a řešení problémů ve spolupráci s hostující entitou.
  - Pokud problém přetrvává, nebo vyžaduje větší technickou znalost, je předán na úroveň L3.
- **Třetí úroveň podpory**:
  - L3 podpora má přístup ke zdrojovému kódu a možnost provádět změny ve skriptech, které ovlivňují běh služeb.

V rámci projektu má tým specifickou roli v každé fázi, která je spojena s technickými a časovými omezeními. Pro účely auditu bylo nezbytné jasně rozdělit a definovat rámcové smlouvy a organizační matici pro každou úroveň, stejně jako dokumentaci odpovídající úrovni.

7.6 Provoz

Kapitola o provozu v rámci ISO certifikace se zaměřuje na podrobný popis každodenního plánování a řízení provozu. Hlavním nástrojem pro dosažení tohoto

cíle je projektový log, který slouží jako rámec pro sledování a dokumentaci důležitých informací. Projektový log musí neustále odpovídat definovaným bodům a požadavkům, které jsou uvedeny a popsány v klíčových vstupech a výstupech. Tato kapitola se věnuje analýze toho, jak jsou tyto parametry naplňovány v praxi. Jsou zkoumány a hodnoceny postupy a procesy související s každodenním provozem a jestli je organizace schopna zhodnotit a zdokumentovat, jakým způsobem provádí plánování a řízení provozu v souladu s požadavky normy.

7.6.1 Projektový log

V rámci auditu bylo nutné přesně prokázat, že projekt je plánován a prováděn v souladu se standardy ITIL. V ITIL se projektové logy využívají k zaznamenávání a sledování informací souvisejících s projektem. I když samotný koncept projektového logu není explicitně definován ani v ITIL 3, ani v ITIL 4, obě verze poskytují směrnice pro řízení projektů a zdůrazňují důležitost udržování projektové dokumentace.

V ITIL 3 se řízení projektů řeší ve fázi „Přechod služby“ (Service Transition), která klade důraz na správné plánování, koordinaci a kontrolu projektů. I když ITIL 3 nezmiňuje projektové logy explicitně, zdůrazňuje potřebu udržování přesné dokumentace projektu a záznamů pro efektivní doručování projektů. [31]

V ITIL 4 se řízení projektů řeší v rámci modulu „Vytvořit, Dodat a Podpořit“ (Create, Deliver, and Support), který se zaměřuje na dodávání produktů a služeb v souladu s požadavky zákazníků. Tento modul zahrnuje i správu projektů a pracovního úsilí. ITIL 4 také zdůrazňuje důležitost správné dokumentace a správy znalostí po celou dobu životního cyklu projektu. [10]

Projektové logy slouží jako nástroj pro správu a dokumentaci projektů a obsahují důležité informace o průběhu projektu, rozhodnutích, rizicích, problémech a dalších aspektech projektového řízení. Pomáhají udržovat transparentnost, poskytují dokumentaci pro následné hodnocení projektu a umožňují efektivní řízení projektových aktivit. Interní týmový reporting se

obvykle provádí nad projektovým logem a na základě těchto informací se připravují reporty pro top management nebo zákazníka.

Projektový log musí obsahovat následující informace:

- **Záznamy o rozhodnutích**: Zaznamenávají se důležitá rozhodnutí, která byla učiněna během projektu, včetně datumu, zúčastněných stran a důvodů pro přijetí daného rozhodnutí. Jedná o zaznamenání plánovaných akcí jako údržba OS systému, nasazení nové verze nebo důležitá odstávka se změnou konfigurace.
- **Záznamy o změnách**: Zaznamenávají se změny, které byly provedeny během projektu, včetně popisu změny, důvodu, rozsahu, schvalovatelů a datumů provedení. Tím se zajišťuje sledování změn a možnost návratu ke předchozímu stavu v případě potřeby nebo investigace při nenadálých problémech sahajících do minulosti.
- **Záznamy o rizicích**: Zaznamenávají se identifikovaná rizika projektu, jejich pravděpodobnost výskytu, dopad a přijatá opatření pro jejich řízení. Tyto záznamy jsou blíže popsané v oddělené kapitole.
- **Záznamy o incidentech**: Zaznamenávají se problémy, které se vyskytly během projektu, včetně popisu problému, data identifikace, příčin, dopadu a opatření k jejich řešení. Opět je tento Incident report popsán blíže v rozdílné kapitole.
- **Záznamy o komunikaci**: Zaznamenávají se důležité komunikační události, jako jsou schůzky, jednání a rozhovory s důležitými zainteresovanými stranami. Tyto záznamy slouží k dokumentaci a sledování průběhu komunikace v rámci projektu a jsou rozebrány blíže v samostatné kapitole.

Hlavním přínosem dodržování těchto bodů v projektovém logu je zajištění transparentnosti, řádné dokumentace a sledování důležitých událostí a rozhodnutí během projektu. Toto přispívá minimalizaci rizik, identifikaci problémů a zvýšení efektivity týmu.

7.6.2 Klíčové vstupy a klíčové výstupy

V rámci projektu se používají pojmy klíčové vstupy a klíčové výstupy k popisu důležitých informací, dokumentů a prvků, které jsou potřebné pro provádění procesů. Mezi definované body patří:

- **Plánování nových dodávek** systému v pravidelném cyklu včetně bezpečnostních záplat, které nemusí být součástí dlouhodobého plánu.
- **Rozšiřování týmu** odkazuje na postup, který umožňuje rozšíření nebo posílení stávajícího týmu. Členové týmu se sdílí kapacitu s dalšími týmy v rámci projektu. Tím se tým rozšíří o další členy s potřebnými dovednostmi a zkušenostmi, kteří přispějí k úspěšnému dokončení úkolu. Tito členové rozšířeného týmu se aktivně zapojují do projektových aktivit nebo úkolů po delší dobu a spolupracují s pevným jádrem zaměstnanců týmu. Tento přístup pomáhá optimalizovat práci, zvýšit efektivitu a dosáhnout lepších výsledků projektů nebo úkolů tím, že rozšiřuje schopnosti a zdroje týmu.
- **Roadmap** je strategický plán, který poskytuje přehled o hlavních cílech a milnících, které mají být dosaženy v nejbližších dvou letech za účelem dosažení určité vize. Je to dokument, který obsahuje nejen grafické zobrazení plánu, ale také seznam s důležitými informacemi. Roadmap slouží k určení směru a priorit projektu, a poskytuje jasný rámec pro dosažení stanovených cílů.

Klíčové výstupy jsou výsledky nebo produkty, které vznikají po dokončení procesu. Tyto výstupy představují cíle nebo výsledky procesních aktivit. V rámci projektu byly sledovány tyto hlavní definované výstupy:

- **Organizační a komunikační schéma**: Auditorem se provádí kontrola, zda jsou organizační struktury a komunikační kanály jasně definované. Podrobnější informace jsou popsány v samostatné kapitole.
- **Zákaznická dokumentace**: S cílem zajistit transparentnost a sdílení informací je dokumentace dostupná jak pro zákazníka, tak

pro poskytovatele služeb. Tato dokumentace zahrnuje následující klíčové prvky:

  - komunikační standardy,
  - dokumentace prostředí,
  - standardní postupy pro poskytování služeb,
  - znalostní databáze (nový prvek, který bude rozšířen).

- **Úspěšně dokončené úkoly**: Cíle a milníky, které byly splněny v rámci „Roadmap“, jsou zařazeny do této kategorie spolu s případnými získanými zkušenostmi.

Představené prvky jsou klíčové pro úspěšnou a transparentní komunikaci se zákazníkem, včetně zpětného hodnocení úspěchů projektu.

7.7 Hodnocení výkonosti

V této kapitole dochází k podrobnému rozboru fungování reportování na projektu z interního i externího pohledu. Důraz je kladen na popis současného stavu reportování a jeho analýzu, která zahrnuje interní reportování v rámci projektového týmu a externí reportování směrem k zákazníkům a dalším zainteresovaným stranám.

Dále je v této kapitole představena problematika volby nového monitorovacího nástroje, který byl vybrán na základě komunikace se zákazníkem a potřeb inovací. Důležitým kritériem bylo zohlednění požadavků zákazníka, který byl předmětem inovací a také schopnost nástroje plnit požadavky reportování v souladu s cíli projektu.

7.7.1 Report

Během auditu bylo prověřováno, jak je projekt reportován. Projektový report je rozdělen na dvě části – interní a externí.

Interní report slouží pro lepší hodnocení a kontrolu projektu a byl zaveden pravidelný týdenní report mezi řídícím pracovníkem (Project Manager)

a odpovědnou osobou za provádění běžných úkolů (Team Leader). Pro zajištění dostatečné kontroly je nutné, aby na interním setkání byly zkontrolovány a oznámeny následující body:

- **Počet tiketů**: Aktuální počet a stav otevřených tiketů v Jira portálu je sledován. Zohledňuje se typ požadavku (servisní požadavek, přístupový požadavek, incident) a kontroluje se dodržování dohodnuté úrovně služby (SLA) a průběh vyšetřování.
- **TMS**: Hodnocení stavu projektu se provádí na základě zaznamenaných hodin práce, které musí odpovídat skutečnému odvedenému úsilí a musí být v souladu s předpovídaným rozvrhem projektu.
- **Risk**: Pravidelně se provádí kontrola seznamu rizik a znovu hodnotí se aktivní rizika a hrozby.
- **Incidenty**: Provádí se retrospektivní vyhodnocení incidentů a problémů s důrazem na získané poznatky a učení se z nich.
- **Budoucí akce**: Projednávají se plánované budoucí akce a diskutuje se o nich v rámci projektového logu.
- **Shrnutí projektu**: Souhrn aktuálních sub-projektů zahrnující informace o jejich postupu, klíčových milnících, rozpočtu a plánu do dalších měsíců. Toto shrnutí může také zahrnovat nové projekty, které byly spuštěny během příslušného měsíce.

Interní reportování vůči top managementu pak musí zahrnovat následující body a aktivity v rámci zhodnoceni týdenního statusu:

- **Balancování hodin** v projektu zahrnuje řízení a optimalizaci práce nebo pracovní doby alokované mezi členy projektového týmu za účelem efektivního využití pracovního potenciálu a dosažení stanovených cílů projektu. Při balancování hodin se sleduje a spravuje množství času, které jednotliví členové týmu věnují různým úkolům a činnostem v rámci projektu. To může zahrnovat plánování a přidělování práce, přerozdělování zdrojů a časových omezení, aby byly splněny požadavky projektu při zachování rovnováhy mezi pracovní zátěží a dostupnými zdroji. Cílem

vyvažování času je maximalizovat produktivitu, minimalizovat přetížení jednotlivých členů týmu a zajistit dodržení harmonogramu projektu.

- Aplikace interní **metodiky pro řízení projektů**: Vyplňování tabulky, která se řídí osvědčenými parametry založenými na šesti omezeních – nákladech, riziku, přínosech, kvalitě, rozsahu a času. Ke každému kritériu je přiřazen odpovídající stav (V pořádku, Upozornění, Problém). Tímto způsobem lze snadno kontrolovat stav projektu na základě těchto kritérií.
- **Milník**: Vyplnění nejbližšího data, ve kterém má proběhnout důležitá, předem naplánovaná akce. Na základě tohoto milníku lze potom lépe plánovat a přidělovat zdroje.
- **Shrnutí aktuálního týdne**: Shrnutí stavu z posledního interního týmového setkání pro rychlý přehled.
- **Finanční informace**: Informace o finančním stavu projektu a rozpočtu, včetně nákladů na hardware, software, licencování, služby třetích stran atd.

Externí měsíční report je pravidelný dokument shrnující klíčové události, aktivity a výsledky za předchozí měsíc. Zpráva se obvykle připravuje v rámci IT oddělení nebo organizace, aby poskytla přehled o stavu a vývoji IT infrastruktury, projektů, bezpečnosti, uživatelské podpory a dalších důležitých oblastí. Účelem je poskytnout managementu a dalším zainteresovaným stranám přehled o činnosti a výsledcích IT oddělení tak, aby mohli sledovat vývoj, identifikovat problémy, přijímat strategická rozhodnutí a plánovat budoucí akce, které se poté implementují, např. v rámci CAB mítinku.

Externí měsíční report musí obsahovat následující základní prvky, které jsou požadovány jak při interní politikou, tak také zákazníkem:

- **Incidenty**: Kapitola obsahující počet incidentů, kolik jich je nově otevřených oproti počtu zavřených a také kolik z nich se týká bezpečnostních problémů. Následuje rozdělení incidentů na základě priority, komponenty, první odezvy a času vyřešení.

- **Problémy**: V návaznosti na každý Incident je vytvořená návaznost v podobě Problému. Problémy obsahují určitý počet Incidentů a musí mít před zavřením systémové trvalé řešení, nikoliv pouze dočasné.
- **Servisní požadavky**: Standardní požadavky od zákazníků na zlepšení služeb či prověření dotazu.
- **Dostupnost**: Pro každý server nebo službu musí existovat jednoznačně změřitelné metriky, report pak obsahuje:
    - Doba provozu: Měří, kolik času byla služba nebo systém v provozu. Obvykle se vyjadřuje jako procento času, minimální úroveň je stanovena v rámci SLA projektu.
    - Doba výpadku: Měří, kolik času byla služba nebo systém nedostupná.
    - Průměrná doba obnovení služby: Měří průměrný čas, který je potřeba k obnovení služby nebo systému po incidentu. Udává se obvykle v minutách.
    - Výpadky a incidenty: Měří se počet výpadků nebo incidentů, které se vyskytly během určitého časového období. Tyto informace poskytují přehled o stabilitě a spolehlivosti služeb.
- **Incident porušující SLA**: Incidenty, které narušují SLA, se vyskytují, když nedochází k dodržování nebo porušování dohodnutých úrovní služby (Service Level Agreements – SLA) mezi poskytovatelem a uživatelem. Pokud dojde, byť jen k jedinému Incidentu v této kategorii, je následně jedním z témat pravidelných mítinků se zákazníkem.

Kapitola o měsíčním externím reportu je klíčová pro sledování výkonnosti a poskytuje komplexní přehled o incidentech, problémech, servisních požadavcích a dostupnosti služeb, což umožňuje pravidelnou komunikaci se zákazníky a zajistí dodržování dohodnutých úrovní služby (SLA).

