Implementace ISMS za využití agilních metod

Bc. Jiří Diviš

Diplomová práce
2022

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Jiří Diviš**
Osobní číslo:	**A20173**
Studijní program:	**N1032A020003 Bezpečnostní technologie, systémy a management**
Specializace:	**Bezpečnostní management**
Forma studia:	**Kombinovaná**
Téma práce:	**Implementace ISMS za využití agilních metod**
Téma práce anglicky:	**ISMS Implementation Using Agile Methods**

Zásady pro vypracování

1. Seznámte se s problematikou agilních metod a ISMS a stručně je popište.
2. Proveďte základní analýzu současného stavu ISMS v podniku.
3. Stanovte rozsah ISMS s ohledem na velikost a ekonomické možnosti podniku tak, aby byla zachována rovnováha mezi požadovanou bezpečností a náklady na opatření.
4. Na základě provedené analýzy a stanoveného rozsahu navrhněte postup zavedení ISMS pomocí agilních metod.
5. Zhodnoťte přínosy navrhnutého řešení.

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

Seznam doporučené literatury:

1. ČSN EN ISO/IEC 27002 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací
2. ŠOCHOVÁ, Zuzana a Eduard KUNCE. *Agilní metody řízení projektů*. Brno: Computer Press, 2014. ISBN 978-80-251-4194-6.
3. SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.
4. JAŠEK, Roman a David MALANÍK. *Bezpečnost informačních systémů*. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2013. ISBN 978-80-7454-312-8.
5. KOLOUCH, Jan, Pavel BAŠTA, Andrea KROPÁČOVÁ a Martin KUNC. *CyberSecurity*. Praha: CZ.NIC, z. s. p. o., 2019. ISBN 978-80-88168-34-8.

Vedoucí diplomové práce: **Ing. Lukáš Králík, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **3. prosince 2021**
Termín odevzdání diplomové práce: **23. května 2022**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 7. února 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl jsem seznámen s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně, dne 22.05.2023 ……..

podpis studenta

ABSTRAKT

Tato diplomová práce se zaobírá problematikou zavedení systému řízení bezpečnosti informací ve středně velkých podnicích. Pro tyto potřeby byla sestavena metodika pro zavedení ISMS vycházející z podpůrných materiálů Národního úřadů pro kybernetickou a informační bezpečnost (konkrétně z minimálního bezpečnostního standardu) a z principů norem řady ISO/IEC 27000. Postup zavedení ISMS vychází z agilního přístupu, konkrétně z metody SCRUM.

Klíčová slova:

ISMS, minimální bezpečnostní standard, agilita, SCRUM

ABSTRACT

This master's thesis deals with the implementation of an information security management system in medium-sized companies. The methodology for the ISMS implementation was developed based on the supporting materials of the National Cyber and Information Security Agency (specifically the minimum-security standard) and the principles of the ISO / IEC 27000 standards. The ISMS implementation process is based on an agile, specifically the SCRUM method.

Keywords:

ISMS, minimum-security standard, agile, SCRUM

„Vzdělávání je učení se toho, o čem jste ani nevěděli, že to nevíte.“ Daniel J. Boorstin

Na tomhle místě bych se chtěl poděkovat vedoucímu práce Ing. Lukášovi Králíkovi, Ph.D. za cenné rady a odborný dohled.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Odvětví kybernetické a informační bezpečnosti zažívá v dnešní době značný rozvoj. V prvním řadě se jedná o důsledek z dob vzniku prvních počítačů a počítačových sítí, kdy byl kladen důraz na funkčnost a komunikace i software byly vyvíjený jako nezabezpečené. Vzniklo tak prostředí náchylné na úmyslné poškození. Časem byly odhalovány další a další potenciální hrozby jak už z kategorie objektivních (např. působení přírodních živlů, elektromagnetické vyzařování) tak subjektivních (např. neúmyslné poškození správcem nebo uživatelem). Cílem kybernetické a informační bezpečnosti je v takovémto rizikovém kybernetickém prostředí dosáhnout stav, kdy není bezprostředně ohrozena důvěrnost, dostupnost a integrita chráněných informací a služeb.

Důležitost ochrany kybernetického prostoru si uvědomil také zákonodárce, který začal tuhle oblast regulovat prostřednictvím zákona o kybernetické bezpečnosti (zákon č. 181/2014 Sb.). Zákon stanovuje povinnosti pro subjekty provozující kritickou informační infrastrukturu. Regulované jsou informační a komunikační infrastruktury zásadní pro ekonomiku, bezpečnost státu a ovlivňující dostupnost základních potřeb obyvatelstva. Povinnosti tak nedopadají na všechny subjekty pohybující se v kybernetickém prostoru ČR, co však neznamená, že tyto subjekty se nemusí ochranou v tomhle odvětví věnovat.

Pro organizace nespadající pod regulaci zákona o kybernetické bezpečnosti vydal Národní úřad pro informační a kybernetickou bezpečnost, ministerstvo vnitra ČR a Národní agentura pro komunikační a informační technologie doporučení, které kompaktně popisuje základní principy ochrany.

Táto diplomová práce navazuje na minimální bezpečnostní standard a rozvíjí ho vytvořením metodiky, kterou mohou vyžit středně velké organizace při zavádění ISMS. Samotná implementace je postavená na agilních metodách, kterých výhoda spočívá v průběžném dodávaní řešení.

I. TEORETICKÁ ČÁST

1 KYBERNETICKÁ A INFORMAČNÍ BEZPEČNOST

V této kapitole budou zpracovány teoretické poznatky k systému řízení informací. Dále pak bude představen minimální bezpečnostní standard – dokument, který byl vydán jako vodítko pro zavádění bezpečnosti pro malé a střední organizace nespadající pod zákon o kybernetické bezpečnosti. Poslední dvě kapitoly se budou blíže zaobírat rozpracováním manažerských a technických opatření systému řízení bezpečnosti informací.

1.1 Systém řízeni bezpečnosti informací

Systém řízení bezpečnosti informací (Information Security Management System – ISMS) je rámec pro systematický procesní přístup k řízení informační a kybernetické bezpečnosti organizace. Dle normy ČSN EN ISO/IEC 27000 sestává „*z politik, postupů, směrnic a příslušných zdrojů a činností, které organizace řídí, aby zajistila ochranu informačních aktiv*“ [1, str. 20].

1.1.1 CIA triáda

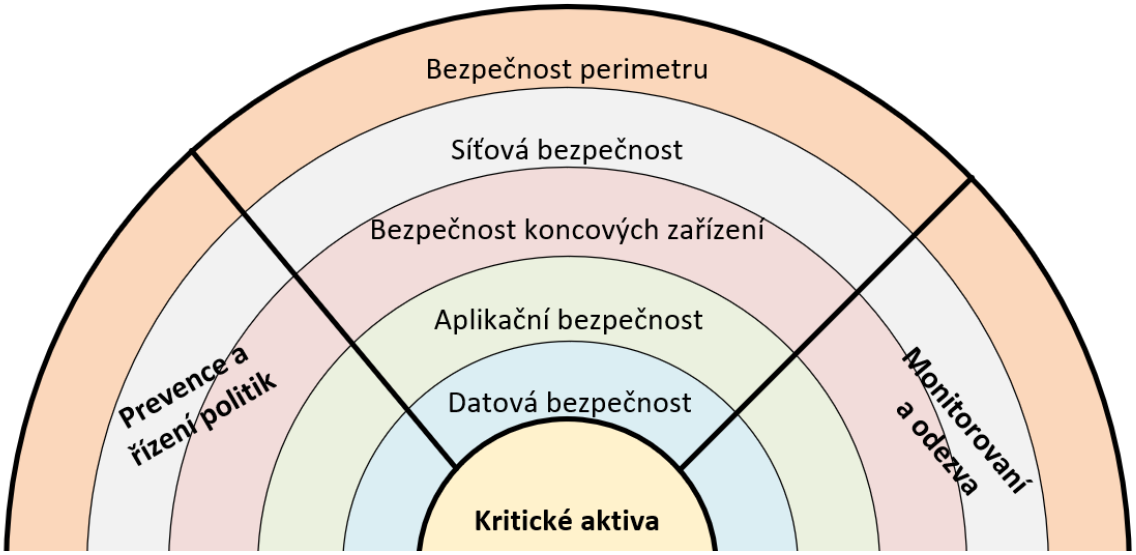
Základní principy informační a kybernetické bezpečnosti jsou implementovány tak, aby byla zajištěna ochrana informačních aktiv dle jednotlivých atributů **CIA** triády:

- **důvěrnost (C – Confidentiality)** – přístup k informacím mají jenom ti, kteří k tomu mají oprávnění (příklad opatření: řízení přístupu, šifrování dat v pohybu nebo během přenosu),
- **integrita (I – Integrity)** – údaje jsou úplné a bezchybné, tj. není ji možné libovolně měnit nebo narušit (příklad opatření: digitální podepisování, řízni přístupu, hashování),
- **dostupnost (A – Availability)** – údaje jsou dostupné v době, v které je subjekty potřebují (příklad opatření: load balancing, funkce návratu – rollback, relokace zařízení, zálohy, redundance) [2, str. 21].

1.1.2 Defense-in-Depth

Další z možností, jak na kybernetickou bezpečnost nahlížet je ochrana no hloubky (defense-in-Depth). Jedná se o vrstevnatý přístup, kde se ve vícero úrovních kumulují bezpečností opatření s cílem vytvoření synergického efektu. V principu se jedná o redundanci bezpečnostních opatření – organizace staví proti útočníkovi různé typy bariér a ochran, čím zabraňuje vzniku jediného bodu selhání bezpečnostních opatření [3].

Přístup Defense-in-Depth minimalizuje míru pravděpodobnosti úspěšného útoku. Důkladné zavedení uvedeného principu vede k výraznému prodloužení času potřebného pro úspěšný útok. Také zvyšuje nároky na zdroje, které by potenciální útočník potřeboval k provedení útoku [3].

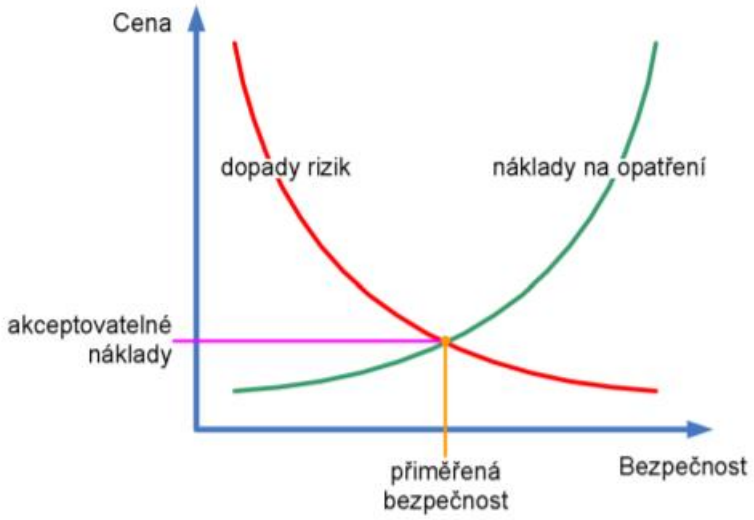


Obr. č. 1: Defence-in-Depth (převzato a upraveno [3])

1.1.3 Přiměřená bezpečnost za akceptovatelné náklady

Bezpečnost je dle terminologického slovníku ministerstva vnitra ČR: „*stav, kdy je systém schopen odolávat známým a předvídatelným (i nenadálým) vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům (případně celému systému) tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost a chování v souladu s cílovostí“* [4, str. 5].

Protože stav absolutní bezpečnosti není možné dosáhnout (vždy bude existovat zbytkové riziko působící na aktiva) je cílem organizace v oblasti ISMS je dosáhnout **přiměřenou bezpečnost**. Jedná se o „*stav, kdy velikost úsilí a investic do bezpečnosti odpovídá hodnotě aktiv a míře možných rizik*“ [5]. Vztah je možné vyjádřit jako přiměřenou bezpečnost za vynaložené akceptovatelné náklady. Pomocí procesu zvážení nákladů na opatření a dopadů rizik dokáže společnost vydefinovat množinu opatření, které jsou akceptovatelná pro stanovenou úroveň bezpečnost informací [4] [6] [7].



Obr. č. 2: Graf přiměřené bezpečnosti za akceptovatelné náklady [8, str. 34]

Riziko, které zůstalo po aplikaci opatření se nazývá **zbytkové** neboli **reziduální** (možnosti opatření: vyhnutí se riziku, odstranění zdroje rizika, změna možnosti výskytu rizika, změna dopadů, sdílení rizika, převzetí rizika ve snaze chopit se příležitosti, ponechání rizika na základě vědomé volby). Jeho součástí jsou i neidentifikovaná rizika [4, str. 99].

Z uvedeného je jasné, že organizace by měla věnovat pozornost procesu řízení rizik, tak aby mohla stanovit jejich dopady. ČSN EN ISO/IEC 27005 staví proces řízení rizik na následujících základních bodech:

- identifikování rizika navázaného na ohrožení CIA triády včetně vlastníků,
- posouzení dopadů rizik a pravděpodobnosti výskytu rizika,
- určení úrovně rizika,
- porovnání výsledků analýzy rizik s kritérií rizik,
- prioritizace rizik pro další řešení [9, str. 9].

1.1.4 Plan-Do-Check-Act cyklus

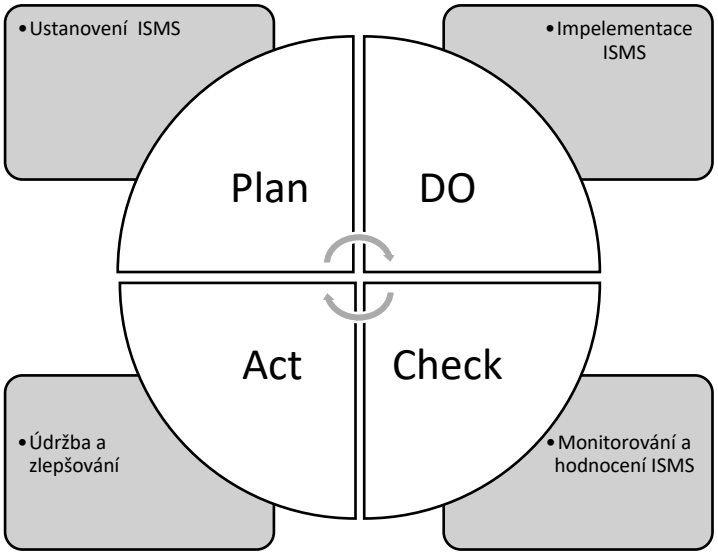
Jak je zobrazeno na následujícím obrázku, procesy kybernetické bezpečnosti jsou řízeny na základě Plan-Do-Check-Act (PDCA) cyklu neustálého zlepšování.

P (Plan, plánuj) – ustanovení o ISMS definuje základ pro celý zbytek cyklu ISMS. V této etapě jsou stanovený cíle a kontroly, které povedou k naplnění těchto cílů. Zavedení ISMS by mělo vycházet z podnikatelských cílů společnosti, jejího zaměření, organizační struktury, dostupných zdrojů apod. [10].

D (Do, dělej) – implementace a provoz ISMS. Neopominutelnou částí této etapy je stanovení odpovědných osob a také vzdělání uživatelů o všech bezpečnostních principech. Ve fázi provozu jsou pravidelně hodnoceny a eliminovány rizika, přičemž jsou využívány politiky, postupy a procesy ISMS [10].

C (Check, kontroluj) – zavedení zpětné vazby ve formě kontrol odpovědných osob, technických a organizačních kontrol, auditů apod. Jedná se o porovnání dokumentovaných postupů vůči reálnému vykonávaní procesů. Výsledkem by měla být doporučení pro změnu procesů nebo úpravu politik, procedur podle výsledků kontrol [10].

A (Act, konej) – na základě zjištěných nedostatků z předchozího kroku jsou vykonána zlepšení v systéme ISMS. V této etapě jsou vykonány nápravné opatření navrhnuty v předcházením kroku, přičemž všechny změny by měli být dokumentované [10].



Obr. č. 3: PDCA cyklus kybernetické bezpečnosti

1.2 Normativní bezpečnostní prostředí ČR

Základní právní dokument, který řeší problematiku ochrany kybernetického prostoru je zákon č. 181/2014 Sb. *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů* (**Zákon o Kybernetické Bezpečnosti – ZoKB).** Na něho navazují další vyhlášky:

- 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 – VoKB**),

- a vyhláška č. 317/2014 Sb. *Vyhláška o významných informačních systémech a jejich určujících kritériích.*

ZoKB definuje typy povinných subjektů, na které se uvedená normativní úprava vztahuje. Dle § 3 se jedná o:

- *„a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b),*
- *b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d),*
- *c) správce a provozovatel informačního systému kritické informační infrastruktury,*
- *d) správce a provozovatel komunikačního systému kritické informační infrastruktury,*
- *e) správce a provozovatel významného informačního systému,*
- *f) správce a provozovatel informačního systému základní služby, pokud nejsou správcem podle písmene c) nebo d), g) provozovatel základní služby, pokud není správcem nebo provozovatelem podle písmene f), a h) poskytovatel digitální služby*“ [11].

ZoKB není tak přímo aplikovatelný ve středních a malých organizacích. V těchto organizacích se teprve začíná zavádět kybernetická bezpečnost. Z tohoto důvodů byl vydán dokument s názvem Minimální bezpečnostní standard lépe reflektující potřeby malých a středních podniků. Minimální bezpečností standard je blíže popsán v následující kapitole. Standard představuje vodítko pro zavedení minimální úrovně zabezpečení – nejedná se tak o náhradu ZoKB ani prováděcích vyhlášek [13, str.4].

1.3 Minimální bezpečností standard

V roku 2020 vydal Národní úřad pro kybernetickou bezpečnost (NÚKIB) a Národní agentura pro komunikační a informační technologie (NAKIT) minimální bezpečnostní standard. Standard byl vydán jako podpůrný materiál pro subjekty, které nespadají pod regulaci zákona o kybernetické bezpečnosti. Jedná se o doporučení, které je určeno organizacím začínajícími se zaváděním kybernetické bezpečnosti [13, str. 4]. Dokument je tvořen dvěma částmi:

- **manažerská** – popisuje postupy a procesy:
  - základní předpoklady pro zavedení,
  - klasifikace a ochrana informací,
  - řízení dodavatelů,
  - řízení lidských zdrojů,
  - řízení změn,
  - řízení kontinuity činností,
  - audit kybernetické bezpečnosti [13];
- **technická** – návody pro zavedení opatření v oblastech:
  - fyzická bezpečnost,
  - řízení přístupů,
  - požadavky v oblasti ochrany před škodlivým kódem,
  - kybernetické bezpečnostní události a incidenty,
  - požadavky v oblasti aplikační bezpečnosti,
  - kryptografické prostředky,
  - požadavky v oblasti zajišťování úrovně dostupnosti informací,
  - požadavky v oblasti cloudových služeb,
  - a další požadavky [13].

1.4 Manažerská opatření

V části manažerské opatření minimální bezpečnostní standard definuje organizační, resp. procesní opatření.

1.4.1 Základní předpoklady pro zavedení

V úvodní fázi zavedení ISMS je potřebné zajistit souhlasný přístup ze strany vedení organizace, nadefinovat cíle ISMS, zdroje a časový harmonogram zavedení jednotlivých opatření.

Rozsah ISMS

Základním krokem při zavedení ISMS je stanovení **rozsahu ISMS**. V této části jsou definovány procesy potřebné pro řízení PDCA cyklu ISMS. Na základě vztahu ke stávajícímu systému řízení, cílům, struktuře organizace a aktivům, které jsou pro činnosti organizace využívána, jsou organizačně vymezené části společnosti, které jsou do ISMS zařazeny [14, str. 7-8].

Stanovení rozsahu ISMS se nedotýká jenom organizačního vymezení ale také určení systémů, které budou do systému řízení ISMS zahrnuty, a to včetně stanovení odpovědných osob. Při určení rozsahu je ISMS je důležité také začlenit nejen in-house aktiva, ale také aktiva, které se geograficky nenacházejí v prostorách organizace (např. datová centra, cloudové úložiště, mobilní zařízení pro vzdálený přístup) [2, str. 73-75].

Politika ISMS

Výsledným dokumentem v této fáze je **politika ISMS**. Dokument by měl obsahovat podporné stanovisko ze strany vedení organizace, stanovení cílů ISMS a také by měl být stanovený kontext řízení rizik v organizaci. Podstata zahrnutí rizik v této etapě netkví v úplném hodnocení aktiv, ale v popsání, resp. stanovení způsobů jakými organizace s riziky nakládá [15, str. 8]. Politika ISMS by měla být znovu schválená vedením organizace po tom, jako bude pro identifikována aktiva určena míra rizika – ta totiž určuje priority při zavádění jednotlivých bezpečnostních opatření. Politiku ISMS je možné rozpracovat do dalších detailnějších politik nebo je možné politiku/politiky zahrnout do již existující dokumentace organizace [14, str. 6].

1.4.2 Klasifikace a ochrana informací

Klasifikace znamená přirazení určitých informací k třídě. Informace bývají klasifikovány na základě **kritičnosti** (jak ztráta informace ovlivní procesy organizace), **citlivosti** (straty v případě vyzrazení informace nepovolané osobě) nebo kombinací obojího [15, str. 230-233]. Příklad klasifikační tabulky je uveden níže.

Tab. č. 1: Příklad klasifikační tabulky pro informace

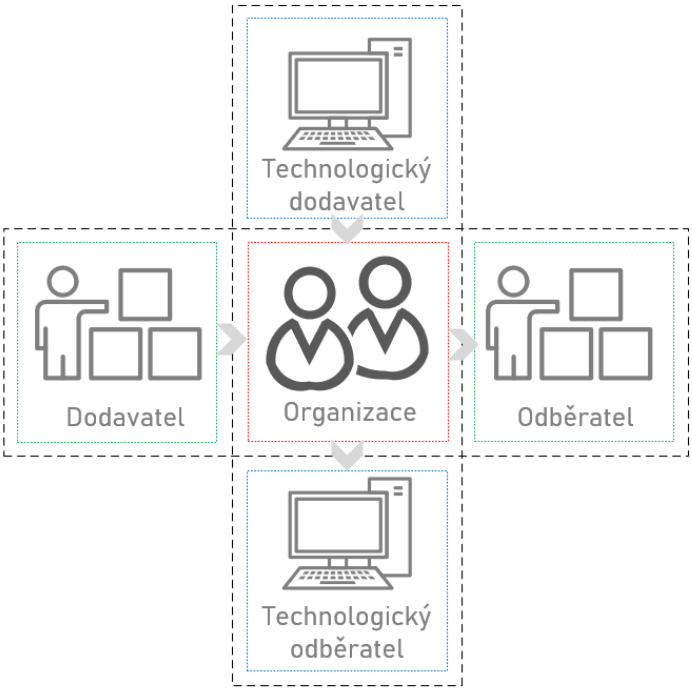
Klasifikace	Popis
Veřejné	- únik dat nezpůsobí dopad na procesy organizace - narušení důvěrnosti nebo dostupnosti neohrožuje činnost organizace
Interní	- vyžadují úplnost a přenosnost - je vyžadována kontrola integrity a ochrana před neautorizovanou modifikací anebo odstraněním - únik dat by mohl způsobit dopad na procesy organizace - při výpadku dostupnosti je nutné situaci řešit bez zbytečného odkladu
Citlivé	- únik dat způsobí vážný dopad na organizaci, ohrozí dobrou pověst organizace - při nedostupnosti organizace není schopna plnit základní funkce - narušení dostupnosti vede k ohrožení oprávněných zájmů organizace

Po zařazení informací do jednotlivých stupňů je potřebné stanovit pravidla, jakým způsobem bude s informacemi možné nakládat. Jedná se o opatření v oblasti:

- označení – označení dokumentů,
- manipulace – dodržovaní principů stanovených pro rozšiřování cílového publika,
- likvidace – jakým způsobem bude nakládáno s nosiči informací poté, až uplyne doba archivace,
- změny – jakým způsobem budou omezeny a evidovány změny dokumentů,
- zálohování – jak často a jakým způsobem bude prováděna záloha dat a následná kontrola čitelnosti záloh [13, str. 9].

1.4.3 Řízení dodavatelů

Organizace v současné době přicházejí do kontaktu s velkým množstvím jiných subjektů – přepojením vzniká ekosystém kybernetické bezpečnosti.



Obr. č. 4: Ekosystém kybernetické bezpečnosti [16, str.17]

Při stanovení a řízení požadavků na dodavatele v oblasti informační a kybernetické bezpečnosti by se nemělo zapomínat na tyto body:

- definování požadavků na kybernetickou bezpečnost prostřednictvím formální dohody (např. ve smlouvě) – při stanovení oblastí, které by měla smlouva obsahovat je možné vyjít z přílohy č.7 k VoKB a uplatnit relevantní body, které se smluvního vztahu dotýkají,
- uzavření dohody s dodavateli, jak budou tyto požadavky ověřovaný a validovány,
- ověření splnění požadavků na bezpečnost prostřednictvím stanovené metodiky (včetně prokazovaní seznámení osob dodavatele s bezpečnostními politikami organizace),
- v případě, že kybernetická bezpečnost (resp. její audit) je řešená externím subjektem, nemělo by se jednat o stejný subjekt, jako provozuje informační a komunikační systémy [16, str. 16] [13, str. 10-11].

V současné době množství společností využívá outsourcing, aby mohli své zdroje lépe soustředit na hlavní podnikatelskou činnost. Outsourcing služeb však neznamená outsourcing rizika (např. úniku dat). Jedním z možných mechanismů, jak zmírnit riziko související s outsourcingem je uzavření **smlouvy o úrovni služeb** (SLA – Service Level Agreement), kde poskytovatel garantuje určitou úroveň služeb [15, str. 164].

V případě, že poskytoval pracuje s důvěrnými nebo interními informacemi organizace je okrem SLA vhodné uzavřít **smlouvu o mlčenlivosti** (NDA – Non-disclosure agreement), zkontrolovat plán kontinuity podnikání poskytovatele a také zkontrolovat, zda je zajištěna smluvená úroveň zabezpečení a ochrany dat [15, str. 164].

1.4.4 Řízení lidských zdrojů

Řízení lidských zdrojů představuje systematické budování povědomí o zásadách kybernetické bezpečnosti mezi zaměstnanci. V této oblasti je potřebné sestavit plán rozvoje prohlubovaní bezpečnostního povědomí a také stanovit pravidla, jak se bude postupovat v případě porušení stanovených pravidel nebo politik. Je vhodné rozdělit zaměstnance na cílové skupiny dle profesní úrovně (uživatelé, administrátoři, managment, specialisti v oblasti kybernetické bezpečnosti apod.) [17, str. 124-125].

V pláně rozvoje je vhodné myslet také na tyto body:

- jakým způsobem budou vzdělávání nový zaměstnanci,
- v jakých intervalech budou školeni stávající zaměstnanci (dle cílových skupin),
- jaký bude obsah školení pro jednotlivé cílové skupiny,
- jak bude získávána zpětná vazba,
- stanovení odpovědných osob pro jednotlivé kroky [17, str. 124-125].

Jedním z využitelných systémů při budování kybernetické bezpečnosti je systém **Awareness, Training, Education (Povědomí, Tréning, Vzdělávaní)**. Cílem úrovně „Povědomí“ je zaměřit pozornost zaměstnanců na bezpečnostní otázky. Nejedná se o formální vzdělávaní, ale o po kouscích budovanou bezpečnostní gramotnost. Budování povědomí je možné rozdělit na budování povědomí všech zaměstnanců a na budování povědomí zaměstnanců pracujících s IT systémy. Úroveň „Tréning“ je zaměřena na bezpečnostní zručnosti pro jiné než bezpečnostní IT obory (např. administrátoři, vývojáři, auditoři). Úroveň „Vzdělávání“ se týče bezpečnostních specialistů a profesionálů – prohlubování jejich vzdělání a zkušeností v obore [18, str. 7-10].

1.4.5 Řízení změn

Řízení změn zahrnuje změny konfigurací, změny funkcí systémů (softwaru) a systémových komponent (hardwaru), provozních postupů, opravu zranitelností apod.

Řízení změn je potřebné rozlišovat od řízení konfigurací. Při řízení konfigurací se jedná o provozní proces, jehož cílem je zajistit, aby konfigurace odpovídali aktuálním hrozbám a provoznímu prostředí [15, str. 997-999].

Všechny změny v informačních nebo komunikačních systémech by měli být řízené. Je doporučen následující postup:

- **žádost o změnu**: odpovědnost za provedení změny by měla být připsána konkrétní osobě,
- **kontrola dopadu na CIA triádu**: kontrola osobou odpovědnou za výkon kybernetické bezpečnost,
- **rozhodnutí o změně**: pověřená autorita rozhodne, zda benefity vyplívající ze změny jsou v souladu s cílem organizace (po zvážení všech rizik),
- **dokumentace změny**: každá změna (i neprovedená) by měla být řádně zdokumentovaná, tj. měl by být o něj vytvořen záznam,
- **testování změny**: změna by měla být testována tak, aby byli odhaleny nepokryté stavy,
- **odsouhlasení změny**: autorita rozhode o akceptaci změny,
- **implementace** – změna je zavedena do produkčního prostředí pomocí stanoveného harmonogramu a pomocí alokovaných zdrojů,
- **report managementu**: souhrnný report by měl být představen managmentu [15, str. 997-999].

V procesu je možné také zvážit penetrační testovaní – jedná se službu, která slouží k hledání slabých míst v IT infrastruktuře zákazníka. Cílem penetračního testování je v tomto případě identifikovat slabá místa aktiv ještě před uvedením do provozu [13, str. 27].

1.4.6 Řízení kontinuity činností

Při řízení kontinuity činností je cílem zabezpečit pokračování činnosti organizace i v případě nepříznivých okolnosti. Plán kontinuity podnikání (Business Continuity Plan – BCP) je dokument, který popisuje, jak pokračovat v činnosti organizace v případě přerušení služeb [19, str.86-89].

Při tvorbě BCP je možné postupovat v několika krocích:

Vytvoření politiky kontinuity – obsahuje souhlasné stanovisko vedení organizace s vytvořením BCP v souladu s právními požadavky. Měla by obsahovat cíle, rozsah a role, které jsou za BCP zodpovědné [19, str.86-89].

Provedení analýzy dopadů na podnikání (Business Impact Analysis – BIA) – cílem tohoto kroku je identifikovat kritické služby, systémy a zdroje. Také by v této části měli být identifikovány hrozby a definované riziko. Je vhodné stanovit následující parametry:

- Maximální přípustní prostoje (Maximum Tolerable Downtime – MTD) – je doba, po jejž uplynutí dojde k významnému nenávratnému narušení funkce nebo činnosti organizace [19, str.86-89].
- Bod obnovení (Recovery Point Objective – RPO) – je bod v čase, který charakterizuje maximální množství dat, které můžou být případě nepříznivých událostí ztraceny [19, str.86-89].
- Čas obnovy (Recovery Time Objective – RTO) – je čas, za který bude proces nebo funkce obnovena do původního stavu. Platí, že RTO < MTD [19, str.86-89].

Identifikace preventivních opatření – vzhledem k již určeným rizikům, by měly být stanoveny a implementovány preventivní opatření [19, str.86-89].

Definice strategie v případě nepředvídatelných událostí – stanovení strategie v oblasti procesů, technologií, dodávek, dat apod. [19, str.86-89].

Vytvoření plánů v případě nepředvídatelných událostí – jedná se o vytvoření systému odezvy po havárii, plánů obnovení po havárii (Disaster Recovery Plan – DRP) včetně odpovědných osob [19, str.86-89].

Testování BCP – prověření planosti BCP a připravenosti všech zainteresovaných stran. Na základě testování je vhodné stanovit opatření ke zlepšení plánů BCP a také identifikovat oblasti, v které je možné dále vzdělávat pracovníky [19, str.86-89].

1.4.7 Audit kybernetické bezpečnosti

Dle § 16 VoKB audit nezávisle dokumentuje „*dodržování bezpečnostní politiky, včetně přezkoumání technické shody*“, dále pak „*posuzuje soulad bezpečnostních opatření s nejlepší praxí, právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky*

vztahujícími se k informačnímu a komunikačnímu systému a určí případná nápravná opatření pro zajištění souladu“ [20].

Vzhledem k tomu, že všechny komerční organizace nespadají pod ZoKB a VoKB, měli by si sami stanovit periodu pro provádění auditu (povinné osoby mají periodu stanovenou na dva nebo tři roky). Dále je pak vhodné provádět audit při významných změnách v jejich rozsahu nebo při výskytu významného kybernetického incidentu [13, str. 15].

Existuje několik typů auditů:

- **Fist party audit (audit první stranou)** – jedná se o audity, které vykonávají interní zaměstnanci. V tomhle případě interní auditorský tým prověřuje shodu vykonávaní procesů s interními nařízeními [21].
- **Second party audit (audit druhou stranou)** – audit je vykonáván u dodavatele. Tenhle druh externího auditu může vykonat buďto zákazník nebo zasmluvněný externí auditor [21].
- **Third party audit (audit třetí stranou**) – tenhle druh externího auditu je vykonáván certifikační autoritou. Může se jednat o prvotní, dozorové nebo recertifikační audity [21].

1.5 Technická opatření

V části technická opatření je minimální bezpečnostní standard orientován na opatření v oblasti informačních a komunikačních systémů, programového vybavení nebo fyzické bezpečnosti.

1.5.1 Fyzická bezpečnost

Oblast fyzické bezpečnosti je velmi úzce svázaná s kybernetickou bezpečností. Je to z toho důvodu, že opatření v této oblasti snižují nebo eliminují některé z vektorů útoku (např. neoprávněný vstup nebo neoprávněný zásah do systému). Fyzickou bezpečnost také uplatňuje principy defense-in-depth, co se projevuje v technických prostředcích, které je možné vhodně kombinovat např.:

- poplachové zabezpečovací a tísňové systémy,
- systémy kontroly vstupu,
- elektrické požární signalizace,
- kamerové systémy [22][23].

V možnosti ochrany z pohledu přístupu do chráněné oblasti můžeme technické prostředky ochrany rozdělit do následujících skupin:

- obvodová ochrana – ochrana zajišťující zabezpečení perimetru (stanovuje hranici systému); např. oplocení, brány, závory,
- plášťová ochrana – ochrana zajišťující zabezpečení vstupu do objektu; např. mříže, bezpečnostní dveře, fólie na sklo, senzory třískajícího skla,
- prostorová ochrana – ochrana prostoru ve vnitřku chráněného objektu; např. senzory pohybu, kamerové systémy, odposlechy,
- předmětová ochrana – v některých případech je možné využit ochranu konkrétních předmětů; např. trezory, laserové clony nebo seizmické senzory [22][23].

1.5.2 Řízení přístupů

Řízení přístupu představuje proces, při kterém je oprávněným subjektům (osobám, účtům, zařízením) povolen přístup k informačním aktivum. V oblasti řízení přístupu se uplatňuje pravidlo AAA (Authentication, Authorization, Accounting). Autentizace představuje proces, při kterém je ověřena identita subjektů; autorizace znamená povolení přístupu subjekt na základě oprávnění; účtování představuje zaznamenávaní aktivity subjektů.

Teorie řízení přístupu v oblasti řízení informací pracuje celkem s pěti možnými modely přístupu:

- Discretionary Access Control (DAC, volitelné řízení přístupu) – vlastnící informací rozhodují o tom, kdo má přístup k informacím,
- Mandatory Access Control (MAC povinné řízení přístupů) – systémy vynucují bezpečnostní politiky na základě štítkování (tagovaní) informací,
- Role-Based Access Control (RBAC, řízení přístupu pomocí rolí) – přístup k informacím je řízen na základě identity/role každého subjektu,
- Rule-Based Access Control (RBAC, řízení přístupu na základě pravidel) – předchozí model je rozšířen o další pravidla – např. časové omezení přístupu,
- Attribute-Based Access Control (ABAC, atributové řízení přístupu) – představuje řízení na základě atributů v systému, nejdetailnější způsob řízení přístupu [24].

1.5.3 Požadavky v oblasti ochrany před škodlivým kódem

Požadavky v této oblastí vedou ke snížení dopadu útoku za pomocí škodlivého kódu. Mezi základní možnosti ochrany řadíme nainstalovaný a pravidelně aktualizovaný antivir a oddělení sítě [13, str. 22].

Antivir je software, který ve svém principu identifikuje a případně odstraňuje škodlivý kód. Škodlivým kódem je na mysli např. viry, ransomware, malwary, spyware, trojské koně [25].

Oddělení sítě představuje metodu, kdy je na logické nebo fyzické úrovni oddělený síťový provoz – řešení omezuje rozsah dopadu škodlivého kódu. Na vrstvě L1 lze sítě oddělit pomocí fyzické separace (dedikovaná kabeláž a aktivní prvky). Na L2 je možné využít virtuální LAN – VLAN. VLAN rozděluje na logické úrovni síť na několik podsítí bez ohledu na fyzické zapojení. Oddělení sítě na L3 je možné prostřednictvím směrování a vytváření podsítí adresních prostorů [17, str. 96].

1.5.4 Kybernetické bezpečnostní události a incidenty

Bezpečnostní incident představuje stav, který nastal jako důsledek bezpečnostní události. Jedná se o „*narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnostních služeb anebo bezpečnosti a integrity sítí elektronických komunikací*“ [11].

V případě, že nastane bezpečnostní událost nebo incident, je vhodné mít sestaven plán zotavení po havárii (Disaster Recovery Plan – DRP). Jedná se o seznam kroků, podle kterých postupovat při obnovení dat, informací a systémů při výskytu incidentu případně události. Cílem plánu je poskytnutí podpory pro rychlé řešení incidentů a snížení prostojů [26].

1.5.5 Požadavky v oblasti aplikační bezpečnosti

Aplikační bezpečnost, jak již z názvu vyplývá, představuje bezpečnostní požadavky v oblasti samotných aplikací. Zabezpečení aplikací probíhá už během vývoje, testováním různých bezpečnostních funkcí, které zabraňují neoprávněnému přístupu, úpravám apod. [13, str. 27].

Oblasti aplikační bezpečnosti můžou výrazně pomoc penetrační testy, které probíhají i na produkčním prostředí. Co se týká různých akceptačních, integrační testů tak tyto testy probíhají právě na testovacím prostředí. Stanovují se speciální testovací kritéria pro testovací

data, navíc tyto data musí být zabezpečeny. Výsledky všech testů musí být vyhodnoceny a zaznamenány [13, str. 27].

1.5.6 Kryptografické prostředky

NÚKIB ve svém doporučení rozdělil jednotlivé kryptografické algoritmy mezi schválené a dosluhující. Mezi schválené algoritmy byly zařazeny ty, které jsou považovány za bezpečné ve střednědobém horizontu. Doporučení se vztahuje na symetrické šifry, asymetrické šifry a hašovací funkce [27].

1.5.7 Požadavky v oblasti zajišťování úrovně dostupnosti informací

Dostupnost představuje jeden z třech hlavních atributů bezpečnosti. Je možné ji vyjádřit jako:

$$\text{dostupnost} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}.$$

Mean Time Between Failures (MTBF) je parametr určující střední dobu mezi poruchami a Mean Time to Recovery (MTTR) je parametr pro střední dobu do obnovení [28].

1.5.8 Požadavky v oblasti cloudových služeb

Požadavek na dodavatele platí i v oblasti bezpečnosti cloudových služeb – vztahuje se na všechny modely bezpečnosti – infrastruktura jako služba, platforma jako služba, software jako služba. Bezpečnost dat v cloudu je možné rozdělit na dvě oblasti:

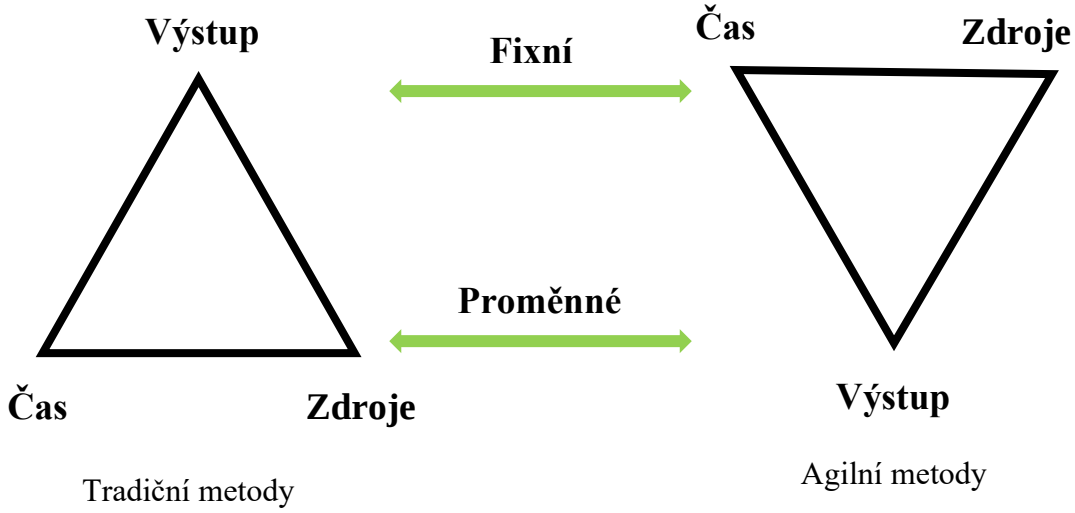
- datová bezpečnost – primárně zodpovědnost zákazníka,
- bezpečnost infrastruktury – primárně zodpovědnost poskytovatele [29].

2 AGILNÍ METODY

Agilní metody se zásadně liší od klasického projektového řízení. Hlavní myšlenky agilního vývoje spočívají v oproštění se od striktních procesů změny, zaměření se na reálný výsledek a na produkci dílčích funkčních výstupů. V agilním přístupu jde hlavně o komunikaci, spolupráci a připravenost na změnu. Agile se soustřední na spolupráci se zákazníkem a jeho vtáhnutí do procesu změny – na základě zpětné vazby se neustále přizpůsobuje vyvíjený produkt. Agile má schopnost reagovat na změny technologií, legislativy a dalších požadavků během projektu. Nevýhodami tohoto přístupu jsou vysoké nároky na koordinaci týmu, potřeba dobře sehraného a dedikovaný týmu z odborníků na jednotlivé oblasti [30, str.15].

K agilním metodám můžeme zařadit například tyto:

- SCRUM (blíže představen v další kapitole),
- Kanban (vizualizace procesů, minimalizace času potřebného na dokončení jednotlivých celků),
- Dynamic System Development Method (celý životní cyklus projektu) [30, str.15-26].



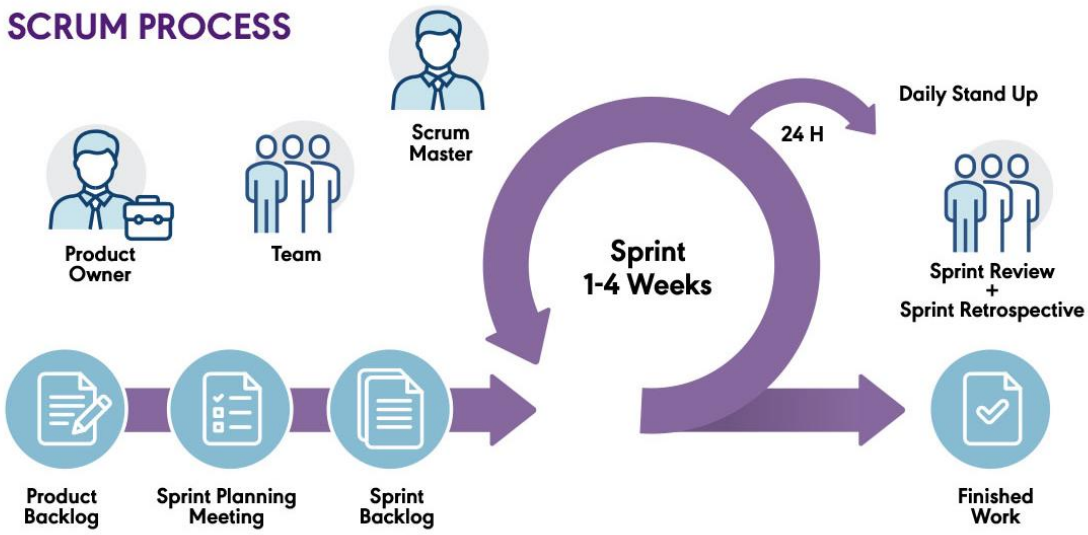
Obr. č. 5: Porovnání tradičních a agilních metod

2.1 SCRUM

SCRUM je nejvíce využívaná agilní metoda. Dá se definovat jako rámec, v kterém lidé mohou řešit složité problémy a produktivně a kreativně dodávat produkt a jeho

subdodávky. Jak již bylo zmíněno agile (a tedy i SCRUM) stojí na komunikaci a spolupráci se zákazníkem. Při dodávce produktu je potřeba znát požadavky zákazníka – požadavky musí být pochopitelné i pro implementační tým.

SCRUM dodává dílčí části projektu pomocí takzvaných iterací, které se jmenují sprint. Sprint trvá od 1 do 4 týdnů v závislosti na specifikaci projektu. Nejčastěji se využívá sprint o trvání 2 týdnů. Tým se orientuje pouze na cíl sprintu, který tvoří dodávku dílčí části projektu. Pokud dílčí část projektu není tým schopný dodat v rámci sprintu, znamená to, že se musí rozdělit ještě na menší části. Dílčí části projektu jsou zaznamenány v backlogu – řazení v rámci backlogu probíhá na základě prioritizace. V rámci sprintu má každý člen rozdělené svoje úkoly. Tým se schází pravidelně na operativních poradách tzv. daily stand-up [30, str.26].



Obr. č. 6: Scrum proces [31]

2.1.1 Epic

Pod názvem Epic se v rámci metodiky SCRUM rozumí projekt, který je definován. V některých případech se dá projekt rozdělit do více epiců – záleží na specifikaci projektu. Epic zastřešuje jednotlivé user story, přičemž nelze zaplánovat do sprintu [32].

2.1.2 User story

User story je dílčí část epicu. Při vytváření user story se dodržuje formát *„já jako uživatel chci funkcionalitu, abych dosáhl business value“*. Z toho vyplývá, že user story musí být jednoznačně definovaná, relativně nezávislá a musí přinášet hodnotu. Zároveň se nesmí

zapomenout, že user story musí být dostatečně malá, aby ji bylo možné dodat v rámci sprintu [32].

2.1.3 Sprint

V rámci SCRUMu je trvání sprintu konzistentní, a to o délce 2-4 týdny. Zvolení délky sprintu začíná v rané fázi projektu. Sprint umožňuje určitou formu předvídatelnosti, a to pomocí kontroly. Každý sprint můžeme považovat za krátký projekt. Na plánování sprintu, se podílí celý tým. Za dodávku sprintu odpovídá product owner [33].

2.1.4 Backlog

Backlog si můžeme ve SCRUMu představit jako seznam potřebných úkolů, které čekají na splnění. Pracuje se se dvěma typy backlogů:

- product backlog – kompletní seznam dílčích úkolů pro dokončení projektu,
- sprint backlog – seznam úkolů, které je potřeba splnit v rámci daného sprintu [33].

2.1.5 Velocity

Velocity představuje týmovou kapacitu práce. Do velocity týmu se musí počítat s plánovanou dovolenou, určitou mírou rizika onemocnění, protože tyto vlivy způsobují snížení kapacity týmu.

Velocity souvisí s pracností jednotlivých user-story. Pracnost se odhaduje pomocí Fibonacciho posloupnosti – obvykle v rozmezí 1-13. Do sprintu se přidávají jednotlivé user-story – součet jejich pracnosti vypovídá o celkové velocitě týmu za daný sprint. V případě nedodržení cíle sprintu si tým musí velocitu snížit [33].

2.1.6 Daily stand-up

Daily stand-up je každodenní schůzka, na které se sejde celý tým. Každý člen týmu sdělí, co stihl udělat předchozí den a na čem hodlá pracovat dnes. Účelem této schůzky je sdílení informací a plnění plánu v rámci dne. Zároveň daily stand-up představuje prostor pro sdělení pracovních překážek, které se mohou řešit přednostně. Z povahy schůzky vyplývá, že probíhá každé ráno na začátku pracovní doby. Na schůzce by se neměli řešit problémy, jedná se čistě o informační schůzku [30, str. 107].

2.1.7 Sprint review

Sprint review představuje předání dílčí části projektu, který tým zvládl za jeden sprint. Agilní tým předloží dílčí část projektu zákazníkovi, který rozhodne o akceptaci či neakceptaci výsledů. Výsledek se dá akceptovat pouze za předpokladu, že je splněn na 100 %. Nedodělky je možné opravit do konce sprintu. Pokud se to nepodaří, úkol se přesouvá zpátky do backlogu a určuje se mu nová priorita řešení [30, str. 125].

2.1.8 Retrospektiva

Retrospektiva je porada agilního týmu na konci sprintu, kde se hodnotí uplynulý sprint – zpětné ohlédnutí za věcmi, které se nepovedly nebo povedly. Výstupem je seznam věcí, které fungují a nefungují. Druhou částí retrospektivy je zamýšlení se nad tím jak věci, které nefungují zlepšit [33].

2.1.9 SCRUM tým

Velikost SCRUM týmu je maximálně 9 lidí, kteří mají na starost hlavní dodávku projektu. Dále by měl být členem týmu SCRUM master a product owner. SCRUM master má roli mezičlánku mezi týmem a okolím. Cílem jeho práce je vytvořit samo-organizující tým, který je spolehlivý a samostatný. SCRUM master napomáhá týmů dosahovat cílů a motivuje ho k lepším výsledkům. Má na starosti řešení konfliktů a stará se o to aby SCRUM proces byl efektivní. [31, str. 43-46,49-54]

Role product owner se doslovně dá přeložit jako vlastník produktu. Stará se o vizi celého projektu, je mezi článkem mezi týmem, zákazníkem a společností. Zodpovídá za plnění product backlogu a v rámci backlogu určuje také priority. Dá se říct, že na základě prioritizace řídí celý projekt [31, str. 47-48].

II. PRAKTICKÁ ČÁST

3 ZAVEDENÍ ISMS

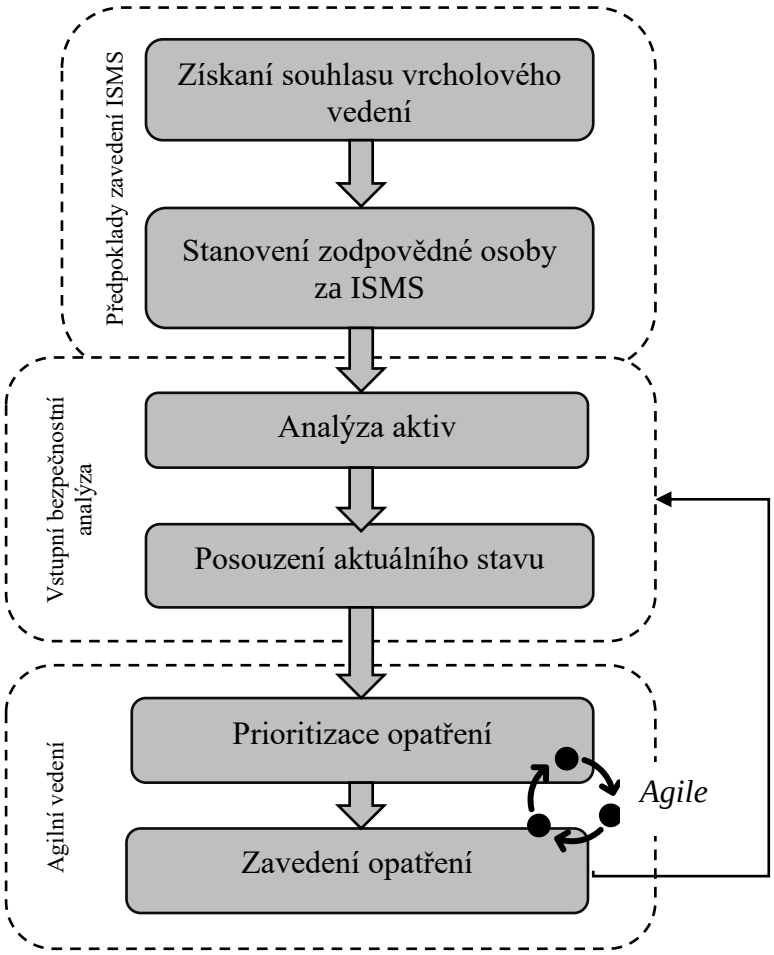
V rámci praktické části bude vytvořen metodický postup pro zhodnocení základního stavu bezpečnosti pro středně velké organizace, tj. pro subjekty nespadající pod regulaci zákona o kybernetické bezpečnosti. Postup bude vycházet z následujících bezpečnostních rámců a norem:

- **Rodina standardů ISO/IEC 27000**:
  - rodina mezinárodních standardů pro řízení informační bezpečnosti (Information Security Management),
  - podklady k navrhování, implementování a provozováni systému ISMS,
- **NIST SP 800-53B:**
  - publikace amerického NISTu uvádějící kontrolní procedury pro informační systémy a organizace,
- **Minimální bezpečnostní standard**:
  - podpůrný materiál NÚKIB a NAKIT pro subjekty nespadající pod ZoKB/VoKB,
- **Metodika pro minimální bezpečnostní opatření kategorie I – Analýza rizik:**
  - Metodika analýzy rizik vydána ministerstvem investicí, regionálního rozvoje a informatizace Slovenské republiky,
- **ZoKB a VoKB**.

3.1 ISMS

Proces ISMS je zobrazen na následujícím obrázku a skládá se z několika podprocesů:

- předpoklady zavedení ISMS:
  - získaní souhlasu vrcholového vedení,
  - stanovení zodpovědné osoby za ISMS,
- vstupní bezpečnostní analýza:
  - analýza aktiv,
  - posouzení aktuálního stavu,
- agilní vedení:
  - prioritizace opatření,
  - zavedení opatření.



Obr. č. 7: Podprocesy ISMS

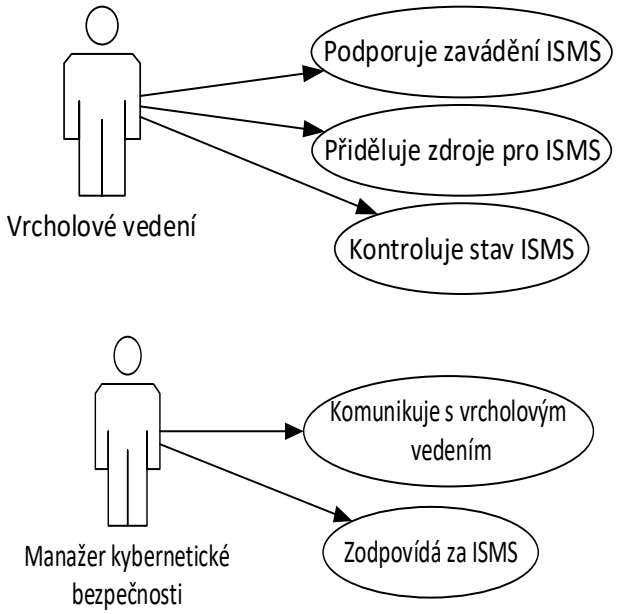
3.2 Předpoklady zavedení ISMS

Před tím, než začne společnost řídit informační bezpečnost, je nutné získat souhlas a podporu vrcholového vedení so systematickým přístupem v této oblasti. Systém ISMS předpokládá, že vrcholové vedení vyčlení pro tuto oblast finanční, technické a personální zdroje.

V oblasti lidského zabezpečení musí být minimálně stanovená osoba zodpovědná za kybernetickou bezpečnost (např. manažer kybernetické bezpečnosti). Je možné stanovit i další bezpečnostní role – u subjektů neregulovaných ZoKB a VoKB to však není nezbytně nutné. Manažer kybernetické bezpečnosti může mít v náplni práce i další činnosti, avšak role není slučitelná s rolemi, které zodpovídají za provoz ICT.

3.2.1 Seznam rolí

V podprocesu splnění předpokladů zavedení ISMS vystupují následující role.



Obr. č. 8: Základní role procesu ISMS

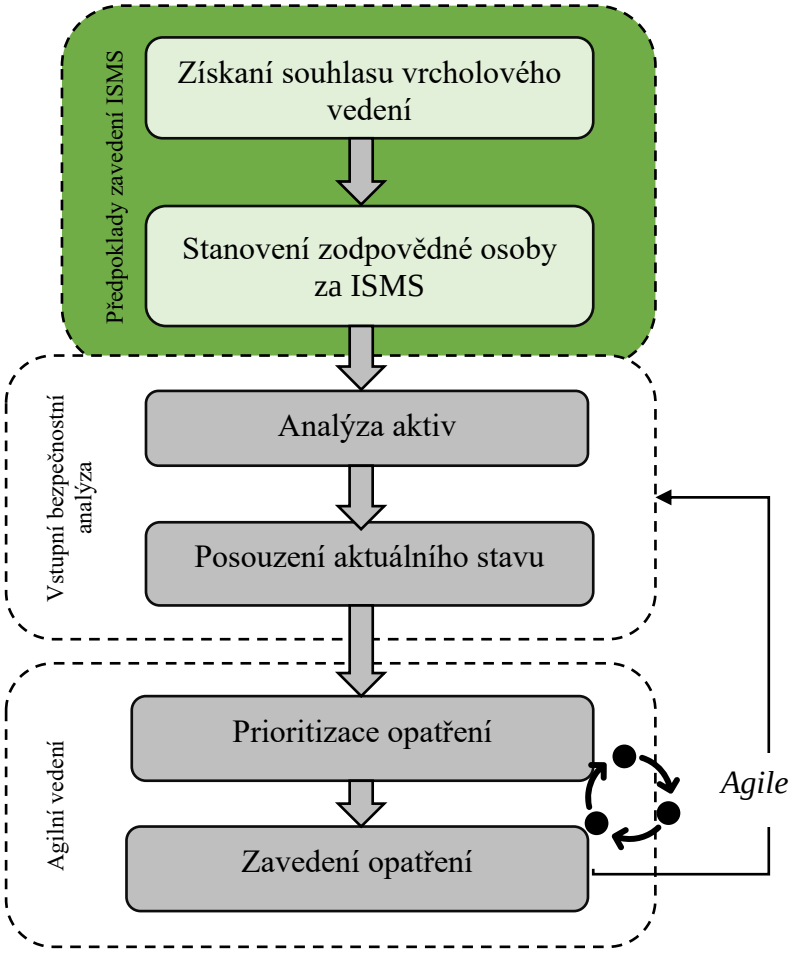
Zodpovědnost jednotlivých rolí v rámci procesu je možné vyjádřit také v podobě RACI matice.

Tab. č. 2: Základní role procesu ISMS

	Vrcholové vedení	Manažer kybernetické bezpečnosti
Vydání souhlasného stanoviska se zavedením ISMS (podpora zavedení ISMS)	A	I
Přidělení zdrojů pro ISMS	A, R	C
Kontrola stavu ISMS	A, R	C
Komunikace s vrcholovým vedením	C	R, A
Odpovědnost za zavedení ISMS	I	R, A

3.2.2 Stav podprocesů po naplnění předpokladů ISMS

Po získání souhlasu vrcholového vedení a stanovení zodpovědné osoby za ISMS pokračuje proces zavedení ISMS vstupní bezpečností analýzou – viz. následující obrázek.

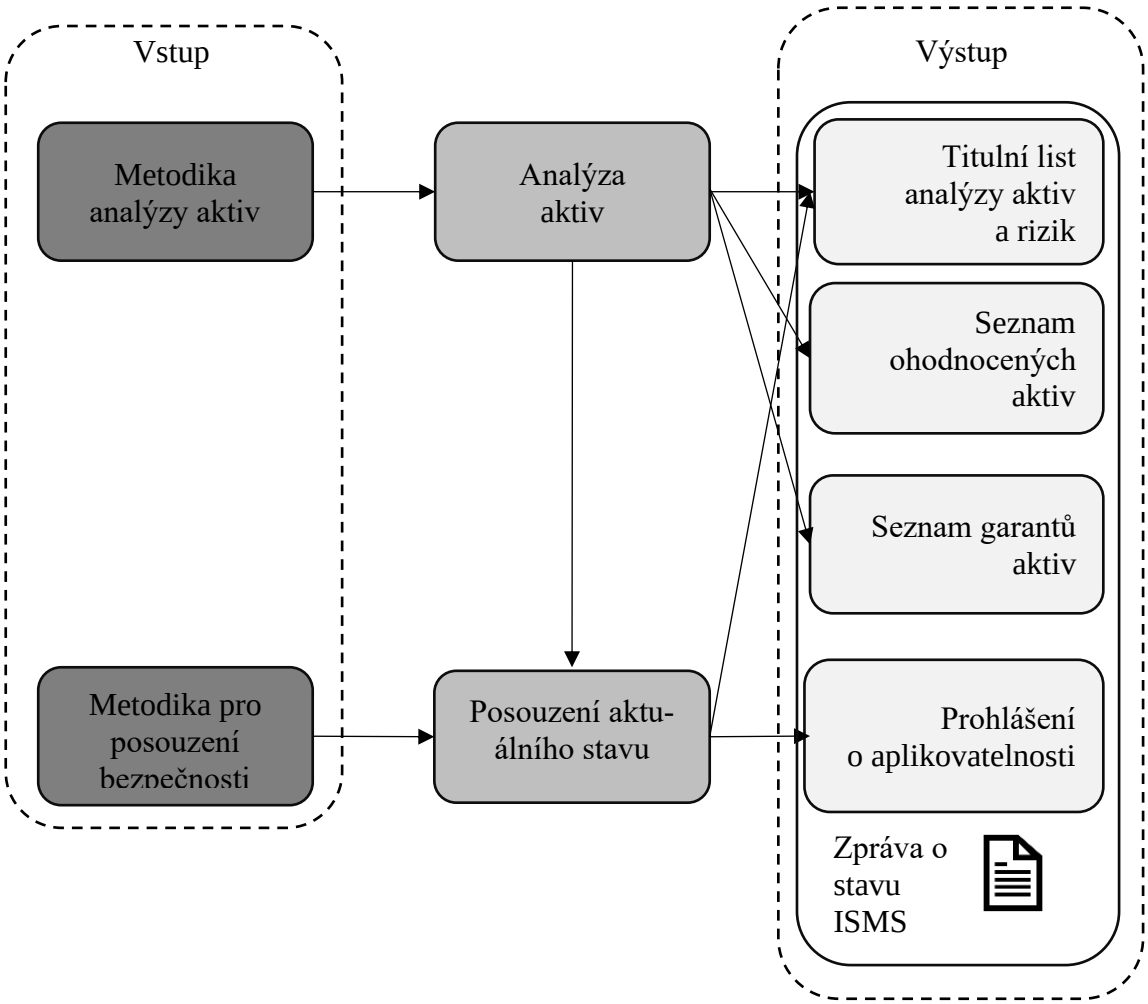


Obr. č. 9: Stav vstupních procesů po naplnění předpokladů ISMS

3.3 Vstupní bezpečnostní analýza

Východiskovým bodem pro zavádění kybernetické bezpečnosti bude vstupní analýza aktiv a posouzení aktuálního stavu bezpečnosti v organizaci. Na základě této analýzy je pak možné stanovit opatření vedoucí ke zlepšení aktuálního stavu. Uvedený postup vychází z předpokladu, že podnik začíná se zavedením kybernetické bezpečnosti formou sebeposouzení. Bezpečnostní analýzu je po zavedení ISMS potřebné vykonávat v pravidelných intervalech např. 1x ročně.

Procesy vstupní bezpečnostní analýzy jsou zobrazeny na obrázku níže. Podprocesy jsou rozepsány v následujícím textu.



Obr. č. 10: Procesy vstupní bezpečností analýzy

Podprocesy vstupní analýzy rizik jsou blíže zpracování na následujícím obrázku. Jedná se o podprocesy:

- analýza aktiv,
- posouzení aktuálního stavu.

Před tím, než podnik začne s analýzou, je potřebné stanovit metodiku, která bude obsahovat postup pracovní činnosti. Vstupní bezpečnostní analýzu je vhodné provádět v tabulkovém procesoru (např. Microsoft Excel), kde je možné pracovat s rozevíracími seznamy, automatickými výpočty, filtrováním nebo dynamickým podbarvením, co zjednodušuje následné vyhodnocení. Při tvoření bezpečností analýzy spolupracuje manažer kybernetické bezpečnosti s garantem aktiva, který představuje rolu zodpovědnou za zajištění rozvoje, použití a bezpečnosti aktiva. Garant aktiva může k analýze přizvat také jiné role např. administrátora systémů.

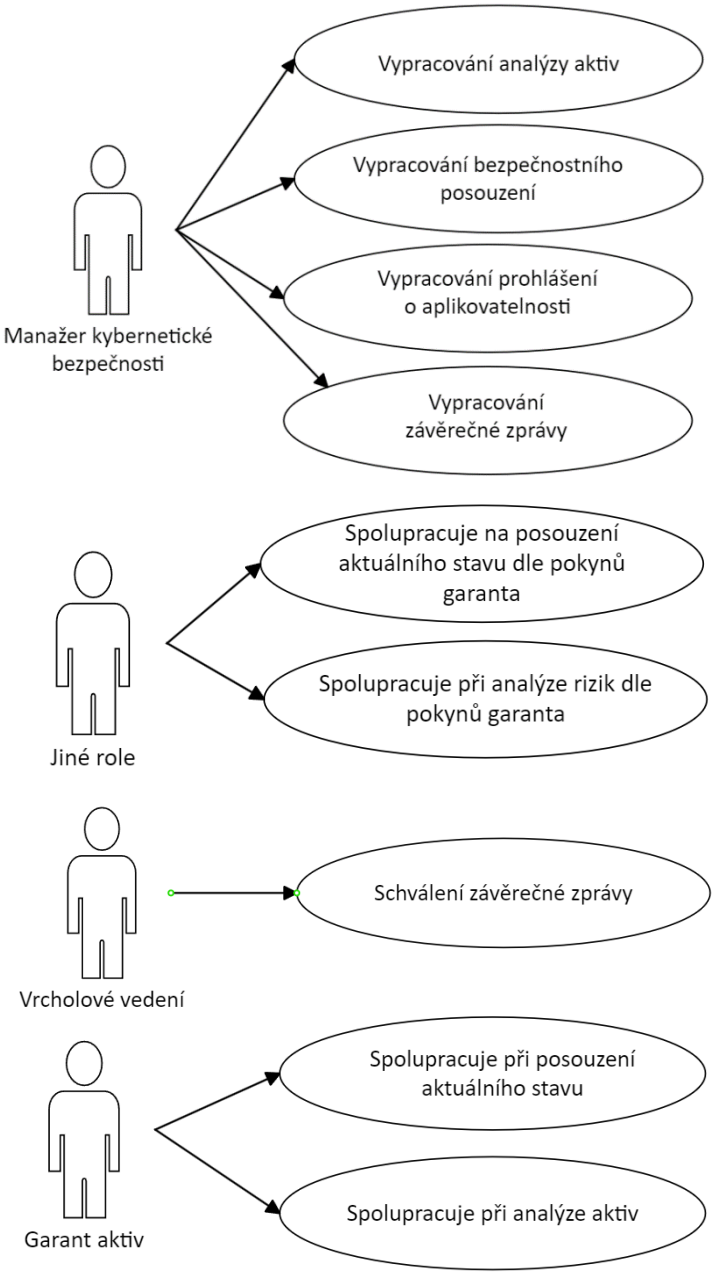
Výstupní řízený dokument by měl obsahovat minimálně s následujícími výstupy:

- titulní list – obsahuje základní údaje o řízeném dokumentu,
- seznam aktiv – seznam identifikovaných a ohodnocených aktiv,
- seznam garantů aktiv,
- zhodnocený stav bezpečnosti – výsledek plnění opatření z checklistu.

Závěry bezpečnostní analýzy je potřebné prezentovat a reportovat vrcholovému vedení. K tomuto účelu je možné sestavit zprávu o hodnocení aktiv ISMS, která bude obsahovat agregované výsledky. Dokument je schválen vrcholovým vedením po seznámením se s jeho obsahem.

3.3.1 Seznam rolí

V podprocesu vstupní bezpečnostní analýzy vystupují následující role.



Obr. č. 11: Seznam rolí vstupní bezpečnostní analýzy

Zodpovědnost jednotlivých rolí v rámci procesu je možné vyjádřit také v podobě RACI matice.

Tab. č. 3: Seznam rolí vstupní bezpečnostní analýzy

	Vrcholové vedení	Manažer kybernetické bezpečnosti	Jiné role (správce, administrátor)	Garant aktiv
Vypracování analýzy aktiv	I	A, R	C	C
Vypracování bezpečnostního posouzení	I	A, R	C	C
Vypracování zprávy	I	A, R	C	C
Schválení zprávy	A, R	C	C	C

3.3.2 Metodika analýzy aktiv

Analýza aktiv představuje proces, při kterém jsou identifikované a ohodnocené všechny aktiva, a to včetně jejich garantů. Na základě tohoto kroku je stanoven rozsah řízení ISMS společnosti.

Proces řízení aktiv je čtyřkrokový:

- vyplnění titulního listu (společný dokument pro bezpečnostní analýzu),
- identifikace všech primárních a podpůrných aktiv,
- ohodnocení všech aktiv,
- stanovení garantů aktiv.

Titulní list

Titulní list obsahuje základní údaje o řízeném dokumentu s názvem Bezpečnostní analýza společnosti. Návrh pro vzor titulního listu je uveden v následující tabulce.

Tab. č. 4: Návrh titulního listu vstupní analýzy rizik a aktiv

Bezpečnostní analýza společnosti *(doplňte obchodní jméno společnosti)*			
Identifikátor dokumentu:			
Místo uložení čistopisu:			
Datum zpracování:			
Datum vydání:			
Garant dokumentu:			
Autorizace dokumentu			
	Jméno, příjmení, název pozice	Podpis	
Zpracoval:			
Schválil:			
Změnové řízení dokumentu			
Číslo revize	Popis změn	Zpracovatel změny	Datum změny
1.0	Výchozí dokument		

Identifikace aktiv

Identifikace aktiv musí být provedená minimálně v následujícím rozsahu:

- **Primární aktiva**:
  - služba – služba poskytovaná informačním systémem, je potřebná pro fungování organizace (např. objednání zboží z e-shopu),
  - informace – informace, které informační systém zpracovává nebo poskytuje.

- **Podpůrné aktiva**:
    - hardware – fyzické vybavení společnosti (pracovní stanice – stolové, přenosné, mobilní zařízení, všechny druhy serverů, firewallů, routerů, datových uložišť, kabelážní systémů apod.),
    - software – programové a aplikační vybavení společnosti,
    - objekty – budovy, prostory, areál, ve kterých jsou aktiva uložena,
    - jiné podpůrné technické prostředky – napájení, klimatizace, systémy kontroly vstupu apod.,
    - pracovníci – uživatelé, administrátoři a jiné role bezpečnostním přesahem,
    - organizace – pravidla, směrnice, dokumentace, organizační schéma,
    - dodavatelé – dodavatelé podílejíce se na provozu, rozvoj a správě HW a SW.

Příklad výstupu identifikace aktiv je uveden v následující tabulce.

Tab. č. 5: Příklad části seznamu aktiv

ID Aktiva	Název aktiva	Typ aktiva	Druh aktiva	Popis	Datum identifikace
E-01	Objednání zboží z e-shopu	Primární	Služba	Proces objednání zákazníkem	
E-02	Informace o zboží	Primární	Informace	Informace o dostupném zboží	
E-HW01	Webový server	Podpůrné	Hardware		
E-HW02	Kabelážní Systém	Podpůrné	Hardware		
E-SW01	Databáze e-shopu	Podpůrné	Software		
E-SW02	Operační Systém	Podpůrné	Software		
E-OB01	Serverovna	Podpůrné	Objekty		
E-PP01	Klimatizace – Serverovna	Podpůrné	Jiné podpůrné prostředky		
E-PR01	Administrátoři	Podpůrné	Pracovníci		
E-OR01	Dokumentace Databáze	Podpůrné	Organizace		
E-DO01	Správci HW	Podpůrné	Dodavatelé		

Ohodnocení aktiv

Všechny identifikována aktiva je potřebné ohodnotit pomocí kvalitativní analýzy z pohledu jejich důležitosti. Při hodnocení je potřebné zohlednit dopad narušení bezpečnosti, a to včetně nákladů potřebných na uvedení systémů do původního stavu.

Hodnocení aktiv bude různé pro primární a podpůrná aktiva.

Pro primární aktiva se hodnocení bude řídit přílohou č. I Vodítka pro hodnocení dopadů (podpůrný materiál NÚKIB). Dle uvedeného budou využity čtyři klasifikační stupně – uvedené v následující tabulce.

Tab. č. 6: Klasifikační stupnice

Klasifikační stupeň dopadu
Kritický
Vysoký
Střední
Nízký

Příklad části ohodnocených primárních aktiv je uveden v následující tabulce.

Tab. č. 7: Příklad ohodnocených primárních aktiv

ID aktiva	Hodnota primárního aktiva
E-01	Kritická
E-02	Kritická
E-HW01	Vysoká
E-DO01	Střední

Pro **podpůrné aktiva** budou využité stupnice přílohy k vyhlášce č. 82/2018 Sb. s názvem hodnocení aktiv– uvedena v příloze 2. Podpůrná aktiva budou hodnocené na základě třech parametrů:

- integrita – zachování konzistentnosti informací,
- důvěrnost – informace jsou přístupné jen tomu, kdo je oprávněn s nimi nakládat,
- dostupnost – narušení dostupnosti služeb, dostupností informací.

Výslední hodnota podpůrného aktiva bude určena výběrem nejvyššího stupně z ohodnocené integrity, důvěrnosti a dostupnosti. Hodnota podpůrného aktiva by měla především odrazit jeho dopad na primární aktiva. Příklad hodnoty podpůrných aktiv je uveden v následující tabulce.

Tab. č. 8: Příklad ohodnocených podpůrných aktiv

ID aktiva	Dostupnost	Důvěrnost	Integrita	Hodnota podpůrného aktiva
E-HW01	4 Kritická	1 Nízká	3 Vysoká	4 Kritická
E-DO01	4 Vysoká	2 Střední	1 Nízká	4 Vysoka

Stanovení garantů aktiv

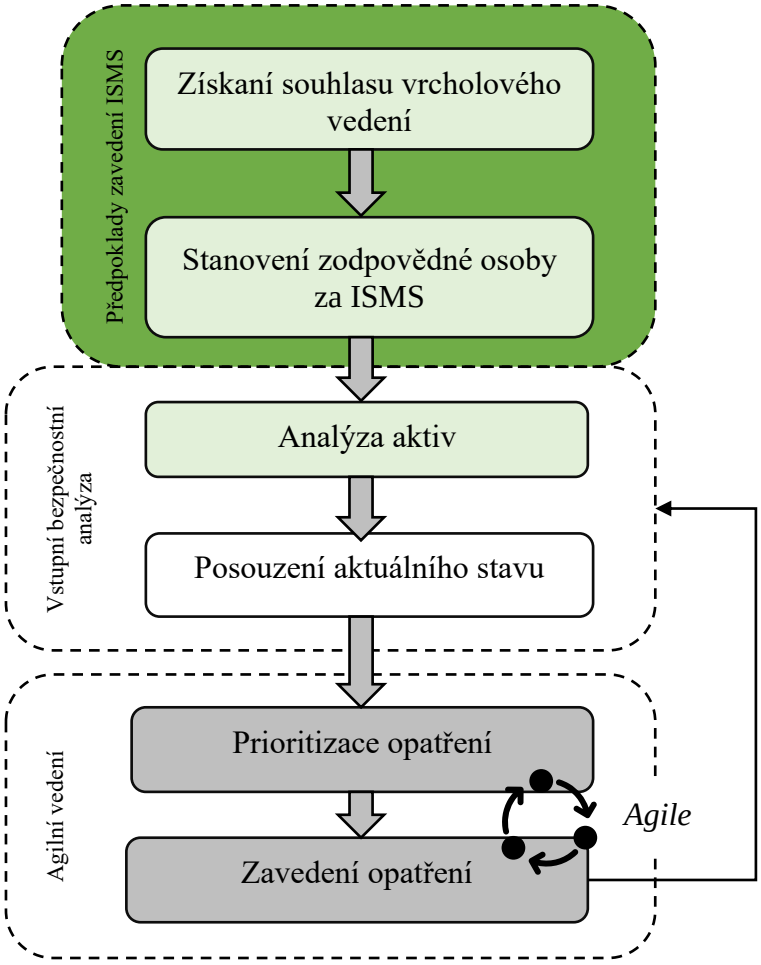
Posledním krokem analýzy aktiv je stanovení garantů aktiv pro všechny identifikovaná primární aktiva. Tuto roli je vhodné stanovit pomocí názvu pozice zodpovědného zaměstnance. V případě personální změny není při takto stanovených garantech nutné měnit řídící dokumenty. Příklad stanovení garantů je uveden v následující tabulce.

Tab. č. 9: Příklad stanovení garantů aktiv pro identifikovány primární a podpůrná aktiva

ID aktiva	Garant aktiva
E-01	Vedoucí útvaru nákupu
E-02	Vedoucí útvaru nákupu

3.3.2.1 Stav podprocesů po provedení analýzy aktiv

Po provedení analýzy aktiv pokračuje proces vstupní bezpečností analýzy posouzením aktuálního stavu ISMS– viz. následující obrázek.



Obr. č. 12: Stav naplnění procesů po vykonání vstupní bezpečnostní analýzy

3.3.3 Metodika posouzení aktuálního stavu bezpečnosti

Posouzení aktuálního stavu bezpečnosti bude probíhat v manažerské a technické oblasti, kterých bližší specifikace je uvedená v následující tabulce. Její struktura vyplývá z minimálního bezpečnostního standartu.

Tab. č. 10: Struktura vstupního posouzení ISMS

Oblasti hodnocení bezpečnostních rizik	
A. Manažerská oblast	**B. Technická oblast**
A.1 Základní předpoklady	B.1 Fyzická bezpečnost
A.2 Klasifikace a ochrana informací	B.2 Řízení přístupů
A.3 Řízení kontinuity činností	B.3 Požadavky v oblasti ochrany před škodlivým kódem
A.4 Řízení změn	B.4 Požadavky v oblasti aplikační bezpečnosti
A.5 Řízení dodavatelů	B.5 Kryptografické prostředky
A.6 Řízení lidských zdrojů	B.6 Požadavky v oblasti zajišťování úrovně dostupnosti informací
A.7 Audit kybernetické bezpečnosti	B.7 Požadavky v oblasti cloudových služeb
	B.8 Jiné

Každá podoblast (např. A.3 Řízení dodavatelů) bude hodnocena na základě checklistu s dvěma možnými odpověďmi – splněno/ nesplněno. Závěrečné hodnocení plnění jednotlivých oblastí je stanoveno dle vzorce:

$$\frac{\text{Počet plněných položek v oblasti}}{\text{Počet všech v položek v oblasti}} * 100\ [\%].$$

Checklisty pro jednotlivé oblasti jsou uvedeny v následujících tabulkách.

Tab. č. 11: Checklist podoblast A.1 Základní předpoklady

A.1	Základní předpoklady	Plněno
A.1.1	Existuje interní řídící dokumentace – ***manažerská oblast*** (klasifikace a ochrana informací, řízení dodavatelů, řízení lidských zdrojů, řízení změn, řízení kontinuity činností, audit kybernetické bezpečnosti). Dokumentace je schválená vrcholovým vedením.	
A.1.2	Existuje interní řídící dokumentace – ***technická oblast*** (fyzická bezpečnost, řízení přístupů, požadavky v oblasti ochrany před škodlivým kódem, požadavky v aplikační bezpečnosti, kryptografické prostředky, požadavky v oblasti zajišťováni úrovně dostupnosti informací, požadavky v oblasti cloudových služeb). Dokumentace je schválená vrcholovým vedením.	
A.1.3	Existuje interní řídící dokumentace – ***prohlášení o aplikovatelnosti*** *a* ***plán zavádění bezpečnostních opatření.***	
A.1.4	Pro interní řídící dokumentaci (manažerská oblast, technická oblast, prohlášení o aplikovatelnosti, plán zavádění bezpečnostních opatření) je stanoven interval aktualizace a dokumentace je v tomto intervalu pravidelně aktualizována.	
A.1.5	Je pravidelně vykonávaná analýza aktiv.	

Tab. č. 12: Checklist podoblast A.2 Klasifikace a ochrana informací

A.2	Klasifikace a ochrana informací	Plněno
A.2.1	Je stanovená osoba odpovědná za veřejný kontent a kontent je oprávněnou osobou kontrolován před zveřejněním.	
A.2.2	Je kontrolován veřejně přístupný obsah, odstraňují se neveřejné informace dostupné z veřejně přístupného internetu.	
A.2.3	Uložené/ zpracovávané/ přenášené informace jsou kategorizovány a řádně označeny.	
A.2.4	Jsou stanovené pravidla pro manipulaci/ likvidaci/ zálohování nebo změny klasifikovaných informací.	
A.2.5	Jsou využívané technické opatření při manipulaci/ likvidaci/ změně klasifikovaných informací.	

Tab. č. 13: Checklist pro podoblast A.3 Řízení kontinuity činností

A.3	Řízení kontinuity činností	Plněno
A.3.1	V interní řídící dokumentaci je popsán systém záloh (co bude zálohováno, kdy, jak dlouho bude záloha uchována, kolik záloh bude uchovaných, kdo zálohu vykoná).	
A.3.2	Existuje alespoň jedna off-line záloha.	
A.3.3	Informace jsou pravidelně zálohovány dle pravidla 3-2-1 (tři zálohy, na dvou místech, z toho minimálně jedna off-line).	
A.3.4	Zálohy chráněných/citlivých informací jsou šifrované.	
A-3.5	Existuje systém ochrany integrity záloh (digitální podpis nebo heš zálohy).	
A.3.6	Čitelnost záloh je pravidelně testována.	
A.3.7	Existuje plán kontinuity podnikání (Business Continuity Plan – BCP).	
A.3.8	Existuje plán zotavení po havárii (Disaster Recovery Plan – DRP).	
A.3.9	Je stanoven interval pro testování BCP a DRP plánů a v tomhle intervalu jsou plány testovány.	
A.3.10	Existují postupy pro hlášení bezpečnostních incidentů/ událostí.	
A.3.11	Existují postupy pro řešení bezpečnostních incidentů/ událostí (včetně eskalace situace).	

Tab. č. 14: Checklist pro podoblast A.4 Řízení změn

A.4	Řízení změn	Plněno
A.4.1	Jsou analyzovány změny z hlediska dopadu do bezpečnosti.	
A.4.2	Změny jsou dokumentovány (včetně změn konfigurace).	
A.4.3	V případě potřeby jsou přijata opatření za účelem snížení dopadů spojených se změnami.	
A.4.4	Při změnách je zajištěná možnosti obnovy do původního stavu.	
A.4.5	Změny jsou před nasazením testovány.	

Tab. č. 15: Checklist A.5 Řízení dodavatelů

A.5	Řízení dodavatelů	Plněno
A.5.1	V dodavatelských vztazích jsou vymáhaný relevantní bezpečností požadavky.	
A.5.2	Pro provoz relevantních systémů je vztah s dodavateli řízen pomocí SLA.	

Tab. č. 16: Checklist pro podoblast A.6 Řízení lidských zdrojů

A.6	Řízení lidských zdrojů	Plněno
A.6.1	Je určen manažer kybernetické bezpečnosti.	
A.6.2	Administrátoři a osoby zastávající bezpečnostní role mají uzavřenou dohodu o mlčenlivosti (NDA – Non-disclosure agreement).	
A.6.3	Zaměstnanci jsou v oblasti bezpečnosti školení formou vstupního a pravidelného školení (včetně manažerů).	
A.6.4	Bezpečnostní role a IT zaměstnanci jsou pravidelně školení odborným a specializovaným školením (v oboru a také v oblasti bezpečnosti).	
A.6.5	Existují sankční postupy při nedodržování zavedených bezpečnostních zásad.	

Tab. č. 17: Checklist pro podoblast A.7 Audit kybernetické bezpečnosti

A.7	Audit kybernetické bezpečnost	Plněno
A.7.1	Je stanoven auditor kybernetické bezpečnosti (i externí subjekt).	
A.7.2	Auditor kybernetické bezpečnosti je nezávislou osobou od provozních nebo bezpečnostních rolí.	
A.7.3	Je prováděno nezávislé hodnocení dodržování bezpečnostních politik.	
A.7.4	Jsou prováděné nezávislé bezpečnostní technické kontroly (např. penetrační testování).	
A.7.5	Výsledky auditů jsou zohledňovány při návrhu bezpečnostních opatření.	

Tab. č. 18: Checklist pro podoblast B.1 Fyzická bezpečnost

B.1	Fyzická bezpečnost	Plněno
B.1.1	Zařízení jsou umístněná ve vhodném prostředí. V případě zhoršeného prostřední (voda, prach, teplo apod.) probíhá monitorování environmentálních podmínek.	
B.1.2	Existuje systém pro detekci požáru, potlačení požáru.	
B.1.3	Existuje systém pro potlačení úniku vody (dostupnost uzavíracích ventilů). Ventily jsou funkční a personál je znalí obsluhy.	
B.1.4	Jsou aplikována technická opatření ochrany perimetru (např. kamerový systém).	
B.1.5	Vstupu do chráněných oblastí je řízen (např. zamykání dveří, přístupový systém).	
B.1.6	Existuje postup řešení ztráty autentizačních faktorů (např. ztráta klíčů).	
B.1.7	Existuje nezávislý zdroj napájení (např. UPS).	

Tab. č. 19: Checklist pro podoblast B.2 Řízení přístupů

B.2	Řízení přístupů	Plněno
B.2.1	Existují dohody o přístupu zaměstnanců k zařízením (např. dohoda o přijatelném užívaní/ / pravidla chování).	
B.2.2	Po ukončení pracovního poměru jsou odebrané přístupová práva (odebrání účtů/ odebrání administrátorské nebo jiné dokumentace/ odebrání přístupových karet apod.).	
B.2.3	Přístupy jsou řízeny (řízení na systémové/aplikační úrovni).	
B.2.4	Je stanovená odpovědná osoba za řízení účtů.	
B.2.5	Jsou stanoveny povinností a práva pro systémové role.	
B.2.6	Neexistují skupinové účty.	
B.2.7	Systémy vynucují autentizaci.	
B.2.8	Jsou kontrolovány oprávnění při organizační změně (změna pozice).	
B.2.9	Je aplikované automatické zamykání účtů/ automatické opožďování dalšího pokusu o přihlášení/ upozornění správce systému, když je překročen maximální počtu neúspěšných pokusů.	
B.2.10	Je nastavený limit maximálního počtu neúspěšných pokusů o přihlášení.	
B.2.11	Je technicky vynucována komplexita hesel/ pravidelná změna hesla / okamžitá změna hesla po obnovení účtu. Autentizační údaje se během ověřovaní totožnosti osob nezobrazují.	
B.2.12	Mobilních zařízen zaměstnanců se nepřipájejí do sítě organizace nebo je stanovena politika BYOD.	
B.2.13	Připojené mobilní zařízení se autentizují / jsou stanoveny požadavky na konfiguraci mobilních zařízení.	
B.2.14	Vzdálená údržba a diagnostika je striktně řízená. Dochází k ukončení spojení po provedení vzdálené údržby/ diagnostiky.	
B.2.15	Existuje dokumentace k řízení vzdálených přístupů – VPN (dokumentace možnosti využívaní, konfiguračních požadavků a pokynů k připojení).	
B.2.16	Wi-Fi sítě jsou adekvátně zabezpečeny.	

Tab. č. 20: Checklist podoblast B.3 Požadavky v oblasti ochrany před škodlivým kódem

B.3	Požadavky v oblasti ochrany před škodlivým kódem	Plněno
B.3.1	Koncové stanice jsou opatřeny antivirovým softwarem.	
B.3.2	Antivirový software je minimálně 1x denně aktualizován (včetně virových signatur).	
B.3.3	Sítě jednotlivých systémů jsou logicky nebo fyzicky oddělené (segmentované) minimálně na úrovni provoz-správa.	
B.3.4	Je prováděn pravidelný scan zranitelností systému.	
B.3.5	Seznam zranitelností ke scanování je pravidelně aktualizován.	
B.3.6	Jsou aplikovány kontroly souborů z externích zdrojů při stahování/otevíraní soborů (např. v testovacím prostředí).	

Tab. č. 21: Checklist podoblast B.4 Požadavky v oblasti aplikační bezpečnosti

B.4	Požadavky v oblasti aplikační bezpečnosti	Plněno
B.4.1	Jsou omezené instalační práva uživatelů.	
B.4.2	Aplikace jsou pravidelně aktualizovány.	
B.4.3	Systém má omezeny funkce aplikací/ porty/ protokoly	
B.4.4	Je vykonáván pravidelný licenční auditu/ pravidelná kontrola instalovaného software.	
B.4.5	Není povoleno využití neschválených kolaborativních aplikací a zařízení (Teams, Skype apod.).	
B.4.6	Jsou stanoveny pravidla výměny dat mezi dvěma systémy.	

Tab. č. 22: Checklist pro podoblast B.5 Kryptografické prostředky

B.5	Kryptografické prostředky	Plněno
B.5.1	Využité kryptografické prostředky respektují doporučení NÚKIB.	
B.5.2	Autentizační údaje jsou šifrované při přenose. Uložení v heši.	
B.5.3	Hesla jsou uložená v heši se solí.	

Tab. č. 23: Checklist pro podoblast B.6 Požadavky v oblasti zajišťování úrovně dostupnosti informací

B.6	Požadavky v oblasti zajišťování úrovně dostupnosti informací	Plněno
B.6.1	Jsou logovány operační systémy.	
B.6.2	Jsou logovány bezpečností nástroje a software.	
B.6.3	Je logován chod aplikací.	
B.6.4	Všechny typy logů obsahují úplné informace – kdy k událostí došlo, kde k událostí došlo, zdroj událostí, výsledek akce, identifikace objektů/identit.	
B.6.5	Existuje centrální místo sběru logů.	
B.6.6	Kritická infrastruktura systému neobsahuje jediný bod selháni (Single Point of Failure).	
B.6.7	Architektura kritické infrastruktury je redundantní na relevantních místech.	
B.6.8	Systém je udržován dle předpisů výrobce nebo dodavatele.	

Tab. č. 24: Checklist pro podoblast B.7 Požadavky v oblasti cloudových služeb

B.7	Požadavky v oblasti cloudových služeb	Plněno
B.7.1	Data jsou uložena v rámci EÚ.	
B.7.2	Poskytovatel cloudu předložil certifikát ISO/IEC 27 001 nebo auditní správu SOC 2 Type II.	
B.7.3	Pro komunikaci je využité šifrované VPN spojení.	
B.7.4	Vztah s dodavatelem cloudu je řízen pomocí SLA.	
B.7.5	Existují exit plány včetně postupů předání dat.	
B.7.6	Existují koordinované postupy v případě vzniku incidentu.	

Tab. č. 25: Checklist pro podoblast B.8 Jiné

B.8	Jiné	Plněno
B.8.1	Rozhraní k systémům jsou řízená (firewall, router apod.).	
B.8.2	Existují seznamy komponent systému.	
B.8.4	Na relevantních místech je využita demilitarizovaná zóna.	
B.8.5	Zastaralé komponenty jsou vyřazované (např. nepodporovaný OS).	
B.8.6	Jsou stanovené metriky, které je potřeba sledovat (např. vytížení procesoru serverů).	
B.8.7	Firmware je pravidelně aktualizován.	

3.3.4 Zpráva o stavu ISMS

Zpráva o stavu ISMS je dokument, který agreguje výsledky identifikace a ohodnocení aktiv a výsledků posouzeni aktuálního stavu bezpečnosti. Slouží jako podklad pro vrcholový managment, kterému je správa předkládaná manažerem kybernetické bezpečnosti.

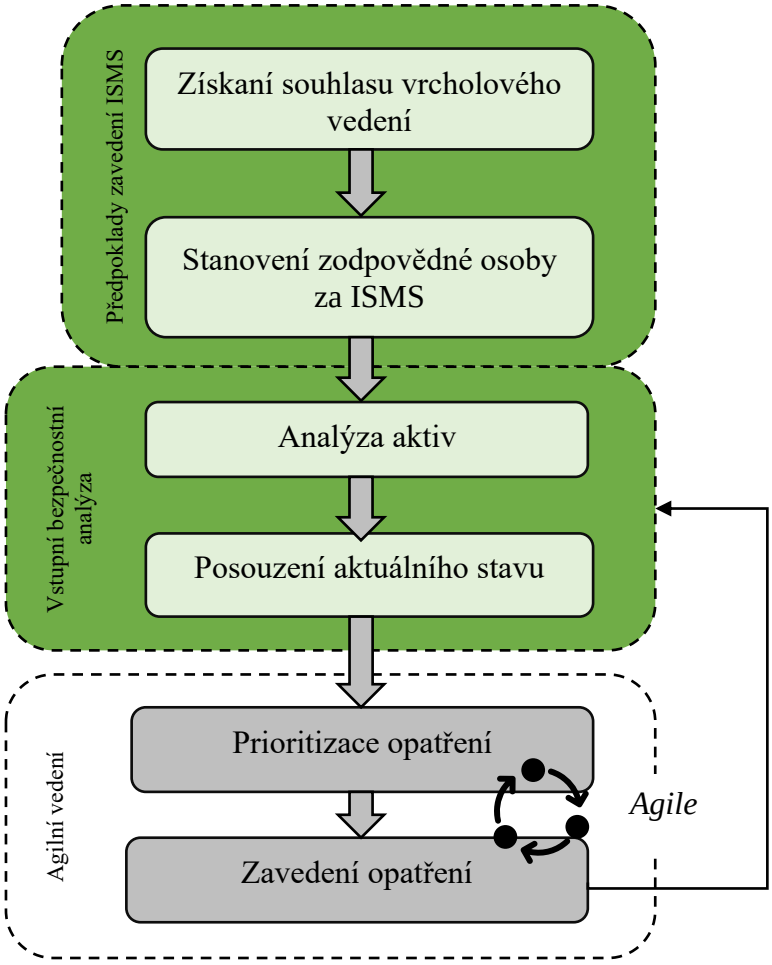
Součástí závěrečné správy by mělo být také prohlášení o aplikovatelnosti, kde bude uvedeno hodnocení za všechny podoblasti. Vzor prohlášení o aplikovatelnosti je uveden v následující tabulce.

Tab. č. 26: Prohlášení o aplikovatelnosti

Oblast	S-01	S-02	S-03	S-04
Manažerská oblast				
A.1 Základní předpoklady				
A.2 Klasifikace a ochrana informací				
A.3 Řízení kontinuity činností				
A.4 Řízení změn				
A.5 Řízení dodavatelů				
A.6 Řízení lidských zdrojů				
A.7 Audit kybernetické bezpečnosti				
Technická oblast				
B.1 Fyzická bezpečnost				
B.2 Řízení přístupu				
B.3 Požadavky v oblasti ochrany před škodlivým kódem				
B.4 Požadavky v oblasti aplikační bezpečnosti				
B.5 Kryptografické prostředky				
B.6 Požadavky v oblasti zajišťování úrovně dostupnosti informací				
B.7 Požadavky v oblasti cloudových služeb				
B.8 Jiné				

3.3.4.1 Stav podprocesů po provedení posouzení aktuálního stavu

Po provedení posouzení aktuálního stavu bezpečnosti pokračuje proces agilní části – prioritizací opatření a následným zavedením opatření.



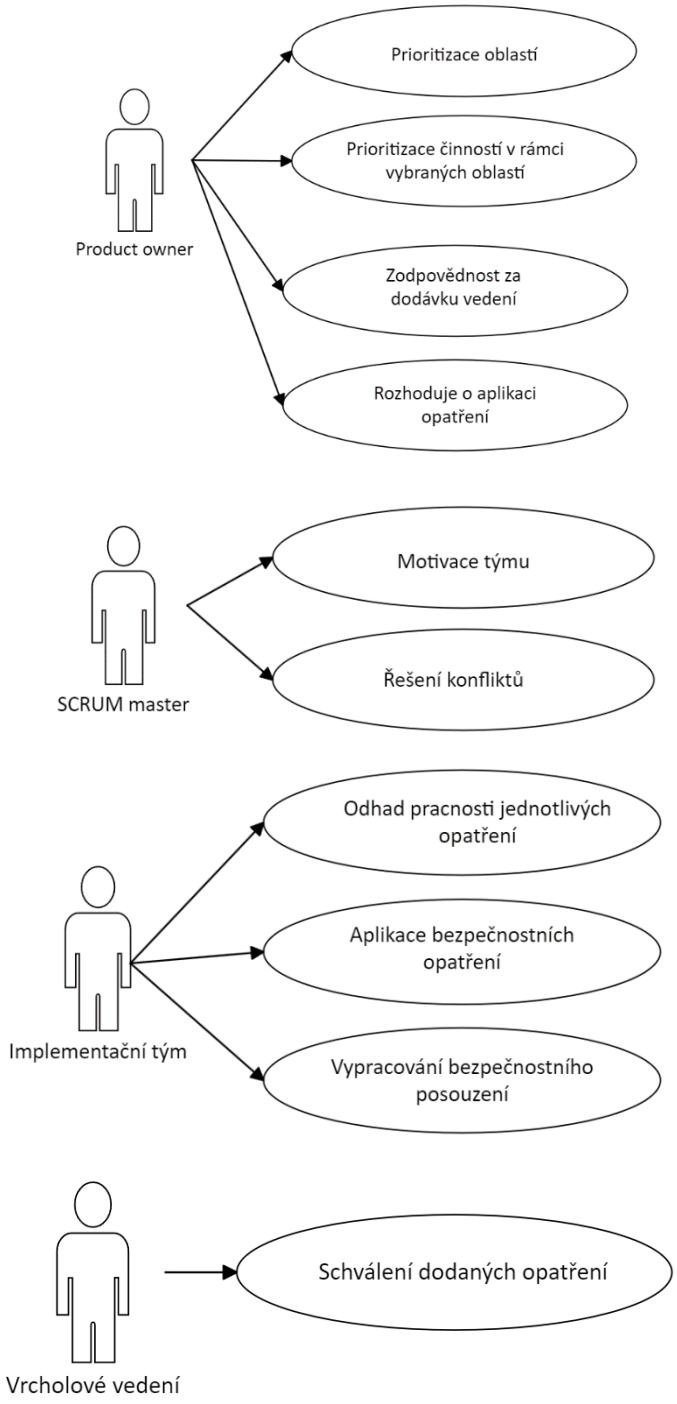
Obr. č. 13: Stav naplnění procesů po vykonání posouzení stavu ISMS

3.4 Agilní řízení

Po ukončené vstupní analýze následuje proces vytvoření agilního týmu, kteří bude pracovat na zavedení a prioritizaci opatření. Pro vytvoření agilního týmu potřebujeme zajistit základní role SCRUM master, product owner a implementační tým složený ze zkušených lidí v rámci oboru kybernetické bezpečnosti (např. formou zasmluvnění externí konzultantské společnosti).

3.4.1 Seznam rolí

Seznam rolí, kteří se budou podílet na zavedení daných opatření budou uvedené v následujícím obrázku.



Obr. č. 14: Seznam rolí agilního řízení

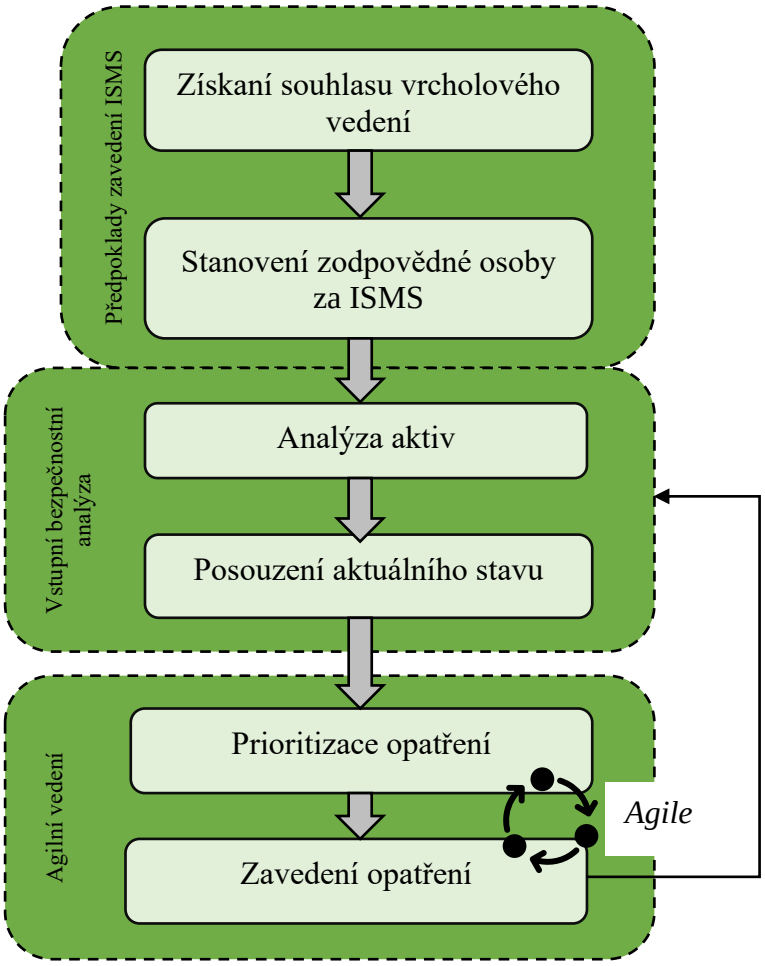
Zodpovědnost jednotlivých rolí v rámci agilního řízení je možné vyjádřit také v podobě RACI matice.

Tab. č. 27: Seznam rolí agilního řízení

	Product owner	SCRUM master	Implementační tým	Vrcholové vedení
Prioritizace oblastí	R, A	I	I	C
Prioritizace činností v rámci vybraných oblastí	R, A	I	I	C
Zodpovědnost za dodávku	R, A	C	C	I
Rozhoduje o aplikaci opatření	R, A	C	C	C
Motivace týmu	C	R, A	C	I
Řešení konfliktů	C	R, A	C	I
Odhad pracnosti jednotlivých opatření	A	C	R	I
Aplikace bezpečnostních opatření	A	C	R	I
Vypracování bezpečnostního posouzení	A	C	R	I
Schválení dodaných opatření	C	C	I	R

3.4.2 Stav podprocesů po provedení návrhu bezpečnostních opatření

Po provedení návrhu bezpečnostních opatření je úvodní cyklus ISMS (zavedení ISMS) ukončen.



Obr. č. 15: Stav naplnění procesů po návrhu

Bezpečnostních opatření

3.5 Náklady na zavedení ISMS

Práce se zabývá středně velikou společností. Tato skutečnost bude zohledněná stanovením přiměřeného rozsahu ISMS, tak aby náklady na zavedení nepřesáhly možnosti podniku. Celá tvorba metodického přístupu bude ovlivněna touto skutečností. Díky implementaci pomocí agilních metody SCRUM, je společnost schopna ovlivnit náklady na bezpečnostní opatření pomocí prioritizace jednotlivých opatření.

4 APLIKACE VE VYBRANÉ SPOLEČNOSTI

Cílem praktické části je aplikovat metodiku vytvořenou v kapitole 3. Zavedení ISMS ve vybrané společnosti. Na přání společnosti budou informace anonymizovány. Bude provedena analýza aktiv a zhodnocení aktuálního stavu ISMS. Na základě výsledků bude sestaveno prohlášení o aplikovatelnosti.

4.1 Představení organizace, titulní list

Vybraná společnost byla založena jako společnost s ručením omezením. Organizace podniká v oboru potravinářství, konkrétně se jedná o výrobu nanuků. Z hlediska velikosti podnikatele představuje společnost středního podnikatele.

Tab. č. 28: Titulní list vstupní bezpečnostní analýzy

Analýza aktuálního stavu ISMS společnosti Alfa		
Identifikátor dokumentu:	ISMS-01	
Místo uložení čistopisu:	Sdílené úložiště	
Datum zpracování:	1.5.2022	
Datum vydání:	15.5.2022	
Garant dokumentu:	Manažer kybernetické bezpečnosti	
Autorizace dokumentu		
	Jméno, příjmení, název pozice	Podpis
Zpracoval:	Manažer kybernetické bezpečnosti	
Schválil:	Ředitel společnosti	

Změnové řízení dokumentu			
Číslo revize	Popis změn	Zpracovatel změny	Datum změny
1.0	Výchozí dokument	Manažer kybernetické bezpečnosti	1.5.2022

4.2 Analýza aktiv organizace

K podpoře své podnikatelské činnosti využívá společnost následující systémy:

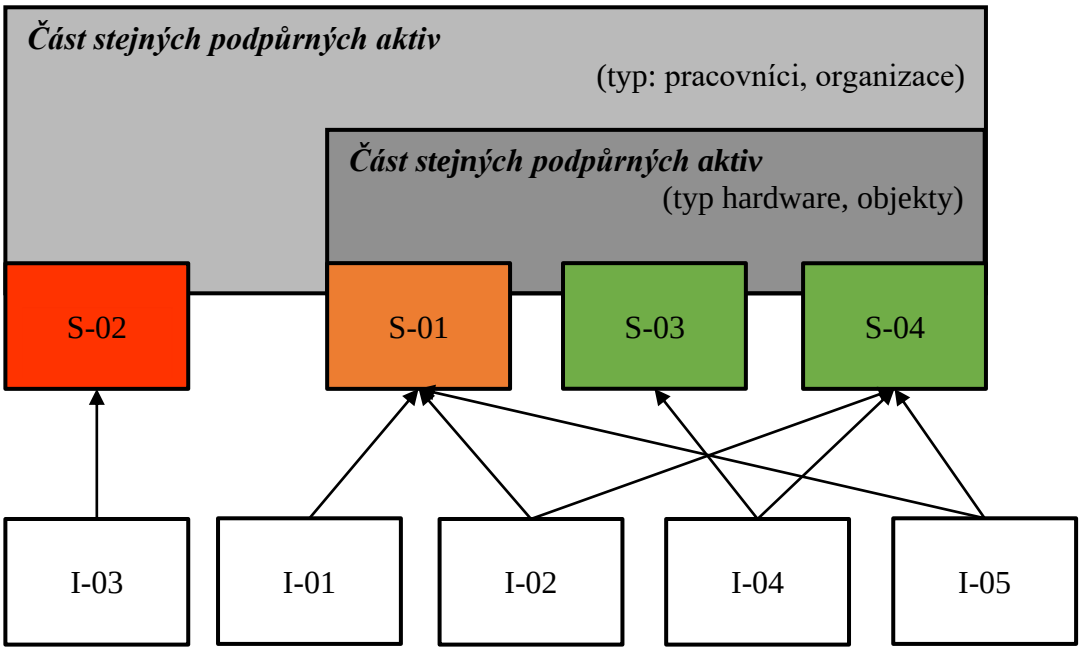
- mzdový, účetní a pokladní systém,
- technologický výrobní systém,
- web,
- email.

Uvedené systémy nakládají s informacemi – osobní údaje o zaměstnancích, obchodní informace, technologická data a veřejné informace.

Tab. č. 29: Identifikace primárních aktiv společnosti

ID Aktiva	Název aktiva	Typ Aktiva	Druh Aktiva	Popis	Datum identifikace
S-01	Mzdový, účetní a pokladní systém	Primární	Služba	Zajišťuje personální agendu a účetnictví	1.5.2022
S-02	Technologický výrobní systém	Primární	Služba	Zajišťuje procesy výroby	1.5.2022
S-03	Web	Primární	Služba	Zveřejňování Informací	1.5.2022
S-04	E-mail	Primární	Služba	Komunikace z/do společnosti	1.5.2022
I-01	Osobní údaje o zaměstnancích	Primární	Informace	Zaměstnanecká agenda	1.5.2022
I-02	Obchodní Informace	Primární	Informace	Faktury, objednávky, prodeje, kontakty	1.5.2022
I-03	Technologické data	Primární	Informace	Parametry pro řízení technologického celku	1.5.2022
I-04	Veřejné Informace	Primární	Informace	Zveřejněné informace o společnosti	1.5.2022
I-05	Interní Informace	Primární	Informace	Předpisy, reporty, směrnice apod.	1.5.2022

Vzájemné propojení systémů je zobrazeno na následujícím obrázku. Systémy S-01 až S-04 mají společnou část podpůrných aktiv – spolupracovníci, organizace. Systémy S-01, S-03, S-04 mají okrem spolupracovníků a organizace společné podpůrná aktiva typu hardware a objekty.



Obr. č. 16: Vztah informací, systémů a podpůrných aktiv

K jednotlivým systémům je potřebné stanovit garanty, kteří zodpovídají zajištění rozvoje, použití a bezpečnost aktiva. Pro systémy byly stanovení následující garanti:

- S-01: správce systému S-01,
- S-02: vedoucí technického oddělení,
- S-03: správce webu,
- S-04: správce systému S-04.

Systémy S-01 až S-04 ohodnotíme podle jejich dopadu, přičemž se bude vycházet vodítek uvedených v příloze I. Nejdůležitějším aktivem je S-02 Technologický výrobní systém, který zabezpečuje hlavní podnikatelskou činnost společnosti. Jeho výpadek vede k ohrožení funkce celé společnosti s potenciálním dopadem do ukončení podnikatelské činnosti.

Tab. č. 30: Hodnocení primárních aktiv společnosti

ID Aktiva	Stupeň dopadu	Popis dopadu
S-01	Vysoký	- V oblasti ochrany osobních údajů může způsobit porušení právních předpisů vedoucí k negativním dopadům na jednotlivce - V oblasti zákonných a smluvních povinností může zapříčinit správní nebo občanskoprávní řízení vedoucí k pokutě nebo k náhradě škody - Může omezit provádění důležitých činností organizace - Může přímo nebo nepřímo vést ke ztrátám vyšším než 2 % a nižším či rovným 10 % ročního rozpočtu, popř. obratu organizace
S-02	Kritický	- Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) větší skupiny osob, nebo ohrožení na životě jednotlivců - Může zapříčinit správní nebo občanskoprávní řízení vedoucí k pokutě nebo k náhradě škody - Závažným způsobem může zasáhnout do fungování celé organizace a může vést až k ukončení činnosti - Může přímo nebo nepřímo vést ke ztrátám přesahujícím 10 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace)
S-03	Nízký	- Může narušit řádné řízení nefungování části nebo celé organizace - Může negativně ovlivnit vztahy s jinými částmi organizace, jinými organizacemi nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhé trvání - Může přímo nebo nepřímo vést ke ztrátám menším než 0,05 % ročního rozpočtu, popř. obratu organizace
S-04	Nízký	- Může způsobit porušení etických, nikoli však právních předpisů vedoucí k negativním osobním dopadům na jednotlivce nebo skupinu osob - V oblasti ochrany osobních údajů může zapříčinit porušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností - Může negativně ovlivnit vztahy s jinými částmi organizace, jinými organizacemi nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhé trvání

4.3 Podpůrné aktiva systému S-01

Systém S-01 mzdový, účetní a pokladní systém pracuje s osobními údaje o zaměstnáních a také s obchodními informacemi. Aktivum zajišťuje personální agendu a účetnictví. Rozpad na jednotlivé podpůrná aktiva je uveden v následující tabulce.

Tab. č. 31: Podpůrná aktiva systému S-01

ID Aktiva	Název aktiva	Typ Aktiva
S-01	Mzdový, účetní a pokladní systém	Primární
I-01	Osobní údaje o zaměstnancích	Primární
I-02	Obchodní informace	Primární
S-01-01	Cloudové úložiště	Hardware, software
S-01-02	Uživatelé systému S-01	Pracovníci
S-01-03	Správce systému S-01	Pracovníci
S-01-04	Dodavatel systému S-01	Dodavatelé
S-01-05	Dokumentace systému S-01	Organizace
S-01-06	Komunikační síť (včetně ISP)	Jiné technické podpůrné prostředky

Pro podpůrná aktiva byl stanoven jejich dopad na aktiva primární. Nejdůležitějším podpůrným aktivem je S-01-01 cloudové úložiště. Narušení integrity dat by mohlo vést k sankčnímu jednání. Bez cloudového úložiště není možné analyzovaný systém provozovat.

Tab. č. 32: Hodnocení dopadu podpůrných aktiv systému S-01

ID aktiva	Dostupnost	Důvěrnost	Integrita	Hodnota podpůrného aktiva
S-01-01	Střední	Vysoká	Kritická	Kritická
S-01-02	Střední	Střední	Vysoká	Vysoká
S-01-03	Střední	Vysoká	Vysoká	Vysoká
S-01-04	Střední	Vysoká	Nízká	Vysoká
S-01-05	Nízká	Střední	Střední	Střední
S-01-06	Střední	Vysoká	Vysoká	Vysoká

4.4 Podpůrné aktiva systému S-02

Systém S-02 technologický výrobní systém je nejkritičtějším systémem – zajišťuje poloautomatizovanou výrobu nanuků. Systém pracuje s technologickými daty. Rozpad na jednotlivé podpůrná aktiva je uveden v následující tabulce.

Tab. č. 33: Podpůrná aktiva systému S-02

ID aktiva	Název aktiva	Typ Aktiva
S-02	Technologický výrobní systém	Primární
I-03	Technologické data (včetně konfigurací)	Primární
S-02-01	SCADA systém	Software
S-02-02	Dohledové pracoviště (HW vybavení Velín)	Hardware
S-02-03	Klíčové PLC	Hardware
S-02-04	Ostatní PLC	Hardware
S-02-05	Aktivní prvky mimo PLC (switche, routery, firewally)	Hardware
S-02-06	Servery	Hardware
S-02-07	Polní instrumentace	Hardware
S-02-08	Pasivní častí sítě	Hardware
S-02-09	Serverovna	Objekty
S-02-10	Místnost – Velín	Objekty
S-02-11	Výrobní hala	Objekty
S-02-12	Centrální UPS	Jiné podpůrné technické prostředky
S-02-13	Klimatizace serverovny	Jiné podpůrné technické prostředky
S-02-14	Napájení komunikačních uzlů	Jiné podpůrné technické prostředky
S-02-15	Dokumentace systému S-02	Organizace
S-02-16	Správci systému	Pracovníci
S-02-17	Uživatelé systému	Pracovníci
S-02-18	Administrativní pracovníci	Pracovníci

Pro podpůrná aktiva byl stanoven jejich dopad v následující tabulce. Hodnota podpůrných aktiv se pohybuje na úrovni kritická a vysoká. Pro centrální UPS, klimatizaci serverů, uživatelé systému a administrativní pracovníky je hodnota stanovená jako střední.

Tab. č. 34: Hodnocení dopadu podpůrných aktiv systému S-02

ID aktiva	Dostupnost	Důvěrnost	Integrita	Hodnota podpůrného aktiva
S-02-01	Kritická	Střední	Kritická	Kritická
S-02-02	Vysoká	Střední	Kritická	Kritická
S-02-03	Kritická	Střední	Kritická	Kritická
S-02-04	Vysoká	Střední	Vysoká	Vysoká
S-02-05	Kritická	Střední	Vysoká	Kritická
S-02-06	Vysoká	Střední	Vysoká	Vysoká
S-02-07	Vysoká	Nízká	Vysoká	Vysoká
S-02-08	Vysoká	Nízká	Nízká	Vysoká
S-02-09	Vysoká	Střední	Nízká	Vysoká
S-02-10	Vysoká	Střední	Nízká	Vysoká
S-02-11	Kritická	Nízká	Nízká	Kritická
S-02-12	Střední	Nízká	Nízká	Střední
S-02-13	Střední	Nízká	Nízká	Střední
S-02-14	Kritická	Nízká	Nízká	Kritická
S-02-15	Střední	Vysoká	Střední	Vysoká
S-02-16	Střední	Vysoká	Vysoká	Vysoká
S-02-17	Nízká	Střední	Vysoká	Střední
S-02-18	Nízká	Střední	Střední	Střední

4.5 Podpůrné aktiva systému S-03

Systém S-03 web pracuje s veřejnými informacemi firmy. Aktivum zajišťuje provoz webu firmy. Na webu firma má zveřejněné informace o firmě. Rozpad na jednotlivá podpůrná aktiva jsou uvedena v následující tabulce.

Tab. č. 35: Podpůrná aktiva systému S-03

ID Aktiva	Název aktiva	Typ aktiva
S-03	Web	Primární
I-04	Veřejné informace	Primární
S-03-01	Cloudové úložiště	Hardware, software
S-03-02	Uživatelé systému S-03	Pracovníci
S-03-03	Správci systému S-03	Pracovníci
S-03-04	Dodavatel systému S-03	Dodavatelé
S-03-05	Komunikační síť (včetně ISP)	Hardware

Pro podpůrná aktiva byl stanoven jejich dopad na aktiva primární. Nejdůležitějšími podpůrnými aktivem je cloudové úložiště. Cloudové úložiště je zdroj dat pro web, bez kterého by nebyl možný provoz webu.

Tab. č. 36: Hodnocení dopadu podpůrných aktiv systému S-03

ID aktiva	Dostupnost	Důvěrnost	Integrita	Hodnota podpůrného aktiva
S-03-01	Střední	Nízká	Střední	Střední
S-03-02	Střední	Střední	Vysoká	Střední
S-03-03	Střední	Střední	Vysoká	Střední
S-03-04	Střední	Střední	Nízká	Střední
S-03-05	Střední	Střední	Střední	Střední

4.6 Podpůrné aktiva systému S-04

Systém S-04 e-mailová služba pracuje s obchodními a veřejnými informacemi, a také s osobními údaji o zaměstnancích. Aktivum zajišťuje provoz e-mailové komunikace. Rozpad na jednotlivá podpůrná aktiva jsou uvedena v následující tabulce.

Tab. č. 37: Podpůrná aktiva systému S-04

ID Aktiva	Název aktiva	Typ aktiva
S-04	E-mail	Primární
I-02	Obchodní informace	Primární
I-04	Veřejné informace	Primární
I-05	Interní informace	Primární
S-04-01	Cloudové úložiště	Hardware, software
S-04-02	Uživatelé systému S-04	Pracovníci
S-04-03	Správci systému S-04	Pracovníci
S-04-04	Dodavatel systému S-04	Dodavatelé
S-04-05	Komunikační síť (včetně ISP)	Hardware

Pro podpůrná aktiva byl stanoven jejich dopad. Nejdůležitějšími podpůrnými aktivy jsou komunikační síť, uživatelé systému S-04. bez dostupnosti komunikační sítě a uživatelů nebude e-mail vhodně fungovat a může ohrozit komunikaci s dodavateli, zákazníky.

Tab. č. 38: Hodnocení dopadu podpůrných aktiv systému S-04

ID aktiva	Dostupnost	Důvěrnost	Integrita	Hodnota podpůrného aktiva
S-04-01	Střední	Střední	Vysoká	Střední
S-04-02	Střední	Střední	Vysoká	Střední
S-04-03	Střední	Střední	Vysoká	Střední
S-04-04	Střední	Střední	Střední	Střední
S-04-05	Střední	Střední	Střední	Střední

4.7 Checklist bezpečnostního posouzení ISMS

V této kapitole jsou uvedeny checklisty pro jednotlivé podoblasti. Na konci každé podoblasti je uvedené hodnocení (v procentech).

Tab. č. 39: Hodnocení podoblasti A.1 Základní předpoklady

A.1	Základní předpoklady	S-01	S-02	S-03	S-04
A.1.1	Existuje interní řídící dokumentace – ***manažerská oblast*** (klasifikace a ochrana informací, řízení dodavatelů, řízení lidských zdrojů, řízení změn, řízení kontinuity činností, audit kybernetické bezpečnosti). Dokumentace je schválená vrcholovým vedením.	Ne	Ne	Ne	Ne
A.1.2	Existuje interní řídící dokumentace – ***technická oblast*** (fyzická bezpečnost, řízení přístupů, požadavky v oblasti ochrany před škodlivým kódem, požadavky v aplikační bezpečnosti, kryptografické prostředky, požadavky v oblasti zajišťováni úrovně dostupnosti informací, požadavky v oblasti cloudových služeb). Dokumentace je schválená vrcholovým vedením.	Ne	Ne	Ne	Ne
A.1.3	Existuje interní řídící dokumentace – ***prohlášení o aplikovatelnosti.***	Ne	Ne	Ne	Ne
A.1.4	Pro interní řídící dokumentaci (manažerská oblast, technická oblast, prohlášení o aplikovatelnosti, plán zavádění bezpečnostních opatření) je stanoven interval aktualizace a dokumentace je v tomto intervalu pravidelně aktualizována.	Ne	Ne	Ne	Ne
A.1.5	Je pravidelně vykonávaná analýza aktiv.	Ne	Ne	Ne	Ne
	Vyhodnocení plnění	**0 %**	**0 %**	**0 %**	**0 %**

Tab. č. 40: Hodnocení podoblasti A.1 Klasifikace a ochrana informací

A.2	Klasifikace a ochrana informací	S-01	S-02	S-03	S-04
A.2.1	Je stanovená osoba odpovědná za veřejný kontent a kontent je oprávněnou osobou kontrolován před zveřejněním.	N/A	N/A	Ne	N/A
A.2.2	Je kontrolován veřejně přístupný obsah, odstraňují se neveřejné informace dostupné z veřejně přístupného internetu.	N/A	N/A	Ne	N/A
A.2.3	Uložené/ zpracovávané/ přenášené informace jsou kategorizovány.	Ne	Ne	Ne	Ne
A.2.4	Jsou stanovené pravidla pro manipulaci/ likvidaci/ zálohování nebo změny klasifikovaných informací.	Ne	Ne	Ne	Ne
A.2.5	Jsou využívané technické opatření při manipulaci/ likvidaci/ změně klasifikovaných informací.	Ne	Ne	Ne	Ne
	Vyhodnocení plnění	**0 %**	**0 %**	**0 %**	**0 %**

Tab. č. 41: Hodnocení podoblasti A.3 Řízení kontinuity činností

A.3	Řízení kontinuity činností	S-01	S-02	S-03	S-04
A.3.1	V interní řídící dokumentaci je popsán systém záloh (co bude zálohováno, kdy, jak dlouho bude záloha uchována, kolik záloh bude uchovaných, kdo zálohu vykoná).	N/A	Ne	N/A	N/A
A.3.2	Existuje aspoň 1 off-line záloha	N/A	Ano	N/A	N/A
A.3.3	Informace jsou pravidelně zálohovány dle pravidla 3-2-1 (tři zálohy, na dvou místech, z toho minimálně jedna off-line).	N/A	Ne	N/A	N/A
A.3.4	Zálohy chráněných/citlivých informací jsou šifrované.	N/A	Ne	N/A	N/A
A.3.5	Existuje systém ochrany integrity záloh (digitální podpis nebo heš zálohy).	N/A	Ne	N/A	N/A
A.3.6	Čitelnost záloh je pravidelně testována.	N/A	Ne	N/A	N/A
A.3.7	Existuje plán kontinuity podnikání (– Business Continuity Plan – BCP).	Ne	Ne	Ne	Ne
A.3.8	Existuje plán zotavení po havárií (Disaster Recovery Plan – DRP).	Ne	Ne	Ne	Ne
A.3.9	Je stanoven interval pro testování BCP a DRP plánů a v tomhle intervalu jsou plány testovány.	Ne	Ne	Ne	Ne
A.3.010	Existují postupy pro hlášení bezpečnostních incidentů/ událostí.	Ano	Ano	Ano	Ano
A.3.011	Existují postupy pro řešení bezpečnostních incidentů/ událostí (včetně eskalace situace).	Ano	Ano	Ano	Ano
	Vyhodnocení plnění	**40 %**	**27 %**	**40 %**	**40 %**

Tab. č. 42: Hodnocení podoblasti A.4 Řízení změn

A.4	**Řízení změn**	**S-01**	**S-02**	**S-03**	**S-04**
A.4.1	Jsou analyzovány změny z hlediska dopadu do bezpečnosti.	N/A	Ne	N/A	N/A
A.4.2	Změny jsou dokumentovány (včetně změn konfigurace).	N/A	Ne	N/A	N/A
A.4.3	V případě potřeby jsou přijata opatření za účelem snížení dopadů spojených se změnami.	N/A	Ne	N/A	N/A
A.4.4	Při změnách je zajištěná možnosti obnovy do původního stavu.	N/A	Ano	N/A	N/A
A.4.5	Změny jsou před nasazením testovány.	N/A	Ne	N/A	N/A
	Vyhodnocení plnění	**N/A**	**20 %**	**N/A**	**N/A**

Tab. č. 43: Hodnocení podoblasti A.5 Řízení dodavatelů

A.5	Řízení dodavatelů	S-01	S-02	S-03	S-04
A.5.1	V dodavatelských vztazích jsou vymáhaný relevantní bezpečností požadavky.	Ano	N/A	Ne	Ne
A.5.2	Pro provoz relevantních systémů je vztah s dodavateli řízen pomocí SLA.	Ano	N/A	Ano	Ano
	Vyhodnocení plnění	**100 %**	**N/A**	**50 %**	**50 %**

Tab. č. 44: Hodnocení podoblasti A.6 Řízení lidských zdrojů

A.6	Řízení lidských zdrojů	S-01	S-02	S-03	S-04
A.6.1	Je určen manažer kybernetické bezpečnosti.	Ano	Ano	Ano	Ano
A.6.2	Administrátoři a osoby zastávající bezpečnostní role mají uzavřenou dohodu o mlčenlivosti (Non-disclosure agreement – NDA).	Ano	Ano	Ano	Ano
A.6.3	Zaměstnanci jsou v oblasti bezpečnosti školení formou vstupního a pravidelného školení (včetně manažerů).	Ne	Ne	Ne	Ne
A.6.4	Bezpečnostní role a IT zaměstnanci jsou pravidelně školení odborným a specializovaným školením (v oboru a také v oblasti bezpečnosti).	Ne	Ne	Ne	Ne
A.6.5	Existují sankční postupy při nedodržování zavedených bezpečnostních zásad.	Ne	Ne	Ne	Ne
	Vyhodnocení plnění	**40 %**	**40 %**	**40 %**	**40 %**

Tab. č. 45: Hodnocení podoblasti A.7 Audit kybernetické bezpečnosti

A.7	Audit kybernetické bezpečnosti	S-01	S-02	S-03	S-04
A.7.1	Je stanoven auditor kybernetické bezpečnosti (i externí subjekt).	Ne	Ne	Ne	Ne
A.7.2	Auditor kybernetické bezpečnosti je nezávislou osobou od provozních nebo bezpečnostních rolí.	Ne	Ne	Ne	Ne
A.7.3	Je prováděno nezávislé hodnocení dodržování bezpečnostních politik.	Ne	Ne	Ne	Ne
A.7.4	Jsou prováděné nezávislé bezpečnostní technické kontroly (např. penetrační testování).	Ne	Ne	Ne	Ne
A.7.5	Výsledky auditů jsou zohledňovány při návrhu bezpečnostních opatření.	Ne	Ne	Ne	Ne
	Vyhodnocení plnění	**0 %**	**0 %**	**0 %**	**0 %**

Tab. č. 46: Hodnocení podoblasti B.1 Fyzická bezpečnost

B.1	Fyzická bezpečnost	S-01	S-02	S-03	S-04
B.1.1	Zařízení jsou umístněná ve vhodném prostředí. V případě zhoršeného prostřední (voda, prach, teplo apod.) probíhá monitorování environmentálních podmínek.	Ano	Ne	Ano	Ano
B.1.2	Existuje systém pro detekci požáru, potlačení požáru.	Ano	Ano	Ano	Ano
B.1.3	Existuje systém pro potlačení úniku vody (dostupnost uzavíracích ventilů). Ventily jsou funkční a personál je znalí obsluhy.	Ano	Ano	Ano	Ano
B.1.4	Jsou aplikována technická opatření ochrany perimetru (např. kamerový systém).	Ano	Ano	Ano	Ano
B.1.5	Vstupu do chráněných oblastí je řízen (např. zamykání dveří, přístupový systém).	Ano	Ano	Ano	Ano
B.1.6	Existuje postup řešení ztráty autentizačních faktorů (např. ztráta klíčů).	Ano	Ano	Ano	Ano
	Vyhodnocení plnění	**100 %**	**100 %**	**100 %**	**100 %**

Tab. č. 47: Hodnocení podoblasti B.2 Řízení přístupů

B.2	Řízení přístupů	S-01	S-02	S-03	S-04
B.2.1	Existují dohody o přístupu zaměstnanců k zařízením (např. dohoda o přijatelném užívaní/ / pravidla chování).	Ano	Ne	Ano	Ano
B.2.2	Po ukončení pracovního poměru jsou odebrané přístupová práva (odebrání účtů/ odebrání administrátorské nebo jiné dokumentace/ odebrání přístupových karet apod.).	Ano	Ne	Ano	Ano
B.2.3	Přístupy jsou řízeny (řízení na systémové/aplikační úrovni).	Ano	Ano	Ano	Ano
B.2.4	Je stanovená odpovědná osoba za řízení účtů.	Ano	Ano	Ano	Ano
B.2.5	Jsou stanoveny povinností a práva pro systémové role.	Ano	Ne	Ano	Ano
B.2.5	Neexistují skupinové účty.	Ano	Ne	Ano	Ano
B.2.7	Systémy vynucují autentizaci.	Ano	Ne	Ano	Ano
B.2.8	Jsou kontrolovány oprávnění při organizační změně (změna pozice).	Ne	Ne	Ne	Ne
B.2.9	Je aplikované automatické zamykání účtů/ automatické opožďování dalšího pokusu o přihlášení/ upozornění správce systému, když je překročen maximální počtu neúspěšných pokusů.	Ano	Ne	Ano	Ano
B.2.10	Je nastavený limit maximálního počtu neúspěšných pokusů o přihlášení.	Ano	Ano	Ano	Ano
B.2.11	Je technicky vynucována komplexita hesel/ pravidelná změna hesla / okamžitá změna hesla po obnovení účtu. Autentizační údaje se během ověřovaní totožnosti osob nezobrazují.	Ano	Ne	Ano	Ano
B.2.12	Mobilních zařízen zaměstnanců se nepřipájejí do sítě organizace nebo je stanovena politika BYOD.	Ano	Ano	Ano	Ano
B.2.13	Připojené mobilní zařízení se autentizují / jsou stanoveny požadavky na konfiguraci mobilních zařízení.	Ano	N/A	Ano	Ano
	Vyhodnocení plnění	**92 %**	**67 %**	**92 %**	**92 %**

Tab. č. 48: Hodnocení podoblasti B.3 Požadavky v oblasti ochrany před škodlivým kódem

B.3	Požadavky v oblasti ochrany před škodlivým kódem	S-01	S-02	S-03	S-04
B.3.1	Koncové stanice jsou opatřeny antivirovým softwarem.	Ano	Ano	Ano	Ano
B.3.2	Antivirový software je minimálně 1x denně aktualizován (včetně virových signatur).	Ano	Ne	Ano	Ano
B.3.3	Sítě jednotlivých systémů jsou logicky nebo fyzicky oddělené (segmentované) minimálně na úrovni provoz-správa.	Ano	Ne	Ano	Ano
B.3.4	Je prováděn pravidelný scan zranitelností systému.	Ne	Ne	Ne	Ne
B.3.5	Seznam zranitelností ke scanování je pravidelně aktualizován.	N/A	N/A	N/A	N/A
B.3.6	Jsou aplikovány kontroly souborů z externích zdrojů při stahování/otevíraní soborů (např. v testovacím prostředí).	Ne	Ne	Ne	Ne
	Vyhodnocení plnění	**60 %**	**20 %**	**60 %**	**60 %**

Tab. č. 49: Hodnocení podoblasti A.1 Požadavky v oblasti aplikační bezpečnosti

B.4	Požadavky v oblasti aplikační bezpečnosti	S-01	S-02	S-03	S-04
B.4.1	Jsou omezené instalační práva uživatelů.	Ano	Ne	Ano	Ano
B.4.2	Aplikace jsou pravidelně aktualizovány.	Ano	Ne	Ano	Ano
B.4.3	Systém má omezeny funkce aplikací/ porty/ protokoly.	Ano	Ne	Ano	Ano
B.4.4	Je vykonáván pravidelný licenční auditu/ pravidelná kontrola instalovaného software.	Ne	Ne	Ne	Ne
	Vyhodnocení plnění	**75 %**	**0 %**	**75 %**	**75 %**

Tab. č. 50: Hodnocení podoblasti B.5 Kryptografické prostředky

B.5	Kryptografické prostředky	S-01	S-02	S-03	S-04
B.5.1	Využité kryptografické prostředky respektují doporučení NÚKIB.	N/A	Ano	N/A	N/A
B.5.2	Autentizační údaje jsou šifrované při přenose. .	Ano	Ne	Ano	Ano
B.5.3	Hesla jsou uložená v heši se solí.	Ano	Ne	Ano	Ano
	Vyhodnocení plnění	**100 %**	**33 %**	**100 %**	**100 %**

Tab. č. 51: Hodnocení podoblasti B.6 Požadavky v oblasti zajišťování úrovně dostupnosti informací

B.6	Požadavky v oblasti zajišťování úrovně dostupnosti informací	S-01	S-02	S-03	S-04
B.6.1	Jsou logovány operační systémy.	Ne	Ne	Ne	Ne
B.6.2	Jsou logovány bezpečností nástroje a software.	Ne	Ne	Ne	Ne
B.6.3	Je logován chod aplikací.	Ne	Ne	Ne	Ne
B.6.4	Všechny typy logů obsahují úplné informace – kdy k události došlo, kde k události došlo, zdroj událostí, výsledek akce, identifikace objektů/identit.	Ne	Ne	Ne	Ne
B.6.5	Existuje centrální místo sběru logů.	Ne	Ne	Ne	Ne
B.6.7	Kritická infrastruktura systému neobsahuje jediný bod selháni (Single Point of Failure).	N/A	Ne	N/A	N/A
B.6.8	Architektura kritické infrastruktury je redundantní na relevantních místech.	N/A	Ano	N/A	N/A
B.6.9	Systém je udržován dle předpisů výrobce nebo dodavatele.	Ano	Ano	Ano	Ano
	Vyhodnocení plnění	**14 %**	**22 %**	**14 %**	**14 %**

Tab. č. 52: Hodnocení podoblasti B.7 Požadavky v oblasti cloudových služeb

B.7	Požadavky v oblasti cloudových služeb	S-01	S-02	S-03	S-04
B.7.1	Data jsou uložena v rámci EÚ.	Ano	N/A	Ano	Ano
B.7.2	Poskytovatel cloudu předložil certifikát ISO/IEC 27 001 nebo auditní správu SOC 2 Type II.	Ne	N/A	Ne	Ne
B.7.3	Pro komunikaci je využité šifrované VPN spojení.	Ano	N/A	Ano	Ano
B.7.4	Vztah s dodavatelem cloudu je řízen pomocí SLA.	Ano	N/A	Ano	Ano
B.7.5	Existují exit plány včetně postupů předání dat.	Ano	N/A	Ano	Ano
B.7.6	Existují koordinované postupy v případě vzniku incidentu.	Ano	N/A	Ano	Ano
	Vyhodnocení plnění	**83 %**	**N/A**	**83 %**	**83 %**

Tab. č. 53: Hodnocení podoblasti B.8 Jiné

B.8	Jiné	S-01	S-02	S-03	S-04
B.8.1	Rozhraní k systémům jsou řízená (firewall, router apod.).	Ano	Ano	Ano	Ano
B.8.2	Existují seznamy komponent systému.	Ano	Ne	Ano	Ano
B.8.4	Na relevantních místech je využita demilitarizovaná zóna.	Ano	Ne	Ano	Ano
B.8.5	Zastaralé komponenty jsou vyřazované (např. nepodporovaný OS).	Ano	Ne	Ano	Ano
B.8.6	Jsou stanovené metriky, které je potřeba sledovat (např. vytížení procesoru serverů).	Ne	Ano	Ne	Ne
B.8.7	Firmware je pravidelně aktualizován.	Ano	Ne	Ano	Ano
	Vyhodnocení plnění	**86 %**	**29 %**	**86 %**	**86 %**

4.8 Agilní vedení

Product Backlog bude tvořen jednotlivými oblastmi ISMS. Bude seřazen dle priorit realizace. V rámci plánovaní sprintu stanovíme prioritní činnosti a naplníme sprint aktivitami dle velocity. Ke konci každého sprintu je potřeba provést bezpečnostní analýzu, protože aplikací opatření může dojít k změně priorit.

Podoblasti bezpečnostního posouzení včetně priorit umístíme do backlogu SCRUM týmu. Priorita jednotlivých oblastí se stanoví na základě možného dopadu na společnost a důležitost pro systém ISMS. Klasifikační tabulka priorit je uvedena v následující tabulce.

Tab. č. 54: Klasifikační tabulka pro prioritizaci

Priorita	Popis
1	neprodleně zavést opatření, nebo začít podnikat kroky pro zavedení opatření
2	opatření je potřeba zavést v co nejkratší možné době
3	opatření je potřeba zavést nebo je potřebné jich naplánovat
4	opatření je na akceptovatelné úrovni

4.8.1 Product backlog

Product backlog seřazen dle priorit je uveden v následující tabulce.

Tab. č. 55: Product backlog

ID podoblasti	Podoblast opatření	Priorita
A.2	Klasifikace a ochrana informací	1
A.3	Řízení kontinuity činností	1
A.1	Základní předpoklady	2
A.4	Řízení změn	2
A.6	Řízení lidských zdrojů	2
A.7	Audit kybernetické bezpečnost	2
B.3	Požadavky v oblasti ochrany před škodlivým kódem	2
B.4	Požadavky v oblasti aplikační bezpečnosti	2
B.6	Požadavky v oblasti zajišťování úrovně dostupnosti informací	2
A.5	Řízení dodavatelů	3
B.8	Jiné	3
B.1	Fyzická bezpečnost	4
B.2	Řízení přístupů	4
B.5	Kryptografické prostředky	4
B.7	Požadavky v oblasti cloudových služeb	4

4.8.2 První sprint

Pro první sprint vybereme ty podoblasti, které mají nejvyšší prioritu. Jsou to oblasti Klasifikace a ochrana informací a Řízení kontinuity činností. V tuto chvílí musí proběhnout rozpad na jednotlivé činnosti. Pracnost činností odhadneme pomocí Fibonacciho posloupností a to hodnotami 1, 2, 3, 5, 8, 13, 21. Vyšší číslo představuje větší pracnost neboli složitost.

V rámci prvního sprintu nevíme přesně definovat velocitu týmu. Z toho důvodu si pro první sprint, který bude trvat 4 týdny, odhadem zvolíme velocitu na 70. Velocitu snížíme o 20 % z důvodu započtení rizika onemocnění člena týmu a nemožnosti odhadu fungováni agilního teamu. Velocita týmu je tak stanovena na 56.

V rámci prioritizace dílčí úkonů v podoblastech byly vynechány ty, které společnost naplňuje a tím pádem, se jimi nebudeme zaobírat. V následující tabulce je uveden odhad pracnosti činností aktivit pro sprint 1.

Tab. č. 56: Aktivity prvního sprintu

	S-01	S-02	S-03	S-04	Priorita	Pracnost
A.2						
A.2.1	N/A	N/A	Ne	N/A	1	1
A.2.2	N/A	N/A	Ne	N/A	1	3
A.2.3	Ne	Ne	Ne	Ne	2	8
A.2.4	Ne	Ne	Ne	Ne	3	5
A.2.5	Ne	Ne	Ne	Ne	3	8
A.3						
A.3.1	N/A	Ne	N/A	N/A	3	5
A.3.3	N/A	Ne	N/A	N/A	4	13
A.3.4	N/A	Ne	N/A	N/A	1	8
A.3.5	N/A	Ne	N/A	N/A	2	13
A.3.6	N/A	Ne	N/A	N/A	2	5
A.3.7	Ne	Ne	Ne	Ne	3	8
A.3.8	Ne	Ne	Ne	Ne	3	8

4.8.3 Sprint backlog

V tabulce výše vidíme prioritizované činnosti včetně jejich pracnosti. Důležitým prvkem, který se bude vyskytovat v rámci celého projektu (a v každém sprintu) je bezpečnostní analýza – zavedení opatření může ovlivnit ostatní činnosti a body.

Tab. č. 57: Sprint backlog

ID	Položka	Priorita	Pracnost
A.2.1	Je stanovená osoba odpovědná za veřejný kontent a kontent je oprávněnou osobou kontrolován před zveřejněním.	1	1
A.2.2	Je kontrolován veřejně přístupný obsah, odstraňují se neveřejné informace dostupné z veřejně přístupného internetu.	1	3
A.3.4	Zálohy chráněných/citlivých informací jsou šifrované.	1	8
A.2.3	Uložené/ zpracovávané/ přenášené informace jsou kategorizovány.	2	8
A.3.5	Existuje systém ochrany integrity záloh (digitální podpis nebo heš zálohy).	2	13
A.3.6	Čitelnost záloh je pravidelně testována.	2	5
A.2.4	Jsou stanovené pravidla pro manipulaci/ likvidaci/ zálohování nebo změny klasifikovaných informací.	3	5
A.3.1	V interní řídící dokumentaci je popsán systém záloh (co bude zálohováno, kdy, jak dlouho bude záloha uchována, kolik záloh bude uchovaných, kdo zálohu vykoná).	3	5
Bezpečnostní analýza po zavedení opatření v rámci sprintu			5
		Velocita:	53 z 56

Může se stát, že uvedené aktivity stihne team zrealizovat i dříve. Z toho důvodu určíme aktivity, kterým se můžeme věnovat po dokončení hlavních aktivit.

Tab. č. 58: Aktivity v záloze

Aktivity v záloze			
A.3.7	Existuje plán kontinuity podnikání (BCP – Business Continuity Plan).	3	8
A.3.8	Existuje plán zotavení po havárií (DRP – Disaster Recovery Plan).	3	8
A.2.5	Jsou využívané technické opatření při manipulaci/ likvidaci/ změně klasifikovaných informací.	3	8
A.3.3	Informace jsou pravidelně zálohovány dle pravidla 3-2-1 (tři zálohy, na dvou místech, z toho minimálně jedna off-line).	4	13

Na základě výstupů z bezpečnostní analýzy a dokončení sprintu provedené product owner novou prioritizaci backlogu.

ZÁVĚR

Tato diplomová práce se zabývá zavedením ISMS do středně velkého podniku, kterého podnikatelská činnost orientována v oblasti výrobou nanuků. Na přání podniku byly informace anonymizované. Společnost, podobně jako i jiné střední podniky, doposud kybernetickou a informační bezpečnost.

Práce klade důraz na efektivní posouzení stavu ISMS. Byla vytvořena obecná metodika posouzení ISMS navazující na minimální bezpečnostní standard. Důležitým výstupem je checklist, kterým je možné posoudit aktuální stav kybernetické a informační bezpečnosti subjektů nespadajících pod regulaci zákona o kybernetické bezpečnosti. Checklist pracuje s podoblastmi v manažerské a technické oblasti.

Po vytvoření checklistu byla prakticky provedena analýza aktiv a aktuálního bezpečnostního stavu ISMS. Pomocí metody SCRUM byla stanovena priorita opatření. Metoda SCRUM bude dále využita i při implementaci. Na základě specifik kybernetické a informační bezpečnost byl zvolen sprint o délce 4 týdnů.

Je potřeba si uvědomit, že každé zavedené opatření může mít dopad i do ostatních oblastí informační a kybernetické bezpečnosti. Z toho důvodu bude probíhat analýza aktuálního bezpečnostního stavu na závěr každého sprintu. Na základě nově zjištěných informací proběhne prioritizace opatření, které budou implementována. V práci je na základě aktuálního bezpečnostního stavu naplánován první sprint. Agilní implementace umožní společnosti rozhodovat o zavedení bezpečnostních opatření dle aktuální dostupnosti zdrojů (lidských, finančních nebo technických).

SEZNAM POUŽITÉ LITERATURY

[1] ČSN EN ISO/IEC 27000. *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

[2] OLEJÁR, Daniel. Informačná 84polečné84t: Manažment IB. *FMPH UNIBA* [online]. Bratislava: Fakulta matematiky, fyziky a informatiky Univerzity Komenského [cit. 2022-01-22]. Dostupné z: https://new.dcs.fmph.uniba.sk/files/uib/specialistiUIB.pdfDs

[3] SEKER, Ensar. Defense-in-Depth. *Data Driven Investor* [online]. 30.9.2020 [cit. 2022-01-22]. Dostupné z: https://medium.datadriveninvestor.com/defense-in-depth-d6c070eac12d

[4] Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánovaní obrany státu. *Ministerstvo vnitra ČR* [online]. Praha: Ministerstvo vnitra ČR, 2016 [cit. 2022-01-22]. Dostupné z: https://www.mvcr.cz/soubor/terminologicky-slovnik-mv-verze-ke-stazeni.aspx

[5] Kritéria pro přijatelnosti rizik. *Osveta – NÚKIB* [online]. Brno: NÚKIB [cit. 2022-01-22]. Dostupné z: https://osveta.nukib.cz/mod/page/view.php?id=815

[6] JAŠEK, Roman a David MALANÍK. *Bezpečnost informačních systémů.* Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2013. ISBN 978-80-7454-312-8.

[7] Nepřiměřené náklady. *NÚKIB* [online]. Brno: NÚKIB, 29.1.2019 [cit. 2022-01-22]. Dostupné z: https://nukib.cz/download/publikace/podpurne_materialy/Neprimerene-naklady_v2.1.pdf

[8] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice.* Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

[9] ČSN EN ISO/IEC 27005. *Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

[10] OTTERLOO, Siuwert. Information security and PDCA (Plan-Do-Check-Act). *ICT Insititute* [online]. Utrecht: ICT Insitute, 8.2.2017 [cit. 2022-01-22]. Dostupné z: https://ictinstitute.nl/pdca-plan-do-check-act/

[11] Zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

[12] Důvodová zpráva. *Zákony pro lidi* [online]. 23.10.2016 [cit. 2022-01-22]. Dostupné z: https://www.zakonyprolidi.cz/media2/file/1705/File9530.pdf?attachment-file-name=5845137-2016-11-23-duvodova-zprava-6042062.pdf

[13] Minimální bezpečnostní standard: podpůrný materiál pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti. *NÚKIB* [online]. Brno: NÚKIB, 17.7.2020 [cit. 2022-01-22]. Dostupné z: https://www.nukib.cz/download/publikace/pod-purne_materialy/2020-07-17_Minimalni-bezpecnostni-standard_v1.0.pdf

[14] ČSN EN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Požadavky.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[15] HARRIS, Shon a Fernando MYMI. *CISSP – EXAM GUIDE*. 8th ed. New York: McGraw-Hill Education, 2019. ISBN 978-1-26-014264-8.

[16] Framework for Improving Critical Infrastructure Cybersecurity. *NIST-GOV* [online]. Gaithersburg: National Insitiute of Standards and Technology, 16.4.2018 [cit. 2022-01-23]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

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

[18] NIST SPECIAL PUBLICATION 800-50. *Building an Information Technology Security Awareness and Training Program: Computer Security.* Gaithersburg: National Institute of Standards and Technology, 2003.

[19] WILLS, Miké a Wesley PHILLIPS. *(ISC)2 SSCP Systems Security Certified Practitioner Official Study Guide* [online]. Clearwater: John Wiley, 2019 [cit. 2022-01-23]. ISBN 9781119542940.

[20] 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

[21] Aký je rozdiel medzi interným a externým auditom a čo majú 85polečné?. *Ceritifikácia Manžerských Systémov* [online]. [cit. 2022-01-23]. Dostupné z:

https://www.cems.sk/blog/347-aky-je-rozdiel-medzi-internym-a-externym-auditom-a-co-maju-spolocne

[22] HUSÁK, Miroslav. Perimetrická, plášťová, prostorová a předmětová ochrana. *ELZ* [online]. Praha: ČVUT FEL, 2018 [cit. 2022-05-07]. Dostupné z: https://www.pslib.cz/jiri.kubin/ELZ/03_20Perimetricka_20plastova_20prostorova_20predmetova_20ochrana.pdf

[23] LUCKI, Michal. Moderní zabezpečovací systémy. *Moderní zabezpečovací systémy* [online]. Praha: ČVUT, 2015 [cit. 2022-05-07]. Dostupné z: https://publi.cz/books/255/01.html

[24] GOLLMANN, Dieter. Authentication, Authorisation & Accountability (AAA) Knowledge Area. *CYBOK* [online]. Hamburg: Hamburg University of Technology & Nanyang Technological University Singapore, 2019 [cit. 2022-05-07]. Dostupné z: https://www.cybok.org/media/downloads/AAA_issue_1.0_q3qspzo.pdf

[25] Antivirus. *ESET* [online]. Praha: ESET [cit. 2022-05-11]. Dostupné z: https://www.eset.com/cz/antivirus-software/

[26] BRUSH, Kate a Paul CROCETTI. Disaster recovery plan (DRP). *TechTarget* [online]. TechTarget [cit. 2022-05-11]. Dostupné z: https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-plan

[27] Minimální požadavky na kryptografické algoritmy. *NÚKIB* [online]. Brno: NÚKIB [cit. 2022-05-11]. Dostupné z: https://www.nukib.cz/download/uredni_deska/Kryptograficke_prostredky_doporuceni_v1.0.pdf

[28] MTBF, MTTR, MTTA, and MTTF. *ATLASSIAN* [online]. Sydney, 2022 [cit. 2022-05-11]. Dostupné z: https://www.atlassian.com/incident-management/kpis/common-metrics

[29] Cloud Data Security Solutions. *Thales* [online]. [cit. 2022-05-11]. Dostupné z: https://cpl.thalesgroup.com/cloud-security

[30] ŠOCHOVÁ, Zuzana a Eduard KUNCE. *Agilní metody řízení projektů*. Brno: Computer Press, 2014. ISBN 978-80-251-4194-6.

[31] The Agile Journey: A Scrum overview. *Pm-partners* [online]. Sydney, c1996-2022, 23.6.2021 [cit. 2022-05-11]. Dostupné z: https://www.pm-partners.com.au/the-agile-journey-a-scrum-overview/

[32] Agile Project Management. *Agile Project Management* [online]. Sydney: Atlassian, 2022 [cit. 2022-05-04]. