



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

BUDOVÁNÍ SYSTÉMU BEZPEČNOSTI VE SPOLEČNOSTI VYVÍJEJÍCÍ ZDRAVOTNICKÝ PROSTŘEDEK

BUILDING A SECURITY MANAGEMENT SYSTEM IN A COMPANY DEVELOPING A MEDICAL DEVICE

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Bc. et Bc. Veronika Tesařová

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. Petr Sedlák

BRNO 2025

Zadání diplomové práce

Ústav: Ústav informatiky
Studentka: **Bc. et Bc. Veronika Tesařová**
Vedoucí práce: **Ing. Petr Sedlák**
Akademický rok: 2024/25
Studijní program: Informační management

Garant studijního programu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Budování systému bezpečnosti ve společnosti vyvíjející zdravotnický prostředek

Charakteristika problematiky úkolu:

Cíle práce
Teoretický úvod
Popis současného stavu
Návrh řešení
Ekonomické zhodnocení
Závěr

Cíle, kterých má být dosaženo:

Cílem této diplomové práce je vybudovat systém bezpečnosti v prostředí společnosti vyvíjející zdravotnický prostředek v souladu s normou ISO/IEC 27001, včetně analýzy bezpečnosti, přípravy na certifikaci a dalších legislativních požadavků.

Základní literární prameny:

DOUCEK Petr, Martin KONEČNÝ a Luděk NOVÁK, Řízení kybernetické bezpečnosti a bezpečnosti informací, Praha: Professional Publishing, 2020. ISBN 978-80-88260-39-4.

SEDLÁK Petr, Martin KONEČNÝ, Přeměna ISMS v manažerské informatice. Brno: CERM, Akademické nakladatelství, 2023. ISBN 978-80-7623-110-8.

SEDLÁK Petr, Martin KONEČNÝ a kolektiv, Kybernetická (ne)bezpečnost. CERM, Akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

SEDLÁK Petr, Martin KONEČNÝ a kolektiv, Případové studie řízení kybernetické bezpečnosti. CERM, Akademické nakladatelství, 2024. ISBN 978-80-7623-126-9.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2024/25

V Brně dne 9.2.2025

L. S.

doc. Ing. Miloš Koch, CSc.
garant

prof. Ing. et Ing. Stanislav Škapa, Ph.D.
děkan

Abstrakt

Tato diplomová práce se věnuje návrhu a implementaci systému řízení bezpečnosti informací (ISMS) ve startupové společnosti zaměřené na vývoj zdravotnického prostředku. Součástí práce je analýza současného stavu bezpečnosti, identifikace rizik, vytvoření rizikových scénářů a návrh na bezpečnostní opatření. Dále byly zorganizovány penetrační testy, jejichž výsledky vedly k bezpečnostním změnám testovaných objektů. Významnou část tvoří příprava povinné dokumentace ISMS a návrh dalších kroků k dosažení souladu s legislativními a normativními požadavky.

Klíčová slova

systém řízení bezpečnosti informací, ISMS, ISO/IEC 27001, zdravotnický prostředek, zdravotnická informatika, umělá inteligence, AI

Abstract

The diploma thesis focuses on the planning and implementation of an Information Security Management System (ISMS) in a startup company developing medical device. The thesis includes an analysis of the current security state, risk identification, creation of risk scenarios, and the proposal of security measures. Penetration tests were also organized, with their results leading to security improvements of the tested assets. A significant part of the thesis is the preparation of mandatory ISMS documentation and the proposal of further steps to achieve compliance with legislative and normative requirements.

Keywords

Information Security Management System, ISMS, ISO/IEC 27001, Medical Device, Health Informatics, Artificial Intelligence, AI

Bibliografická citace

TESAŘOVÁ, Veronika. *Budování systému bezpečnosti ve společnosti vyvíjející zdravotnický prostředek* [online]. Brno, 2025 [cit. 2025-05-04]. Dostupné z: <https://www.vutbr.cz/studenti/zav-prace/detail/164774>. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Ing. Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 4. 5. 2025

Bc. et Bc. Veronika Tesařová

autor

Poděkování

Tímto bych chtěla poděkovat Ing. Petru Sedlákoví za odborné vedení mé diplomové práce, cenné rady a konzultace, které mi pomohly při budování systému bezpečnosti. Velké poděkování patří také konzultantovi a auditorům z certifikační autority za jejich profesionální přístup a konstruktivní kritiku. Děkuji také analyzované společnosti za projevenou důvěru a podporu během celého procesu implementace.

Největší poděkování však patří mému manželovi za jeho nekonečnou trpělivost, podporu a pochopení v průběhu celé práce.

OBSAH

ÚVOD.....	10
1 CÍLE, METODIKA A POSTUP ZPRACOVÁNÍ.....	12
1.1 Cíle.....	12
1.2 Metodika a postup zpracování.....	12
1.2.1 Metodika	12
1.2.2 Anonymizace	13
1.2.3 Další zpracování	14
2 TEORETICKÁ ČÁST	15
2.1 Základní pojmy a definice.....	15
2.2 Aktualizace normy ISO/IEC 27001.....	17
2.3 Informační a kybernetická bezpečnost ve startupovém prostředí.....	18
2.4 Informační a kybernetická bezpečnost ve zdravotnictví.....	19
2.5 Bezpečnostní normy a legislativa v oblasti umělé inteligence.....	22
2.5.1 Akt o umělé inteligenci	23
3 ANALÝZA SOUČASNÉHO STAVU.....	25
3.1 Popis společnosti	25
3.2 Bezpečnost před implementací ISMS	25
3.2.1 Vedení, role a odpovědnosti.....	25
3.2.2 Dokumentace a procesy	26
3.2.3 Technické a systémové zabezpečení	28
3.3 Asistované zhodnocení aktuálního stavu – GAP analýza.....	29
3.3.1 Organizační opatření	30
3.3.2 Opatření v oblasti lidských zdrojů	33
3.3.3 Opatření fyzické bezpečnosti.....	33
3.3.4 Technologická opatření	34

4	NÁVRH ŘEŠENÍ	37
4.1	Plán implementace	37
4.1.1	Spolupráce s VUT	37
4.1.2	Ganttův diagram	42
4.1.3	Penetrační testy	42
4.1.4	Další legislativní požadavky a související normy	47
4.2	Implementace	50
4.2.1	První etapa	50
4.2.2	Druhá etapa	53
4.2.3	Třetí etapa	56
4.2.4	Čtvrtá etapa	61
4.2.5	První kolo certifikačního auditu	66
4.2.6	Pátá etapa	70
4.3	Ekonomický aspekt	85
4.4	Nástroje	86
	ZÁVĚR	88
	SEZNAM POUŽITÝCH ZDROJŮ	90
	SEZNAM ZKRATEK	93
	SEZNAM OBRÁZKŮ	95
	SEZNAM TABULEK	96
	PŘÍLOHY	97

ÚVOD

Bezpečnost dat a informací hraje v dnešní digitální době klíčovou roli napříč obory, nicméně ve zdravotnictví nabývá na zvláštním významu. S rostoucím využíváním umělé inteligence a softwarových zdravotnických prostředků se objevují nové výzvy v oblasti zabezpečení citlivých údajů, ochrany patientských dat i souladu s legislativními požadavky.

Tato diplomová práce se zaměřuje na budování systému bezpečnosti ve společnosti, která vyvíjí zdravotnický prostředek založený na analýze medicínských dat, a to včetně využití prvků umělé inteligence. Jedná se o oblast, kde se střetává zdravotnická informatika, vývoj softwaru a kybernetická bezpečnost, tedy obory, v nichž dosud chybí dostatek provázaných praktických návodů pro efektivní zajištění bezpečnosti.

Impulesem pro vznik této práce byla absence komplexního přístupu k ochraně informací a bezpečnostnímu chování ve společnosti, ve které autorka působí. Téma je aktuální zejména v kontextu nedávných legislativních a plánovaných změn, jako jsou nařízení *NIS2*, Akt o umělé inteligenci (AI Act) a Zákon o kybernetické bezpečnosti (ZKB), které kladou zvýšené nároky na bezpečnost v oblasti zdravotnických technologií.

Motivací nebyla pouze interní potřeba zvýšit úroveň zabezpečení dat, ale také příprava na expanzi společnosti na zahraniční trhy, kde je certifikace dle mezinárodně uznávaných standardů často klíčovým požadavkem pro důvěryhodnost a konkurenceschopnost.

Diplomová práce nevytváří pouze obecný postup zavádění systému bezpečnosti, ale přináší specifická a praktická doporučení pro společnosti z oblasti zdravotnických technologií, které zpracovávají citlivé osobní údaje a pracují s algoritmy umělé inteligence. Práce podrobně mapuje proces zavedení systému řízení informační bezpečnosti rozdělený do pěti etap, počínaje asistovanou analýzou současného stavu, přes návrh a implementaci bezpečnostních opatření až po interní audit a první kolo certifikačního auditu. Ukončena je závěrem příprav na druhé kolo certifikace, které proběhlo začátkem dubna 2025.

Na projektu se podíleli také odborní konzultanti z akademického i praktického prostředí, konkrétně výzkumný tým z Vysokého učení technického v Brně, v čele s vedoucím této diplomové práce, a interní specialista na kybernetickou bezpečnost působící ve dvou

významných zdravotnických zařízeních. Díky této spolupráci mohla být vytvořena dokumentace reflektující jak požadavky norem, tak potřeby specifického zdravotnického prostředí.

1 CÍLE, METODIKA A POSTUP ZPRACOVÁNÍ

1.1 Cíle

Cílem této diplomové práce je vybudování systému řízení bezpečnosti informací ve společnosti vyvíjející softwarovou aplikaci pro analýzu digitálních snímků pro účely screeningového vyšetření. Systém je navržen v souladu s normou ISO/IEC 27001:2023, přičemž zahrnuje analýzu původní úrovně bezpečnosti, přípravu na certifikaci a zajištění souladu s legislativními požadavky. Implementace systému se zaměřuje především na oblast informační bezpečnosti s přesahem do kybernetické bezpečnosti. Společnost má již zavedený systém řízení kvality dle normy ISO 13485:2016, na který nový systém bezpečnosti navazuje. Cílem je provázat oba systémy tak, aby byl zajištěn jednotný a efektivní přístup k řízení bezpečnosti, přičemž do plánování jsou zahrnuty i specifické požadavky normy ISO/IEC 27799:2016 pro oblast zdravotnictví, IEC 81001-5-1:2021 zaměřený na zdravotnický software a bezpečnost a také legislativa vztahující se k umělé inteligenci, konkrétně regulační nařízení Akt o umělé inteligenci. V současné době ve společnosti neexistuje řízený systém bezpečnosti, nicméně povědomí o bezpečnostních požadavcích je přítomné, a proto je kladen důraz právě na sladění nového systému s již zavedenými procesy v rámci řízení kvality.

1.2 Metodika a postup zpracování

1.2.1 Metodika

Metodika a postup zpracování této diplomové práce jsou rozděleny do dvou hlavních částí: teoretické a praktické analytické.

Teoretická část se zaměřuje na odborné zdroje, které tvoří základ pro analýzu a návrh systému bezpečnosti. Mezi klíčové podklady patří technické normy, právní předpisy a doporučení, včetně tematicky specifických norem zdravotnické informatiky a norem řady ISO/IEC 27001:2023. Dále jsou využity materiály České asociace umělé inteligence a odborné publikace, například *Přeměna ISMS v manažerské informatice*, *Kybernetická (ne)bezpečnost* a *Případové studie řízení kybernetické bezpečnosti*. Tyto zdroje poskytují teoretický rámec pro zavádění systému řízení informační bezpečnosti v organizaci.

Praktická část práce je založena na analýze sesbíraných dat a podnětů získaných během jednotlivých fází implementace ISMS. Primárním zdrojem informací byla analýza

aktuálního stavu, která se zaměřila na posouzení stavu informační bezpečnosti ve společnosti před zahájením implementace. Následně byla provedena analýza stavu po prvním kole certifikačního auditu, která umožnila vyhodnotit přijatá opatření a identifikovat zbývající nedostatky.

Dalším zdrojem informací byly řízené rozhovory, které probíhaly se všemi zaměstnanci společnosti, včetně vrcholového managementu. Tyto rozhovory se zaměřovaly na vnímání bezpečnostních opatření, jejich aplikaci v praxi a případné podněty ke zlepšení. Významným přínosem byly rovněž konzultace s odborníky, a to jak v rámci spolupráce s vedoucím diplomové práce, tak s interním auditorem a specialisty z oblasti kybernetické a informační bezpečnosti. Součástí analytické části byla také fyzická kontrola bezpečnostních opatření, která probíhala zejména v rámci řízených rozhovorů o fyzické a technologické bezpečnosti. Tato kontrola zahrnovala rovněž monitorování běžného provozu v kanceláři a sledování bezpečnostního chování zaměstnanců. Důležitou součástí bylo rovněž přezkoumání dokumentace společnosti, které zahrnovalo nejen analýzu stávajících interních směrnic a bezpečnostních politik, ale také jejich přezkoumání a tvorbu nové dokumentace v souladu s požadavky normy ISO/IEC 27001. Tento proces umožnil nejen vyhodnotit stávající stav dokumentace, ale také zajistit její soulad s nově zaváděnými bezpečnostními opatřeními.

1.2.2 Anonymizace

Tato diplomová práce byla zpracována s důrazem na ochranu citlivých informací a zachování anonymity analyzované společnosti. Veškeré údaje týkající se společnosti, jejích systémů, konkrétních technologií a infrastruktury byly anonymizovány nebo modifikovány tak, aby nebylo možné jednoznačně identifikovat konkrétní subjekt. Tento přístup byl zvolen s ohledem na bezpečnostní aspekty a důvěrnost informací souvisejících s implementací systému řízení informační bezpečnosti.

Anonymizace se vztahuje především na názvy systémů, organizační strukturu, detailní technické specifikace a další prvky, které by mohly vést k identifikaci společnosti. Přestože veškeré údaje byly pozměněny či zobecněny, metodické postupy, analytické výstupy a závěry této práce vycházejí z reálného průběhu implementace a skutečných výsledků. Popisované procesy, analýzy, bezpečnostní opatření i závěry tedy odpovídají skutečnosti a jsou plně aplikovatelné v praxi. Tento přístup umožňuje zachovat autenticitu

práce a její přínos pro oblast informační a kybernetické bezpečnosti, aniž by došlo k ohrožení důvěrných údajů analyzované společnosti.

1.2.3 Další zpracování

Při zpracování této práce byl využit nástroj umělé inteligence *Elicit*¹ v asistující roli, a to pro orientaci v dostupných zdrojích. Výsledný obsah je výsledkem kritického vyhodnocení a vlastního zpracování autorky.

¹ Elicit. *Elicit: The AI Research Assistant* [online]. [cit. 2025-02-15]. Dostupné z: <https://elicit.com>. AI nástroj.

2 TEORETICKÁ ČÁST

2.1 Základní pojmy a definice

Zdravotnická informatika

Zdravotnická informatika je „vědecká disciplína, která se zabývá poznávacími, informačně-zpracovatelskými a komunikačními úkoly zdravotnické praxe, vzděláním a výzkumem včetně informační vědy a technologií na podporu těchto úkolů.“² Jde o obor, který propojuje zdravotnictví a informatiku s cílem optimalizovat využití zdravotnických informací ve prospěch pacientů i zdravotnických pracovníků. Zdravotnická informatika zahrnuje návrh, vývoj a využití systémů, které podporují sběr, uchovávání, zpracování a sdílení zdravotních dat. Význam tohoto oboru roste s rozvojem digitalizace zdravotní péče, implementací elektronických zdravotních záznamů, využitím umělé inteligence v diagnostice a léčbě a rostoucím důrazem na ochranu osobních zdravotních informací.

Zdravotnický prostředek

Pojem zdravotnický prostředek označuje jakýkoli nástroj, zařízení, software nebo jiný předmět určený výrobcem k použití za některým z konkrétních zdravotnických účelů. Mezi tyto účely patří například diagnostika, prevence, monitorování, predikce, prognóza atd.³

Systém AI

Systémem AI se podle definice z nařízení Akt o umělé inteligenci (*AI Act*) rozumí „strojový systém navržený tak, aby po zavedení fungoval s různými úrovněmi autonomie a který po zavedení může vykazovat adaptabilitu a který za explicitními nebo implicitními účely z obdržených vstupů odvozuje, jak generovat výstupy, jako jsou predikce, obsah, doporučení nebo rozhodnutí, které mohou ovlivnit fyzická nebo virtuální prostředí.“ Takový systém může být implementován pro různé účely a míru samostatnosti, a je proto

² ČSN EN ISO 27799: Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO 27002, 2017. Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

³ Evropská unie. Nařízení Evropského parlamentu a Rady (EU) 2017/745 ze dne 5. dubna 2017 o zdravotnických prostředcích a o zrušení směrnic Rady 93/42/EHS a 90/385/EHS. In: Úřední věstník Evropské unie. 5. 5. 2017, L 117/1, s. 1-175. ISSN 1977-0677.

zásadní chápat ho v kontextu jeho interakcí s okolím i schopnosti učit se nebo přizpůsobovat chování.⁴

Osobní zdravotní informace, Citlivé osobní údaje

Osobní zdravotní informace představují údaje vztahující se k fyzickému nebo psychickému zdraví konkrétní osoby, která je přímo nebo nepřímo identifikovatelná. Tyto informace mohou vznikat například při lékařském vyšetření, laboratorním testování či analýze biologických vzorků, a obsahují údaje o zdravotním stavu jednotlivce, jeho diagnózách nebo poskytované péči.⁵ V kontextu právní úpravy ochrany osobních údajů, zejména podle *Nařízení EU 2016/679 (GDPR)*, jsou zdravotní údaje považovány za citlivé osobní údaje, jejichž zpracování podléhá zpřísněným podmínkám a vyžaduje zvláštní ochranu.⁶

Identifikovatelná osoba

Pojem identifikovatelná osoba je klíčovým termínem v oblasti ochrany osobních údajů, zejména ve zdravotnictví, kde dochází ke zpracování citlivých informací. Jedná se o osobu, „*která může být přímo či nepřímo identifikována prostřednictvím identifikačního čísla (rodného čísla), případně jedním nebo více faktory upřesňujícími její fyzickou, fyziologickou, mentální, ekonomickou, kulturní či sociální identitu*“⁷ V oblasti zdravotnických prostředků se může jednat například o údaje získané ze zobrazovacích zařízení, tyto informace často obsahují biometrické údaje nebo jiné charakteristiky, podle kterých lze pacienta přímo či nepřímo rozpoznat.

⁴ Evropská unie. Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanovují harmonizovaná pravidla pro umělou inteligenci a mění se nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (Akt o umělé inteligenci). In: Úřední věstník Evropské unie. 12. 7. 2024, L 1689, s. 1-144. ISSN 1977-0626.

⁵ ČSN EN ISO 27799: Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO 27002, 2017. Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

⁶ Evropská unie. Nařízení Evropského parlamentu a Rady (EU) 2017/745 ze dne 5. dubna 2017 o zdravotnických prostředcích a o zrušení směrnic Rady 93/42/EHS a 90/385/EHS. In: Úřední věstník Evropské unie. 5. 5. 2017, L 117/1, s. 1-175. ISSN 1977-0677.

⁷ ČSN EN ISO 27799: Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO 27002, 2017. Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

Systém řízení informační bezpečnosti

Systém řízení informační bezpečnosti (ISMS) je součástí systému řízení organizace, zaměřený na ochranu důvěrnosti, integrity a dostupnosti informací. ISMS představuje rámec procesů a opatření pro řízení rizik v oblasti informační bezpečnosti s cílem je implementovat, přezkoumávat a neustále zlepšovat úroveň informační bezpečnosti. Konceptně vychází z cyklu PDCA (*Plan-Do-Check-Act*) a zahrnuje stanovení bezpečnostní politiky, analýzu rizik, zavádění bezpečnostních opatření (technických i organizačních) a průběžný dohled nad jejich účinností. Mezinárodním standardem pro ISMS je norma ISO/IEC 27001:2023.

2.2 Aktualizace normy ISO/IEC 27001

V roce 2022 byla vydána revidovaná verze mezinárodní normy ISO/IEC 27001, která po téměř deseti letech aktualizovala požadavky na systém řízení informační bezpečnosti. Nový název normy *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky* zahrnuje širší zaměření i na kybernetickou bezpečnost a ochranu osobních údajů. Mezi klíčové změny patří zejména nová struktura bezpečnostních opatření (Příloha A), jejichž počet byl zredukován ze 114 na 93 a nově rozdělen do čtyř tematických skupin: organizační, v oblasti lidských zdrojů, fyzická bezpečnost a technologická opatření.

Norma byla rozšířena o nová opatření, která reflektují současné hrozby a technologický vývoj, například zpravodajství o hrozbách, bezpečnost cloudových služeb, připravenost ICT na narušení provozu, vymazání informací nebo bezpečné kódování. Současně byly upřesněny požadavky na plánování změn, řízení procesů, interní audit a přezkoumání vedením. Pro organizace certifikované podle verze z roku 2013 je stanoveno přechodné období do konce října 2025.⁸

⁸ EUCert. *Norma ISO/IEC 27001:2022. Jaké jsou klíčové změny v normě ISO/IEC 27001:2022?* [online]. 22. května 2023 [cit. 2025-04-11]. Dostupné z: <https://eucert.cz/norma-iso-27001-2022/>.

Změny byly implementovány také v související normě ISO/IEC 27002:2022, která obsahuje podrobný výklad opatření a jejich mapování vůči předchozí verzi prostřednictvím Přílohy B, čímž zajišťuje zpětnou kompatibilitu.⁹

2.3 Informační a kybernetická bezpečnost ve startupovém prostředí

Prostředí startupů a malých podniků je charakteristické specifickým kontextem, který je při budování systému řízení informační bezpečnosti nezbytné zohlednit. V této souvislosti je důležité brát v úvahu omezenou organizační zralost, omezené finanční a personální zdroje, stejně jako časové možnosti.

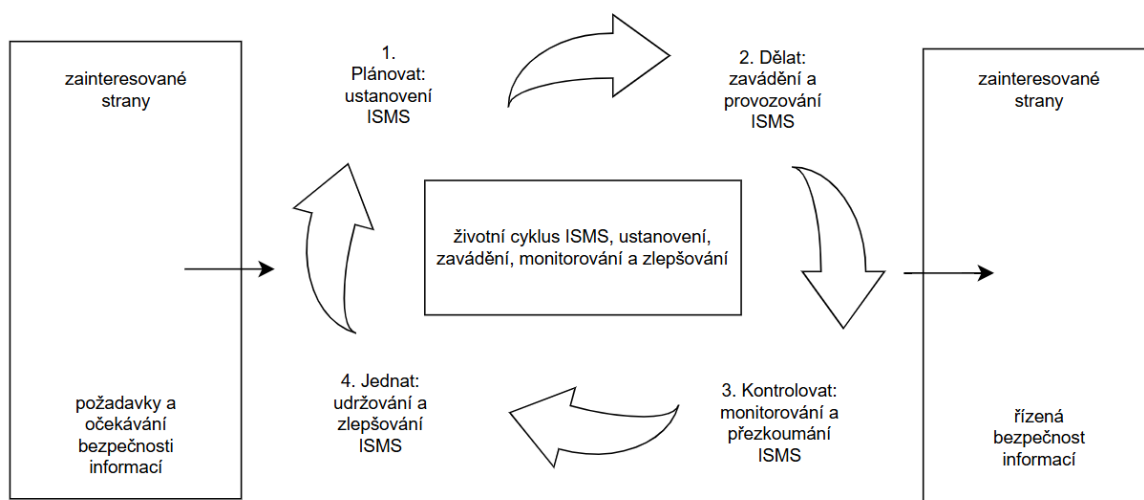
Pro účely této práce byly vybrány klíčové závěry ze studie *A GAP Analysis Tool For SMEs Targeting ISO/IEC 27001 Compliance* zaměřené na analýzu souladu malých a středních podniků (SME) s požadavky normy. Cílem této studie bylo identifikovat silné a slabé stránky malých a středních podniků vzhledem k požadavkům normy. Bylo zjištěno, že není nezbytné procházet každý jednotlivý požadavek normy, neboť některé požadavky jsou redundantní a vhodné ke sloučení. Dále se ukázalo, že různé požadavky se vztahují k různým rolím a odpovědnostem v rámci podniku, což v prostředí s omezeným počtem pracovníků způsobuje určitou neefektivitu. Zároveň bylo zjištěno, že některé požadavky, zejména v oblasti řízení rizik, jsou pro pracovníky bez předchozí zkušenosti s informační bezpečností příliš složité. Proto je nutné poskytovat dodatečné metodické pokyny a objasnění klíčových otázek.¹⁰

Organizační struktura startupů přináší při implementaci ISMS další výzvy. Tyto společnosti často prosperují díky své flexibilitě a schopnosti rychle reagovat na změny, zatímco systém řízení informační bezpečnosti má spíše formální a byrokratický charakter. Navíc je pro startupy typická snaha o rychlý růst, což může být v rozporu se statickým nastavením ISMS, pokud systém není dynamicky upravován.

⁹ ČSN EN ISO/IEC 27002: Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti, 2022. Třetí vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

¹⁰ VALDEVIT, Thierry, Nicolas Mayer, 2010. A GAP ANALYSIS TOOL FOR SMES TARGETING ISO/IEC 27001 COMPLIANCE. In *Proceedings of the 12th International Conference on Enterprise Information Systems – Volume 2: ICEIS*. ISBN 978-989-8425-06-5. ISSN 2184-4992, SciTePress, s. 413-416.

Navzdory těmto odlišnostem přístup k hodnocení současného stavu bezpečnosti vychází z obecně uznávaných principů a není zásadně odlišný. I v kontextu malého podniku je aplikován princip cyklického modelu neustálého zlepšování, tzv. *PDCA cyklus* (Plan-Do-Check-Act), který je znázorněn na *Obrázku 1*. Organizace nejprve plánuje potřebné činnosti v oblasti bezpečnosti, následně je implementuje, vyhodnocuje jejich účinnost a na základě výsledků přijímá odpovídající nápravná opatření. Díky tomuto přístupu ISMS není vnímán jako soubor pravidel, ale jako dynamický systém, který se dokáže přizpůsobovat měnícím se hrozbám a novým regulatorním požadavkům.



Obrázek 1: PDCA model

(Zdroj: Vlastní zpracování dle ČSN EN ISO 27799, 2017, str. 63)

2.4 Informační a kybernetická bezpečnost ve zdravotnictví

V posledních letech došlo ve zdravotnických organizacích, obdobně jako v jiných odvětvích, k významnému posunu v chápání bezpečnosti informací. Bezpečnost již není vnímána pouze jako technická či *back office* funkce, ale stala se významnou organizační odpovědností. Tato změna v přístupu reflektuje rostoucí důležitost ochrany zdravotnických informací a potřebu komplexního řízení rizik.¹¹

Zdravotnické informace, které musí být chráněny, zahrnují široké spektrum dat, mezi které patří osobní zdravotní informace, pseudonymizovaná data získaná z osobní

¹¹ ČSN EN ISO 27799: Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO 27002, 2017. Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

zdravotní dokumentace, anonymizované statistické a výzkumné údaje, klinické lékařské znalosti nesouvisející s konkrétními pacienty, údaje o zdravotnických pracovnících, informace související s veřejným dohledem nad zdravotnictvím, auditní záznamy a systémová bezpečnostní data pro zdravotnické informační systémy.¹²

„Bez ohledu na velikost, umístění a formu poskytovaných služeb všechny zdravotnické organizace musí mít zavedena nezbytná opatření k ochraně zdravotnických informací“¹³

V oblasti řízení bezpečnosti informací se zdravotnické organizace kromě ISO/IEC 27001 řídí také normou ISO 27799, která specifikuje požadavky a doporučení zaměřená právě na ochranu zdravotnických informací.

Norma ISO 27799 stanovuje například tyto požadavky:

- **Pokyny managementu organizace k bezpečnosti informací:** Politika bezpečnosti musí obsahovat jasné prohlášení o ochraně zdravotnických informací a postupy pro sdílení dat, zejména pro účely výzkumu a klinických studií.
- **Mobilní zařízení a práce na dálku:** Organizace musí zavést politiku preventivních opatření, která chrání data při práci mimo prostory organizace.
- **Před vznikem pracovního poměru:** Již při náboru zaměstnanců nebo smluvních stran je nutné ověřit identitu a předchozí zkušenosti uchazečů. Zaměstnanci a smluvní strany jsou také povinni hlásit jakékoliv incidenty spojené s narušením bezpečnosti zdravotnických informací.
- **Ukončení a změna pracovního poměru:** Vzhledem k častým změnám pozic a přístupových práv (v rámci různých programů a rotací) musí být proces ukončení či změny zaměstnání spojen se správnou revizí a úpravou přístupových práv.
- **Odpovědnost za aktiva:** Organizace musí identifikovat a spravovat svá informační aktiva, zajistit pravidla jejich používání a chránit jejich integritu a dostupnost. Zaměstnanci a smluvní strany musí po ukončení zaměstnání zajistit, aby všechny zdravotnické informace, které mají v držení v elektronické formě

¹² SEDLÁK, Petr a Martin KONEČNÝ. *Přeměna ISMS v manažerské informatice*. Brno: CERM, Akademické nakladatelství, 2023. ISBN 978-80-7623-110-8, s. 216.

¹³ SEDLÁK, Petr a Martin KONEČNÝ. *Přeměna ISMS v manažerské informatice*. Brno: CERM, Akademické nakladatelství, 2023. ISBN 978-80-7623-110-8, s. 218.

byly aktualizovány v relevantních zdravotních systémech a poté bezpečně vymazány ze všech zařízení, na kterých byly uloženy.

- **Klasifikace informací:** Osobní zdravotní informace musí být vždy klasifikovány jako důvěrné (důvěrnost osobních zdravotních informací závisí na jejich kontextu), přičemž klasifikace má zohledňovat také kritičnost, dostupnost a integritu informací. Uživatelé zdravotnických informačních systémů potřebují vědět, kdy data, ke kterým přistupují, obsahují osobní zdravotní informace.
- **Požadavky organizace na řízení přístupu:** Organizace musí evidovat všechny strany, se kterými sdílí zdravotnická data, a uzavírat odpovídající dohody o přístupu k těmto datům. Je doporučeno zvážit zavedení sdílení identity v reálném čase a řešení řízení přístupu, které podpoří technologie přístupu s vyšší úrovní bezpečnosti, jako je například metoda jednorázového přihlášení. Zdravotnické informační systémy zpracovávající osobní zdravotní informace umožnit autentizaci obsahující alespoň dva faktory.
- **Zařízení:** Zajištění bezpečného používání zdravotnických zařízení, včetně zařízení používaných mimo prostory organizace.
- **Provozní postupy a odpovědnosti:** Vývojová a testovací prostředí musí být oddělena (fyzicky nebo virtuálně) od produkčního prostředí, aby byla zajištěna ochrana osobních zdravotních informací.
- **Zálohování:** Osobní zdravotní informace musí být pravidelně zálohovány a uloženy ve fyzicky bezpečném prostředí, aby byla zajištěna jejich budoucí dostupnost.
- **Zaznamenávání formou logů a monitorování:** Auditní záznamy musí být dostatečně podrobné, identifikovat uživatele, subjekty péče, provedené úkoly a časové údaje. Přístup k těmto datům musí být přísně kontrolován. Doba uchovávání těchto auditních záznamů musí být zvážena se zvláštním zřetelem na klinické profesní normy a zákonné povinnosti. Integrita auditních záznamů může hrát klíčovou roli například při vyšetřování lékařského zanedbávání povinné péče. Synchronizace času na podporu trasování a rekonstruování časových os aktivit je také klíčová, pokud by to v budoucnu bylo požadováno.

- **Přenos informací:** Organizace musí zajistit bezpečný přenos zdravotnických informací mezi odborníky, například prostřednictvím šifrovaných e-mailů. Pokud jsou kryptografické nástroje příliš složité, mohou se uživatelé ve zdravotnictví zdráhat je používat.
- **Bezpečnostní požadavky informačních systémů:** Data umožňující osobní identifikaci musí být uchovávána pouze tehdy, je-li to nezbytné, a musí být použity techniky pro vymazání, anonymizaci a pseudonymizaci.
- **Data pro testování:** Organizace zpracovávající osobní zdravotní informace by jako data pro testování neměla používat aktuální osobní zdravotní informace.
- **Řízení incidentů bezpečnosti informací a zlepšování:** Organizace musí mít zavedené postupy pro řízení incidentů, včetně povinnosti informovat subjekty péče v případě úniku jejich osobních údajů. Typické incidenty informační bezpečnosti zahrnují zničení, neúmyslné vyzrazení osobních zdravotních informací nebo ztrátu dostupnosti zdravotnických informačních systémů.
- **Přezkoumání bezpečnosti informací:** Důraz je kladen na interoperabilitu zdravotnických systémů a zajištění technické shody při výměně zdravotnických dat, protože rozsáhlé zdravotnické informační systémy se obvykle sestávají z mnoha vzájemně spolupracujících systémů.¹⁴

Přehled všech požadavků a doporučení je k dispozici v kontrolním seznamu shody s normou ISO 27799 uvedeném v Příloze C této normy.

2.5 Bezpečnostní normy a legislativa v oblasti umělé inteligence

Dosavadní standardy kybernetické a informační bezpečnosti, včetně mezinárodní normy ISO/IEC 27001, se na problematiku systémů AI nevztahují přímo a pojem umělá inteligence v nich není explicitně zmíněn. S cílem řešit tuto oblast se v současné době připravuje norma *ISO/IEC 27090 – Kybernetická bezpečnost – Umělá inteligence – Pokyny pro řešení bezpečnostních hrozeb systémů umělé inteligence*.

¹⁴ ČSN EN ISO 27799: Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO 27002, 2017. Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

Vznikla také potřeba nového regulačního rámce, který by reflektoval specifika AI systémů, a to jak z hlediska jejich návrhu, tak způsobu nasazení a dohledu nad jejich fungováním. Reakcí Evropské unie je nařízení o umělé inteligenci, známé jako Akt o umělé inteligenci neboli AI Act.¹⁵

2.5.1 Akt o umělé inteligenci

Nařízení Evropského parlamentu a Rady (EU) o umělé inteligenci (tzv. AI Act) představuje první komplexní právní rámec pro regulaci umělé inteligence v Evropské unii. Jeho cílem je zajistit bezpečné a důvěryhodné nasazení systémů AI, a to zejména prostřednictvím povinností v oblasti řízení rizik, správy dat, robustnosti systémů a kybernetické bezpečnosti.

AI Act vychází z přístupu založeného na riziku, přičemž systémy jsou rozděleny do čtyř kategorií: zakázané, vysoce rizikové, omezeně rizikové a minimálně rizikové. Pro vysoce rizikové systémy AI, mezi které mohou patřit i systémy zpracovávající zdravotní data nebo využívané v oblasti zdravotnictví, se uplatňují přísnější bezpečnostní a organizační požadavky. Patří mezi ně například povinnost registrace systému ve veřejné databázi EU¹⁶, vedení technické dokumentace, zavedení systému řízení rizik, pravidelné testování a monitoring systému a správa dat včetně jejich integrity, původu a ochrany před zkreslením či zneužitím.

Nařízení dále vyžaduje, aby tyto systémy zaznamenávaly relevantní provozní údaje (logy) a měly implementována opatření pro detekci incidentů, jejich hlášení a rychlou reakci. Klade důraz na *security by design* a požaduje, aby systémy byly technicky i organizačně navrženy tak, aby odolaly selhání, chybám i úmyslným útokům. To zahrnuje i ochranu proti manipulaci se vstupy, trénovacími daty nebo modely samotnými, a schopnost detekce anomálií.¹⁷

¹⁵ Evropská unie. Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanovují harmonizovaná pravidla pro umělou inteligenci a mění se nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (Akt o umělé inteligenci). In: Úřední věstník Evropské unie. 12. 7. 2024, L 1689, s. 1-144. ISSN 1977-0626.

¹⁶ Česká asociace umělé inteligence. *Nejsrozumitelnější průvodce EU AI Act* [online]. 4. února 2025 [cit. 2025-05-03]. Dostupné z: <https://asociace.ai/eu-ai-act/>.

¹⁷ Evropská unie. Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024 o umělé inteligenci a změně některých legislativních aktů Unie (Akt o umělé inteligenci), čl. 9-15. Úřední

AI Act reflektuje také potřebu přizpůsobení požadavků pro malé a střední podniky a startupy, např. prostřednictvím regulačních sandboxů, které umožňují vývoj v kontrolovaném prostředí pod dohledem národního regulátora.¹⁸

Z hlediska dopadu na systém řízení informační bezpečnosti znamená AI Act nutnost začlenit specifická rizika AI systémů do analýzy rizik ISMS, upravit technická opatření, jako je řízení přístupu, šifrování, zabezpečení vývoje, správa záznamů o provozu a monitoring provozních událostí.

věstník Evropské unie, L 2024/1689, 18. 4. 2025. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=OJ:L_202401689.

¹⁸ Česká asociace umělé inteligence. *Nejsrozumitelnější průvodce EU AI Act* [online]. 4. února 2025 [cit. 2025-05-03]. Dostupné z: <https://asociace.ai/eu-ai-act/>.

3 ANALÝZA SOUČASNÉHO STAVU

3.1 Popis společnosti

Tato práce se zabývá implementací bezpečnostních opatření do prostředí technologické společnosti, startupu, jejíž název a některé detaily zůstávají z důvodu ochrany důvěrných informací anonymizovány. Jedná se o startup, který vytvořil inovativní software využívající umělou inteligenci k analýze obrazových dat za účelem detekce konkrétních onemocnění. Společnost software nejen vyvinula, ale dále jej spravuje a aktivně rozvíjí. Produkt je přístupný prostřednictvím online platformy, která umožňuje uživatelům nahrávat obrazová data, získávat výsledky analýz a spravovat související informace.

Analyzovaná společnost již implementovala systém managementu kvality, který slouží k zajištění základních standardizovaných procesů. Tento systém je podložen certifikací, která dokládá závazek společnosti poskytovat služby na vyšší úrovni kvality. Oblast bezpečnosti informací však dosud nebyla systematicky řešena.

3.2 Bezpečnost před implementací ISMS

3.2.1 Vedení, role a odpovědnosti

Vedení společnosti se jednotně shodlo na nutnosti zavedení vyšší úrovně bezpečnosti. Nicméně, v původní podobě kompetenční matice není definována žádná specifická role, která by zajišťovala nebo převzala odpovědnost za informační bezpečnost. Vedení organizace přistupuje k posuzování rizik z různých perspektiv: CEO se zaměřuje na hodnocení rizik z obchodního hlediska, zatímco CTO posuzuje rizika z technologického hlediska. Ani Team Lead SW developer a AI Engineer nejsou v rámci svých rolí zodpovědní za bezpečnostní opatření.

V organizaci zatím neexistovala specifická role CISO (Chief Information Security Officer), která by byla primárně zodpovědná za informační bezpečnost. Avšak v rámci systému řízení kvality je v kompetenční matici zohledněna role QM (Quality Managera), která zahrnuje mimo jiné odpovědnost za řízení rizik podle normy ISO 14971, správu životního cyklu software dle IEC 62304, požadavky na bezpečnost zdravotnického software podle normy IEC 82304-1:2016 a zajištění kybernetické bezpečnosti zdravotnických prostředků podle směrnice MDCG 2019-16. Dále je v kompetenční matici popsána role PRRC (Person Responsible for Regulatory Compliance), která nemá

přímou odpovědnost za bezpečnost, ale má pravomoc nařídit nebo provést kontrolu všech procesů ve společnosti s ohledem na kvalitu, bezpečnost a účinnost zdravotnických prostředků, a to i bez předchozího ohlášení.

Role Office Managera je definována v oblasti bezpečnosti práce, kde zajišťuje bezpečné a ochranné pracovní podmínky, avšak v oblasti kybernetické bezpečnosti má větší pravomoci a zodpovědnosti Product Manager, který má definované kompetence vyplývající z požadavků na kybernetickou bezpečnost zdravotnických prostředků dle směrnice MDCG 2019-16.

Zodpovědnost za ochranu dat je přiřazena roli Data Engineera, který se postupně transformuje na pozici CISO. U této role bude kladen důraz na implementaci systému řízení informační bezpečnosti, čímž se zajistí komplexní přístup k ochraně citlivých informací a aktiv ve společnosti.

3.2.2 Dokumentace a procesy

Společnost vede dokumentaci prostřednictvím dokumentačního portálu Confluence od společnosti Atlassian, kde jsou vytvořeny dva základní prostory – VALID Integrovaný systém managementu a DRAFT Integrovaný systém managementu. Dokumentace je vedena v obou těchto prostorech, přičemž prostor VALID obsahuje schválené a podepsané verze dokumentů, které již nelze upravovat. Tyto dokumenty jsou závazné pro všechny pracovníky a mají k nim nepřetržitý a neomezený přístup. Struktura těchto prostorů umožňuje jejich další rozdělení na část věnující se již zavedenému *Systému řízení kvality* a část zaměřenou na *Technickou dokumentaci*.

Systém řízení kvality se otázkám bezpečnosti věnuje zejména v rámci manažerských procesů, mezi něž patří *Řízení dokumentů a záznamů*, *Validace procesů a nástrojů* a *Řízení rizik*. Součástí řízení rizik je organizační směrnice, která definuje postupy spojené s řízením rizik produktů a procesů. Tato směrnice však není plně v souladu s požadavky normy ISO/IEC 27001. Realizační procesy, například *Návrh a vývoj softwaru*, detailně popisují řízení vývoje produktů, jejich změn, testování či přípravu release balíčku. V této oblasti je však stále prostor pro úpravy v rámci implementace systému řízení informační bezpečnosti. Organizační směrnice *IT Operations* definuje procesy související se službami a údržbou zdravotnického prostředku, který je realizován jako softwarová

aplikace. Zahrnuje stručný popis plánování údržby a monitoringu, specifikaci prováděných činností a řešení softwarových chyb.

Podpůrné procesy jsou z hlediska implementace systému řízení informační bezpečnosti lépe připraveny. Organizační směrnice *Interní audit* se v současnosti zaměřuje výhradně na systém řízení kvality, avšak její struktura umožňuje budoucí rozšíření na systém řízení informační bezpečnosti. Dokument obsahuje definování cílů auditu, požadavky na kvalifikaci interního auditora, plánování a průběh auditu, stejně jako vyhodnocení a tvorbu auditní zprávy. Směrnice *Řízení lidských zdrojů* zahrnuje aspekty personální agendy z hlediska bezpečnosti, přičemž se zaměřuje na zabezpečení záznamů, vstupní školení zaměstnanců v oblasti informační bezpečnosti, interní vzdělávací plán a postupy pro ukončení pracovního poměru.

Z pohledu bezpečnosti je klíčovým dokumentem organizační směrnice *Informační bezpečnost*. Před implementací systému řízení informační bezpečnosti obsahovala pouze základní bezpečnostní opatření, mezi něž patřilo fyzické zabezpečení s obecnými požadavky na bezpečnost, ochrana dokumentů obsahujících personální údaje a tištěné dokumentace, zabezpečení majetku během výstav a ochrana pracovních stanic. Dále se zabývala chováním uživatelů, politikou hesel, která zahrnovala i ověřování síly hesla prostřednictvím webového nástroje, přístupovými právy ke zdrojům v cloudovém prostředí a zabezpečením dat, zejména z pohledu pseudonymizace a anonymizace, přístupů k datům a pravidel pro práci s daty na lokálních zařízeních. Směrnice rovněž obsahovala pravidla pro školení v oblasti informační bezpečnosti, konkrétní povinné kurzy, pravidelnou kontrolu uživatelů, popis postupu při bezpečnostních incidentech a zásady zálohování dat.

Společnost také vytvořila GDPR kodex chování, označovaný jako *Kodex chování při zpracování osobních údajů*. Tento dokument byl vypracován za účelem stanovení nezbytných zásad, požadavků a povinností vyplývajících z nařízení Evropského parlamentu a Rady (EU) a je závazný pro analyzovanou organizaci.

Kromě dokumentace popisující chod organizace vede společnost také schválenou technickou dokumentaci, která zahrnuje *architektonické review*. Tento dokument popisuje bezpečnostní prvky infrastruktury, oddělení jednotlivých prvků a bezpečné ukládání patientských a klientských dat. Součástí technické dokumentace je rovněž seznam používaného softwaru třetích stran. Technická složka dále obsahuje metodické pokyny,

včetně systému sledování a hlášení nežádoucích příhod, známého jako *Vigilance – Systém ostrahy*. V kontextu systému řízení kvality zdravotnických prostředků (MDR) se nežádoucí příhoda vztahuje k bezpečnosti pacientů a zdravotnických prostředků, nikoli k informační bezpečnosti organizace.

V rámci technické složky jsou prováděny dílčí rizikové analýzy zdravotnického prostředku, které se v některých aspektech podobají analýze rizik ISMS. Výsledkem těchto analýz je registr rizik zdravotnického prostředku, jenž obsahuje identifikovaná nebezpečí a nebezpečné situace. Zatímco analýza rizik ISMS se zaměřuje na rizikové scénáře týkající se fyzické bezpečnosti, organizačních opatření, lidských zdrojů a technologických aspektů, analýza rizik zdravotnického prostředku vychází z klinického sledování po uvedení na trh (PMCF), prováděných klinických hodnocení a monitoringu provozních logů aplikace.

Obě analýzy mohou obsahovat podobné scénáře, například softwarové chyby vedoucí k nesprávné diagnostice, neautorizovaný přístup, nespolehlivou infrastrukturu nebo změny v softwarových algoritmech, které mohou ovlivnit zabezpečení aplikace. V těchto případech je vždy kladen důraz na bezpečnost architektury aplikace, avšak s odlišným cílem. Zatímco analýza rizik v rámci ISMS usiluje o minimalizaci bezpečnostních rizik pro informační aktiva organizace, včetně samotného softwaru, analýza rizik z pohledu systému řízení kvality zdravotnického prostředku se soustředí na ochranu pacienta, uživatele a třetích stran před zdravotními riziky.

3.2.3 Technické a systémové zabezpečení

Společnost technologicky funguje především na cloudových platformách *Microsoft* a *Atlassian*, přičemž u obou platí povinnost dvoufaktorového ověření. Privilegované role a přístupy jsou však přidělovány bez stanovených postupů a pravidel, což znamená, že tento proces neprobíhá prostřednictvím oficiálních žádostí nebo tiketů. Počet privilegovaných rolí není omezen. Azure Subscriptions, tedy prostředí nebo také základní zdroje, jsou rozdělena pro vývoj, data a produkci, přičemž pouze jedno z nich je nasazeno na šabloně *Blueprint ISO 27001*. Tento šablonový rámec předdefinuje požadavky uvedené normy, například tím, že neumožňuje geografické umístění dat v jiné oblasti.

Společnost nevlastní síťové prvky, včetně routerů, a nemá smlouvu na poskytování VPN od přidružené kliniky. Antivirus není implementován, přičemž je doporučen pouze

Microsoft Defender, který je nainstalován defaultně pro Microsoft zařízení. Společnost neomezuje výběr programovacích, aplikačních ani podpůrných softwarů pro své pracovníky. Přístupy, role a samotné účty, včetně Microsoft Entra ID, nejsou adekvátně kontrolovány, deaktivovány ani blokovány včas. Pracovníci používají zařízení, přičemž není jasné, jaké operační systémy a kolik zařízení je v rámci organizace používáno, ani zda pracovníci oddělují osobní a pracovní účty a data.

Co se týče zdravotnického prostředku, v již zmíněném *architektonickém review* je uvedeno, že aplikace je postaveny na principech *secure by design*. Datacentrum se nachází v Evropě a zahrnuje aktivní prvky proti kybernetickým útokům. Data jsou bezpečně oddělena pro jednotlivá oddělení organizace a aplikace běží na Azure Kubernetes Service Cluster, což umožňuje bezpečné oddělení různých částí systému a dynamické řízení výkonu. Nicméně chybí dokumentace monitoringu aplikace, která by umožnila detekci konfiguračních výpadků, a rovněž není vedena dokumentace logů.

Uložiště typu Microsoft Azure Storage je postupně dokumentováno a konfigurováno. Sdílené úložiště SharePoint, používané napříč organizací, obsahuje dokumenty a soubory s osobními a citlivými údaji. Systém pro řízení vztahů se zákazníky není dokumentován, kontrolován ani spravován, přístupy a administrátorská práva jsou nejasná.

Pokud jde o hardware, společnost vlastní především zdravotnická zobrazovací zařízení, server na trénování a testování AI modelů a koncová zařízení pro některé pracovníky. Hardware je často ponecháván bez dozoru, zabezpečení některých zařízení není vyžadováno ani kontrolováno. Server je umístěn volně v kanceláři, což není ideální, a neobsahuje auditní logy ani omezení práv, pouze přístupy pro vybrané pracovníky.

3.3 Asistované zhodnocení aktuálního stavu – GAP analýza

Na začátku roku 2024 začala společnost seriózně zvažovat zavedení systému řízení informační bezpečnosti s cílem dosáhnout certifikace podle normy ISO/IEC 27001:2023. Po třech měsících diskusí bylo v polovině března rozhodnuto o zahájení asistovaného zhodnocení aktuálního stavu prostřednictvím GAP analýzy, která se zaměřila na posouzení jednotlivých bezpečnostních opatření popsanych v doprovodné normě ISO/IEC 27002:2023.

Ve stejném období, nezávisle na výsledcích analýzy, bylo vedením společnosti podepsáno oficiální prohlášení o zavádění systému řízení informační bezpečnosti, které formalizovalo závazek k jeho implementaci. Asistované zhodnocení probíhalo od poloviny března do poloviny srpna téhož roku. V rámci realizace projektu byla navázána spolupráce s vybranými zaměstnanci společnosti, kterým byly pokládány cílené dotazy vztahující se ke konkrétním hodnoceným opatřením. Odpovědi byly zpracovávány koordinovaně a doplněny o relevantní interní dokumentaci a platné organizační směrnice. Celá analýza zabrala značné množství času a úsilí, což se projevilo jak v rozsáhlé dokumentaci, tak v počtu otázek a hodin věnovaných projektu.

Výstupy analýzy byly rozděleny do čtyř hlavních oblastí odpovídajících členění normy, konkrétně organizační opatření, opatření v oblasti lidských zdrojů, opatření fyzické bezpečnosti a technologická opatření. Pro každé z nich byla připravena podrobná tabulka obsahující identifikaci opatření, jeho vysvětlení podle normy, otázky zaměřené na aktuální stav a odpovědi zodpovědných osob. Dále byly uvedeny návrhy na očekávané změny a doporučení, stejně jako hodnocení stavu opatření s možnostmi *zavést*, *zavedeno* nebo *aktualizovat*. Nechyběl také sloupec s uvedenou metodou hodnocení, která většinou spočívala v dotaznících nebo rozhovorech, a označení navržené zodpovědné osoby, spolu s datumem posouzení a případné změny.

Metodologie zhodnocení spočívala v systematické přípravě této tabulky, formulaci relevantních otázek a navržení odpovědných osob. Následně byly naplánovány schůzky, během nichž se jednotlivé otázky podrobně řešily. Výstupy z těchto diskusí sloužily jako podklad pro formulaci závěrů v každé oblasti bezpečnostních opatření.

Tento dokument poskytl cenné vstupy pro tvorbu Prohlášení o aplikovatelnosti, které umožnilo stanovit aplikovatelnost jednotlivých opatření, přiřadit odpovědné osoby a odůvodnit neaplikovatelnost některých opatření.

3.3.1 Organizační opatření

V rámci asistovaného zhodnocení aktuálního stavu bylo identifikováno celkem 37 bezpečnostních opatření spadajících do kategorie organizačních opatření. Z tohoto počtu bylo **13 opatření zavedeno**, dalších **13 opatření vyžaduje aktualizaci** a **11 opatření je nutné nově zavést**.

Mezi zavedená opatření patří například odpovědnosti vedení, kde však dosud nebyla stanovena formální očekávání v oblasti informační bezpečnosti nebo chybí důvěrný kanál pro podávání zpráv o případném porušení bezpečnosti. Přípustné používání informací a souvisejících aktiv je částečně upraveno, avšak je nezbytné doplnit pravidla pro používání dalších aktiv a definovat jejich bezpečnou likvidaci. Oblast řízení přístupu vyžaduje zavedení kategorizace informací a formálního procesu žádosti o přístup.

V oblasti managementu identit bude nutné zvážit povolení možnosti více identit pro jednoho uživatele a případně zavést podpůrný proces pro zpracování změn informací o uživatelských identitách, ačkoli aktuálně tato potřeba není považována za prioritní. Informační bezpečnost ve vztazích s dodavateli je částečně řešena stávající směrnicí, přičemž je třeba zohlednit skutečnost, že většina dodavatelů představuje externí pracovníky společnosti.

Management informační bezpečnosti v dodavatelském řetězci ICT zatím postrádá plošně definované požadavky, které bude vhodné zvážit. Monitorování a přezkoumávání změn v rámci dodavatelských vztahů by mělo být rozšířeno o přezkoumávání auditních záznamů dodavatelů a záznamů o bezpečnostních událostech.

V oblasti plánování a přípravy na management bezpečnostních incidentů je doporučeno zvážit školení či certifikaci pracovníků odpovědných za reakce na incidenty a zavedení postupů pro identifikaci zkušeností a zlepšování současných postupů. Posuzování a rozhodování o bezpečnostních událostech pak vyžaduje zamyšlení nad rozdílem mezi bezpečnostními incidenty a softwarovými chybami (tzv. *bugy*), přičemž je nezbytné stanovit konkrétní schéma kategorizace těchto událostí.

Ochrana záznamů by měla být rozšířena o definici doby uchovávání jednotlivých kategorií záznamů a přípustných typů médií. Problematika ochrany soukromí a osobních údajů (PII) je řešena v kodexu chování a organizační směrnici zaměřené na informační bezpečnost. Nezávislé přezkoumávání informační bezpečnosti aktuálně probíhá s cílem identifikovat příležitosti ke zlepšení a potřeby změn v přístupu k bezpečnosti.

V rámci analýzy současného stavu bezpečnosti byla identifikována řada opatření, která dosud nebyla zavedena a jejichž implementace je zásadní pro zvýšení úrovně informační bezpečnosti ve společnosti. Mezi těmito opatřeními je klíčová definice rolí a odpovědností v oblasti informační bezpečnosti, neboť dosud nejsou jednoznačně

stanoveny odpovědnosti za ochranu informací a souvisejících aktiv, stejně jako vlastnictví těchto aktiv a úrovně přístupových oprávnění.

Další prioritou je oddělení povinností, kde je nutné identifikovat kritické procesy, které by měly být odděleny s ohledem na prevenci potenciálních rizik, například v oblasti správy plateb, verzování softwaru, přístupu k produkční infrastruktuře či ochraně před úniky citlivých údajů o pacientech. Rovněž je vhodné zavést proces systematického shromažďování informací o bezpečnostních hrozbách a konkrétních útocích, pokud to vzhledem k velikosti organizace a zaměření na zdravotnickou informatiku bude relevantní.

Dalším opomíjeným opatřením je proces vrácení aktiv, který by měl být formalizován a zahrnovat jasné pokyny pro evidenci vracených aktiv, ukončování přístupů a nakládání s informacemi či znalostmi souvisejícími s těmito aktivy. Rovněž chybí systematická klasifikace informací, včetně schémat označování citlivých dokumentů a nastavení odpovídajících přístupových práv.

V oblasti informační bezpečnosti při používání cloudových služeb je nutné zavést pravidla pro jejich bezpečné využívání, přezkoumávání a ukončování smluv, a to v souladu s normami ISO/IEC 27017 a 27018. Neméně důležitá je také implementace postupů pro shromažďování důkazů, zejména zálohování logů obsahujících potenciální informace o útocích a jejich zabezpečení proti přepisování.

Organizace by rovněž měla identifikovat veškeré zákonné, statutární, regulatorní a smluvní požadavky týkající se informační bezpečnosti a zajistit jejich plnění. To zahrnuje mimo jiné otázky platnosti digitálních podpisů, pečeti a certifikátů, přičemž minimálním krokem by mělo být zavedení digitálních podpisů. V neposlední řadě je třeba věnovat pozornost právům duševního vlastnictví, která dosud nejsou řešena. Je nutné definovat postupy pro jejich ochranu, identifikovat aktiva vyžadující ochranu duševního vlastnictví a zajistit dodržování práv jak externích subjektů, tak samotné organizace.

Posledním významným nezavedeným opatřením je připravenost ICT na zajištění kontinuity činnosti organizace. Vzhledem k tomu, že společnost nevlastní vlastní ICT infrastrukturu a využívá primárně cloudových služeb, například od společnosti Microsoft, která zajišťuje vysokou dostupnost, odolnost vůči výpadkům a kontinuitu ICT i v případě narušení, je nezbytné vytvořit komplexní plán pro zvládání kontinuity činností. Tento plán

by měl zohlednit nejen samotné technické aspekty, ale také organizační a procesní opatření pro minimalizaci dopadů případných incidentů na provoz společnosti.