7.7.2 Volba monitorovacího nástroje

V souladu s požadavky zákazníka na neustálé zlepšování a dodržování podmínek SLA je nutné vybrat vhodný monitorovací nástroj pro účinnější sledování zhruba 30 komponent. V této fázi není zvažováno nasazení

kontejnerizace, například pomocí platformy Docker s využitím správy za pomocí Kubernetes. Zároveň probíhá výběr monitorovacího nástroje pro celé prostředí, což zahrnuje následující komponenty uvedené v seznamu níže:

- **Aplikace** (několik aplikací v rámci této skupiny)
  - hardwarové prostředky,
  - kontroly aplikací,
  - kontroly JMX/ActiveMQ (fronty).
- **Webový server**
  - hardwarové prostředky,
  - HTTP web a služby IIS.
- **Databázový server**
  - hardwarové prostředky,
  - služba MySQL.
- **AMQP proxy** (prostředník pro Advanced Message Queuing Protocol)
  - hardwarové prostředky,
  - služba NGINX.
- **HTTPs proxy** (šifrovaný prostředník pro protokol HTTP)
  - hardwarové prostředky,
  - služba NGINX.
- **Socks forwarder** (prostředník pro protokol SOCKS)
  - hardwarové prostředky,
  - služba Dante.
- **Server pro monitorování**
  - hardwarové prostředky,
  - webová služba.

V současné době je monitorovací server Nagios provozován již nějakou dobu. Nicméně, kvůli potřebě inovací a novému prostředí je nezbytné znovu posoudit vhodný monitorovací nástroj. V rámci finálního výběru jsou zvažovány tři monitorovací systémy:

1. **Nagios** – stávající monitorovací systém pro projekt.

2. **Zabbix** – běžné monitorování pro ostatní projekty hostované společností.
3. **Prometheus + Grafana + Elasticsearch** – monitorovací systém, který se používá pro nové projekty, které běží převážně v kontejnerech, dostupnost konfigurací a dashboardů z ostatních projektů společnosti.

Při srovnávání monitorovacích systémů jsou zahrnuty tyto aspekty definované zákazníkem:

- kompatibilita se všemi komponentami,
- funkčnost s vlastními Python skripty,
- hardwarové požadavky,
- složitost instalace,
- typ licence,
- pozitiva a negativa daného řešení.

Pro srovnání monitorovacích nástrojů s uvedením více kritérií existuje několik typů srovnávacích analýz. Mezi ně patří:

- Analýza vícekriteriálního rozhodování (MCDA): Tento analytický přístup nám umožňuje zhodnotit a porovnat nástroje na základě různých kritérií a vážit jejich relativní důležitost. MCDA je ideální pro vyhodnocení komplexních situací s více možnostmi.
- Analýza nákladů a přínosů (CBA) nebo Analýza nákladové efektivity (CEA): CBA je metoda, která slouží k porovnání nákladů a přínosů. Cílem je určit, zda jsou přínosy dané volby nebo investice vyšší než náklady a zjistit, kolik stojí dosažení daného výsledku.

Nicméně v tomto případě došlo pouze k rozhodnutí na základě základního popisu a jednoduché prezentace pro zákazníka. Následně proběhla diskuse na schůzce a rozhodnutí bylo učiněno na základě pocitu a individuálních preferencí. V tomto případě nebyla uplatněna žádná z výše zmíněných analýz, které se nabízely.

Pro větší přehlednost jsou základní vlastnosti uvedeny v jednoduché srovnávací analýze (bez pozitiv a negativ) ve formě tabulky (Tabulka 2).

NÁZEV	OS	PYTHON	HW	SPRÁVA	LICENCE
NAGIOS	Linux, Windows	Ano, složitější	Nízká náročnost	Jednoduchá správa	Open-source
ZABBIX	Linuxu, Windows a další	Ano	Střední náročnost	Složitější instalace	Open-source
PROMETHEUS	Kontejnerizované prostředí, různé systémy	Ano, dodatečné nástroje	Vysoká náročnost	Náročná správa	Open-source a dodatečné licence

Tabulka 2: Srovnání monitorovacích nástrojů

1. **Nagios**:

    - **Kompatibilita**: Nagios je kompatibilní s různými operačními systémy, včetně Linuxu a Windows.
    - **Funkčnost s Python skripty**: Nagios umožňuje použití Python skriptů pro vlastní monitorovací úlohy, i když jeho implementace může být složitější.
    - **Hardwarové požadavky**: Nagios je známý pro svou nízkou spotřebu zdrojů, což je výhodné zejména z finančního pohledu a pro komunikaci s hostingem.
    - **Složitost instalace**: Nagios má poměrně jednoduchou instalaci a konfiguraci, která je navíc dobře zdokumentována v rámci projektu.
    - **Typ licence**: Nagios je dostupný jako open-source nástroj s licencí GPL.
    - **Pozitiva**: Spolehlivý a jednoduchý nástroj pro základní monitorování.

- **Negativa**: V náročnějších prostředích může být omezený a nevyhovující. Jeho grafické rozhraní je zastaralé a může být obtížněji orientovat se v něm.

2. **Zabbix**

- **Kompatibilita**: Zabbix je kompatibilní s různými operačními systémy, včetně Linuxu, Windows a dalších.
- **Funkčnost s Python skripty**: Zabbix podporuje použití Python skriptů pro pokročilé monitorovací úlohy.
- **Hardwarové požadavky**: Pro provoz Zabbixu jsou vyžadovány vyšší zdroje než u Nagiosu, zejména při velkém množství monitorovaných zařízení. Pro potřeby projektu se však nejedná o patrný rozdíl.
- **Složitost instalace**: Instalace Zabbixu vyžaduje více konfigurace a nastavení než Nagios.
- **Typ licence**: Zabbix je také dostupný jako open-source nástroj s licencí GPL.
- **Pozitiva**: Nabízí rozsáhlé funkce a možnosti přizpůsobení, vhodný pro středně až vysoko náročné monitorování. Toto je velkým pozitivem zejména díky možnostem spolupráce s dalšími projekty.
- **Negativa**: Vyžaduje více zdrojů a úsilí pro nasazení a správu. Avšak nabízí využití šablon z ostatních projektů, což může snížit náročnost implementace.

3. **Prometheus + Grafana + Elasticsearch**

- **Kompatibilita**: Systém Prometheus + Grafana + Elasticsearch je navržen pro použití v kontejnerizovaných prostředích a je kompatibilní s různými operačními systémy. Pro projektové účely však stále není kontejnerizace plně plánovaná.
- **Funkčnost s Python skripty**: Při kombinaci s dalšími nástroji je možné používat Python skripty.

- **Hardwarové požadavky**: Implementace tohoto systému vyžaduje značné zdroje, zejména kvůli použití Elasticsearch pro ukládání dat. Nicméně lze redukovat na základě vhodně zvolených retencí.
- **Složitost instalace**: Implementace tohoto systému je náročnější a vyžaduje konfiguraci a integraci několika nástrojů. Odhad potřebných hodin pro implementaci může být nadměrný pro schválení.
- **Typ licence**: Prometheus a Grafana jsou open-source s licencí Apache, Elasticsearch má různé licence, včetně open-source licencí. Záleží na potřebě konzultace s nabídkou dodatečných vlastností.
- **Pozitiva**: Nabízí pokročilé funkce a analýzu dat, vhodné pro náročná a rozsáhlá prostředí.
- **Negativa**: V náročnějších prostředích může být omezený a nevyhovující. Jeho grafické rozhraní je zastaralé a může být obtížněji orientovat se v něm.

Z výše uvedeného rozboru je patrné, že každý monitorovací systém má své vlastnosti a omezení. Nagios se považuje za spolehlivý a jednoduchý nástroj, který nevyžaduje velké množství zdrojů. Avšak v náročnějším prostředí nemusí být dostatečný. Zabbix poskytuje rozsáhlé funkce a možnosti přizpůsobení, avšak jeho nasazení vyžaduje více zdrojů a úsilí. Na druhé straně, systém Prometheus + Grafana + Elasticsearch je navržen pro použití v kontejnerizovaných prostředích a nabízí pokročilé funkce. Nicméně jeho implementace vyžaduje značné zdroje a úsilí, a proto je spíše vhodný pro prostředí založená na cloudu.

Po důkladném zhodnocení všech monitorovacích systémů byl vybrán Zabbix jako nejlepší volba. Zabbix nabízí širokou škálu pokročilých funkcí a zároveň umožňuje přizpůsobení podle specifických potřeb projektu. I když vyžaduje více zdrojů a úsilí při nastavení ve srovnání s Nagiosem, jeho vyspělé funkce převažují nad tímto případným nedostatkem. Zabbix disponuje robustním a flexibilním prostředím pro monitorování a je schopen se přizpůsobit i složitějším

prostředím. Tímto je zajištěna jeho spolehlivost a schopnost efektivně monitorovat a spravovat různé komponenty.

Dalším klíčovým faktorem, který přispěl k výběru Zabbixu, je jeho schopnost plnit funkční požadavky projektu a být kompatibilní s různými komponenty. I když Zabbix vyžaduje určité množství zdrojů a úsilí při instalaci a konfiguraci, jeho výhody a možnosti převyšují tyto nároky. Zabbix je schopen poskytnout spolehlivý a výkonný monitorovací systém pro zákazníka s širokými možnostmi přizpůsobení a kompatibilitou s různými komponenty. Tímto se zajišťuje účinné sledování a správa projektu, a tedy vyšší úroveň kvality a stabilita.

7.8 Zlepšování

Tato poslední kapitola se zaměřuje na proces zlepšování definovaný ISO certifikací. Tento proces zahrnuje implementaci neustálého zlepšování, průběh samotného auditu a nastínění nového portálu. V rámci týmu bylo rozhodnuto, že projekt bude pro ISO audity certifikován pomocí nového portálu, který bude podrobněji popsán v následujících kapitolách.

7.8.1 Zavedení procesu neustálého zlepšování

Proces neustálého zlepšování stanovuje, jak provádět významné změny s cílem předejít opakování nesouladů. Na základě dlouholetých zkušeností v rámci společnosti z mnoha různých projektů jsou v současné době implementovány následující činnosti:

- Zavedení znalostní databáze.
- Definování cílů na nejbližší dva roky v souladu schopností dodávek vývojových týmů.
- Vyhodnocení KPI reportů.
- Identifikace risků a příležitostí. Na základě risk listu dochází k pravidelným fyzickým schůzkám, kde se tyto příležitosti diskutují a následně předkládají finančnímu oddělení pro kalkulaci.
- Implementace změn a drobných změnových požadavků v souladu s ITIL postupy a metodologiemi.

- Pravidelné kontrolní dny se zákazníkem v podobě mítinků.
- Školení v rámci interního výukového systému.

V rámci bezpečnosti a uvědomění si jsou povinné následující kurzy:

- základy informační bezpečnosti,
- GDPR kurz,
- bezpečnost a ochrana zdraví při práci a požární ochrana.

Kapitola o neustálém zlepšování představuje klíčové prvky, které umožňují dosahovat lepšího rozvoje projektu a bezpečného pracovního prostředí.

7.8.2 Zavedení interního auditního procesu

Po dokončení plánu a zpracování bodů, které byly podrobně diskutovány v předchozích kapitolách, je realizován proces interního auditu. Tento proces představuje klíčový krok v rámci celého projektu, zaměřený na posouzení a vyhodnocení stavu a souladu s definovanými standardy, postupy a požadavky. Jedná se také o primární část této diplomové práce a jehož výsledek je závislý na provedení a úspěšné implementaci předchozích bodů.

Implementace procesu interního auditu je nezbytná pro důkladné monitorování a hodnocení kvality a efektivity prováděných činností. Tímto způsobem je možné identifikovat potenciální nedostatky, slabiny a příležitosti ke zlepšení, které by mohly mít vliv na výkonnost projektu a dosažení stanovených cílů. Samotný proces interního auditu zahrnuje systematickou kontrolu procesů, postupů, dokumentace a implementovaných opatření. Auditoři provádějí vyhodnocování, porovnávání s předepsanými normami a standardy a posuzování souladu, účinnosti prováděných činností. Informace a zjištění získané během auditu jsou pečlivě dokumentovány a analyzovány, což umožňuje přijetí vhodných opatření a zlepšení celkové výkonnosti projektu.

Během provedeného auditu byly pečlivě posouzeny a prověřeny klíčové prvky projektu. Jednotlivé prvky jsou podrobně popsány v samostatných kapitolách praktické části práce. Hlavní důraz auditorů byl primárně kladen

na vybraných následujících deset bodů, seřazených dle důležitosti a délky jejich kontroly:

- **Projektový log**, jakožto hlavní nástroj pro transparentní sledování průběhu projektu.
- **Klíčové vstupy a klíčové výstupy**, které ukazují a zajišťují, že projekt má potřebné informace a zdroje pro implementaci a servis projektu.
- **Rámcové smlouvy** mezi organizací a zákazníkem, které stanovují základní rámec pro dohody a povinnosti pro poskytování služeb.
- **Reporty** ve strukturované formě, které obsahuje informace nebo výsledky pro pravidelné monitorování průběhu projektu, poskytování relevantních informací účastníkům projektu a managementu.
- **Zavedení evidence incidentů a korektivních opatření**, zajišťující zaznamenávání a řízení bezpečnostních incidentů, následných opravných opatření pro ochranu informačních aktiv. Zavedení procesu řízení incidentů pro rychlé a efektivní řešení incidentů a obnovení služeb v rámci definovaných SLA.
- Reportování **nesouladů a korektivních opatření** týmu pro přezkoumání řízení pro vhodná opatření k odstranění zjištěných nedostatků.
- Nový **projektový portál**, který musí obsahovat nezbytné prvky dle standardu a mít je viditelné pro každého člena organizace na základě jeho role.
- **Organizační a komunikační schéma** obsahující definované role jak týmu a organizace, tak zákazníka, aby komunikace probíhala účinně a bez časových zpoždění.
- **Předpoklady budoucího rozvoje** pro dlouhodobé plánování projektů z hlediska zdrojů finančních i časových a proaktivní reakce na očekávané změny projektu.

Během auditu nebyl zjištěn žádný zásadní problém, spíše byl definován bod vyžadující zlepšení. Tím bodem je potřeba vylepšit seznam rizik a začlenit jej do naší znalostní databáze. Jak bylo uvedeno v kapitole „Zavedení evidence incidentů a korektivních opatření“, projekt pracuje s vytvořeným risk listem v podobě tabulky, která obsahuje risky zapříčiňující incident nebo způsobující jinou hrozbu. Tento prvek však dle auditu není dostatečně automatizovaný, a kromě častější kontroly je třeba ho také rozšířit o více podrobný risk list. V současné době obsahuje list pouze identifikaci, dopad, popis a řešení.

Pro zlepšení byly doporučeny následující body:

- **Komplexnější identifikace rizik** by měla zahrnovat širší spektrum potenciálních rizik, včetně technických i obchodních, které by měly být popsány v širším měřítku.
- **Prioritizace rizik** umožňující na základě hodnocení a pořadí pomoci určit vážnost rizik, která by měla být řešena co nejdříve.
- Každé riziko by mělo být přiřazeno **odpovědnému týmu** nebo i specifické osobě, která bude za toto riziko zodpovědná.
- **Automatizované nástroje** pro správu rizik mohou zjednodušit proces kontroly a sledování pokroku v řešení.
- **Pravidelná aktualizace** pomůže organizaci se lépe chránit před riziky a potenciálními hrozbami.

Při vyhodnocení doporučení bylo uznáno, že prioritizace a přiřazení zodpovědnosti jsou klíčovými body, které lze implementovat relativně snadno a bez velkých nároků na čas a finance. Tyto kroky nejsou rozhodovány pouze projektovým týmem, ale jsou výsledkem spolupráce se zákazníky, kteří jsou přímo ovlivněni danými rozhodnutími.

Z doporučených rizik byla prvním prvkem, na který se zaměřila pozornost, implementace automatizovaných nástrojů. Moderní nástroje pro správu rizik poskytují užitečné a přehledné informace pro řízení rizik. Pro zlepšení této oblasti bude organizace dodržovat standardy a implementovat bezpečnostní nástroje pro

statickou analýzu kódu, které jsou schopny identifikovat podezřelou nebo nebezpečnou aktivitu a pomáhají tak předejít kybernetickým útokům. Díky automatizaci se minimalizuje lidská chyba a úsilí, což přináší výhody pro organizaci. Následné výsledky automatizovaných skenů však vyžadují manuální vyhodnocení ze strany servisních pracovníků.

Je důležité si uvědomit, že každý bod má své místo a přispívá k celkové bezpečnosti projektu. Jejich správná implementace a spolupráce se zákazníky jsou klíčové pro úspěšné řízení rizik a zajištění bezpečnosti informací a infrastruktury.

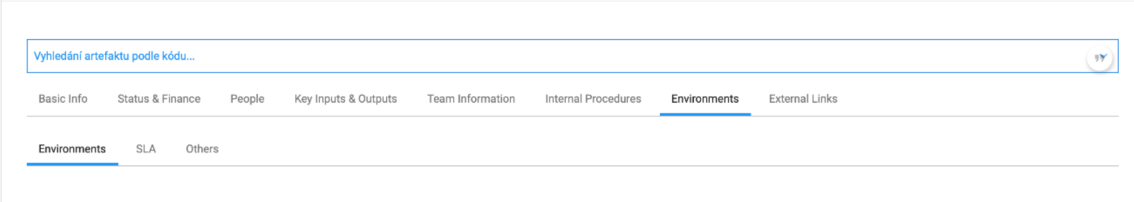
7.8.3 Nový projektový portál

Během přípravy na interní audit ISO probíhá rozhodovací proces o výběru mezi dvěma možnostmi. První možností je provést audit stávajícího, ale staršího projektového portálu, který je stále plně funkční. Druhou možností je přepracovat projekt a přenést jej na nový portál.

Rozhodnutí vyžadovalo pečlivé zvážení a srovnání pro a proti obou možností. Audit využívající stávající portál měl za sebou již zavedené procesy a fungující strukturu. To usnadňuje samotný proces kontroly a minimalizuje nejistotu spojenou s přechodem na nový portál. Na druhou stranu má stávající portál omezené funkce a nemůže se plně přizpůsobit novým požadavkům a standardům certifikace ISO.

Místo toho přepracování projektu jako nového portálu nabízí možnost využít moderní a přizpůsobitelné prostředí, které lépe odpovídá potřebám certifikace ISO a organizace. Nový portál by mohl poskytnout vylepšené funkce a nástroje pro řízení a monitorování projektů, což by mohlo být přínosem pro audit a zajištění souladu s normami ISO. Přepracování projektů a migrace na nový portál však vyžaduje čas a zdroje. I přes to, že čas byl omezený, díky důkladnému naplánování, bylo možné využit velké množství hodin pracovníků týmů pro migraci.

Nakonec tedy došlo k rozhodnutí přepracovat a přenést celý projektový portál, který slouží jako systémový nástroj pro správu a sdílení informací o bezpečnosti aktiv a financí. Pro přehlednost bylo zvoleno a vytvořeno několik klíčových bodů obsahující dodatečné pod body. Toto rozvržení je znázorněno v obrázku níže (Obrázek 5).



Obrázek 5: Náhled projektového portálu [Vlastní šetření]

Krom výše zmíněných důvodů existovalo několik důvodů, které vedly k rozhodnutí předělat tento portál a zlepšit jeho funkčnost:

- **Narůstající objem informací**: V průběhu několika let se objem informací v informačním systému postupně zvětšoval. To mělo za následek, že informace o jednotlivých prvcích projektu se staly obtížně dohledatelné. Bylo nutné přehodnotit a přepracovat strukturu portálu, aby bylo možné efektivněji organizovat a vyhledávat informace.
- **Nedostatečně udržovaná znalostní databáze**: Existující databáze přestala být správně udržovaná. Její struktura byla roztříštěná mezi různými artefakty a noví členové týmu měli problém úspěšně vyhledat potřebné informace. Bylo třeba vytvořit novou strukturu a zajistit její správné udržování, aby se zlepšila dostupnost a sdílení informací.
- **Sdílení informací a přístupová práva**: Zákazník měl specifické požadavky na sdílení informací týkajících se jejich vlastního prostředí. Starý informační systém nedokázal jednoduše splnit tyto požadavky kvůli omezeným možnostem rozdělení přístupových práv. Bylo nezbytné přepracovat systém tak, aby bylo možné snadno nastavit a spravovat přístupová práva pro jednotlivé uživatele a zabezpečit tak sdílení informací v souladu s požadavky zákazníka.

- **Centrální ukládání informací pro top management**: Byla zde snaha o snížení nutnosti udržovat informace pro top management na různých místech. Cílem bylo vytvořit jeden centralizovaný artefakt, ve kterém by bylo možné uchovávat všechny důležité informace a udělovat přístupová práva k nim v souladu s bezpečnostními požadavky. Tím by se zjednodušilo a zefektivnilo řízení a přístup k důležitým informacím.
- **Kontrola financí**: Jedním z důvodů pro přepracování portálu bylo usnadnění kontroly financí. Bylo třeba vytvořit přehlednější formát, který by umožnil lepší sledování a správu finančních aspektů projektu.

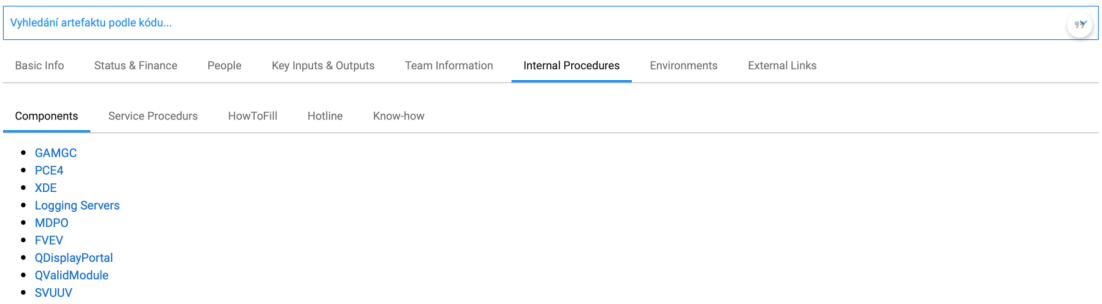
Zavedení nového systémového portálu, který zohledňuje výše uvedené důvody, mělo za cíl zlepšit bezpečnost aktiv a správu financí v rámci projektu. Tím by se zajistila lepší organizace informací, efektivnější sdílení, přehlednost a transparentnost, což přispělo k úspěšnému průběhu projektu a splnění stanovených cílů. Z pohledu projektu byl nejbližší cíl prezentace změn projektu na novém portálu.

Při vytváření nového projektového portálu bylo nejprve nutné rozhodnout, jak logicky a graficky rozčlenit všechna témata tak, aby bylo možné rychle a úspěšně nalézt požadované informace. Při zpracovávání portálu se mohly uplatnit různé přístupy při zachování pravidel z hlediska ITIL a ISMS:

- **Kompletní výpis informací**: Jeden z přístupů byl zahrnout všechny potřebné informace, tabulky a další prvky přímo na vybranou stránku projektového portálu. Tím by odpadla nutnost přepínat mezi různými artefakty a všechny relevantní informace by byly soustředěné na jednom místě. Tento přístup by měl za výhodu přehlednost a snadnou dostupnost veškerých informací. Nicméně, nevýhodou by byla možná obsáhlost každé stránky, která by mohla ztěžovat rychlé vyhledávání specifických informací.
- **Odkazy na artefakty**: Dalším přístupem bylo vypsat pouze nadpisy, které by sloužily jako odkazy na konkrétní artefakty, jež by obsahovaly veškeré informace. Tím by se snížila obsáhlost jednotlivých stránek projektového portálu a zvýšila se přehlednost při prvotním vyhledávání.

Uživatelé by přes nadpisy mohli snadno navigovat na stránky s detailními informacemi, pokud by je potřebovali.

Na základě zvažování bylo rozhodnuto, že přístup s minimalizací obsahu a udržováním přehlednosti na projektovém portálu je primárním cílem. Proto byla upřednostněna druhá možnost, tj. použití nadpisů sloužících jako odkazy na artefakty s konkrétními informacemi. Tím by se dosáhlo snadného vyhledávání a přehledné prezentace informací na portálu, jak je znázorněno na obrázku níže (Obrázek 6). Ve zobrazené sekci „Components“ jsou uvedeny odkazy na všechny aplikace spravované na projektu. Následné otevření jednotlivých komponent teprve zobrazí kompletní obsah a popis aplikací, namísto uvedení všech relevantních informací přímo na této stránce.



Obrázek 6: Volba struktury informací na informačním portálu [Vlastní šetření]

7.9 Rozdělení pravomocí

ITIL sice neuvádí explicitně konkrétní role nebo přístupová práva pro projektový portál, ale poskytuje obecné směrnice a osvědčené postupy pro řízení IT služeb a informační bezpečnosti, které mohou sloužit jako základ definic rolí a přístupových práv v rámci projektového portálu.

Na základě těchto rámců je možné zvážit následující aspekty při definování rolí a přístupových práv v projektovém portálu:

- **Odpovědné osoby**: Osoby zodpovědné za projekt mohou mít vyšší úroveň přístupových práv, která jim umožní zobrazovat a upravovat veškeré informace související s projektem. Měly by mít pravomoc činit klíčová

rozhodnutí, schvalovat změny a přidělovat zdroje. Tato role je často obsazována členy top managementu a kontrolními složkami v systému. Pro projekt není tato role využívána.

- **Projektoví manažeři a vedoucí týmu**: Tito členové týmu mají přístupová práva, která jim umožňují dohlížet a řídit průběh projektu. Měli by mít možnost přidělovat úkoly, sledovat činnosti a monitorovat milníky. Jejich přístup se často týká projektových plánů, harmonogramů a přidělování zdrojů. V rámci projektového portálu by tedy měli mít zvýhodněný přístup k těmto informacím. Ve výsledku má tuto roli pouze jedna osoba a neliší se tolik od nejvyššího oprávnění.
- **Operativci**: Tito členové týmu mají přístupová práva, která jsou specifická pro jejich přidělené úkoly a odpovědnosti v rámci projektu. Měli by mít možnost přístupu k projektovým dokumentům, přispívat do diskusí a aktualizovat informace týkající se jejich úkolů. Přístup k finančním informacím není potřebný. V týmu je tato role přidělená zástupci projektového managera pro správu úkolů, milníků a dalších klíčových nefinančních prvků.
- **Účetní**: Účetní nebo finanční pracovníci mají přístupová práva k finančním datům a reportům v rámci projektového portálu. Jsou zodpovědní za sledování nákladů projektu, rozpočtování a generování finančních reportů.
- **Projektový tým**: Členové projektového týmu z různých oddělení mají přístupová práva odpovídající jejich rolím a odpovědnostem v rámci projektu. Mají přístup k relevantním projektovým dokumentům.
- **Audit**: Auditní pracovníci, interní nebo externí, mohou mít omezený přístup k prohlížení dokumentace projektu, procesů a kontrol. Jejich přístupová práva se zaměřují na specifické oblasti týkající se dodržování předpisů, řízení rizik nebo zajištění kvality.
- **Hosté**: Externí zúčastněné strany, které nejsou přímo zapojeny do projektu, mohou mít omezený přístup k určitým informacím nebo reportům relevantním pro jejich zapojení nebo zájem.

Definování jasných rolí a přístupových práv pomáhá zajistit vhodnou ochranu dat, důvěrnost a zodpovědnost v prostředí projektu.

8 Shrnutí výsledků

Cílem této práce bylo provést analýzu požadavků a podrobně popsat přípravu a průběh interního ISO auditu s důrazem na dodržování metodiky ITIL. Významnou součástí tohoto auditu byl také přechod na nový informační portál, který představoval výzvu pro splnění všech požadavků. Autor této práce se aktivně podílel na měsíční přípravě, která začala teoretickým studiem odborné literatury a následně byla doplněna pohovorem s auditory, kteří představili hlavní požadavky.

Otázka 1: Jaké jsou hlavní požadavky auditora ISO 27001 na přípravu projektu a projektového portálu v organizaci?

Hlavním požadavkem auditorského týmu bylo nejprve prokázat, že projekt řádně dokumentuje veškerou komunikaci se zákazníkem a top managementem. To vyžadovalo přípravu projektového logu pro zaznamenávání milníků, systematické zaznamenávání průběhu schůzek a pravidelné reportování projektu jak v rámci týmu, tak směrem k top managementu. Důležitým poznatkem z této části byla nutnost vhodného vedení dokumentace a zaznamenávání všech aktivit, které ovlivňují projekt.

Z hlediska projektového managementu byl kladen důraz na správné a aktuální vedení rámcových smluv se zákazníkem a dodržování dohodnutých NDA (Nondisclosure Agreement) v rámci týmu. Vzhledem ke kritické povaze oblasti, ve které projekt působil – energetika, byly tyto body zvláště důležité a jejich dodržování bylo nezbytné.

Otázka 2: Jak je úroveň souladu přípravy projektu a projektového portálu s metodikou ITIL a požadavky auditora ISO 27001?

Během provedeného auditu bylo provedeno podrobné hodnocení a kontrola všech dalších klíčových prvků projektu. Tato kontrola se zaměřovala na plánování, podporu, provoz, hodnocení výkonu a zlepšování. Každý z těchto prvků je důkladně popsán v jednotlivých kapitolách této práce, spolu s praktickým

způsobem jejich implementace. Tímto způsobem je poskytnut podrobný přehled o tom, jak tyto prvky fungují v reálném prostředí projektu. Hlavní důraz byl kladen na praktické a konkrétní aspekty projektového řízení, místo abstraktních teoretických pokynů. Auditorský tým se zaměřoval na efektivní provádění a dodržování postupů a pravidel týkajících se řízení projektu, což umožnilo praktickou implementaci, namísto pouhého následování teoretických směrnic.

Otázka 3: Jaká je míra implementace standardních požadavků organizace v rámci interního ISO auditu projektu?

V diplomové práci jsou podrobně popsány kroky a úroveň implementace požadavků na novém informačním portálu, které odpovídají definovaným požadavkům. Přechod na tuto novou platformu umožnil týmu znovu vytvořit strukturu a částečně implementovat vlastní přístup, který nejenom vyhovoval samotnému týmu, ale také splňoval požadavky ISO auditorů, metodiky ITIL a standardů společnosti. Míra implementace požadavků na novém informačním portálu byla vysoká a měla pozitivní dopad na celý projekt.

Otázka 4: Jaký je význam a přínos provedených změn během auditu a migrace na nový informační portál?

Díky minimalistickému přístupu a uzpůsobení kompletní nové struktury dle uvážení autora, tým mohl lépe organizovat svou práci. Tento přístup vedl k zefektivnění komunikace a možnostem sdílet informace za pomoci moderních funkcí, které nový portál nabízí. To výrazně zlepšilo produktivitu týmu, který získal možnost upravit, aktualizovat a vylepšit stávající pracovní postupy. Také umožnilo vedení efektivněji řídit, sledovat průběh projektu a pružněji reagovat na aktuální potřeby projektu. Nová struktura portálu také splnila náročné požadavky auditorů a metodiky ITIL.

Hlavním přínosem této práce by mohla být praktická ukázka toho, jak efektivně sladit různé metodiky, pravidla a předpisy do funkčního celku, který pomáhá dlouhodobě řídit směr a rozvoj IT projektu.

9 Závěry a doporučení

Důležitou informací je, že projekt úspěšně absolvoval ISO audit a obdržel certifikaci. Přestože příprava auditu musela být přizpůsobena firemní kultuře, výsledky práce jsou v souladu s očekáváními. V rámci analýzy požadavků byly popsány všechny klíčové prvky a procesy, které by měly být součástí interního ISO auditu. Příprava auditu byla systematická a zahrnovala teoretické studium a konzultace s auditory. Úspěšné zavedení nového informačního portálu splňovalo požadavky ISO auditorů, metodiky ITIL a standardů společnosti.

Během přípravy bylo přijato několik rozhodnutí, která nebyla původně součástí auditu, ale byla zkoumána v rámci kontinuálního zlepšování. Kromě implementace nového informačního portálu bylo zkoumáno rozhodování ohledně výběru nového monitorovacího nástroje pro plnění SLA (Service Level Agreement) a přechodu na nový nástroj pro správu požadavků a incidentů.

Výsledky a hodnocení všech klíčových prvků projektu ukazují, jak tyto prvky fungují v reálném prostředí a potvrzují jejich účinnost. Přestože tato práce splnila své původní zadání, stále existují další možnosti pro hlubší zkoumání této problematiky. Například byly zohledněny pouze hlavní body auditu a další firma nebo projekt by mohl provést kontrolu více aspektů. Další rozvoj této práce by mohl zahrnovat posouzení účinnosti dalších metodik a standardů v rámci interního auditu.

Během přípravy a samotného auditu se několikrát nabízela možnost využít pokročilejší manažerské metody, jako například vícekriteriálního rozhodování nebo analýza nákladů a přínosů pro výběr implementace nových řešení. K přípravě a vizualizaci procesu recertifikace a implementace metodiky ITIL by šel také využít BPMN (Business Process Model and Notation), což by umožnilo získat komplexní přehled o jednotlivých krocích, postupech a zúčastněných stranách v celém procesu implementace. Z důvodů časových limitů projektu a obecného nevyužívání pokročilých nástrojů pro rozhodování a plánování ve firmě, nebyly tyto metody implementovány.

V průběhu auditu byly identifikovány některé problémy, například potřeba zlepšit risk list a integrovat ho do znalostní databáze. Kontrola by také měla být více automatizovaná nebo by alespoň měla zahrnovat integraci s automatickým skenováním prostředí. Optimalizace těchto procesů by mohla být předmětem dalšího studia.

Celkově tato práce poskytuje ucelený obraz o správné přípravě a provedení auditu a implementaci nového informačního portálu. Výsledky a postupy mohou sloužit jako základ pro další rozvoj v oblasti ISO auditu, implementace metodiky ITIL a řízení IT projektů, jak z krátkodobého hlediska, tak s ohledem na dlouhodobý rozvoj.

10 Seznam použité literatury

[1] BRENNER, Michael, Thomas SCHAAF a Alexander SCHERER. Towards an information model for ITIL and ISO/IEC 20000 processes. In: *2009 IFIP/IEEE International Symposium on Integrated Network Management (IM)*: *2009 IFIP/IEEE International Symposium on Integrated Network Management* [online]. New York, NY, USA: IEEE, 2009, s. 113–116 [vid. 2023-07-27]. ISBN 978-1-4244-3486-2. Dostupné z: doi:10.1109/INM.2009.5188795

[2] MATARACIOGLU, Tolga a Sevgi OZKAN. Governing Information Security In Conjunction With Cobit And Iso 27001. *International Journal of Network Security & Its Applications* [online]. 2011, **3**. Dostupné z: doi:10.5121/ijnsa.2011.3410

[3] ORREGO, VLADIMIR MONTANO. The management in the security of the information according to COBIT, ITIL and ISO 27000. *Revista Pensamiento Americano*. 2011, **4**(6), 21–23. ISSN 2027-2448.

[4] ELHASNAOUI, S., H. MEDROMI, S.Faris - a H.Iguer -. Designing a Multi Agent System Architecture for IT Governance Platform. *International Journal of Advanced Computer Science and Applications* [online]. 2014, **5**(5) [vid. 2023-06-03]. ISSN 21565570, 2158107X. Dostupné z: doi:10.14569/IJACSA.2014.050524

[5] *ISO 27001 - ISMS, Bezpečnost informací, audity a certifikace, Praha* [online]. [vid. 2023-06-10]. Dostupné z: https://www.cqs.cz/Nase-sluzby/ISO-IEC-27001.html

[6] ESTUDIO.CZ. *ČSN EN ISO/IEC 27001 (369797)* [online]. [vid. 2023-06-08]. Dostupné z: https://www.technicke-normy-csn.cz/csn-en-iso-iec-27001-369797-199814.html

[7] *Nová verze normy ISO/IEC 27001: Nejdůležitější změny v ISO/IEC 27001: 2022 | Bureau Veritas Czech Republic Blíží se aktualizace normy ISO 27001: Které změny nastanou s příchodem ISO 27001:2022?* [online]. [vid. 2023-07-02]. Dostupné z: https://www.bureauveritas.cz/newsroom/nova-verze-normy-isoiec-27001-nejdulezitejsi-zmeny-v-isoiec-27001-2022

[8] JF. ISO/IEC 27001:2022. Jaký je rozdíl mezi ISO/IEC 27001:2013 a ISO/IEC 27001:2022? Jak postupovat v přechodném období do října 2025? *eucert - certifikace ISO* [online]. 9. leden 2023 [vid. 2023-06-17]. Dostupné

z: http://eucert.cz/iso-iec-270012022/

[9] *Information technology. Security techniques. Information security management guidelines for telecommunications organizations based on ISO/IEC 27002:* [online]. B.m.: BSI British Standards. nedatováno [vid. 2023-07-12]. Dostupné z: doi:10.3403/30166243

[10] AXELOS. *ITIL foundation: ITIL 4 edition*. First edition. Norwich: TSO (The Stationery Office), 2019. ISBN 978-0-11-331607-6.

[11] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 27001:2022, Third Edition: Information security, cybersecurity and privacy protection - Information security management systems - Requirements*. B.m.: Multiple. Distributed through American National Standards Institute (ANSI), 2022. Third Edition. ISBN 978-92-67-11311-1.

[12] *Certifikát ISO 27001. Vše co potřebujete vědět o certifikaci dle ISO/IEC 27001 - eucert - certifikace ISO* [online]. [vid. 2023-06-03]. Dostupné z: https://eucert.cz/vse-o-certifikaci-dle-iso-iec-27001/

[13] *Katalogy a databáze NK ČR* [online]. 2014 [vid. 2023-06-04]. Dostupné z: https://aleph.nkp.cz/F/KF21DSGUIXEN46LJH5HRCXBCXU9MJ9V2XDQHBR1S6GDJU389U1-37167?func=find-acc&acc_sequence=000007060

[14] INFO@AION.CZ, AION CS-. 82/2018 Sb. Vyhláška o kybernetické bezpečnosti. *Zákony pro lidi* [online]. [vid. 2023-06-03]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

[15] ITIL® V3 vs. ITIL® V4: The Major Differences | Simplilearn. *Simplilearn.com* [online]. 4. únor 2019 [vid. 2023-07-03]. Dostupné z: https://www.simplilearn.com/itil-4-vs-itil-v3-whats-new-article

[16] VIDAR DEGRUM. *COBIT, ITIL and ISO27001: Similarities and differences | LinkedIn* [online]. [vid. 2023-08-03]. Dostupné z: https://www.linkedin.com/pulse/cobit-itil-iso27001-similarities-differences-vidar-degrum/

[17] THEMEZHUB. Service Value System in ITIL 4 Explained | Sprintzeal. *Sprintzeal.com* [online]. [vid. 2023-08-04]. Dostupné z: https://www.sprintzeal.com/blog/service-value-system

[18] INFO@AION.CZ, AION CS-. 181/2014 Sb. Zákon o kybernetické bezpečnosti.

Zákony pro lidi [online]. [vid. 2023-06-04]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[19] *ZKB_blokove_schema.pdf* [online]. [vid. 2023-07-24]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/ZKB_blokove_schema.pdf

[20] 11 Best ITSM Tools (IT Service Management Software) In 2023. *Software Testing Help* [online]. 17. červenec 2023 [vid. 2023-06-03]. Dostupné z: https://www.softwaretestinghelp.com/itsm-tools/

[21] LINKS, Recommended. *ServiceNow Platform Compliance - ServiceNow* [online]. [vid. 2023-06-12]. Dostupné z: https://www.servicenow.com/company/trust/compliance.html

[22] ATLASSIAN. Global Category: Compliance Resource Center. *Atlassian* [online]. [vid. 2023-06-12]. Dostupné z: https://www.atlassian.com/trust/compliance/resources

[23] *Account documentation – Zendesk help* [online]. [vid. 2023-06-12]. Dostupné z: https://support.zendesk.com/hc/en-us/sections/5283084031898-Account-documentation

[24] *Národní úřad pro kybernetickou a informační bezpečnost - Nový zákon o kybernetické bezpečnosti je nezbytností pro Českou republiku, zaznělo ve Sněmovně* [online]. [vid. 2023-06-16]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1957-novy-zakon-o-kyberneticke-bezpecnosti-je-nezbytnosti-pro-ceskou-republiku-zaznelo-ve-snemovne/

[25] *ISO 9001 - QMS - Certifikace systémů managementu kvality, Praha* [online]. [vid. 2023-06-10]. Dostupné z: https://www.cqs.cz/Nase-sluzby/ISO-9001.html

[26] *ISO 14001 - EMS, Životní prostředí, Audity a certifikace, Praha* [online]. [vid. 2023-06-10]. Dostupné z: https://www.cqs.cz/Nase-sluzby/ISO-14001.html

[27] *ISO 20000 - ICT, Management služeb pro informační technologie, Praha* [online]. [vid. 2023-06-10]. Dostupné z: https://www.cqs.cz/Nase-sluzby/ISO-IEC-20000-1.html

[28] BARKER, Stuart. ISO 27001 Clause 10.1 Continual Improvement - Ultimate Certification Guide 2023. *High Table* [online]. 10. listopad 2022 [vid. 2023-06-05]. Dostupné z: https://hightable.io/iso-27001-clause-10-1-continual-improvement/

[29] *Kontext organizace v rámci ISO 9001 - ISO CERTIFIKACE* [online]. 27. prosinec 2022 [vid. 2023-07-02]. Dostupné z: https://iso-certifikace.cz/iso-9001/kapitoly-normy-iso-9001/kapitola-4/

[30] TURAN, Hazel. The Interactions in between ITIL, Cobit and ISO27001. *Hazel Turan* [online]. 3. březen 2016 [vid. 2023-06-04]. Dostupné z: https://hazelturan.wordpress.com/2016/03/03/the-interactions-in-between-itil-cobit-and-iso27001/

[31] BON, Jan van, ed. *Foundations of ITIL V3*. Zaltbommel: Van Haren Publ, 2011. Best Practice, 1. ed., 6. impr. ISBN 978-90-8753-057-0.

11 Seznam obrázků

12 Seznam tabulek

UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Akademický rok: 2023/2024

Studijní program: Informační management
Forma studia: Kombinovaná

Podklad pro zadání DIPLOMOVÉ práce studenta

Jméno a příjmení:	**Bc. Karel Kavuljak**
Osobní číslo:	**I2100456**
Adresa:	Hradecká 1152/11, Hradec Králové, 50003 Hradec Králové 3, Česká republika
Téma práce:	Příprava projektu a implementace požadavků metodiky ITIL pro interní audit ISO 27001
Téma práce anglicky:	Analysis and implementation of ITIL methodology requirements for ISO 27001 internal audit
Jazyk práce:	Čeština
Vedoucí práce:	doc. Ing. Pavel Čech, Ph.D. Katedra informačních technologií

Zásady pro vypracování:

1. Metodika zpracování
2. ISO audit
3. ITIL 4 metodika
4. ISO recertifikace
5. Hodnocení výkonosti

Seznam doporučené literatury:

[1] Certifikace systému podle ISO/IEC 27001:2022 Systémy managementu bezpečnosti informací Systémy managementu bezpečnosti informací – Požadavky [online] CQS 2023 [cit. 03.06.2023]. Dostupné z: https://www.cqs.cz/Nase-sluzby/ISO-IEC-27001.html
[2] Národní úřad pro kybernetickou a informační bezpečnost, 2018 – Úvodní stránka [online].[cit.03.06.2023]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/ZKB_blokove_schema.pdf
[3] ČSN EN ISO/IEC 27001 (369797). Technické normy ČSN. Bezpečnostní tabulky. | TECHNOR print, s.r.o. Hradec Králové [online]. 2020 [cit. 04.06.2023]. Dostupné z: https://www.technicke-normy-csn.cz/csn-en-iso-iec-27001-369797-199814.html
[4] Foundations of IT service management: based on ITIL V3. Editor Jan VAN BON. Zaltbommel: Van Haren, c2007. ISBN 978-90-8753-057-0
[5] Certifikát ISO 27001. Vše co potřebujete vědět o certifikaci dle ISO/IEC 27001 – eucert – certifikace ISO. – eucert – certifikace ISO [online]. 2023 [cit. 03.06.2023]. Dostupné z: https://eucert.cz/vse-o-certifikaci-dle-iso-iec-27001/

Podpis studenta: Datum:

Podpis vedoucího práce: Datum: