Zavedení a certifikace systému řízení bezpečnosti informací

Veronica Nicole Kejda

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Veronica Nicole Kejda**
Osobní číslo:	**L21011**
Studijní program:	**B1022A020002 Management rizik**
Forma studia:	**Prezenční**
Téma práce:	**Zavedení a certifikace systému řízení bezpečnosti informací**

Zásady pro vypracování

1. Zpracujte literární rešerši vztahující se k zavedení a certifikaci systému řízení bezpečnosti informací.
2. Proveďte rozdílovou analýzu potřebnou k porovnání stávajícího nastavení zabezpečení informací v organizaci s požadavky normy.
3. Na základě zjištění analýzy navrhněte potřebná opatření pro řízení dokumentace systému řízení bezpečnosti informací.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. CALDER, Alan a WATKINS, Steve. *IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002*. Seventh edition. London: Kogan Page, 2020. ISBN 978-0749496951.
2. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
3. SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. 1. vydání. Plzeň: Vykladatelství a nakladatelství Aleš Čeněk, s.r.o., 2019. ISBN 978-80-7380-765-8.

Další odborná literatura dle doporučení vedoucí bakalářské práce.

Vedoucí bakalářské práce: **Ing. Slavomíra Vargová, PhD.**
Ústav krizového řízení

Datum zadání bakalářské práce: **1. prosince 2023**
Termín odevzdání bakalářské práce: **3. května 2024**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

V Uherském Hradišti dne 4. prosince 2023

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 3. 5. 2024

Jméno a příjmení studenta: Veronica Nicole Kejda

.....
podpis studenta

ABSTRAKT

Bakalářská práce se zaměřuje na problematiku bezpečnosti informací. Cílem práce je zavedení systému pro řízení dokumentace. Teoretická část bude věnována nejen informační, ale také kybernetické bezpečnosti. Zaměří se na samotný systém řízení a bezpečnostní politiku. V praktické části bude pomocí rozdílové analýzy zjištěn aktuální stav plnění či neplnění požadavků normy společnosti. Pro certifikaci bude prostřednictvím prohlášení o aplikovatelnosti zkoumána míra aplikování opatření s ohledem na informační bezpečnost. Výsledkem práce bude vytvoření nového systému, který bude zajišťovat bezpečné a přehledné řízení dokumentace.

Klíčová slova: systém řízení bezpečnosti informací, kybernetická bezpečnost, triáda CIA, posouzení rizik, systém pro řízení dokumentů

ABSTRACT

The bachelor thesis focuses on the issue of information security. The aim of the thesis is to implement a secure system for documentation management. The theoretical part will be devoted not only to information security but also to cyber security. It will be focused on the management system itself and the security policy. The practical part will use a difference analysis to determine the current state of compliance or non-compliance of company´s processes with requirements of ISO 27001:2022 standard. For certification purpose will be used Statement of Applicability to determine the degree of application of measures with regard to information security. The result of the work will be the development of a new system that will provide secure and clear documentation management.

Keywords: information security management system, cybersecurity, CIA triad, risk assessment, document management system

Ráda bych poděkovala vedoucí práce Ing. Slavomíře Vargové, PhD. za její cenné rady a odborné vedení při zpracování bakalářské práce.

OBSAH

ÚVOD

Bezpečnost informací je v dnešní digitální době stále více a více aktuálním tématem. Jedná se o problematiku, která se dotýká značné části populace. Oblast zájmu či ohrožení zahrnuje nejen podniky či organizace, ale také samotné jedince, kteří jakýmkoli způsobem fungují v online prostředí či jej jakoukoli formou využívají. Online svět, jakožto místo, které nemá žádného konkrétního vlastníka, představuje prostor plný nebezpečí. Proto je vyžadována potřeba mít zajištěné formy bezpečnostních opatření.

V dnešní urychlené době markantně roste počet digitálních hrozeb, díky čemuž jsou organizace i samotní uživatele internetu nuceni se před těmito hrozbami chránit. Bohužel je tato doba schopna vytvořit nespočet variant různých kybernetických útoků, přičemž je někdy až nerozeznatelné, co je realita a co ne. Hrozby se mohou vyskytovat v mnoha formách. Nejběžnějšími jsou počítačové viry a škodlivé programy, falešné e-mailové zprávy či webové stránky. Těmito útoky je možné získat citlivé informace uživatelů, ať už se jedná o hesla či o platební údaje. Hackeři mohou proniknout do databází organizací, kde mohou zneužít nejen citlivá data zaměstnanců, ale také know-how či tajná data dané organizace. Proto je třeba mít veškeré citlivé informace velmi dobře zabezpečené. Je nutné mít ve firmách povědomí o tomto tématu, neboť by v nejhorších případech mohly mít fatální následky pro existenci firmy.

Cílem této práce je posoudit současný stav bezpečnosti informací ve společnosti. Je třeba se zaměřit na analýzu aktiv, která by mohla být ohrožena a bude-li to třeba, navrhnout pro taková aktiva ošetření. Je třeba zjistit, jak daná společnost plní požadavky s ohledem na normu bezpečnosti informací. Z důvodu tématu práce a citlivých údajů zde nebude společnost konkrétně jmenována.

Téma bakalářské práce je voleno z důvodu aktuální rozšířenosti problémů spojených s informační bezpečností. Teoretická část se zabývá literární rešerší, která poslouží jako teoretický základ pro tuto práci. V úvodní části je rozebrána kybernetická bezpečnost. Další část bakalářské práce je věnována informační bezpečnosti, jejímž důležitým tématem je triáda CIA. Tato triáda představuje základní ochranu informací a je třeba nad jejím konceptem uvažovat při jakékoli manipulaci s daty. Práce se zaobírá i modelem neustálého zlepšování PDCA, samotným systémem řízení bezpečnosti informací a bezpečnostní politikou.

Aby mohla být pochopena ohrožená aktiva společnosti, na úvod praktické části bude provedeno posouzení rizik. Toto posouzení zahrnuje prvotní identifikaci, následnou analýzu a finální hodnocení rizik. Při vzniku kritických rizik bude nutné těmto rizikům stanovit jejich opatření.

Za pomocí rozdílové analýzy bude následně posouzen aktuální stav zabezpečení a řízení dokumentace. Z této analýzy vyplynou oblasti, u kterých je třeba provést zlepšení nebo je nově implementovat.

Závěrem bakalářské práce bude návrh opatření k zajištění bezpečnosti informací a správu dokumentace. Cílem práce je nastavení nového systému řízení dokumentace, jenž bude splňovat požadavky informační bezpečnosti dle ISO 27001 a řízení dokumentace dle ISO 9001.

I. TEORETICKÁ ČÁST

1 KYBERNETICKÁ A INFORMAČNÍ BEZPEČNOST

První kapitola bakalářské práce se zaměřuje na základní teoretické pojmy spojené s problematikou informační bezpečnosti. Nejprve budou přiblíženy terminologické aspekty v této oblasti, následně budou rozebrány koncepty kybernetické a informační bezpečnosti. Dále bude zkoumán význam bezpečnostního auditu a závěrečná část se bude věnovat metodikám pro řízení bezpečnosti informací.

1.1 Základní terminologie

Aktiva představují veškeré hodnotové prvky, které organizace vlastní či využívá k dosažení svých cílů. Jsou základem každé firmy a mohou zahrnovat finanční prostředky, produkty, služby, informace, technologie či lidské zdroje. Jejich ochrana je zásadní pro stabilitu a úspěch organizace. Je třeba si uvědomit, že aktivem nemusí být jen to, co firma vlastní a také nemusí mít vždy fyzickou podobu. (Aptien, 2023)

Bezpečnostní incident označuje jakékoli porušení bezpečnosti, které může nastat jak v informačních systémech, tak v elektronických komunikačních sítích. K bezpečnostnímu incidentu může dojít v důsledku kybernetických událostí, přičemž toto porušení může ohrozit bezpečnost dat či funkčnost služeb. (Sedlák, Konečný, 2021)

Data jsou v počítačovém prostředí informace, které byly převedeny do formy, jež je efektivní pro pohyb nebo zpracování. Vzhledem k dnešním počítačům a přenosovým médiím jsou data informace převedena do binární digitální podoby. Data nyní zahrnují textové, zvukové a obrazové informace, a také záznamy protokolů a webových aktivit. (Vaughan, 2019)

Hrozba představuje možnou událost s potenciálem způsobit nežádoucí incident, který by mohl vést k poškození systému nebo organizace. (Jirásek et al., 2015) Hrozby lze rozlišit dle úmyslu jako hrozby náhodné a úmyslné, nebo podle zdroje na hrozby vnitřní a vnější. Dále se klasifikují podle dopadu na systém, kde se rozlišují aktivní a pasivní hrozby. (Šulc, 2018)

Informace je jakékoli sdělení nebo zobrazení znalostí, jako jsou fakta, údaje nebo názory, a to v jakémkoli médiu nebo formě, například textové, číselné, grafické, kartografické, narativní nebo audiovizuální. (NIST, 2024)

Kybernetická kriminalita označuje trestný čin, při kterém kdokoli neoprávněně proniká do počítačových systémů a manipuluje s jejich obsahem, aniž by k tomu měl oprávnění.

Přestože se jedná o závažný problém, z dlouhodobého hlediska může být pro organizace méně nebezpečný než samotné kybernetické války. (Calder, Watkins, 2020)

Kybernetická válka představuje realitu současného světa, kde každá významná teroristická či zločinecká organizace disponuje schopnostmi v oblasti kybernetiky. Tyto schopnosti využívá k plánování a provádění digitálních útoků. (Calder, Watkins, 2020)

Kybernetický prostor, jako virtuální realita, existuje bez hranic, tudíž bez začátku a konce, avšak zcela závisí na fyzických technologiích, které fungují v reálném světě. (Kolouch, Bašta, 2019)

Kybernetický útok je v téhle době stále častější, nákladnější a mnohem sofistikovanější. Útočníci cílí na kritickou infrastrukturu zemí, včetně veřejných služeb, obranných systémů a mechanismů řízení letového provozu a dopravy. (Augenbaum, 2019)

Plán kontinuity je systém prevence a obnovy po potenciálních hrozbách pro společnost. Plán zajišťuje ochranu zaměstnanců a majetku, a také se zaměřuje na zajištění provozuschopnosti a obnovy provozu v případě havárie či jiných mimořádných událostí. Zahrnuje definování všech rizik, která mohou ovlivnit činnost společnosti, a je tak důležitou součástí strategie řízení rizik organizace. Rizika mohou zahrnovat přírodní katastrofy, blackouty či kybernetické útoky. (Investopedia, 2024)

Riziko představuje šance na to, že se stane nepříznivá událost s potenciálně negativními důsledky. Lze jej definovat jako pravděpodobnost vzniku nežádoucích důsledků v daném časovém intervalu nebo za určitých podmínek. (VÚBP, 2024)

Zranitelnost může být charakteristikou aktiva, což znamená, že není omezena pouze na softwarové prvky, ale může se vyskytovat také v hardwaru, procesech a lidských faktorech, které jsou součástí informačního systému. (Šulc, 2018)

1.2 Kybernetická bezpečnost

V poslední dekádě se kybernetická bezpečnost stala jedním z klíčových bodů mnoha národních politik. Tento nárůst popularity je způsoben překročením hranic do jiných bezpečnostních oblastí a rovněž kvůli incidentům, které tuto problematiku nechvalně proslavily, vystavily veřejnému zájmu a přiměly širokou veřejnost přemýšlet o důležitosti a nutnosti zabezpečení v kyberprostoru. S tím souvisí naléhavá potřeba chránit kyberprostor tak, aby byla zajištěna co nejvyšší míra komplexní bezpečnosti České republiky a zároveň respektována práva jednotlivců na informační sebeurčení. (Kolouch, Bašta, 2019)

Zahrnuje různá opatření, která jsou implementována za účelem chránit počítačové systémy před neoprávněným přístupem nebo útokem. Tyto opatření zahrnují prvky právní, organizační, technické a vzdělávací, které slouží k zabezpečení kybernetického prostoru. (Kolouch, Bašta, 2019) Kybernetický prostor je v podstatě veřejným prostranstvím, což znamená, že nepatří nikomu konkrétnímu – žádné organizaci, osobě ani státu. Z toho důvodu je nutné, aby byla bezpečnostní opatření pečlivě řízena mezi různými subjekty a na různých úrovních. V této souvislosti je důležité, aby tyto subjekty aktivně sdílely informace o potenciálních rizicích a byly připraveny reagovat na nebezpečí, které může ohrozit nebo narušit kybernetický prostor. (Doucek et al., 2019) Obrázkem 1 jsou vyobrazeny oblasti kybernetické bezpečnosti.

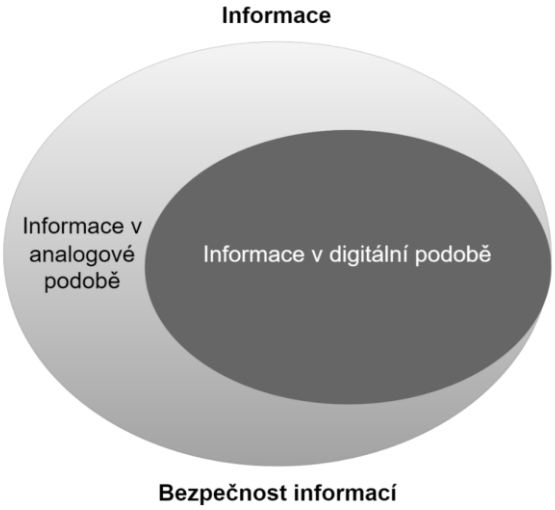
Obrázek 1 - Kybernetická bezpečnost. Zdroj: Doucek et al., 2019

1.3 Informační bezpečnost

Bezpečnost informací (Information Security) má za cíl primárně zajistit, aby byly informace chráněny s ohledem na jejich důvěrnost, integritu a dostupnost. (Doucek et al., 2019) Internet je digitálně nebezpečný prostor. Organizace musí podniknout vhodné kroky k ochraně před trestnou činností jak zvenčí, tak i zevnitř, stejným způsobem, jakým se chrání ve fyzickém světě. (Calder, Watkins, 2020)

Informační bezpečnost zahrnuje nástroje a procesy, které organizace používají k ochraně informací. To zahrnuje nastavení politik, které brání neoprávněným osobám v přístupu k podnikovým či osobním informacím. Bezpečnost informací chrání citlivé informace před neoprávněnými činnostmi, včetně prohlížení, úpravy, záznamu a jakéhokoli narušení nebo

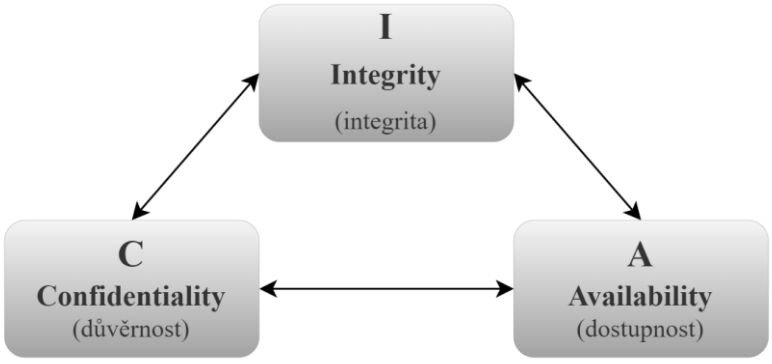
zničení. Cílem je zajistit bezpečnost a ochranu kritických dat, jako jsou údaje o zákaznících, finanční údaje nebo duševní vlastnictví. Následky bezpečnostních incidentů zahrnují krádež soukromých informací, manipulaci s daty a jejich smazání. Útoky mohou narušit pracovní procesy, poškodit pověst společnosti a mohou také vést k hmatatelným nákladům. (Imperva, 2024) Oblasti spadající do bezpečnosti informací graficky znázorňuje Obrázek 2.



Obrázek 2 - Informační bezpečnost. Zdroj: Doucek et al., 2019

1.4 Triáda CIA

Triáda CIA, graficky vyobrazena Obrázkem 3, představuje základní pilíř informační bezpečnosti. Definuje tři klíčové aspekty rizik spojených s daty, informacemi a znalostmi. Zkratka CIA zastupuje tři základní vlastnosti bezpečnosti informací, a to konkrétně důvěrnost (Confidentiality), integritu (Integrity) a dostupnost (Availability). (Aptien, 2023)



Obrázek 3 - Triáda CIA. Zdroj: Kolouch, Bašta, 2019

1.4.1 Důvěrnost

Jedná se o zásadní pojem v oblasti bezpečnosti informací věnující se zajištění ochrany citlivých dat a informací, a to nejen před neoprávněným přístupem, ale i před jejich sdílením či únikem. Zajišťuje, že k citlivým údajům mají přístup pouze oprávněné osoby. (Šulc, 2018)

Pro zajištění důvěrnosti je třeba informace správně klasifikovat. Klasifikační schéma se odvíjí nejen podle sektoru, ale také podle požadavků jednotlivých organizací.

Ve státní sféře se využívá následujícího klasifikačního schématu:

1. **Přísně tajné (Top Secret)** – Jedná se o nejvyšší stupeň důvěrnosti a neoprávněné zpřístupnění takových informací může mít až fatální dopad na národní bezpečnost.
2. **Tajné (Secret)** – Neoprávněné zpřístupnění těchto informací může závažně ohrozit národní bezpečnost.
3. **Důvěrné (Confidential)** – Neoprávněné umožnění vstupu k takovým informacím může mít značný dopad na národní bezpečnost.
4. **Citlivé, ale neklasifikované (Sensitive but Unclassified)** – Nežádoucí zpřístupnění citlivých informací by nemělo mít zásadní dopad na národní bezpečnost.
5. **Neklasifikované (Unclassified)** – Informace se nacházejí na nejnižším stupni. Pokud by došlo k jejich neoprávněnému zpřístupnění, nemělo by to na národní bezpečnost žádný dopad. (Šulc, 2018)

V případě komerční sféry se často uvádí jednodušší schéma obsahující následující stupně:

1. **Důvěrné (Confidential)** – Nejvyšší stupeň, kde by nežádoucí zpřístupnění těchto informací mohlo mít až katastrofální dopad na společnost. K důvěrným informacím mají přístup pouze vybraní zaměstnanci. K takovému stupni patří strategické plány společností či zdrojové kódy.
2. **Soukromé (Private)** – V případě neoprávněného zveřejnění soukromých informací, jako jsou osobní údaje nejen zaměstnanců, ale i klientů, by mohly být důsledky velmi negativní.
3. **Citlivé (Sensitive)** – Do této skupiny se řadí informace o projektech či cenovém vývoji. Neoprávněné zpřístupnění by mohlo ohrozit bezpečnost firemních plánů s nepříznivými následky.

4. **Veřejné (Public)** – Takové informace se nacházejí na nejnižším stupni a dle názvu je patrné, že jsou určeny pro veřejnost. Nedovolené zveřejnění by nemělo mít významný dopad na společnost, neboť do této kategorie spadají pouze údaje jako telefonní čísla, jména zaměstnanců nebo e-mailové adresy. (Šulc, 2018)

1.4.2 Integrita

Integrita definuje stav, ve kterém jsou informace, data, počítačové systémy a jejich nastavení chráněny před neoprávněným zásahem či manipulací. Tento stav zajišťuje, že pouze osoba s odpovídajícím oprávněním může provádět jakékoli změny či úpravy v těchto systémech.

Definujeme čtyři úrovně integrity:

1. **Nízká** – V tomto případě aktivum nepotřebuje ochranu vzhledem k integritě a porušení integrity nepředstavuje hrozbu pro legitimní zájmy dotyčné osoby.
2. **Střední** – Zde aktivum může vyžadovat ochranu, a pokud by došlo k jeho poškození, mohlo by to ohrozit oprávněné zájmy osob s méně závažnými dopady. Pro zajištění integrity na této úrovni jsou používány běžné metody, jako například omezení přístupových práv pro zápis.
3. **Vysoká** – Pokud se aktivum nachází v této úrovni, je vyžadována ochrana. Narušení integrity způsobuje poškození legitimních zájmů osob s významnými dopady na klíčová aktiva. K zajištění integrity se využívají speciální prostředky umožňující identifikaci osoby provádějící změny.
4. **Kritická** – Na této úrovni je ochrana aktiv nezbytná. Jakékoli narušení integrity by mohlo mít vážné důsledky pro oprávněné zájmy osoby. Pro zachování integrity se používají speciální prostředky pro jednoznačnou identifikaci osoby provádějící změny, jako je například technologie digitálního podpisu. (Kolouch, Bašta, 2019)

1.4.3 Dostupnost

Dostupnost lze popsat jako zajištění přístupu k informacím, datům či počítačovým systémům v době, kdy je to potřeba.

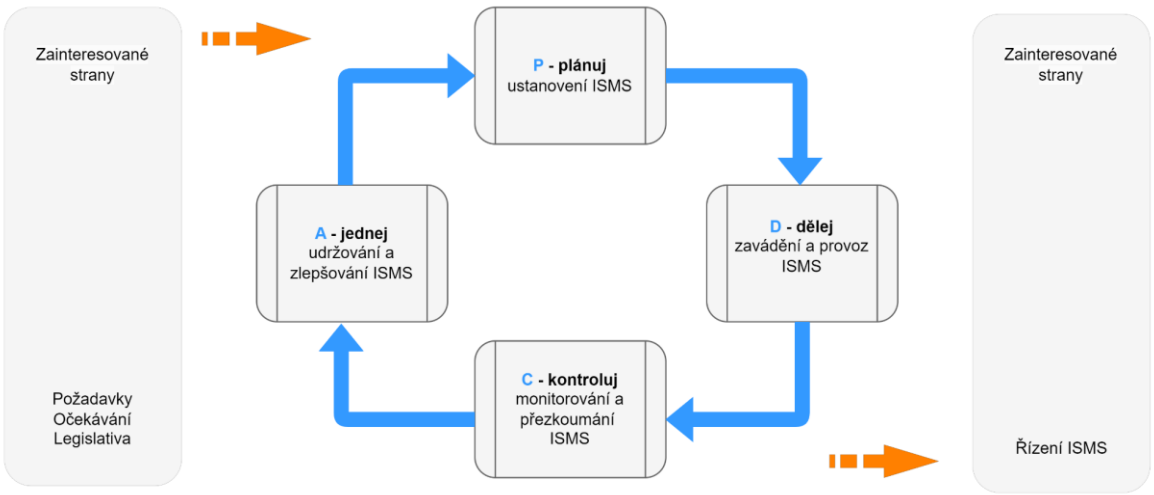
Lze definovat čtyři úrovně dostupnosti:

1. **Nízká** – V případě nízké úrovně není narušení dostupnosti aktiva prioritní a je obvykle akceptováno delší časové období pro jeho obnovu v případě výpadku. Pro zajištění ochrany dostupnosti postačuje pravidelné provádění zálohování.

2. **Střední** – Na úrovni střední by nemělo narušení přesahovat pracovní dobu. Delší výpadky by mohly představovat potenciální riziko. Pro zabezpečení se využívají standardní postupy zálohování a obnovy.
3. **Vysoká** – Nároky na dostupnost neumožňují poruchy trvající déle než několik hodin. Každý výpadek musí být okamžitě řešen, neboť může představovat přímé ohrožení zájmů. Aktiva jsou považována za klíčová, a proto jsou k zajištění ochrany zavedeny záložní systémy.
4. **Kritická** – Jakékoli přerušení dostupnosti aktiv je nepřijatelné, a i krátkodobý výpadek trvající několik málo minut může vážně ohrozit legitimní zájmy. Aktiva jsou v tomto případě považována za kritická. K zajištění dostupnosti se využívají záložní systémy a obnova poskytování služeb probíhá rychle a automaticky. (Kolouch, Bašta, 2019)

1.5 Model Plan-Do-Check-Act

PDCA cyklus, známý také jako Demingův cyklus, představuje metodiku postupného zlepšování kvality výrobků, služeb, procesů, aplikací či dat k vyšší úrovni. Tento cyklus se skládá ze čtyř fází, které jsou znázorněny Obrázkem 4: Plan (Plánuj) – Do (Dělej) – Check (Kontroluj) – Act (Jednej). (Sedlák, Konečný, 2023)



Obrázek 4 - Model PDCA. Zdroj: Břicháček, 2015

V první fázi plánování se zaměřuje na přípravu a definování cílů a strategií pro zlepšení. Druhým krokem je realizace, během níž se provádí zamýšlené kroky. Poté přichází fáze kontroly, kde se prověřuje dosažený výsledek, který se porovnává s původními záměry.

Poslední fází je fáze jednání, kde se na základě výsledků provedené kontroly provádí případné korekce a úpravy plánu. Následně dochází k implementaci zlepšení do praxe. (Sedlák, Konečný, 2023)

1.5.1 Užití modelu v systému řízení bezpečnosti informací

Proces PDCA pochází z oblasti zajištění kvality a nyní je požadavkem normy ISO/IEC 27001: 2013 pro systémy řízení bezpečnosti informací (ISMS). Je-li norma ISO 27001 analyzována pomocí cyklu PDCA, poskytuje lepší představu o implementaci řízení.

1. Fáze – „Plan“: Zavedení ISMS

Tato fáze normy ISO 27001 pomáhá organizaci stanovit rozsah cílů a kontrol ISMS. Při implementaci plánovací fáze je třeba analyzovat vnější a vnitřní problémy společnosti. Identifikace těchto problémů může organizaci pomoci při implementaci postupů ISMS a při odstraňování překážek.

2. Fáze – „Do“: Implementace ISMS

V této fázi organizace implementuje a využívá politiku, kontrolní mechanismy, procesy a postupy ISMS. Organizace vytváří hodnocení rizik a vyhodnocuje důvody, které stojí za každou její strukturou. Připravuje řadu postupů s uvedením rizik a jejich ošetření. Musí zajistit, aby dokumentace postupů a politik byla dostupná, adekvátně chráněna, distribuována a uložena ve spravovaném systému. Dokumenty externího původu musí spadat do rozsahu ISO 27001. Tímto způsobem je následně fáze „Do“ splněna.

3. Fáze – „Check“: Monitorování a přezkoumání ISMS

Tato fáze zahrnuje kontroly monitorování, měření, analýzy a hodnocení v rámci organizace. Odpovědné osoby musí měřit výkonnost procesů v porovnání se zásadami, cíli a praktickými zkušenostmi v dokumentovaném postupu stanoveném v předchozí fázi. Odpovědní vedoucí pracovníci musí předložit veškeré výsledky, po nichž následuje implementace výsledků těchto politik. Je to nejlepší způsob, jak zkontrolovat, kde byly problémy identifikovány, ošetřeny, odstraněny a kde je nutné je revidovat a zlepšit.

4. Fáze – „Act“: Aktualizace a zlepšení ISMS

Organizace musí přijmout nápravná a preventivní opatření na základě výsledků interního auditu ISMS a přezkoumání vedením. Může být jmenován vedoucí pracovník pro informace, který bude zodpovědný za monitorování a měření bezpečnosti informací. Řídící pracovník

musí jednat na základě jakéhokoli zjištění, které se týká porušení bezpečnosti informací. Nedílnou součástí normy ISO 27001 je neustálé zlepšování. Norma vyžaduje, aby se organizace neustále zlepšovaly a eliminovaly tak další hrozby. (Bestpractice.biz, 2020)

1.5.2 Aplikace v praxi

Aby mohla být metoda PDCA úspěšně aplikována, je nezbytné zajistit, aby byla bezpečnost informací vnímána jako opakující se činnost, nikoli pouze jako jednorázový projekt. Prvním krokem k dosažení tohoto cíle je vytvoření stálého týmu pro bezpečnost informací. Tým absolvuje pravidelné schůzky, které jsou naplánovány v pevně stanovených intervalech (např. měsíčně nebo čtvrtletně). Pravidelné schůzky jak s týmem, tak s vedením, pomáhají dosahovat neustálého zlepšování a efektivního řízení. Program schůzek by měl být založen na metodě PDCA. Začíná se zpětným přezkoumáváním metrik a zpětnou vazbou z minulých setkání (Check), následuje rozhodování o předchozích změnách a formulování nových opatření (Act). Činnost „Do“ se odehrává mezi schůzkami. (Otterloo, 2017)

Důležité je však vyvarovat se příliš mnoha experimentům. Myšlenka PDCA spočívá v tom, že se experimenty provádějí postupně, neboť je třeba získat jasné informace o jejich účinnosti. Dobré týmy informační bezpečnosti si proto dávají na čas a každý měsíc nebo čtvrtletí provedou jen několik málo změn. (Otterloo, 2017)

1.6 Audit a certifikace

ISACA (Information Systems Audit and Control Association) je mezinárodní asociace zaměřující se na oblasti auditu, řízení, kontroly a bezpečnosti informačních systémů. Také poskytuje certifikace, standardy a vzdělávací programy v oblasti informační technologie, dále jen „IT“, a bezpečnosti informací. Standardy ISACA přinášejí potřebné informace ke splnění potřeb odborníků v oblasti auditu a ověřování dodržování předpisů. Zároveň poskytují základní pokyny ke zlepšení efektivity a účinnosti. (Smejkal et al., 2019)

Audit představuje systematický proces, který je důkladně dokumentovaný a nezávislý na subjektech, které zkoumá. Jeho účelem je shromažďovat důkazy a analyzovat je s cílem posoudit, do jaké míry jsou splněna stanovená kritéria. Předmětem analýzy jsou definované oblasti, které mohou zahrnovat fyzické prostory, organizační struktury, prováděné činnosti či procesy. (Sedlák, Konečný, 2023)

Certifikační audit je účinným a ekonomicky výhodným prostředkem ke splnění požadavků na nezávislou kontrolu bezpečnosti informací, a zároveň slouží k prokázání shody s normou

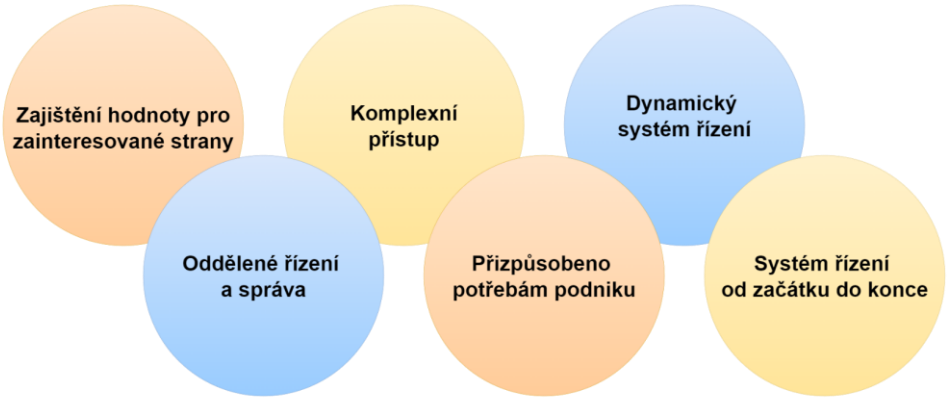
ISO 27001. Tento typ auditu často využívá negativního hodnocení, což znamená, že se zaměřuje především na odhalování nedostatků než na hodnocení adekvátnosti. Jeho úkolem je prověřit, zda dokumentované postupy, procesy a skutečné aktivity organizace, včetně záznamů o implementaci, odpovídají požadavkům normy ISO 27001. Výsledkem auditu je pak písemná zpráva, která je obvykle dostupná krátce po jeho dokončení, obsahující seznam neshod a pozorování spolu s navrženými nápravnými opatřeními. (Calder, Watkins, 2020)

1.7 Metodiky řízení bezpečnosti informací

Přístupové metodiky k řízení informací jsou navrhovány s cílem zajistit jejich celkovou bezpečnost z různých perspektiv a s ohledem na určitá omezení. Tyto metodiky mohou být aplikovány nezávisle na sobě nebo v kombinaci částečné či úplné. Kombinace těchto metod pak může vést k efektivní implementaci správy bezpečnosti informací. (Smejkal et al., 2019)

1.7.1 Control Objectives for Information and Related Technology

Zkratka COBIT nese označení pro Kontrolní cíle pro informační a související technologie. Tato metodika je mezinárodně uznávaná a úzce spjata s organizací ISACA, jež ji vyvinula. Je klíčovým nástrojem podporujícím efektivní řízení informačních technologií v organizacích. (Smejkal et al., 2019) Následující Obrázek 5 prezentuje principy systému řízení.

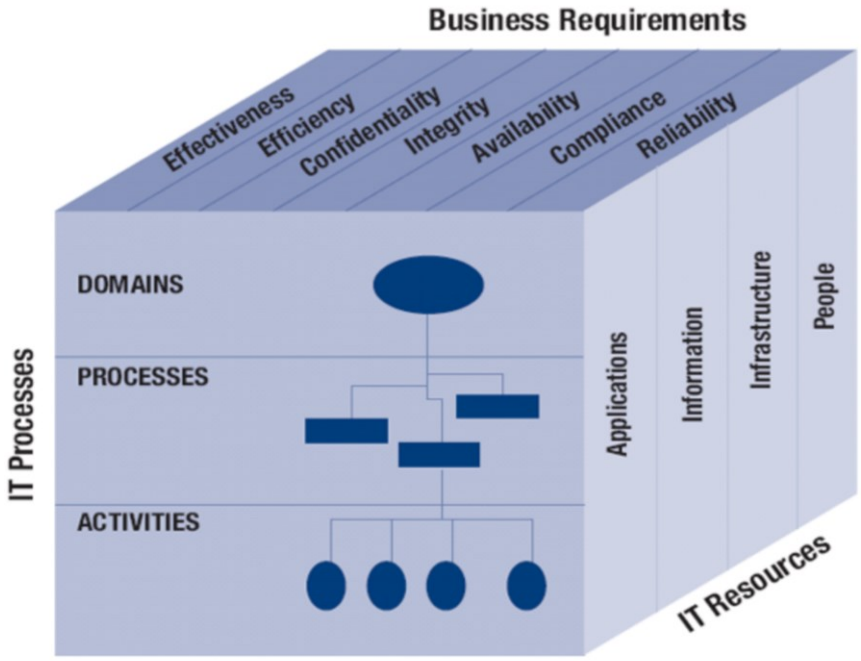


Obrázek 5 - Principy systému řízení. Zdroj: Smejkal et al., 2019

Metodika COBIT si klade za cíl přehledně uspořádat složité systémy řízení IT tak, aby byla tato struktura srozumitelná jak pro vedoucí pracovníky, tak pro uživatele bez podrobných znalostí IT. Umožňuje jim stanovit adekvátní objektivní kritéria pro vyhodnocování

úspěšnosti nebo neúspěšnosti jednotlivých aspektů řízení IT. COBIT se zaměřuje na spojení zásad obecného řízení organizace s pravidly platnými v IT prostředí. Při vytváření této metodiky byly použity osvědčené postupy a zdroje zahrnující například COSO (Committee of Sponsoring Organizations), ITIL (Information Technology Infrastructure Library), ISO/IEC 27000 a další. (Sedlák, Konečný, 2023)

Základní principy této metodiky lze vyobrazit Obrázkem 6 pomocí COBIT kostky, která se skládá ze tří základních komponent: zdrojů IT (IT Resources), procesů IT (IT Processes) a informačních kritérií (Business Requirements). Zdroje IT zahrnují aplikace (Applications), informace (Information), personál (People) a infrastrukturu (Infrastructure), zatímco procesy IT zahrnují domény (Domains), procesy (Processes) a aktivity (Activities). Mezi kritéria informací patří nejen důvěrnost (Confidentiality), integrita (Integrity) a dostupnost (Availability), ale také spolehlivost (Reliability), účinnost (Efficiency), dodržování (Compliance) a efektivita (Effectiveness). (Sedlák, Konečný, 2023)

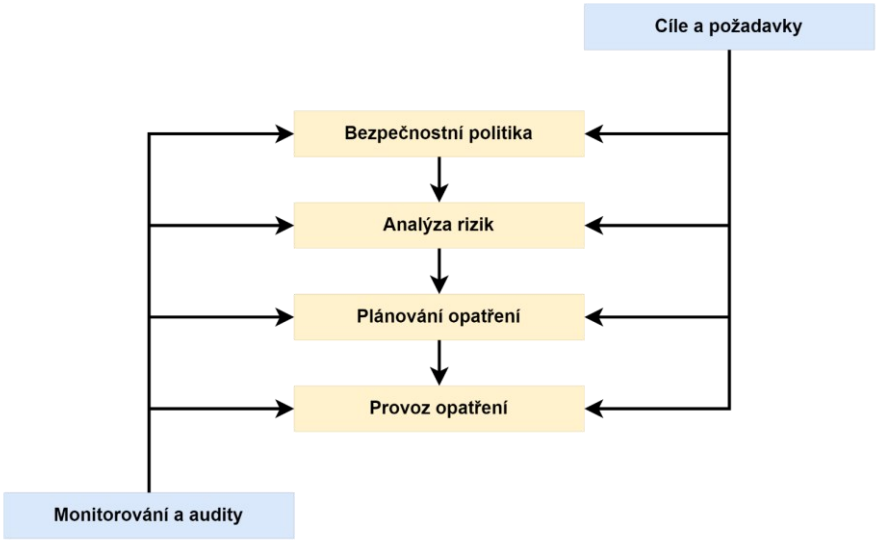


Obrázek 6 - COBIT Kostka. Zdroj: Kidd, 2019

1.7.2 Information Technology Infrastructure Library

Jedná se o rámec pro zajištění poskytování kvalitních IT služeb za přijatelné náklady, vycházející z osvědčených praktik. Aktuálně je považován za mezinárodní standard pro správu IT služeb. Knihovna ITIL je strukturována do různých částí, které se specializují

na konkrétní oblasti správy IT služeb a vzájemně se doplňují. Dodávka IT služeb (IT Service Delivery) a podpora IT služeb (IT Service Support) jsou běžně označovány jako řízení IT služeb ITSM (IT Service Management). ITIL není normou, ale obsahuje doporučení a osvědčené postupy. Díky svému rámcovému charakteru jsou výstupy všech poskytovatelů v daném odvětví vzájemně kompatibilní a univerzálně použitelné. Jejich provázanost vykresluje Obrázek 7 níže. (Sedlák, Konečný, 2023)



Obrázek 7 - Základní procesy řízení bezpečnosti informací dle ITIL.
Zdroj: Sedlák, Konečný, 2023

ITIL zahrnuje následující oblasti:

- strategie služeb, soustředící se na celkovou strategii poskytování IT služeb,
- návrh služeb, který průběžně posuzuje a navrhuje služby,
- přechod služeb, zabývající se řízením a plánováním změn,
- průběžné zlepšování služeb, včetně měření a analýzy problémů za účelem optimalizace,
- provoz služeb, jež spravuje provozní záležitosti pomocí podpůrných opatření, jako je zálohování dat. (Sedlák, Konečný, 2023)

V současnosti je nejaktuálnější verzí ITIL 4, jehož zásadním prvkem je hodnotový řetězec služeb (Service Value Chain), který umožňuje poskytování IT služeb pomocí moderních metodik a přístupů. ITIL 4 je vytvořen s důrazem na komplexní řízení procesů poskytování služeb, které zahrnuje čtyři základní dimenze relevantní pro každou organizaci:

1. organizace a lidé,
2. informace a technologie,
3. partneři a dodavatelé,
4. procesy.

V této verzi je stanoveno sedm hlavních principů, které jsou formulovány obecně, díky čemuž je lze aplikovat na organizace jakéhokoli rozsahu. V průběhu realizace programu jsou tyto principy upravovány, aby lépe odpovídaly konkrétním potřebám a vztahům mezi jednotlivými pracovními skupinami.

Těmito principy jsou:

1. **Zaměřte se na hodnotu (Focus on Value).** Organizace se zaměřuje na hodnotu poskytovaných služeb, přičemž klade důraz na vyvážení zájmů všech subjektů procesu, včetně uživatelů, poskytovatelů služeb a externích účastníků.
2. **Začněte tam, kde jste (Start Where You Are).** Při navrhování procesů je doporučeno zhodnotit současné postupy a upravit je tak, aby co nejlépe odpovídaly potřebám organizace.
3. **Postupujte iterativně se zpětnou vazbou (Progress Iteratively with Feedback).** V metodice je klíčové strukturování aktivit do menších a dobře spravovatelných částí, které je možné rychle provést a dokončit. Je nezbytné před každou iterací zkontrolovat zpětnou vazbu.
4. **Spolupracujte a propagujte svou viditelnost (Collaborate and Promote Visibility).** Spolupráce není požadována pouze mezi týmy v rámci poskytovatele služeb, ale je klíčová i ve vztahu k zákazníkům, uživatelům a dodavatelům. Je důležité spolupracovat s kýmkoli dalším, kdo se účastní vašich projektů.
5. **Myslete a pracujte v celkovém kontextu (Think and Work Holistically).** Důležité je, aby byly veškeré činnosti prováděny v souladu s ostatními, a aby dosažené výsledky byly zhodnocovány nejen samostatně, ale také ve spojitosti s celkovým požadovaným cílem.
6. **Držte to jednoduché a praktické (Keep It Simple and Practical).** Klíčem je se zaměřit na jednoduchost a praktičnost, díky čemuž se minimalizuje složitost

a maximalizuje efektivita. Je třeba se soustředit na ty prvky, které přinášejí skutečnou hodnotu, namísto sledování složitých procesů.

7. **Optimalizujte a automatizujte (Optimize and Automate).** Je třeba optimalizovat využití všech dostupných zdrojů s maximální efektivitou. To zahrnuje automatizaci na místech, kde je to možné, s cílem minimalizace manuální práce. Snahou je zapojit lidské zdroje pouze do činností, které nelze automatizovat. (Smejkal et al., 2019)

2 SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

Information Security Management System, známý pod zkratkou ISMS, se zaměřuje na systematický přístup nastavení, implementování, udržování a zdokonalování bezpečnosti informací tak, aby byly dosaženy stanovené cíle. Tento systém vychází z analýzy rizik a rozhodnutí organizace o přijetí úrovně rizika, která byla navržena pro efektivní zpracování a řízení těchto rizik. (ÚNMZ, 2023)

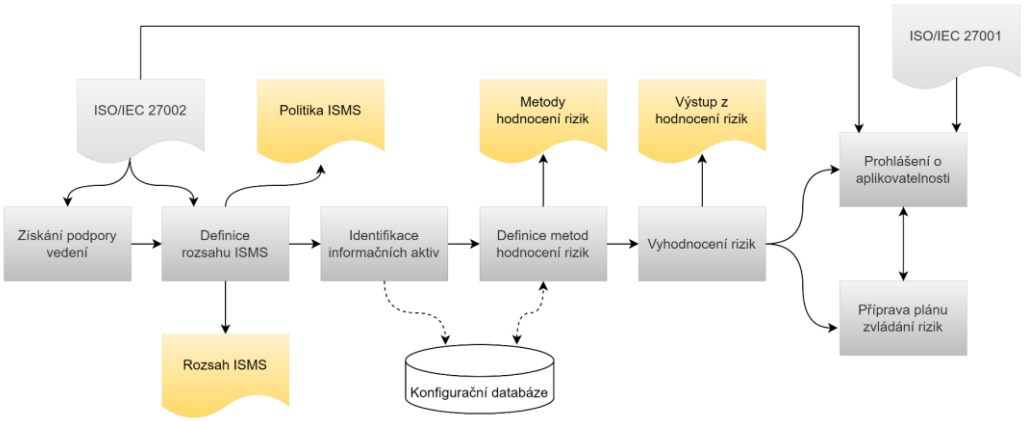
V této části bude zpracována problematika jednotlivých fází ISMS, stejně jako standardy a interní požadavky, které jsou klíčové pro správu informační bezpečnosti.

2.1 Fáze ISMS

Fáze ISMS zahrnují ustanovení, implementaci, monitorování, přezkoumání, údržbu a zlepšování. Organizace musí projít řadou postupných činností, které obsahují množství povinných požadavků, jež vyžadují provádění specifických úkonů, aktivit a procesů. Tyto požadavky jsou rozděleny do následujících kategorií: kontext organizace, vedení, plánování, podpora, provoz, hodnocení výkonnosti a zlepšení. (Humphreys, 2016)

2.1.1 Ustanovení ISMS

Prvním krokem cyklu PDCA v ISMS je ustanovení, během kterého se definuje rozsah, formulují politiky a systematicky se přistupuje k hodnocení rizik. Obrázek 8 ilustruje celou podstatu tohoto kroku. Při zajišťování podpory vedení organizace se často setkáváme s nedostatkem povědomí o výhodách implementace ISMS podle ISO/IEC 27001:2013 pro Systém managementu bezpečnosti informací. V této fázi je nezbytné přesvědčit vedení o přínosech. Určení rozsahu ISMS udává, která oddělení budou začleněna do systému řízení informační bezpečnosti. (Břicháček, 2015)

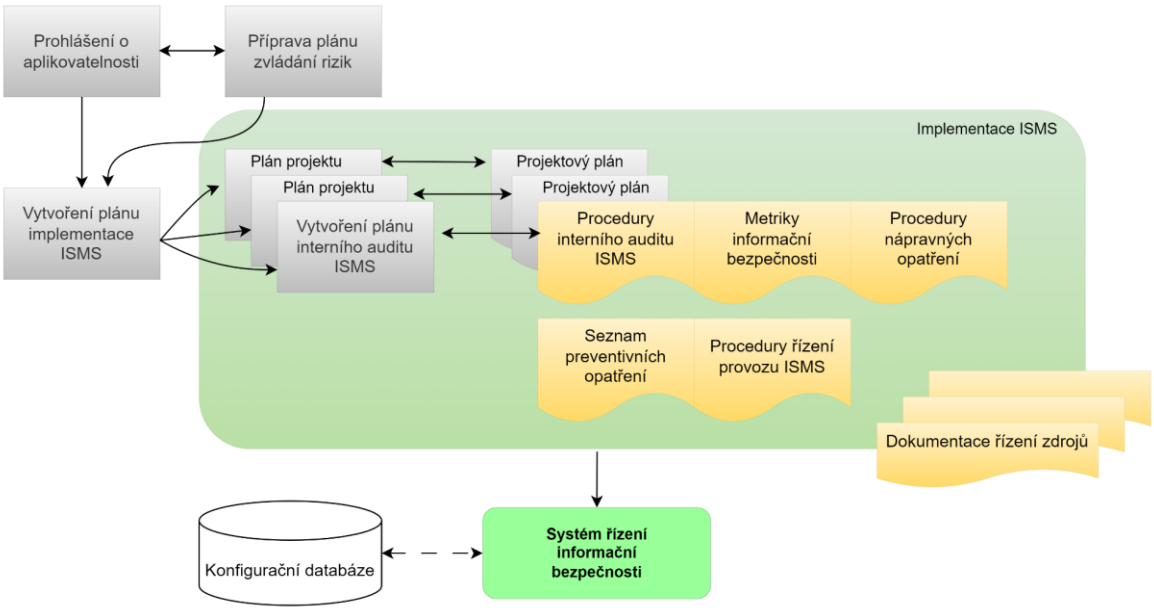


Obrázek 8 - Ustanovení ISMS. Zdroj: Břicháček, 2015

Základem pro další kroky, jako je hodnocení rizik a plánování opatření pro jejich zvládnutí, je identifikace informačních aktiv. Je zde připraveno prohlášení o aplikovatelnosti systému řízení informační bezpečnosti spolu s plánem zvládání v případě ohrožení bezpečnosti informací. Po zvážení rizik management schvaluje zbývající rizika, což je důležitý krok směrem k implementaci a provozu ISMS. (Břicháček, 2015)

2.1.2 Implementace ISMS

Po dokončení fáze ustanovení následuje fáze implementace, během které se připravuje plán a jeho realizace formou konkrétních projektů, včetně plánování interního auditu, aplikace strategií do praxe či úprava směrnic. Plánování implementace ISMS následuje po vyhodnocení prohlášení o použitelnosti a vypracování plánu řízení rizik. Při aplikaci normy je vhodné rozdělit standard na jednotlivé projekty s vlastními plány. V této fázi se uskutečňuje zavedení systému, vytváření postupů pro interní audit, definice metrik a sestavení seznamu nápravných a preventivních opatření pro identifikovaná rizika. Následuje již samotná implementace ISMS a příprava příslušné dokumentace. Tyto kroky vysvětluje Obrázek 9. (Břicháček, 2015)



Obrázek 9 - Implementace ISMS. Zdroj: Břicháček, 2015

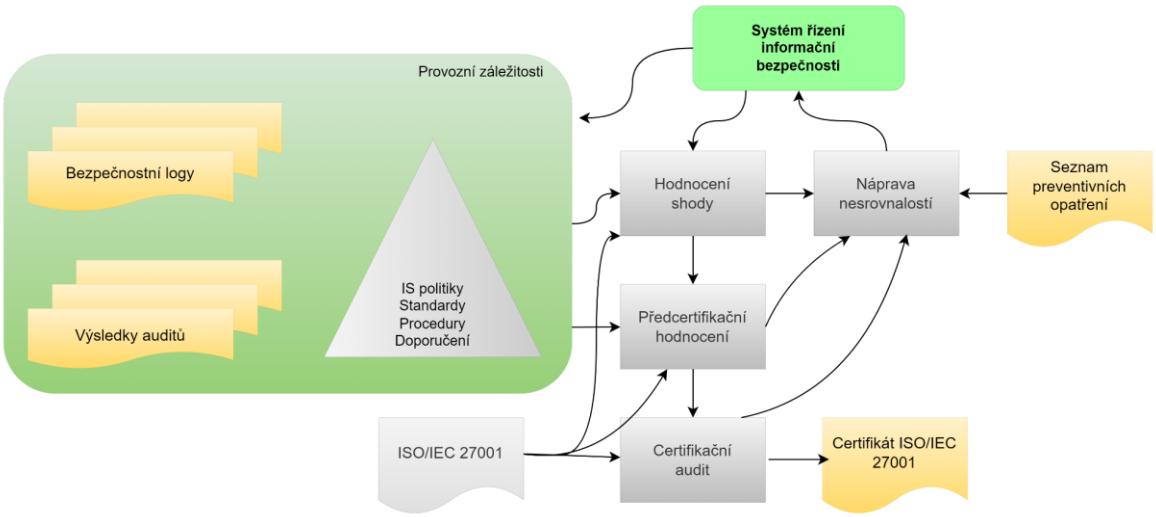
2.1.3 Monitorování a přezkoumání ISMS

Pro zajištění souladu s požadavky během implementace systému je nezbytné pravidelné sledování a provádění dalších kontrolních opatření. Tato kontrolní opatření jsou vykovávána

buď interními, nebo externími auditory v přesně definovaných časových intervalech. (Břicháček, 2015)

Hodnocení souladu zahrnuje revizi zbývajícího rizika a jeho přijatelnosti vzhledem ke změnám v organizaci, právním předpisům nebo novým požadavkům regulačních orgánů. Pro zajištění účinného provádění kontrol a auditů informačních systémů je nezbytné mít k dispozici dostatečné informace, jako jsou politiky, standardy, procedury a doporučení. Hodnocení shody slouží k ověření, zda systém odpovídá jak interním, tak externím požadavkům. (Břicháček, 2015)

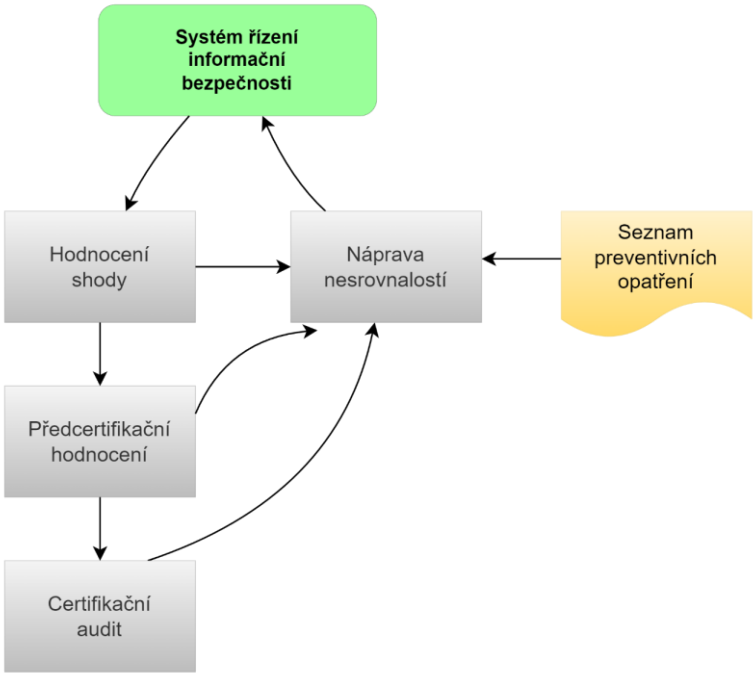
Předcertifikační posouzení poskytuje nezávislý pohled na fungování ISMS po stabilizaci systému, zatímco certifikační audit zajišťuje shodu s normou ISO/IEC 27001 a praktický provoz ISMS. Pokud se během kontrol objeví nedostatky, jsou tyto řešeny v rámci procesu údržby a zlepšování ISMS. Na Obrázku 10 je přehledně zobrazeno, jak probíhá tato fáze. (Břicháček, 2015)



Obrázek 10 - Monitorování a přezkoumání ISMS. Zdroj: Břicháček, 2015

2.1.4 Údržba a zlepšování ISMS

Závěrečnou etapou celého PDCA cyklu je údržba a zlepšování ISMS, zobrazena na Obrázku 11. Úkolem této fáze je zhodnotit výsledky auditů a kontrolních činností týkajících se účinnosti zavedených bezpečnostních opatřená a samotného ISMS. Tyto výsledky pak slouží jako podnět pro spuštění dalšího cyklu PDCA. V tomto novém cyklu budou provedena a zhodnocena veškerá nápravná a preventivní opatření. Společně s řízením kvality umožňuje vedení organizací systematické řízení informačních bezpečnostních procesů. Zahrnuje také provádění nápravných a preventivních opatření. (Břicháček, 2015)



Obrázek 11 - Údržba a zlepšování ISMS. Zdroj: Břicháček, 2015

2.2 Standardy bezpečnosti informací

Původně bylo vydávání standardů řízeno státními institucemi. Avšak v dnešní době jsou standardy často publikovány přímo organizacemi specializujícími se na oblast počítačové a komunikační technologie. (Smejkal et al., 2019)

Na mezinárodní úrovni jsou hlavními vydavateli standardů Mezinárodní elektrotechnická komise (International Organization Commission – IEC) a Mezinárodní organizace pro normalizaci (International Organization for Standardization – ISO). ISO, jako mezinárodní standardizační organizace, má za členy národní organizace specializující se na vydávání standardů v různých zemích. Naopak IEC je celosvětovou institucí, která se zaměřuje na vytváření a publikaci mezinárodních norem v oblastech elektrotechniky, elektroniky, sdělovací techniky a souvisejících odvětvích. V rámci bezpečnosti informací tyto organizace úzce spolupracují. (Smejkal et al., 2019)

Mimo tyto standardizační organizace existují v oblasti informační bezpečnosti aktivní i další subjekty, které plní podobné funkce na národní úrovni. Jedním z příkladů může být Národní institut standardů a technologie ve Spojených státech amerických. (Smejkal et al., 2019)

2.2.1 ISO/IEC 27001:2013

ISO/IEC 27001 je základní normou řady ISO/IEC 27000. Tato norma specifikuje požadavky na zavedení, implementaci, monitorování a správu systémů řízení bezpečnosti informací (ISMS). Součástí této skupiny norem jsou také ISO/IEC 27002, 27003, 27004 a 27005, které nabízejí pokyny a doporučení pro implementaci ISMS a splnění požadavků ISO/IEC 27001. Tato norma spadá do skupiny norem, které jsou známy pod zkratkou MSS (Management Systems Standards), česky označovány jako Standardy řízení systémů. MSS zahrnuje normy jako ISO 9001 (řízení kvality), ISO 14001 (environmentální management), ISO 22000 (bezpečnost potravin) a ISO 20000-1 (IT Service Management). (Humphreys, 2016)

2.2.2 National Institute of Standards and Technology

Národní institut standardů a technologie (dále jen „NIST“) vytváří a publikuje normy a směrnice, nabízí odbornou pomoc v oblasti technologické a vede výzkum v oblasti počítačů a telekomunikačních sítí. (Smejkal et al., 2019)

NIST navrhuje a připravuje normy, směrnice, pokyny a další zdroje v oblasti kybernetické bezpečnosti, které odpovídají potřebám amerického průmyslu, federálních úřadů a širší veřejnosti. Zároveň rozvíjí povědomí o rizicích v oblasti ochrany soukromí, z nichž některá přímo souvisejí s kybernetickou bezpečností, a zlepšuje jejich řízení. (NIST, 2024)

2.3 Aktualizace normy ISO/IEC 27001:2013 na verzi 2022

Na konci října 2022 Mezinárodní organizace pro normalizaci (ISO) vydala novou verzi normy ISO/IEC 27001:2022. Norma ISO 27001:2022 představuje mírnou aktualizaci předchozí verze normy: ISO 27001:2013. Tato aktualizace se zaměřuje zejména na body normy 4 až 10. Nová verze normy zachovává stejný počet ustanovení jako předchozí verze, ale text byl mírně upraven s cílem lepšího sladění s ostatními normami ISO pro management. (A-LIGN, 2023)

K podstatným změnám došlo v příloze A, kdy tato příloha prošla kompletní revizí a přepracováním. Tato nová verze představuje významné zjednodušení, které zahrnuje snížení počtu kontrol ze 114 na 93 a nové rozdělení do čtyř sekcí místo původních čtrnácti. Tyto čtyři sekce tvoří oblasti organizační kontroly, kontroly osob, fyzické kontroly a technologické kontroly. (Eucert, 2023)

Hlavní změny se týkají plánování, definování kritérií procesů a standardů monitorování. Společnosti, které chtějí získat certifikaci podle normy ISO 27001:2022, budou muset

aktualizovat svá prohlášení o použitelnosti a zajistit, že nové požadavky budou zahrnuty do jejich systému ISMS. Důležité je si uvědomit, že tato aktualizace neovlivňuje platnost stávajících certifikací podle normy ISO 27001:2013, neboť jejich platnost vyprší k 30. dubnu 2024. (A-LIGN, 2023)

Organizace, které jsou v současnosti certifikovány podle normy ISO 27001:2013, mají čas do 31. října 2025 na přechod na novou revizi normy. Je však doporučeno, aby začaly co nejdříve aktualizovat své procesy a mechanismy tak, aby odpovídaly požadavkům této nové revize. (A-LIGN, 2023)

2.4 ISO/IEC 9001:2015

S bezpečnosti informací se pojí také norma ISO/IEC 9001:2015. Bod 7.5 normy, jenž nese název Dokumentované informace, požaduje po společnosti dokumentované postupy pro řízení dokumentace. Dle normy je nutné zajistit aktuálnost a vhodnost veškeré dokumentace, je požadováno zajistit dostupnost jakékoli dokumentované informace a v souvislosti s bezpečnosti informací také zajistit vhodnou ochranu a uchování dokumentace. (ÚNMZ, 2016)

2.5 Souvislost mezi ISMS a DMS

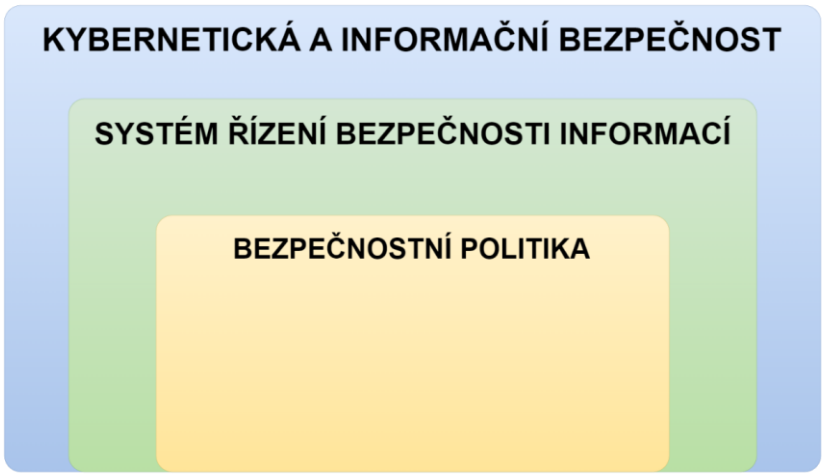
Souvislost mezi systémem řízení bezpečnosti informací (ISMS) a systémem pro správu dokumentů (DMS) se nachází v normě ISO/IEC 27001:2013. Nachází se v bodě 7.5, který nese název Dokumentované informace. Konkrétně se jedná o body 7.5.2 Vytváření a aktualizace dokumentovaných informací a 7.5.3 Řízení dokumentovaných informací. (ÚNMZ, 2014) V nově vydané verzi normy ISO/IEC 27001:2022 zůstává členění i znění bodů normy stejné. (ÚNMZ, 2023)

3 BEZPEČNOSTNÍ POLITIKA

Bezpečnostní politika představuje soubor pravidel, směrnic a postupů, které určují, jak spravovat, chránit a distribuovat veškerá aktiva organizace, včetně důvěrných informací. Tyto úkony jsou prováděny v souladu s normou ISO 27001:2013. (Doucek et al., 2019)

Politika bezpečnosti informací by měla brát v úvahu charakter podniku, jeho organizaci, umístění, majetek a technologii. Je vhodné, aby politika zahrnovala nebo odkazovala na rámec pro stanovení cílů bezpečnosti informací. Důležité je také zohlednit všechny relevantní obchodní, právní, regulační a smluvní bezpečnostní požadavky. Je nezbytné stanovit strategický kontext pro organizaci a rizikové faktory, ve kterých bude ISMS fungovat, včetně kritérií pro hodnocení a struktury hodnocení rizik. Politika by měla být pravidelně revidována a aktualizována s ohledem na měnící se okolnosti, prostředí a zkušenosti. (Calder, Watkins, 2020)

Obrázek 12 vyobrazuje provázanost jednotlivých kapitol zaměřených na informační bezpečnost. Oblast, která zahrnuje všechny ostatní kapitoly, nese název „Kybernetická a informační bezpečnost“. V bakalářské práci se jedná o kapitolu 1, která představuje celkovou podstatu bezpečnostních opatření. Na tuto kapitolu úzce navazuje kapitola 2 s názvem „Systém řízení bezpečnosti informací“. Při této kapitole již dochází k samotné implementaci ISMS a v obrázku je graficky zpracována uprostřed. V rámci obou kapitol se zde nachází poslední kapitola 3 pro Bezpečnostní politiku. Tato kapitola zahrnuje samotná pravidla spojená s informační bezpečností.



Obrázek 12 - Provázanost kapitol. Zdroj: Vlastní zpracování

Tato kapitola zacílí na klíčové aspekty bezpečnosti informací a ochrany osobních údajů. Bude zde rozebrána fyzická bezpečnost, nařízení o ochraně osobních údajů a legislativní požadavky v této oblasti. Poslední část kapitoly bude vyhrazena bezpečnostním týmům.

3.1 Fyzická bezpečnost

I přesto, že jsou technická opatření na ochranu počítačových dat klíčová, mnoho bezpečnostních problémů či incidentů souvisí s krádeží nebo ztrátou samotných zařízení. Incidenty mohou nastat i při likvidaci zastaralého vybavení nebo mohou být data získána z jiných hardwarových zařízení, jako jsou flash paměti a pevné disky. (Nezmar, 2017)

V oblasti fyzické bezpečnosti je nezbytné zvážit různé aspekty, jako je kvalita dveří a zámků, instalace alarmových systémů, osvětlení zajišťující bezpečnost prostoru a kamerový dohled. Dále je důležité řešit správu přístupu do budov a areálů, například prostřednictvím čipových karet nebo monitorováním pohybu osob v prostorách. (Nezmar, 2017)

3.2 General Data Protection Regulation

Neboli zkráceně GDPR, je obecné nařízení o ochraně osobních údajů. Jedná se o právní rámec, jež platí v celé Evropské unii. Slouží k zajištění ochrany práv občanů před neoprávněným zpracováním a manipulací s jejich osobními údaji či daty. Toto nařízení přebírá a upravuje veškeré předchozí postupy a principy ochrany osobních údajů, které tvoří základ evropského systému ochrany osobních údajů. (Nezmar, 2017)

Zpracování osobních údajů zahrnuje veškeré činnosti týkající se osobních údajů, bez ohledu na to, zda jsou prováděny ručně nebo pomocí automatizovaných prostředků. Tyto činnosti zahrnují shromažďování, ukládání, sdílení, vyhledávání, organizaci či jakékoli jiné zpracování, odstranění nebo zničení osobních údajů. (Nezmar, 2017)

Osobními údaji jsou jakékoli informace, které jsou spojeny s identifikovanou nebo identifikovatelnou živou osobou. Mezi příklady osobních údajů patří jméno a příjmení, adresa bydliště, číslo identifikační karty nebo například IP adresa. (European Commission, 2024)

3.3 Legislativní požadavky

Internet jako komplexní síťový systém není právnickou subjektivitou, ale spíše globálním prostředím propojujícím jednotlivce a firmy po celém světě. Využívání internetových služeb je rozšířené mezi různými subjekty, ať už jsou to jednotlivci či právnické osoby. V případě,

že je zapotřebí zkoumat odpovědnost za nezákonné činy, je nanejvýš důležité zohlednit jak národní (včetně trestněprávních i občanskoprávních), tak mezinárodní nástroje (například Úmluva o kybernetické kriminalitě). (Kolouch, 2016)

3.3.1 Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 definuje práva a povinnosti jednotlivců a rozsah působnosti a pravomoci veřejných institucí v oblasti kybernetické bezpečnosti. Důvody přijetí tohoto zákona souvisejí s nárůstem různých forem terorismu, včetně kybernetického terorismu, a neustále se zvyšující závislost společnosti na informačních technologiích. Cílem zákona je zlepšit spolupráci mezi soukromým sektorem a veřejnou správou, aby bylo možné účinněji řešit kybernetické bezpečnostní incidenty a zvýšit celkovou bezpečnost kybernetického prostoru. (Smejkal et al., 2019)

3.3.2 Směrnice NIS

Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 se snaží dosáhnout vysoké úrovně bezpečnosti sítí a informačních systémů v rámci Evropské unie. Tato směrnice je navržena s cílem posílit bezpečnost informačních a komunikačních technologií v členských státech unie. (Sedlák, Konečný, 2021)

Účelem směrnice NIS (Network Information Security) je stanovit základní kritéria, jež by měla být naplněna všemi členskými státy. Směrnice byla zveřejněna a účinně vstoupila v platnost v srpnu 2016. (Duračinská, 2016) Evropská unie nyní rozšiřuje a prohlubuje svůj rámec s novou směrnicí o kybernetické bezpečnosti, která nese označení NIS2. Změny, které s sebou tato směrnice přináší, jsou natolik podstatné, že Národní úřad pro kybernetickou a informační bezpečnost, dále jen „NÚKIB“, reagoval přípravou úplně nového právního předpisu a jeho vyhlášek v oblasti kybernetické bezpečnosti. Podle transpoziční lhůty stanovené ve směrnici NIS2 musí nový zákon nabýt účinnosti do 18. října 2024. (NÚKIB, 2024)

3.4 Bezpečnostní tým

Týmy odpovědné za bezpečnost mají rozsáhlé spektrum úkolů spojených s řešením bezpečnostních incidentů v různých kontextech, jako jsou státy, organizace, sítě či komunity. Jejich činnosti sahají od preventivních opatření a zvyšování povědomí přes detekci, monitorování a reakci na incidenty, až po vyhodnocování získaných zkušeností. Hlavním

účelem těchto týmů je zabezpečit rychlou a efektivní reakci na kybernetické bezpečností události. (Sedlák, Konečný, 2021)

V rámci bezpečnosti v digitálním prostředí existují v České republice dva bezpečnostní týmy podporované zákonem. Vládní CERT, řízený NÚKIB, a Národní CERT, známý též jako CSIRT.CZ. Národní je spravován asociací CZ.NIC, a to na základě veřejnoprávní smlouvy podepsané s NÚKIB. (Sedlák, Konečný, 2021)

3.4.1 CERT

Computer Emergency Response Team, česky označován jako Tým pro reakci na počítačové hrozby, se zabývá řešením problémů, které mají rozsáhlé důsledky pro kybernetickou bezpečnost, a vyvíjí pokročilé metody a nástroje k jejich řešení. (Moyle, 2024)

3.4.2 CSIRT

Computer Security Incident Response Team, česky Tým pro reakci na bezpečnostní incidenty, je skupina specializující se na identifikaci, analýzu a řešení různých hrozeb v oblasti kybernetiky. (Moyle, 2024)

4 CÍLE A POUŽITÉ METODY

Cílem práce je nastavení systému řízení dokumentace společnosti, který bude splňovat požadavky z pohledu bezpečnosti informací ISO 27001 a řízení dokumentace dle ISO 9001. Nejdříve bude třeba posoudit stávající stav organizace a zjistit v rámci gap analýzy řízení dokumentů a záznamů dle normy ISO 27001. Výstupem práce bude vývoj nového systému DMS.

Rozdílová analýza, známá také jako srovnávací či gap analýza, slouží k posouzení úrovně bezpečnosti informací v organizaci a porovnání s doporučenými postupy stanovenými v normách řady 27000. Jedná se o zhodnocení odchylek od normy ISO/IEC 27001. Princip této analýzy spočívá v porovnání aktuálního stavu s referenčním stavem a identifikace případných rozdílů. Cílem je poskytnout komplexní posouzení zabezpečení informací bez ohledu na jejich formu nebo způsob zpracování. (Sedlák, Konečný, 2023)

Analýza je založená na identifikaci a posouzení aktiv. Na základě stanovených kritérií se provádí gap analýza s následujícím vyhodnocením: splněno/částečně splněno/nesplněno. Hlavní výhodou této metody je poskytnutí vyváženého a podrobného přehledu o stavu bezpečnosti informací v organizace spolu s konkrétními doporučeními pro řešení identifikovaných nedostatků, které jsou kategorizovány podle priority a obtížnosti provedení. (Sedlák, Konečný, 2023)

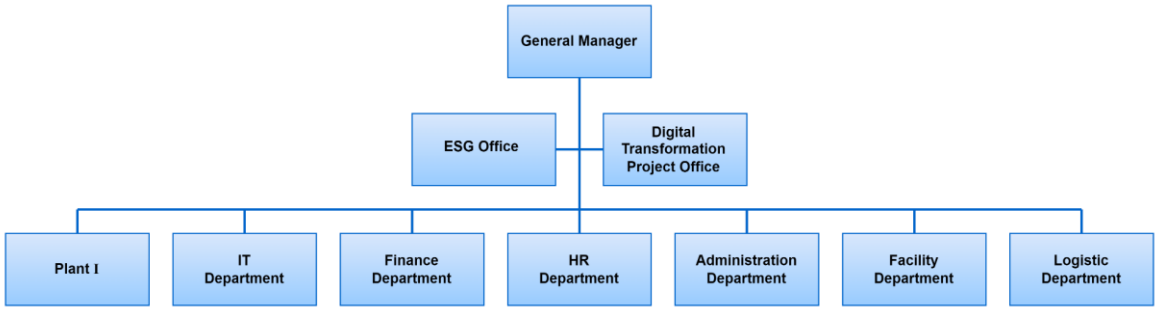
II. PRAKTICKÁ ČÁST

5 CHARAKTERISTIKA SPOLEČNOSTI

Společnost, na kterou je bakalářská práce zaměřena, rozprostírá pobočky po celém světě. Specializuje se na výrobu a servis serverů a datových věží a zaujímá významné postavení mezi výrobci elektronických zařízení. V České republice má společnost přibližně 600 zaměstnanců, avšak celosvětově zaměstnává více než 60 000 pracovníků. Certifikované systémy společnosti jsou vytvářeny s ohledem na požadavky a potřeby zákazníků a zahrnují certifikace v oblasti řízení kvality (ISO 9001:2015), environmentálního managementu (ISO 14001:2015), bezpečnosti a ochrany zdraví při práci (ISO 45001:2018), energetické efektivity (ISO 50001:2018), emisí skleníkových plynů (ISO 14064-1:2018) a specifikací pro správu škodlivých látek v elektronických výrobcích (QC 080000:2017). Společnost je rovněž pravidelně podrobována přísným bezpečnostním auditům, jež jsou prováděny samotnými zákazníky.

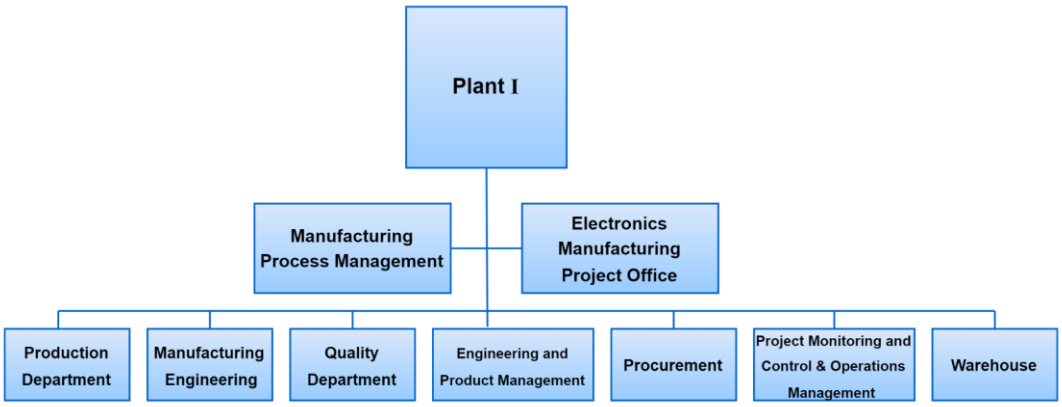
5.1 Organizační struktura

Obrázek 13 vyobrazuje základní organizační strukturu společnosti.



Obrázek 13 - Organizační struktura společnosti. Zdroj: Interní dokumentace

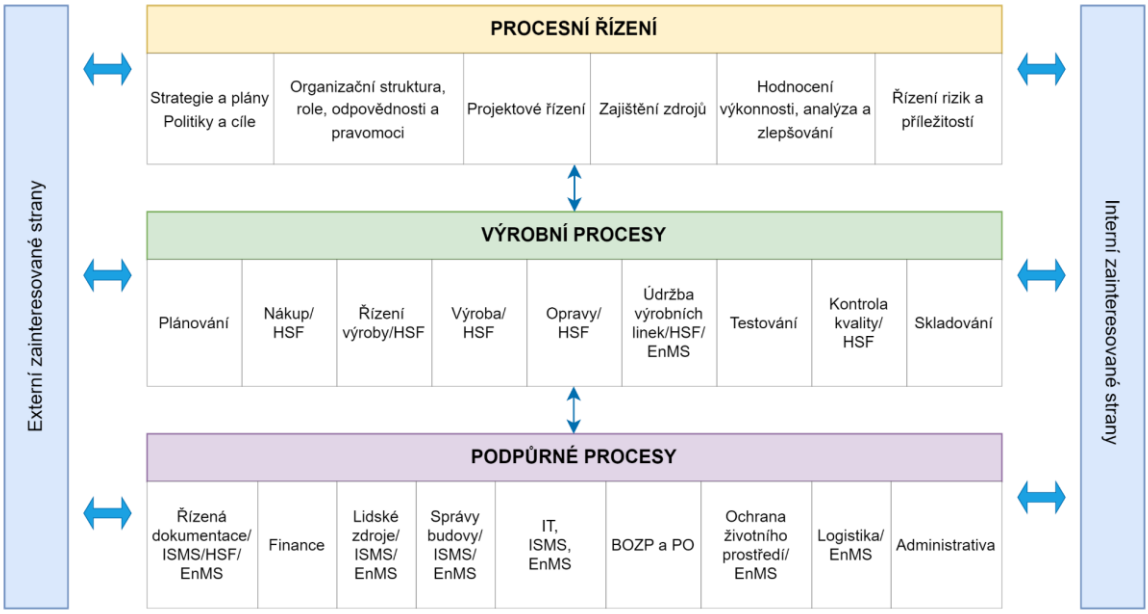
Obrázkem 14 je znázorněna rozšířená organizační struktura začínající výrobním závodem.



Obrázek 14 - Rozšířená organizační struktura. Zdroj: Interní dokumentace

5.2 Procesní mapa

Procesní mapa na Obrázku 15 vykresluje nejen vzájemnou interakci různých částí společnosti, ale zobrazuje také oblasti, které souvisí s ISMS.



Obrázek 15 - Procesní mapa. Zdroj: Interní dokumentace

5.3 Odpovědnosti v rámci ISMS

Za bezpečnost informací ve společnosti zodpovídají pozice zástupce vedení, člen Bezpečnostní komise a ISMS specialista. Všechny pozice spolu úzce spolupracují a zajišťují veškeré kroky k ochraně citlivých dat. Podílí se na tvorbě a realizaci bezpečnostních opatření, kterým společně dozorují.

5.3.1 Zástupce vedení

Pracovní pozice tohoto typu má za úkol dohlížet nad zaváděním požadavků normy ISO 27001 do procesů společnosti. Zajišťuje, že zavedený systém ISMS odpovídá požadavkům normy a připravuje a přezkoumává programy auditů. Je odpovědný za předkládání zpráv o výkonnosti ISMS včetně příležitostí ke zlepšení a vede interní audity společnosti. Mezi jeho funkce spadá také přezkoumání a aktualizace ISMS manuálu a souvisejících systémových dokumentů a v neposlední řadě organizuje školení a vzdělávání, které souvisejí s ISMS.

5.3.2 Člen Bezpečnostní komise

Při této pozici se člen aktivně se zapojuje do řešení bezpečnostních incidentů a nežádoucích událostí. Přezkoumává efektivnost každého přijatého opatření k odstranění příčin bezpečnostního incidentu nebo nežádoucí události s vlivem na bezpečnost informací. Má za úkol zpracovat plán pro minimalizaci rizik v oblasti bezpečnosti informací a dohlíží na pravidelná školení v oblasti bezpečnosti informací IT týmu. Uchovává a kontroluje dokumentované záznamy kontrol bezpečnosti informací a vyhodnocuje případnou nutnost aktualizace. Podílí se na strategii společnosti v oblasti bezpečnosti informací.

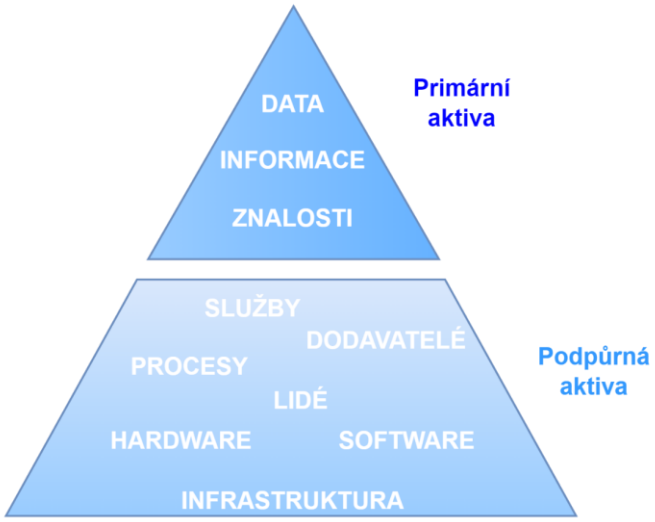
5.3.3 ISMS Specialista

Osoba na této pozici je odpovědná za funkčnost systému managementu bezpečnosti informací dle norem řady ISO/IEC 27000 a za komunikaci ISMS požadavků u nových či aktualizovaných verzí smluv vedoucích k nákupu produktů nebo služeb, které mají možný vliv na bezpečnost informací. Úzce spolupracuje se zástupcem vedení na implementaci požadavků ISMS do procesů společnosti, či se také podílí se na přípravě školicích materiálů ISMS a koordinuje školení v této oblasti. Provádí hodnocení rizik informační bezpečnosti. Aktivně se zapojuje do řešení bezpečnostních incidentů a nežádoucích událostí, a také přezkoumává efektivnost každého přijatého opatření k odstranění příčin bezpečnostního incidentu nebo nežádoucí události s vlivem na bezpečnost informací. Dohlíží na pravidelná školení v oblasti bezpečnosti informací IT týmu a zpracovává plán pro minimalizaci rizik pro tuto oblast. Stejně jako člen Bezpečnostní komise má za úkol uchovávat a kontrolovat dokumentované záznamy i se podílí na strategii společnosti v této oblasti.

5.4 Aktiva

Informační aktiva lze rozdělit do dvou hlavních kategorií, které znázorňuje Obrázek 16. Jedná se o aktiva primární a aktiva podpůrná. Primární aktiva, jako jsou data, informace a znalosti, jsou klíčovými prvky pro fungování organizace a rozhodovací procesy. Tyto aktiva jsou uchovávána, zpracovávána nebo poskytována prostřednictvím firemního systému, ve formě papírových dokumentů, nebo v myslích zaměstnanců. Dojde-li k ohrožení těchto aktiv, organizace může čelit potenciálnímu výpadku či narušení běžného provozu. Příklady primárních aktiv zahrnují obchodní data, informace o zakázkách či údaje o zákaznících, osobní údaje zaměstnanců, odborné znalosti, přihlašovací údaje, data o produktech nebo technologiích. (Aptien, 2024)

Podpůrná aktiva, též označována jako sekundární, zahrnují širokou škálu prvků, jako je hardware, software, lidé, IT služby, dodavatelé a infrastruktura, která zahrnuje i budovy a zařízení. Podpůrná aktiva jsou klíčová pro zajištění dostupnosti a správného fungování primárních aktiv. Pokud by došlo k selhání některých z těchto podpůrných aktiv, mohlo by to mít za následek narušení běžného chodu organizace. Tyto aktiva také přispívají k zabezpečení informačního systému. (Aptien, 2023)



Obrázek 16 - Členění aktiv. Zdroj: Aptien, 2023

5.4.1 Hardware

Hardware zahrnuje veškeré fyzické komponenty počítače. Tyto komponenty jsou nezbytné pro jeho funkci. Neodborně bývá hardware označován jako všechny části, na které si lze fyzicky sáhnout. Patří sem grafická karta, operační paměť RAM, pevný disk či základní deska. Kromě toho sem spadají i periferní zařízení, jako jsou klávesnice, reproduktory nebo USB flash disky. (IT Slovník, 2024)

Hardwarem společnosti jsou nejen počítače, ale také telefony, tablety nebo osobní digitální asistenti, dále jen „PDA“. Tabulka 1 představuje označení, pomocí kterého společnost identifikuje svá hardwarová aktiva.

Tabulka 1 - Klasifikace hardwaru. Zdroj: Interní dokumentace

Kód skupiny	Název skupiny
H1	Kritické zařízení
H2	Obecné zařízení
H3	Testovací zařízení
H4	Kritické síťové zařízení
H5	Obecné síťové zařízení
H6	Infrastruktura
H7	Osobní počítače a periferní zařízení

Tabulka 2 zmiňuje již konkrétní aktiva společnosti, která budou detailněji zkoumána v následující části práce.

Tabulka 2 - Seznam konkrétního hardwaru společnosti. Zdroj: Vlastní zpracování

Kód skupiny	Název informačního aktiva
H7	Desktopové počítače pro THP
H7	Desktopové počítače pro dělnické pozice
H7	Počítačový kiosk
H7	Chytré telefony
H7	Tablety
H7	PDA
H7	Pronajaté tiskárny
H7	Spektrometr
H6	Bezpečnostní kamery
H6	Terminály docházky
H6	Terminál pro řízení přístupu dveří
H6	Dieselový generátor
H6	Požární hasicí přístroj pro místnost serverů
H6	Klimatizace
H2	Záložní server
H2	Server SharePointu
H2	Server kamer

Kód skupiny	Název informačního aktiva
H2	Úložiště kamer
H5	Spínač

5.4.2 Software

Software představuje programové vybavení počítače zahrnující celou řadu programů a aplikací. Rozdělujeme jej do dvou hlavních kategorií, a to na software aplikační a systémový. Aplikační software je určen pro konkrétní aplikace, které uživatelé přímo používají. Systémový software slouží k řízení a správě počítače. (IT Slovník, 2024)

Software společnosti zahrnuje antivirové programy, virtuální privátní síť, dále jen „VPN“, Gmail či například Google Drive. V Tabulce 3 jsou zobrazeny kódy skupin sloužící k rozlišení jednotlivých softwarových aktiv společnosti.

Tabulka 3 - Klasifikace softwaru. Zdroj: Interní dokumentace

Kód skupiny	Název skupiny
S1	Kritický software
S2	Obecný software
S3	Softwarový nástroj pro testovací zařízení
S4	Osobní software

Tabulka 4 specifikuje aktiva společnosti, na něž se bude zaměřovat následující část bakalářské práce.

Tabulka 4 - Seznam konkrétního softwaru společnosti. Zdroj: Vlastní zpracování

Kód skupiny	Název informačního aktiva
S2	Systém pro mzdy
S2	Systém pro správu letenek
S2	Systém pro evidenci majetku
S2	Microsoft 365
S2	Microsoft Office
S2	Systém docházky

Kód skupiny	Název informačního aktiva
S4	Google Drive
S1	Antivirový software
S4	Software pro tvorbu grafů
S2	Záložní server
S2	Ovladač kamer
S2	Produkční servery (jídelna, dokumenty zaměstnaneckých smluv)
S2	Tiskový server pro tiskárny v kanceláři

5.4.3 Data

Data jsou informace, které jsou zpracovávány nebo uchovávány v počítači. (IT Slovník, 2024)

Následující Tabulka 5 obsahuje kódy, které slouží ke klasifikaci dat společnosti.

Tabulka 5 - Klasifikace dat. Zdroj: Interní dokumentace

Kód skupiny	Název skupiny
D1	Důvěrná data
D2	Interní data
D3	Veřejná data

Konkrétními daty společnosti se zabývá následující Tabulka 6.

Tabulka 6 - Seznam konkrétních dat společnosti. Zdroj: Vlastní zpracování

Kód skupiny	Název informačního aktiva
D2	Oracle databáze pro skladové hospodářství
D2	Oracle databáze pro dodavatelskou kvalitu
D2	Oracle databáze pro ESD
D2	Oracle databáze pro interní systém
D1	Veškeré záznamy z kamerových systémů

5.4.4 Papírové dokumenty

Papírovými dokumenty jsou ve firmě konkrétní smlouvy, licence či důležitá dokumentace. Následující Tabulka 7 představuje způsob, jakým společnost rozlišuje jednotlivá aktiva.

Tabulka 7 - Klasifikace papírových dokumentů. Zdroj: Interní dokumentace

Kód skupiny	Název skupiny
F1	Důvěrný papírový dokument
F2	Interní papírový dokument
F3	Veřejný papírový dokument

Tabulka 8 prezentuje specifické dokumenty, se kterými společnost nakládá.

Tabulka 8 - Seznam konkrétních dokumentů společnosti. Zdroj: Vlastní zpracování

Kód skupiny	Název informačního aktiva
F2	Dokumenty o certifikacích
F2	Legislativa v oblasti ochrany zdraví a bezpečnosti
F3	Přijaté faktury
F2	Platné smlouvy s odběrateli
F3	Zprávy z auditu
F3	Zakládací dokumenty
F1	Mzdové údaje
F1	Osobní složky zaměstnanců v aktivním a ukončeném stavu
F1	Přesčasy
F2	Dokumentace projektu
F2	Smlouvy se dodavateli
F1	Zaměstnávání cizinců
F3	Faktury
F2	Licence

5.4.5 Lidé

V této kategorii dochází ke členění do tří sektorů:

- P1: management společnosti včetně jejich zástupců,
- P2: kritičtí dodavatelé služeb, jimiž jsou elektřina, teplo, voda, software dodavatelé a externí společnosti nastavující infrastrukturu,
- P3: kontakty na zákazníky.

Z bezpečnostních důvodů nelze specifikovat informace podrobně.

5.4.6 Objekty

Objekty spadají do podpůrných aktiv firmy. Ve společnosti se nacházejí objekty, jimiž jsou spisovny, serverovny, kanceláře a sklady.

5.5 Vymezení aktiv pro posouzení rizik

V následující Tabulce 9 jsou vyobrazena aktiva, se kterými bude pracováno v následující kapitole z hlediska možných rizik. Tabulka obsahuje identifikační číslo aktiva, které poslouží k přehledné orientaci v následující části. Každé aktivum je přiřazeno konkrétnímu oddělení společnosti.

Tabulka 9 - Definování aktiv. Zdroj: Vlastní zpracování

ID číslo	Oddělení	Konkrétní aktivum
1.	Personální	Docházková karta zaměstnanců
2.	Personální	Šanon s osobními údaji zahraničních zaměstnanců
3.	Personální	Osobní složky zaměstnanců v aktivním a ukončeném stavu
4.	Personální	Klíč od kanceláře personálního oddělení
5.	Finanční	Smlouvy s externími dodavateli
6.	ESG	Zaměstnanci
7.	ESG	Politika a požadavky bezpečnosti informací
8.	ESG	Interní dokumentace společnosti
9.	ESG	Externí dokumentace společnosti
10.	Oddělení výroby	Infrastruktura
11.	Kvalita	Šanon s originálním postupem pro klíčového zákazníka
12.	IT	Notebook a stolní počítač

ID číslo	Oddělení	Konkrétní aktivum
13.	IT	Notebook a stolní počítač
14.	IT	Notebook a stolní počítač
15.	IT	Přenosná úložná zařízení
16.	IT	Server a síť
17.	IT	Server a síť
18.	IT	Softwarové vybavení
19.	IT	Uživatelský účet
20.	Správa budovy	Vniknutí na cizí pozemek
21.	Správa budovy	Vniknutí na cizí pozemek
22.	Správa budovy	Žebříky na střeše společnosti
23.	Správa budovy	Ztráta dat z kamerových systémů
24.	Správa budovy	Fyzická bezpečnost
25.	Správa budovy	Rozbití okna v přízemí
26.	Správa budovy	Klíč od kanceláře personálního oddělení
27.	Správa budovy	Zloděj

6 POSOUZENÍ RIZIK

Hodnocení rizik je proces identifikace nebezpečí, jež by mohlo negativně ovlivnit schopnost organizace vykonávat činnost. Tato hodnocení pomáhají identifikovat vrozená rizika a vyvolat opatření, procesy a kontroly ke snížení dopadu těchto rizik na provoz organizace. (Gillis, 2023)

Tato kapitola se bude zabývat celkovým zhodnocením rizik. Pro daná aktiva se zaměří na možné vyskytující se situace, na které navážou teoretické události, jež by mohly následovat. Na základě těchto podkladů budou vytvořeny pravděpodobné scénáře následků. Další část této kapitoly se bude zabývat hodnocením rizik, které nám pomocí tabulky zobrazí nejrizikovější aktiva s jejich potenciálními následky. Poslední část bude prezentovat opatření pro dané situace s cílem minimalizovat jejich dopad či jim úplně předcházet.

6.1 Metodika pro hodnocení aktiv

*Hodnota rizik = Hodnota aktiva (hodnota důvěrnosti + hodnota integrity + hodnota dostupnosti) * Pravděpodobnost výskytu*

Pokud je hodnota rizika větší nebo rovna 21, je nutné provést ošetření rizika, neboť se jedná o riziko kritické. Kritická rizika by mohla ohrozit samotnou existenci společnosti. (Interní dokumentace pro hodnocení rizik společnosti)

Pravidla pro určení každé hodnoty jsou uvedeny v Tabulkách 10-13 níže.

Tabulka 10 - Hodnocení důvěrnosti. Zdroj: Interní dokumentace

Důvěrnost (C): Úroveň důvěrnosti aktiv

Hodnota	Popis
3	Informační aktiva, která nesou, zpracovávají nebo mají přístup k důvěrným informacím a vyžadují vysokou úroveň ochrany.
2	Informační aktiva, která nesou, zpracovávají nebo mají přístup k citlivým informacím a vyžadují střední úroveň ochrany.
1	Informační aktiva, která nesou, zpracovávají nebo mají přístup k veřejným informacím s nízkou citlivostí a vyžadují nejnižší úroveň ochrany.

Tabulka 11 - Hodnocení integrity. Zdroj: Interní dokumentace

Integrita (I): Úroveň požadavků na integritu aktiv.

Hodnota	Popis
3	Pokud je obsah aktiv neúplný, má to významný dopad na podnikání nebo může vést k vážnému narušení podnikání.
2	Pokud je obsah aktiva neúplný, snižuje provozní efektivitu nebo způsobuje nepříjemnosti při práci, ale nevede k narušení podnikání.
1	Pokud je obsah aktiv neúplný, má minimální nebo žádný dopad na provoz.

Tabulka 12 - Hodnocení dostupnosti. Zdroj: Interní dokumentace

Dostupnost (A): Přípustná doba výpadku aktiva.

Hodnota	Popis
3	1. Pokud není aktivum přístupné po celou dobu, vede to k přerušení provozu. 2. Pokud aktivum nemůže poskytovat nepřetržité služby, je přijatelná doba obnovy co nejkratší.
2	1. Pokud aktivum není přístupné po celou dobu, snižuje to provozní efektivitu, ale nevede to k narušení provozu. 2. Pokud aktivum nemůže poskytovat nepřetržité služby, je přijatelná doba obnovy střední.
1	1. Pokud aktivum není po celou dobu dostupné, má to minimální nebo žádný vliv na provozní efektivitu. 2. Pokud aktivum nemůže poskytovat nepřetržité služby, je přijatelná doba obnovy nejdelší.

Tabulka 13 - Hodnocení výskytu. Zdroj: Interní dokumentace

Pravděpodobnost výskytu

Hodnota	Kvalitativní popis	Kvantitativní popis
3	Vyskytuje se často.	Vyskytuje se alespoň jednou měsíčně.
2	Vyskytuje se v určitých případech.	Vyskytuje se alespoň jednou za sezónu.
1	Obvykle se nevyskytuje.	Vyskytuje se méně než jednou ročně.

6.2 Eventuální situace

Tabulka níže se zabývá rizikovými událostmi, které by mohly nastat v souvislosti s danými aktivy.

Tabulka 14 - Eventuální situace. Zdroj: Vlastní zpracování

ID číslo	Situace
1.	Ztráta docházkové karty.
2.	Krádež a zneužití dokumentace.
3.	Zneužití dokumentů o zaměstnancích (Nafocení dokumentů).
4.	Ztráta klíče od kanceláře personálního oddělení.
5.	Smlouvy nepokrývají ochranu osobních dat a know-how.
6.	Zaměstnanci nemají povědomí o nastavených pravidlech pro ISMS.
7.	Nejsou nastavena pravidla pro bezpečnost informací u externích firem.
8.	Dokumenty nejsou uloženy na zabezpečeném úložišti.
9.	Dokumenty nejsou chráněné proti změnám, tisku či mazání.
10.	Sesterská společnost má přístup do budovy.
11.	Někdo může zneužít citlivá data.
12.	Vkládání nefiremních periferních zařízení USB do firemních zařízení.
13.	Šíření virusu po síti.
14.	Zaměstnanec odchází nebo je přeložen.
15.	Uživatelé používají ke kopírování dat externí pevný disk.

ID číslo	Situace
16.	Používání nezabezpečené sítě.
17.	Výpadek proudu.
18.	Zaměstnanci používají na počítačích společnosti neautorizovaný software.
19.	Sdělení přihlašovacích údajů k vybavení a systémům jiné osobě.
20.	Nestřežená okna v zasedacích místnostech.
21.	Průchod dvou osob turniketem na jednu ID kartu.
22.	Kdokoli může poškodit zámek.
23.	Může dojít ke smazání dat z kamerových systémů.
24.	Neprobíhá žádná pravidelná kontrola zabezpečení budovy.
25.	Vniknutí do budovy.
26.	Ztráta klíče od kanceláře.
27.	Vniknutí do budovy.

6.3 Potenciální událost

V tabulce 15 jsou uvedeny možné události spojené s příslušnými aktivy.

Tabulka 15 - Potenciální událost. Zdroj: Vlastní zpracování

ID číslo	Událost
1.	Cizí osoba se může dostat do budovy.
2.	Dokumenty mohou být ztraceny či zneužity.
3.	Dokumenty mohou být odcizeny nebo zneužity.
4.	Zcizení citlivých informací o zaměstnancích společnosti.
5.	Osobní data a ochrana know-how mohou být zneužita.
6.	Neodpovědné chování zaměstnanců může vést ke ztrátě citlivých dat.
7.	Možnost útoku na kybernetickou bezpečnost, vstup cizí osoby.
8.	Osoba může zkopírovat výrobní dokumentaci a předat ji někomu zvenčí.
9.	Ztráta či zneužití dokumentace zákazníka.
10.	Zaměstnanci sesterské společnosti mohou ukrást citlivá data společnosti.
11.	Uložením dokumentu na nezabezpečením místě může dojít k odcizení.
12.	Zaměstnanec má oprávnění využívat USB porty pro externí disky.

ID číslo	Událost
13.	V počítači není nainstalován antivirový software.
14.	Počítač není vrácen společnosti.
15.	Použití externího disku pro přístup k počítačům bez jeho skenování.
16.	Používání nezabezpečeného veřejného Wifi připojení mimo společnost.
17.	UPS v serverovně nefunguje správně.
18.	Žaloby ze strany prodejců.
19.	Heslo bylo odhaleno.
20.	Otevřenými okny v zasedací místnosti může kdokoliv vstoupit do budovy.
21.	Dvě osoby mohou vstoupit těsně za sebou.
22.	Kdokoli se může dostat na střechu.
23.	Chybí záznam o nehodách.
24.	Některý z vchodů do budovy zůstává nezajištěný.
25.	Majetek může být odcizen.
26.	Možnost vstupu cizí osoby do kanceláře.
27.	Neoprávněný vstup cizí osoby do kanceláře.

6.4 Možné následky

Následující tabulka představuje eventuální následky událostí, které byly zmíněny v tabulce 16.

Tabulka 16 - Možné následky. Zdroj: Vlastní zpracování

ID číslo	Následky
1.	Ztráta citlivých dat, například nafocení prostor haly.
2.	Zneužití citlivých údajů o zaměstnancích.
3.	Zneužití citlivých údajů o zaměstnancích.
4.	Osoba může vstoupit do kanceláře, kde nikdo není.
5.	Ztráta osobních dat, know-how, ztráta celkového byznysu.
6.	Ztráta know-how.
7.	Ztráta citlivých dat, know-how, ztráta podnikání.
8.	Osoba může zkopírovat data a předat je někomu zvenčí.

ID číslo	Následky
9.	Ztráta důvěry zákazníka, ztráta byznysu.
10.	Únik informací.
11.	Osoba může vstoupit do kanceláře, kde nikdo není.
12.	Počítač je napaden virem.
13.	Počítač je infikovaný.
14.	Majetek je ztracen.
15.	Počítače jsou infikované.
16.	Firemní data mohou být zneužita, komunikace může být monitorována.
17.	Náhlé výpadky proudu s dopadem na služby.
18.	Vysokou sankcí může být ohroženo dobré jméno společnosti.
19.	Účet může být zneužit.
20.	Ztráta majetku.
21.	Ztráta majetku.
22.	Škody na majetku.
23.	Ztráta důležitých dat.
24.	Ztráta majetku.
25.	Ztráta majetku a citlivých údajů.
26.	Ztráta citlivých údajů.
27.	Ztráta citlivých údajů.

6.5 Hodnocení rizik

V Tabulce 17 jsou uvedeny konkrétní výsledky analýzy rizik pro jednotlivá aktiva společnosti.

Tabulka 17 - Hodnocení rizik. Zdroj: Vlastní zpracování

ID číslo	Pravděpodobnost výskytu	Hodnota aktiva			Hodnota rizika	Má být zařazen do plánu řešení rizik?
		C	I	A		
1.	2	2	2	1	10	Ne
2.	1	3	2	2	7	Ne
3.	1	3	2	2	7	Ne

ID číslo	Pravděpodobnost výskytu	Hodnota aktiva			Hodnota rizika	Má být zařazen do plánu řešení rizik?
		C	I	A		
4.	1	3	2	2	7	Ne
5.	3	3	3	3	27	Ano
6.	3	3	2	2	21	Ano
7.	3	3	3	3	27	Ano
8.	3	3	3	3	27	Ano
9.	3	3	3	3	27	Ano
10.	3	3	3	3	27	Ano
11.	1	3	2	1	6	Ne
12.	2	2	2	1	10	Ne
13.	2	2	3	2	14	Ne
14.	1	3	1	2	6	Ne
15.	2	2	3	2	14	Ne
16.	1	1	1	1	3	Ne
17.	1	3	3	3	9	Ne
18.	2	2	2	3	14	Ne
19.	3	2	2	2	18	Ne
20.	3	3	2	2	21	Ano
21.	3	2	1	1	12	Ne
22.	2	1	1	1	6	Ne
23.	2	2	1	1	8	Ne
24.	2	2	1	1	8	Ne
25.	3	3	2	2	21	Ano
26.	3	3	2	2	21	Ano
27.	2	2	2	2	12	Ne

6.6 Opatření rizik

Tabulka 18 popisuje jednotlivá opatření pro aktiva, u kterých vyšly hodnoty v kritické rovině.

Tabulka 18 - Opatření kritických rizik. Zdroj: Vlastní zpracování

ID číslo	Opatření
5.	Je nutné provést revizi všech platných smluv s externími partnery a aktualizovat všechny smlouvy přidáním nových požadavků normy ISO 27001.
6.	Je třeba vytvořit víceúrovňové školení pro zaměstnance společnosti, pro operátorskou úroveň, střední, management a top management. Je třeba v tomto školení seznámit s pravidly, které se musí dodržovat v rámci BI a testem ověřit získané znalosti.
7.	Je třeba vytvořit seznam společností, které mají volný přístup do budovy (kantýna, úklidová společnost, Security společnost). Je třeba zakotvit požadavky na BI do smluv s dodavateli služeb a připravit školení, které bude popisovat pravidla pro BI a proškolit na ně všechny servisní společnosti.
8.	Je třeba vyvinout nový DMS, který bude řešit uchovávání, aktualizace, revize a práva k dokumentaci a připravit školení na nové verze dokumentů.
9.	Součástí DMS bude i řízení externí dokumentace včetně nastavení práv v rámci jednotlivých projektů.
10.	Je třeba provést revize smluv.
20.	Opatřením by mohla být instalace bezpečnostní fólie na okna + instalace omezovače otevírání.
25.	Instalace bezpečnostní fólie na okna, instalace omezovače otevírání.
26.	Změna způsobu zámku na kancelářských dveřích – digitální kontrolní systém (otisk prstu, identifikační karta apod.).

7 ROZDÍLOVÁ ANALÝZA

GAP analýza bývá zpracovávána jako první krok při zavádění normy pro systém řízení bezpečnosti informací ISO/IEC 27001:2022. Na základě výsledků organizace dostane přehled o zranitelných místech a chybějících požadavcích, které norma vyžaduje. Rozdílová analýza spočívá v rozboru celé normy. Z důvodu rozsáhlosti budou v této kapitole rozebrány pouze klíčové části normy.

Tabulka 19 graficky znázorňuje, zda společnost plní či neplní požadavky normy. Pokud společnost požadavky neplní, je uvedeno, kde jsou mezery.

V prvním sloupci tabulky jsou číselně označeny jednotlivé otázky analýzy. Druhý sloupec obsahuje konkrétní čísla článků normy, na něž se otázky vztahují. Následuje požadavek normy, který definuje oblast daného článku a teoreticky jej popisuje. Tento sloupec slouží jako výchozí bod pro následné určení hodnocení plnění. Pokud nelze odpovědět na všechny otázky z požadavku normy ANO, vzniká GAP neboli mezera. V takovém případě není požadavek splněn, a to buď zcela nebo jen částečně. Poslední sloupec formuluje odůvodnění, které již konkrétně popisuje důvody nedostatečného plnění požadavku normy.

Tabulka 19 - GAP Analýza. Zdroj: Vlastní zpracování dle čerpání informací z ÚNMZ, 2023

Číslo otázky	Článek normy	Požadavek normy	Hodnocení plnění	Odůvodnění
1	4	Kontext organizace		
	4.4	Systém managementu informační bezpečnosti		
		Je systém managementu informační bezpečnosti ustanoven, zaveden, udržován a neustále zlepšován v souladu s požadavky této mezinárodní normy?	NE	V současné době není systém ve společnosti v plném rozsahu ustanovený, implementovaný, udržovaný a není předmětem neustálého zlepšování.
2	5	Vůdčí role		
	5.2	Politika		
		Je politika přiměřená účelům organizace? Zahrnuje cíle BI nebo poskytuje rámec pro nastavení cílů BI? Je dostupná jako dokumentovaná informace? Je komunikována v rámci organizace? Je přiměřeně dostupná zainteresovaným stranám?	NE	Neboť není politika BI zpracována, nezahrnuje povinné cíle ani závazky na BI. Politika ISMS není dostupná jako dokumentovaná informace, není komunikována či dostupná zainteresovaným stranám.

Číslo otázky	Článek normy	Požadavek normy	Hodnocení plnění	Odůvodnění
3	6	Plánování		
		Cíle informační bezpečnosti a plánování jejich dosažení		
	6.2	Jsou cíle BI měřitelné? Jsou komunikovány a monitorovány? Jsou dostupné jako dokumentované informace? Určila organizace, co bude vykonáváno, jaké zdroje budou vyžadovány, kdo bude odpovědný či termín dokončení?	NE	Cíle ISMS nejsou vytvořeny ani komunikovány, tudíž nejsou splněny ani další kritéria na řízení a plánování plnění cílů bezpečnosti informací.
4	7	Podpora		
		Komunikace		
	7.4	Má organizace ve vztahu k BI zavedený systém pro interní a externí komunikaci, který zahrnuje: Co má být komunikováno? Kdy má být komunikováno? S kým má být komunikováno? Jak má být komunikováno?	ANO	Organizace má vytvořený a zavedený proces pro interní a externí komunikaci i s ohledem na ISMS.

Číslo otázky	Článek normy	Požadavek normy	Hodnocení plnění	Odůvodnění
	7	Podpora		
		Dokumentované informace		
5	7.5	Určila organizace, které dokumentované informace jsou nezbytné pro efektivnost ISMS? Zajišťuje při vytváření a aktualizaci dokumentovaných informací: - identifikaci a popis, - formát, - přezkoumání, - schválení vhodnosti a přiměřenosti? Jsou dostupné a vhodné pro použití? Jsou odpovídajícím způsobem chráněny? Jsou dokumentované informace externího původu odpovídajícím způsobem označeny a řízeny?	NE	Organizace určila dokumentované informace nezbytné pro efektivnost ISMS, Dokumenty jsou řízeny i označeny. Umístění na SharePoint pro zajištění čitelnosti, řízení změn, uchováváním a vypořádáním. Dokumenty jsou uložené na SharePoint systému ve formě, kdy je možné dokumenty stáhnout do PC zaměstnanců, není efektivně řízena aktualizace dokumentace, pravidelné revize, neprobíhá seznamovaní zaměstnanců s dokumentací, není možné archivovat dokumenty na stejném místě.

Číslo otázky	Článek normy	Požadavek normy	Hodnocení plnění	Odůvodnění
	8	Provozování		
		Posuzování rizik informační bezpečnosti		
6	8.2	Posuzuje organizace rizika BI v pravidelných intervalech? Uchovává organizace dokumentované informace o výsledcích ošetření rizik BI?	NE	Rizika bezpečnost informací jsou posuzována v rámci prověrek IT a interních auditů procesů. Do posuzování nejsou však zahrnuta všechna rizika ve vztahu k normě ISO 27001:2022. Nejsou uchovávány dokumentované informace o výsledcích rizik bezpečnosti informací.
	9	Hodnocení výkonnosti		
		Monitorování, měření, analýza a hodnocení		
7	9.1	Provádí organizace monitorování, měření, analýzu a hodnocení? Uchovává odpovídající dokumentované informace jako důkazy o výsledcích monitorování a měření?	NE	Není nastaveno, co je potřeba monitorovat a měřit dle ISO 27001:2022. Nejsou nastavena kritéria měření a monitoringu, periodicita monitoringu a měření, ani termíny pro předávání výsledků. Dokumentované informace o výkonnosti ISMS nejsou uchovávány.

Číslo otázky	Článek normy	Požadavek normy	Hodnocení plnění	Odůvodnění
8	10	Zlepšování		
	10.1	Neustálé zlepšování		
		Zlepšuje organizace neustále vhodnost, přiměřenost a efektivnost systému managementu ISMS?	NE	Systém není kompletně implementován, tudíž není zajištěna celkově vhodnost, přiměřenost a efektivnost systému managementu.

8 PROHLÁŠENÍ O APLIKOVATELNOSTI

Prohlášení o aplikovatelnosti (dále jen „POA“) je nutné zpracovat pro certifikační orgán při žádosti o certifikaci ISO 27001. POA detailně rozebírá každou část přílohy A v normě ISO 27001:2022. Vzhledem k rozsahu normy není možné zmínit každý jeden bod. Proto následující Tabulka 20 představuje výběr pouze nejpodstatnějších bodů přílohy, které nejvíce odpovídají tématu bakalářské práce.

První sloupec tabulky značí konkrétní článek Přílohy A normy ISO 27001. Ve druhém sloupci je uveden název daného článku přílohy. Následuje sloupec, jenž obsahuje znění konkrétních opatření stanovených v normě, dle kterých je posuzováno, zda jsou jednotlivá opatření společností aplikována či nikoli. Poslední sloupec tabulky obsahuje odůvodnění, které již konkrétně vysvětluje důvody, proč bylo rozhodnuto o aplikování či neaplikování daného opatření. Pro získání certifikace ISO 27001 by muselo být každé opatření splněno.

Tabulka 20 - Prohlášení o aplikovatelnosti. Zdroj: Vlastní zpracování dle čerpání informací z ÚNMZ, 2023

Příloha A ISO 27001	**Název**	**Opatření**	**Aplikováno**	**Odůvodnění**
5 Organizační opatření				
5.1	Politiky pro informační bezpečnost	Politika musí být definována, schválena vedením organizace, zveřejněna, sdělena a vzata na vědomí příslušnými pracovníky a zainteresovanými stranami a přezkoumávány v plánovaných intervalech a v případě významných změn.	NE	Politiky ISMS nejsou plně definovány. Úroveň naplnění je procentuálně přibližně 70 %. Jakmile bude systém implementován, veškeré politiky budou doplněny.
5.3	Oddělení povinností	Protichůdné povinnosti a oblasti odpovědnosti musí být odděleny.	ČÁSTEČNĚ	Principy oddělení povinností jsou implementovány. Zaměstnanci mají přístup k aktivům pouze na základě svých oprávnění. Neprobíhají žádné audity k této oblasti.
5.11	Vrácení aktiv	Pracovníci a případně další zainteresované strany musí po změně nebo ukončení pracovního poměru, smlouvy nebo dohody vrátit veškerá aktiva organizace, která mají k dispozici.	ČÁSTEČNĚ	Není kompletně evidován přehled vydaných aktiv do oběhu. Chybí přehledná identifikace vrácených aktiv.

Příloha A ISO 27001	Název	Opatření	Aplikováno	Odůvodnění
5.12	Klasifikace informací	Informace musí být klasifikovány podle potřeb organizace v oblasti BI na základě CIA a požadavků příslušných zainteresovaných stran.	NE	Není uvedeno rozdělení dokumentů na interní, veřejné a citlivé.
5.13	Označování informací	Musí být vypracován vhodný soubor postupů pro označování informací a zaveden v souladu se systémem klasifikace informací přijatým organizací.	NE	Není prováděno.
5.14	Předávání informací	Pravidla, postupy nebo dohody pro předávání informací v organizaci a mezi dalšími stranami musí být zavedeny pro všechny typy přenosových zařízení.	NE	Politiky, postupy a opatření nejsou zpracovány.
5.30	Příprava ICT na zajištění kontinuity činnosti.	Připravenost ICT musí být plánována, zavedena, udržována a testována na základě cílů kontinuity činnosti organizace.	ČÁSTEČNĚ	Pro bezpečnost informací kontinuita není zpracována. Je zpracována pouze kontinuita výroby.
5.32	Práva na duševní vlastnictví	Organizace musí zavést vhodné postupy na ochranu práv duševního vlastnictví.	ANO	Společnost dodržuje legislativní požadavky.

Příloha A ISO 27001	Název	Opatření	Aplikováno	Odůvodnění
6 Opatření v oblasti lidských zdrojů				
6.1	Prověřování	Prověřování minulosti všech uchazečů musí být prováděno před nástupem do organizace.	ANO	Před nástupem musí každý uchazeč předložit výpis svého trestního rejstříku. Má-li uchazeč majetkovou trestnou činnost, nelze jej přijmout. Postupy jsou v souladu s legislativou.
6.5	Odpovědnosti po ukončení nebo změně pracovního poměru	Odpovědnosti a povinnosti v oblasti BI, které zůstávají v platnosti i po ukončení nebo změně pracovního poměru, musí být definovány.	ANO	Vše probíhá v souladu s nastavenými standardy. Zaměstnanci jsou školeni i proškolováni na pracovišti, a to buď fyzicky ve školicích místnostech, nebo lze absolvovat školení online formou přes své pracovní účty. Každý zaměstnanec má podepsanou mlčenlivosti, která má platnost i po ukončení pracovního poměru či změně pracovního vztahu.

Příloha A ISO 27001	Název	Opatření	Aplikováno	Odůvodnění
6.7	Práce na dálku	Pokud pracovníci pracují na dálku, musí být zavedena bezpečnostní opatření na ochranu informací.	ČÁSTEČNĚ	Kromě výroby má ve společnosti notebook většina zaměstnanců. U THP pracovníků je to 100% obsazení. Notebooky, které se vynáší z prostředí společnosti, jsou značeny nálepkou a probíhá u nich proces schvalování. Společnost má vedenou evidenci zařízení. Každé mobilní zařízení má možnost zálohování na OneDrive. Klasické zálohování se neprovádí. Politikou je nařízeno používání antivirových programů, které jsou pod heslem. Je vydána politika, jenž obsahuje zákaz jakékoli instalace. Jsou nastaveny automatické aktualizace. Probíhá pravidelná změna hesla pro zvýšení zabezpečení veškerých zařízení.

Příloha A ISO 27001	Název	Opatření	Aplikováno	Odůvodnění
6.8	Podávání zpráv o událostech BI	Organizace musí pracovníkům poskytnout mechanismus pro včasné podávání zpráv o podezřelých událostech BI.	ANO	Probíhá hlášení, konkrétně přes Helpdesk.
7 Opatření fyzické bezpečnosti				
7.3	Zabezpečení kanceláří, místností a vybavení	Musí být navržena a zavedena opatření pro fyzickou bezpečnost kanceláří, místností a vybavení.	ČÁSTEČNĚ	Za klíče zodpovídá personální oddělení – vlastní je a v případě potřeby je vydává. Při ztrátě docházkové karty je karta blokována. Klíče nejsou řádně evidovány, a nikdo není informován o tom, kdo má vydáno, zejména klíče od kanceláří.
7.4	Monitorování fyzické bezpečnosti	Prostory musí být nepřetržitě monitorovány pro neoprávněný fyzický přístup.	ANO	Místa jsou velmi dobře zabezpečená. Po celém prostoru se nacházejí kamery. Přístup není povolen cizím osobám. Na každém vstupu se nachází Security služba.

Příloha A ISO 27001	Název	Opatření	Aplikováno	Odůvodnění
8 Technologická opatření				
8.24	Používání kryptografie	Musí být definována a zavedena pravidla pro efektivní používání kryptografie.	ANO	Je šifrována veškerá záloha dat.
8.3	Omezení přístupu k informacím	Přístup k informacím musí být omezen v souladu s politikou řízení přístupu.	ČÁSTEČNĚ	Přístup k informacím mají uživatelé omezen, a to pouze pro účely sloužící k výkonu jejich práce.

9 NÁVRHY OPATŘENÍ

Mezi organizační i technická opatření patří zavedení nového systému DMS (Document Management System). Zavedení je třeba z důvodu zajištění kompletní bezpečnosti informací u veškeré dokumentace společnosti. V rámci organizačního opatření bude nutné vytvořit postupy a pravidla pro práci s dokumentací. V systému se také nastaví povolené přístupy k jednotlivým informacím podle potřeb dané pracovní pozice. Technické opatření zahrnuje celkové nastavení systému, a to včetně zálohování dat či ochrany před neoprávněným přístupem. Tento systém bude zajišťovat přehlednější a bezpečnější řízení veškeré dokumentace. DMS umožní uchovávat a sdílet spravované dokumenty, díky čemuž bude zvýšena efektivita práce.

9.1 Zavedení systému

V rámci aktualizace schvalovacího procesu od Microsoftu došlo k omezení přehledu, kdo a jakým způsobem dokument schválil. Není možné na SharePoint systému vytvořit záložku pro archivaci dokumentů, neboť by se stále objevovaly v rámci filtrování všem uživatelům. To znamená, že se zobrazí veškeré verze, včetně těch neaktuálních, a hrozí u finálního uživatele, že může využít starší formát dokumentace. Neprobíhá zde ani pravidelná revize aktualizací dokumentace po 12 měsících. Vzhledem k množství dokumentů je manuální vyhledávání a zasílání dokumentů k revizi vlastníkům dokumentace neefektivní. Není také možné zajistit, aby zaměstnanci nestahovali dokumenty do svých počítačů.

Na základě těchto podstat je třeba vyvinout svůj vlastní DMS, který bude plně automatizován. Systém zajistí vzory nových dokumentů a umožní vytváření dokumentů uvnitř systému, a to bez možnosti stahovat dokumenty do vlastního počítače. Jakmile vlastník dokumentu požádá o vydání nové dokumentace či aktualizace nynější verze dokumentu, systémem přejde dokument na kontrolu DMS administrátorovi. Pokud dokument bude splňovat všechny náležitosti dokumentace a kontrola u Data Control Center (dále jen „DCC“) proběhne v pořádku, nastaví se schvalovací proces, kdy mohou odpovědné osoby dokument připomínkovat, či jej případně vrátit vlastníkovi k úpravě.

Úkolem DCC je také nastavení potřebných metadat k dokumentům, jako například:

- kdo je vlastníkem,
- kdo je vlastníkův nadřízený,
- do jaké složky se má dokument uložit,

- kdo má být s tímto dokumentem seznámen,
- zdali se dokument tiskne a pokud ano, tak kolik verzí.

O všem je vedena historie i je měřeno, jak dlouho je dokument ve schvalovacím procesu. Po finálním schválení generálním ředitelem dojde k uložení dokumentu na jeho přiřazené místo a automaticky se nastaví datum platnosti. Předchozí verze dokumentu se stáhne do archivu, vygeneruje se oficiální e-mail, který bude informovat zaměstnance o vydání a o proběhlých změnách v tomto dokumentu. Každý zaměstnanec bude mít povinnost se s tímto dokumentem seznámit. Systém bude kontrolovat, kolik zaměstnanců zbývá proškolit na novou verzi nebo dokument, a taktéž je bude pravidelně informovat, že tak ještě neučinili. Nastaví se lhůta 12 měsíců, po jejímž uplynutí automaticky dojde k informování vlastníka dokumentace, že je třeba provést revizi.

Vlastník dokumentu bude mít následující možnosti:

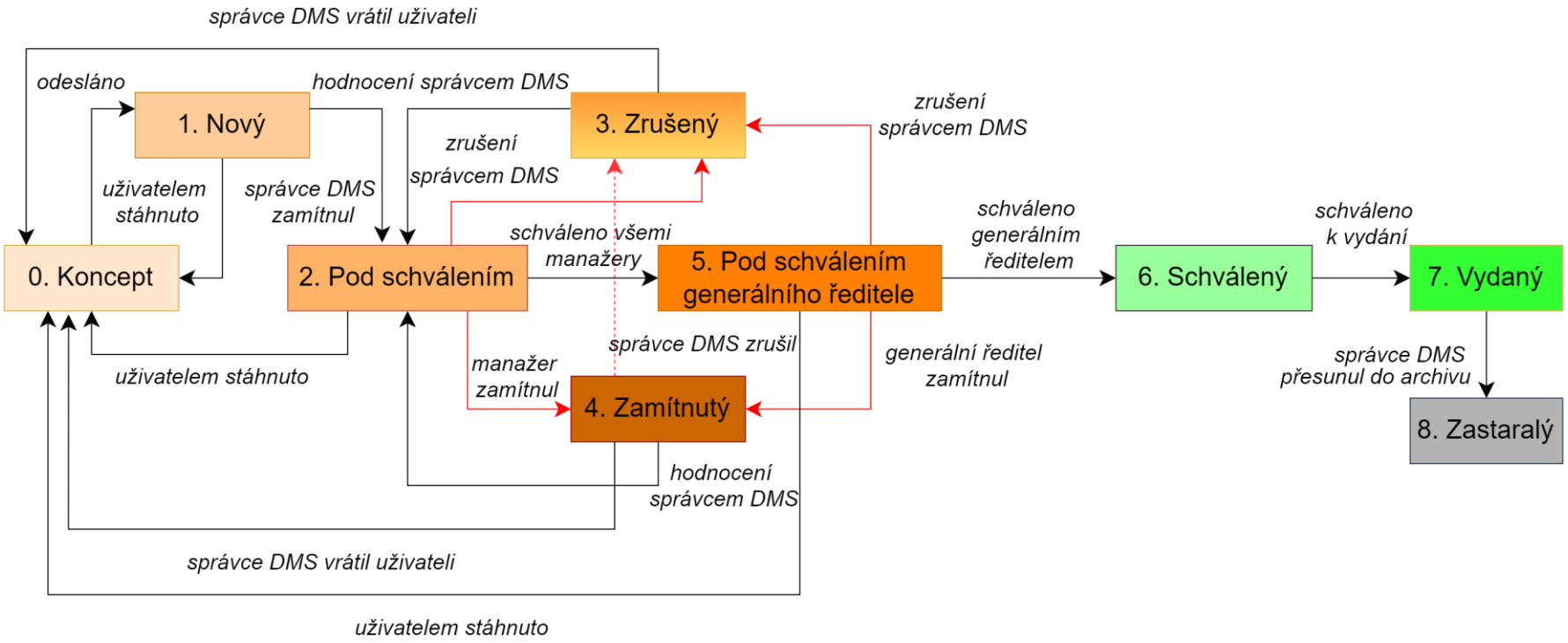
- Možnost zakliknout, že je dokument stále platný, díky čemuž se lhůta posune o dalších 12 měsíců.
- Možnost provést aktualizaci, přičemž se spustí běžný schvalovací proces.

V normě ISO/IEC 27001:2022 se jedná konkrétně o body 7.5.3 a) dostupnost a použití dokumentovaných informacích + 7.5.3 b) jejich ochrana. (ÚNMZ, 2023) To zajistí nastavení metadat pro každý dokument, kdy bude zřejmé, komu je dokument určen a kdo s ním musí být seznámen. V systému bude probíhat snadné filtrování napříč dokumenty. Na SharePointu bude vydána pouze PDF verze dokumentu, aby se zabránilo zneužití dat. Tuto verzi nebude možné nijak měnit či jiným způsobem upravit a přes každý dokument bude veden vodoznak.

Konkrétní ukázka a představení DMS systému je znázorněno v Příloze P I.

9.2 Flowchart vydání nového dokumentu

Následující Obrázek 17 graficky znázorňuje princip, jakým funguje vydání nového dokumentu v DMS.



Obrázek 17 - Flowchart DMS systému. Zdroj: Interní dokumentace

ZÁVĚR

Bakalářská práce se zabývala celkovým zhodnocením bezpečnosti informací společnosti. Cílem práce bylo posoudit míru plnění či neplnění požadavků na informační bezpečnost dle normy ISO/IEC 27001:2022. Za účelem dosažení uvedeného cíle byla provedena analýza interní dokumentace společnosti.

Pro provedení počáteční analýzy bylo třeba provést posouzení rizik. Toto posouzení si kladlo za cíl odhalit nejvíce ohrožená aktiva společnosti. Prvním krokem bylo třeba identifikovat aktiva, která budou předmětem dalšího zkoumání. Každé z těchto aktiv bylo označeno identifikačním číslem a přiřazeno k příslušnému oddělení společnosti. Poté byla stanovena metodika, dle které bude probíhat analýza rizik u jednotlivých aktiv. Tato metodika vychází z konceptu triády CIA, jež zohledňuje důvěrnost, integritu i dostupnost aktiv. V této fázi byly stanoveny možné situace, které by se mohly vztahovat k jednotlivým aktivům, a pro každou situaci byla definována potenciální událost a následné dopady. Na základě těchto výsledků byla pomocí stanovené metodiky ohodnocena míra ohrožení aktiv. V případě kritického ohrožení bylo třeba pro tato aktiva nastavit okamžité bezpečnostní opatření.

Při zavádění systému řízení bezpečnosti informací je třeba zjistit míru plnění požadavků normy. Pro tento krok byla zpracována rozdílová analýza, která odhaluje nedostatky informační bezpečnosti, fyzické bezpečnosti a GDPR. Na základě analýzy vzniká přehled o nedostatcích a zranitelných místech v souladu s požadavky normy, které budou společnosti předloženy. Společnost by následně měla tyto nedostatky co nejdříve odstranit, aby mohl být systém plně zaveden.

Norma ISO/IEC 27001:2022 obsahuje také přílohu A, dle které se řídí Prohlášení o aplikovatelnosti. Tato příloha obsahuje seznam bezpečnostních opatření, které jsou normou vyžadována. Aby mohla společnost získat certifikaci ISO 27001, musí naplňovat veškeré požadavky. Bylo nezbytné posoudit, do jaké míry společnost daný výběr opatření implementuje. Mnoho z těchto opatření společnost realizuje pouze částečně, což signalizuje, že i v této oblasti jsou nedostatky, jež by měly být do doby podání oficiální žádosti o certifikaci certifikačnímu orgánu odstraněny.

Cílem této práce bylo navrhnout opatření, které by zajišťovalo bezpečné řízení veškeré dokumentace společnosti. Pro tento cíl byl navrhnut interní vývoj nového automatizovaného systému řízení dokumentace DMS. Tento systém umožňuje tvorbu dokumentace, nastavení přístupů k jednotlivým dokumentům společnosti dle odpovídajících pracovních pozic,

zajišťuje kompletní schvalovací a vyhlašovací proces dokumentů, klasifikaci dokumentů, kontroly aktuálnosti dle stanovených termínů, zálohování dat a chrání dokumenty před jakýmkoli neoprávněným přístupem. Je možné zde dokumenty dle potřeby filtrovat. Každý krok manipulace s dokumentací je automaticky ukládán. Díky DMS je zajištěno přehledné, efektivní, systémové, ale především bezpečné řízení dokumentace společnosti.

SEZNAM POUŽITÉ LITERATURY

A-LIGN. *What's the Difference Between ISO 27001:2013 and ISO 27001:2022?* Online. A-LIGN. 2023. Dostupné z: https://www.a-lign.com/articles/blog-whats-the-difference-between-iso-27001-2013-and-iso-27001-2022. [cit. 2024-03-01].

APTIEN. *Co je aktivum*. Online. Aptien. 2023, 16.02.2024. Dostupné z: https://aptien.com/cs/kb/articles/what-is-asset. [cit. 2024-02-27].

APTIEN. *Co je CIA triáda informační bezpečnosti*. Online. Aptien. 2023, 15.12.2023. Dostupné z: https://aptien.com/cs/kb/articles/what-is-cia-triad. [cit. 2024-02-12].

APTIEN. *Co jsou podpůrná informační aktiva*. Online. Aptien. 2023, 21.09.2023. Dostupné z: https://aptien.com/cs/kb/articles/what-are-supporting-assets. [cit. 2024-03-24].

APTIEN. *Co jsou primární informační aktiva*. Online. Aptien. 2024, 30.01.2024. Dostupné z: https://aptien.com/cs/kb/articles/what-are-primary-information-assets. [cit. 2024-03-24].

AUGENBAUM, Scott E. *The Secret to Cybersecurity: A Simple Plan to Protect Your Family and Business from Cybercrime*. New York: Forefront Books, 2019. ISBN 978-1-948677-08-0.

BESTPRACTICE.BIZ. *PDCA: An Implementation Guide To ISO 27001:2013*. Online. Bestpractice.biz. 2020, 08.12.2020. Dostupné z: https://bestpractice.biz/pdca-an-implementation-guide-to-iso-270012013/. [cit. 2024-02-12].

BŘICHÁČEK, Zdeněk. *Audit informační bezpečnosti – systém řízení informační bezpečnosti (ISMS)*. Online. 2015, 03.06. 2015. Dostupné z: https://blog.brichacek.net/audit-informacni-bezpecnosti-system-rizeni-informacni-bezpecnosti-isms/. [cit. 2024-02-27].

CALDER, Alan a WATKINS, Steve. *IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002*. Seventh edition. London: Kogan Page, 2020. ISBN 978-0749496951.

DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

DURAČINSKÁ, Zuzana. *NIS: Co přináší nová směrnice EU o síťové a informační bezpečnosti?* Online. IT Strategie. 2016. Dostupné z: https://www.nic.cz/files/nic/doc/ITSystems_NIS_102016.pdf. [cit. 2024-02-29].

EUCERT. *Norma ISO/IEC 27001:2022: Jaké jsou klíčové změny v normě ISO/IEC 27001:2022?* Online. EUCERT. Certifikační orgán. 2023, 22.05.2023. Dostupné z: https://eucert.cz/norma-iso-27001-2022/. [cit. 2024-03-01].

EUROPEAN COMMISSION. *What Is Personal Data?* Online. European Commission. 2024. Dostupné z: https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en. [cit. 2024-02-13].

GILLIS, Alexander S. *What is a Risk Assessment?* Online. TechTarget. 2023. Dostupné z: https://www.techtarget.com/searchsecurity/definition/risk-assessment. [cit. 2024-04-01].

HUMPHREYS, Edward. *Implementing the ISO/IEC 27001 ISMS Standard*. Second edition. Information Security and Privacy Series. Boston: Artech House, 2016. ISBN 978-1-60807-930-8.

IMPERVA. *Information Security: The Ultimate Guide*. Online. Imperva. 2024. Dostupné z: https://www.imperva.com/learn/data-security/information-security-infosec/. [cit. 2024-02-29].

INVESTOPEDIA. *What Is a Business Continuity Plan (BCP), and How Does It Work?* Online. KENTON, Will. Investopedia. 2024, 20.02.2024. Dostupné z: https://www.investopedia.com/terms/b/business-continuity-planning.asp. [cit. 2024-03-27].

IT SLOVNÍK. *Co je to Data?* Online. IT Slovník. 2024. Dostupné z: https://it-slovnik.cz/pojem/data. [cit. 2024-03-24].

IT SLOVNÍK. *Co je to Hardware?* Online. IT Slovník. 2024. Dostupné z: https://it-slovnik.cz/pojem/hardware. [cit. 2024-03-24].

IT SLOVNÍK. *Co je to Software?* Online. IT Slovník. 2024. Dostupné z: https://it-slovnik.cz/pojem/software. [cit. 2024-03-24].

JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. Výkladový slovník kybernetické bezpečnosti. Online. Třetí vydání. Praha: AFCEA, 2015. Dostupné z: https://www.cybersecurity.cz/data/slovnik_v310.pdf. [cit. 2024-02-27].

KIDD, Chrissy. *What is COBIT? COBIT Explained*. Online. 2019. Dostupné z: https://www.bmc.com/blogs/cobit/. [cit. 2024-04-18].

KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.

KOLOUCH, Jan. *CyberCrime*. Online. Praha: CZ.NIC, z. s. p. o., 2016. ISBN 978-80-88168-18-8. Dostupné z: https://knihy.nic.cz/files/edice/cybercrime.pdf. [cit. 2024-02-29].

MOYLE, Ed. *CERT vs. CSIRT vs. SOC: What's the difference?* Online. TechTarget. 2024, 17.01.2024. Dostupné z: https://www.techtarget.com/searchsecurity/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference. [cit. 2024-02-29].

NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Právo pro praxi. Praha: Grada Publishing, 2017. ISBN 978-80-271-0668-4.

NIST. *CyberSecurity*. Online. NIST. 2024. Dostupné z: https://www.nist.gov/cybersecurity. [cit. 2024-02-29].

NIST. *Information*. Online. Computer Security Resource Center. 2024. Dostupné z: https://csrc.nist.gov/glossary/term/information. [cit. 2024-02-27].

NÚKIB. *Nová směrnice EU o kybernetické bezpečnosti „NIS2“*. Online. NÚKIB. 2024. Dostupné z: https://osveta.nukib.cz/mod/page/view.php?id=2582. [cit. 2024-02-29].

OTTERLOO, Sieuwer. *Information security and PDCA (Plan-Do-Check-Act)*. Online. ICT Institute. 2017. Dostupné z: https://ictinstitute.nl/pdca-plan-do-check-act/. [cit. 2024-02-12].

SEDLÁK, Petr a KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

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

SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. 1. vydání. Plzeň: Vykladatelství a nakladatelství Aleš Čeněk, s.r.o., 2019. ISBN 978-80-7380-765-8.

ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ [ÚNMZ]. ČSN EN ISO/IEC 27001:2022, *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky*. Česká agentura pro standardizaci, 2023.

ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ [ÚNMZ]. ČSN EN ISO/IEC 27001:2013, *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky.* Česká agentura pro standardizaci, 2014.

ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ [ÚNMZ]. ČSN EN ISO/IEC 9001:2015, Kvalita – *Systémy managementu kvality – Požadavky*. Česká agentura pro standardizaci, 2016.

VAUGHAN, Jack. *Data*. Online. TechTarget. 2019. Dostupné z: https://www.techtarget.com/searchdatamanagement/definition/data. [cit. 2024-02-27].

VÝZKUMNÝ ÚSTAV BEZPEČNOSTI PRÁCE [VÚBP], V. V. I. *Rizika a nebezpečí*. Online. Znalostní Systém Prevence Rizik v BOZP. 2024. Dostupné z: https://zsbozp.vubp.cz/rizika-a-nebezpeci. [cit. 2024-02-27].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BI	Bezpečnost informací
	Information Security
BOZP	Bezpečnost a ochrana zdraví při práci
CIA	Confidentiality, Integrity, Availability
	Důvěrnost, Integrita, Dostupnost
COBIT	Control Objectives for Information and Related Technology
	Kontrolní cíle pro informační a související technologie
COSO	Committee of Sponsoring Organizations
	Výbor sponzorujících organizací
DCC	Data Control Center
	Středisko pro řízení dat
DMS	Document Management System
	Systém pro správu dokumentů
EnMS	Energy Management System
	Systém pro řízení energie
ESD	Electrostatic Discharge
	Elektrostatický výboj
ESG	Environment, Social and Governance
	Životní prostředí, sociální odpovědnost a správa
EU	European Union
	Evropská unie
HSF	Hazardous Substance Free
	Bez nebezpečných látek
ICT	Information and Communication Technology
	Informační a komunikační technologie

IEC	International Organization Commission
	Mezinárodní organizační komise
IP	Internet Protocol
	Internetový protokol
ISACA	Information Systems Audit and Control Association
	Asociace auditu a řízení informačních systémů
ISMS	Information Security Management System
	Systém řízení bezpečnosti informací
ISO	International Organization for Standardization
	Mezinárodní organizace pro normalizaci
IT	Information Technology
	Informační technologie
ITIL	Information Technology Infrastructure Library
	Knihovna infrastruktury informačních technologií
ITSM	IT Service Management
	Řízení služeb IT
NIS	Network and Information Security
	Síťová a informační bezpečnost
NIST	National Institute of Standards and Technology
	Národní institut pro normy a technologii
PDA	Personal Digital Assistant
	Osobní digitální asistent
PDCA	Plan-Do-Check-Act
	Plánuj, dělej, kontroluj a jednej
PDF	Portable Document Format
	Přenosný formát dokumentu

PO	Požární ochrana
QC	Quality Control
	Kontrola kvality
RAM	Random Access Memory
	Paměť s náhodným přístupem
THP	Technickohospodářský pracovník
UPS	Uninterruptible Power Supply
	Nepřetržitelný zdroj napájení
USB	Universal Serial Bus
	Univerzální sériová sběrnice
VPN	Virtual Private Network
	Virtuální privátní síť

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

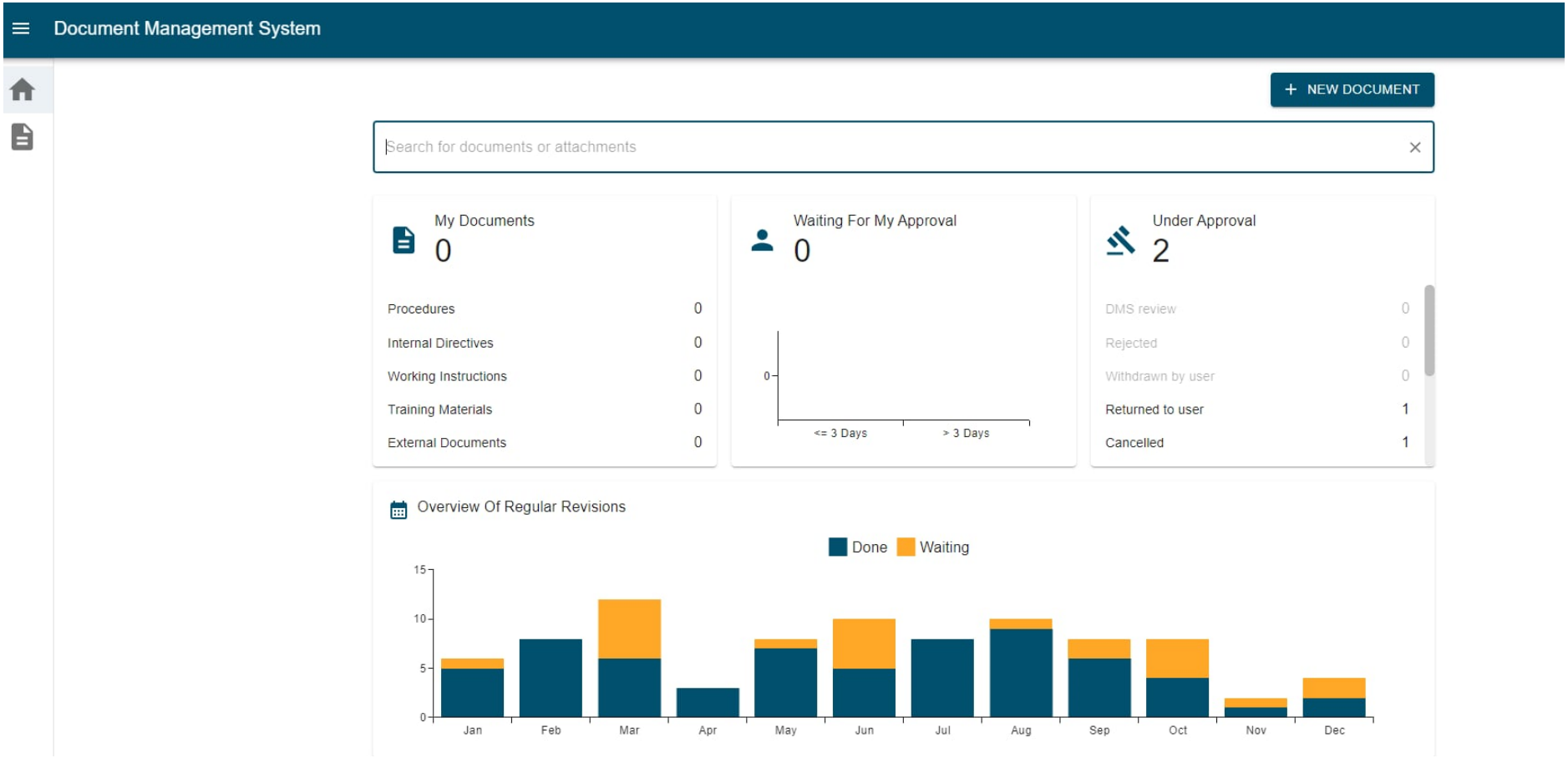
SEZNAM PŘÍLOH

PŘÍLOHA P I: PŘEDSTAVENÍ DMS SYSTÉMU

Obrázek 18 zobrazuje oficiální logo systému DMS.

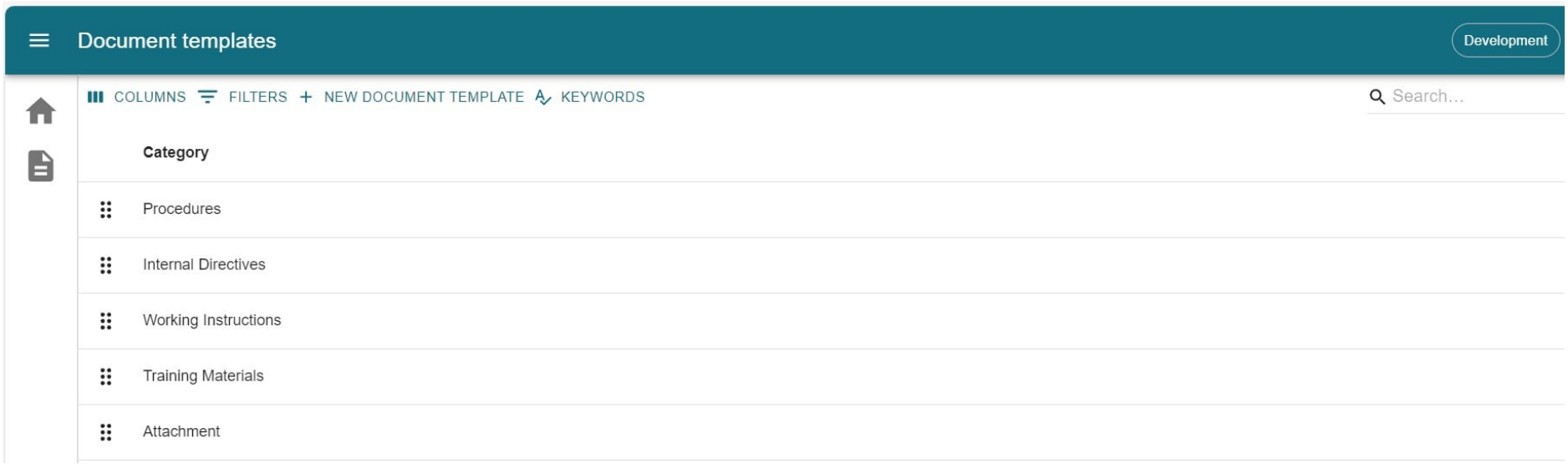
Obrázek 18 - Oficiální logo systému DMS. Zdroj: Interní systém společnosti

Obrázkem 19 je vyobrazena hlavní stránka systému, na které jsou ukazatele počtu vlastních dokumentů a dokumentů čekajících na schválení.



Obrázek 19 - Homepage. Zdroj: Interní systém společnosti

Obrázek 20 představuje vzor vložení nového dokumentu. Lze vybrat z kategorií, jako například postupy, vnitřní směrnice, pracovní pokyny, školicí materiály či přílohy. V systému je možné dokumenty filtrovat dle potřeby.



Obrázek 20 - Oficiální vzory dokumentace. Zdroj: Interní systém společnosti