3.3.2 Opatření v oblasti lidských zdrojů

V oblasti lidských zdrojů byla dosud zavedena pouze **2 bezpečnostní opatření, 3 opatření byla aktualizována a další 3 je nutné zavést**. Všechna opatření jsou přitom aplikovatelná.

Mezi zavedená opatření patří například zajištění povědomí, vzdělávání a školení o informační bezpečnosti, kde je nezbytné pokračovat v pravidelném vzdělávání zaměstnanců. Dalším zavedeným opatřením je proces podávání zpráv o událostech informační bezpečnosti. Přestože by bylo vhodné pracovníky znovu upozornit na tento mechanismus a poskytnout jim jasné pokyny, jak a komu incidenty hlásit, základní systém je již funkční.

Mezi nezavedená opatření, která je třeba implementovat, patří především prověřování pracovníků. Je nezbytné zavést systematické prověřování všech zaměstnanců a začít shromažďovat informace o uchazečích o zaměstnání. Dále je vhodné zavést ověřování úplnosti a přesnosti životopisů, přičemž je nutné určit osobu způsobilou k provádění tohoto ověřování. Součástí tohoto opatření by mělo být rovněž zavedení ověřovacího přezkoumání a definování postupu při nástupu pracovníka, pokud ověření ještě není dokončeno, včetně zmínění možných dopadů.

Dalším nezbytným opatřením je vytvoření procesu disciplinárního řízení, který doposud v organizaci chybí. Je třeba určit jasný postup, který bude aplikován v případě potřeby řešit závažné porušení pravidel či bezpečnostních incidentů. Posledním klíčovým opatřením je zavedení specifické politiky pro práci na dálku, což je pro organizaci s vysokým podílem práce na dálku zásadní. Tato politika by měla definovat pravidla pro práci s daty, stanovit vhodné pracovní prostředí a nástroje a jasně specifikovat hrozby a pokyny pro bezpečnou práci na dálku.

3.3.3 Opatření fyzické bezpečnosti

V oblasti opatření fyzické bezpečnosti bylo **zavedeno pouze 1 opatření, přičemž aktualizaci vyžaduje 7 opatření, další 3 je nezbytné zavést a 3 opatření jsou na společnost neaplikovatelná**.

Mezi zavedená opatření patří údržba zařízení. Ačkoli je tento proces již zaveden, doporučuje se zaměřit na kontrolu, která by zajistila, že se zařízením nebylo neoprávněně manipulováno a že funguje správně. Rovněž je vhodné upravit stávající směrnici tak, aby obsahovala detailnější postupy pro bezpečnou likvidaci zařízení, včetně paměťových médií.

Mezi klíčová nezavedená opatření, která je nutné implementovat, patří monitorování fyzické bezpečnosti. Organizace aktuálně nemá přehled o činnostech ostrahy, rozmístění kamer, zónách poplašného systému na příslušném patře a v budově, ani o použití kontaktních, zvukových a pohybových detektorů. Rovněž chybí informace o přístupech k monitorovacím systémům a o místech zabezpečených alarmem. Další nezbytné opatření představuje zavedení politiky prázdného stolu a prázdné obrazovky. Je nutné pracovníkům sdělit jasná pravidla týkající se tohoto opatření, včetně ochrany koncových zařízení pomocí zámků na klíče. Doporučuje se také zavést lepší kontrolu přístupu k tiskárnám a paměťovým médiím, nastavit pravidla pro konfiguraci vyskakovacích oken na obrazovkách a stanovit postupy pro situace, kdy je vybavení opuštěno.

Další nezbytné opatření se týká správy paměťových médií. Je třeba definovat všechny typy paměťových médií, jako jsou USB disky nebo CD, a stanovit politiku jejich správy, která by zahrnovala uchovávání, ochranu, odstraňování, šifrování, formátování a likvidaci těchto médií. Tato politika by měla být následně sdělena příslušným pracovníkům.

Na společnost se naopak nevztahují opatření, která jsou v jejím kontextu bezpředmětná. Mezi taková neaplikovatelná opatření patří práce v zabezpečených oblastech, které vzhledem k povaze činnosti organizace nejsou relevantní. Stejně tak je irelevantní problematika podpůrných služeb, jež jsou plně zajišťovány poskytovatelem. Bepředmětné je rovněž řešení bezpečnosti kabelových rozvodů, neboť společnost sídlí v pronajatých prostorách kliniky, která je součástí administrativní budovy, jejíž správu zajišťuje externí správce.

3.3.4 Technologická opatření

V oblasti technologických opatření bylo identifikováno celkem 34 opatření. Z toho bylo **zavedeno 10 opatření, aktualizaci vyžaduje 13, zavedení je nezbytné u 6 opatření a 5 opatření je pro společnost neaplikovatelných.**

Mezi zavedená opatření patří privilegovaná přístupová práva, která jsou jasně definována. Dále bylo zavedeno omezení přístupu k informacím, avšak doporučuje se zvážit, zda je možné implementovat dynamický management přístupu, například na základě geografické polohy, času nebo aktuálních rizik. Rovněž je zaveden management kapacit a management konfigurací, přičemž se doporučuje definovat standardní šablonu pro bezpečnou konfiguraci hardwaru, softwaru, služeb a sítí v souladu s politikou informační bezpečnosti organizace.

Další zavedené opatření se týká vymazání informací, kde je však třeba klasifikovat informace a specifikovat očekávané i nepřípustné chování při jejich využívání. V oblasti monitorovacích činností by bylo vhodné zvážit podpůrný proces pro zpracování změn informací týkajících se identit uživatelů. Mezi další zavedená opatření patří instalace softwaru na provozních systémech, používání kryptografie, oddělení prostředí vývoje, testování a produkce, nebo management změn. U posledního opatření je vhodné zvážit definování postupů pro nouzové a havarijní situace, pokud by pro organizaci mohly nastat.

Technologická opatření jsou tedy v určitých oblastech již implementována, avšak existuje prostor pro zlepšení a zavedení dalších kroků s cílem posílit bezpečnostní rámec organizace.

Mezi nezavedená technologická opatření, která je třeba zvážit a implementovat, patří zejména management technických zranitelností. V této oblasti by bylo vhodné u seznamu aktiv specifikovat informační zdroje používané pro identifikaci zranitelností jednotlivých softwarových komponent. Rovněž je nezbytné zavést zásady bezpečného programování a definovat způsoby detekce a postupy pro přijímání zpráv o zranitelnostech, a to jak interně, tak externě. Dále je vhodné zvážit vytvoření procesu pro management aktualizací softwaru a proces pro řízení technických zranitelností.

Synchronizace hodin představuje další klíčový bod, kde by měla být definována standardní referenční časová hodnota pro použití v rámci organizace. Oblast používání privilegovaných obslužných programů vyžaduje definici a identifikaci těchto programů a stanovení pravidel pro jejich autorizaci.

Další významné opatření se týká bezpečnostních požadavků na aplikace. Ačkoli existují dokumenty jako *Obecné požadavky na bezpečnost a účinnost*, tak ty se zaměřují na jiné oblasti. Při výběru softwarových nástrojů se sice využívají validační zprávy a protokoly,

avšak ty se zaměřují na ověření a očekávané výsledky, nikoli na bezpečnostní požadavky. Je tedy nezbytné zaměřit se na formulaci specifických bezpečnostních požadavků při pořizování aplikací.

Bezpečné programování představuje další klíčový prvek, který vyžaduje definování konkrétních zásad v závislosti na používaných programovacích jazycích.

Ochrana informačních systémů během auditního testování je zatím nedefinovanou oblastí. Ačkoli auditní testování jako takové organizace neprovádí, pokud by auditní testování zahrnovalo například penetrační testování prováděné externím dodavatelem, je nezbytné zavést pokyny pro průběh a ochranu systémů během těchto činností.

Mezi technologická opatření, která nejsou na společnost aplikovatelná a jejich zavedení nedává smysl, patří redundance vybavení pro zpracování informací. Tento přístup mohl být relevantní před deseti lety, avšak zcela opomíjí vývoj a současnou existenci cloudových služeb, které společnost využívá.

Bezpečnost sítí rovněž není relevantní, neboť společnost neprovozuje vlastní vnitřní síťovou infrastrukturu. Přístup k systémům a datům je zajištěn prostřednictvím vzdáleného připojení odkudkoli, včetně práce z domova, přičemž komunikace probíhá přes zabezpečené protokoly.

Podobně bezpečnost síťových služeb a oddělení sítí nejsou aplikovatelné, protože společnost nepoužívá žádnou interní síťovou architekturu a veškerá infrastruktura je umístěna v cloudových úložištích.

Filtrování webových stránek je rovněž bezpředmětné, jelikož společnost neprovozuje centralizované firemní prostředí, kde by podobná kontrola přístupu k webovým stránkám byla potřebná či efektivní.

4 NÁVRH ŘEŠENÍ

Tato část práce je věnována návrhu implementačního plánu, rozdělení průběhu do jednotlivých etap a samotnému průběhu implementace. Kapitola věnovaná plánování zahrnuje návrh harmonogramu, výběr a spolupráci s odbornými konzultanty, získání podkladových materiálů a šablon, jejich přizpůsobení pro tvorbu interních směrnic a povinné dokumentace potřebné k certifikaci. Současně je zde zohledněna kontrola souladu s dalšími legislativními požadavky.

Další kapitola popisuje zahájení implementace, která po úvodním zorientování probíhala podle detailního harmonogramu. Proces byl rozdělen do pěti etap, přičemž následovaly interní audit, první kolo certifikačního auditu, zapracování požadavků vzešlých ze zprávy tohoto auditu a příprava na druhé kolo. Samotný průběh druhého kola již není součástí této práce.

4.1 Plán implementace

4.1.1 Spolupráce s VUT

V březnu roku 2024 zahájila společnost proces vyhledávání odborných konzultantů se specializací na zdravotnickou informatiku, kteří by disponovali odbornými znalostmi v oblasti kybernetické a informační bezpečnosti. Hlavním cílem bylo získat expertní podporu při zavádění systému řízení informační bezpečnosti v souladu s normou ISO/IEC 27001:2023 a následné přípravě na certifikaci. Hledání vhodných odborníků bylo zahájeno na Podnikatelské fakultě Vysokého učení technického v Brně, konkrétně u vyučujícího bezpečnostních předmětů, který je zároveň vedoucím této diplomové práce. Na základě vzájemné dohody byla navázána výzkumná spolupráce s univerzitou, přičemž v průběhu následujících tří měsíců byla připravena smlouva a stanoveny podmínky spolupráce.

V rámci této spolupráce bylo dohodnuto, že výzkumný tým vypracuje potřebnou dokumentaci pro zavedení systému řízení informační bezpečnosti v souladu s normou ISO/IEC 27001:2023. Mezi stanovené dílčí cíle projektu patřilo zpracování Příručky ISMS, metodiky řízení aktiv, metodiky školení vlastníků aktiv a vedení organizace, metodiky analýzy rizik, katalogu relevantních zranitelností a hrozeb, obecných směrnic vycházejících z bezpečnostní politiky ISMS a formulářů povinné dokumentace ISMS.

Ke konci června 2024 byly výzkumnému týmu pod vedením Ing. Sedláka poskytnuty předem domluvené podklady, mezi něž patřila organizační struktura společnosti, procesy spadající pod schválený integrovaný systém managementu, strategický plán organizace a seznam aktiv. Výjimkou byl seznam aktiv, který v té době ve společnosti nebyl nijak definován ani dokumentován.

První návrh struktury seznamu aktiv byl členěn na kategorie, typy aktiv, konkrétní názvy aktiv a k nim přiřazené vlastníky (garanty). Následující *Tabulka 1* uvádí pouze *Kategorii*, *Typ aktiva* a v omezené míře i další rozdělení sloupce *Název aktiva*.

Tabulka 1: Seznam aktiv, první verze

Kategorie	Typ aktiva	Název aktiva	Vlastník/garant aktiva
Hardware	Stolní počítače a příslušenství		
	Server		
	Notebooky	operační systém	
	Soukromá zařízení	operační systém	
		mobilní zařízení	
	Tablety		
	Zdravotnická zobrazovací zařízení	typ 1	
		typ 2	
	Externí paměťové disky (nosiče dat)	paměťové disky	
		USB flash disk	
	Síťová infrastruktura		
	VMs		
	Fyzické přístupy	přístupové karty	
		přístupové klíče	
Software a licence	Mobilní a datové prostředky	SIM karty	
		USB modemy	
	Licence		
	Programovací software		
	Aplikační a systémový software		

	Software pro zdravotnické zobrazovací zařízení		
	Vývojové a testovací prostředí		
	Produkční prostředí		
	Testovací prostředí		
	Úložiště 1		
	Úložiště 2		
	API		
	VPN		
Data a informace	Datasety, lékařské informace	zpřístupněné datové sady	
		externí volně přístupné datové sady	
	Přístupové údaje	klíče	
		identity	
	Web		
	Životopisy	elektronická verze	
		fyzická verze	
	Smlouvy	elektronická verze	
		fyzická verze	
Služby	Anotovací nástroj, výsledky anotací		
	Poskytování softwaru ZP		
	AI modely		
Dokumentace a know-how	Confluence dokumentace	prostory	
		záloha	
	Procesy, organizační směrnice		
	Kodexy		
	Návod k použití ZP		

	Technické složky (klinická a technická dokumentace)	Confluence	
		úložiště 1	
		fyzická verze	
	Šablony		
	Zdrojové kódy		
	Vývoj a výzkum – projekty		
	Sales		
Objekty	Umělá inteligence		
	Kancelář a vybavení		
	Sídlo společnosti		

(Zdroj: Vlastní zpracování, poskytnuto společností)

Po akceptaci poskytnutých podkladů ze strany VUT byla zahájena příprava smluvených dokumentů. V průběhu letních měsíců probíhaly pravidelné konzultace, během nichž byl postupně vysvětlován význam jednotlivých dokumentů a poskytovány rady k jejich přizpůsobení specifickým potřebám analyzované společnosti. Nejprve byl vypracován návrh Bezpečnostní strategie, Příručky ISMS a bezpečnostních metodik převzatých z kybernetické vyhlášky, které byly využity jako podklad pro přípravu na shodu s požadavky Zákona o kybernetické bezpečnosti.

Přípravené návrhy dokumentů bylo nezbytné provázat s již existujícími relevantními organizačními směrnici a sjednotit v nich používanou terminologii. Nejvýraznější úpravy byly provedeny v části *Bezpečnostní strategie*, přičemž do hlavních cílů byla doplněna ochrana aktiv společnosti, konkrétně prostřednictvím vypracování *Plánu kontinuity činnosti organizace* (Business Continuity Plan) a *Plánu obnovy po havárii* (Disaster Recovery Plan). *Příručka ISMS* vyžadovala především provázání s existujícími procesy a organizačními směrnici, přičemž dobrým východiskem pro její strukturu byla již schválená *Příručka kvality*. Na základě této dokumentace byla vytvořena kostra nové příručky a doplněna kapitola vysvětlující vzájemné vztahy mezi jednotlivými prvky systému řízení bezpečnosti, vždy s navázáním na konkrétní dokument sloužící jako referenční vodítko pro auditora. V rámci této konzultace bylo rovněž upozorněno na nutnost zavedení sedmi základních procesů, mezi něž patří řízení rizik, řízení incidentů, řízení zranitelností, řízení změn, řízení konfigurací, řízení oprav a proces uvolnění. V době první konzultace měla společnost zavedenou pouze organizační

směrnici *Release Management*, která pokrývala proces uvolnění, řízení oprav a nepřímo i řízení konfigurací. Dále byla v platnosti organizační směrnice *Řízení rizik*, která však zahrnovala pouze analýzu a hodnocení rizik z pohledu kvality, nikoliv bezpečnosti. Organizační směrnice *Informační bezpečnost* se pouze stručně zmiňovala o procesu řízení incidentů, zatímco proces řízení zranitelností v dokumentaci společnosti zcela chyběl.

Během druhé konzultační schůzky byl předán zbývajícím nasmlouvané dokumenty a podklady. Obecné bezpečnostní směrnice, dále označované jako bezpečnostní metodiky, byly vypracovány v souladu se Zákonem o kybernetické bezpečnosti a jejich celkový počet činil 23. Tyto dokumenty byly připraveny jako šablony určené k doplnění o specifické procesy společnosti a následnému začlenění do stávajících směrnic. Přestože nejsou součástí povinné dokumentace ISMS, jejich vytvoření bylo klíčové pro přípravu na implementaci systému řízení bezpečnosti, a to zejména v oblastech řízení aktiv, bezpečnosti lidských zdrojů, řízení přístupu, bezpečného chování uživatelů, bezpečného předávání a výměny informací, fyzické bezpečnosti a kryptografické ochrany. Kromě bezpečnostních metodik byl poskytnut také dokument *Budování bezpečnostního povědomí*, šablona *Prohlášení o aplikovatelnosti*, šablona *Plán zvládání rizik*, která je považována za klíčový dokument pro auditní proces, a šablona zprávy z auditu určená pro interní audity, kterou bylo nutné upravit dle požadavků aktuální verze normy. Dále byl předán implementační harmonogram rozpracovaný na jednotlivé dny a seznam povinných a relevantních dokumentů nutných k zavedení systému řízení bezpečnosti.

Při třetí a čtvrté konzultaci již byla velká část doporučení zapracována a poskytnuté podklady převedeny do webového prostředí Confluence, kde k nim měli přístup všichni pracovníci společnosti. Diskutovány a vysvětleny byly nejasnosti týkající se detailního rozpracování seznamu aktiv, možnosti sjednocení nebo odstranění některých kapitol *Příručky ISMS* a oddělení klasifikace a řízení aktiv od samotné příručky. Rovněž byl analyzován harmonogram a plán implementace, který byl následně přepracován tak, aby odpovídal specifikům společnosti. Implementace byla rozvržena do jednotlivých etap, přičemž každá fáze měla trvat přibližně jeden měsíc. Plán vycházel z odhadované délky trvání jednotlivých činností, avšak vzhledem k omezeným zkušenostem v této oblasti docházelo k prodlevám, přeplánování termínů a častým aktualizacím již schválených verzí dokumentace.

4.1.2 Ganttův diagram

Ke grafickému znázornění harmonogramu budování systému bezpečnosti ve vybrané společnosti, zahrnujícího nejen zavádění a certifikaci dle normy ISO/IEC 27001:2023, byl využit Ganttův diagram (viz Příloha 1) a software GanttPRO. Tento diagram byl rozdělen do deseti hlavních částí, které reflektovaly klíčové fáze projektu: Zvažování zavedení ISO/IEC 27001:2023, Plán implementace, První etapa – říjen, Druhá etapa – listopad, Třetí etapa – prosinec, Čtvrtá etapa – leden, Pátá etapa – únor, březen a Certifikační audit – druhé kolo.

Plánování pomocí Ganttova diagramu bylo pravidelně aktualizováno a vždy měsíc dopředu podrobněji rozpracováno. Na základě konzultací byly průběžně přehodnocovány priority, což vedlo k úpravám harmonogramu. Zvláštní důraz byl kladen na rozpracování povinné dokumentace ISMS, která byla rozdělena do jednotlivých etap podle důležitosti. Dokumenty byly kategorizovány jako nejdůležitější, důležité a vhodné k vytvoření před interním auditem.

Kromě diagramu byl vypracován dokument *Plán implementace změny ISO/IEC 27001*, který sloužil jako přehled pro řízení kvality a usnadnění procesu schvalování a řízení změn v dokumentaci. Tento přehled obsahoval název dokumentu (nově vytvořeného nebo již existujícího), jazykovou verzi (českou nebo anglickou), odpovědnou osobu za jeho vytvoření, ověření a schválení, stav nebo fázi zpracování (draft, finální draft, valid), odkazy na související procesy a dokumenty, předpokládané datum platnosti, termín a rozsah školení pracovníků a určení osoby odpovědné za jeho realizaci.

Podrobnější obsah jednotlivých etap implementace je dále vysvětlen v kapitole 4.2 Implementace.

4.1.3 Penetrační testy

Penetrační testování představovalo vhodnou metodu ověření úrovně bezpečnosti infrastruktury společnosti a jejího přístupu k ochraně informačních aktiv. Vzhledem k omezeným finančním možnostem startupu nebylo reálné financovat takto nákladné testování z vlastních zdrojů. Naskytla se však příležitost využít plně hrazený program Digitální Evropy a Národního plánu obnovy, který umožňuje mikropodnikům získat

expertní podporu v oblasti kybernetické bezpečnosti. V rámci tohoto programu byla navázána spolupráce s expertním týmem CyberSecurityHub, přičemž první seznamovací schůzka proběhla na konci března 2024. Během této schůzky byly diskutovány očekávání, požadavky a podmínky spolupráce. Proces přípravy a podpisu smlouvy se následně protáhl až do července, přičemž klíčovým krokem ze strany společnosti bylo podepsání dohody o mlčenlivosti (NDA) všemi členy testovacího týmu. Již v rámci úvodních jednání bylo dohodnuto, že nejbližší možný termín pro realizaci penetračního testování připadne na srpen nebo září, tedy ještě před implementací první etapy systému řízení informační bezpečnosti. Harmonogram testování tak odpovídal plánovaným aktivitám.

Na přelomu srpna a září byla zahájena specifikace podmínek a rozsahu penetračních testů (tzv. *scope*). Kontaktní osobou za společnost a zároveň odpovědnou osobou za koordinaci průběhu testování a poskytování součinnosti byl určen CISO. Hlavním cílem testování bylo prověření kybernetické bezpečnosti serverové infrastruktury a softwarové aplikace společnosti z hlediska požadavků certifikace ISO/IEC 27001 a dalších souvisejících norem. Testování bylo zaměřeno na identifikaci potenciálních zranitelností, které by mohly být zneužity externím i interním útočníkem, a na formulaci doporučení pro jejich odstranění. Rozsah penetračního testu zahrnoval jak testování serverové infrastruktury, tak samotné aplikace.

Penetrační testování bylo zaměřeno na prověření bezpečnosti serverové instance využívané pro vývoj aplikace s reálnými uživateli a daty. Prioritou bylo identifikovat přístupové body, které by mohly být zneužity k neoprávněnému průniku do systému. Testování bylo realizováno v režimu *white-box*, což znamenalo, že testeré měli k dispozici všechnu potřebnou dokumentaci. Součástí testu bylo rovněž posouzení rizik a návrh doporučených opatření k eliminaci identifikovaných hrozeb.

V rámci přípravy testování byly definovány IP adresy testovaného serveru, časové rozmezí provádění testů (včetně konkrétních dat, možnosti nárazového testování a testování v pracovních dnech) a rozsah IP adres, ze kterých budou testy prováděny. Testování bylo prioritizováno na základě míry rizika zneužití jednotlivých zranitelností a jejich dopadu na bezpečnost infrastruktury. K prověření odolnosti systému byly využity pouze exploity s minimálním rizikem poškození provozovaných služeb. V případě, že by během testování nebyla identifikována žádná zranitelnost umožňující neoprávněný

přístup do systému, byl aplikován přístup *assumed breach*, simulující zero-day zranitelnost či jinou dosud neodhalenou chybu. Veškeré testovací scénáře a odpovídající úrovně oprávnění byly testovacímu týmu poskytovány bezpečnou cestou. Po úspěšném průniku do systému bylo provedeno hodnocení lokálních zranitelností a test možnosti eskalace oprávnění na úroveň administrátora (root/administrator). Součástí testování byla také analýza síly hesel pomocí kontrolního porovnání hashovaných hodnot z testovaného serveru.

Dále byly provedeny externí penetrační testy z prostředí internetu proti předem připravené instanci webového aplikaci naplněné testovacími daty. Prioritou bylo ověření bezpečnosti veřejně přístupných rozhraní, která by mohla být zneužita k neoprávněnému přístupu do systému. Testování bylo opět realizováno v režimu *white-box*, kdy testeré měli přístup nejen k relevantní dokumentaci, ale i ke zdrojovým kódům testované aplikace. Postup testování vycházel z metodiky OWASP Web Security Testing Guide a zahrnoval také posouzení rizik a návrh opatření ke zmírnění identifikovaných hrozeb. V rámci testování byla opět specifikována testovaná infrastruktura, IP adresy testovaného prostředí a rozsah adres, z nichž testy probíhaly. Testovací scénáře byly prioritizovány na základě rizika zneužití jednotlivých zranitelností a jejich potenciálního dopadu na bezpečnost systému.

Součástí dohody o provedení penetračního testu byla také specifikace obsahu závěrečné zprávy. Tato zpráva obsahuje potvrzení nezávislosti a odborné kvalifikace testerů, manažerské shrnutí výsledků testování včetně jeho délky a zaměření, popis použitých testovacích metod, technický popis identifikovaných zranitelností včetně jejich závažnosti, podrobný postup pro reprodukci nalezených zranitelností a doporučení k jejich odstranění. Na žádost zadavatele byla závěrečná zpráva zpracována v anglickém jazyce, a to s ohledem na plánovanou expanzi na zahraniční trh a možné bezpečnostní požadavky potenciálních zákazníků.

Na konci září byla zahájena příprava testovacího prostředí pro aplikaci, která zahrnovala vytvoření přístupů pro jednotlivé role a oprávnění v aplikaci, konkrétně pro role hosta, uživatele, administrátora organizace a administrátora. Součástí přípravy bylo také vytvoření potřebné technické dokumentace, včetně uživatelského návodu běžně poskytovaného uživatelům aplikace. Na serveru byl vytvořen jeden účet pro testera, přičemž přístup k němu měl omezený okruh pracovníků a všichni uživatelé měli stejná

oprávnění. Dále byl vygenerován SSH přístupový klíč a doplněna podrobnější neoficiální technická dokumentace k serveru, která zahrnovala návody na připojení k serveru (SSH, RDP, IPMI karta), strukturu serveru a seznam uživatelů.

Poté byla informována třetí strana, tedy náš poskytovatel prostorů a sítě, a jejich správce sítě. Byly telefonicky a e-mailem informovány dvě zodpovědné osoby za poskytovatele a dvě osoby za správce infrastruktury. Informace o důvodu provádění testů, jejich průběhu a nejvhodnějším čase pro jejich realizaci byly konzultovány a s těmito osobami byl dohodnut začátek testování a následně i jeho ukončení. Podklady a přístupové údaje byly po předchozí domluvě předány prostřednictvím uzamčených složek a přístupové údaje byly zaslány odděleně prostřednictvím SMS zprávy.

Samotné testování serveru a aplikace probíhalo nezávisle na sobě, a proto byly podklady a instrukce upřesněny v rozdílných termínech. Testování bylo dokončeno v listopadu a o několik dní později byla společnosti předána závěrečná zpráva o penetračních testech. Tato zpráva obsahovala důležité informace, jako prohlášení o důvěrnosti, vyloučení odpovědnosti a potvrzení nezávislosti testerů. Dále byla součástí zprávy i škála hodnocení závažnosti nalezených zranitelností a použitá testovací metodologie. Hlavní část zprávy se zaměřovala na shrnutí nálezů, přehled identifikovaných zranitelností a hodnotící kartu (viz *Tabulka 2*), kde každému nálezu byla přiřazena jeho závažnost, popis nálezu, důkaz v podobě screenshotu stránky nebo příkazového řádku a návrh na nápravu dané zranitelnosti.

Tabulka 2: Zranitelnost a její závažnost

ZÁVAŽNOST	DEFINICE
KRITICKÁ	Exploatace je přímočará a obvykle vede ke kompromitaci systému na úrovni správy. Doporučuje se okamžitě naplánovat opatření a aplikovat opravu.
VYSOKÁ	Exploatace je složitější, ale může vést k získání vyšších oprávnění a potenciálně ke ztrátě dat nebo výpadku. Doporučuje se co nejdříve naplánovat opatření a aplikovat opravu.

STŘEDNÍ	Zranitelnosti existují, ale nejsou snadno zneužitelné nebo vyžadují dodatečné kroky, například sociální inženýrství. Doporučuje se naplánovat opatření a aplikovat opravu po vyřešení prioritních problémů.
NÍZKÁ	Zranitelnosti nejsou zneužitelné, ale jejich odstranění by snížilo plochu útoku organizace. Doporučuje se naplánovat opatření a aplikovat opravu během příští plánované údržby.
INFORMATIVNÍ	Žádná zranitelnost neexistuje. Poskytují se dodatečné informace o zjištěních během testování, silných kontrolních mechanismech a další dokumentaci.

(Zdroj: Vlastní zpracování, poskytnuto společností)

Vzhledem k citlivosti obsahu dokumentu nebudou v této části uváděny žádné konkrétní nálezy. Interně byla tato zpráva projednána pouze v úzkém okruhu a fyzicky ji mají k dispozici pouze čtyři osoby: CISO, CTO, garant aplikace a současně SW Developer, a garant serveru a současně AI Engineer. Na základě této zprávy byly otevřeny nové úkoly zaměřené na opravu zranitelností střední závažnosti u serveru a kritických a vysokých závažností u aplikace. Vzhledem k tomu, že některé z těchto nálezů byly vysoce závažné, došlo k pozastavení vývoje aplikace a prioritnímu řešení nalezených zranitelností.

Následující tabulky ukazují počet identifikovaných zranitelností podle závažnosti. První tabulka popisuje zranitelnosti serveru (viz *Tabulka 3*) a zranitelnosti aplikace (viz *Tabulka 4*).

Tabulka 3: Zranitelnosti – server

KRITICKÁ	VYSOKÁ	STŘEDNÍ	NÍZKÁ	INFORMATIVNÍ
0	0	2	2	2

(Zdroj: Vlastní zpracování, poskytnuto společností)

Tabulka 4: Zranitelnosti – aplikace

KRITICKÁ	VYSOKÁ	STŘEDNÍ	NÍZKÁ	INFORMATIVNÍ
1	3	2	5	1

(Zdroj: Vlastní zpracování, poskytnuto společností)

4.1.4 Další legislativní požadavky a související normy

Tato diplomová práce se nezaměřuje pouze na bezpečnostní požadavky vyplývající z normy ISO/IEC 27001, ale, jak již naznačuje její název, na komplexní budování systému bezpečnosti. Z tohoto důvodu byly při zpracování brány v úvahu i další aktuální legislativní požadavky.

Na začátku roku 2024 se v bezpečnostní komunitě stalo velmi aktuálním tématem přijetí **evropské směrnice NIS2** a z ní vyplývající připravovaný nový Zákon o kybernetické bezpečnosti. Tento zákon se bude vztahovat mimo jiné i na regulované služby, mezi něž patří například výroba zdravotnických prostředků.¹⁹ Vzhledem k tomu, že nebylo zcela jednoznačné, zda se nové požadavky budou vztahovat i na analyzovanou společnost a v jakém rozsahu, bylo nutné tuto otázku dále zkoumat. Nejasnosti vyplývaly především z toho, že v době vznesení dotazu, tedy na začátku března 2024, byly právní předpisy stále ve fázi příprav a bylo pravděpodobné, že v průběhu času dojde k jejich dalším úpravám.

Za účelem získání relevantních informací byl vznesen dotaz v rámci výzvy a osvěty Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) na vedoucího Oddělení regulace soukromého sektoru, ten následně poskytl podrobné a srozumitelné vysvětlení k postupu, který umožní organizaci samostatně posoudit, zda naplňuje kritéria stanovená zákonem.²⁰

¹⁹ *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* [online], 2014. Česká republika [cit. 2025-03-10]. Dostupné z: <https://www.psp.cz/sqw/sbirka.sqw?cz=181&r=2014>. Sbírka zákonů.

²⁰ ŠVÉDA, Martin. 8. ledna. 2024. *Dotaz k identifikaci jako povinná osoba*. E-mailová komunikace.

Návrh vyhlášky o regulovaných službách obsahuje seznam regulovaných služeb, přičemž pro analyzovanou společnost je nejrelevantnější kategorie *Zdravotnictví – Výroba zdravotnických prostředků*. Pokud organizace poskytuje tuto službu a zároveň spadá do kategorie středního nebo velkého podniku, vztahují se na ni povinnosti vyplývající ze zákona.²¹ Další možností, která může vést k zařazení společnosti mezi regulované subjekty, je rozhodnutí NÚKIB, které by bylo učiněno v rámci správního řízení a dotčená organizace by byla o této skutečnosti informována. Základním mechanismem však zůstává samoidentifikace, tedy povinnost organizace sama posoudit, zda splňuje kritéria pro regulované subjekty.

Mezi relevantní ukazatele pro zařazení do regulovaných služeb patří zejména předmět činnosti odpovídající regulovaným službám, počet zaměstnanců (překročení hranice 50 zaměstnanců) a finanční ukazatele, jako je roční obrát nebo bilanční suma roční rozvahy přesahující 10 000 000 EUR, přičemž je nutné zohlednit i partnerské a propojené podniky.

Na základě těchto kritérií bylo vyhodnoceno, že analyzovaná společnost nenaplnuje podmínky pro zařazení mezi regulované subjekty dle návrhu Zákona o kybernetické bezpečnosti. Přesto bylo jako nejvhodnější postup zvoleno postupné zavádění bezpečnostních metodik, které byly poskytnuty Ing. Sedlákem v rámci konzultací. Tyto metodiky přímo vycházejí z požadavků Zákona o kybernetické bezpečnosti a umožní organizaci efektivně posílit její bezpečnostní opatření, aniž by na ni byly kladeny legislativní povinnosti regulovaného subjektu.

Hlavní činností společnosti je vývoj a výroba zdravotnického prostředku, což s sebou přináší odpovědnost za správu a bezpečné zacházení se zdravotními informacemi. Tento aspekt je tematicky upraven normou **ISO 27799 – Zdravotnická informatika**²², která stanovuje specifická bezpečnostní opatření v této oblasti.

V průběhu října 2024 byl zpracován zjednodušený kontrolní seznam, který vycházel z přílohy uvedené normy. Tento seznam byl vytvořen v zjednodušené formě, obsahoval

²¹ Úřad vlády České republiky. Návrh prováděcích právních předpisů [online], 2024 [cit. 2025-03-05]. Dostupné z: <https://www.odok.gov.cz/portal/veklep/material/ALBSCSSFKU7S/>.

²² ČSN EN ISO 27799: Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO 27002, 2017. Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

pouze název opatření, výběr odpovědi ano/ne (tedy zda bylo opatření zavedeno či nezavedeno) a odkaz na referenční interní dokument. Přestože analýza nebyla ke dni druhého certifikačního kola dokončena, byla zahrnuta do *Akčního plánu ISMS 2025*, s plánovaným termínem dokončení v říjnu 2025.

Již během implementace systému řízení informační bezpečnosti byla věnována pozornost specifickým kapitolám normy, které jsou v kontextu zdravotnické informatiky klíčové. Mezi tyto oblasti patří mobilní zařízení a práce na dálku, klasifikace informací, požadavky organizace na řízení přístupu, správa a řízení přístupu uživatelů, kryptografická opatření, zařízení, správa bezpečnosti sítě, data pro testování, bezpečnost informací ve vztazích s dodavateli, řízení bezpečnosti informací a jeho zlepšování a kontinuita bezpečnosti informací. Tyto aspekty jsou systematicky zapracovávány do interních procesů společnosti s cílem zajistit plný soulad s požadavky normy ISO 27799.

Další technickou normou, která v době zpracování této diplomové práce nebyla nová, avšak pro společnost se stala aktuální, byla norma **IEC 81001-5-1:2021** s názvem *Zdravotnický software a bezpečnost, účinnost a ochrana zdravotnických IT systémů*²³. Vzhledem k její relevanci byl v průběhu července 2024 zpracován kontrolní seznam požadavků, který umožnil detailní analýzu souladu společnosti s touto normou.

Tato část normy se zaměřuje především na bezpečnost v životním cyklu produktu zdravotnického prostředku, čímž se tematicky prolíná s bezpečnostním opatřením normy ISO/IEC 27001, konkrétně s požadavkem 8.25 *Životní cyklus bezpečného vývoje*. Z celkového počtu 53 tematických kapitol bylo 18 označeno jako nezavedené, přičemž zavedení systému řízení informační bezpečnosti pokryje čtyři z nich a dalších pět bude implementováno prostřednictvím vytvoření *threat modeling* neboli modelu hrozeb. Tento přístup je často redukován pouze na sestavení seznamu relevantních zranitelností, avšak jeho důsledná implementace zahrnuje komplexní analýzu rizik a návrh odpovídajících bezpečnostních opatření.

Zmapované chybějící požadavky byly systematicky zahrnuty do *Akčního plánu ISMS 2025*, přičemž do konce dubna 2025 je plánováno dokončení podrobnější analýzy hrozeb

²³ ČSN EN IEC 81001-5-1. Zdravotnický software a bezpečnost, účinnost a ochrana zdravotnických IT systémů – Část 5-1: Činnosti v životním cyklu produktu. 2022. Ženeva: Mezinárodní elektrotechnická komise.

a zranitelností v rámci životního cyklu zdravotnického prostředku. Následná implementace opatření bude probíhat až do konce listopadu 2025.

4.2 Implementace

Následující kapitoly detailně popisují rozplánované a korigované etapy budování systému bezpečnosti ve společnosti, přičemž každá etapa je zaměřena na konkrétní oblast implementace s cílem zajistit postupné a systematické zavedení všech požadovaných dokumentů a souvisejících opatření.

Tato část implementace již nebyla konzultována přímo s vedoucím práce Ing. Sedlákem, avšak vycházela z jeho poskytnutých podkladů a doporučení. V pozdější fázi implementace byla navázána spolupráce s odborným konzultantem specializujícím se na informační a kybernetickou bezpečnost ve zdravotnickém zařízení, který poskytl další odborné vedení a podporu při zavádění bezpečnostních opatření.

4.2.1 První etapa

Jedním z prvních oficiálních kroků v procesu implementace systému řízení informační bezpečnosti bylo sepsání a schválení ***Prohlášení vedení o zavádění ISMS***, které bylo již začátkem roku rozpracováno v podobě *project charteru*. Tento dokument byl následně oficiálně schválen a podepsán vedením společnosti, včetně sponzora projektu, a definoval očekávané klíčové výsledky a rozsah implementace ISMS.

Mezi klíčové výsledky byly zahrnuty především zásadní dokumenty, které tvoří základ systému řízení informační bezpečnosti, a to: *Asistované zhodnocení aktuálního stavu* (GAP analýza), *Bezpečnostní strategie*, *Průručka ISMS*, *Bezpečnostní metodiky*, *Zpráva o zhodnocení rizik*, *Plán zvládnutí rizik*, *Plán kontinuity činnosti*, *Roční plán školení a vzdělávání*, *Budování bezpečnostního povědomí*, *Plán a program interních auditů ISMS* a *Prohlášení o aplikovatelnosti*. Posledně jmenovaný dokument byl navíc zpracován také v anglické verzi jako *Statement of Applicability*, aby mohl být v případě potřeby poskytnut zahraničním zákazníkům nebo kolegům. Dalším klíčovým výsledkem definovaným v tomto dokumentu byla samotná implementace normy ISO/IEC 27001:2023 do souvisejících procesů společnosti, dále úprava infrastruktury

společnosti tak, aby odpovídala požadavkům této normy, a nakonec certifikace ISO/IEC 27001:2023 provedená nezávislým auditorem.

Současně s tímto prohlášením byla dokončena a následně v prvním týdnu daného měsíce schválena první verze **Bezpečnostní strategie**. Tento dokument zahrnoval vizi, principy, výzvy a hlavní cíle společnosti a jeho implementace byla provázána na akční plán, který v této fázi implementace ještě nebyl finalizován. Stejně jako ostatní dokumenty připravené výzkumným týmem z VUT, i *Bezpečnostní strategie* prošla přizpůsobením specifickým charakteristikám a požadavkům společnosti, aby odpovídala jejím potřebám a interním procesům.

Společnost se ve své vizi zavazuje zajistit bezpečné podmínky v kyberprostoru, které umožní hladké fungování informační společnosti. Klíčovým závazkem je neustálé rozšiřování expertní základny v oblasti informační a kybernetické bezpečnosti a posílení schopnosti čelit nejnovějším kybernetickým hrozbám. V rámci zabezpečení vlastní infrastruktury klade společnost důraz na zavedení ISMS a podporuje spolupráci a dialog s dalšími subjekty, včetně zahraničních organizací zabývajících se informační a kybernetickou bezpečností. Dále si klade za cíl efektivně zajišťovat bezpečnost sítí a kyberprostoru, ve kterém se pohybují její zaměstnanci i dodavatelé, a který je zásadní pro ekonomické a sociální zájmy organizace. Neméně důležitým aspektem strategie je spolupráce s akademickými a soukromými subjekty v oblasti výzkumu a vývoje zabezpečení informačních a komunikačních technologií.

Mezi základní principy společnosti patří ochrana základních lidských práv a svobod, komplexní přístup ke kybernetické bezpečnosti, budování důvěry a spolupráce s poskytovateli zdravotních služeb a rozvoj kapacit pro zajišťování kybernetické bezpečnosti.

Zmíněnými výzvami jsou například zajištění kybernetické bezpečnosti systémů AI v souladu s požadavky AI Act, což zahrnuje zajištění odolnosti vůči neoprávněným útokům, manipulaci s tréninkovými daty a eliminaci zranitelností systémů. Dalším významným aspektem je integrace a kompatibilita se zdravotnickými systémy, kde otevřená rozhraní přinášejí bezpečnostní rizika, zejména v oblasti souladu s bezpečnostními standardy zdravotnických zařízení. Mezi další výzvy patří narůstající kritičnost selhání informačních a komunikačních technologií, stále rostoucí množství

mobilního malware, otázka bezpečného skladování dat v nových prostředích a nízká digitální gramotnost koncových uživatelů.

Hlavní cíle společnosti zahrnují vytvoření metodologie pro hodnocení rizik v souladu se zaváděním ISMS, přičemž klíčovou součástí je průběžná analýza a aktualizace materiálů s ohledem na dynamicky se vyvíjející kybernetické hrozby. Společnost se dále zaměřuje na kontinuální sledování zabezpečení systémů, vypracování *Plánu kontinuity činností organizace* (Business Continuity Plan) a *Plánu obnovy po havárii* (Disaster Recovery Plan). Dalším strategickým bodem je pravidelné testování bezpečnosti, identifikace chyb a zranitelností v informačních systémech prostřednictvím penetračních testů a koordinace spolupráce s dodavateli zejména v oblastech vývoje a prodeje. V neposlední řadě je klíčovým cílem zvyšování odborných znalostí a školení zaměstnanců, a to nejen v oblasti informační a kybernetické bezpečnosti.

V první fázi implementace byla vytvořena ***Příručka ISMS***, která v této rané verzi ještě obsahovala samostatný dokument ***Politika ISMS***. *Příručka ISMS* byla vypracována na základě již existující *Příručky kvality* a doplněna o požadavky normy ISO/IEC 27001:2022. Struktura dokumentu byla rozdělena do 13 částí, počínaje úvodní částí, která obsahovala účel, základní informace, rozsah platnosti, odpovědnosti, definice pojmů a použitých zkratk. Hlavní část dokumentu se zaměřovala na obecné vysvětlení systému managementu informační bezpečnosti, včetně identifikace aktiv, analýzy rizik a přístupů k jejich zvládnutí, jakož i požadavků na dokumentaci, odpovědnosti managementu a plánování bezpečnostních opatření. Dokument rovněž zahrnoval kapitoly věnované lidským zdrojům, budování bezpečnostního povědomí a přezkoumávání kvalifikačních požadavků. Další části se věnovaly řízení bezpečnosti v oblasti nákupu, poskytování služeb a komunikace se zákazníky, přičemž závěrečná část obsahovala měření, analýzu a zlepšování ISMS, včetně interních auditů, monitorování a opatření k nápravě.

Politika ISMS byla v této fázi vytvořena jako samostatná podstránka *Příručky ISMS*, čímž s ní byla úzce provázána. Dokument definoval dlouhodobé strategické cíle v oblasti řízení bezpečnosti, které se soustředily na zajištění důvěrnosti, integrity a dostupnosti dat. *Politika ISMS* dále obsahovala analýzu rizik a opatření pro zajištění požadované dostupnosti dat a minimalizaci doby nedostupnosti služeb. Dokument rovněž zahrnoval dva diagramy, znázorňující strukturu dokumentace ISMS a blokové schéma

implementace a provozování ISMS. Po interním auditu a následně po prvním kole certifikačního auditu bylo navrženo zjednodušení dokumentace, přičemž cíle definované v *Politice ISMS* byly integrovány přímo do *Příručky ISMS*.

Dalším zásadním prvkem implementace byl ***Seznam aktiv***, který byl vytvořen již před zahájením výzkumné spolupráce s VUT. Po přehodnocení jeho granularity byl dokument schválen vedením společnosti a následně proběhlo školení vlastníků aktiv, čímž byl vytvořen základ pro efektivní řízení bezpečnostních opatření spojených s ochranou klíčových aktiv společnosti.

4.2.2 Druhá etapa

V listopadu 2024 byla zahájena druhá etapa implementace, jejímž hlavním cílem byla příprava podkladů pro interní audit. Klíčovým výstupem této fáze měly být především metodiky, konkrétně tři organizační směrnice: *Identifikace a hodnocení aktiv*, *Klasifikace a řízení aktiv* a *Analýza rizik ISMS*, a dále samotné zhodnocení a analýza aktiv. Přestože se této etapě původně věnovala značná pozornost, ukázalo se, že byla zpracována příliš obsáhle a složitě, a to nejen s ohledem na velikost společnosti, ale i na její zdrojové možnosti. Po konzultaci s interním auditorem byly všechny dokumenty kompletně přepracovány. Žádná z původních organizačních směrnic ani základních dokumentů nakonec nebyla schválena a jejich podoba byla výrazně změněna.

V rámci ***Hodnocení aktiv*** byly vytvořeny tři tabulky, které sloužily k rozdělení aktiv podle jejich významu a funkce. První tabulka obsahovala primární aktiva, druhá podpůrná aktiva I. úrovně a třetí podpůrná aktiva II. úrovně. Metodiku pro identifikaci a hodnocení aktiv poskytl výzkumný tým VUT, přičemž tato metodika definovala primární aktiva jako informace, služby a procesy, k nimž bylo nutné identifikovat garanty. Podpůrná aktiva zahrnovala technická aktiva, zaměstnance a dodavatele, kteří se podílejí na provozu společnosti. Hlavním rozdílem mezi úrovněmi podpůrných aktiv bylo, že aktiva II. úrovně jsou tvořena komponentami aktiv I. úrovně. Příkladem může být stolní počítač, který byl klasifikován jako aktivum I. úrovně, zatímco monitor nebo mobilní zařízení spadají do aktiv II. úrovně. Nicméně se ukázalo, že toto pojetí nebylo vhodné, a proto bude v následujících měsících upraveno.

Všechny tři tabulky obsahovaly detailní klasifikaci aktiv, přičemž u každého aktiva byly uvedeny následující údaje: ID aktiva, název, typ aktiva (primární/podpůrné), kategorie

(hardware, software a licence, data a informace, služby, dokumentace a know-how, objekty), lokalita neboli umístění, garant aktiva, popis aktiva, a dále informace o zpracování osobních údajů (ano/ne) a citlivých osobních údajů (ano/ne). Dále bylo u aktiv sledováno, zda jsou umístěna v kritické informační infrastruktuře (KII), významném informačním systému (VIS) nebo základní službě (ZS). V rámci hodnocení aktiv byla posuzována také triáda C-I-A (confidentiality – důvěrnost, integrity – integrita, availability – dostupnost), přičemž u každého aktiva byla stanovena úroveň důvěrnosti, integrity a dostupnosti (nízká, střední, vysoká, kritická) a následně byla určena celková hodnota aktiva odpovídající nejvyšší hodnotě v rámci této triády.

Samotné hodnocení aktiv bylo velmi náročné, neboť bylo identifikováno 20 primárních aktiv, 86 podpůrných aktiv I. úrovně a 16 podpůrných aktiv II. úrovně. Celková přehlednost dokumentu byla značně omezena nepřizpůsobivým zpracováním v prostředí Confluence, namísto specializovaného softwaru určeného pro správu aktiv. Dalším problematickým faktorem bylo rozhodnutí hodnotit aplikační, systémový a programovací software zvlášť, bez ohledu na frekvenci jeho využívání v organizaci. To vedlo k situaci, kdy i software, který byl využíván pouze jedním pracovníkem několikrát ročně, byl zahrnut do hodnocení jako samostatné aktivum, což dále komplikovalo přehlednost a efektivitu celého procesu.

Na takto strukturované hodnocení aktiv navazoval další klíčový dokument, ***Analýza rizik ISMS***, který se zaměřoval na identifikaci a hodnocení zranitelností, hrozeb a stanovení míry rizika. Tento dokument byl zpracován formou jednotné tabulky, jejíž sloupce zahrnovaly ID aktiva, typ aktiva (primární/podpůrné), kategorii aktiva (hardware, software a licence, data a informace, služby, dokumentace a know-how, objekty), lokalitu neboli umístění a garanta aktiva. V této části byla struktura dokumentu shodná s hodnocením aktiv, což by bylo přínosné zejména v případě využití vhodného softwarového prostředí, které by umožňovalo efektivní indexaci dat a neomezovalo rychlost práce s dokumentem.

Zásadní informace přineslo posledních pět sloupců *Analýzy rizik ISMS*, které se zaměřovaly na identifikaci zranitelností, jejich hodnocení (nízká, střední, vysoká, kritická), identifikaci hrozeb, hodnocení hrozeb (nízká, střední, vysoká, kritická) a výpočet míry rizika. Ta byla stanovena na základě pravděpodobnosti a dopadu

potenciálních hrozeb na aktiva společnosti, přičemž míra rizika byla vypočtena jako součin hodnoty aktiva, hodnoty zranitelnosti a hodnoty hrozby.

Pro demonstraci přístupu k hodnocení zranitelností a hrozeb lze uvést příklad primárního aktiva – zdravotnického zobrazovacího zařízení. V rámci analýzy bylo identifikováno deset základních a pravděpodobných zranitelností, ke kterým byly přiřazeny odpovídající hrozby. Mezi tyto zranitelnosti patřily například nedostatečné programy pravidelné výměny zařízení, které mohou způsobit poškození zařízení nebo médií, či náchylnost zařízení na vlhkost, prach a znečištění, což může vést k jeho poškození korozí nebo mrazem. Další zranitelnost byla nedostatečná péče při likvidaci, která zvyšuje riziko úniku citlivých dat, nebo nesprávné použití softwaru a hardwaru, vedoucí k poruše zařízení či celého systému. V rámci analýzy byla rovněž identifikována hrozba spojená se špatným povědomím o bezpečnosti, což může vést k nedodržení bezpečnostních zásad, dále absence odhlášení při spuštění pracovní stanice, což umožňuje neoprávněné používání zařízení. Mezi další zranitelnosti patřilo nekontrolované stahování a používání softwaru, které může vést ke stažení škodlivého kódu, nechráněné zařízení, které zvyšuje riziko neoprávněného přístupu, nebo nedostatečná kontrola aktiv mimo provozní prostory, což může vést k manipulaci s hardwarem či jeho krádeži. Každá identifikovaná zranitelnost byla kvantifikována, přičemž následně byla manuálně vypočítána míra rizika. V případě, že by stejný postup byl aplikován na všech 122 vydefinovaných základních aktiv společnosti, přičemž by ke každému aktivu bylo přiřazeno maximálně 10 zranitelností a hrozeb, výsledná tabulka by obsahovala téměř 5 000 individuálních položek zahrnujících hodnocení a míru rizika. Navíc každá z těchto hodnot byla navržena CISO a následně schválena garantem aktiva, což dále prodloužilo celkový čas zpracování *Analýzy rizik ISMS*. Z těchto důvodů analýza rizik nebyla dokončena před konáním interního auditu.

Před samotným auditem byla v průběhu listopadu připravena pouze základní struktura ***Plánu zvládnutí rizik***, který byl následně kompletně přepracován. Původní návrh byl totiž koncipován příliš detailně, což vedlo k jeho nepraktické aplikovatelnosti, a bylo proto nutné revidovat jeho pojetí tak, aby byl přehlednější a efektivně využitelný v praxi.

4.2.3 Třetí etapa

Interní audit systému řízení informační bezpečnosti společnosti proběhl začátkem třetí etapy, a to s cílem ověřit soulad s normou ISO/IEC 27001, identifikovat případné neshody a navrhnout doporučení pro zlepšení bezpečnostních opatření. Audit byl zaměřen na přezkoumání klíčových oblastí ISMS včetně kontextu organizace, vedení, plánování, provozu, hodnocení výkonnosti a kontinuálního zlepšování. Výstupem auditu bylo potvrzení, že společnost má zavedeny základní bezpečnostní procesy a řadu kontrolních mechanismů, nicméně byla identifikována oblast pro další rozvoj a optimalizaci.

Auditní proces zahrnoval kombinaci metod, mezi které patřily řízené rozhovory s klíčovými pracovníky, přezkoumání bezpečnostní dokumentace ISMS, fyzická obhlídka pracoviště a technické schůzky s vývojovým týmem, které se zaměřily na bezpečnostní aspekty umělé inteligence a cloud computingu. Významným bodem bylo také propojení ISMS se systémem řízení kvality (QMS), které může přispět k efektivnější správě a provázanosti bezpečnostních opatření.

Mezi hlavní zjištění auditu patřilo například nedostatečné zdokumentování interních a externích faktorů ovlivňujících ISMS, absence formálního definování odpovědností za jednotlivé role v oblasti bezpečnosti či složitá a obtížně spravovatelná metodika analýzy rizik. Bylo doporučeno zavést jednodušší a přehlednější systém řízení rizik, doplnit krizové scénáře a propojit analýzu rizik s plánem zvládání rizik. Dalším významným zjištěním byla absence pravidelného sledování výkonnosti ISMS a efektivity zavedených opatření, což vedlo k doporučení vytvoření standardizovaných metrik pro hodnocení bezpečnostních opatření.

V oblasti provozních opatření audit identifikoval nutnost zlepšení řízení přístupů, včetně zavedení pravidelných auditů přístupových oprávnění, formální správy aktiv a jasného definování odpovědností za jednotlivá aktiva. Rovněž bylo doporučeno rozšířit *Plán kontinuity provozu* (BCP) a *Plán obnovy po havárii* (DRP), aby společnost lépe reagovala na možné výpadky nebo bezpečnostní incidenty.

Doporučení auditu se zaměřila na konkrétní kroky, které by měly organizaci pomoci posílit úroveň bezpečnosti a zvýšit shodu s normou ISO/IEC 27001. Mezi hlavní návrhy patří zjednodušení analýzy rizik, zavedení efektivního řízení identit (IAM), formální propojení ISMS s QMS, pravidelný monitoring bezpečnostních incidentů a posílení

školení zaměstnanců v oblasti informační bezpečnosti. Kromě toho bylo doporučeno zavést přehled technických opatření a vytvořit dokument převodu požadavků ISMS, který by zajistil transparentnost při implementaci bezpečnostních opatření.

Celkově audit potvrdil, že společnost systematicky pracuje na zavedení ISMS, avšak před plánovanou certifikací je nutné provést řadu optimalizací. Implementace doporučených opatření přispěje k efektivnějšímu řízení bezpečnostních procesů, lepší ochraně citlivých dat a zvýšení celkové bezpečnostní odolnosti organizace. Vrcholovému vedení bylo doporučeno zvážit navržené změny a implementovat je do doby plánovaného certifikačního auditu, aby bylo dosaženo plného souladu s požadavky ISO/IEC 27001.

Během interního auditu byl společnosti vysvětlen význam dokumentu ***Prohlášení o aplikovatelnosti*** (*Statement of Applicability*) a zejména pojetí samotné aplikovatelnosti. Každé bezpečnostní opatření je v rámci tohoto dokumentu hodnoceno z hlediska své relevance pro společnost, nikoliv z pohledu, zda již bylo implementováno. Na základě tohoto vysvětlení bylo rozhodnuto o přepracování původního návrhu, který vznikl v předchozí fázi auditu. Nová verze vycházela z původní analýzy aktuálního stavu (*Asistované zhodnocení aktuálního stavu*), která byla strukturována dle opatření normy ISO/IEC 27002. Byly odstraněny sloupce týkající se aktuálního stavu, očekávaných změn a hodnocení, a naopak přidány informace o aplikovatelnosti opatření, odkazy na konkrétní interní dokumenty, které dané opatření vysvětlují, zdůvodnění případné neaplikovatelnosti a nové datum ověření.

Na základě doporučení auditora byla v prosinci rovněž zpracována ***Deklarace bezpečnosti informací***, která slouží jako veřejně přístupné prohlášení o politice informační bezpečnosti společnosti. Tento dokument, určený ke zveřejnění na webových stránkách, vyjadřuje hlavní zásady přístupu společnosti k ochraně důvěrnosti, integrity a dostupnosti informací, dodržování právních a normativních požadavků a závazku k neustálému zlepšování systému řízení bezpečnosti informací.

Bezpečnostní strategie společnosti byla doplněna o nový implementační dokument nazvaný ***Akční plán ISMS pro rok 2025***. Tento plán obsahuje konkrétní kroky a cíle, termíny jejich splnění a určení odpovědných a klíčových osob. Plán začíná vyznačením termínů prvního a druhého kola certifikačního auditu a dále obsahuje úkoly spojené s přípravou smluvních podmínek s poskytovatelem síťového připojení. Tyto podmínky mají společnosti usnadnit budoucí realizaci penetračních testů a zajistit přístup k síťovým

logům pro účely jejich analýzy, včetně určení kontaktních osob. Plán dále obsahuje úkol provést analýzu hrozeb a zranitelností (tzv. *threat modeling*) v souladu s normou IEC 81001-5-1:2021, revizi opatření zaznamenávání formou logů pro software a podpůrné aplikace uvedené v seznamu aktiv, a přezkum aktuálně přidělených přístupů včetně zavedení metodiky jejich udělování. Součástí plánu je také prověření aplikovatelnosti požadavků nařízení AI Act a vypracování plánu změn pro jejich naplnění, včetně jejich implementace podle priorit. Dále jsou v plánu definovány úkoly spojené s tvorbou *Plánu kontinuity činností* (BCP), *Plánu obnovy po havárii* (DRP) a organizační směrnice pro budování bezpečnostního povědomí a školení. Plán rovněž zahrnuje naplnění požadavků normy ISO 27799, zaměřené na bezpečnostní systémy ve zdravotnictví, aktualizaci organizační směrnice Informační bezpečnost o nové kapitoly týkající se přístupu BYOD (Bring Your Own Device) a integraci bezpečnostních metodik podle vyhlášky o kybernetické bezpečnosti.

Zásadní změnou v rámci revize aktiv bylo přepracování *Seznamu aktiv*. Ten byl rozdělen na dvě základní části: primární a podpůrná aktiva, a dále systematicky rozčleněn podle oblastí, procesů a informací. Nově byla zavedena vztahová propojení mezi primárními a podpůrnými aktivy, klasifikace dle C-I-A modelu stanovení hodnoty aktiva a jeho dopadu na business. Součástí seznamu podpůrných aktiv je nyní i samostatná tabulka přístupů, zvýrazněná žlutými buňkami. Tato tabulka obsahuje údaje o počtu uživatelů a privilegovaných uživatelů, metodě autentizace, využití dvoufaktorového ověření (2FA) a způsobu logování aktivit. Informace slouží k efektivnějšímu řízení a kontrole přístupů. Rozsah seznamu byl zároveň zmenšen, zejména u často využívaného softwaru, aby se zvýšila jeho přehlednost a udržitelnost.

Na základě doporučení vzešlých z interního auditu byly dále sjednoceny a přehodnoceny tři dříve samostatné procesy – *Identifikace a hodnocení aktiv*, *Klasifikace a řízení aktiv* a *Analýza rizik ISMS* do jediné konsolidované směrnice s názvem ***Správa aktiv***. Tento krok přispěl k přehlednosti a efektivnímu řízení této oblasti.

Společnost je mimo jiné povinna dodržovat legislativní požadavky v oblasti informační bezpečnosti, včetně Zákona o kybernetické bezpečnosti a GDPR. Zákony, nařízení a normy, které musí společnost splňovat jsou proto uvedeny v nově rozšířeném dokumentu ***Knihovna externí dokumentace***. Zajištění souladu s těmito požadavky je součástí ISMS a pravidelně se přezkoumává. Tento dokument obsahuje velmi široké

sekce od regulace zdravotnických prostředků, po nařízení o ochraně osobních údajů, doporučující a interpretační dokumenty MEDDEV (*Medical Devices Documents*), podpůrná dokumenty od koordinační skupiny pro zdravotnické pomůcky MDCG (*Medical Device Coordination Group*), pokyny SÚKL, Akt o umělé inteligenci, související české a slovenské zákony a technické normy pro zdravotnické prostředky a systém řízení informační bezpečnosti.

Koncem roku 2024 bylo ještě vydefinováno 20 základních rizikových scénářů:

- „Zranitelnost v podobě známé chyby v softwaru (*označení neuvedeno*) zapříčiní manipulaci se softwarem nebo zpřístupnění informací.
- Zranitelnost v podobě známé chyby v softwaru (*označení neuvedeno*) zapříčiní manipulaci se softwarem nebo zpřístupnění informací.
- Zranitelnost v podobě známé chyby v softwaru (*označení neuvedeno*) zapříčiní manipulaci se softwarem nebo zpřístupnění informací.
- Nesprávné nastavení parametrů pro autentizaci, chybné přidělení přístupových práv k jednotlivým složkám nebo stejně vysoká přístupová oprávnění na serveru mohou vést k chybě při používání a zneužití práv nebo oprávnění.
- Výpadek produkčního prostředí (konfigurační výpadek, nefungující komponenta atd.) vedou především k selhání poskytovatele služeb.
- Nesprávné použití hardwaru a softwaru zdravotnického zobrazovacího zařízení, špatné povědomí o jejich bezpečnosti nebo pouze nechráněné zařízení (zdravotnické zobrazovací zařízení a jeho příslušenství) může vést k neoprávněnému používání, manipulaci, krádeži nebo úniku citlivých dat. Běžným příkladem je zanechání zdravotnického zobrazovacího zařízení a jejího příslušenství spuštěné a bez dozoru, například na nějaké konferenci, výstavě nebo v nákupním centru.
- Chybějící politika bezpečného zacházení se soukromými zařízeními (také jako BYOD, *Bring Your Own Device* neboli Přines si své vlastní zařízení) může vést k úniku nebo poškození dat, ale také k bezpečnostním incidentům.
- Chybějící segmentace oddělující organizační informace od osobních informací uživatele může vést ke zpřístupnění nebo poškození informací.
- Chybějící nebo neúplné smluvní podmínky, závislost na externím poskytovateli a nedostatečná kontrola nad přístupovými logy a monitoringem sítě může vést

k možným právním problémům při incidentu, odmítnutí činností, nemožností detekovat narušení nebo nedostatečnou kontrolou nad nedostupností služby. Omezující je to například při provádění penetračních testů, kdy jsme jejich průběh oznamovali třetí straně nebo při vytváření nových přístupů na VPN.

- Sdílené fyzické prostory, nedostatečné nebo nedbalé používání fyzické kontroly přístupu do budov a místností a nedostatečné monitorování pohybu osob už od recepcie mohou vést ke krádeži nebo poškození vybavení, médií nebo dokumentů. Dochází například k přidržení dveří otevíraných kartou cizími pracovníky, kteří sdílejí kancelářské prostory, karty a klíče navíc neposkytuje správce kancelářských prostor, ale jeden z nájemců.
- Chybějící politika sdílení dokumentů, nesprávné nebo nedbalé umístění dokumentů obsahujících citlivé nebo osobní údaje (jako jsou například smlouvy nebo životopisy) mohou vést ke krádeži nebo zpřístupnění informací.
- Nedostatečné vedení přístupových a privilegovaných přístupových práv, chybné přidělení přístupových práv nebo nenastavené pravidelné kontroly uživatelských přístupů mohou vést ke zneužití práv nebo oprávnění a zpřístupnění informací.
- Nedostatečné odstranění v případě odchodu pracovníka nebo úprava přístupových práv včetně sloučení/vytvoření účtů například při změně jména uživatele může vést ke zpřístupnění a zneužití informací a firemního know-how.
- Nedostatečná kontrola přístupů nebo chybné přidělení přístupových práv a nekontrolovatelné používání CRM softwaru může vést k úniku citlivých dat a zpřístupnění firemního know-how.
- Chybějící opatření vycházející z oborové normy ISO 27799 - Systémy řízení bezpečnosti informací ve zdravotnictví, zaměřené na data, databáze a datové sady, může vést k jejich neoprávněné manipulaci, zneužití a zpřístupnění dat.
- Nedostatečná kontrola nad přístupovými logy a nesprávné nastavení parametrů může ztížit nebo znemožnit detekci narušení a vést k nedostatku důkazů při šetření bezpečnostních incidentů.
- Nedostatečné nastavení parametrů u všech (3) Microsoft Azure Subscriptions, které samotná platforma navrhuje (non-compliant policies), jako je například nenastavená detekce hrozeb pro správu identit a přístupů, nenastavené oddělování a limity pro privilegované role a administrátory, chybějící detekce, klasifikace

a označování citlivých dat nebo nedostatečná ochrana před DDoS útoky, což může vést ke zneužití slabín síťové infrastruktury, poškození nebo zpřístupnění dat nebo zneužití práv a oprávnění.

- Nedostatečná politika správy hesel, kdy především u soukromých zařízení nebo zdravotnického zobrazovacího zařízení a souvisejících softwarů tolerujeme slabé výchozí nebo žádné heslo. Samotná entropie hesel je kontrolována nevhodným způsobem a obměňování hesel není zavedeno. Toto může vést k neoprávněnému přístupu, zneužití, krádeži nebo úniku informací a know-how.
- Chybějící nastavení podmínek pro spolupráci s potencionálním zákazníkem, kdy není stanovena (a zavedena) povinná úroveň bezpečnosti, to může vést k odmítnutí spolupráce, nedostupnosti služby nebo možným právním problémům při bezpečnostním incidentu. Vytvoření takového dokumentu ulehčí a urychlí budoucí uzavírání spolupráce.
- Nedostatečné nebo nedostatečně aktuální bezpečnostní školení může vést k nesprávnému používání softwaru a hardwaru nebo nevědomému zpřístupnění informací. Budování bezpečnostního povědomí by se proto mělo věnovat více pozornosti.²⁴

Tyto rizikové scénáře byly více rozpracovány v následující čtvrté etapě.

4.2.4 Čtvrtá etapa

Čtvrtá etapa implementace systému řízení informační bezpečnosti byla zahájena v lednu roku 2025 a představovala závěrečnou fázi přípravy před prvním kolem certifikačního auditu. V rámci této etapy bylo plánováno dokončení a úprava dokumentu *Analýza rizik ISMS* a na něj navazujícího dokumentu *Plán zvládání rizik*. Současně byly prováděny náhodné fyzické kontroly koncových zařízení a kancelářských prostor za účelem ověření souladu s bezpečnostními opatřeními. V této fázi došlo rovněž k rozšíření jedné ze stávajících organizačních směrnic, konkrétně směrnice *Interní audit*, a hlavní důraz byl kladen na proškolení zaměstnanců v oblasti nově schválených dokumentů a organizačních směrnic, které tvoří základ systému řízení informační bezpečnosti ve společnosti.

²⁴ Poskytnuto společností.

Analýza rizik ISMS zahrnuje identifikaci, hodnocení a řízení rizik ISMS, která mohou ohrozit bezpečnost informačních aktiv organizace. Cílem je odhalit potenciální hrozby a zranitelnosti, stanovit míru rizika a navrhnout opatření k jejich minimalizaci. Identifikaci rizik, jejich hodnocení a bezpečnostní opatření navrhuje CISO, který také pomůže každému vlastníkovu rizika pochopit a upřesnit parametry. Vlastník rizik navrhuje nebo rozporuje navržené hodnoty a opatření, CTO je ověřuje a CEO schvaluje.

Identifikace zranitelností a hrozeb se zaměřuje na odhalování všech relevantních hrozeb a zranitelností, jež mohou ohrozit bezpečnost informačních aktiv společnosti. Tento proces zahrnuje identifikaci vnitřních a vnějších hrozeb, jako jsou kybernetické útoky, přírodní katastrofy nebo lidské chyby, a zároveň se hodnotí zranitelnosti systémů, procesů a lidí, které mohou umožnit těmto hrozbám proniknout a způsobit škody. Identifikace zranitelností a hrozeb je základem pro následné hodnocení a řízení rizik ISMS, která mohou ovlivnit bezpečnost organizace.

Tabulka *Analýza rizik ISMS* eviduje ID rizika (označováno Rxx), Rizikový scénář, ID primárního aktiva (označováno PAxx), ID souvisejícího podpůrného aktiva (označováno SAxx), Vektor útoku, Pravděpodobnost rizikového scénáře (1 - Nízká, 2 - Střední, 3 - Vysoká, 4 - Kritická), Dopad (1 - Nízký, 2 - Střední, 3 - Vysoký, 4 - Kritický), Míru inherentního rizika, Řízení rizik (akceptace, snížení, přenesení, pozorování), ID bezpečnostního opatření, Bezpečnostní opatření, Míru reziduálního rizika, Vlastníka rizika a Termín splnění.

Analýza rizik ISMS vychází z identifikovaných hrozeb a zranitelností, které jsou podrobně uvedeny v následujících tabulkách převzatých z normy ISO/IEC 27005:2023. Tyto seznamy poskytují základ pro hodnocení potenciálních rizik a umožňují přiřadit konkrétní zranitelnosti k odpovídajícím hrozbám, čímž usnadňují tvorbu rizikových scénářů.

Identifikace rizik zahrnuje zjišťování potenciálních rizik, která mohou ohrozit bezpečnost informačních aktiv společnosti. V rámci toho byly vytvářeny rizikové scénáře, ty jsou identifikována na základě relevantních kombinací aktivum-zranitelnost-hrozba. Každý rizikový scénář je popsán a přiřazen k odpovídajícím primárním a souvisejícím podpůrným aktivům. Vektor útoku popisuje, zda se jedná o rizikový scénář z pohledu externího útočníka, zda jde o interní pochybení nebo kombinace interní/externí.

Identifikace a hodnocení rizik a samotné rizikové scénáře zohledňují proběhlé kybernetické bezpečnostní incidenty, bezpečnostní audit a závěry z penetračního testování.

Hodnocení rizik zachycuje seznam hrozeb působících na aktiva a stanovuje příslušná každému zranitelnému místu a hrozbě. U hodnocení rizik si klademe na úkol snížení rizik na přijatelnou úroveň, respektive akceptaci zbytkových rizik tam, kde je jejich minimalizace neefektivní.

Analýza rizik ISMS stanovuje závažnost rizik na základě dvou klíčových faktorů – pravděpodobnost rizikového scénáře a dopad, každá z těchto hodnot je posuzována pomocí čtyřstupňové škály: 1 - Nízký, 2 - Střední, 3 - Vysoký, 4 - Kritický. Pravděpodobnost rizikového scénáře vyjadřuje výpočet hrozby a zranitelnosti. Tento přístup je jednodušeji uchopitelné vyjádření pravděpodobnosti výskytu rizika. Dopad pro každý rizikový scénář je nejvyšší hodnota souvisejícího podpůrného aktiva. Míra inherentního rizika se vypočítá jako součin pravděpodobnosti rizikového scénáře a dopadu, slouží jako podklad pro návrh a implementaci vhodných bezpečnostních opatření. Míra reziduálního rizika vyjadřuje součin snížené pravděpodobnosti rizikového scénáře, které se sníží po zavedení navrženého bezpečnostního opatření, a dopadu, který je v kontextu daného rizikového scénáře stejný.

Toto vyjadřují následující vzorce:

Míra inherentního rizika = Pravděpodobnost rizikového scénáře x Dopad

Míra reziduálního rizika = Pravděpodobnost rizikového scénáře (nižší po zavedení bezpečnostního opatření) x Dopad (nezměněná hodnota)

Zvládání a řízení rizik ISMS zahrnuje identifikaci bezpečnostních opatření vhodných k identifikovaným rizikům. Každému rizikovému scénáři je přiřazen konkrétní způsob řízení rizik, mezi které patří akceptace, snížení, přenesení nebo pozorování, odvíjí se z hodnoty míry inherentního rizika.

Možnosti řízení rizik:

- Akceptace – Pokud je splněno jedno nebo více kritérií přijetí rizika, je možné rozhodnout, zda je riziko akceptováno, a připravit se na zvládnutí jakýchkoli negativních dopadů v případě, že riziko nastane. Kritéria jsou:
 - Míra inherentního rizika je nízká.

- Náklady na implementaci a provoz bezpečnostních opatření by překročily potenciální ztráty spojené s možnými důsledky rizika.
- Je velmi obtížné implementovat požadovaná bezpečnostní opatření.
- Jsou nedostupné prostředky (finance, lidské zdroje, čas) pro implementaci požadovaných bezpečnostních opatření.
- Přenesení – Příslušné činnosti a opatření jsou převedeny na třetí strany, jako jsou například externí dodavatelé.
- Snížení – Použijí se vhodná bezpečnostní opatření k snížení rizika na přijatelnou úroveň neboli míru reziduálního rizika.
- Pozorování – Sledují se změny hodnoty rizika v průběhu času z hlediska dopadu a hrozby.

Tabulka 5: Míra inherentního rizika a mez přijatelnosti

Míra inherentního rizika		Popis
do 6	akceptace, pozorování	Riziko je považováno za akceptovatelné nebo je vhodné pro sledování změn hodnoty rizika v průběhu času.
6-12	snížení, přenesení	Riziko by mělo být zmírněno. Riziko lze snížit pomocí méně náročných bezpečnostních opatření. V případě vyšších nároků nebo nemožnosti implementovat bezpečnostní opatření lze riziko přenést.
nad 12	snížení	Riziko je nepřijatelné a musí být okamžitě přijata opatření ke snížení na přijatelnou úroveň. Takové riziko musí být řešeno co nejdříve.

(Zdroj: Vlastní zpracování, poskytnuto společností)

Podle rozhodnutí vedení je hodnota 6 považována za horní mez přijatelnosti rizika. Součástí této fáze je také návrh bezpečnostních opatření, která vedou ke snížení míry reziduálního rizika na přijatelnou úroveň. U každého rizikového scénáře je stanoven vlastník rizika, který je odpovědný za jeho implementaci, a určen termín splnění navržených bezpečnostních opatření. Tento strukturovaný přístup zajišťuje efektivní řízení rizik v souladu s cíli ISMS. Cílem těchto kroků je snížit hodnotu míry reziduálního rizika na přijatelnou úroveň.

Zvládání a řízení rizik ISMS tvoří základ pro navazující **Plán zvládání rizik**. Tento plán rozpracovává bezpečnostní opatření s cílem zajistit systematické a efektivní řízení identifikovaných rizik.

V rámci zavedení systému řízení bezpečnosti informací jsou z pohledu zvládání rizik využity následující činnosti: aplikování vhodných opatření, vědomé a objektivní akceptování rizik za předpokladu, že naplňují politiku společnosti a kritéria pro akceptaci rizik, vyhnutí se rizikům aplikací nápravných opatření, přenesení rizik spojených s činností společnosti na třetí strany.

Plán zvládání rizik je základní dokumentem, který specifikuje bezpečnostní opatření identifikovaných v rámci dokumentu *Analýza rizik ISMS*. *Plán zvládání rizik*, jednotlivá bezpečnostní opatření a jejich parametry navrhuje CISO. Zodpovědná osoba navrhuje nebo rozporuje navržené hodnoty a opatření, CTO je ověřuje a CEO schvaluje.

Bezpečnostní opatření specifikují konkrétní kroky, které společnost přijímá, aby minimalizovala identifikovaná rizika. Priorita stanovuje důležitost daného opatření, je vyjádřena číselnými hodnotami 1-3, přičemž 1 značí nejvyšší prioritu, která vyžaduje okamžitou implementaci, 2 označuje střední prioritu a 3 nízkou prioritu, která může být realizována později. Relevantní riziko odkazuje na ID relevantního rizika z dokumentu *Analýza rizik ISMS*. U každého bezpečnostního opatření je uvedená zodpovědná osoba a termín splnění, zodpovědná osoba zajišťuje, že opatření bude realizováno podle plánu a včas. Ve sloupci Jira Task je uveden odkaz na konkrétní úkol v nástroji pro správu projektů, v samotném tasku je uveden aktuální stav požadavku (To Do, In Progress, In Review, Done). Zdroj může být lidský nebo finanční. Pokud je zdroj interní uvádí se v jednotkách MD (man-day). Pokud je však zdroj externí, například financování od třetích stran nebo náklady na externí služby, uvádí se v Kč. Tato klasifikace byla zavedena s cílem zachovat diskrétnost ohledně interního odměňování jednotlivých pracovníků.

Tabulka *Plán zvládání rizik* eviduje ID bezpečnostního opatření (označováno jako SMxx), Bezpečnostní opatření, Prioritu (1-3), Relevantní riziko, Zodpovědná osoba, Termín splnění, Jira Task (odkaz na relevantní tiket), Zdroj (lidský, finanční). *Plán zvládání rizik* je dynamický a pravidelně aktualizovaný, aby reflektoval změny v rizicích a stav odpovídajících bezpečnostních opatření.

V průběhu zpracování výše popsaných dokumentů také probíhaly již zmíněné kontroly koncových zařízení a kanceláře, ty probíhaly dvěma způsoby. První byly náhodně vybraní pracovníci, kterým byly pokládány otázky relevantní informační bezpečnosti, například kde najdou platnou a aktuální dokumentaci týkající se informační bezpečnosti, zdali mají přístup k této dokumentaci, jsou-li garantem nějakého aktiva a jaké mu z toho plynou povinnosti, jaké jsou postupy při bezpečnostním incidentu nebo při žádosti o přístupy, co jsou to osobní údaje a co citlivé údaje, jak správně reagovat na podvodný e-mail, otázky týkající se politiky hesel a jiné. Druhý způsob kontroly byla spíše dlouhodobější kontrola dodržování pravidel prázdného stolu pro papírová a přenosná paměťová média a pravidel prázdné obrazovky a zajištění, aby koncové zařízení bylo vždy uzamčeno při opuštění pracovního místa.

Byla také aktualizovaná směrnice *Interní audit* s cílem stanovení požadavků a kritérií na roční interní audit informační bezpečnosti, a to požadované kvalifikace interního auditora, plánování a průběhu auditu, obsahu zprávy a vyhodnocení auditů. Tato směrnice již existuje a vztahuje se na všechny oblasti a procesy systému řízení kvality, proto bylo jednodušší a rychlejší integrovat do ní i systém řízení informační bezpečnosti.

4.2.5 První kolo certifikačního auditu

První kolo certifikačního auditu proběhlo na začátku února 2025. Audit byl realizován dvěma auditory, konkrétně vedoucím auditorem označeným jako *A* a dalším členem auditního týmu označeným jako *B*. Kromě úvodního zahajovacího setkání a závěrečného shrnutí výsledků, kterých se účastnil i vrcholový management společnosti, byl samotného průběhu auditu přítomen především pracovník zodpovědný za informační bezpečnost (CISO) a manažer kvality (QM).

Plán prvního kola certifikačního auditu byl společnosti poskytnut přibližně týden před jeho konáním. Částečný výňatek z tohoto plánu je uveden v *Tabulce 6*.

Tabulka 6: Plán prvního stupně certifikačního auditu

Datum/čas	Procesy/Činnosti/Požadavky	Zúčastněné osoby	Auditor
8:30	Zahajovací setkání Seznámení agendou programu auditu	Management	A, B

	• Potvrzení plánu rozsahu a případně i vlastní agendy auditu		
9:00	Prezentace současného stavu ISMS • Seznámení s jednotlivými kroky, které společnost přijala ke v rámci implementace ISMS	Osoby odpovědné za ISMS	A, B
9:30	Systém ISMS: Požadavky podle 4.1 (kontext), 4.2 (zainteresované strany), 4.3 (rozsah systému managementu), 4.4 (systém managementu informační bezpečnosti) + A.5.9 (inventář informací a souvisejících aktiv) a A.5.12 (klasifikace informací) Jedná se o přezkoumání důkazů k základním požadavkům k uvedeným požadavkům normy.	Osoby odpovědné za ISMS	A, B
10:30	ICT organizace – stručná prezentace ICT infrastruktury organizace (s přihlédnutím ke klíčovým technologiím, míře využívání externích služeb a cloudových řešení)	Osoby odpovědné za ICT	A, B
11:00	Vůdčí role • 5.1 Vůdčí role a závazek • 5.2 Politika • 5.3 Role, odpovědnosti a pravomoci v rámci organizace	Osoby odpovědné za ISMS	A
11:00	Plánování • 6.1 Činnosti zaměřené na rizika a příležitosti • 6.2 Cíle informační bezpečnosti a plánování jejich dosažení • 6.3 Plánování změn	Osoby odpovědné za ISMS	B
12:00	Polední přestávka	---	A, B
12:30	Zpracování výsledků, koordinace týmu	---	A, B
13:00	Provozování • 8.1 Plánování a řízení provozu • 8.2 Posuzování rizik informační bezpečnosti • 8.3 Ošetření rizik informační bezpečnosti	Osoby odpovědné za ISMS	A

13:00	Podpora • 7.1 Zdroje • 7.2 Kompetence • 7.3 Povědomí • 7.4 Komunikace • 7.5 Dokumentované informace	Osoby odpovědné za ISMS	B
14:15	Přezkoumání připraveného Prohlášení o aplikovatelnosti: • Rozsah aplikovaných a vyloučených požadavků • Zdůvodnění vyloučení požadavků • Odkazy na vypracované/zavedené bezpečnostní politiky Jedná se o přezkoumání důkazů k základním požadavkům k uvedeným požadavkům normy.	Osoby odpovědné za ISMS	A
14.15	Hodnocení výkonnosti • 9.1 Monitorování, měření, analýza a hodnocení • 9.2 Interní audit • 9.3 Přezkoumání vedením Zlepšování • 10.1 Neustálé zlepšování • 10.2 Neshody, nápravná opatření	Osoby odpovědné za ISMS	B
15:30	Otevřené a nedokončené položky	Podle potřeby	A, B
16:00	Zpracování výsledků 1. st. auditu	---	A, B
16:30	Shrnutí auditu a prezentace výsledků 1.st auditu	Management	A, B
17:00	Ukončení 1.st auditu		

(Zdroj: Vlastní zpracování, poskytnuto společností)

Do harmonogramu auditu bylo ještě před samotnou prezentací současného stavu společnosti zařazeno úvodní seznámení auditorů s vyvíjeným zdravotnickým prostředkem. Cílem tohoto kroku bylo umožnit auditorům lépe porozumět charakteru nabízených služeb, velikosti a rozsahu činností společnosti a tím i kontextu, ve kterém je systém řízení informační bezpečnosti implementován.

Samotný audit se zaměřoval zejména na systém řízení informační bezpečnosti, jak je popsán v dokumentu *Příručka ISMS*. Konkrétně byly hodnoceny oblasti, jako je stanovený rozsah ISMS, kontext organizace, role vrcholového vedení, plánování, provozní řízení, podpora, hodnocení výkonnosti a procesy zlepšování. Dále byly přezkoumány klíčové dokumenty, včetně *Seznamu aktiv*, *Analýzy rizik ISMS* a *Plánu zvládání rizik*. Významná pozornost byla věnována také dokumentu *Prohlášení o aplikovatelnosti*, kde byla detailně ověřována implementace jednotlivých bezpečnostních opatření, jejich odůvodnění vyloučení a případná neaplikovatelnost v kontextu analyzované společnosti.

Ve zprávě z prvního kola certifikačního auditu bylo zaznamenáno celkem sedm nedostatků. Tyto nedostatky byly klasifikovány jako požadavky na doplnění nebo doložení důkazů o implementaci konkrétních opatření, k nimž byl v době auditu poskytnut pouze částečný důkaz. Všechna následující zjištění byla vedena jako tzv. *findings* a musí být plně odstraněna a doložena do druhého kola certifikačního auditu:

- „Kontext – V předložené dokumentaci (Příručka, Bezpečnostní strategie) lze interní/externí aspekty identifikovat, nicméně ucelený popis dohledán nebyl.
- Rozsah ISMS – Aktualizovat rozsah ISMS v příručce podle dohody ze zahajovacího jednání.
- Identifikace a kritéria procesů ISMS – Procesy jsou identifikovány pouze v „makropohledu“ a metriky jsou aktuálně zaměřeny zejména na zavádění ISMS.
- Prohlášení o aplikovatelnosti – Aktuálně předložené PoA je z XII/2024, mezi tím došlo k progresu (opatření uváděná jako rozpracovaná již byla dokončena a nebo budou před zahájením 2. stupně) – je nutno aktualizovat PoA.
- Plánování – Je zapotřebí formulovat vhodné příležitosti k opatřením.
- Interní audit – Je zapotřebí přepracovat zprávu z provedení interního auditu ISMS tak, aby zohledňoval všechny požadavky podle 9.2.1 a 9.2.2.
- Přezkoumání – Je zapotřebí dopracovat dokumentovanou informaci pro vstup přezkoumání vedením v rozsahu podle 9.3.2. Je zapotřebí dopracovat dokumentovanou informaci s výsledky z přezkoumání vedením v rozsahu podle 9.3.3²⁵

²⁵ Poskytnuto společností.

Během prvního kola certifikačního auditu byly kromě formálně zaznamenaných nedostatků identifikovány také tzv. *příležitosti ke zlepšování* (Opportunities for Improvement, OFIs). Celkem byly zaznamenány tři takové příležitosti:

- „Rozhraní a závislosti mezi činnostmi organizace a činnostmi vykonávanými jinými organizacemi. Je vhodné tuto problematiku detailněji popsat v Příručce.
- Kontakt se zájmovými skupinami – Přesněji definovat workflow schvalování kontaktu se zájmovými atd. skupinami (odpověď v PoA není jasná).
- Plánován – Zlepšit provázanost Cílů definovaných v Akčním plánu 2025 s Plánem zvládání rizik, rev.1 a Analýzou rizik, rev.1.“²⁶

Certifikační audit prvního stupně trval celkem osm hodin a naplnil očekávaný výsledek. Na základě jeho průběhu bylo rozhodnuto o pokračování v certifikačním procesu a realizaci druhého stupně certifikačního auditu.

4.2.6 Pátá etapa

Na následující dva měsíce, které zbývaly do uskutečnění druhého kola auditu, byl vytvořen podrobný plán. Ten byl zpracován v prostředí Confluence formou nové samostatné stránky, kde byly systematicky zaznamenány veškeré poznámky a poznatky z auditu. Tyto informace byly seřazeny dle priorit, přičemž nejdůležitější body byly uvedeny na začátku. Celá struktura byla přehledně zpracována ve formě kontrolního seznamu (*checklistu*), který sloužil jako nástroj pro sledování plnění jednotlivých úkolů a přípravu na druhé kolo auditu.

- Findings
- OFIs
- Rychlé změny
- Náročnější změny
 - Základní dokumenty
 - Organizační směrnice
 - Prohlášení o aplikovatelnosti – všechna opatření, stav, očekávaná změna

²⁶ Poskytnuto společností

Stránka s úkoly, která byla vytvořena po prvním kole certifikačního auditu, byla dále propojena s platformou Jira. V rámci již existujícího projektu s názvem *ISO 27001* byly v tomto nástroji vytvořeny nové úkoly, jež byly přehledně rozděleny do tří hlavních kategorií, tzv. *epics*. Konkrétně šlo o *epics* s názvy *Zavedení ISO 27001*, *Změny směrnice* a *Roční plán ISMS 2025*.

V této fázi bylo klíčové úkoly nejen přesně identifikovat, ale také správně prioritizovat. Každému úkolu byla přiřazena odpovídající kategorie (*epic*), odpovědná osoba, podrobný popis zadání, termín dokončení, úroveň priority, a především i odkaz na relevantní obsah v dokumentačním portálu Confluence, se kterým úkol přímo souvisel. Důležitou součástí evidence bylo rovněž propojení jednotlivých úkolů s konkrétními požadavky, což umožnilo jak zadavateli, tak i pověřené osobě efektivně sledovat, zda daný úkol například neblokuje jiný úkol, není duplicitní nebo není závislý na dokončení jiné aktivity.

Toto systematické propojení úkolů, zejména v rámci *epics Zavedení ISO 27001* a *Změna směrnice*, významně usnadnilo řízení dokumentace a její zařazování mezi schválené dokumenty označované jako „VALID“ dokumentace společnosti. Celkový plán dokončení projektu *ISO 27001* byl denně aktualizován a průběžně revidován na týdenních schůzkách vedení společnosti, tzv. *management meetingu*.

Zjištění z prvního certifikačního auditu označené jako *finding 1* se týká nedostatečně rozpracovaného popisu interního a externího kontextu v dokumentu *Příručka ISMS*. Na základě doporučení auditorů byla tato část doplněna a přepracována s cílem zajistit plnou shodu s požadavky normy.

Externí kontext společnosti zahrnuje zejména legislativní a regulatorní faktory, mezi které patří povinnost organizace dodržovat zákonné požadavky v oblasti informační bezpečnosti. Mezi klíčové právní předpisy patří Zákon o kybernetické bezpečnosti, Obecné nařízení o ochraně osobních údajů (GDPR) a další nařízení, směrnice a normy uvedené v dokumentu *Knihovna externí dokumentace*. Soulad s těmito požadavky je pravidelně přezkoumáván v rámci ISMS. Technologický kontext je ovlivněn rychlým vývojem v oblastech jako je cloud computing, umělá inteligence a mobilní práce. Tyto změny vyžadují neustálou aktualizaci bezpečnostních opatření, včetně řešení nových hrozeb jako jsou phishingové kampaně, DDoS útoky nebo zabezpečení vzdáleného přístupu. Ekonomické faktory, včetně dostupných finančních prostředků, ovlivňují

možnosti investic do ISMS. Společnost využívá dostupné dotační programy ke zvýšení bezpečnosti. V sociální a kulturní rovině je kladen důraz na vzdělávání zaměstnanců, prevenci sociálního inženýrství a budování bezpečnostního povědomí. Politické a geopolitické faktory jsou rovněž sledovány, zejména v kontextu regulatorních změn, na které společnost pružně reaguje úpravou interních politik a procesů.

Interní kontext zahrnuje zejména lidské zdroje, kde za řízení ISMS odpovídají bezpečnostní manažer (CISO) a IT administrátor (CTO). Role a odpovědnosti zaměstnanců jsou definovány v dokumentu *Kompetenční matice*. Data Engineer odpovídá za bezpečnost dat a všichni zaměstnanci absolvují pravidelná školení v oblasti informační bezpečnosti. Technické zdroje tvoří zejména IT infrastruktura, včetně cloudových služeb (Microsoft Azure a Atlassian), přičemž přístupová práva jsou řízena na základě role a principu minimálních oprávnění (RBAC). V oblasti procesních a organizačních znalostí má organizace zavedené bezpečnostní politiky, klasifikaci informací, řízení rizik, bezpečnostní strategii a každoročně aktualizovaný *Akční plán ISMS*. Klíčovým dokumentem je *Příručka ISMS*, kterou doplňuje směrnice *Informační bezpečnost*. Finanční a materiální zajištění ISMS je podloženo ročním rozpočtem, ze kterého jsou hrazeny školení, správa infrastruktury i audity. Pro specifické oblasti jsou dostupní externí bezpečnostní konzultanti. V rámci vnitřních zúčastněných stran panuje všeobecné povědomí o bezpečnosti mezi zaměstnanci i dodavateli. Vrcholové vedení aktivně podporuje ISMS, za jehož implementaci odpovídá CISO. V oblasti standardů a směrnic společnost dodržuje ISO/IEC 27001, se zaměřením na specifika zdravotnické informatiky dle ISO/IEC 27799. Interní směrnice *Informační bezpečnost* pokrývá pravidla pro hesla, vícefaktorové ověřování (MFA) a šifrování. Samozřejmostí je dodržování požadavků GDPR. V oblasti smluvních vztahů má organizace uzavřeny příkazní a pracovní smlouvy, dohody o mlčenlivosti (NDA) a smlouvy o důvěrnosti. Technická bezpečnost je posilována také prostřednictvím interních auditů a kontrol třetích stran. Společnost rovněž využívá outsourcing IT služeb a má definované SLA s poskytovateli cloudových služeb.

V rámci *finding 2* byla identifikována potřeba aktualizace a upřesnění rozsahu. Rozsah a hranice ISMS popisují dotčené části systému určené k implementaci, a to „na základě posouzení specifických rysů činností organizace, jejího uspořádání, organizační

struktury, lokace a topologie, aktiv a technologií.“²⁷ Nově vydefinovaný rozsah certifikace zní: Vývoj, poskytování a podpora zdravotnického prostředku jako SaaS.

Finding 3 se týká doplnění *Příručky ISMS* o přehled směrnic, procesů a metrik souvisejících s informační bezpečností. Tento krok byl realizován za účelem splnění požadavků normy, která stanovuje povinnost identifikovat procesy důležité pro fungování systému řízení informační bezpečnosti, definovat jejich vzájemné vazby a nastavit metody pro jejich efektivní řízení.

Příručka ISMS byla proto rozšířena o následující výčet konkrétních směrnic, procesů a hodnotících metrik a cílů.

Tabulka 7: Přehled směrnic, procesů, metrik a cílů souvisejících s ISMS

Název směrnice	Proces	Metrika, cíl
<i>Řízení dokumentů a záznamů</i>	Zabezpečení dokumentace	Frekvence 1x ročně a záznam přezkoumání přístupových oprávnění
<i>Validace procesů a nástrojů</i>	Revalidace	Frekvence revalidace kritických nástrojů – Program validace
<i>Řízení změn</i>	Řízení změn	U 100 % změnových řízení byl zhodnocen vliv na bezpečnost – Jira Automation bezpečnost – Jira bezpečnost – Jira změny na bezpečnost
<i>Kvality review</i>	Pravidelné meetingy	Pravidelnost kvality meetingu 1x měsíčně
<i>Používání nástroje JIRA</i>	Kontrola stavu a správného nastavení projektů a tasků	Jira Automation Rule – Kontrola nastavení Jira
<i>Release management</i>	Release management	Dodržování plánu release (technický plán – vlastní release)
	Patch management	
<i>IT Operations</i>	Záznamy o provedených činnostech v rámci údržby	Měsíční report
	Řízení konfigurací	Dostupnost aplikace $\geq 99\%$

²⁷ SEDLÁK, Petr a Martin KONEČNÝ. *Přeměna ISMS v manažerské informatice*. Brno: CERM, Akademické nakladatelství, 2023. ISBN 978-80-7623-110-8, s. 82.

<i>Řízení lidských zdrojů</i>	Skončení pracovního poměru	Se skončením pracovního poměru jsou účty (a tím i přístupy) deaktivovány do 24 hodin
<i>Uživatelská podpora</i>	Dokumentace uživatelské podpory	Měsíční report
<i>Informační bezpečnost</i>	Zabezpečení dokumentů s personálními údaji	Frekvence 1x ročně a záznam přezkoumání přístupových oprávnění
	Aktualizace přístupových práv ke zdrojům v cloudu	Nastavení pravidla, kdy je uživatel 1x za 180 dní vyzván ke změně hesla v prostředí Microsoft a Atlasian
	Revize přístupových práv	Jira Automation Rule – Revize přístupů
	Řízení bezpečnostního incidentu	Doba odezvy na bezpečnostní incident (MTTA) Doba plánu reakce na bezpečnostní incident Doba do uzavření bezpečnostního incidentu (MTTR) Doba do nahlášení bezpečnostního incidentu národnímu CIRT
<i>Správa aktiv</i>	Řízení rizik	Počet identifikovaných rizik (rizikových scénářů)
	Řízení zranitelností	Jira Automation Rule – Kontrola seznamu zranitelností

(Zdroj: Vlastní zpracování, poskytnuto společností)

Finding 4 se vztahuje k aktualizaci dokumentu *Prohlášení o aplikovatelnosti* a zavádění všech doposud pouze naplánovaných a rozpracovaných bezpečnostních opatření.

Finding 5 se týká potřeby vymezit konkrétní příležitosti ke zlepšování systému řízení informační bezpečnosti, a to ze zvoleného pohledu zvyšování bezpečnostního povědomí zaměstnanců a z hlediska dlouhodobého udržování souladu s aktuální legislativou a technologickým vývojem. Mezi vhodná zlepšení byla identifikována například implementace pravidelných phishingových testů jako forma vzdělávání a ověřování připravenosti zaměstnanců, stejně jako sledování vývoje v oblasti regulace informačních

technologií a systémů umělé inteligence. Jedním z konkrétních legislativních rámců je nařízení Akt o kybernetické odolnosti (Cyber Resilience Act, CRA), které klade důraz na bezpečnost digitálních produktů v celém jejich životním cyklu. Ačkoli se podle znění návrhu CRA „nařízení (se) nepoužije na produkty s digitálními prvky spadající do oblasti působnosti nařízení (EU) 2017/745 a nařízení (EU) 2017/746 (...), neboť obě nařízení obsahují požadavky týkající se prostředků, včetně softwaru, a obecné povinnosti výrobců vztahující se na celý životní cyklus produktů, jakož i postupy posuzování shody“²⁸, je tento přístup uplatňovaný v rámci CRA pro naši společnost inspirací a je užitečné převzít tyto principy.

V rámci *finding 6* byla zpráva z provedení interního auditu ISMS přepracována, aby zohlednila všechny požadavky (dle 9.2.1 a 9.2.2) a kvůli *finding 7* byly dopracovány dokumentované informace pro vstup a výstup (dle 9.3.2 a 9.3.3) přezkoumání vedením v daném rozsahu.

Na základě doporučení auditorů byly identifikované příležitosti ke zlepšení již implementovány. V dokumentu *Průručka ISMS* byl doplněn podrobnější popis rozhraní a závislostí mezi činnostmi organizace a aktivitami vykonávanými externími subjekty. Dále byl přesněji definován postup schvalování kontaktu se zájmovými skupinami (především s lékaři a experty v oblasti informační a kybernetické bezpečnosti) aktualizován odpovídající pracovní postup. V oblasti plánování byla zajištěna provázanost cílů uvedených v *Bezpečnostní strategii* s *Akčním plánem ISMS 2025*, dále pak s dokumenty *Analýza rizik ISMS* a *Plán zvládnutí rizik*, čímž bylo posíleno jejich praktické uplatnění a návaznost v rámci systému řízení informační bezpečnosti.

V rámci příprav na druhé kolo certifikačního auditu byla provedena rozsáhlá aktualizace základní dokumentace a organizačních směrnic. Celkem bylo aktualizováno nebo nově vytvořeno 26 organizačních směrnic, základních dokumentů systému řízení informační bezpečnosti nebo dokumentových šablon. Převážně se jednalo o implementaci naplánovaných bezpečnostních opatření, pouze v kratším intervalu, než se předpokládalo.

²⁸ Evropská unie. Nařízení Evropského parlamentu a Rady (EU) 2024/2847 ze dne 23. října 2024, o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) č. 168/2013 a (EU) 2019/1020 a směrnice (EU) 2020/1828 (Akt o kybernetické odolnosti). In: Úřední věstník Evropské unie. 20. 11. 2024, L 2847, s. 1–81. ISSN 1977-0677.

Tyto úpravy přispěly k posílení dokumentační základny ISMS a zvýšily jeho připravenost na certifikaci.

Byl navržen nový ***Seznam aktiv***, rozdělený na dvě rozsáhlé tabulky – primární a podpůrná aktiva. Aktiva jsou dále rozdělena do jednotlivých oblastí a kategorií, zaznamenají se jejich vazby na podpůrná aktiva, ohodnotí se dle triády C-I-A) a určí se důsledky v případě výpadku nebo nedostupnosti aktiva, závěrem se zaznamená datum, kdy vlastník aktiva schválil veškeré hodnoty. CISO společně s vlastníky aktiv sestavuje matici závislostí primárních a podpůrných aktiv, kdy pomocí značky “x” znázorní vzájemné vazby.

Seznam primárních aktiv zahrnuje také hodnocení dopadů na podnikání k určení závažnosti důsledků jejich případné nedostupnosti. Aktivům je přiřazena hodnota představující dobu, po kterou proces nebo informace mohou být maximálně nedostupné: až 3 hodiny (3 h), což představuje krátkodobý výpadek s omezeným vlivem; až 3 dny (3 d), kdy může dojít k závažnějšímu narušení provozu a závazků; 1 týden (1 w) a více, což může způsobit dlouhodobé riziko pro klíčové činnosti, finanční ztráty a ztrátu důvěry. Toto hodnocení pomáhá určit kritičnost aktiv, plánovat odpovídající opatření a zaměřit se na ochranu nejdůležitějších oblastí.

„Tabulka s primárními aktivy eviduje:

- Oblast, do které spadá primární aktivum
- ID primárního aktiva (označováno PAXx)
- Název primárního aktiva
- Kategorii – proces/informace
- Popis primárního aktiva
- Vlastník aktiva
- Vazba na podpůrná aktiva
- Celkový počet vazeb na primární aktivum
- Hodnocení dle triády C-I-A (více viz kapitola 6.5)
- Hodnota aktiva (nejvyšší hodnota dle hodnocení C-I-A)
- Důsledky v případě výpadku nebo nedostupnosti (3 hodiny, 3 dny, 1 týden)

- Datum schválení (schvaluje vlastník aktiva)²⁹

Podpůrná aktiva jsou aktiva nutná pro správnou funkčnost, zpracování, uchování a zajištění bezpečnosti primárních aktiv. Sama o sobě podpůrná aktiva netvoří hodnotu pro organizaci. Podpůrná aktiva jsou členěna do následujících kategorií: technické vybavení (HW), programové vybavení (SW), lidské zdroje, dodavatelé (součástí jsou i externí systémy a služby), objekty.

„Tabulka s podpůrnými aktivy eviduje:

- Oblast, do které spadá podpůrné aktivum
- ID podpůrného aktiva (označováno SAxx)
- Název podpůrného aktiva
- Popis podpůrného aktiva
- Počet uživatelů podpůrného aktiva
- Počet privilegovaných uživatelů podpůrného aktiva
- Autentizační metoda
- Vynucení dvoufaktorového ověřování (2FA)
- Logování aktivity
- Množství podpůrného aktiva (pokud lze určit)
- Hodnocení dle triády C-I-A
- Hodnota aktiva (nejvyšší hodnota dle hodnocení C-I-A)
- Vlastník aktiva³⁰

Součástí Podpůrných aktiv také *tabulka* s přístupy, která je zvýrazněna žlutými buňkami. Tato tabulka obsahuje informace o počtu uživatelů a privilegovaných uživatelů daného aktiva, používané autentizační metodě, vynucení dvoufaktorového ověřování (2FA) a logování aktivity. Údaje slouží k lepšímu řízení a kontrole přístupů k podpůrným aktivům.

Proces ***Validace nástrojů a procesů*** byl rozšířen o posouzení z hlediska informační bezpečnosti. V případech, kdy je validován nástroj nebo proces, který by mohl

²⁹ Poskytnuto společností.

³⁰ Poskytnuto společností.

potenciálně ovlivnit informační bezpečnost společnosti, je nově do validačního týmu zařazen také CISO. Ten na základě analýzy rizik stanovuje požadavky na informační bezpečnost, které musí být v rámci validace zohledněny. Mezi tyto požadavky zpravidla patří: ověření mechanismů autentizace, omezení přístupových práv, zajištění integrity dat, ochrana dat během jejich zpracování, přenosu a uložení, dále požadavky na šifrovanou komunikaci, možnosti logování a monitoringu a případně i další bezpečnostní opatření. Tento přístup zajišťuje, že validované nástroje a procesy splňují požadavky ISMS a nepředstavují bezpečnostní riziko pro organizaci.

V rámci posilování technologických bezpečnostních opatření byla zavedena řada konkrétních technických změn, jejichž cílem je zvýšení odolnosti vůči bezpečnostním incidentům a zajištění souladu s požadavky systému řízení informační bezpečnosti.

Jako preventivní opatření proti škodlivému softwaru bylo zavedeno důkladné skenování systémů pomocí nástroje *Kaspersky Virus Removal Tool*, který je uložen na přenosném médiu (USB disk). V případech podezření na napadení systému nebo při důkladné kontrole disků se používá také *Kaspersky Rescue Disk*, rovněž dostupný na samostatném USB zařízení.

Nově byl zaveden strukturovaný postup pro hlášení bezpečnostních incidentů, a to prostřednictvím elektronického formuláře. Po jeho vyplnění a ověření správnosti všech údajů odpovědná osoba, zpravidla CTO nebo CISO, odešle formulář elektronickou poštou na kontaktní adresu Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Pro zajištění bezpečné a důvěryhodné komunikace je využíváno *PGP* šifrování pomocí nástroje *Gpg4win*.

Na úrovni serverové infrastruktury bylo zakázáno ověřování uživatelů prostřednictvím hesla. Autentizace je nově řešena výhradně pomocí kryptografie s veřejným klíčem, přičemž soukromý klíč je chráněn silným heslem.

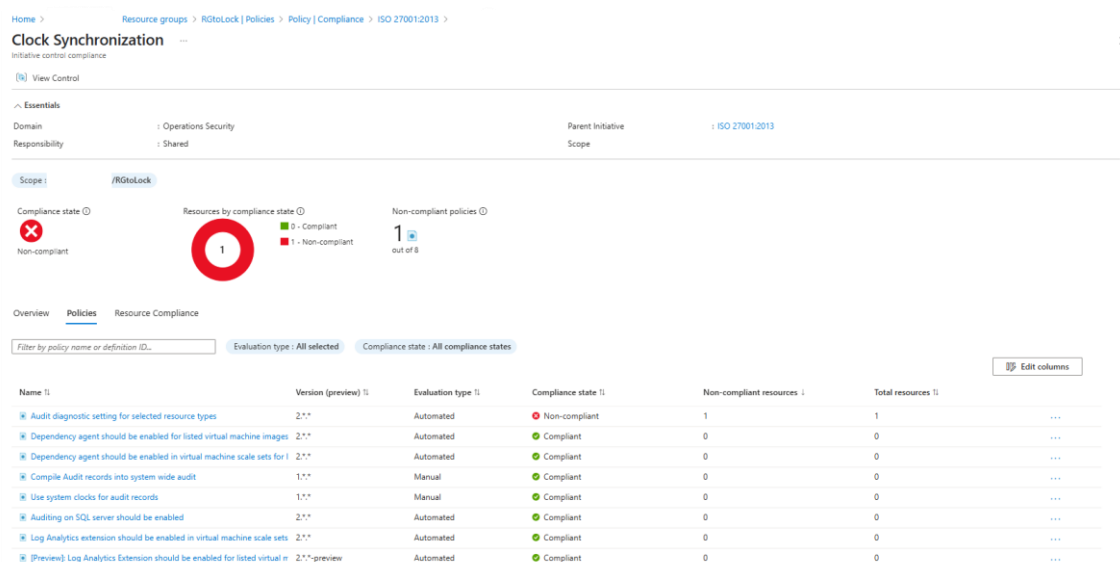
V rámci nástroje *Jira* byly implementovány automatizační pravidla, která zajišťují správu úkolů projektu ISO 27001. Ve výchozím nastavení jsou nově vytvořené úkoly automaticky přiřazeny CISO, pokud není určena jiná odpovědná osoba. Součástí automatizace je také pravidelné upozorňování na nutnost revize přístupových práv, provizorní kontrola seznamu zranitelností, a nastavení odpovídajícího *workflow* (viz *Obrázek 2*), jehož úkolem je podpořit kontinuitu řízení bezpečnostních opatření a usnadnit dohled nad jejich plněním.



Obrázek 2: Jira workflow

(Zdroj: Nástroj Jira, poskytnuto společností)

S výhledem na implementaci systému řízení informační bezpečnosti byl již dříve zaveden tzv. *Blueprint ISO 27001*, což představuje standardizovaný rámec (šablonu), který poskytuje ucelený soubor zásad a pravidel pro udržování bezpečného prostředí v souladu s požadavky normy ISO/IEC 27001. Nasazením tohoto prostředí došlo k zavedení jednotného postupu při nastavování a řízení bezpečnostních opatření, přičemž součástí jsou i definované zásady neboli *policies*. Tyto zásady umožňují transparentní a konzistentní řízení bezpečnosti napříč organizací. Přehled konkrétního nastavení bezpečnostních pravidel bezpečnostního opatření 8.17 *Synchronizace hodin* je znázorněn na následujícím *Obrázku 3*.



Obrázek 3: Blueprint v MS Azure

(Zdroj: Nástroj MS Azure, poskytnuto společností)

V rámci zajištění souladu s požadavky aktuální legislativy v oblasti umělé inteligence došlo k posunu také ve zpracování problematiky Aktu o umělé inteligenci (AI Act) z pohledu bezpečnosti. Na základě jeho požadavků byly identifikovány specifické hrozby, které se vztahují k provozu systémů AI. Tyto hrozby budou zahrnuty do následující revize *Analýzy rizik ISMS*. Jedná se konkrétně o: *data poisoning* (záměrná kontaminace trénovacích dat), *model poisoning* (vlození škodlivých prvků do modelu), *adversarial examples/model evasion* (vstupy navržené k tomu, aby model uvedly v omyl), *confidentiality attacks* (útoky zaměřené na odhalení citlivých dat) a *model flaws* (využití vnitřních chyb modelu). Těmito hrozbami a relevantními bezpečnostními opatřeními bude rozšířen stávající rámec řízení rizik v oblasti informační a kybernetické bezpečnosti o prvky zaměřené na specifika systémů umělé inteligence.³¹

Další bezpečnostní opatření zavedená v této etapě byla například **klasifikace informací a označování informací**.

„Pro komerční sféru platí 4 stupně:

- *Důvěrné (Confidential)* – se zničujícím dopadem na společnost;

³¹ Evropská unie. Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanovují harmonizovaná pravidla pro umělou inteligenci a mění se nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (Akt o umělé inteligenci). In: Úřední věstník Evropské unie. 12. 7. 2024, L 1689, s. 1-144. ISSN 1977-0626.

- *Soukromé (Private)* – s negativním dopadem na společnost (osobní údaje o zaměstnancích a zákaznících);
- *Citlivé (Sensitive)* – s negativní dopadem na společnost (projekty, cenová politika, ...);
- *Veřejné (Public)* – veřejně známé informace.³²

Pro potřeby a kontext této společnosti byly zvoleny kategorie:

- *Veřejné (Public)* – určeno pro širokou veřejnost, nemá žádná omezení pro zveřejnění, organizaci nezpůsobí škodu, pokud se dostane do nepovolaných rukou;
- *Interní (Internal only)* – neveřejné informace, určené pouze pro pracovníky a partnery organizace, únik může způsobit menší provozní komplikace, ale nepředstavuje vážné riziko;
- *Důvěrné (Confidential)* – přístup pouze pro vybrané osoby v rámci organizace (např. na základě role), únik může mít významný negativní dopad (např. finanční ztráty, právní důsledky);
- *Kritické (Critical)* – nejcitlivější informace, přístup mají pouze vybrané osoby s autorizací a přístup je protokolován, únik by mohl způsobit kritickou újmu organizaci (např. právní postihy, ohrožení bezpečnosti).³³

V rámci zavedení klasifikace informací byla původně zvažována implementace služby *Microsoft Purview*, která by umožňovala správu, označování a klasifikaci dat napříč různými službami Microsoft, jako jsou dokumenty, cloudové služby Azure, e-mailové komunikace atd. Tato služba umožňuje vytváření štítků, tzv. *labels*, a nastavování pravidel pro zacházení s jednotlivými kategoriemi informací. Ačkoli byla cena za jedno označení velmi nízká, služba byla zpoplatněna na měsíční bázi, což se z dlouhodobého hlediska ukázalo jako finančně neudržitelné řešení pro malý podnik.

Z tohoto důvodu byla zavedena alternativní forma klasifikace informací, která nevyžaduje podobné finanční náklady. Tato metoda zahrnuje barevné odlišení složek, označení klasifikace přímo v názvu souboru nebo dokumentu, a využití funkce

³² SEDLÁK, Petr a Martin KONEČNÝ. *Přeměna ISMS v manažerské informatice*. Brno: CERM, Akademické nakladatelství, 2023. ISBN 978-80-7623-110-8, s. 150.

³³ Poskytnuto společností.

označování (label/tag) v prostředí nástroje Confluence, která umožňuje viditelné označení dokumentace například štítkem *CONFIDENTIAL*. Dále je možné používat značky i u služeb Microsoft Azure, čímž je klasifikace informací realizována v souladu s požadavky na bezpečné zacházení s daty i bez nutnosti investice do licencovaného nástroje.

V rámci implementace klasifikace informací byl zaveden systém označování a ochrany informací dle úrovně jejich citlivosti. Systém rozlišuje čtyři základní klasifikační úrovně a definuje způsob jejich uchovávání, označování i přístupová pravidla.

Informace označené jako Public (Veřejné) nevyžadují zvláštní ochranu. Jsou ukládány například v týmu *Marketing* v prostředí MS Teams, konkrétně ve složce schválených marketingových podkladů, nebo na jiných veřejně přístupných úložištích. Na platformě SharePoint jsou tyto složky odlišeny zelenou barvou.

Internal only (Interní) označuje informace, které jsou určeny výhradně pro vnitřní potřebu organizace. Jsou ukládány a sdíleny v rámci interní infrastruktury nebo přímo ve fyzických prostorách společnosti. Na platformě SharePoint jsou tyto složky odlišeny žlutou barvou.

Za Confidential (Důvěrné) jsou považovány informace, které vyžadují řízený a protokolovaný přístup. Elektronická aktiva jsou uložena v zabezpečeném prostředí interní infrastruktury, zatímco fyzická aktiva jsou uchovávána v uzamykatelných objektech vnitřního perimetru III, například v kanceláři společnosti nebo v uzamykatelných skříních. Dokumenty jsou označeny vodoznakem *CONFIDENTIAL* nebo uloženy ve složkách s tímto označením v názvu. V prostředí Microsoft Azure je využíváno označení tagem *CONFIDENTIAL*. Na platformě SharePoint jsou tyto složky odlišeny oranžovou barvou.

Critical (Kritické) informace představují nejvyšší úroveň citlivosti. Elektronická aktiva jsou uložena výhradně na šifrovaných úložištích s autorizovaným a protokolovaným přístupem. Fyzická aktiva jsou zabezpečena v odděleném uzamykatelném prostoru tvořícím samostatný perimetr. Dokumenty této klasifikace nesou vodoznak *CRITICAL* a na platformě SharePoint jsou tyto složky odlišeny červenou barvou.

Během postupné implementace požadavků normy IEC 81001-5-1 byla v hodnoceném období věnována pozornost především podrobnějšímu studiu dostupných metodik

a praktických nástrojů. Za mimořádně užitečný byl v tomto směru vyhodnocen materiál *Playbook for Threat Modeling Medical Devices*³⁴ vydaný organizací MITRE, který poskytuje praktický rámec pro identifikaci a analýzu hrozeb specifických pro zdravotnické prostředky.

Současně byla analyzována příloha normy (*Annex C*)³⁵ zmíněné normy, která popisuje přístup založený na vytváření seznamu známých potenciálních zranitelností (*List of known potential vulnerabilities*). Tento přístup je plánováno dále rozpracovat po ukončení druhého kola certifikačního auditu, kdy bude zahájena i příprava automatizovaného monitoringu zranitelností v souladu s rámcem NIST, a to především prostřednictvím databáze známých zranitelností *CVE* (Common Vulnerabilities and Exposures). Tento krok bude představovat zásadní posun směrem k efektivnějšímu a proaktivnímu řízení kybernetických rizik souvisejících s vývojem zdravotnického softwaru.

Jedním z posledních klíčových dokumentů, který společnost neměla vytvořený, byl ***Plán kontinuity činností*** (Business Continuity Plan, BCP). Cílem zavedení tohoto dokumentu bylo zajistit ucelený rámec pro zachování nebo obnovení klíčových činností organizace v případě výpadků, incidentů nebo krizových situací. Po jeho vytvoření byl plán také prakticky otestován.

Součástí dokumentu je *Analýza dopadů na podnikání* (Business Impact Analysis, BIA), která byla koncipována jako analýza zaměřená na dopad incidentů na chod společnosti, nikoliv na jejich příčiny. Tato analýza je včleněna do stávajícího dokumentu *Seznam aktiv* a identifikuje procesy a činnosti kritické pro udržení provozuschopnosti společnosti, konkrétně například procesy *PAXx – Data management* a *PAXx – IT support and operations*.

Na základě mapování procesů a identifikace souvisejících zdrojů byla provedena analýza rizik vztahujících se ke konkrétním zdrojům. Byla stanovena nutnost tato rizika řídit a snižovat. Dále byly identifikovány tzv. *Single Points of Failure* (SPoF), tedy jediné

³⁴ MITRE Corporation. *Playbook for Threat Modeling Medical Devices* [online]. 30. listopad 2021 [cit. 2025-03-12]. Dostupné z: <https://www.mitre.org/sites/default/files/2021-11/Playbook-for-Threat-Modeling-Medical-Devices.pdf>.

³⁵ ČSN EN IEC 81001-5-1. Zdravotnický software a bezpečnost, účinnost a ochrana zdravotnických IT systémů – Část 5-1: Činnosti v životním cyklu produktu, 2022. Ženeva: Mezinárodní elektrotechnická komise.

body selhání, a to ve třech oblastech: klíčových pracovníků s unikátní znalostí klíčových služeb, klíčových dodavatelů, bez nichž by nebylo možné poskytovat služby a specifických technologií, které by mohly ohrozit technologickou nezávislost společnosti.

Plán kontinuity činností obsahuje strukturovaný přehled všech klíčových komponent, které jsou nezbytné pro účinnou reakci na incident a následnou obnovu provozu. Jednotlivé scénáře obnovy byly rozpracovány tak, aby reflektovaly všechny důležité aspekty plánování a realizace. Mezi tyto komponenty patří:

- účel a rozsah plánu,
- vymezení rolí a odpovědností,
- aktivační mechanismus plánu,
- určení adekvátních lidských a materiálních zdrojů (včetně posouzení dopadů jako jsou ušlé zisky, pokuty či ztráta zákazníků),
- časový rámec zahrnující dobu obnovení provozu (RTO) a bod obnovení dat (RPO),
- stanovení priorit a minimální úrovně poskytovaných služeb (MBCO),
- komunikační strategie, včetně kontaktních údajů a preferovaných kanálů (telefon, e-mail, *MS Teams*),
- a plán návratu k normálnímu provozu.

Plán definuje tři základní scénáře krizových situací:

- 1. Výpadek produkčního prostředí, kdy dojde k narušení klíčové dodávky služby ze strany poskytovatele (např. *Microsoft*), což znemožní společnosti přístup k datům.**
- 2. Výpadek produkčního prostředí způsobený selháním aplikace, což má za následek nedostupnost dat pro koncového zákazníka.**
- 3. Přírodní katastrofa, konkrétně požár, který by vedl ke ztrátě všech fyzických dokumentů uložených v kancelářských prostorách společnosti.**

Každý z těchto scénářů byl v dokumentu detailně rozpracován s cílem zajistit připravenost na jejich zvládnutí a minimalizaci negativních dopadů na fungování společnosti.

Diplomová práce zachycuje celý průběh implementace systému řízení informační bezpečnosti až po přípravu na druhé kolo certifikačního auditu, jehož výsledek je zmíněn v poslední kapitole práce – Závěru.

4.3 Ekonomický aspekt

Implementace systému řízení informační bezpečnosti ve společnosti byla spojena s významnými investicemi. Náklady zahrnovaly především odborné konzultace, služby smluvního výzkumu, mzdové náklady interních pracovníků, náklady na certifikační audit, realizaci penetračních testů a implementaci opatření doporučených po jejich provedení. Celkové náklady na zavedení bezpečnostního systému dosáhly přibližně 1,2 milionu korun.

Významnou položkou byly zejména mzdové náklady pracovníků zapojených do projektu, kde bylo prostřednictvím platformy Jira zaznamenáno přibližně 1 650 hodin práce. Další vyšší nákladová položka byly externí penetrační testování bezpečnosti aplikace a implementace následných bezpečnostních opatření v oblasti vývoje softwaru. Významnou část investic představovaly také konzultace a smluvní výzkum, které přispěly k efektivnímu návrhu dokumentace a implementaci bezpečnostních opatření.

Z ekonomického hlediska byla návratnost investic vyhodnocena pomocí modelu ROSI (Return on Security Investment). Tento model porovnává náklady vynaložené na zavedení bezpečnostních opatření s potenciálními škodami, které byly jejich zavedením zmírněny nebo jim bylo částečně zabráněno.³⁶

První model návratnosti vycházel z předpokládaných výdajů spojených se sankcemi za neplnění požadavků GDPR, a to na základě reálné události v nemocnici v Portugalsku z roku 2018, která dostala pokutu 400 000 € za nedostatečnou ochranu údajů pacientů, kdy měl personál neoprávněný přístup k datům přes falešné profily.³⁷ Návratnost investice (ROSI) v tomto případě vychází přibližně na 7 300 %, což znamená, že by případná

³⁶ SEDLÁK, Petr, Martin KONEČNÝ a kolektiv. *Případové studie řízení kybernetické bezpečnosti*. Brno: CERM, Akademické nakladatelství, 2024. ISBN 978-80-7623-126-9. s. 79–80.

³⁷ OBERSCHELP DE MENESES, Anna, Kristof VAN QUATHEM. *Portuguese Hospital Receives and Contests €400,000 Fine for GDPR Infringement* [online]. The National Law Review, 26.8.2018, roč. 8, č. 299. ISSN 2161-3362. Covington & Burling LLP. Dostupné z: <https://natlawreview.com/article/portuguese-hospital-receives-and-contests-400000-fine-gdpr-infringement> [cit. 2025-04-25].

pokuta byla 73krát vyšší než náklady vynaložené na zavedení bezpečnostních opatření, šlo by tedy o 73násobné zhodnocení investice do bezpečnosti společnosti.

V rámci alternativního vyhodnocení byla zohledněna také tržní hodnota technologické společností vyvíjející obdobné produkty, ta představuje náklady na vývoj a zhodnocení společnosti jako takové. Na základě dostupných údajů o prodeji společnosti zabývající se vývojem AI zdravotnického softwaru³⁸ dosahuje odhadovaná návratnost investice (ROSI) hodnoty až přibližně 9 900 %, což znamená, že by případný únik dat, který by ohrozil její existenci, by mohl vést ke ztrátám až ve výši 99násobku původní investice, tedy ztrátě celé tržní hodnoty společnosti.

Tyto hodnoty potvrzují vysokou návratnost a ekonomickou přínosnost investic do bezpečnostního systému. Přijatá bezpečnostní opatření nejen významně snížila riziko regulatorních sankcí a reputační újmy, ale zároveň přispěla ke zvýšení tržní hodnoty společnosti.

Je třeba rovněž zmínit přínosy vyplývající ze smluvního výzkumu realizovaného ve spolupráci s Vysokým učením technickým v Brně, který umožnil využití odborných konzultací a přístup k vybraným normám bez nutnosti nákupu licencí, což rovněž přispělo k optimalizaci nákladů.

4.4 Nástroje

Následující (pouze zvažované) nástroje jsou v této části práce krátce zmíněny, neboť by mohly významně zkrátit čas potřebný na provedení analýzy a tvorbu dokumentace, a tím i snížit celkové náklady spojené s implementací systému řízení informační bezpečnosti, ale po zvážení všech rozhodujících aspektů doposud nebyly pořízeny.

Esko-KB³⁹ je nástroj pro snadnou inventarizaci informačních aktiv, analýzu jejich zranitelností a hodnocení souvisejících rizik. Výstupem je konzistentní ohodnocení rizik a návrh bezpečnostních opatření, které jsou dokumentovány v elektronické i tisknutelné

³⁸ Revenio Group invests in artificial intelligence by acquiring AI software company Thirona Retina from Dutch company Thirona [online]. Revenio Group Corporation – Investor News, 20.8.2024. Nasdaq. Dostupné z: Revenio Group invests in artificial intelligence by acquiring AI software company Thirona Retina from Dutch company Thirona [cit. 2025-04-25].

³⁹ Esko-KB. *Nástroj pro garanty aktiv a shodu s VKB* [online]. [cit. 3. 5. 2025-03-30]. Dostupné z: <https://www.esko-sw.com/>.

formě a slouží jako základ pro audit kybernetické bezpečnosti. Díky neustálé aktualizaci zabezpečení a legislativy zůstávají informace v tomto nástroji vždy aktuální, což umožňuje organizacím efektivně reagovat na legislativní změny bez potřeby individuálního informování. Společnost se rozhodla nástroj v dané fázi nepořídít, neboť by představoval finanční náklad, který aktuálně přesahuje rozpočtové možnosti vyhrazené pro oblast informační a kybernetické bezpečnosti.

Na základě doporučení byl autorce práce také představen nástroj s názvem Audit Master AI.⁴⁰, který byl následně prezentován i formou ukázky v rámci demo verze. Na rozdíl od dříve zmíněného nástroje, který je zaměřen na správu aktiv, se Audit Master AI soustředí především na správu interní dokumentace. Jeho hlavními funkcemi je automatizovaná analýza rozdílů mezi aktuálním a požadovaným stavem, tvorba plánů nápravných opatření, automatické sestavování auditních zpráv a podpora při zavádění požadavků vyplývajících z nařízení NIS2.

Přestože uvedené funkce představují významný potenciál pro zajištění souladu s legislativními požadavky a pro zvýšení efektivity řízení bezpečnosti, aktuální potřeby společnosti pokrývají spíše plánovaná rozšíření tohoto nástroje, která jsou v současnosti ve fázi vývoje. Mezi připravované funkce patří například generování směrnic a dokumentace na základě analýzy bezpečnostních rizik, slabých míst a informací o společnosti, kontinuální monitoring shody s právními předpisy za účelem proaktivní identifikace nesouladů a jejich včasného odstranění, a v neposlední řadě plánovaná integrace s požadavky normy ISO/IEC 27001. Tyto funkce by mohly v budoucnu výrazně přispět ke zjednodušení implementace a řízení systému informační bezpečnosti, avšak v době zpracování této práce nebyly ještě dostupné.

⁴⁰ AuditMaster AI. *Váš specialista na dodržování předpisů v oblasti kybernetické bezpečnosti* [online]. [cit. 2025-03-30]. Dostupné z: <https://auditmaster.ai>.

ZÁVĚR

Hlavním cílem této diplomové práce bylo navrhnout, zavést a zdokumentovat systém řízení informační bezpečnosti (ISMS) ve společnosti vyvíjející zdravotnický prostředek. Tato společnost doposud neměla zavedený ucelený přístup k informační bezpečnosti, a proto bylo nutné celý systém vytvořit od základů. Cílem bylo nejen dosažení souladu s požadavky mezinárodní normy ISO/IEC 27001, ale také reflektování specifických rizik spojených s vývojem zdravotnických systémů využívajících prvky umělé inteligence.

V rámci práce byla provedena analýza stávajícího stavu, navržena a implementována bezpečnostní opatření, vytvořena klíčová dokumentace a společnost byla připravena na první kolo certifikačního auditu. V návaznosti na to byl vybudován funkční a provázaný systém, který pokrývá nejen informační bezpečnost, ale rovněž podporuje soulad s relevantní legislativou. Tím byly naplněny stanovené cíle práce.

Zavedením systému řízení informační bezpečnosti došlo ke zvýšení důvěryhodnosti společnosti, a to jak ze strany zákazníků, tak i regulačních autorit. V návaznosti na úspěšné absolvování druhého kola certifikačního auditu byl společnosti udělen certifikát ISO/IEC 27001:2023, přičemž auditní tým identifikoval i tři výrazné silné stránky (tzv. *strong points*). Také zhodnocení návratnosti investic ukázalo, že přijatá opatření vedla k odhadem 73 až 99násobnému zhodnocení vložených prostředků, a to jak ve vztahu k potenciálním sankcím vyplývajícím z nedodržení legislativních požadavků, tak i při zohlednění tržní hodnoty obdobné technologické společnosti. Praktický dopad této diplomové práce se projevil i ve formě profesní nabídky na spolupráci, konkrétně zájmem o konzultace ze strany technologického startupu taktéž zaměřeného na vývoj zdravotnického prostředku využívajícího umělou inteligenci.

Implementace ISMS přinesla společnosti systematický přístup k řízení bezpečnostních rizik a významně přispěla k rozvoji bezpečnostního povědomí napříč celou organizací. Přínos projektu však přesahuje hranice společnosti, protože zavedení systému ochrany informací zvyšuje důvěru pacientů v bezpečné nakládání s jejich osobními a zdravotními údaji. Tato práce zároveň poukazuje na tematickou analogii mezi prevencí ve zdravotnictví a prevencí v oblasti kybernetické bezpečnosti, které spojuje důraz na prevenci, tedy včasné rozpoznání hrozeb a jejich systematické zvládnutí.

Tato práce může dále sloužit jako praktický metodický rámec pro další malé a střední technologické společnosti ve zdravotnictví, které plánují implementaci ISMS, protože nabízí aplikovatelný a realistický postup implementace. Projekt byl navíc realizován v časově zkráceném režimu. To umožnila hluboká znalost vnitřního prostředí společnosti a přímé zapojení autorky práce do organizačních struktur. Mezi běžné výzvy, kterým čelí malé organizace při implementaci ISMS, patří omezené finanční a personální kapacity, nedostatek odbornosti v oblasti kybernetické bezpečnosti a složitost interpretace požadavků norem. V tomto projektu se tyto překážky podařilo překonat, především díky zjednodušené interní komunikaci a silné podpoře ze strany vedení.

Určité technické limity se projevily například při hodnocení aktiv, což si vyžádalo úpravu metodiky a více manuálního zpracovávání. Některé požadavky aktuální legislativy zůstaly k datu uzavření práce částečně rozpracované, zejména z důvodu jejich časové a kapacitní náročnosti a nižší prioritizace ve fázi přípravy na certifikaci.

Po úspěšném absolvování druhého kola certifikačního auditu je doporučeno zaměřit se na hlubší integraci bezpečnostních požadavků vyplývajících z AI Act, včetně formalizace procesů pro monitoring, logování a řízení incidentů vztahujících se k AI komponentám. V souladu s *Akčním plánem ISMS* pro rok 2025 by měla být zajištěna jejich průběžná implementace.

Dále je doporučeno pokračovat v rozvoji nástrojů pro automatizaci správy zranitelností a bezpečnostních incidentů a posilovat procesy kontinuálního zlepšování ISMS. Vzhledem k rychle se vyvíjejícímu legislativnímu prostředí, zejména v oblasti zdravotnické informatiky a kybernetické odolnosti, je důležité nadále sledovat nové předpisy a přizpůsobovat jim bezpečnostní strategii společnosti.

SEZNAM POUŽITÝCH ZDROJŮ

Česká asociace umělé inteligence. *Nejsrozumitelnější průvodce EU AI Act* [online]. 4. února 2025 [cit. 2025-05-03]. Dostupné z: <https://asociace.ai/eu-ai-act/>.

ČSN EN ISO/IEC 27000: *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník*, 2020. Páté vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN EN ISO/IEC 27001: *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky*, 2022. Třetí vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN EN ISO/IEC 27002: *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti*, 2022. Třetí vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN EN ISO/IEC 27005: *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Pokyny pro management rizik informační bezpečnosti*, 2022. Čtvrté vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN EN ISO 27799: *Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO 27002*, 2017. Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ČSN EN IEC 81001-5-1. *Zdravotnický software a bezpečnost, účinnost a ochrana zdravotnických IT systémů – Část 5-1: Činnosti v životním cyklu produktu*, 2022. Ženeva: Mezinárodní elektrotechnická komise.

Elicit. *Elicit: The AI Research Assistant* [online]. [cit. 2025-02-15]. Dostupné z: <https://elicit.com>. AI nástroj.

EUcert. *Norma ISO/IEC 27001:2022. Jaké jsou klíčové změny v normě ISO/IEC 27001:2022?* [online]. 22. května 2023 [cit. 2025-04-11]. Dostupné z: <https://eucert.cz/norma-iso-27001-2022/>.

Evropská unie. *Nařízení Evropského parlamentu a Rady (EU) 2017/745 ze dne 5. dubna 2017 o zdravotnických prostředcích a o zrušení směrnic Rady 93/42/EHS a 90/385/EHS*. In: Úřední věstník Evropské unie. 5. 5. 2017, L 117/1, s. 1-175. ISSN 1977-0677.

Evropská unie. *Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanovují harmonizovaná pravidla pro umělou inteligenci a mění se nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (Akt o umělé inteligenci)*. In: Úřední věstník Evropské unie. 12. 7. 2024, L 1689, s. 1-144. ISSN 1977-0626.

Evropská unie. *Nařízení Evropského parlamentu a Rady (EU) 2024/2847 ze dne 23. října 2024, o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) č. 168/2013 a (EU) 2019/1020 a směrnice (EU) 2020/1828 (Akt o kybernetické odolnosti)*. In: Úřední věstník Evropské unie. 20. 11. 2024, L 2847, s. 1–81. ISSN 1977-0677.

MITRE Corporation. *Playbook for Threat Modeling Medical Devices* [online]. 30. listopad 2021 [cit. 2025-03-12]. Dostupné z: <https://www.mitre.org/sites/default/files/2021-11/Playbook-for-Threat-Modeling-Medical-Devices.pdf>.

OBERSCHELP DE MENESES, Anna, Kristof VAN QUATHEM. *Portuguese Hospital Receives and Contests €400,000 Fine for GDPR Infringement* [online]. The National Law Review, 26.8.2018, roč. 8, č. 299. ISSN 2161-3362. Covington & Burling LLP. Dostupné z: <https://natlawreview.com/article/portuguese-hospital-receives-and-contests-400000-fine-gdpr-infringement> [cit. 2025-04-25].

Revenio Group invests in artificial intelligence by acquiring AI software company Thirona Retina from Dutch company Thirona [online]. Revenio Group Corporation – Investor News, 20.8.2024. Nasdaq. Dostupné z: Revenio Group invests in artificial intelligence by acquiring AI software company Thirona Retina from Dutch company Thirona [cit. 2025-04-25].

ŠVÉDA, Martin. 8. ledna. 2024. *Dotaz k identifikaci jako povinná osoba*. E-mailová komunikace.

Úřad vlády České republiky. *Návrh prováděcích právních předpisů* [online], 2024 [cit. 2025-03-05]. Dostupné z: <https://www.odok.gov.cz/portal/veklep/material/ALBSCSSFKU7S/>.

VALDEVIT, Thierry, Nicolas Mayer, 2010. *A GAP ANALYSIS TOOL FOR SMES TARGETING ISO/IEC 27001 COMPLIANCE*. In Proceedings of the 12th International Conference on Enterprise Information Systems – Volume 2: ICEIS. ISBN 978-989-8425-06-5. ISSN 2184-4992, SciTePress, s. 413-416.

Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) [online], 2014. Česká republika [cit. 2025-03-10]. Dostupné z: <https://www.psp.cz/sqw/sbirka.sqw?cz=181&r=2014>. Sbírka zákonů.

SEZNAM ZKRATEK

AI	Artificial Intelligence
API	Application Programming Interface
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BYOD	Bring Your Own Device
CEO	Chief Executive Officer
CIA	Confidentiality, Integrity, Availability
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CRA	Cyber Resilience Act
CRM	Customer Relationship Management
CTO	Chief Technology Officer
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
DRP	Disaster Recovery Plan
GDPR	General Data Protection Regulation
IAM	Identity and Access Management
IPMI	Intelligent Platform Management Interface
ISMS	Information Security Management System
MBCO	Minimum Business Continuity Objective
MDCG	Medical Device Coordination Group
MDR	Medical Devices Regulation
MFA	Multi-factor Authentication
MTTA	Mean Time to Acknowledge
MTTR	Mean Time To Respond
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology

NIS2	Network and Information Security Directive 2
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
KII	Kritická informační infrastruktura
OFI	Opportunity for Improvement
OWASP	Open Worldwide Application Security Project
PDCA	Plan-Do-Check-Act
PGP	Pretty Good Privacy
PII	Personally Identifiable Information
PMCF	Post-Market Clinical Follow-up
PoA	Prohlášení o aplikovatelnosti
PRRC	Person Responsible for Regulatory Compliance
QMS	Quality Management System
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
RTO	Recovery Time Objective
ROSI	Return on Security Investment
RPO	Recovery Point Objective
SEA	Security Awareness Education
SME	Small and Medium Enterprises
SOA	Statement of Applicability
SPoF	Single Point of Failure
SSH	Secure Shell
SÚKL	Státní ústav pro kontrolu léčiv
VIS	Významný informační systém
VPN	Virtual Private Network
ZKB	Zákon o kybernetické bezpečnosti
ZP	Zdravotnický prostředek
ZS	(Informační systém) základní služby

SEZNAM OBRÁZKŮ

Obrázek 1: PDCA model	19
Obrázek 2: Jira workflow	79
Obrázek 3: Blueprint v MS Azure	80

SEZNAM TABULEK

Tabulka 1: Seznam aktiv, první verze	38
Tabulka 2: Zranitelnost a její závažnost.....	45
Tabulka 3: Zranitelnosti – server	46
Tabulka 4: Zranitelnosti – aplikace.....	47
Tabulka 5: Míra inherentního rizika a mez přijatelnosti.....	64
Tabulka 6: Plán prvního stupně certifikačního auditu	66
Tabulka 7: Přehled směrnic, procesů, metrik a cílů souvisejících s ISMS	73

PŘÍLOHY

V příloze je uveden Ganttův diagram znázorňující harmonogram budování systému řízení informační bezpečnosti. Slouží k ilustraci časového rozvržení jednotlivých fází implementace bezpečnostních opatření a certifikace podle normy ISO/IEC 27001.

Task name		+	Duration	End date	Start date	January 2024																												February																	
						01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
1	☐ Zkvalitování zavedení ISO/IEC 27001		2656h	08/04/2025	01/01/2024																																														
1.1	Zkvalitování zvýšení bezpečnosti		808h	20/05/2024	01/01/2024																																														
1.2	Project charter		808h	20/05/2024	01/01/2024																																														
2	☐ Plán implementace		2288h	07/02/2025	05/01/2024																																														
2.1	☐ Příprava smlouvy a podmínek s VUT		104h	26/06/2024	10/06/2024																																														
2.1.1	Podpis smlouvy		80h		10/06/2024																																														
2.1.2	Podpis NDA		32h		21/06/2024																																														
2.2	☐ Podklady pro vytvoření směrníc		920h		11/03/2024																																														
2.2.1	☐ Seznam aktiv		224h		14/05/2024																																														
2.2.1.1	Sepsání seznamu aktiv		224h		14/05/2024																																														
2.2.1.2	Přidělení garantů aktiv		16h 1m		18/06/2024																																														
2.2.2	Nadřazení Organizační strukturu		16h		26/06/2024																																														
2.2.3	Nadřazení Seznam procesů		16h		26/06/2024																																														
2.2.4	Nadřazení Strategie společnosti		16h		26/06/2024																																														
2.2.5	Asistované zhodnocení aktuálního stavu (GAP analýza)		880h		11/03/2024																																														
2.2.6	Akceptace podkladů ze strany VUT		256h		04/07/2024																																														
2.3	☐ Šablony dokumentace od VUT		592h		01/07/2024																																														
2.3.1	Bezpečnostní strategie organizace		280h		01/07/2024																																														
2.3.2	Získat feedback a připomínky k návrhu		39h		05/08/2024																																														
2.3.3	☐ Příručka ISMS		104h		24/07/2024																																														
2.3.3.1	Návrh od VUT		104h		24/07/2024																																														
2.3.4	☐ Bezpečnostní směrnice		56h		22/08/2024																																														
2.3.4.1	Návrhy od VUT		56h		22/08/2024																																														
2.3.5	☐ Model budování bezpečnostního povědomí (SAE)		96h		30/08/2024																																														
2.3.5.1	Návrh od VUT		96h		30/08/2024																																														
2.3.6	☐ Vzor povinné dokumentace dle ISMS		120h		05/09/2024																																														
2.3.6.1	Návrh od VUT		96h		05/09/2024																																														
2.3.6.2	Seznámení se s povinnou dokumentací		24h		23/09/2024																																														
2.3.7	Návrh časového harmonogramu pro implementaci ISMS		40h		23/09/2024																																														
2.3.8	Akceptace dokumentace od VUT - všech dokumentů		32h		07/10/2024																																														
2.4	☐ Penetrační testování		1432h		26/03/2024																																														
2.4.1	Seznamovací služba		2h		26/03/2024																																														
2.4.2	Příprava a podpis smlouvy		160h		22/07/2024																																														
2.4.3	Podpis NDA		120h		29/07/2024																																														
2.4.4	Specifikace parametrů (scope) - příloha smlouvy		88h		30/08/2024																																														
2.4.5	Příprava prostředí, přílohových údajů a dokumentace		48h		30/09/2024																																														
2.4.6	Předání podkladů, seznámení s prostředím		80h		03/10/2024																																														

Task name		Start date	End date	Duration	March 2024																																													
				+	26	27	28	29	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	01	02	03	04	05	06	07	08	09	10	11
1	☒ Zavádění zavedení ISO/IEC 27001	01/01/2024	08/04/2025	2655h																																														
1.1	Zavádění zvýšení bezpečnosti	01/01/2024	20/05/2024	808h																																														
1.2	Project charter	28/02/2024	29/02/2024	16h																																														
2	☒ Plan implementace	05/01/2024	07/02/2025	2288h																																														
2.1	☒ Příprava smlouvy a podmínek s VUT	10/06/2024	26/06/2024	104h																																														
2.1.1	Podpis smlouvy	10/06/2024	21/06/2024	80h																																														
2.1.2	Podpis NDA	21/06/2024	26/06/2024	32h																																														
2.2	☒ Podklady pro vytvoření směrníc	11/03/2024	16/08/2024	920h																																														
2.2.1	☒ Seznam aktiv	14/05/2024	20/06/2024	224h																																														
2.2.1.1	Sepsání seznamu aktiv	14/05/2024	20/06/2024	224h																																														
2.2.1.2	Přidělení garantů aktiv	18/06/2024	20/06/2024	16h 1m																																														
2.2.2	Nasdílet Organizační strukturu	26/06/2024	27/06/2024	16h																																														
2.2.3	Nasdílet Seznam procesů	26/06/2024	27/06/2024	16h																																														
2.2.4	Nasdílet Strategie společnosti	26/06/2024	27/06/2024	16h																																														
2.2.5	Asistované zhodnocení aktuálního stavu (GAP analýza)	11/03/2024	09/08/2024	880h																																														
2.2.6	Akceptace podkladů ze strany VUT	04/07/2024	16/08/2024	256h																																														
2.3	☒ Šablony dokumentace od VUT	01/07/2024	10/10/2024	592h																																														
2.3.1	Bezpečnostní strategie organizace	01/07/2024	16/08/2024	280h																																														
2.3.2	Získat feedback a připomínky k návrhu	05/08/2024	09/08/2024	39h																																														
2.3.3	☒ Příručka ISMS	24/07/2024	09/08/2024	104h																																														
2.3.3.1	Návrh od VUT	24/07/2024	09/08/2024	104h																																														
2.3.4	☒ Bezpečnostní směrnice	22/08/2024	30/08/2024	56h																																														
2.3.4.1	Návrhy od VUT	22/08/2024	30/08/2024	56h																																														
2.3.5	☒ Model budování bezpečnostního povědomí (SAE)	30/08/2024	16/09/2024	96h																																														
2.3.5.1	Návrh od VUT	30/08/2024	16/09/2024	96h																																														
2.3.6	☒ Vzor povinné dokumentace dle ISMS	05/09/2024	25/09/2024	120h																																														
2.3.6.1	Návrh od VUT	05/09/2024	20/09/2024	96h																																														
2.3.6.2	Seznámení se s povinnou dokumentací	23/09/2024	25/09/2024	24h																																														
2.3.7	Návrh časového harmonogramu pro implementaci ISMS	23/09/2024	27/09/2024	40h																																														
2.3.8	Akceptace dokumentace od VUT - všech dokumentů	07/10/2024	10/10/2024	32h																																														
2.4	☒ Penetrační testování	26/03/2024	29/11/2024	1432h																																														
2.4.1	Seznamovací služba	26/03/2024	26/03/2024	2h																																														
2.4.2	Příprava a podpis smlouvy	22/07/2024	16/08/2024	160h																																														
2.4.3	Podpis NDA	29/07/2024	16/08/2024	120h																																														
2.4.4	Specifikace parametrů (scope) - příloha smlouvy	30/08/2024	13/09/2024	88h																																														
2.4.5	Příprava prostředí, přihlašovacích údajů a dokumentace	30/09/2024	07/10/2024	48h																																														
2.4.6	Předání podkladů, seznámení s prostředím	03/10/2024	16/10/2024	80h																																														
					Penetrační testování 26/03/2024 - 29/11/2024																																													
					Workload																																													

[illegible]

Task name		Start date	End date	Duration	+																															
		01/01/2024	08/04/2025	2656h	...																															
1	☐ Zavádění zavedení ISO/IEC 27001	01/01/2024	20/05/2024	808h	...																															
		01/01/2024	20/05/2024	808h	...																															
1.1	Zavádění zvýšení bezpečnosti	01/01/2024	20/05/2024	808h	...																															
1.2	Project charter	28/02/2024	29/02/2024	16h	...																															
2	☐ Plan implementation	05/01/2024	07/02/2025	2288h	...																															
2.1	☐ Příprava smlouvy a podmínek s VUT	10/06/2024	26/06/2024	104h	...																															
2.1.1	Podpis smlouvy	10/06/2024	21/06/2024	80h	...																															
2.1.2	Podpis NDA	21/06/2024	26/06/2024	32h	...																															
2.2	☐ Podklady pro vytvoření směrníc	11/03/2024	16/08/2024	920h	...																															
2.2.1	☐ Seznam aktiv	14/05/2024	20/06/2024	224h	...																															
2.2.1.1	Sepání seznamu aktiv	14/05/2024	20/06/2024	224h	...																															
2.2.1.2	Přidělení garantů aktiv	18/06/2024	20/06/2024	16h 1m	...																															
2.2.2	Nasdílet Organizační strukturu	26/06/2024	27/06/2024	16h	...																															
2.2.3	Nasdílet Seznam procesů	26/06/2024	27/06/2024	16h	...																															
2.2.4	Nasdílet Strategie společnosti	26/06/2024	27/06/2024	16h	...																															
2.2.5	Aktivované zhodnocení aktuálního stavu (CAP analýza)	11/03/2024	09/08/2024	880h	...																															
2.2.6	Akceptace podkladů ze strany VUT	04/07/2024	16/08/2024	256h	...																															
2.3	☐ Šablony dokumentace od VUT	01/07/2024	10/10/2024	592h	...																															
2.3.1	Bezpečnostní strategie organizace	01/07/2024	16/08/2024	280h	...																															
2.3.2	Získat feedback a připomínky k návrhu	05/08/2024	09/08/2024	39h	...																															
2.3.3	☐ Příručka ISMS	24/07/2024	09/08/2024	104h	...																															
2.3.3.1	Návrh od VUT	24/07/2024	09/08/2024	104h	...																															
2.3.4	☐ Bezpečnostní směrnice	22/08/2024	30/08/2024	56h	...																															
2.3.4.1	Návrhy od VUT	22/08/2024	30/08/2024	56h	...																															
2.3.5	☐ Model budování bezpečnostního povědomí (SAE)	30/08/2024	16/09/2024	96h	...																															
2.3.5.1	Návrh od VUT	30/08/2024	16/09/2024	96h	...																															
2.3.6	☐ Vzory povinné dokumentace dle ISMS	05/09/2024	25/09/2024	120h	...																															
2.3.6.1	Návrh od VUT	05/09/2024	20/09/2024	96h	...																															
2.3.6.2	Seznámení se s povinnou dokumentací	23/09/2024	25/09/2024	24h	...																															
2.3.7	Návrh časového harmonogramu pro implementaci ISMS	23/09/2024	27/09/2024	40h	...																															
2.3.8	Akceptace dokumentace od VUT - všech dokumentů	07/10/2024	10/10/2024	32h	...																															
2.4	☐ Penetrační testování	26/03/2024	29/11/2024	1432h	...																															
2.4.1	Seznamovací služba	26/03/2024	26/03/2024	2h	...																															
2.4.2	Příprava a podpis smlouvy	22/07/2024	16/08/2024	160h	...																															
2.4.3	Podpis NDA	29/07/2024	16/08/2024	120h	...																															
2.4.4	Specifikace parametrů (scope) - příloha smlouvy	30/08/2024	13/09/2024	88h	...																															
2.4.5	Příprava prostředí, přiřazení úkolů a dokumentace	30/09/2024	07/10/2024	48h	...																															
2.4.6	Předání podkladů, seznámení s prostředím	03/10/2024	16/10/2024	80h	...																															

July 2024

Aug

01020304050607080910111213141516171819202122232425262728293031010203040506070809101112131415

☐ Workflow

Příručka ISMS ; 24/07/2024 - 09/08/2024

Návrh od VUT

Získat feedback a př...

Akceptace podkladů ze strany VUT

Bezpečnostní strategie organizace

Příprava a podpis smlouvy

Podpis NDA

Task name		Start date	End date	Duration	+
2.3.3	Příněkka ISMS	24/07/2024	09/08/2024	104h	...
2.3.3.1	Návrh od VUT	24/07/2024	09/08/2024	104h	...
2.3.4	Bezpečnostní směrnice	22/08/2024	30/08/2024	56h	...
2.3.4.1	Návrhy od VUT	22/08/2024	30/08/2024	56h	...
2.3.5	Model budování bezpečnostního povědomí (SAE)	30/08/2024	16/09/2024	96h	...
2.3.5.1	Návrh od VUT	30/08/2024	16/09/2024	96h	...
2.3.6	Vzory povinné dokumentace dle ISMS	05/09/2024	25/09/2024	120h	...
2.3.6.1	Návrh od VUT	05/09/2024	20/09/2024	96h	...
2.3.6.2	Seznámení se s povinnou dokumentací	23/09/2024	25/09/2024	24h	...
2.3.7	Návrh časového harmonogramu pro implementaci ISMS	23/09/2024	27/09/2024	40h	...
2.3.8	Akceptace dokumentace od VUT - všech dokumentů	07/10/2024	10/10/2024	32h	...
2.4	Penetrační testování	26/03/2024	29/11/2024	1432h	...
2.4.1	Seznamovací schůzka	26/03/2024	26/03/2024	2h	...
2.4.2	Přprava a podpis smlouvy	22/07/2024	16/08/2024	160h	...
2.4.3	Podpis NDA	29/07/2024	16/08/2024	120h	...
2.4.4	Specifikace parametrů (scope) - příloha smlouvy	30/08/2024	13/09/2024	88h	...
2.4.5	Přprava prostředí, přílohažových údajů a dokumentace	30/09/2024	07/10/2024	48h	...
2.4.6	Předání podkladů, seznámení s prostředím	03/10/2024	16/10/2024	80h	...
2.4.7	Informování řešitelů stran	16/09/2024	20/09/2024	40h	...
2.4.8	Penetrační a záložové testování	16/10/2024	11/11/2024	152h	...
2.4.8.1	Testování serveru	16/10/2024	31/10/2024	96h	...
2.4.8.2	Testování aplikace	24/10/2024	11/11/2024	104h	...
2.4.9	Zpracování zpráv o penetračních testech	15/11/2024	29/11/2024	88h	...
2.5	Referse - legislativní požadavky	05/01/2024	07/02/2025	2288h	...
2.5.1	ISO 81 001-5-1:2021	30/05/2024	10/07/2024	240h	...
2.5.2	AI Act	04/02/2025	07/02/2025	32h	...
2.5.3	NIS2	05/01/2024	05/03/2024	344h	...
3	První etapa - řízení	01/10/2024	31/10/2024	176h	...
3.1	Bezpečnostní strategie	01/10/2024	07/10/2024	40h	...
3.1.1	Kontrola a ověření	01/10/2024	02/10/2024	16h	...
3.1.2	Schválení, podepsání a přetiskopí do VALIDu	03/10/2024	07/10/2024	24h	...
3.1.3	Skolení + vytvoření záznamu	07/10/2024	07/10/2024	8h	...
3.1.4	Prohlášení o vedení a zavádění ISMS	01/10/2024	07/10/2024	40h	...
3.1.4.1	Kontrola a ověření	01/10/2024	02/10/2024	16h	...
3.1.4.2	Schválení, podepsání a přetiskopí do VALIDu	03/10/2024	07/10/2024	24h	...
3.2	Komunikace s 3EC	01/10/2024	17/10/2024	96h 1m	...
3.2.1	Zjistit kolik stojí předauditi	01/10/2024	01/10/2024	8h	...
3.2.2	Dohlavnutí termínu na předauditi	16/10/2024	17/10/2024	8h 1m	...

Task name					Start date	End date	Duration	+	October 2024																												Nov		
2.4.5	Připrava prostředí, přihlašovacích údajů a dokumentace							30/09/2024	07/10/2024	48h	...																												
2.4.6	Předání podkladů, seznámení s prostředím							03/10/2024	16/10/2024	80h	...																												
2.4.7	Informování třetích stran							16/09/2024	20/09/2024	40h	...																												
2.4.8	Penetrační a zátěžové testování							16/10/2024	11/11/2024	152h	...																												
2.4.8.1	Testování serveru							16/10/2024	31/10/2024	96h	...																												
2.4.8.2	Testování aplikace							24/10/2024	11/11/2024	104h	...																												
2.4.9	Zpracování zpráv o penetračních testech							15/11/2024	29/11/2024	88h	...																												
2.5	Referenční - legislativní požadavky							05/01/2024	07/02/2025	2288h	...																												
2.5.1	ISO 81 001-5-1:2021							30/05/2024	10/07/2024	240h	...																												
2.5.2	AI Act							04/02/2025	07/02/2025	32h	...																												
2.5.3	NIS2							05/01/2024	05/03/2024	344h	...																												
3	První etapa - říjen							01/10/2024	31/10/2024	176h	...																												
3.1	Bezpečnostní strategie							01/10/2024	07/10/2024	40h	...																												
3.1.1	Kontrola a ověření							01/10/2024	02/10/2024	16h	...																												
3.1.2	Schválení, podepsání a překlopení do VALIDU							03/10/2024	07/10/2024	24h	...																												
3.1.3	Školení + vytvoření záznamu							07/10/2024	07/10/2024	8h	...																												
3.1.4	Prohlášení o vedení a zavádění ISMS							01/10/2024	07/10/2024	40h	...																												
3.1.4.1	Kontrola a ověření							01/10/2024	02/10/2024	16h	...																												
3.1.4.2	Schválení, podepsání a překlopení do VALIDU							03/10/2024	07/10/2024	24h	...																												
3.2	Komunikace s 3EC							01/10/2024	17/10/2024	96h 1m	...																												
3.2.1	Zjistit kolik stojí předaudit							01/10/2024	01/10/2024	8h	...																												
3.2.2	Domluvení termínu na předaudit							16/10/2024	17/10/2024	8h 1m	...																												
3.3	Seznam aktiv							07/10/2024	15/10/2024	56h	...																												
3.3.1	Kontrola a ověření							07/10/2024	08/10/2024	16h	...																												
3.3.2	Schválení, podepsání a překlopení do VALIDU							09/10/2024	14/10/2024	32h	...																												
3.3.3	Školení vlastních aktiv + vytvoření záznamu							15/10/2024	15/10/2024	8h	...																												
3.4	Příručka ISMS							08/10/2024	22/10/2024	88h	...																												
3.4.1	Kontrola a ověření							08/10/2024	21/10/2024	80h	...																												
3.4.2	Schválení, podepsání a překlopení do VALIDU							17/10/2024	22/10/2024	32h	...																												
3.5	Politika ISMS							14/10/2024	28/10/2024	88h	...																												
3.5.1	Kontrola a ověření							14/10/2024	16/10/2024	24h	...																												
3.5.2	Schválení, podepsání a překlopení do VALIDU							14/10/2024	25/10/2024	80h	...																												
3.5.3	Školení všech - Příručka ISMS a Politika ISMS							28/10/2024	28/10/2024	8h	...																												
3.6	Standardy informační bezpečnosti							02/10/2024	18/10/2024	104h	...																												
3.6.1	Referenční ISO/IEC 27799 - Příprava pro případné asistovan...							02/10/2024	18/10/2024	104h	...																												
3.7	Konec první etapy							31/10/2024	31/10/2024	208h	...																												
4	Druhá etapa - listopad							01/11/2024	06/12/2024	208h	...																												
4.1	Identifikace a hodnocení aktiv							01/11/2024	06/12/2024	208h	...																												

Task name			Start date	End date	Duration	+
3.7	Konec první etapy		31/10/2024	31/10/2024	208h	...
4	Druhá etapa - listopad		01/11/2024	06/12/2024	208h	...
4.1	Identifikace a hodnocení aktiv		01/11/2024	06/12/2024	208h	...
4.1.1	Úprava organizační směrnice		01/11/2024	01/11/2024	8h	...
4.1.2	Kontrola a ověření směrnice		04/11/2024	06/12/2024	200h	...
4.1.3	Hodnocení primárních aktiv		01/11/2024	08/11/2024	48h	...
4.1.4	Hodnocení podpůrných aktiv		04/11/2024	08/11/2024	40h	...
4.1.5	Kontrola a ověření samotného hodnocení aktiv		18/11/2024	22/11/2024	40h	...
4.2	Analýza rizik ISMS		01/11/2024	04/12/2024	192h	...
4.2.1	Úprava organizační směrnice		01/11/2024	15/11/2024	88h	...
4.2.2	Kontrola a ověření směrnice		25/11/2024	29/11/2024	40h	...
4.2.3	Provedení analýzy primárních aktiv		12/11/2024	18/11/2024	40h	...
4.2.4	Provedení analýzy podpůrných aktiv		12/11/2024	04/12/2024	136h	...
4.3	Risk Treatment Plan «ENG»		11/11/2024	04/12/2024	144h	...
4.4	Klasifikace a řízení aktiv		28/11/2024	28/11/2024	8h	...
4.4.1	Úprava organizační směrnice		28/11/2024	28/11/2024	8h	...
4.4.2	Kontrola a ověření směrnice		28/11/2024	28/11/2024	8h	...
4.5	Konec druhé etapy		29/11/2024	29/11/2024	...	...
5	Interní audit		04/12/2024	04/12/2024	...	...
6	Třetí etapa - prosinec		05/12/2024	03/02/2025	344h	...
6.1	Zpracování poznatků z interního auditu		05/12/2024	06/12/2024	16h	...
6.2	Úprava Prohlášení o spolehlivosti		09/12/2024	16/12/2024	48h	...
6.2.1	Udělat z Asistovaného zhodnocení aktuálního stavu		09/12/2024	09/12/2024	8h	...
6.2.2	Přidat Aplikovatelnost, Dokumenty, Datum ověření		09/12/2024	09/12/2024	8h	...
6.2.3	Poslat na ověření zodpovědným osobám		10/12/2024	10/12/2024	8h	...
6.2.4	Schválení a přelápení do VALIDu		10/12/2024	16/12/2024	40h	...
6.3	Deklarace bezpečnostní informací		09/12/2024	24/01/2025	280h	...
6.3.1	Vytvořit a poslat na revizi		09/12/2024	09/12/2024	8h	...
6.3.2	Zveřejnit na webu		13/01/2025	24/01/2025	80h	...
6.4	Úprava bezpečnostní strategie		10/12/2024	02/01/2025	144h	...
6.4.1	Aktualizace bezpečnostní strategie		12/12/2024	12/12/2024	8h	...
6.4.2	Vytvoření Akčního plánu 2025		10/12/2024	02/01/2025	144h	...
6.4.3	Zapojení ostatních + ověření + schválení		30/12/2024	02/01/2025	32h	...
6.5	Úprava Seznamu aktiv		27/12/2024	09/01/2025	80h	...
6.5.1	Rozdělit na kategorie, snížit rozsah		27/12/2024	06/01/2025	56h	...
6.5.2	Přidat procesy z organizační struktury		27/12/2024	30/12/2024	16h	...
6.5.3	Nechat ověřit + schválit + zaskóit		02/01/2025	09/01/2025	48h	...
6.6	Přístupy		30/12/2024	06/01/2025	48h	...

Task name		Start date	End date	Duration	+	December 2024												January 2025											
4.5	Konec druhé etapy	29/11/2024	29/11/2024		...																								
5	Interní audit	04/12/2024	04/12/2024		...																								
6	☒ Třetí etapa - prosinec	05/12/2024	03/02/2025	344h	...																								
6.1	Zpracování poznatků z interního auditu	05/12/2024	06/12/2024	16h	...																								
6.2	☒ Úprava Prohlášení o aplikovatelnosti	09/12/2024	16/12/2024	48h	...																								
6.2.1	Ukládat z Aektovaného zhodnocení aktuálního stavu	09/12/2024	09/12/2024		...																								
6.2.2	Přidat Aplikovatelnost. Dokumenty, Datum ověření	09/12/2024	09/12/2024	8h	...																								
6.2.3	Poslat na ověření zodpovědným osobám	09/12/2024	10/12/2024	8h	...																								
6.2.4	Schválení a přeložení do VALIDu	10/12/2024	16/12/2024	40h	...																								
6.3	☒ Deklarace bezpečnosti informací	09/12/2024	24/01/2025	280h	...																								
6.3.1	Vytvořit a poslat na revizi	09/12/2024	09/12/2024	8h	...																								
6.3.2	Zveřejnit na webu	13/01/2025	24/01/2025	80h	...																								
6.4	☒ Úprava bezpečnostní strategie	10/12/2024	02/01/2025	144h	...																								
6.4.1	Aktualizace bezpečnostní strategie	12/12/2024	12/12/2024	8h	...																								
6.4.2	Vytvoření Akčního plánu 2025	10/12/2024	02/01/2025	144h	...																								
6.4.3	Zapojení ostatních + ověření + schválení	30/12/2024	02/01/2025	32h	...																								
6.5	☒ Úprava Seznamu aktiv	27/12/2024	09/01/2025	80h	...																								
6.5.1	Rozdělit na kategorie, snížit rozsah	27/12/2024	06/01/2025	56h	...																								
6.5.2	Přidat procesy z organizační struktury	27/12/2024	30/12/2024	16h	...																								
6.5.3	Nechat ověřit + schválit + zaskořit	02/01/2025	09/01/2025	48h	...																								
6.6	☒ Přístup	30/12/2024	06/01/2025	48h	...																								
6.6.1	Vytvořit speciální tabulku (součást Seznamu aktiv)	30/12/2024	06/01/2025	48h	...																								
6.7	Aktualizovat a schválit organizační strukturu	13/01/2025	03/02/2025	128h	...																								
6.8	☒ Proces správy aktiv - sjednocení 3 procesů do 1	10/12/2024	20/01/2025	240h	...																								
6.8.1	Sjednotit a nechat ověřit	10/12/2024	20/01/2025	240h	...																								
6.8.2	Schválení + přeložení do VALIDu + zaskoření	17/01/2025	20/01/2025	16h	...																								
6.9	Výběr 20 nejzávažnějších rizikových scénářů	31/12/2024	03/01/2025	32h	...																								
6.10	Rozšíření knihovny externí dokumentace - bezpečnost	23/12/2024	22/01/2025	184h	...																								
6.11	Konec třetí etapy	31/12/2024	31/12/2024		...																								
7	☒ Čtvrtá etapa - leden	31/12/2024	24/01/2025	152h	...																								
7.1	Úprava Analýzy rizik	31/12/2024	16/01/2025	104h	...																								
7.2	Schválení a ověření Analýzy rizik ISMS	13/01/2025	17/01/2025	40h	...																								
7.3	Úprava Plánu zvládnání rizik	02/01/2025	16/01/2025	88h	...																								
7.4	Schválení a ověření Plánu zvládnání rizik	13/01/2025	17/01/2025	40h	...																								
7.5	☒ Fyzické kontroly	01/01/2025	20/01/2025	112h	...																								
7.5.1	Koncová zařízení + kancelář	01/01/2025	20/01/2025	112h	...																								
7.6	Aktualizace procesu Interní audit	16/01/2025	24/01/2025	56h	...																								
7.7	Školení Správa aktiv + Analýza rizik ISMS + Plán zvládnání rizik	20/01/2025	20/01/2025	8h	...																								

Task name		Start date	End date	Duration	+	January 2025																														Fe
6.8	☐ Proces správy aktiv - sjednocení 3 procesů do 1	10/12/2024	20/01/2025	240h	...																															
6.8.1	☐ Sjednotit a nechat ověřit	10/12/2024	20/01/2025	240h	...																															
6.8.2	Schválení + překopírování do VALDU + zaskolení	17/01/2025	20/01/2025	16h	...																															
6.9	Výběr 20 nejzávažnějších rizikových scénářů	31/12/2024	09/01/2025	32h	...																															
6.10	Rozšíření knihovny externí dokumentace - bezpečnost	23/12/2024	22/01/2025	184h	...																															
6.11	Konec třetí etapy	31/12/2024	31/12/2024	...	...																															
7	☐ Čtvrtá etapa - leden	31/12/2024	24/01/2025	152h	...																															
7.1	Úprava Analýzy rizik	31/12/2024	16/01/2025	104h	...																															
7.2	Schválení a ověření Analýzy rizik ISMS	13/01/2025	17/01/2025	40h	...																															
7.3	Úprava Plánu zvládání rizik	02/01/2025	16/01/2025	88h	...																															
7.4	Schválení a ověření Plánu zvládání rizik	13/01/2025	17/01/2025	40h	...																															
7.5	☐ Fyzické kontroly	01/01/2025	20/01/2025	112h	...																															
7.5.1	Koncová zařízení + kancelář	01/01/2025	20/01/2025	112h	...																															
7.6	Aktualizace procesu Interní audit	16/01/2025	24/01/2025	56h	...																															
7.7	Školení Správa aktiv + Analýza rizik ISMS + Plán zvládání rizik	20/01/2025	20/01/2025	8h	...																															
7.8	Konec čtvrté etapy	01/01/2025	01/01/2025	...	...																															
8	Certifikační audit - 1. kolo	03/02/2025	03/02/2025	8h	...																															
9	☐ Pátá etapa - únor, březen	04/02/2025	04/04/2025	352h	...																															
9.1	☐ Zpracování auditní zprávy	04/02/2025	14/02/2025	72h	...																															
9.1.1	Rozplánování priorit	04/02/2025	05/02/2025	16h	...																															
9.1.2	Rozdělení úkolů	05/02/2025	14/02/2025	64h	...																															
9.2	Finding 1 - Definovat kontext	18/02/2025	20/02/2025	24h	...																															
9.3	Finding 2 - Aktualizovat rozsah ISMS	05/02/2025	05/02/2025	8h	...																															
9.4	☐ Finding 3	11/02/2025	19/03/2025	216h	...																															
9.4.1	Identifikace procesů ISMS	11/02/2025	11/02/2025	8h	...																															
9.4.2	Kritéria a metricky procesů ISMS	11/02/2025	19/03/2025	216h	...																															
9.5	Finding 4 - aktualizovat PoA	05/02/2025	27/03/2025	296h	...																															
9.6	☐ Finding 5	19/02/2025	20/02/2025	16h	...																															
9.6.1	Plánování	20/02/2025	20/02/2025	8h	...																															
9.6.2	Definovat příležitosti	19/02/2025	20/02/2025	16h	...																															
9.7	Finding 6 - Interní audit	07/02/2025	28/02/2025	128h	...																															
9.8	Finding 7 - přezkoumání	24/02/2025	05/03/2025	64h	...																															
9.9	OFI 1 - rozhraní a závěšlosti	24/03/2025	26/03/2025	24h	...																															
9.10	OFI 2 - kontakt se zájmovými skupinami	19/02/2025	20/02/2025	16h	...																															
9.11	OFI 3 - zlepšit provázanost definovaných cílů	20/02/2025	28/02/2025	56h	...																															
9.12	Aktualizace interních směrnic	04/02/2025	31/03/2025	320h	...																															
9.13	Školení + kontrola bezpečnosti	01/04/2025	04/04/2025	32h	...																															
10	Certifikační audit - 2.kolo	07/04/2025	08/04/2025	16h	...																															

Task name	February 2025												March 2025											
	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27						
Duration	+																							
6.8	📄 Proces správy aktiv - sjednocení 3 procesů do 1																							
6.8.1	Sjednotit a nechat ověřit																							
6.8.2	Schválení + přeložení do VALIDu + zaškolení																							
6.9	Výběr 20 nejzávažnějších rizikových scénářů																							
6.10	Rozřízení knihovny externí dokumentace - bezpečnost																							
6.11	Konec třetí etapy																							
7	📄 Čtvrtá etapa - leden																							
7.1	Úprava Analýzy rizik																							
7.2	Schválení a ověření Analýzy rizik ISMS																							
7.3	Úprava Plánu zvládnutí rizik																							
7.4	Schválení a ověření Plánu zvládnutí rizik																							
7.5	📄 Fyzické kontroly																							
7.5.1	Koncová zařízení + kancelář																							
7.6	Aktualizace procesu Interní audit																							
7.7	Školení Správa aktiv + Analýza rizik ISMS + Plán zvládnutí rizik																							
7.8	Konec čtvrté etapy																							
8	Certifikační audit - 1. kolo																							
9	📄 Pátá etapa - únor, březen																							
9.1	📄 Zpracování auditní zprávy																							
9.1.1	Rozplánování priorit																							
9.1.2	Rozdělení úkolů																							
9.2	Finding 1 - Definovat kontext																							
9.3	Finding 2 - Aktualizovat rozsah ISMS																							
9.4	📄 Finding 3																							
9.4.1	Identifikace procesů ISMS																							
9.4.2	Kritéria a metricky procesů ISMS																							
9.5	Finding 4 - aktualizovat PoA																							
9.6	📄 Finding 5																							
9.6.1	Plánování																							
9.6.2	Definovat příležitosti																							
9.7	Finding 6 - Interní audit																							
9.8	Finding 7 - přezkoumání																							
9.9	OFI 1 - rozhraní a závislosti																							
9.10	OFI 2 - kontakt se zájmovými skupinami																							
9.11	OFI 3 - zlepšit prováděnost definovaných cílů																							
9.12	Aktualizace interních směrnic																							
9.13	Školení + kontrola bezpečnosti																							
10	Certifikační audit - 2. kolo																							