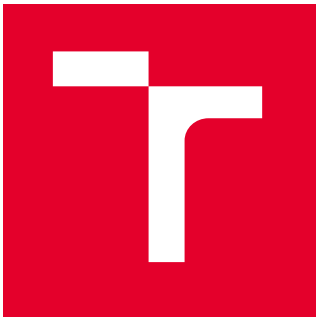


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

ZVÝŠENÍ ÚROVNĚ KYBERNETICKÉ BEZPEČNOSTI V ORGANIZACI

INCREASING THE LEVEL OF CYBER SECURITY IN THE ORGANIZATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Jiří Bartoš**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2025

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Jiří Bartoš**
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2024/25
Studijní program:	Informační management

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

Zvýšení úrovně kybernetické bezpečnosti v organizaci

Charakteristika problematiky úkolu:

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

Cíle, kterých má být dosaženo:

Cílem je analyzovat stávající stav vybrané organizace z pohledu kybernetické bezpečnosti, posoudit tento stav a navrhnout změny, směřující k zvýšení úrovně kybernetické bezpečnosti.

Základní literární prameny:

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

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

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

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

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

V Brně dne 9.2.2025

L. S.

doc. Ing. Miloš Koch, CSc. garant	prof. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

ABSTRAKT

Diplomová práce analyzuje stávající úroveň kybernetické bezpečnosti ve vybrané organizaci. Práce identifikuje klíčové nedostatky a navrhuje opatření pro zvýšení celkové ochrany podle vybrané normy. Na základě teoretického rámce a provedené analýzy je formulován komplexní soubor doporučení ke zlepšení odolnosti organizace vůči kybernetickým hrozbám a vylepšení systému řízení bezpečnosti informací.

ABSTRACT

This thesis analyzes the current cybersecurity of a chosen organization. It finds key weaknesses and suggests ways to improve overall protection based on a specific standard. Using theory and analysis, it provides a full set of recommendations to make the organization more resistant to cyber threats and to improve its information security management.

KLÍČOVÁ SLOVA

ISMS, aktiva, analýza rizik, bezpečnostní opatření

KEYWORDS

ISMS, assets, risk analysis, security measures

BIBLIOGRAFICKÁ CITACE

Citace tištěné práce – listinná verze:

BARTOŠ, Jiří. *Zvýšení úrovně kybernetické bezpečnosti v organizaci*. Diplomová práce. Petr SEDLÁK (vedoucí práce). Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2025.

Citace elektronického zdroje – elektronická verze:

BARTOŠ, Jiří. *Zvýšení úrovně kybernetické bezpečnosti v organizaci*. Online, diplomová práce. Petr SEDLÁK (vedoucí práce). Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2025. Dostupné z: https://www.vut.cz/studenti/zav-prace/detail/167905. [cit. 2025-05-19].

ČESTNÉ PROHLÁŠENÍ

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

V Brně dne 19. května 2025

PODĚKOVÁNÍ

Tímto bych rád poděkoval vedoucímu mé diplomové práce panu Ing. Petru Sedlákovi za společné konzultace, nápomoc při řešení problémů a spoustu doporučení. Taktéž děkuji panu Ing. Janu Rosenbergovi za oponenturu této práce. Na závěr bych chtěl poděkovat vybrané společnosti, ve které jsem měl možnost zpracovávat tuto práci, za poskytnutý čas a informace.

OBSAH

ÚVOD

V dnešní době jsou data a informační systémy nedílnou součástí každé organizace a slouží jako klíčové aktivum, které je nezbytné chránit vůči negativním vnějším vlivům. Přesun organizací do digitálního prostředí umožňuje efektivnější práci, ale zvyšuje důraz na kybernetickou bezpečnost a ochranu dat proti kybernetickým útokům. Data a informace jsou základem moderního podnikání a musí být u nich zajištěna důvěrnost, integrita a dostupnost. Ignorování kybernetické bezpečnosti může vést až k vážným následkům jako finanční ztráty, poškození značky společnosti a ztráty konkurenceschopnosti.

Tato diplomová práce se zabývá problematikou kybernetické bezpečnosti a bezpečnosti informací ve vybrané společnosti. V teoretické části je čtenář obeznámen s klíčovými normami, legislativou a postupy v oblasti bezpečnosti informací, jenž slouží jako základ k následujícím analýzám. V analýze stávajícího stavu je provedena GAP analýza vůči vybrané normě ČSN EN ISO/IEC 27001:2023, pomocí které jsou identifikována slabá místa a celkové zhodnocení stavu v organizaci v přístupu k systému řízení bezpečnosti informací.

Výstupem práce jsou konkrétní návrhy řešení, doporučení pro společnost a ekonomické zhodnocení. Tento výstup má za úkol pomoci společnosti zlepšit svůj stav vůči bezpečnosti informací, kybernetické bezpečnosti a nastavit metodiku pro budoucí kroky v této oblasti.

1 CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

1.1 Cíle práce

Cílem je analyzovat stávající stav vybrané organizace z pohledu kybernetické bezpečnosti, posoudit tento stav a navrhnout změny, směřující k zvýšení úrovně kybernetické bezpečnosti.

1.2 Metody a postupy zpracování

Vzhledem k obecnějšímu cíli se práce primárně zaměřuje na to, aby bylo přistupováno k problematice kybernetické bezpečnosti a bezpečnosti informací metodicky. V práci bude cíl zpracováván na nejmenované firmě s určitou mírou anonymity, aby nedošlo k prozrazení tajemství nebo know-how společnosti.

První částí práce je zpracování teoretických východisek jako seznámení se s normami, legislativou a ověřenými postupy v oblasti bezpečnosti informací a kybernetické bezpečnosti.

Zjištění stávajícího stavu je provedeno pomocí GAP analýzy vůči vybrané normě ČSN EN ISO/IEC 27001:2023 jako uznávanou normou v oblasti systému řízení bezpečnosti informací. GAP analýza je základním vstupem pro následující návrhy řešení, protože specifikuje slabá místa a nedostatky v systému řízení bezpečnosti informací v organizaci a provádí základní kategorizaci.

Návrh řešení navazuje na GAP analýzu a provádí doporučení a návrh řešení pro nevyhovující body, včetně závěrečného ekonomického zhodnocení.

2 TEORETICKÁ VÝCHODISKA

2.1 Základní názvosloví

IT – informační technologie.

ICT – informační a komunikační technologie.

IS – informační systém.

ISMS – systém řízení informační bezpečnosti. (1)

2.2 Základní pojmy v oboru ISMS

Kybernetický prostor

Kybernetický prostor představuje prostředí pro vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací. (2)

Kybernetická bezpečnost

Kybernetická bezpečnost je soubor prostředků zahrnující právní předpisy, technické nástroje, organizační struktury a vzdělávací programy vedoucí k zajištění ochrany kybernetického prostoru. (2)

Bezpečnost informací

Bezpečnost informací se zabývá ochranou informací. Jedná se o zachování dostupnosti, integrity a důvěrnosti. Bezpečnost informací zahrnuje bezpečnost IS/ICT a zároveň bezpečnost informací v nedigitální formě. (1)

Dostupnost

Dostupnost je spolehlivé poskytnutí informací pro oprávněného uživatele v potřebném čase. (1)

Důvěrnost

Důvěrnost je zajištění informací pouze oprávněnému uživatele, aby nedošlo k neautorizovanému odhalení. (1)

Integrita

Integrita je zajištění správnosti a úplnosti informace a zamezení neautorizované modifikaci. (1)

Aktivum

Aktivum je cokoli, co má pro organizaci hodnotu a z toho důvodu vyžaduje ochranu. Základní dělení aktiv je na primární aktiva a podpůrná aktiva.

Aktiva lze dělit i na konkrétnější části. Norma ISO/IEC 27002 rozděluje primární aktiva na informace a procesy a činnosti společnosti, podpůrná aktiva na hardware, software, síť, pracovníci, lokalita a struktura organizace. Vyhláška o kybernetické bezpečnosti rozděluje primární aktiva na informace a služby, podpůrná aktiva na technická aktiva, zaměstnance a dodavatelé. Tyto kategorie lze upravit dle potřeby podniku. (3; 4)

Hrozba

Hrozba je potenciální příčinou incidentu, který může způsobit poškození systému nebo organizace. (4)

Zranitelnost

Zranitelnost je slabým místem aktiva nebo opatření. Toto místo může být využito jednou nebo více hrozbami. (4)

Opatření

Opatření je prostředkem řízení, jehož cílem je udržovat úroveň rizika nebo jej modifikovat.

Opatření lze dělit na:

a) Organizační opatření,
b) opatření v oblasti lidských zdrojů,
c) opatření fyzické bezpečnosti,
d) technologické opatření. (4)

Riziko

Riziko je míra ohrožení aktiva. Lze jej chápat jako vyjádření pravděpodobnosti, že dojde ke vzniku škody na daném aktivu. (1)

Dopad

Dopad vyjadřuje škodu, pokud by zapůsobila hrozba na určité aktivum. (1)

Bezpečnostní událost

Bezpečnostní událost je zjištěný stav systému, služby nebo sítě, které naznačuje možné narušení politiky bezpečnosti informací nebo selhání opatření. (5)

Bezpečnostní incident

Bezpečnostní incident je případ, kdy bezpečnostní událost nebo série událostí mohou ovlivnit a ohrozit bezpečnost informací. (5)

2.3 Legislativa v oboru ISMS

2.3.1 Pojmy

Legislativa

Legislativa je tvorba právních předpisů, primárně se jedná o zákony. Rozděluje se na dvě části, první částí je politická, kde dochází k politické vůli přijmout zákon, druhá část je legislativní, kde dochází k formulaci zákonné normy. (6)

Zákon

Zákon je právní akt nejvyšší právní síly vydávaný parlamentem. V České republice jsou zákony přijímány Poslaneckou sněmovnou Parlamentu ČR a jsou zveřejňovány ve Sbírce zákonů. (6)

Vyhláška

Vyhláška je obecně závazný právní předpis. V České republice jsou vyhlášky vydávány na podkladě příslušného zákona ústředními orgány státní správy jako ministerstva a další úřední orgány. Vyhláška nemění obsah zákona, ale upřesňuje jej a konkretizuje, jakým způsobem se má provést. (6)

Směrnice

„Směrnice je právní akt stanovující cíl, který musejí všechny země EU splnit. Je však na jednotlivých zemích, jak formulují příslušné vnitrostátní zákony a jak těchto cílů dosáhnou.“ (7)

Nařízení

„Rozhodnutí je závazné pro všechny, kterým je určeno (např. pro členský stát EU nebo určitou obchodní společnost), a je přímo použitelné.“ (7)

2.3.2 Zákon o kybernetické bezpečnosti

Zákon v české legislativě zabývající se kybernetickou bezpečností je zákon o kybernetické bezpečnosti (ZKB) č. 181/2014 Sb. Tento zákon upravuje práva a povinnosti osob, zároveň upravuje působnost a pravomoci veřejné moci v oblasti kybernetické bezpečnosti. (8)

2.3.3 Vyhláška o kybernetické bezpečnosti

Prováděcím předpisem zákona o kybernetické bezpečnosti je vyhláška o kybernetické bezpečnosti (VKB) č. 82/2014 Sb. zpracovaná Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB). (3)

2.3.4 Směrnice NIS2

Směrnice NIS2 (Network and Information Systems Directive) je směrnice vydaná Evropskou unií v roce 2016. Nabytí směrnice by mělo proběhnout v rámci zákona o kybernetické bezpečnosti s odhadovaným vydáním v půlce roku 2025. Primárním cílem je harmonizovat přístup členských států EU k bezpečnosti sítí a informačních systémů a zavést jednotný standard pro zlepšení fungování vnitřního trhu. Stěžejními změnami bude zavedení dvou režimů povinností (vyšší a nižší), povinnosti pro poskytovatele regulovaných služeb jako zavádění bezpečnostních opatření, hlášení kybernetických bezpečnostních incidentů a další. (9; 10)

2.4 Normy v oboru ISMS

2.4.1 Organizace

ISO

ISO (International Organization for Standardization) je organizace, která se zabývá tvorbou mezinárodních norem. Oficiálně byla založena v roce 1947 a sdružuje globální odborníky, aby se shodli na nejlepším způsoby dělání věcí od tvorby produktu až po vedení procesu. Normy slouží, aby dělaly život jednodušší, bezpečnější a lepší. (11)

IEC

IEC je celosvětová, nezisková členská organizace sdružující 173 států a 20000 odborníků z celého světa. Ověřuje bezpečnost, výkon a interoperabilitu elektrických a elektronických zařízení a systémů jako například mobilní telefony, lednice, kancelářské a zdravotní vybavení, informační technologie, výrobu elektřiny a další. Organizace byla založena v roce 1906. (12)

EN

EN je zkratka pro Evropskou normu. Evropská norma je technický dokument, který udává pravidla, pokyny nebo specifikace pro výrobky, procesy nebo služby. Normy jsou vytvářeny organizacemi CEN, CENELEC a ETSI. K tvorbě norem přispívá více než 200000 odborníků. (13)

ČSN

ČSN je zkratkou pro Česká technická norma, která je zřizovaná ČAS (Česká agentura pro standardizaci). ČAS je zřízená státní příspěvková organizace Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. ČAS se využívá pro několik různých účelů. Základní účel činnosti agentury je zabezpečování tvorby, vydávání a distribuce českých technických norem. (14; 15)

2.4.2 ČSN EN ISO/IEC 27000:2020

Norma popisuje přehled a slovník v oblasti ISMS. Primárními oblastmi je přehled norem ISMS, úvod k ISMS a termíny a definice použité v řadě norem ISMS.

V přehledu norem se jedná o normy: 27000, 27001, 27002, 27003, 27004, 27005, 27006, 27007, TR 27008, 27009, 27010, 27011, 27013, 27014, TR 27016, 27017, 27018, 27019, 27021. Normy jsou rozděleny do čtyř základních sekcí: normy slovníku, normy požadavků, normy směrnice, normy směrnic podle oborů. (5)

2.4.3 ČSN EN ISO/IEC 27001:2023

Norma ISO/IEC 27001 stanovuje požadavky na ustavení, implementaci, provoz, monitorování, přezkoumávání, udržování a vylepšování ISMS v kontextu činnosti organizace. Tuto normu lze používat ve všech organizacích bez ohledu na typ, velikost

a povahu. V případě, že organizace chce být auditována a certifikována v oblasti ISMS, musí mít shodu s touto normou. (5)

Přijetí ISMS v organizaci je strategickým rozhodnutím, požadavky na bezpečnost a je potřeba jej zasadit do celkové strategie firmy a cílů. Je podstatné, aby ISMS bylo začleněno do celkové struktury managementu organizace a informační bezpečnost byla zohledněna při navrhování procesů, informačních systémů a opatření. (16)

2.4.4 ČSN EN ISO/IEC 27002:2023

Norma ISO/IEC 27002 zahrnuje oblast opatření a detailně popisuje jednotlivá opatření, která mají být použity jako návod při implementaci a výběru opatření. (5)

Normu lze využít na všechny typy a velikosti organizací, slouží jako seznam opatření obecně uznávaná v oblasti opatření informační bezpečnosti. Informační bezpečnosti je dosáhnuto za pomocí správného výběru opatření. Organizace má tato opatření definovat, zavést, monitorovat, přezkoumávat a zlepšovat. Opatření má za cíl riziko udržovat, nebo jej modifikovat. Stanovení opatření je na základě rozhodnutí organizace a mělo by být po posouzení rizik s jasně definovaným rozsahem. (4)

2.4.5 ČSN EN ISO/IEC 27003:2018

Norma ISO/IEC 27003 obsahuje postup a návod pro ISO/IEC 27001. (5)

Tato norma popisuje postup, jakým způsobem zavádět ISO/IEC 27001. Organizace není povinná dodržovat veškeré body v této normě.

V rámci ISMS jsou zdůrazněny následující fáze:

- Pochopení potřeb organizace a ustanovení politiky a cílů organizace v oblasti bezpečnosti informací,
- posouzení rizik organizace v oblasti bezpečnosti informací,
- implementace, provozování procesu, kontrol a opatření v oblasti bezpečnosti informací,
- monitorování a prozkoumávání výkonnosti ISMS,
- neustálé zlepšování.

ISMS zahrnuje několik klíčových komponent jako politiku, definované osoby s definovanými odpovědnostmi, procesy (ustavení politiky, poskytování

povědomí, plánování, implementace a další), dokumentované informace a posuzování rizik bezpečnosti informací a jejich ošetření.

Normu lze využít na všechny typy a velikosti organizací. (17)

2.4.6 ČSN EN ISO/IEC 27005:2023

Norma ISO/IEC 27005 poskytuje směrnice pro řízení rizik bezpečnosti informací. Poskytuje tím návod pro implementaci přístupu k řízení rizik, aby byly v dostatečné míře splněny požadavky z ISO/IEC 27001 v oblasti řízení rizik bezpečnosti informací. (5)

Normu lze využít na všechny typy a velikosti organizací. Pomáhá organizacím splnit požadavky ISO/IEC 27001 a provádět aktivity v oblasti managementu rizik informační bezpečnosti, primárně posuzování rizik a jejich ošetření. (18)

2.5 Postup zavádění ISMS

Postup zavádění ISMS je podrobně popsán v normě ČSN EN ISO 27003:2018. Následující kapitola je tvořena kombinací této normy a zbývajících norem řady 27000 jako ČSN EN ISO/IEC 27000:2020 a ČSN EN ISO/IEC 27001:2023. V případě potřeby většího detailu je doporučeno využít napřímo zmíněné normy nad rámec následujícího popisu, který je zjednodušen na nejpodstatnější části. (17; 5; 16)

2.5.1 Kontext organizace

První částí implementace ISMS je sběr informací o vnitřním a vnějším prostředí dané společnosti. Vzhledem k tomu, že norma je obecně použitelná pro různé velikosti a typy firem, bude vymezení rozsahu ISMS určovat zpracování následujících částí.

2.5.1.1 Pochopení organizace a jejího kontextu

Pro dosažení zamýšleného výsledku ISMS organizace určuje vnější a vnitřní prostředí, které nějakým způsobem ovlivňuje bezpečnost informací. Účelem je porozumět tomuto prostředí, aby šlo rozhodnout o rozsahu ISMS, zjistit rizika a příležitosti a zajištění přizpůsobení ISMS vnějším a vnitřním záležitostem.

Vnější záležitosti organizace jsou například:

- Aspekty jako sociální a kulturní, politické, právní a jiné regulatorní, ekonomické a finanční, technologické, přirozené, konkurenční,
- katastrofy jako požár, povodeň a zemětřesení,
- obecný požadavek na služby organizace.

Vnitřní záležitosti organizace jsou například:

- Kultura organizace,
- vnitřní politiky, cíle, strategie,
- dříve zavedené normy, směrnice,
- procesy a postupy.

Vnitřních a vnějších záležitostí může být mnohem více, záleží na typu a velikosti firmy.

2.5.1.2 Pochopení potřeb a očekávání zainteresovaných stran

Organizace určuje zainteresované strany. Opět se využívá přístupu vnitřních a vnějších zainteresovaných stran. Zainteresovaná strana je osoba nebo skupina osob, které mohou ovlivnit nebo být ovlivněny organizací. Mohou mít požadavky nebo očekávání na organizaci, v tomto případě v kontextu ISMS.

Vnější zainteresované strany jsou například:

- Akcionáři, vlastníci a investoři,
- dodavatelé, subdodavatelé,
- konkurence,
- zákazníci a spotřebitelé.

Vnitřní zainteresované strany jsou například:

- Vrcholové vedení a jiní klíčoví rozhodovatelé,
- ostatní zaměstnanci,
- vlastníci procesů, informací, systémů.

Vnitřních a vnějších zainteresovaných stran může být mnohem více, záleží na typu a velikosti firmy.

Je třeba zjistit vnější a vnitřní zainteresované strany a jejich požadavky a v průběhu času přezkoumávány vzhledem k jejich změnám.

2.5.1.3 Určení rozsahu ISMS

Určení rozsahu ISMS vzniká kombinací vstupů z vnitřních a vnějších záležitostí, zainteresovaných stran a jejich požadavků a dalšími body popsané v této kapitole.

Ustanovení rozsahu ISMS je klíčová a nezbytná činnost pro všechny následující činnosti, aby bylo jasně zřetelné, do jaké míry bude ISMS uplatňováno. Rozsah může být od jednoho procesu až po celý subjekt nebo i dodavatele.

Určení rozsahu může být zpracování po iteracích, kdy prvotní iterací je stanovení předběžného rozsahu a postupně je upřesňován do dostatečného detailu. Rozsah by měl být schválen a zadokumentován zástupci vedení organizace. Dokumentace by měla obsahovat rozsah z pohledu organizačního, hranicemi informačních a komunikačních technologií a fyzického rozsahu.

2.5.2 Vůdčí role

Před zaváděním ISMS musí být organizace připravena poskytnout těmto činnostem dostatečnou podporu a dodat pro tyto činnosti potřebné zdroje.

2.5.2.1 Vůdčí role a závazek

Vedení společnosti si zachovává zodpovědnost za ISMS a jeho údržbu. Má možnost delegovat aktivity a poskytovat prostředky, ale v závěru nese veškerou zodpovědnost. Existuje několik aktivit, které by vedení mělo provádět. Mezi ně patří:

- Zajištění, že je vytvořena politika bezpečnosti informací a cíle v oblasti bezpečnosti informací a lze je zapojit do strategického směrování firmy.
- Zajištění, že budou pro ISMS dostatečné zdroje finanční, lidské, zařízení a technická infrastruktura.
- Zajištění, že jsou oznámeny požadavky a potřeby ISMS do organizace a důvody jejich plnění.
- Zajištění, že dochází k přezkoumávání dodržování a efektivnosti ISMS.

Principiálně by měla být podpora u činností ISMS a potřeby zavádění změn, pokud budou potřeba.

2.5.2.2 Politika

Organizace by měla vytvořit politiku bezpečnosti informací, jejíž obsahem by měl být stručný popis a prohlášení o záměru zavádění bezpečnosti informací. Tato politika by měla být upravena podle konkrétní organizace (vzhledem k její náplni, činnostem, kultuře apod.) a to z toho důvodu, aby byla pro uživatele pochopitelná a mohli se identifikovat se směřováním této politiky. Politika by měla obsahovat cíle nebo rámec směrování bezpečnosti informací a být upravena takovým způsobem, aby byl dostatečný rozpad pro všechny zainteresované strany.

Vedení určuje, komu bude politika nasdílena a zdali nebude spojena s existujícími politikami v jiných oblastech. Politika musí být sestavena s povědomím, kdo bude k politice přistupovat. Pokud by například měla být sdílena externím stranám, politika by neměla obsahovat důvěrné informace.

2.5.2.3 Organizační role, odpovědnosti a pravomoci

Pro zajištění správnosti musí vedení společnosti zajistit přidělení odpovědností a pravomocí, aby mohly být splněny veškeré požadavky ISMS.

Mezi činnosti spadá:

- Implementace, údržba, hlášení o stavu a výkonnosti ISMS,
- řízení incidentů bezpečností informací,
- hodnocení a ošetřování rizik bezpečnosti informací,
- konfigurace a provoz opatření bezpečnosti informací,
- audit ISMS.

Vedení nemusí nutně přidělovat veškeré role, ale případně v dostatečné míře delegovat, aby mohlo být ISMS zajištěno do požadované míry.

2.5.3 Plánování

2.5.3.1 Činnosti pro řešení rizik a příležitostí

V rámci normy se rozdělují rizika do 2 základních kategorií:

1. Rizika spojené se zamýšleným výsledkem ISMS.

2. Rizika bezpečnosti informací z pohledu důvěrnosti, integrity a dostupnosti v rámci ISMS.

V první kategorii se jedná o obecná rizika se zaváděním ISMS a jeho výsledkem. Ve druhé kategorii rizik se jedná o rizika v souvislosti rozsahu ISMS, kde postup tohoto zpracování bude v samotné kapitole. Zpracování rizik má několik motivací jako zajištění, že ISMS bude zajišťovat očekávané výsledky, předcházet negativním účinkům a trvalé zlepšování.

Organizace stanovuje procesy, podle kterých posuzuje rizika bezpečnosti informací. Nastavuje si kritéria vedoucí k akceptaci rizika a kritéria pro posuzování bezpečnosti informací (např. pravidla pro určení úrovně rizika, odhady dopadu a pravděpodobnosti apod.). Tento proces by měl být opakovatelný a konzistentní, aby při opakování přinášel srovnatelné výsledky.

Proces rizik bezpečnosti informací je rozdělen na tři hlavní části:

- Identifikace rizik bezpečnosti informací,
- analýza rizik bezpečnosti informací
- vyhodnocení rizik bezpečnosti informací.

Identifikace rizik zahrnuje identifikaci rizik spojené se ztrátou důvěrnosti, integrity a dostupnosti a identifikaci vlastníků rizik jako osoby s pravomocemi a odpovědnostmi za řízení identifikovaných rizik.

Analýza rizik informací se zabývá odhadováním dopadu, pokud by se rizika projevila (např. vyjádřené peněžně). Dále se zabývá odhadem pravděpodobnosti, že dané riziko nastane. Celkové riziko vzniká kombinací dopadu a pravděpodobnosti. Dopad a pravděpodobnost mohou být vyjádřené kvalitativně, semikvantitativně nebo kvantitativně.

Vyhodnocení rizik pracuje s variantou přijetí rizika (na základě dříve určeného kritéria), nebo s nastavováním priority u nepřijatelných rizik. Mělo by dojít k určení priority a pořadí, ve kterém se budou zavádět pro daná rizika opatření.

Analýza rizik jsou uchovány jako dokumentované informace.

Detailní popis managementu řízení rizik bezpečnosti informací bude popsán v samostatné kapitole.

2.5.3.2 Cíle bezpečnosti informací a plánování jejich dosažení

Organizace stanovuje, plánuje a zveřejňuje cíle bezpečnosti informací. Cíle jsou podstatné z pohledu strategických cílů a implementace politiky bezpečnosti informací. Cíle se taktéž využívají pro specifikaci a měření výkonnosti procesů a opatření v souladu s politikou bezpečnosti informací a využívají se jako vstup pro posuzování rizik.

Cíle bezpečnosti informací jsou zapadající do politiky bezpečnosti informací, pokud je možné, tak jsou měřitelné pomocí vybrané metriky, propojeny s požadavky a výsledky posuzování rizik, oznámeny do organizace a aktualizovány.

2.5.4 Podpora

2.5.4.1 Zdroje

Pro stanovení, implementaci a údržbu a zlepšování ISMS organizace poskytuje dostatečné množství zdrojů.

2.5.4.2 Kompetence

Organizace určuje kompetence, aby byla zajištěna pro činnosti zpracování bezpečnosti informací. Kompetence lze zajistit interně nebo externě. V případě interního zajištění může organizace zvýšit pomocí školení jako kurzy, semináře, workshopy nebo odborného vedení. V případě externího zajištění může být využito smlouvy s externími odborníky a využití jejich kompetenci pro naplnění cílů ISMS.

2.5.4.3 Povědomí

Systém řízení bezpečnosti informací, její politika a cíle jsou v rámci organizace předávány osobám v organizaci pracujícím. Základním principem povědomí je namotivovat pracovníky, aby podporovali cíle ISMS a dodržovali pravidla ISMS na denní bázi. Musí být předána informace o dopadech při nedodržování pravidel ISMS. Úroveň sdíleného detailu politiky nemusí být do nejnižší, musí znát pravidla pro jejich pracovní pozici.

Organizace by měla připravit plán sdělení pro jednotlivé skupiny zaměstnanců, včetně očekávání, předat informace a ověřovat porozumění zaměstnanců s pravidly, jak na úrovni po školení, tak v náhodných intervalech.

Normy NIST uvádí metodiku pro oblast povědomí, která je postavena na čtyřech pilířích. Jedná se o pilíře:

- Awareness – povědomí,
- Training – výcvik (školení),
- Education – vzdělávání,
- Professional Development – profesní rozvoj.

Povědomí rozděluje do tří základních skupin: Začátečníci, středně pokročilí a pokročilí. Bezpečnostního povědomí je dosaženo plánovaným přístupem a přesnou specifikací školení pro jednotlivé skupiny uživatelů. Výstupem je matice SAE (Security Awareness Education) s individuálním plánem. (2)

2.5.4.4 Komunikace

Komunikace je klíčová při zavádění ISMS. Jedná se o komunikaci jak z interními, tak s externími zainteresovanými stranami na různých úrovních. Organizace si určuje, jaký obsah bude sdělovat, v jaký okamžik, jaké skupině osob, kdo zahajuje a jaké procesy komunikaci řídí.

2.5.4.5 Dokumentované informace

Dokumentované informace zahrnuje dokumentaci v rámci celého ISMS. Může se jednat o definice cílů, politik, procesů a dalších typů informací. Některé části zavádění ISMS a jeho údržby vyžaduje dokumentované informace povinně z důvodu zajištění efektivnosti ISMS a případných auditů.

Organizace si definuje strukturu dokumentovaných informací a způsob aktualizace. Dokumentované informace podléhají vybranému vedení a jejímu přezkoumání a schválení, aby byla zajištěna správnost, vhodnost pro daný účel, odpovídající formát a dostatečnou úroveň detailu. Dokumentované informace mohou být uchovány v jakékoli formě – papírová nebo elektronická. Organizace by měla vytvořit strukturovanou bázi dokumentovaných informací se vzájemným propojením (struktura dokumentu, šablony, odpovědnost za přípravu, schválení a zveřejnění). Styl by měl být přizpůsoben uživatelům.

Veškeré dokumenty by měly být klasifikovány, aby tím byla nastavena pravidla na jejich úpravu a distribuci. Detailní popis klasifikace informací je popsán v samostatné kapitole. Organizace by měla definovat, jak se bude nakládat s dokumentovanými informacemi po ukončení jejich platnosti.

2.5.5 Provozování

2.5.5.1 Plánování a řízení provozu

V rámci plánování a řízení provozu je zapotřebí, aby organizace plánovala, implementovala a řídila procesy podle dříve nastavených postupů, aby došlo k souladu s požadavky bezpečnosti informací a jejich cílů.

2.5.5.2 Posuzování rizik bezpečnosti informací

Organizace dodržuje stanovený proces v rámci posuzování rizik bezpečnosti informací a udržuje si dokumentované informace o výsledcích.

Pokud nastane výrazná změna v přístupu k ISMS nebo incidentu, organizace stanovuje, jaké změny nebo incidenty vyžadují další iteraci posouzení rizik bezpečnosti informací.

2.5.5.3 Ošetření rizik bezpečnosti informací

Organizace zavádí plány ošetření rizik bezpečnosti informací a udržuje si dokumentované informace o výsledcích. Plán ošetření rizik bezpečnosti informací by se měl aplikovat po každé iteraci posuzování rizik bezpečnosti informací. Implementace opatření by měla být řízena a může znamenat aktualizaci politiky, směrnic a komunikaci pro zainteresované strany.

2.5.6 Hodnocení výkonnosti

2.5.6.1 Monitorování, měření, analýza a hodnocení

Monitorováním, měřením, analýzou a následným vyhodnocením organizace kontroluje výkonnost a efektivnost ISMS. Cílem je vyhodnotit, zdali očekávaný výsledek odpovídá naměřenému stavu a je tak dosaženo plánu. V rámci monitoringu je třeba nastavit, co se má měřit, kdo a kdy má tuto věc měřit a jakou metodou. Následné analýze je třeba určit kdo a kdy má tuto analýzu provádět, pomocí jaké metody.

Hodnocení je rozděluje na dva základní atributy. První je hodnocení výkonnosti, které se zaměřuje na to, jak organizace pracuje podle očekávání a druhé je hodnocení efektivnosti, které se zaměřuje na to, jestli organizace provádí správné věci.

2.5.6.2 Interní audit

Interní audit je nástroj, pomocí kterého lze hodnotit ISMS v organizace v plánovaných intervalech a poskytuje vedení informaci o tom, zdali je ISMS ve správném stavu.

Organizace má povinnost udržovat program auditu a jeho výsledek jako dokumentovanou informaci.

V program auditu je definována struktura, odpovědnosti, vedení a komunikace zpráv o činnostech interního auditu a jeho dodržování. Norma nestanovuje konkrétní rozsah a četnost auditů, organizace si tyto atributy zvolí na základě její velikosti, povahy a komplexnosti. Program auditu by měl být navržen takovým způsobem, aby pokryl nezbytné oblasti a byl adekvátní.

Auditor určený pro interní audit může být vybrán jako interní zaměstnanec, nebo externí dodavatel. Auditor by měl být vybrán, aby měl dostatečnou kompetenci, nezávislost a dostatečnou míru školení.

Provedení auditu primárně zkoumá soulad požadavků normy s realitou v organizaci, plnění cílů ISMS, soulad s vlastními požadavky organizace, konzistence plánu ošetření rizik s identifikovanými riziky a jejich kritérii, popřípadě další prvky na základě potřeby organizace. Pokud jsou výsledkem neshody, kontrolovaný organizace stanovuje plán nápravy, který je odsouhlasený auditorem. Auditní zpráva se předkládá vedení organizace.

2.5.6.3 Přezkoumání vedením organizace

Vedení organizace by mělo vyžadovat podávání zpráv o výkonnosti ISMS, kdy účelem je zajistit, aby pokračovala vhodnost, adekvátnost a efektivnost ISMS v organizaci. K přezkoumání by mělo docházet alespoň jednou za rok za pomocí stanoveného časového a obsahového harmonogramu na schůzích vedení. Častější přezkoumávání se doporučuje u organizací s čerstvě nebo méně vyspělém ISMS, aby docházelo k rychlejšímu zvýšení efektivnosti.

2.5.7 Zlepšování

2.5.7.1 Neshody a nápravná opatření

V rámci ISMS může dojít k neshodám. Neshody mohou být vůči normě, implementaci opatření, nedodržení podmínek zákazníka apod.

Reakce na neshodu by měla být definovaná pomocí procesu zacházení s neshodou, jehož obsahem je určení rozsahu a dopadu neshody, rozhodnutí o opravě, komunikace s adekvátními osobami, provedení opravy a následném monitoringu. Celkovým cílem je dosáhnout řízeného stavu neshod a jejich dopadů. Organizace musí udržovat dokumentované informace o tom, že přiměřeně reagovala na opatření neshody a vyhodnotila důsledky a zdali opatření dosáhlo očekávaného výsledku.

2.5.7.2 Neustálé zlepšování

Neustálé zlepšování vede organizaci k tomu, aby neustále rozvíjela ISMS vzhledem ke změnám kontextu a požadavkům zainteresovaných stran. Systematický přístup ke zlepšování vede k efektivnějšímu ISMS a ke zlepšení bezpečnosti informací v organizaci. ISMS by mělo být vnímáno jako živá součást činností organizace a mělo by se vracet k průběžnému vyhodnocování.

Rozšířeným modelem neustálého zlepšování je Demingův cyklus taktéž zvaný PDCA. Zkratka PDCA odkazuje na činnosti prováděné v rámci cyklu:

- Plan – plánování záměru nebo procesu,
- do – realizování plánu,
- check – kontrola výsledku realizace oproti původnímu plánu,
- act – úprava plánu na základě výsledku. (19)

2.6 Klasifikace informací

Klasifikace informací je jedním ze základních opatření, jakým způsobem chránit informace před nežádoucí manipulací jako sdílení v organizaci, mezi organizacemi a s třetími stranami s osobami nebo skupinami, které mohou způsobit porušení důvěrnosti nebo integrity těchto informací.

2.6.1 Traffic Light Protocol

Pro účel klasifikace informací vznikl koncept Traffic Light Protocol (TLP) stanovující úrovně důvěrnosti informací, včetně jejich označení. TLP doporučuje i NÚKIB jako vhodný nástroj pro nastavení sdílení chráněných informací. (20)

TLP specificky nastavuje úrovně důvěrnosti, jejich popis a povinnosti při jejich používání v dokumentech (štítky, jejich velikost, barvy apod.).

TLP využívá 4 úrovně: TLP:RED, TLP:AMBER, TLP:GREEN a TLP:CLEAR. Každá úroveň má svůj popis, jakým osobám může být s danou úrovní dokument nasdílen a jaké jsou dopady při porušení. Tyto úrovně lze využít v rámci analýzy rizik ISMS. (21)

Tabulka 1: Traffic Light Protocol úrovně
(Zdroj: Vlastní zpracování dle: (21))

Označení úrovně	Úroveň	Popis úrovně
1	TLP:CLEAR	„Pouze pro oči a uši jednotlivých příjemců – osob, bez možnosti dalšího sdílení. Zdroje mohou použít klasifikaci TLP:RED, pokud s informacemi nelze efektivně nakládat bez významného rizika pro soukromí, reputaci nebo činnost zúčastněných organizací. Příjemci proto nesmějí sdílet informace označené TLP:RED s nikým dalším. Například informace označené TLP:RED získané na konkrétní schůzce jsou určeny výhradně osobám, které se této schůzky samy účastnily.“
2	TLP:GREEN	„Možnost sdílení omezena, příjemci mohou takto označené informace šířit pouze na základě zásady “need-to-know”3 v rámci své organizace a mezi její klienty. Povšimněte si, že TLP:AMBER+STRICT omezuje možnost sdílení pouze na organizaci samotnou. Zdroje mohou použít označení TLP:AMBER, pokud lze s informací efektivně nakládat pouze s další podporou, avšak případné sdílení

		informace mimo zúčastněné organizace s sebou nese riziko pro soukromí, reputaci nebo činnosti. Příjemci mohou sdílet informace označené TLP:AMBER se členy své vlastní organizace a jejími klienty, ale pouze na základě principu "need-to-know", aby zajistili ochranu své organizace, její klienty a zabránili případným dalším škodám. Poznámka: Pokud chce zdroj omezit sdílení pouze na samotnou organizaci, musí použít označení TLP:AMBER+STRICT."
3	TLP:AMBER	„Možnost sdílení omezena, příjemci mohou takto označené informace šířit v rámci své komunity. Zdroje mohou používat označení TLP:GREEN, pokud je informace užitečná pro zvýšení povědomí v jejich širší komunitě. Příjemci mohou sdílet informace označené TLP:GREEN s kolegy a partnerskými organizacemi v rámci své komunity, avšak nesmí k tomu využívat veřejně přístupné kanály. Informace označené TLP:GREEN nesmějí být sdíleny mimo komunitu. Poznámka: Pokud „komunita" není definována, jedná se o odbornou komunitu v oblasti kybernetické bezpečnosti/obrany."
4	TLP:RED	„Příjemci mohou takto označené informace šířit po světě, sdílení není nijak omezeno. Zdroje mohou používat označení TLP:CLEAR pro informace, s nimiž je spojeno minimální nebo žádné předvídatelné riziko zneužití, v souladu s relevantními pravidly a postupy pro zveřejňování. S přihlédnutím k standardním autorským právům mohou být informace označené TLP:CLEAR sdíleny bez omezení."

2.7 Management rizik informační bezpečnosti

Management rizik informační bezpečnosti je podrobně popsán v normě ČSN EN ISO/IEC 27005:2023. Následující kapitola je tvořena kombinací této normy a zbývajících norem řady 27000 jako ČSN EN ISO/IEC 27000:2020 a ČSN EN ISO/IEC 27001:2023 a ČSN EN ISO 27003:2018. V případě potřeby většího detailu je doporučeno využít napřímo zmíněné normy nad rámec následujícího popisu, který je zjednodušen na nejpodstatnější části. (18; 5; 17; 16)

Před samotným zpracováním a posouzením rizik by organizace měla ustanovit kontext, což zahrnuje aktivity jako identifikaci požadavků zainteresovaných stran, stanovení kritérií akceptace rizika, kritéria posuzování rizik a kritéria následků, pravděpodobnosti a úrovně rizika. Organizace by si měla zvolit vhodnou metodu, aby byla schopna zajistit konzistenci, srovnatelnost a odrážet realitu.

2.7.1 Proces posuzování rizik informační bezpečnosti

2.7.1.1 Obecné

Posuzování rizik se skládá z činností:

1. Identifikace rizik (vyhledávání rizik a jejich popis),
2. analýza rizik (pochopení daného rizika, určení jeho typu a úrovně rizika),
3. hodnocení rizik (porovnání výsledků z analýzy rizik vůči tomu, zdali je riziko akceptovatelné, nebo je nutné zvážit opatření).

Pomocí posuzování rizik lze stanovit priority rizik na základě parametrů pravděpodobnosti, následků a dalších zvolených.

2.7.1.2 Identifikace rizik informační bezpečnosti

Identifikace rizik je prvotním krokem v oblasti posuzování rizik a jedná se primárně o vyhledávání a popisování rizik. Rizika by měla být strukturovaná a popsaná takovým způsobem, aby šla efektivně řídit. Zároveň může docházet k iteracím a postupným detailnějším rozpadům, pokud je to vyžadováno situací a následující analýzou.

Není pevně stanoven přístup, jak organizace mají tuto činnost splnit, ale nejčastěji využívané jsou přístupy založené na událostech, nebo založené na aktivech.

Přístup založený na událostech je principem způsob identifikace na základě analýzy událostí a jejich následků. Využívají se konzultace s vedením organizace k učení klíčových rizik a jejich dopadů. Tento přístup umožňuje pracovat s obecnými a strategickými scénáři, aniž by bylo nutné identifikovat podrobně jednotlivá aktiva.

Přístup založený na aktivech identifikuje rizika skrze aktiva a jejich zranitelností a možných hrozeb. Aktiva jsou posuzována z pohledu jejich hodnoty pro organizaci. Tento přístup umožňuje přesnější identifikaci specifických rizik a cílená opatření, aby došlo k minimalizaci těchto rizik.

Přístupy jsou rozdílné v tom, že v jednom případě analýza začíná na úrovni obecných a strategických scénářů a popřípadě do většího detailu, kdežto v druhém případě začíná na detailní úrovni jednotlivých aktiv až ke scénářům.

K rizikům mají být přiřazeni vlastníci aktiv, což mohou být vedení společnosti, vedoucí oddělení, vlastníci aktiv a podobně. Tito vlastníci jsou za riziko zodpovědní a mají pravomoc řídit rizika, která vlastní.

2.7.1.3 Analýza rizik informační bezpečnosti

Cílem analýzou rizik je určit úroveň rizik. Primárně se zaměřuje na rizika a opatření, která při správném řízení snižují pravděpodobnost, že by negativně působily na cíle organizace. Posuzování rizik může být náročné na čas.

Základními technikami pro analýzu rizik jsou:

- Kvalitativní, kde je využita stupnice slovních atributů (např. nízké, střední, vysoké),
- semikvantitativní, kde je využita stupnice s číselnými hodnotami v kombinaci se slovními atributy
- kvantitativní, kde je využita stupnice s číselnými hodnotami (např. peněžní náklady).

V rámci analýzy musí být krok posouzení následků při nezachování důvěrnosti, integrity a dostupnosti informací. Tato analýza musí být provedena vždy, pokud dojde ke změně ve vytvořeném seznamu rizik, nebo jsou zjištěny další změny, které mají na tuto oblast vliv. V rámci analýzy následků se určují následky, pokud by došlo ke ztrátě důvěrnosti, integrity nebo dostupnosti informací, což obvykle odhaduje vlastník na

základě odhadu ztrát při narušeném provozu, závažnosti následku a nákladů na obnovení do původního stavu.

Pravděpodobnost výskytu je analyzována kvalitativně nebo kvantitativně. Při posuzování je třeba uvažovat, jak často se zdroje vyskytují a jak snadno je lze využít. Pravděpodobnost se určuje na základě zkušenosti, statistiky, přírodních katastrof, známé zranitelnosti a stávajících opatření. Vzhledem k tomu, že určení pravděpodobnosti nemusí být přesné, protože nemusel problém historicky vůbec nastat, z důvodu zjednodušeného pohledu a zkreslením posuzovatele. Pro zvýšení přesnosti odhadu pravděpodobnosti lze využít nástroje jako týmové posuzování, externí zdroje a podobně. U pravděpodobnosti je vhodné uvědomění, že některé události mohou být provázány a vzájemně závislé (např. pokud událost B může nastat pouze pokud nastane událost A, nelze posuzovat pravděpodobnosti odděleně).

Úroveň rizika může být určena různými způsoby, jednou z variant může být kombinace následku a pravděpodobnosti.

2.7.1.4 Hodnocení rizik informační bezpečnosti

Hodnocení rizik se provádí nad seznamem rizik s přiřazenými hodnotami úrovní. Pro hodnocení se využívá kritéria akceptace rizika. Pokud riziko je akceptovatelné, nemusí se provádět další činnosti, v případě neakceptovatelného rizika se stanovuje priorita pro opatření. Úroveň rizika lze ověřit mezi vlastníky rizik a specialisty.

Při získaném seznamu neakceptovatelných rizik organizace provádí prioritizaci, podle které budou nastavena opatření. Tyto priority mají zohledňovat nejen vstup posuzovatelů, ale cíle organizace a požadavky zainteresovaných stran.

2.7.2 Proces ošetření rizika bezpečnosti

Proces ošetření rizika bezpečnosti je navazujícím krokem hodnocení rizik a zahrnuje činnosti jako výběr vhodných možností ošetření rizika, určení opatření nezbytných, porovnání opatření vůči opatřením v normě a vypracování prohlášení o aplikovatelnosti a plánu ošetření.

Variant pro ošetření rizik je několik:

- Akceptace rizika pomocí rozhodnutí pravomocných osob.

- Vyhnutí se riziku vypnutím nebo utlumením činnosti, která riziko způsobuje.
- Modifikace rizik snížením její pravděpodobnosti nebo snížením závažnosti následku.
- Sdílení rizika mezi více stran externě nebo interně (např. pomocí pojištění).

Pro výběr opatření se využívá příloha A z normy, ve které jsou popsány jednotlivá opatření, jejich náležitosti a význam. Organizace určuje všechny nezbytná opatření, provádí zdůvodnění jejich výběru, stav zavedení a porovnává všechna stanovená opatření s opatřeními v normě. Pokud není využito některé opatření, musí zdůvodnit, proč nedošlo k zavedení daného opatření.

Prohlášení o aplikovatelnosti je klíčový dokument v oblasti ISMS shrnující body v ošetření rizik – nezbytná opatření, důvod výběru, stav zavedení a zdůvodnění vyloučených opatření vůči normě, pokud taková jsou. Dokument slouží jako formální zápis způsobu řízení rizik ze strany organizace a lze jej využít pro komunikaci s třetími stranami jako auditoři, zákazníky a podobně.

Oblast plánu ošetření rizik je rozdělena do dvou částí – formulace plánu a jeho schválení. Hlavním účelem plánu je zajištění, aby nalezené neakceptovatelné rizik bylo sníženo na akceptovatelnou úroveň. Plány mohou být jednotlivé nebo společné, musí dohromady pokrývat veškerá neakceptovatelná rizika. Uspořádání plánů může být na základě umístění informací, podle aktiv nebo podle událostí. Při tvorbě plánu musí být jasná priorita a naléhavost ošetření, rozmezí mezi implementací a provoz, odpovědné osoby, jednotlivé činnosti, stav zavádění, termín a další náležitosti potřebné k sestavení plánu. Plán musí být akceptován ze strany odpovědných osob.

3 ANALÝZA SOUČASNÉ SITUACE

Analýza současné situace je prováděna vůči bodům v ČSN EN ISO/IEC 27001:2023. Celá práce záměrně nekonkretizuje společnost, pro kterou bude analýza stavu a návrh změn prováděn, aby nedošlo k nechtěnému prozrazení interních informací. Informace jsou zobecněny do takové úrovně, aby byla i přes nekonkrétnost užitečná pro čtenáře jako možná metodika zvýšení úrovně kybernetické bezpečnosti v organizaci.

3.1 Představení společnosti

Tato práce se zaměřuje na společnost střední velikosti podnikající v oblasti analýzy, vývoje, testování a údržbu software na zakázku. Jedná se primárně o webové portály a aplikace, informační systémy, transakční systémy a další.

Společnost má v aktuální době tři pobočky v různých městech České republiky.

3.2 Kontext organizace

3.2.1 Porozumění organizace a jejího kontextu

Organizace nemá formálně identifikované externí a interní aspekty pro oblast ISMS.

3.2.2 Porozumění potřebám a očekáváním zainteresovaných stran

Organizace nemá formálně identifikované externí a interní zainteresované strany a jejich požadavky pro oblast ISMS.

3.2.3 Stanovení rozsahu systému managementu informační bezpečnosti

Organizace se v oblasti ISMS zaměřuje na celou společnost, ale nemá formálně ustanoven rozsah ISMS, neexistuje organizační rozsah, hranice a rozhraní, neexistuje rozsah, hranice a rozhraní informačních a komunikačních technologií a fyzický rozsah, hranice a rozhraní.

3.2.4 Systém managementu informační bezpečnosti

Organizace nemá formálně ustanovený systém řízení informační bezpečnosti.

3.3 Vůdčí role

3.3.1 Vůdčí role a závazek

Organizace má vyhrazeného bezpečnostního manažera, který zároveň plní funkci CTO a v případě potřeby využívá některé další role v organizaci. Přesná specifikace této role není nastavena.

3.3.2 Politika

Organizace má vytvořenou bezpečnostní politiku s vlastní stanovenou strukturou. Bezpečnostní politika obsahuje, proč je bezpečnost dat pro organizaci důležitá, na jaká data se zaměřuje a několik pravidel a opatření, jak využívat svá zařízení a jak se v organizaci chovat z pohledu bezpečnosti dat. Mezi tyto opatření a pravidla patří například pravidla nastavených hesel, nastavení přístupů, politika čistého stolu a další.

3.3.3 Organizační role, odpovědnosti a pravomoci

Organizace má pro většinu potřebných odpovědností vyhrazeného bezpečnostního manažera. Není stanovena odpovědnost ohledně podávání zpráv o výkonnosti a zlepšování ISMS a pro audit ISMS.

3.4 Plánování

3.4.1 Činnosti zaměřené na rizika a příležitosti

3.4.1.1 Obecně

Formálně neexistuje sepsaný postup hodnocení rizik. Existují 4 týmy v oblasti realizace, obchodu, lidských zdrojů a finance. Tým identifikuje rizika za svoji oblast, rizikům je přiřazena hodnota mezi 1-5 na základě závažnosti rizika. Pro tyto rizika je stanoven akční krok. V některých případech je přidělena osoba. Termín a finance nejsou stanoveny. Organizace provádí SWOT jednou ročně v rámci strategického plánování.

3.4.1.2 Posuzování rizik bezpečnosti informací

Organizace neaplikuje formální posuzování rizik a jejich kritéria, pro tento účel není nastavena metodika. Rizika nejsou identifikována a posuzována ve spojení ztráty

důvěrnosti, integrity a dostupnosti informací. Vzhledem k absenci identifikovaných rizik nejsou přiděleni vlastníci. Analýza rizik nevyužívá atributy dopadu a pravděpodobnosti a z toho plynoucího celkového rizika. Dokumentované informace v této oblasti nejsou zajištěny.

3.4.1.3 Ošetření rizik bezpečnosti informací

Organizace má aplikovaná některá opatření na základě vlastního uvážení, formálně neodpovídají identifikovaným a analyzovaným rizikům, vzhledem k jejich absenci. Stanovená opatření má za zodpovědnost bezpečnostní manažer. Opatření nemají Prohlášení o aplikovatelnosti a vlastníky.

3.4.2 Cíle informační bezpečnosti a plánování jejich dosažení

Cíle ISMS jsou částečně stanoveny, organizace dává důraz na důležitost bezpečnosti informací zaměstnancům. Formálně nejsou cíle stanoveny v plném rozsahu, chybí zdroje, termín a způsob vyhodnocení.

3.4.3 Plánování změn

Z pohledu oblasti ISMS není stanoven proces plánovaných změn.

3.5 Podpora

3.5.1 Zdroje

Organizace je připravena alokovat dostatek zdrojů podle potřeby. Není formálně stanovené, jaké zdroje budou nutné pro splnění cílů.

3.5.2 Kompetence

Organizace má stanovenou organizační kompetenci (manažera kybernetické bezpečnosti), nevyžaduje konkrétní vzdělání, školení nebo zkušenosti v oblasti kybernetické bezpečnosti. Dokumentovaná informace jako důkaz o kompetenci neexistuje.

3.5.3 Povědomí

Směrnice pro vzdělání zaměstnanců je nastavena, pro testování zaměstnanců se využívá dedikovaná aplikace s vyhodnocením (zaměstnanec musí provést kontrolní otázky na 100

% úspěšnost, aby mohl být kurz dokončen). Existuje pravidelné školení na bezpečný vývoj na základě OWASP TOP 10. Formálně není nastaveno servisní okno pro aktualizaci bezpečnostní politiky.

3.5.4 Komunikace

Komunikační rámec je definován primárně pro interní komunikaci, včetně vyjmenovaných konkrétních nástrojů. Pro externí komunikaci jsou definovány některé nástroje z oblasti lidských zdrojů a obchodu.

3.6 Dokumentované informace

3.6.1 Obecně

Řízení dokumentů není dostatečně popsáno. Organizace definuje strukturu a styl psaní dokumentů jako základní přehled zaměstnancům.

3.6.2 Vytváření a aktualizace

Identifikace a popis organizace určuje pomocí záznamu ve využívaném softwarovém řešení. Formát je stanoven pomocí příručky, jakým způsobem psát dokumentaci. Schvalování dokumentů není formálně popsáno.

3.6.3 Řízení dokumentovaných informací

Dokumentace je řízená pomocí přístupů pro jednotlivé uživatele nebo skupiny uživatelů. Dokumenty určené pouze pro určitou skupinu zaměstnanců jsou omezené pomocí restrikcí. Potřebné dokumenty pro obecné fungování ve společnosti jsou pro zaměstnance dostupné. Chybí popis ohledně řízení změn a uchovávání a likvidace. Klasifikace informací není určena a nevyužívá se, tudíž nemusí být zajištěna dostatečná ochrana (např. v případě fyzických dokumentů).

3.7 Provozování

3.7.1 Plánování a řízení provozu

Z důvodu absence některých bodů z kapitoly plánování není zajištěno dostatečné řízení procesů pomocí stanovených kritérií. Dokumentované informace v této oblasti neexistují.

3.7.2 Posuzování rizik informační bezpečnosti

Z důvodu absence identifikovaných rizik neexistuje pravidelný interval údržby rizik.

3.7.3 Ošetření rizik informační bezpečnosti

Z důvodu absence identifikovaných a analyzovaných rizik neexistuje odpovídající ošetření, včetně dokumentace.

3.8 Hodnocení výkonnosti

3.8.1 Monitorování, měření, analýza a hodnocení

Organizace má nastaveny některé metriky, k vyhodnocení dochází jednou měsíčně. Metriky nejsou specificky nastavované pro oblast ISMS. Formálně není tento proces nastaven a není zavedený dostatečný detail dokumentovaných informací.

3.8.2 Interní audit

3.8.2.1 Obecně

Interní audit není zaveden.

3.8.2.2 Program interního auditu

Interní audit není zaveden, program neexistuje.

3.8.3 Přezkoumání vedením

3.8.3.1 Obecně

K přezkoumání ISMS ze strany vedení v nedochází v pravidelných intervalech, ale pouze nárazově v případě řešení nové implementace v této oblasti.

3.8.3.2 Vstupy pro přezkoumání vedením

Při přezkoumání nejsou zohledněny některé vstupy doporučené normou, protože nejsou formálně zpracovávány a řízeny, a tudíž nemohou být posuzovány. Při setkávání se pracuje se vstupy jako stav a nové požadavky zákazníků.

3.8.3.3 Výsledky z přezkoumání vedením

Výsledky vedení jsou zahrnuty do strategických cílů, pokud jsou nutné. Z důvodu absence splnění předchozích bodů neprobíhá formálně a neexistuje dokumentovaná informace těchto výsledků.

3.9 Zlepšování a udržování

3.9.1 Neustálé zlepšování

Organizace přináší návrhy na zlepšení v pravidelném intervalu na vyhrazené schůzce. Tyto vstupy jsou jak z interních podnětů, tak externích (např. požadavky zákazníků) a mohou být zahrnuty do strategických cílů.

3.9.2 Neshody a nápravná opatření

Organizace má popsaný proces v případě bezpečnostního incidentu v rámci bezpečnostní politiky. Zaměstnanci jsou školeni každý rok skrze tomu určený software. Dokumentace se zaznamenává.

3.10 Celkové zhodnocení

V rámci celkového zhodnocení je shrnuta GAP analýza stávajícího stavu vůči normě ČSN EN ISO/IEC 27001:2023.

V GAP analýze se pracuje se čtyřmi stavy, které definují míru splnění požadavků normy. Stavy jsou zjednodušeny a je nutné prozkoumat, proč je daný požadavek označen příslušným stavem. V některých případech může jít o případ, kdy je oblast v organizaci definována, ale i přesto nesplňuje požadavky normy, v některých může být ve stavu rozpracovaném. Stavy jsou detailně popsány v tabulce.

Tabulka 2: Stupně stavů
(Zdroj: Vlastní zpracování)

Stav	Definice
Neexistující	Daný požadavek není vůbec nastaven a je potřeba jej nově sestrojit.

Rozpracováno	Daný požadavek není v rámci organizace ukotven a stále je v rozpracovaném stavu, nelze jej prohlásit za odpovídající normě.
Definováno	Daný požadavek je z organizace ukončený a definovaný. Má ale nedostatky z pohledu formality nebo obsahu vůči normě a je nutné jej doplnit o chybějící body.
Vyhovující	Daný požadavek je vyhovující normě a není třeba u něj dělat změny.

Pro vyšší přehlednost jsou požadavky shrnuty do tabulky, včetně určené stavu. Tato tabulka bude sloužit jako vstup pro návrh řešení a úprav.

Tabulka 3: Požadavky normy a vyhodnocení
(Zdroj: Vlastní zpracování)

Označení kapitoly	Oblast	Požadavek	Aktuální stav
4.1	Kontext organizace	Porozumění organizaci a jejímu kontextu	Neexistující
4.2		Porozumění potřebám a očekáváním zainteresovaných stran	Neexistující
4.3		Stanovení rozsahu systému managementu informační bezpečnosti	Neexistující
4.4		Systém managementu informační bezpečnosti	Neexistující
5.1	Vůdčí role	Vůdčí role a závazek	Definováno
5.2		Politika	Definováno
5.3		Role, odpovědnosti a pravomoci v rámci organizace	Definováno
6.1.1	Plánování	Činnosti zaměřené na rizika a příležitosti – obecně	Definováno

6.1.2		Činnosti zaměřené na rizika a příležitosti – posuzování rizik informační bezpečnosti	Rozpracováno
6.1.3		Činnosti zaměřené na rizika a příležitosti – ošetření rizik informační bezpečnosti	Rozpracováno
6.2		Cíle informační bezpečnosti a plánování jejich dosažení	Rozpracováno
6.3		Plánování změn	Rozpracováno
7.1	Podpora	Zdroje	Rozpracováno
7.2		Kompetence	Rozpracováno
7.3		Povědomí	Definováno
7.4		Komunikace	Definováno
7.5.1		Dokumentované informace – obecně	Neexistující
7.5.2		Dokumentované informace – vytváření a aktualizace	Rozpracováno
7.5.3		Dokumentované informace – řízení dokumentovaných informací	Rozpracováno
8.1	Provozování	Plánování a řízení provozu	Neexistující
8.2		Posuzování rizik informační bezpečnosti	Neexistující
8.3		Ošetření rizik informační bezpečnosti	Neexistující
9.1	Hodnocení výkonnosti	Monitorování, měření, analýza a hodnocení	Definováno
9.2.1		Interní audit – obecně	Neexistující
9.2.2		Interní audit – program interního auditu	Neexistující
9.3.1		Přezkoumání vedením – obecně	Definováno

9.3.2		Přezkoumání vedením – vstupy pro přezkoumání vedením	Definováno
9.3.3		Přezkoumání vedením – výsledky z přezkoumání vedením	Definováno
10.1	Zlepšování	Neustálé zlepšování	Rozpracováno
10.2		Neshody a nápravná opatření	Definováno

Graf 1: Stav požadavků vůči normě
(Zdroj: Vlastní zpracování)

Organizace nevyhovuje jediným bodem normě, ale u většiny bodů existuje určitá definice nebo rozpracovanost. Některé body by měly být přesunuty do vyhovujícího stavu po formální nápravě dokumentů, některé body budou vyžadovat aktivní práci ze strany kompetentních osob k doplnění nalezených nedostatků. Organizace si uvědomuje důležitost ISMS a má ochotu napravit tyto nedostatky, pokud v průběhu zpracování nebude překážka ve formě nutnosti vynaložit velké množství financí nebo jiných zdrojů, které by mohly negativně ovlivnit chod organizace.

4 VLASTNÍ NÁVRHY

Vlastní návrh je prováděn vůči bodům v ČSN EN ISO/IEC 27001:2023 a doplněn o chybějící oblasti ze závěrů ze stávajícího stavu ve společnosti. Vlastní návrh rozebírá jednotlivé body zvolené normy a navrhuje možnost jejich nastavení v organizaci, což by mělo vést k zvýšení kybernetické bezpečnosti a bezpečnosti informací. Některá doporučení a body mohou být vypuštěny vzhledem k požadavkům manažera společnosti, pokud by mohla znamenat přílišnou náročnost. Informace ohledně aktuálního stavu jsou zprostředkovány od finančního ředitele společnosti, a tudíž jsou získané informace považovány automaticky za validní a správné. V rámci této práce nejsou využity další speciální nástroje a metodiky pro získání informací od zaměstnanců, vedení a dalších subjektů. Zároveň se jedná o návrh a organizace by měla provést revizi a případně úpravu v případě změny podmínek a kontextu. Některé části mohou být zpracovány detailně, v některých částech může být pouze kladen povel, jak by měla organizace zareagovat.

4.1 Kontext organizace

4.1.1 Porozumění organizace a jejího kontextu

4.1.1.1 Firemní kultura

Firemní kultura organizace je založena na svobodě a týmovém duchu. Z pohledu ISMS je důležité, že vedení firmy neupřednostňuje striktní hierarchii a pravidla při fungování firmy, ale spíše podporuje a vybízí zaměstnance k vlastním iniciativám, myšlenkám a uvědomování si vlastní zodpovědnosti.

4.1.1.2 Politiky a směrnice

Organizace má stanovenou vlastní bezpečnostní politiku, kde specifikuje, jak by se zaměstnanci měli chovat, jak by měli mít nastavená vlastní zařízení a proč je kybernetická bezpečnost důležitá.

4.1.1.3 Zavedené normy a legislativa

Organizace není certifikována na žádné normy, ale usiluje o získání certifikátů ISO 9001 a ISO 14001. Podle vedení společnosti není organizace vázána k dodržování zákona

o kybernetické bezpečnosti nebo jinými zákony, směrnicemi nebo nařízeními specificky pro oblast kybernetické bezpečnosti, vzhledem k tomu, že nespadá mezi regulované subjekty.

4.1.1.4 Cíle

Cílem organizace v oblasti ISMS je minimálně postupovat metodicky adekvátně, ideálně tento postup mít v souladu s odpovídající normou nebo obecně uznávanou knihovnou.

4.1.1.5 Informační systémy

Informační systémy jsou používané v cloudovém prostředí. Firma využívá nástroje jako ERP, CRM, nástroje pro dokumentaci, nástroje pro zaznamenávání úkolů a jejich kontrolu. Podrobný popis využívaných nástrojů se plánuje v analýze aktiv.

4.1.2 Porozumění potřebám a očekáváním zainteresovaných stran

Zainteresované strany jsou podstatné, protože jejich požadavky mění průběh a cíle ISMS. Získání požadavků a informací vychází od finančního ředitele společnosti, vzhledem znalosti jednotlivých zainteresovaných stran a jejich požadavků. Přehled je zahrnut v tabulce.

Tabulka 4: Zainteresované strany
(Zdroj: Vlastní zpracování)

Oblast	Zainteresovaná strana	Požadavek
Interní	Vedení společnosti	Vedení společnosti má v zájmu, aby dodávaný software splňoval co nejvyšší možnou kvalitu s ohledem na rozpočet a žádost zákazníka. V rámci fungování ISMS ve firmě chce mít minimálně metodicky v pořádku. Soulad s příslušnými normami by zlepšilo průběh výběrovými řízeními, ale není nutné, pokud by to výrazně ovlivnilo firemní procesy. Vedení nechce svazovat své zaměstnance komplexními procesy, postupy a příliš striktními pravidly v souladu

		s firemní kulturou, pokud to nebude vyžadovat jiná důležitá zainteresovaná strana.
	Běžní zaměstnanci	Běžní zaměstnanci nemají speciální požadavky, chtějí maximálně udržet pohodlnost používání.
	Provozní tým	Provozní tým nemá speciální požadavky, chtějí maximálně udržet pohodlnost používání.
Externí	Stát a regulační orgány	Organizace svojí činností nespadá pod regulaci dle zákona o kybernetické bezpečnosti.
	Zákazníci	Zákazníci jsou odběratelé jednotlivých softwarových produktů vytvořené na míru. Organizace nemá informaci o konkrétních požadavcích na řízení bezpečnosti, ale je připravena reagovat na nové požadavky.
	Dodavatelé	Dodavatelé nemají speciální požadavky pro oblast ISMS.
	Konkurence	Konkurence by neměla mít přístup k důvěrným informacím společnosti jako strategické plány apod.

Pro sestavování ISMS je podstatná informace, že chce být organizace v souladu s obecně uznávanou metodikou, která by mohla pomoci při výběrových řízeních nových projektů. Zároveň je kladen maximální důraz na zachování pohodlnosti pro uživatele v organizaci, i za cenu vyššího rizika.

4.1.3 Stanovení rozsahu systému managementu informační bezpečnosti

Práce se zaměřuje na celou společnost a na všechny její pobočky. Cílem je pracovat se společností jako celkem, nejde o vymezení na konkrétní pobočky, oddělení nebo část organizační struktury. Vizí organizace je přiblížit se celosvětově uznávaným standardům, pokud by chtěla být v budoucnu podstoupena certifikaci.

4.1.3.1 Organizační rozsah

V rámci organizačního rozsahu se zaměřuje na všechny procesy a s tím spojená oddělení. Jedná se o procesy (zjednodušeně):

- Strategické plánování,
- obchod a marketing,
- návrh a vývoj software,
- řízení projektů,
- finance,
- lidské zdroje,
- správa kanceláří.

Z těchto oddělení budou získávány informace, pokud budou v rámci postupu normy potřebné.

4.1.3.2 Rozsah informačních technologií

Architektura informačních technologií není v práci podrobně popisována, protože by mohlo dojít k vyzrazení know-how společnosti. Z obecného hlediska je zaměřeno na celý rozsah informační technologií, z čehož budou plynout následující analýzy. Nejedná se o vyčlenění pouze některých služeb.

Datová infrastruktura a síťová konektivita je poskytována externím dodavatelem, včetně údržby a pravidelné aktualizace. Poskytovatel je vázán pomocí SLA k nápomoci při výpadku sítě a odstranění problémů ve striktně domluvených časech.

Organizace využívá prakticky pro veškeré služby cloudové služby. Cloudové služby jsou poskytovány od kvalitních a verifikovaných poskytovatelů. Všechna data jsou ukládána na serverech v Evropské unii, čímž automaticky přebírají povinnosti a regulatorní požadavky vydávané EU. Poskytovatelé jsou vázáni pomocí SLA.

4.1.3.3 Fyzický rozsah

Pobočka A

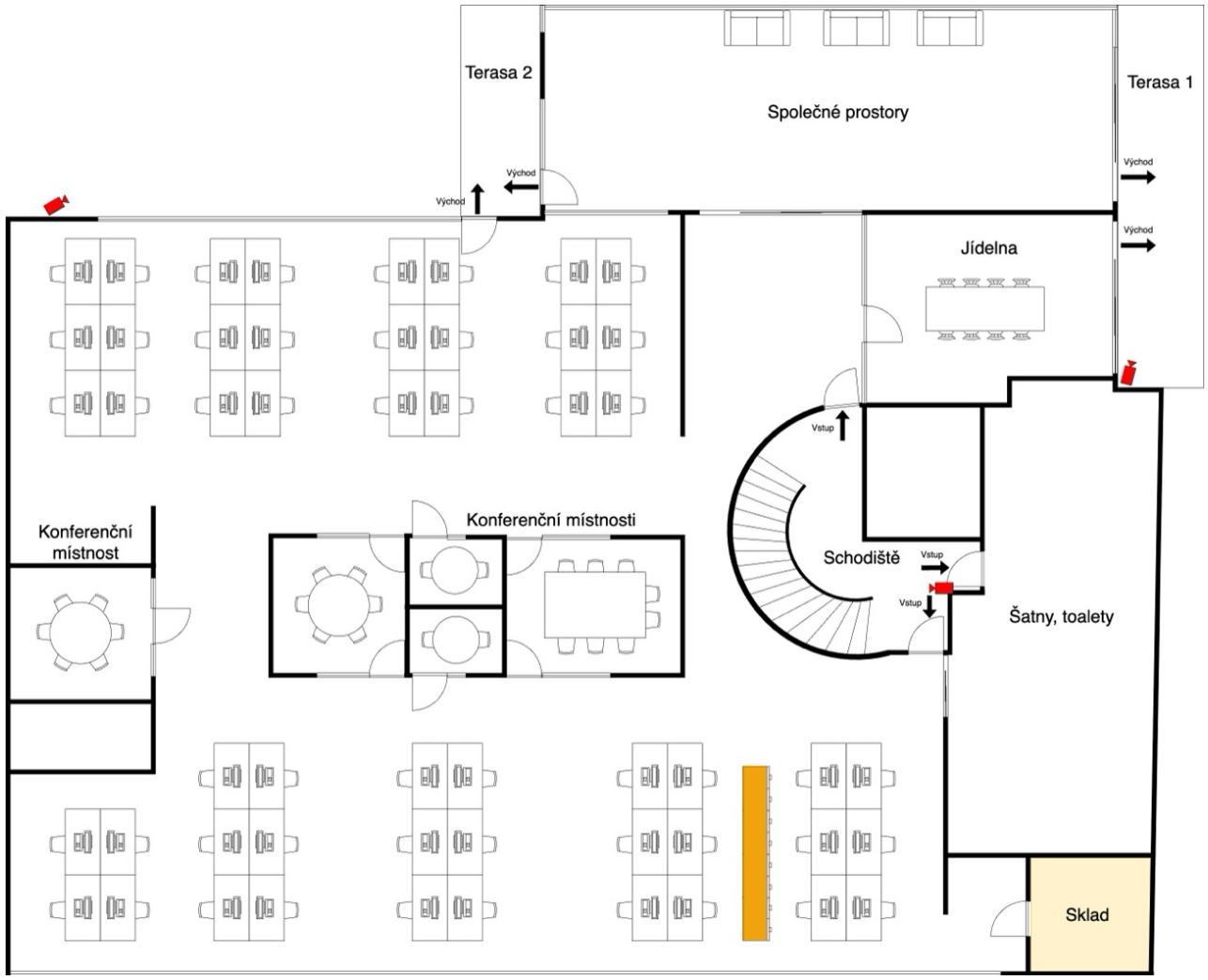
Pobočka A je primární pobočkou společnosti. Je součástí polyfunkčního domu. Pobočka je zabezpečena ostrahou budovy, která monitoruje 24/7 celou budovu a má možnost zavolat služby IZS v případě potřeby. Veškerá kancelář je pokryta pohybovými čidly, což v případě výskytu cizí osoby, při zapnutém alarmu, spustí poplach. Prostor kanceláře je vybaven třemi přístupovými vchody s autentizací pomocí osobního čipu. Dále je vybaven čtyřmi východy, které vedou na terasu sloužící jako sekundární možnost odchodu z budovy, ovšem nelze jej využít pro příchod pomocí čipu. Vchody a východy jsou zaznamenávány kamerami pronajímatele.

Pobočka B

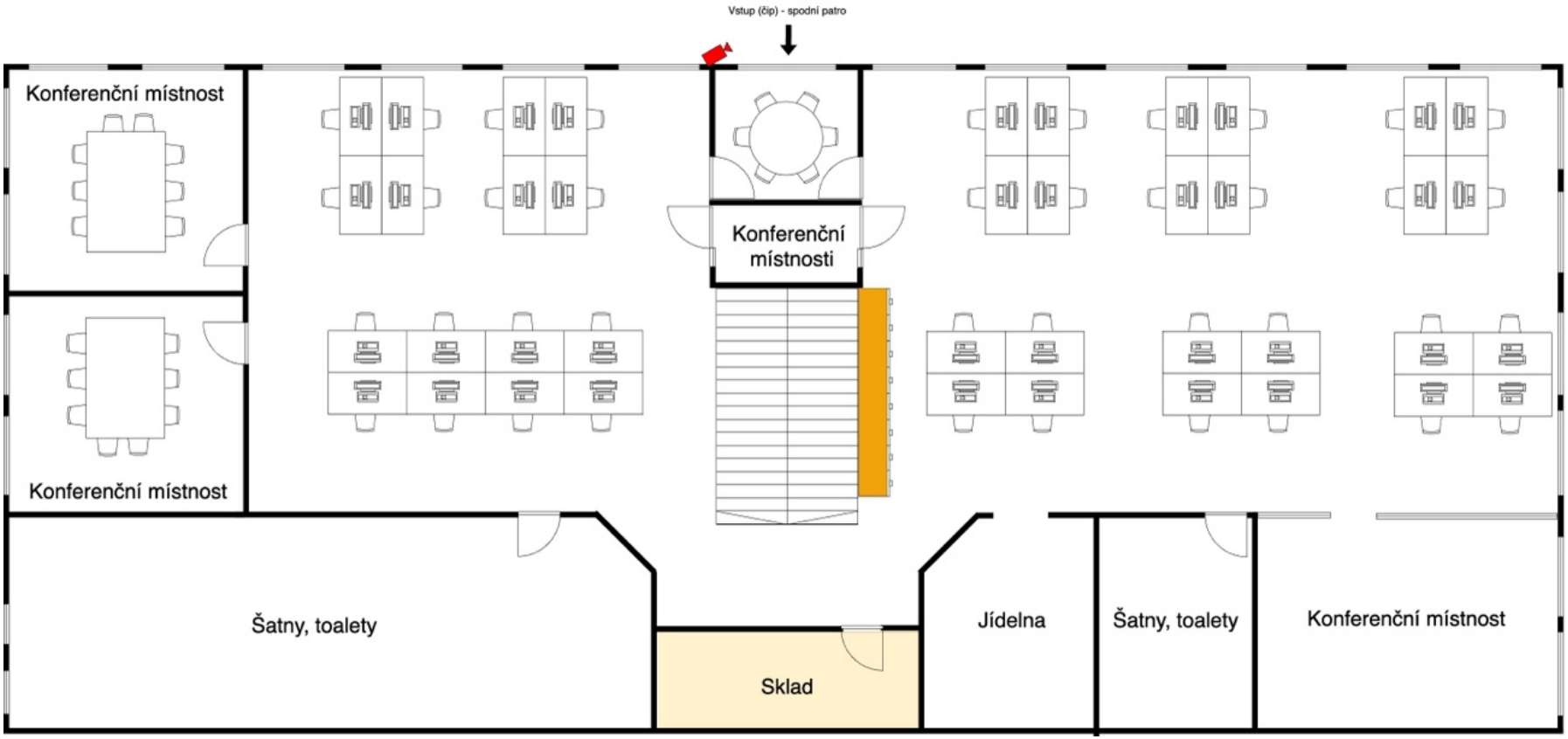
Pobočka B se nachází v 2. NP. Pobočka je zabezpečena pomocí alarmu. Veškerá kancelář je pokryta pohybovými čidly, což v případě výskytu cizí osoby, při zapnutém alarmu, spustí poplach. Prostor kanceláře je vybaven jedním přístupovým vchodem s autentizací pomocí osobního čipu. Vchod je zaznamenáván kamerou pronajímatele.

Pobočka C

Pobočka C se nachází v 6.-8. NP a je součástí polyfunkčního domu. Prostor kanceláře je vybaven jedním přístupovým vchodem, zároveň kvůli komplexnosti budovy musí zaměstnanec využít další předchozí 2 vchody zabezpečené pomocí osobního čipu. Vchod je zaznamenáván kamerou pronajímatele.



Obrázek 1: Půdorys pobočky A
(Zdroj: Vlastní zpracování)



Obrázek 2: Půdorys pobočky B
(Zdroj: Vlastní zpracování)

Obrázek 3: Půdorys pobočky C
(Zdroj: Vlastní zpracování)

4.1.4 Systém managementu informační bezpečnosti

Rozsah systému managementu informační bezpečnosti je definován v předchozích bodech a bude zahrnut v další analýze a pokynech.

4.2 Vůdčí role

4.2.1 Vůdčí role a závazek

Organizace musí vymezit vůdčí role a zavázat se k tomu, že bude poskytovat dostatečnou podporu ISMS. Organizace je připravena a ochotna nadále podporovat důležitost ISMS a vyhradit si případné peněžní prostředky na její zlepšení, včetně alokace osoby, která bude dohlížet na plnění normy v průběhu času a postupnému zlepšování podle měnících se podmínek.

4.2.2 Politika

Bezpečnostní politika obsahuje pokyny, jakým způsobem se mají zaměstnanci chovat a vyzdvihuje důležitost kybernetické bezpečnosti. Kompletní znění bezpečnostní politiky není v této práci uvedeno, v rámci návrhů budou vytvořena opatření, která by se měly do bezpečnostní politiky zahrnout.

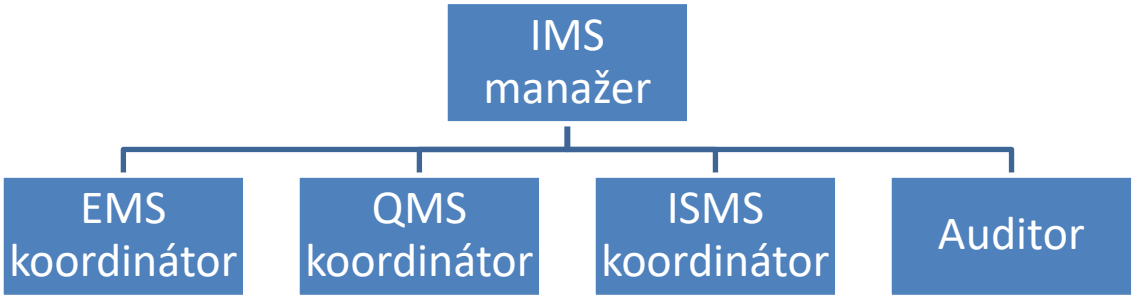
4.2.3 Organizační role, odpovědnosti a pravomoci

Organizace má pro účely kybernetické bezpečnosti zvoleného manažera kybernetické bezpečnosti. Pro soulad s normou je doporučeno provést revizi této role a přizpůsobit ji novým požadavkům normy z pohledu alokace času, kompetencí a odpovídajícímu vzdělání nebo proškolení.

Organizace plánuje zavedení norem ISO 9001 a ISO 14001, kde je vyžadováno určení a definice potřebných rolí. Vzhledem k tomuto plánu je doporučeno vytvořit nový tým, jehož úkolem bude zajišťovat soulad těchto norem jako celku, včetně nových nastavení v rámci ISMS. Pro případnou budoucí certifikaci dle normy ISO 27001 bude tým kompletně nastaven dle potřeb.

Navrhovaný tým je nazván „Compliance tým“ a obsažené role jsou IMS manažer, EMS koordinátor, QMS koordinátor, ISMS koordinátor a auditor. IMS manažer, EMS a QMS koordinátor a jejich detailní popis není součástí této práce. IMS manažer je osoba z vedení

společnosti a sdílení informací k ní je považováno jako předání vedení. Struktura tohoto týmu by mohla být následující, dle obrázku níže.



Obrázek 4: Organizační struktura Compliance týmu
(Zdroj: Vlastní zpracování)

Při tvorbě této struktury je inspirováno definicí rolí z vyhlášky o kybernetické bezpečnosti, kde jsou přesně definovány požadavky na jednotlivé role. Jedná se o role manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti, auditora kybernetické bezpečnosti a garanta aktiva. Organizace chce jmenovat pouze roli manažera kybernetické bezpečnosti jako ISMS koordinátora, jehož cílem bude udržovat správný stav ISMS. Garanti aktiv se budou určovat u jednotlivých aktiv a auditor se zvolí jako třetí strana pro zajištění nezávislosti a objektivity. (3)

Tabulka 5: ISMS koordinátor popis role
(Zdroj: Vlastní zpracování)

Název role:	ISMS koordinátor
Nadřízená role:	IMS manažer
Zodpovědnosti:	Spoluvytváří bezpečnostní politiku ISMS. Spolupracuje a podílí se na implementaci, provozu a údržbě ISMS. Vyjadřuje se k dopadům změn na úroveň bezpečnosti v ISMS. Spolupracuje a provádí hodnocení a analýzy rizik. Spolupracuje na tvorbě programů pro řízení rizik. Vytváří nebo spolupracuje na tvorbě jednotlivých bezpečnostních politik v rámci ISMS.

	Provádí monitorování a měření jednotlivých ukazatelů procesů v ISMS. Odpovídá za vypracování podkladů pro zprávu o stavu ISMS. Zajišťuje provedení interních auditů v ISMS. Zajišťuje provádění bezpečnostních testů v IT infrastruktuře organizace.
Kvalifikace:	Detailní znalost procesů managementu informační bezpečnosti dle ISO 27001. Znalost managementu rizik v ISMS. Znalost procesů managementu kontinuity v ISMS. Znalost rozhraní se všemi procesy organizace. Znalost bezpečnostní politiky a jejích požadavků na procesy a prvky infrastruktury.
Školení:	Školení v oblasti managementu ISMS dle ISO 27001 v min. rozsahu 1 dne, zakončeno osvědčením.
Další podmínky:	-

4.3 Plánování

4.3.1 Činnosti zaměřené na rizika a příležitosti

4.3.1.1 Obecně

Podle normy má organizace plánovat takovým způsobem, aby bylo zajištěno, že ISMS dosáhne nastavených cílů, předcházelo se nebo snižovalo výskytu nežádoucích účinků a docházelo k neustálému zlepšování. Pro tento účel bude zahájeno posuzování rizik na opakované frekvenci, včetně analýzy a nastavení opatření.

4.3.1.2 Posuzování rizik bezpečnosti informací

Ačkoliv má organizace zavedená některá opatření, nemá zajištěné metodicky konzistentní posuzování rizik bezpečnosti informací, a tudíž nelze říct, že opatření jsou ve všech případech adekvátní a správně provedená. Posuzování rizik je základní aktivitou, která je prerekvizitou pro všechny následující činnosti.

Stanovení kritérií

Prvním bodem je výběr a stanovení stupnic kritérií přijetí rizik a kritérií pro posuzování rizik informační bezpečnosti. Norma nestanovuje povinnost využít přesně určené stupnice. Lze využít přílohy v normě, která tyto stupnice doporučuje k využití. Vzhledem k novému nastavení stupnic v rámci organizace jsou vybrány a převzaty stupnice tvořeny Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) v rámci vyhlášky o kybernetické bezpečnosti. Toto rozhodnutí bylo učiněno z následujících důvodů:

1. V případě identifikace organizace v rámci režimu povinností (možné i jako dodavatel v rámci dodavatelského řetězce při zákaznících podléhajících těmto povinnostem) v zákoně o kybernetické bezpečnosti bude organizace mít povinnost se řídit zmíněným zákonem a příslušnou vyhláškou. Výběr stupnic z vyhlášky zjednoduší případné audity ze strany NÚKIB nebo samotného zákazníka.
2. NÚKIB nabízí podrobný postup při zpracování identifikace a analýzy rizik, který může být organizací využit a zajišťuje odborný postup a dostatečný detail oproti normě, kdy nevyužitím těchto stupnic by musel být postup přepracován, z čehož plyne riziko chyby.
3. Stupnice jsou součástí vzorců pro výpočet celkové rizika, ze kterého budou vycházet plány pro opatření. Využitím jiných stupnic by tento výpočet musel být přepracován, z čehož plyne riziko chyby.
4. Bude dodržen obecně známý postup a z dlouhodobého pohledu bude zajištěna jednodušší předávka na nově najaté osoby v rámci ISMS.

Při přes využití stupnic od NÚKIB mohou být definice mírně upraveny pro kontext organizace, která v aktuální době nepodléhá povinnostem podle zákona o kybernetické bezpečnosti. (22)

Stupnice jsou popsány v příslušných tabulkách a budou využívány pro následující kroky identifikace a vyhodnocení rizik.

Tabulka 6: Úrovně důvěrnosti
(Zdroj: Vlastní zpracování dle: (22))

Úroveň	Důvěrnost
1- Nízká	Aktiva lze běžně sdělovat a publikovat. Zveřejnění těchto informací nepředstavuje žádné riziko pro firmu. V případě sdílení takového aktiva s třetími stranami je použito klasifikace Veřejné.
2- Střední	Aktiva nejsou veřejně přístupná a tvoří know-how organizace. Externí přístup k aktivům je na základě podepsaného NDA. V případě sdílení takového aktiva s třetími stranami je použito klasifikace Interní.
3- Vysoká	Aktiva jsou citlivými firemními údaji a daty, které jsou pouze pro omezenou skupinu zaměstnanců na základě podepsaného NDA. V případě sdílení takového aktiva s třetími stranami je použito klasifikace Důvěrné.
4- Kritická	Aktiva jsou citlivými firemními údaji a daty, nejsou veřejné přístupná (například strategické obchodní tajemství, zvláštní kategorie osobních údajů). V případě sdílení takového aktiva s třetími stranami je použito klasifikace Přísně důvěrné.

Tabulka 7: Úrovně integrity
(Zdroj: Vlastní zpracování dle (22))

Úroveň	Integrita
1- Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje společnost.
2- Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození firmy a může se projevit méně závažnými dopady na primární aktiva.

3- Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození firmy s podstatnými dopady na primární aktiva.
4- Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození firmy s přímými a velmi vážnými dopady na primární aktiva.

Tabulka 8: Úrovně dostupnosti
(Zdroj: Vlastní zpracování dle (22))

Úroveň	**Dostupnost**
1- Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).
2- Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne (8 hodin), dlouhodobější výpadek vede k možnému ohrožení firmy.
3- Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení firmy. Aktiva jsou považována za velmi důležitá.
4- Kritická	Narušení dostupnosti aktiva není přípustné, a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení firmy. Aktiva jsou považována za kritická.

Tabulka 9: Úrovně hrozby
(Zdroj: Vlastní zpracování dle (22))

Úroveň	**Hrozba**
1- Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
2- Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozmezí od 1 roku do 5 let.
3- Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozmezí od 1 měsíce do 1 roku.

4- Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Tabulka 10: Úrovně zranitelnost
(Zdroj: Vlastní zpracování dle (22))

Úroveň	Zranitelnost
1- Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
2- Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
3- Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
4- Kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Tabulka 11: Úrovně rizika
(Zdroj: Vlastní zpracování dle (22))

Úroveň rizika	Hranice míry rizika	Popis
Nízká	1–16	Riziko je považováno za přijatelné – akceptovatelné.

Střední	17–31	Riziko může být sníženo méně náročnými opatřeními, nebo je akceptovatelné při vyšší náročnosti opatření.
Vysoká	32–47	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.
Kritická	48–64	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

Tabulka 12: Úrovně rizika výpočet
(Zdroj: Vlastní zpracování dle (22))

	Hrozba x zranitelnost									
	-	**1**	**2**	**3**	**4**	**6**	**8**	**9**	**12**	**16**
Hodnota dopadu aktiva	**1**	1	2	3	4	6	8	9	12	16
	2	2	4	6	8	12	16	18	24	32
	3	3	6	9	12	18	24	27	36	48
	4	4	8	12	16	24	32	36	48	64

Vzorec pro výpočet rizika je následující:

$$Riziko = dopad \times hrozba \times zranitelnost$$

Dopad je určen jako maximální hodnota z atributů důvěrnosti, integrity nebo dostupnosti u daného aktiva. (22)

Identifikace rizik

Identifikaci rizik lze provést dvěma způsoby:

1. Přístup identifikace skrze události, nebo
2. přístup identifikace skrze aktiva, hrozby a zranitelnosti.

Vzhledem k preferenci v organizaci je využitý přístup identifikace skrze aktiva a jejich hrozby a zranitelnosti.

Pro samotnou identifikaci se využívá brainstormingové metody v týmu složen z následujících rolí:

- Finanční ředitel (CFO),
- IT manažer,
- ředitel lidských zdrojů (HR manažer),
- obchodní ředitel (CSO),
- marketingový ředitel,
- bezpečnostní manažer.

Organizace počítá s postupným přidáváním a odebíráním aktiv v čase. Pro základní strukturu jsou aktiva rozdělena na následující oblasti:

- Obecný software,
- fyzická aktiva,
- provoz,
- interní systémy,
- finance,
- obchod,
- marketing,
- HR a backoffice,
- návrh a vývoj software,
- řízení projektů.

Tato struktura umožňuje základní kategorizaci, zjednodušuje přehled a práci s aktivy, a zároveň snižuje pravděpodobnost opomenutí některého z aktiv.

Aktiva jsou seskupena ve formátu tabulky, která umožňuje jednoduchou manipulaci s daty a dostatečnou nastavitelnost. V rámci seznamu aktiv se pracuje s následující strukturou:

Tabulka 13: Popis tabulky seznam aktiv
(Zdroj: Vlastní zpracování)

Sloupec	Popis sloupce
Oblast aktiva	Oblast, do kterého aktivum spadá (viz. dříve zmíněné oblasti).
Název aktiva	Stručný název aktiva.
Typ aktiva	Konkrétnější kategorizace aktiva, kterého je typu. Definice typů je popsána v jiné tabulce.
Druh aktiva	Primární nebo podpůrný druh aktiva.
Vlastník/Garant aktiva	Zodpovědná pozice nebo tým za dané aktivum.
Důvěrnost	Číselná hodnota dle stupnice o důvěrnosti.
Integrita	Číselná hodnota dle stupnice o integritě.
Dostupnost	Číselná hodnota dle stupnice o dostupnosti.
Hodnota aktiva	Číselná hodnota odvozena jako nejvyšší číselná hodnota důvěrnosti, integrity nebo dostupnosti.

Základní rozdělení druhu aktiva vychází z definice normy a vyhlášky o kybernetickém zákoně. Typ aktiva je upraven na základě požadavku organizace pro lepší strukturu. Druh, typ a popis aktiva je uveden v následující tabulce:

Tabulka 14: Popis druhů a typů aktiva
(Zdroj: Vlastní zpracování)

Druh aktiva	Typ aktiva	Popis typu aktiva
Primární	Informace primární	Informace, které se využívají pro naplnění regulovaných služeb. Příklad: Zdrojové kódy aplikací, infrastruktura, dokumentace apod.

	Služba regulovaná	Služba, která je pod regulací (SLA) ze strany zákazníka a souvisí s předmětem podnikání organizace. Příklad: Post implementační podpora dodávaných produktů
Podpůrné	Informace podpůrná	Informace, které se využívají pro podpůrná aktiva. Příklad: Informace o zaměstnancích
	Hardware	Hardware využívaný pro náplň práce. Příklad: Firemní notebook
	Síť	Síť využívaná pro náplň práce. Příklad: Router
	Software	Software využívaný pro náplň práce, který není pod SLA (typicky instalován přímo na zařízení). Příklad: IDE pro vývoj
	Služba dodávaná	Dodávaná služba, která není pod regulací (SLA) ze strany zákazníka. Příklad: Konzultační služby
	Služba odebíraná	Odebíraná služba, která je pod regulací (SLA) ze strany organizace vůči dodavateli. Příklad: Kancelářský balíček
	Objekty	Fyzické objekty využívané pro náplň práce. Příklad: Kancelář
	Zaměstnanci	Zaměstnanci organizace nebo externí dodavatelé potřebné pro naplnění služeb organizace. Příklad: Vedení společnosti

Jednotlivá aktiva jsou zapsána ve formátu tabulky. Z důvodu anonymizace jsou aktiva zobecněna, aby nedošlo k prozrazení konkrétně používaných nástrojů v organizaci.

Tabulka 15: Seznam aktiv
(Zdroj: Vlastní zpracování)

Oblast aktiva	Název aktiva	Typ aktiva	Druh aktiva	Vlastník/Garant aktiva	Hodnota aktiva			
				Jméno nebo funkce	Důvěrnost	Integrita	Dostupnost	Celková
Obecný software	Software dokumentace	Služba odebíraná	Podpůrné	IT manažer	1	1	4	**4**
	Data v Softwaru dokumentace	Informace primární	Primární	CEO	4	4	4	**4**
	Nástroj pro spolupráci	Služba odebíraná	Podpůrné	IT manažer	1	1	3	**3**
	Data v Nástroji pro spolupráci	Informace primární	Primární	CEO	4	4	3	**4**
	Komunikační platforma	Služba odebíraná	Podpůrné	IT manažer	1	1	2	**2**
	Data v Komunikační platformě	Informace podpůrná	Podpůrné	CEO	2	1	2	**2**
	Kancelářský balík	Služba odebíraná	Podpůrné	IT manažer	1	1	2	**2**
	Data v Kancelářském balíku	Informace podpůrná	Podpůrné	CEO	2	2	2	**2**

Fyzická aktiva	Kanceláře	Objekty	Podpůrné	BackOffice Specialist	2	2	1	**2**
	Mobilní telefony	Hardware	Podpůrné	IT manažer	3	3	4	**4**
	Notebook s MacOS	Hardware	Podpůrné	IT manažer	1	1	3	**3**
	Notebook s jiným OS	Hardware	Podpůrné	IT manažer	1	1	3	**3**
	Osobní počítače	Hardware	Podpůrné	IT manažer	1	1	1	**1**
	Data v počítačích	Informace podpůrná	Podpůrné	IT manažer	4	4	4	**4**
	Tiskárny	Hardware	Podpůrné	IT manažer	1	1	2	**2**
	Aktivní prvky infrastruktury	Síť	Podpůrné	IT manažer	2	3	3	**3**
	Poskytovatel internetu	Síť	Podpůrné	IT manažer	2	3	3	**3**
	Příslušenství	Hardware	Podpůrné	IT manažer	2	1	2	**2**
	Počítače v místnostech	Hardware	Podpůrné	IT manažer	2	1	2	**2**
Provoz	Administrační konzole	Služba odebíraná	Podpůrné	IT manažer	3	4	4	**4**
	Nástroj pro správu incidentů	Služba odebíraná	Podpůrné	IT manažer	3	4	4	**4**
	Správa domén a webhostingu	Služba odebíraná	Podpůrné	IT manažer	3	4	4	**4**

	Monitorovací systém	Služba odebíraná	Podpůrné	IT manažer	2	2	4	**4**
	Data v Monitorovacím systému	Informace podpůrná	Podpůrné	IT manažer	2	2	4	**4**
	Správa identit	Služba odebíraná	Podpůrné	IT manažer	3	4	4	**4**
	Nástroj pro školení	Služba odebíraná	Podpůrné	IT manažer	2	2	1	**2**
Interní systémy	Vlastní software	Software	Podpůrné	IT manažer	2	2	1	**2**
	HR software	Software	Podpůrné	IT manažer	4	2	2	**4**
Finance	ERP systém	Služba odebíraná	Podpůrné	CFO	2	1	3	**3**
	Data v ERP systému	Informace podpůrná	Podpůrné	CFO	4	3	3	**4**
	Kartotéka smluv	Informace podpůrná	Podpůrné	BackOffice Specialist	3	3	3	**3**
	Archiv u poradce	Informace podpůrná	Podpůrné	CFO	2	2	2	**2**
	Daňový poradce	Služba odebíraná	Podpůrné	CFO	2	1	2	**2**

	Data na serveru poradce	Informace podpůrná	Podpůrné	CFO	3	2	1	**3**
	Účetní auditor	Služba odebíraná	Podpůrné	CFO	2	1	1	**2**
	Audit IMS	Služba odebíraná	Podpůrné	CFO	3	3	2	**3**
	Certifikační orgán IMS	Služba odebíraná	Podpůrné	CFO	2	2	1	**2**
Obchod	CRM systém	Služba odebíraná	Podpůrné	CSO	1	1	3	**3**
	Data v CRM systému	Informace podpůrná	Podpůrné	CSO	3	3	3	**3**
	Nástroj pro správu	Služba odebíraná	Podpůrné	CSO	1	1	1	**1**
	Firemní značka	Informace podpůrná	Podpůrné	CSO	1	4	4	**4**
Marketing	Data na sítích	Informace podpůrná	Podpůrné	CEO	1	2	1	**2**
	Webové stránky	Informace podpůrná	Podpůrné	CEO	1	3	1	**3**

	Reklamní platforma 1	Služba odebíraná	Podpůrné	CEO	1	1	1	**1**
	Reklamní platforma 2	Služba odebíraná	Podpůrné	CEO	1	1	1	**1**
	Prodejní nástroj	Služba odebíraná	Podpůrné	CEO	1	1	1	**1**
	Nástroj pro nasazení	Služba odebíraná	Podpůrné	CEO	1	1	1	**1**
	Agentury	Služba odebíraná	Podpůrné	CEO	1	1	1	**1**
HR a backoffice	Nástroj pro nábor	Služba odebíraná	Podpůrné	HR manažer	1	1	3	**3**
	Data v náborovém nástroji	Informace podpůrná	Podpůrné	HR manažer	4	3	3	**4**
	Software mzdy	Software	Podpůrné	HR manažer	1	1	2	**1**
	Data v Softwaru mzdy	Informace podpůrná	Podpůrné	HR manažer	4	4	2	**4**
	Zaměstnanecké složky	Informace podpůrná	Podpůrné	HR manažer	3	3	1	**3**

	Nástroj daně	Služba odebíraná	Podpůrné	HR manažer	4	4	1	**4**
	Nástroj pro podpis dokumentů	Služba odebíraná	Podpůrné	HR manažer	4	4	1	**4**
	Nástroj pro správu aktiv	Služba odebíraná	Podpůrné	HR manažer	2	2	1	**2**
	Kniha jízd	Služba odebíraná	Podpůrné	HR manažer	2	2	1	**2**
Návrh a vývoj software	Data v repozitáři	Informace primární	Primární	Projekt manažer	2	4	3	**4**
	Kritické cloudové služby	Služba odebíraná	Podpůrné	IT manažer	2	4	4	**4**
	Obecné cloudové služby	Služba odebíraná	Podpůrné	IT manažer	2	1	1	**2**
	Poskytovatelé cloudu	Služba odebíraná	Podpůrné	IT manažer	2	4	4	**4**
	Vývojové prostředí	Software	Podpůrné	IT manažer	2	3	3	**3**
	Data a konfigurace produktů	Informace primární	Primární	Hlavní architekt	2	4	4	**4**

	Registr artefaktů	Služba odebíraná	Podpůrné	IT manažer	2	2	2	**2**
	Distribuční účty aplikací	Služba odebíraná	Podpůrné	IT manažer	2	2	2	**2**
	Automatizační nástroj	Služba odebíraná	Podpůrné	IT manažer	3	3	3	**3**
Řízení projektů	Pracovníci v provozním týmu	Zaměstnanci	Podpůrné	IT manažer	1	1	4	**4**
	Podpora nastaveného softwaru	Služba regulovaná	Primární	Projekt manažer	2	4	4	**4**
	Podpora vlastního softwaru	Služba regulovaná	Primární	IT manažer	2	4	4	**4**
	Podpora dodávaného softwaru	Služba regulovaná	Primární	IT manažer	2	4	4	**4**

Seznam aktiv a základní analýza dopadu jednotlivých aktiv dává základní přehled a určuje kritická aktiva. Dopad jsou prvním vstupem do vzorce vyhodnocování rizika, v následující části je posouzení aktiva na základě hrozeb a zranitelností.

Analýza a hodnocení rizik

Po identifikaci aktiv následuje analýza, která pracuje s možným následkem a pravděpodobností, že by se riziko realizovalo. Toto posouzení dává dohromady celkovou míru rizika a určuje prioritu zavádění případných opatření.

Za normálních okolností by bylo vhodné, aby byla zranitelnost a hrozba posuzována bez uvažování již zavedených bezpečnostních opatření. Vzhledem k náročnosti tohoto požadavku je proveden jiný postup. Náročnost vychází primárně z těžké představitelnosti posuzujících, protože jsou opatření nastavena v některých případech dlouhé časové období a zároveň některé z aktiv obsahují bezpečností opatření již zabudované při pořízení (příklad: nástroj pro dokumentaci, který obsahuje řízení přístupu jako první krok při nastavování nástroje). Z tohoto důvodu jsou prvně identifikována již dříve zavedena opatření pro každé aktivum a s tímto stavem je posuzována pravděpodobnost zranitelnosti a hrozby. Pro posuzování jsou vytvořeny seznamy hrozeb a zranitelností. Tyto seznamy slouží pro vyhodnocování a vybírá se u každé z aktiv pouze takové hrozby a zranitelnosti, které jsou adekvátní a souvisí s daným aktivem. Seznamy jsou vytvořeny na základě požadavku vedení v kombinaci vlastních návrhů, průvodce od NÚKIB a normy. (18; 22)

Seznam hrozeb:

- Zneužití identity.
- Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení.
- Zneužití nebo neoprávněná modifikace informací.
- Obcházení přihlašovacího loginu.
- Zneužití přístupových práv a účtů.
- Zneužití vzdáleného přístupu.
- Užívání programového vybavení v rozporu s licenčními podmínkami.
- Zavedení poškozujícího nebo poškozeného SW.

- Nedovolené použití, zneužití vnitřních prostředků, sabotáž.
- Cílený kybernetický útok, použití špionážních technik.
- Napadení elektronické komunikace (odposlech, modifikace, infiltrace).
- Poruchy komunikací.
- Chybné směrování síťové komunikace.
- Vložení škodlivého kódu, ransomware.
- Síťové útoky, SPAM.
- "Společenské inženýrství" - metoda ilegálního získávání informací.
- Zneužití zranitelností v informačním systému.
- Porucha EZS, přístupového systému.
- Poškození nebo selhání technického anebo programového vybavení.
- Technická závada síťové komponenty nebo síťové služby.
- Chyba systémového nebo síťového SW.
- Dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb.
- Nedodržení smluvního závazku ze strany dodavatele.
- Závislost na jediném dodavateli.
- Porucha klimatizace, UPS, dieselagregátu aj. podpůrných zařízení.
- Chyba, nefunkčnost aplikačního SW, ztráta databázové integrity, konzistence.
- Chyba, nefunkčnost služby emailové komunikace.
- Chyba/nefunkčnost informačního systému.
- Chyba operátora, administrátora HW, SW.
- Zaměstnanci s nedostatečnou odbornou úrovní znalostí.
- Chyba uživatele.
- Ztráta, odcizení nebo poškození aktiv ze strany vlastních zaměstnanců.
- Ztráta, odcizení nebo poškození aktiv ze strany cizích osob.
- Nesprávné nakládání s citlivými, klasifikovanými informacemi.
- Nedostupnost, nefunkčnost SW aplikace, prostředí.
- Nedodržovaní systémových pravidel, bezpečnostních pravidel.
- Ztráta databázové integrity, konzistence.
- Nedostatečná kapacita zdrojů.

- Náhlé snížení počtu pracovníků.
- Pochybení ze strany uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení.
- Narušení fyzické bezpečnosti.
- Ztráta informací, nemožnost obnovit data.
- Nemožnost obnovit data.
- Nemožnost číst šifrovaná data.
- Zneužití, ztráta vyměnitelných technických nosičů dat.
- Zpřístupnění nebo předání aktiv na základě žádosti státu.
- Požár.
- Poškození vodou nebo povodeň.
- Přírodní pohroma (blesk, vichřice).
- Terorismus.

Seznam zranitelností:

- Běžný uživatel se vydává za někoho jiného.
- Cizí osoba, pracovník smluvní organizace se vydává za někoho jiného.
- Nevhodná organizace uživatelských účtů.
- Nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit podezřelé činnost. Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností pracovníků.
- Dočasné volně přístupné účty.
- Nevhodné nastavení přístupových oprávnění.
- Nedovolené použití aplikace.
- Nedostatečné postupy a procesy pro detekování kybernetických bezpečnostních událostí a identifikování kybernetických bezpečnostních incidentů.
- Nevhodná funkční a bezpečnostní architektura, Nedostatečná ochrana aktiv.
- Nevhodná funkční a bezpečnostní architektura, nedostatečná údržba a profylaxe.
- Nevhodná bezpečnostní architektura.
- Neproškolený, nevycvičený uživatel.
- Opožděné anebo nedostatečné řešení zranitelnosti odhalených při skenování zranitelností a penetračním testování.

- Nedostatečná údržba a kontrola, zastaralost aktiv.
- Technická závada HW/SW zařízení.
- Nedostatečná údržba nebo zastaralost aktiv.
- Nevhodná bezpečnostní nebo funkční architektura.
- Chybějící monitorování smluvních závazků dodavatelů, nedostatky v řízení dodavatelů.
- Nevhodně nastavena funkční a bezpečnostní architektura.
- Nedostatečná údržba aktiv.
- Nedostatečná údržba a profylaxe, nevhodná funkční nebo bezpečnostní architektura.
- Nedostatečné bezpečnostní povědomí nebo proškolení, nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů.
- Nedostatečné bezpečnostní povědomí uživatelů, Chybějící pravidelné vzdělávání a zkušenosti.
- Nedostatečné bezpečnostní povědomí uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení.
- Nedostatečná ochrana aktiv, nedostatečná míra nezávislé kontroly.
- Nedostatečná ochrana aktiv, nedostatečná ochrana perimetru.
- Nedostatečně proškolení pracovníci, Nedostatečné stanovení bezpečnostních pravidel a postupů, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů.
- Testování SW s provozními daty nebo v provozním prostředí.
- Nedostatečné bezpečnostní povědomí, proškolení uživatelů, administrátorů, osob zastávajících bezpečnostní role, dodavatelů a vrcholného vedení.
- Nedostatečná údržba a kontroly.
- Nedostatek pracovníků s potřebnou odbornou úrovní znalostí.
- Nedostatek pracovníků s potřebnou odbornou úrovní znalostí, nevhodné pracovní podmínky.
- Nedostatečná nebo nevhodná dokumentace.
- Nedostatečné proškolení uživatelů/adminů, konzultantů atd.

- Nedostačená ochrana, zabezpečení perimetru, prostor (serverovna).
- Nedostatečné zálohování dat.
- Nedostatečné postupy pro obnovu dat.
- Nevhodná bezpečnostní architektura.
- Nedostatečné bezpečnostní povědomí uživatelů, Nedostatečné postupy zabezpečení aktiv.
- Zneužití státní moci pro přístup k aktivům.
- Nedostatečná ochrana perimetru, nedodržení předpisů, neopatrnost pracovníků.
- Nedostatečná ochrana perimetru.
- Nedostatečná ochrana nebo nevhodné umístění perimetru.

Příkladem vyhodnoceného aktiva bude reprezentovat aktivum „Data v Nástroji pro spolupráci“, což v při identifikaci dopadu má stupeň nejvyšší (stupeň 4). Aktivum bylo vyhodnoceno z 53 kombinací hrozeb a zranitelností adekvátnímu tomuto aktivu. Z vyhodnocení se vyskytly 3 kombinace hrozeb a zranitelností, které by mohly v dlouhodobém pohledu mít negativní dopady a měl by pro ně být vytvořen plán opatření. Při posuzování se pracovalo s již dříve zavedenými opatřeními, což jsou:

- Přístupová bezpečnost – přístup je řízen pomocí pracovních účtů přiřazených ke konkrétním uživatelům, které navíc podléhají více faktorovému zabezpečení. Veškeré účty jsou řízeny a spravovány administrátory provozního týmu a přístup je udělován v případě oprávněné potřeby.
- Externí sdílení – ve výchozím nastavení je omezený přístup pouze pro tvůrce souboru, pro sdílení dalším spolupracovníkům je nutný ruční zásah a nastavení buď konkrétních osob nebo sdílení pro celou organizaci.

V tabulce jsou výsledky pro 3 vybrané kombinace, včetně výpočtu celkového rizika ve stupni dlouhodobě neakceptovatelném (viz. tabulka s hodnotami rizika).

Tabulka 16: Příklad vyhodnoceného aktiva z pohledu hrozby a zranitelnosti
(Zdroj: Vlastní zpracování)

Hrozba / zranitelnost	Hrozba	Zranitelnost	Úroveň rizika
	(H)	(Z)	(R = D*H*Z)
Cílený kybernetický útok, použití špionážních technik. / Nedostatečné postupy a procesy pro detekování kybernetických bezpečnostních událostí a identifikování kybernetických bezpečnostních incidentů.	3	3	36
Ztráta informací, nemožnost obnovit data. / Nedostatečné zálohování dat.	2	4	32
Nemožnost obnovit data. / Nedostatečné postupy pro obnovu dat.	2	4	32

Nalezená rizika se pohybují ve 3. stupni závažnosti (vysoká) a nejsou tedy dlouhodobě přípustná. Žádné z rizik se u aktiv nepohybovala ve 4. stupni závažnosti, a tudíž není nutné dělat okamžitou nápravu. Tohoto stavu bylo dosaženo historickými opatřeními, které dostatečně snižují pravděpodobnost využití zranitelnosti.

4.3.1.3 Ošetření rizik bezpečnosti informací

Výběr opatření je vůči příloze A v normě ČSN EN ISO/IEC 27001:2023 a pro vypracování je použita norma ČSN EN ISO/IEC 27002:2023. Jedná se tedy o obecná opatření a nezahrnují další opatření oborová. Organizace dodává pro různé zákazníky v různých oborech a je možné přidání dalších oborových opatření, pokud bude potřebné. V normě je 93 opatření a pro tuto práci bude vybrána pouze část opatření, která jsou adekvátní k výstupům z analýzy rizik, popřípadě k předmětu podnikání. Může se zároveň jednat o shrnutí opatření zmíněné v předchozích kapitolách. (16; 4)

Z 93 opatření firma historicky zavedla několik opatření, konkrétní výpis není obsahem této práce. K těchto zavedeným opatřeným je doporučeno doplnit stávající o zmíněné body a v některých případech zavést následující opatření nově:

A.5.1 Politiky pro informační bezpečnost

Aktuálně politika pro informační bezpečnost je vytvořena. Vzhledem k tomu, že je primárním zdrojem informací o informační bezpečnosti, musí být doplněna o následující body opatření.

Za politiku zodpovídá ISMS koordinátor, včetně předání adekvátním příjemcům.

Aby politika pro informační bezpečnost plnila svoji roli, musí být komplexní a srozumitelná pro čtenáře, kteří se nepohybují v pojmech ISMS. Zároveň musí být zavedena dostatečná a jednoduchá dostupnost, aby byla co nejnižší bariéra pro uživatele si ji nastudovat.

Politika by měla obsahovat důraz na zodpovědnost jednotlivce a jeho možný efekt na celý zbytek organizace při nedostatečném dodržování.

Politika musí být školena, jak bylo popsáno v samostatné kapitole. Dostatečné přečtení a porozumění musí být ukončeno testem a v případě vysoké chybovosti je doporučena revize bezpečnostní politiky, zdali neobsahuje složité termíny nebo není jiným způsobem nesrozumitelná. Nedodržování by mělo být penalizováno, více popsáno v samostatném opatření.

A.5.2 Role a odpovědnosti v oblasti informační bezpečnosti

V kapitole vůdčích rolí byly zmíněny nově nastavené role a jejich povinností. S tímto musí být seznámené adekvátní zainteresované strany. Veškerá místa, kde jsou uvedeny původní role zajišťující informační bezpečnost, musí být aktualizovány na nový tým Compliance týmu. Compliance tým musí být schválen vedením společnosti a získat dostatečnou důvěru v oblasti ISMS.

Compliance tým musí udržovat pravidelné setkávání a snažit se o neustálé zlepšování. V případě změny osoby v tomto týmu musí být dodržena dostatečná kvalifikace a školení.

Komunikace o Compliance týmu musí být předána do společnosti takovým způsobem, aby zaměstnanci věděli, kdo se dané oblasti věnuje a využil tento tým na případné konzultace nebo doporučení na zlepšení.

Compliance tým musí být pravidelně proškolován a udržovat si dostatečné povědomí, aby mohl konat a nastavovat ISMS.

A.5.4 Odpovědnosti vedení

V práci byly zmíněné nové odpovědnosti vedení a jejich proaktivita a náklonnost při řešení ISMS. IMS manažer by měl tuto informaci mít s vedením potvrzenou a získat shodu na důležitosti ISMS. Vedení musí počítat s dostatečným vyhrazením času a zdrojů při řešení ošetření rizik nebo neshod. ISMS musí být vnímáno jako součást společnosti a být zaintegrováno do diskuzí strategie.

A.5.8 Informační bezpečnost v řízení projektů

Informační bezpečnost musí být zahrnuta v rámci řízení projektů. V případě existující metodiky pro řízení projektů by měla být zabudována bezpečnostní politika do jejího obsahu nebo na něj být odkazována.

Posouzení rizik by nemělo být pouze na úrovni organizace, ale i na úrovni jednotlivých projektů a specifického prostředí nimi vytvořený. Tudíž pro každý projekt v určité fázi zahájit identifikaci a posouzení rizik a provést výběr opatření, aby bylo zamezeno nežádoucím stavům, v horším případě bezpečnostním incidentům. Zodpovědnou osobou zde musí být projektový manažer s konzultací ISMS koordinátora. Bezpečnostní úkoly z tohoto posouzení musí být zahrnuty do projektového plánu a alokovat dostatečné množství zdrojů, aby došlo k zavedení vybraných opatření.

Na externích projektech může dojít k souběhu interních pracovníků, ale i nových dodavatelů a osob od zákazníka. Pro tyto osoby musí být předána bezpečnostní politika a poskytnuta konzultace.

Řízení změn musí zahrnovat ohled i na bezpečnost, tudíž zvážení dopadů na informační bezpečnost.

A.5.12 Klasifikace informací

Klasifikace informací je podstatným opatřením, jak přiřadit informaci do určité úrovni důvěrnosti a tím určuje způsob zacházení ze strany příjemců. Detailně byla popsána klasifikace v samostatné kapitole. Klasifikace informací by měla být zahrnuta v bezpečnostní politice.

A.5.13 Označování informací

Označení informací navazuje na klasifikaci informací, aby příjemce jasně rozpoznal výši klasifikace. Strategie označování informací je popsána v samostatné kapitole a měla by být zahrnuta v bezpečnostní politice.

Označení musí být technicky možné v případě softwarového řešení a vymyšlen proces, jakým způsobem klasifikace bude v softwarovém prostředí udržována. Pokud bude možné, je doporučeno zajistit dostatečné odlišení (např. pomocí barev).

V rámci interního auditu by mělo dojít k revizi označených dokumentů, zdali jsou splněny stanovené podmínky.

A.5.14 Předávání informací

Pravidla pro předávání informací (a jejich likvidaci a uchovávání) je popsáno v samostatné kapitole.

V rámci interního auditu by mělo dojít k revizi předávání dokumentů, zdali jsou splněny stanovené podmínky.

A.5.31 Zákonné, statutární, regulatorní a smluvní požadavky

Vzhledem k předmětu podnikání společnosti, kdy je dodáván software pro různé společnosti, může nastat situace dodávky pro společnost s povinností se řídit zákonem o kybernetické bezpečnosti, popřípadě dalších regulací. Je doporučeno, aby ISMS koordinátor zajistil průzkum zainteresovaných stran a jejich potenciálních regulatorních povinností a případně implementovat požadavky této regulace. Pro tento průzkum je doporučeno zvážení externích konzultantů se zaměřením na regulace.

Tento bod by měl být zohledněn v interním auditu, protože povinnost podle některých regulací může mít až vysoký dopad na společnost.

A.6.2 Podmínky pracovního poměru

Přestože má společnost nastavenou firemní kulturu a nechce své zaměstnance svazovat přísnými podmínkami, je doporučeno zavést do pracovní smlouvy část o tom, že mají povinnost dodržovat bezpečnostní politiku a její nedodržování může vést z peněžnímu nebo jinému trestu. Tímto opatřením a zdůrazněním důležitosti ISMS může být způsobena vyšší pozornost při práci s informacemi ze strany zaměstnanců.

Povinnosti z bezpečnostní politiky by měly být konkrétní a vymahatelné, může jít o detailnější popisy jako zacházení s přidělením zařízením a podobně.

Kromě negativní motivace může být zvážena pozitivní motivaci, kdy aktivním přispíváním může být poskytnuta určitá odměna – jako vzdělávání ostatních pracovníků, nahlašování novinek z oblasti ISMS a další.

A.8.1 Koncová zařízení uživatele

Navzdory svobodnější firemní kultuře je doporučeno zavést správu koncového zařízení. Správa koncových zařízení umožňuje omezit instalaci nežádoucího softwaru, omezit některé části systému, vzdálené zablokování, vymazání nebo uzamčení, analýzu chování uživatelů apod.

Vzhledem k možnosti zachování systému BYOD musí být striktně popsána pravidla, za jakých podmínek mohou být vlastní zařízení využívána a zdůrazněna preference využívat přidělená zařízení.

Ke koncovým zařízením musí být nastavena pravidla v oblasti šifrování disku, ukládání dat přímo na zařízení a jejich záloha, nastavený antivirový software, podmínky hesla, pravidelná aktualizace software a další.

Je doporučena namátková kontrola koncových zařízení uživatelů a kontrola těchto podmínek. Pří častých neshodách je doporučeno zpřísnit opatření.

A.8.7 Ochrana před škodlivým softwarem

Základní ochranou vůči škodlivému software je mít opatřený a zapnutý antivirový software a firewall.

V případě operačního systému MacOS je doporučeno doplnit do bezpečnostní politiky povinnost mít aktivní Firewall, zapnutou funkci FileVault (šifrování souborů) a zapnuté

automatické bezpečnostní aktualizace. Antivirová ochrana je součástí MacOS zvaná XProtect. V případě potřeby může být posouzeno zavedení dalšího nástroje třetí strany. (23)

Pro operační systém Windows je doporučeno do bezpečnostní politiky zahrnout povinnost mít aktivní Firewall Windows Defender, zapnutou funkci BitLocker (šifrování disku) a povolené automatické aktualizace systému Windows Update, které zahrnují i bezpečnostní záplaty a aktualizace služby Microsoft Defender Antivirus (zabudovaná antivirová ochrana). V potřeby může být posouzeno zavedení dalšího nástroje třetí strany. (24; 25)

Zároveň je doporučeno provést analýzu používaných zařízení zaměstnanců a zvážit další ochranu, pokud bude podezření na nedostatečně adekvátní zabezpečení (např. u mobilních zařízení nebo jiných operačních systémů).

A.8.13 Zálohování informací

Veškerá data se vyskytují v cloudovém prostředí od kvalitních dodavatelů. Konkrétní nástroje nejsou v této práci zmíněny, a proto nelze stanovit specifické opatření a postup zálohy pro vybrané nástroje. Je doporučeno, aby ISMS koordinátor provedl analýzu a komunikaci s dodavateli, jakým způsobem jsou data chráněna, jaké jsou možnosti dodatečného zálohování a jaké je postup pro případnou obnovu dat.

Pro jistotu organizace by měl poskytovatel cloudové služby dodat dokumentaci o způsobu zálohování a obnovení dat, včetně zaručení pomocí SLA. Pro činnost obnovení dat je doporučeno stanovit zodpovědnou osobu, která zajistí komunikaci s poskytovatelem a informování vedení společnosti o průběhu zálohování a obnovy dat (osobou může být ISMS koordinátor). Je doporučeno provést testování zálohy a obnovy dat.

V případě nedostatečné služby záloh a obnovy je doporučeno zvážit zapojení dalšího poskytovatele s možností zálohovat data.

Vstupy do prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti je dokument obsahující nezbytná opatření, zdůvodnění jejich zařazení a porovnání vůči zavaděných opatření vůči opatřením v normě a zdůvodnění vyloučení jakéhokoli z nich. V této kapitole není vypracováno prohlášení o aplikovatelnosti jako celek, ale pouze shrnuté vstupy do tohoto významného

dokumentu. Dokument je důležitým vstupem pro vedení, Compliance tým a případný audit.

Nezbytnými opatřeními jsou opatření zmíněna výše. Důvodem zavedení opatření je pokrytí aktiv s dlouhodobě nepřípustným nebo nepřípustným rizikem. Označení těchto aktiv vychází z předchozího provedení analýzy rizik. Výpis opatření je následující:

- A.5.1 Politiky pro informační bezpečnost
- A.5.2 Role a odpovědnosti v oblasti informační bezpečnosti
- A.5.4 Odpovědnosti vedení
- A.5.8 Informační bezpečnost v řízení projektů
- A.5.12 Klasifikace informací
- A.5.13 Označování informací
- A.5.14 Předávání informací
- A.5.31 Zákonné, statutární, regulatorní a smluvní požadavky
- A.6.2 Podmínky pracovního poměru
- A.8.1 Koncová zařízení uživatele
- A.8.7 Ochrana před škodlivým softwarem
- A.8.13 Zálohování informací

Detailní plán implementace v této práci není vypracován, protože nebylo možné získat dostatek vstupů ohledně rozpočtů, alokaci odborníků a časovém prostoru. Tento plán musí být vypracován pro každé zaváděné opatření.

4.3.2 Cíle informační bezpečnosti a plánování jejich dosažení

Cíle informační bezpečnosti musí organizace provést vzhledem k situaci v dané době.

Z pohledu této práce jsou doporučeny vstupy do cílů související s předchozím vypracováním. Cíle by měly v konečné definici splňovat metodu SMART. Následující cíle budou spíše doporučením, které musí být do SMART podoby upraveny.

- Soulad vůči normě ČSN EN ISO/IEC 27001:2023 v rozsahu celé společnosti.
- Zavedena vybraná opatření a jejich vyhodnocení.
- Ustanovena role ISMS koordinátora v rámci Compliance týmu a komunikace této role všem potřebným stranám.

4.3.3 Plánování změn

V případě potřeby provádět změny v ISMS je nutné provést změnu plánovaně. Pro tento účel je doporučeno, aby ISMS koordinátor pro každou změnu vytvořil dokumentovanou informaci. Náležitostmi v tomto dokumentu musí být minimálně důvod změny, potřebné zdroje, časové ohraničení a dopadová analýza na zbytek ISMS zavedením této změny. Další informace závisí na dané změně, měl by být zajištěn záznam o změně.

4.4 Podpora

4.4.1 Zdroje

Zdroje mohou být různé velikosti na základě rozhodnutí organizace a z toho důvodu nejsou v této práci konkrétně rozpracovány.

Při jmenování ISMS koordinátora bude mít organizace dostupnou osobu pro veškeré záležitosti spojeny s ISMS. Při jakékoli potřebě alokovat další zdroje je doporučeno, aby ISMS koordinátor předložil potřebné prostředky a důvod jejich potřeby. Zdroje by měly být zhotoveny jednotlivě na separátní potřeby (např. potřebné zdroje pro zavedení konkrétního opatření).

Vedení společnosti musí být připraveno na uvolnění zdrojů, ať už časových, tak finančních.

4.4.2 Kompetence

V rámci kompetence je nastaven samostatný Compliance tým, jehož úkolem bude zajistit shodu s normami, popřípadě dalšími požadavky určené vedením společnosti. V této práci je popsána role ISMS koordinátor, včetně potřebné kvalifikace a školení. Je žádoucí, aby pro ISMS koordinátora existovalo někde dostupné osvědčení o kvalifikaci. Doporučuje se alespoň jednou za rok zopakování těchto školení minimálně formou samostudia. Doporučuje se mít normy neustále k dispozici v online nebo papírové podobě a využívat je při zpracovávání ISMS a případné nejistotě. V rámci role je doporučeno v minimálně roční frekvenci sledovat změnu legislativy na úrovni České republiky a Evropské unie a provést dopadovou analýzu při zjištění nových povinností v oblasti ISMS, která by mohla mít dopad na organizaci v jejím kontextu.

Doporučuje se vyhledání kompetentního externího auditora pro možnost konzultací a provedení interního auditu před audity od certifikačního orgánu.

ČSN online

Jako nástrojem pro nahlížení do norem lze využít ČSN online, což je platforma od České agentury pro standardizaci. Tento nástroj umožňuje nahlížet do veškerých přeložených norem. Poplatek za uživatele na rok činí 2000 Kč za rok bez možnosti tisku, což v případě používání na zařízení by mělo dostatečně plnit účel. V případě potřeby tisku existují licence umožňující tisk. (15; 26)

4.4.3 Povědomí

Není nutné všechny zaměstnance školit stejným způsobem. Je doporučeno vytvořit matici SAE, uživatelé rozdělit do samostatných skupin a pro tyto skupiny vytvořit samostatné školení.

Jednotlivé skupiny:

- Vedení společnosti,
- Compliance tým,
- běžní zaměstnanci,
- dodavatelé,
- zákazníci.

Všichni zaměstnanci a aktivně zapojení dodavatelé by měli prostudovat bezpečnostní politiku a být otestováni. V aktuálním stavu testování probíhá pomocí softwarového řešení, tudíž je prokazatelné absolvování. Toto testování je doporučeno zanechat v plném rozsahu. Při vysoké chybovosti je doporučena revize kontrolních otázek a případně jejich upravení na srozumitelnější nebo úpravu bezpečnostní politiky, aby byla pochopitelná pro všechny čtenáře. Testování musí být provedeno minimálně jednou ročně nebo při zásadních změnách opatření, technologií s vlivem na ISMS nebo bezpečnostním incidentu.

Tabulka 17: Požadavky na povědomí skupin
(Zdroj: Vlastní zpracování)

Skupina	Požadavek
Vedení společností	Musí být v souladu s nastavením ISMS, podporovat neustálé zlepšování a mít k němu plnou důvěru a přesvědčení. Při nedostatečné důvěře systému může nastat moment demotivace ostatních zaměstnanců a znehodnocení významnosti ISMS. Testování v tomto případě není vyžadováno, ale při plánování strategických cílů a plánování by mělo být zajištěno zahrnutí ISMS. Zodpovědnost této aktivity může náležet roli IMS manažera s podporou ISMS koordinátora.
Compliance tým	Compliance tým je zásadní pro udržování ISMS v plné kvalitě vůči vybrané metodice. ISMS koordinátorovi náleží zodpovědnosti za správnost a je nutné školení alespoň jednou ročně, ideálně zakončeno osvědčením. Více informací je popsáno v předchozí kapitole Kompetence. Zodpovědnost náleží IMS manažerovi.
Běžní zaměstnanci	Nejsou vyžadovány vyšší vědomosti mimo základní školení. Zodpovědnost náleží ISMS koordinátorovi.
Dodavatelé	Musí být provedeno školení v nutné míře pro dodávku, která může být specifická a nemusí vyžadovat plný rozsah školení. O míře rozhoduje projektový manažer za podpory ISMS koordinátor.
Zákazníci	Musí být provedeno školení v nutné míře pro dodávku, která může být specifická a nemusí vyžadovat plný rozsah školení. O míře rozhoduje projektový manažer za podpory ISMS koordinátor.

Navzdory správně nastavenému školení zaměstnanců a jejich testování může docházet k nedodržování pravidel a je nutné zdůraznit následky, pokud by nedodržování

bezpečnostní politiky vedlo k bezpečnostní události, incidentu nebo ovlivnění morálky jiných zaměstnanců, kteří by mohli odvodit nedůležitost systému řízení bezpečnosti informací. Doporučuje se u zaměstnanců podepsat odpovědnost za dodržování bezpečnostní politiky a možné důsledky ve formě peněžního trestu nebo jiné penalizace (je zmíněno i v části ošetření rizik v předchozí kapitole).

4.4.4 Komunikace

Pro správné fungování ISMS musí být zajištěna komunikace jak interní, tak externí. Nemusí být komunikace pro všechny stejná, ale adekvátní pro daného příjemce, aby nedocházelo k přehlcení nepotřebnými informacemi, nebo naopak nepředání dostatečného množství informací.

Tabulka 18: Přehled komunikace ISMS
(Zdroj: Vlastní zpracování)

Oblast	Příjemce	Zodpovědná osoba	Komunikace
Interní	Vedení společnosti	ISMS koordinátor	Bezpečnostní politika a její změny. Bezpečnostní události a incidenty. Změny v ISMS (např. změny vůdčí role apod.). Výstupy auditů. Cíle bezpečnosti informací.
	Běžní zaměstnanci	ISMS koordinátor	Bezpečnostní politika a její změny. Vůdčí role a jejich kontakt.
	Provozní tým	ISMS koordinátor	Bezpečnostní politika a její změny. Vůdčí role a jejich kontakt.
Externí	Stát a regulační orgány	IMS manažer	Na vyžádání v oprávněných případech.

	Zákazníci	Projektový manažer	Bezpečnostní politika související s dodávkou pro zákazníka. Na vyžádání v oprávněných případech.
	Dodavatelé	Projektový manažer	Při podpisu smlouvy bezpečnostní politika, pokud bude vhodné.

Formát komunikace závisí do dohodě mezi zodpovědnou osobou a příjemcem. V některých případech může jít o intranet nástroj (např. u komunikace vůči běžným zaměstnancům), v některých případech o smlouvu (např. u dodavatelů). Je na uvážení zodpovědné osoby, jakým způsobem komunikaci provede. Mělo by být zajištěné, že ke komunikaci došlo (např. zápisem ze schůzky, emailovou komunikací) pro případné dokazování příjemci.

4.5 Dokumentované informace

4.5.1 Obecně

Organizace musí dokumentovat minimálně informace požadované normou, pokud by s ní chtěla být v souladu. Zároveň musí udržovat další informace nezbytné pro efektivitu ISMS. Tato práce může sloužit jako základní dokumentace, musí však být doplněny o případné informace oproti shodě v době auditu.

4.5.2 Vytváření a aktualizace

Identifikace a popis

Organizace využívá k dokumentování informací softwarový nástroj. Tento nástroj se přístupný pouze po přihlášení pracovním účtem daného uživatele, tím pádem automaticky zaznamenává autora a editora, zaznamenává a datum a čas úprav, včetně konkrétních změn mezi jednotlivými verzemi dokumentu.

V případě fyzických dokumentů je doporučeno zavést do šablon tyto informace také, aby čtenář byl ujištěn o validitě dokumentu. Minimálně uvést datum vzniku, datum změn a autora dokumentu.

Formát

Většina dokumentů by měla být v elektronické podobě. Z pohledu formátu je doporučeno dodržovat jednotný jazyk napříč nástrojem, pokud nebude vyžadována jiná jazyková verze (např. z důvodu projektu se zahraničním subjektem a podobně). Formát a struktura dokumentů je již definována a může být zachována – jednoduchost, minimalismus, nepoužívání zkratek apod.

Přezkoumání a schválení

Schvalování dokumentovaných informací je důležitým krokem, aby byla zajištěna vhodnost a platnost informací a aktuálně není ani formálně nastavena. Výhodou vybraného softwarového nástroje jsou přístupová práva a možnost nastavit konkrétní editory daných dokumentů. Vybraný softwarový nástroje je rozdělen do prostorů s konkrétními vlastníky. Tyto prostory mohou být určeny pro různé účely pro vybrané publikum, zároveň přispívatelé a schvalovatelé mohou být jiní. V rámci zachování jednoduchosti pro zahájení tohoto schvalování jsou doporučeny následující pravidla:

- Samotný akt schválení může provést vlastník stránky, který zároveň nemusí být vlastníkem prostoru. Vlastník prostoru zodpovídá, že schválené dokumenty jsou správné a v plné platnosti.
- Vlastník prostoru dává právo, kdo může daný prostor editovat. Pokud má uživatel editační právo, může stránky vytvářet, doplňovat a upravovat a jsou automaticky považovány za schválené.
- Některé prostory nemusí podléhat schválení a mohou tak mít výjimku (mezi tyto prostory spadá např. projektové dokumentace pro zákazníky).
- Schválením nemusí nutně procházet veškeré dokumenty (mezi tyto dokumenty spadá např. zápisy ze schůzek).

V případě zpětných vazeb na nedostatečnost těchto pravidel je doporučena revize a případné zpřísnění pravidel.

4.5.3 Řízení dokumentovaných informací

Distribuce a dostupnost

Organizace využívá softwarové nástroje k ukládání dokumentace v cloudovém prostředí a tím zaručuje dostupnost k využití v potřebné situaci. V této oblasti není procesně chtěné a potřebné dělat změny.

Ochrana

Pro ochránění dokumentů je vhodné využít klasifikaci dokumentů a mít vypracovaný popis jednotlivých stupňů, jak s daným dokumentem pracovat. Pro tento účel je využitá stupnice důvěrnosti, která zároveň stanovuje, jakou klasifikační značkou se dokument označuje.

Jednotlivé klasifikace a její definice jsou upraveny na základě požadavků společnosti. Ačkoliv může v některých případech jít o nestandardní postup nebo používání, jedná se o nejoptimálnější variantu dle fungování společnosti s dokumenty. Toto nastavení je vyžadováno vedením společnosti.

Tabulka 19: Klasifikace informací s označením
(Zdroj: Vlastní zpracování)

Klasifikace	Značka	Definice
Veřejné	VEŘEJNÉ nebo bez označení ve stanovených výjimkách	Informace určené ke zveřejnění, jejichž zveřejnění nepředstavuje riziko. Dokument nemusí být označen, pokud je z povahy věci veřejný (např. zveřejněná účetní závěrka). Označení je u dokumentů, u kterých není jasné, že se jedná o veřejné dokumenty se záměrem je veřejnosti vystavovat.
Interní	INTERNÍ nebo bez označení	Běžné pracovní informace, výchozí úroveň. Přístup mají zaměstnanci dle potřeby, některých případech dle dostatečně nastavených práv. Veškeré neoznačené dokumenty jsou považovány za INTERNÍ, pokud není výjimkou stanoveno jinak (viz. definice klasifikace VEŘEJNÉ).

Důvěrné	DŮVĚRNÉ	Citlivé informace s omezeným přístupem i uvnitř firmy, neoprávněný přístup může způsobit škody. Označené značkou DŮVĚRNÉ.
Přísně důvěrné	PŘÍSNĚ DŮVĚRNÉ	Kritické informace, jejichž vyzrazení by způsobilo závažné škody, podléhají přísné kontrole a legislativním požadavkům. Označené značkou PŘÍSNĚ DŮVĚRNÉ.

Pro jednotlivé klasifikace je definován styl uchovávání, vyjádřeno pomocí tabulky.

Tabulka 20: Klasifikace informací a požadavky uchovávání
(Zdroj: Vlastní zpracování)

Klasifikace	Uchovávání
Veřejné	Žádná speciální ochrana, lze ukládat kdekoliv.
Interní	Pouze firemní úložiště (např. Nástroj pro spolupráci, Software dokumentace) pod přihlášením konkrétního uživatele s více faktorovou autentizací, fyzické dokumenty nesmí být ve volně přístupných prostorech.
Důvěrné	Pouze firemní úložiště (např. Nástroj pro spolupráci, Software dokumentace) pod přihlášením konkrétního uživatele s více faktorovou autentizací, jen pro oprávněné osoby, zálohy šifrované, fyzicky zamčeno, řízený přístup.
Přísně důvěrné	Pouze firemní úložiště (např. Nástroj pro spolupráci, Software dokumentace) pod přihlášením konkrétního uživatele s více faktorovou autentizací, jen pro jmenované osoby, bez ukládání na lokální zařízení, fyzicky zamčeno v trezoru, řízený přístup.

Pro jednotlivé klasifikace jsou definovány požadavky přenos, vyjádřeno pomocí tabulky.

Tabulka 21: Klasifikace informací a požadavky přenosu
(Zdroj: Vlastní zpracování)

Klasifikace	Přenos
Veřejné	Bez omezení.
Interní	Primárně pro interní uživatele, externě jen s NDA. Fyzicky v uzavíratelné složce nebo deskách.
Důvěrné	Primárně uvnitř organizace, při sdílení šifrovaně se zaslaným heslem odděleným kanálem, fyzicky pouze osobně nebo kurýrem s potvrzením.
Přísně důvěrné	Primárně uvnitř organizace, sdílení jen ve výjimečných případech s NDA a schválením IMS manažera, každý přenos evidován, zapečetěné obálky.

Pro jednotlivé klasifikace jsou definovány požadavky na likvidaci, vyjádřeno pomocí tabulky.

Tabulka 22: Klasifikace informací a požadavky likvidaci
(Zdroj: Vlastní zpracování)

Klasifikace	Likvidace
Veřejné	Bez speciálních požadavků.
Interní	Fyzicky pomocí skartovače nebo roztrháním, aby kousek neobsahoval ucelenou informaci. Datové nosiče skrze formátování.
Důvěrné	Fyzicky pomocí skartovače, datové nosiče skrze formátování.
Přísně důvěrné	Fyzicky pomocí skartovače, na lokálním zařízení by se neměla vyskytovat.

Pro jednoduchost rozeznání, jakou klasifikaci danému dokumentu přiřadit, slouží příklady informací, vyjádřeno pomocí tabulky.

Tabulka 23: Klasifikace informací a příklady dokumentů
(Zdroj: Vlastní zpracování)

Klasifikace	Příklady informací
Veřejné	Marketingové materiály, tiskové zprávy, webové stránky, reference, obecné pracovní nabídky, veřejná dokumentace.
Interní	Obchodní dokumenty, smlouvy, komunikace, projektová dokumentace, interní politiky, šablony, zápisy, běžná korespondence.
Důvěrné	Firemní strategie, mzdové výměry, smlouvy s citlivými podmínkami, zdrojové kódy, pracovní smlouvy.
Přísně důvěrné	Privátní klíče, zdravotní dokumentace, krizové plány, obchodní tajemství.

Přístup

Dokumenty jsou řízení pomocí přístupů, tudíž dokumenty jsou zpřístupněny pouze osobám nebo skupinám, které mohou dokumentaci využívat. Zároveň jsou určena práva na úpravu dokumentace, aby nedošlo k nechtěné nebo nežádoucí úpravě.

Řízení změn

V oblasti řízení změn lze využít softwarového řešení, které je na historii verzí připraveno a umožňuje zaznamenat datum změny, autora změny a konkrétní upravené části, včetně možnosti porovnání s konkrétní historickou verzí.

Likvidace

Dokumentované informace se postupem času aktualizují, ale zároveň zastarávají. Aktuálně organizace nemá formálně popsanou likvidaci dokumentů. Pro likvidaci v softwarových nástrojích jsou doporučeny následující pravidla:

- Archivace celé stránky vlastníkem – archivací je míněna funkcionalita softwarového řešení.
- Přesun stránky “Archiv” ve struktuře nástroje.
- Uzamčení vlastníkem stránky, aby k ní ostatní již neměli přístup.

Pravidla pro likvidaci fyzických dokumentů jsou popsána v předchozí části.

4.6 Provozování

4.6.1 Plánování a řízení provozu

Pro plánování a provoz je doporučeno použít tuto práci jako základní dokumentaci a případně si ji doplnit nebo upravit o žádoucí ve chvíli zavádění. Je nutné, aby provoz postupoval podle plánu a případné odchylky a nežádoucí změny byly napraveny.

4.6.2 Posuzování rizik informační bezpečnosti

Posuzování rizik informační bezpečnosti je doporučeno provádět minimálně jednou ročně nebo při větších změnách pod vedením ISMS koordinátora. Posouzení musí být dokumentováno a předloženo IMS manažerovi jako výstup.

4.6.3 Ošetření rizik informační bezpečnosti

Pro ošetření rizik musí vzniknout plány provádějící jejich zavedení. Tyto plány musí být dokumentovány a kontrolovány. Doporučením je provést revizi u těchto plánů minimálně jednou ročně a v případě nedostatků zahájit akční kroky k jeho dokončení nebo úpravu dle daných potřeb.

4.7 Hodnocení výkonnosti

4.7.1 Monitorování, měření, analýza a hodnocení

Vzhledem k novému systému řízení bezpečnosti informací je doporučeno na začátku stanovit pár základních ukazatelů, nad kterými bude moct být prováděna analýza a vyhodnocení. Při velkém množství měřeních parametrů může být způsobena nepraktičnost a ztráta velkého množství času na vyhodnocení, pokud bude vůbec možné. Zároveň může být způsoben negativní efekt ze strany vedení, že ISMS je příliš náročné a nechuť systém vylepšovat. Společnost by měla postupem času zjistit, jaké konkrétní hodnoty potřebuje měřit, aby výsledek byl relevantní pro změnu v rámci ISMS.

Jako příklad položek pro měření může být:

- Doba reakce na bezpečnostní incident.
- Strávený čas na údržbě ISMS a projektů z něj plynoucích.
- Úspěšnost splnění průběžných testů zaměstnanců.

4.7.2 Interní audit

4.7.2.1 Obecně

Interní audit je doporučeno provádět minimálně jednou ročně po setkání Compliance týmu a validaci předchozích bodů. Interní audit může sloužit jako kvalitní nástroj pro odhalení neshod s normou a možnosti včasné nápravy před případným auditem certifikačního orgánu. Musí být v dostatečném předstihu před auditem certifikačního orgánu.

4.7.2.2 Program interního auditu

Četnost

Četnost auditu je doporučena jednou za rok pod vedením ISMS koordinátora. Určité situace mohou vyžadovat dřívější interní audit, může se jednat o případy, kdy jsou v ISMS prováděny rozsáhlé změny z důvodu požadavků externích stran, po významném incidentu nebo nově zavedené technologii.

Zodpovědnosti

Primární zodpovědnost pro zajištění auditu je na ISMS koordinátorovi. Vzhledem k dostatečnému proškolení je doporučené provedení interního auditu minimálně z jeho strany, pokud nebude schopný zajistit auditora externího s objektivním pohledem. Ideálně by měl být audit proveden externí osobou s dostatečnou kvalifikací.

Formát

Interní audit je doporučený v plném rozsahu ISMS. Formát zápisu výstupů může být jako v kapitole Analýza současné situace, celkové zhodnocení, tudíž jednotlivé body normy a vyjádření stavu. Nesmí se opomenout možné změny v rámci ISMS (např. změna požadavků zainteresovaných stran. Tento formát se doporučuje udržovat při každém cyklu interního auditu, aby byla zachována jednotnost zápisu a jednoduchost při orientaci.

Výstupem musí být zápis s těmito náležitostmi: jménem zodpovědné osoby, interního auditora, datum provedení a datum ukončení a výsledek auditu. V případě, že společnost bude mít již provedený audit od certifikačního orgánu, je doporučené formát upravit takovým způsobem, aby se co nejvíce blížil tomuto auditu od kvalifikovaných auditorů.

Předání vedení

Výstup interního auditu musí být předán IMS manažerovi. V případě neshod by měl být popsán důvod neshody a alespoň krátký návrh na jeho vyřešení. IMS manažer má za úkol rozhodnout o nápravě neshody.

4.7.3 Přezkoumání vedením

4.7.3.1 Obecně

IMS manažer by měla být osoba z vrcholového vedení a měla by být schopna zastoupit vrcholové vedení u všech schůzí souvisejících se systémem řízení bezpečnosti informací. V případě potřeby IMS manažer rozhoduje o zapojení dalších členů vrcholového vedení.

4.7.3.2 Vstupy pro přezkoumání vedením

Vzhledem k povaze společnosti budou hlavními vstupy strategické cíle, které by mohly jakkoli modifikovat nebo vytvářet nové požadavky na ISMS. IMS manažer by měl být schopný zprostředkovat veškeré vstupy a vytvářet akční kroky k jejich naplnění, včetně představení ostatním členům vrcholového vedení.

4.7.3.3 Výsledky z přezkoumání vedením

Výsledek z přezkoumání je nutné poznamenat jako dokumentovanou informaci. Zároveň by mělo dojít ze zvážení, zdali zjištěné výstupy nemohou být zahrnuty do cílů organizace, aby docházelo k neustálému zlepšování.

4.8 Zlepšování a udržování

4.8.1 Neustálé zlepšování

ISMS nemůže být brán jako jednorázový projekt, ale jako nekonečně trvající proces. Z tohoto důvodu musí docházet k neustálému zlepšování a společnost by na tom měla být ve shodě. Soustavné zlepšování zvyšuje kvalitu ISMS, snižuje míru rizika negativních incidentů a zvyšuje povědomí o nutnosti se touto oblastí zabývat. ISMS by nemělo být negativně vnímáno, a proto i větší změny tohoto dokumentu jsou přijatelné, pokud budou v souladu s požadavky normy.

Neustálé zlepšování bude dosaženo za pomocí pravidelných porad Compliance týmu, provádění interních auditů, posuzování rizik bezpečnosti informací a stanovení opatření.

4.8.2 Neshody a nápravná opatření

Za výskytu neshody je nutná náprava a zjištění příčiny neshody. Neshodou může být opomenutí v metodice, nedostatečné povědomí nebo komunikace potřebným stranám, porušení bezpečnostní politiky, vyskytnutí bezpečnostní události nebo incidentu, popřípadě jiný nesoulad. Pro všechny tyto případy musí být provedena adekvátní reakce. Při této reakci je doporučena přítomnost ISMS koordinátora, jelikož by měl mít největší povědomí o případných dopadech na ISMS jako celek.

Při neshodě je doporučeno zjistit příčinu problému, historii a následky. Na základě těchto informací musí být vyhodnoceno, jaká reakce bude provedena. Pro posouzení rizika je doporučeno využít dříve zmíněna metodika. Veškeré kroky a rozhodnutí musí být zaznamenány. Informacemi v záznamu jsou doporučeny:

- Jméno nálezce neshody,
- jméno řešitele,
- datum a čas nálezu (popřípadě i datum a čas události),
- popis neshody,
- potenciální následek neshody (popřípadě následek události),
- možnosti opatření,
- konečné rozhodnutí.

4.9 Ekonomické zhodnocení

Z pohledu ekonomického se pracuje se stranou výnosů a nákladů. Vstupy jsou zajištěny vedení společnosti.

Výnosy jsou posuzovány primárně z kvalitativního pohledu vzhledem ke složitosti přesného výpočtu a vyčíslení. Vstupy na straně výnosů jsou:

- Potenciál výnosů do budoucna – při souladu s metodikou pro ISMS, a z toho plynoucí lepší úroveň kybernetické bezpečnosti, může mít firma lepší vyjednávací pozici u nových projektů a lepší konkurenceschopnost. Předpoklad vedení je

zvýšení pocitu odpovědnosti vůči bezpečnosti informací ze strany zákazníků a tím vyšší náklonnosti pro spolupráci. U historických projektů byla vybraná společnost vyloučena z výběrových řízení, protože nebyla certifikována v oblasti ISMS a ztratila možnost nových projektů. Tento argument je pro společnost dostatečný a je hlavním pilířem investice do ISMS.

- Udržení stávajících zákazníků – případná certifikace, ale minimálně postup dle ISMS metodiky, zajistí konkurenceschopnost u aktuálních zákazníků. Z predikce od finančního ředitele se pohybuje objem zakázek na částce cca 100 milionů korun, kde by mohla hrozit ztráta spolupráce při nesplňování metodického postupu.
- Nižší pravděpodobnost ztrát při incidentu – při postupu podle metodiky se slibuje odhalení vážných míst, ze kterých mohou plynout neočekávané náklady při incidentu a jeho nápravě. Nastavená opatření směřují k nižší pravděpodobnosti uskutečnění incidentů a ušetření peněžní částky nebo pověsti společnosti.

Mezi náklady se primárně řadí náklady na konzultanta vybrané metodiky, provedení analýzy, komunikace s vedením a zpracování dokumentace. V aktuální chvíli nebyla ani pro vybraná opatření nutnost pořizovat speciální software a pracuje se s již zavedeným softwarem. Vzhledem k používání softwaru i pro jiné účely ve společnosti nejsou částky za licence zahrnovány do výpočtu nákladů, jelikož by byly zaplaceny nehledě na systém ISMS. Nepracuje se s odhadem nákladů u opatření, protože opatření vyžaduje práci interních pracovníků a jejich náklady spojené se zavedením nejsou vedením zpřístupněny. Organizace musí sama tyto náklady zajistit a zahrnout do výpočtů. Stanovené náklady jsou nutné vnímat jako orientační a provést přepočet nákladů při reálné implementaci. Vstupy pro výpočet nákladů jsou:

- Práce konzultanta ISMS – společnost nemá interně znalce v oblasti ISMS a norem řady ISO 27000. Tato práce slouží jako konzultace, zpracování a nastavení podle vybraných bodů dle ČSN EN ISO/IEC 27001:2023 a může být využita pro řízení bezpečnosti informací. V nákladech se pracuje s výpočtem za konzultanta, jehož prací by bylo vypracování této dokumentace. Náklad může být proměnlivý u případné úpravy rozsahu nebo jiným specifickým požadavkům.
- ČSN online – přístup k normám je klíčový pro ISMS koordinátora a musí mít k dispozici jednotlivé normy, aby podle nich mohl ISMS nastavovat a řídit. (26)

Tabulka 24: Přehled nákladů
(Zdroj: Vlastní zpracování)

Název činnosti	Cena v Kč (bez DPH)	Frekvence
Práce konzultanta	400000	Jednorázově
Školení ISMS pro ISMS koordinátora	20000	Jednorázově (může být i ročně při opakovaném studiu)
ČSN online licence	2000	Ročně

Ekonomické vyhodnocení a přínos je založen primárně na strategickém významu, nikoliv čistým výpočtem, který by mohl působit jako méně přínosný, než by bylo v případě jiného projektu s číselně vyjádřenými výnosy. Vedení společnosti si od těchto kroků slibuje zlepšení pověsti společnosti, zvýšení konkurenceschopnosti a zvýšení úrovně ochrany vůči negativním vlivům.

4.10 Přínos návrhů

Návrh zavedení nové metodiky pro oblast ISMS a návrh opatření

Práce přináší návrh pro zavedení nové metodiky pro oblast ISMS, která vede k formalizaci stávajících procesů, zavedení procesů nových a zavázání se k neustálému zlepšování. Tento krok společnosti dokáže získat velký posun v ISMS, snížení rizika porušení bezpečnosti informací a postupné zvyšování úrovně kybernetické bezpečnosti.

Návrh zahrnuje definici kontextu organizace a vymezení ISMS, zavedení nových rolí, využití uznávané metodiky pro řízení rizik, nastavení školení pro několik skupin příjemců, definici externí a interní komunikace, definici správy a klasifikace dokumentovaných informací a definici průběžné kontroly ISMS, včetně interního auditu.

Neustálé zlepšování povede organizaci k posouvání všech oblastí a postupné vylepšování oblastí k lepšímu stavu v průběhu času.

Tento návrh napomáhá celkové úrovně kybernetické bezpečnosti organizace, protože metodicky vede k upravení existujících nebo zavedení opatření, jež budou informace chránit v kybernetickém prostoru.

Posun k certifikaci ČSN EN ISO/IEC 27001

Návrh byl prováděn v souladu se zmíněnou normou a může posloužit jako velmi kvalitní podklad pro případnou certifikaci organizace vůči normě. Tento krok je výrazně doporučen, protože zajistí dostatečnou jistotu v provádění ISMS, zaručuje validitu pro externí strany a zaváže organizaci nestálému zlepšování dozorovými audity. Certifikace povede k vyšší konkurenceschopnosti a s tím spojeným potenciálem pro zpracování nových projektů vyžadující certifikované dodavatele.

Metodická předpříprava pro zákon o kybernetické bezpečnosti

Některé body v návrhu byly prováděny vůči bodům z vyhlášky o kybernetické bezpečnosti a přibližuje organizaci uznávaným postupům v české legislativě. V případě nutnosti se podřizovat zákonu o kybernetické bezpečnosti bude mít firma výraznou část splněnou a ušetří finanční zdroje a čas spojené s přepracováváním nastavené metodiky.

ZÁVĚR

Tato diplomová práce měla za cíl analyzovat stávající stav kybernetické bezpečnosti ve vybrané organizaci, posoudit jeho úroveň a navrhnout změny vedoucí ke zlepšení a eliminaci nalezených rizik ve vybrané společnosti.

První část je věnována teoretickému základu pro pochopení dané problematiky, studiu základních pojmů v odvětví bezpečnosti informací, klíčových norem, legislativy a osvědčených postupů.

Druhá část se zabývá rozborem stávajícího stavu. Rozbor byl proveden pomocí GAP analýzy vůči vybrané normě ČSN EN ISO/IEC 27001:2023 pro získání znalostí o aktuálním nastavení a identifikaci nedostatků. Výstup rozboru byl seznam zjištěných nedostatků.

Třetí část popisuje jednotlivé návrhy řešení a doporučení identifikovaných nedostatků. Návrhy pro zvýšení úrovně kybernetické bezpečnosti jsou dosaženy pomocí konkrétně navržených opatření a nově nastavených postupů, včetně důrazu na neustálé zlepšování, které zajišťuje procesní zlepšování společnosti a zavádění nových opatření v oblasti kybernetické bezpečnosti. Kybernetické hrozby se neustálé vyvíjí, a proto je nutné opatření zavádět průběžně podle kvalitně nastavených procesů. Tato práce může být využita jako podklad vedení a novému týmu při realizaci změn v oblasti kybernetické bezpečnosti.

Dalším důležitým přínosem této práce je vytvoření obecné metodiky pro zavádění shody s požadavky ISMS v organizaci. Tato metodika představuje systematický postup a může být aplikována v jiných společnostech, což zvyšuje univerzálnost práce.

SEZNAM POUŽITÉ LITERATURY

1. Sedlák, Petr a Konečný, Martin. *Přeměna ISMS v manažerské informace.* Brno : Akademické nakladatelství CERM, s.r.o., 2023. ISBN 978-80-7623-110-8.

2. Sedlák, Petr, Konečný, Martin a a kolektiv. *Kybernetická (ne)bezpečnost, Problematika bezpečnosti v kyberprostoru.* Brno : Akademické nakladatelství CERM, s.r.o., 2021. ISBN 978-80-7623-068-2.

3. Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). *e-Sbírka.* [Online] 28. květen 2018. [Citace: 3. březen 2025.] https://www.e-sbirka.cz/sb/2018/82.

4. ČSN EN ISO/IEC 27002 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Opatření informační bezpečnosti. Praha : Česká agentura pro standardizaci, 2023.

5. ČSN EN ISO/IEC 27000 Informační technologie - Bezpečnostní technicky - Systémy řízení bezpečnosti informací - Přehled a slovník. Praha : Česká agentura pro standardizaci, 2020.

6. Žaloudek, Karel. *Encyklopedie politiky.* Praha : Libri, 1999. ISBN 80-85983-75-3.

7. Druhy právních předpisů. *Evropská unie.* [Online] [Citace: 1. březen 2025.] https://european-union.europa.eu/institutions-law-budget/law/types-legislation_cs.

8. Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). *e-Sbírka.* [Online] 29. 8 2014. [Citace: 3. březen 2025.] https://www.e-sbirka.cz/sb/2014/181.

9. Průvodce směrnicí NIS2. *Portál NÚKIB.* [Online] [Citace: 5. březen 2025.] https://portal.nukib.gov.cz/pruvodce-smernici-nis2.

10. Legislativa KB. *Národní úřad pro kybernetickou a informační bezpečnost.* [Online] [Citace: 3. březen 2025.] https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/.

11. About ISO. *iso.org.* [Online] [Citace: 1. březen 2025.] https://www.iso.org/about.

12. Frequently asked questions. *IEC International Electrotechnical Commission.* [Online] [Citace: 1. březen 2025.] https://www.iec.ch/faq.

13. European Standards. *CENELEC.* [Online] [Citace: 1. březen 2025.] https://www.cencenelec.eu/european-standardization/european-standards/.

14. Úplné znění zřizovací listiny dodatek 7. *Agentura ČAS.* [Online] [Citace: 1. březen 2025.] https://agenturacas.gov.cz/wp-content/uploads/Uplne-zneni-zrizovaci-listiny_dodatek-07.pdf.

15. Agentura. *ČAS Česká agentura pro standardizaci.* [Online] [Citace: 2. březen 2025.] https://agenturacas.gov.cz/o-nas/agentura/.

16. ČSN EN ISO/IEC 27001 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Systémy managementu informační bezpečnosti - Požadavky. Praha : Česká agentura pro standardizaci, 2023.

17. ČSN EN ISO/IEC 27003 Informační technologie - Bezpečnostní technicky - Systémy řízení bezpečnosti informací - Pokyny. Praha : Česká agentura pro standardizaci, 2018.

18. ČSN EN ISO/IEC 27005 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Pokyny pro management rizik informační bezpečnosti. Praha : Česká agentura pro standardizaci, 2023.

19. Doucek, Petr, Konečný, Martin a Novák, Luděk. *Řízení kybernetické bezpečnosti a bezpečnosti informací.* Praha : Professional Publishing, 2020. ISBN 978-80-88260-39-4.

20. Doporučení k používání protokolu TLP ke sdílení chráněných informací. *Národní úřad pro kybernetickou a informační bezpečnost.* [Online] [Citace: 10. březen 2025.] https://nukib.gov.cz/cs/infoservis/doporuceni/1593-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci/.

21. TRAFFIC LIGHT PROTOCOL (TLP). *First Improving Security Together.* [Online] [Citace: 10. březen 2025.] https://www.first.org/tlp/docs/v2/tlp-v2-cz.pdf.

22. Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti. *NÚKIB.* [Online] [Citace: 5. březen 2025.] https://nukib.gov.cz/download/publikace/podpurne_materialy/Prvodce%20zenm%20aktiv%20a%20rizik%20dle%20vyhlky%20o%20kybernetick%20bezpenosti.pdf.

23. Apple Platform Security Protecting against malware in MacOS. *Apple.com.* [Online] 19. 12 2024. [Citace: 10. duben 2025.] https://support.apple.com/cs-cz/guide/security/sec469d47bd8/web.

24. Windows security, safety, and privacy Firewall and Network Protection in the Windows Security App. *Microsoft.com.* [Online] [Citace: 10. duben 2025.] https://support.microsoft.com/en-us/windows/firewall-and-network-protection-in-the-windows-security-app-ec0844f7-aebd-0583-67fe-601ecf5d774f.

25. Microsoft Defender antivirus in Windows Overview. *Microsoft.com.* [Online] 5. 2 2024. [Citace: 12. duben 2025.] https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-antivirus-windows.

26. Registrace uživatele. *ČSN online pro jednotlivce.* [Online] [Citace: 1. květen 2025.] https://csnonline.agentura-cas.cz/registraceff.aspx.

SEZNAM OBRÁZKŮ

SEZNAM GRAFŮ

SEZNAM TABULEK

SEZNAM POUŽITÝCH ZKRATEK

BYOD	Bring Your Own Device
CEO	Chief Executive Officer
CFO	Chief Finance Officer
CSO	Chief Sales Officer
CTO	Chief Technology Officer
ČAS	Česká agentura pro standardizaci
ČSN	Česká technická norma
EN	Evropská norma
HR	Human Resources
HW	Hardware
IEC	International Electrotechnical Commission
IMS	Integrovaný systém řízení
ISMS	Systém řízení bezpečnosti informací
ISO	International Organization for Standardization
IT	Information Technology
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
SAE	Security Awareness Education
SLA	Service Level Agreement
SW	Software
TLP	Traffic Light Protocol
VKB	Vyhláška o kybernetické bezpečnosti
ZKB	Zákon o kybernetické bezpečnosti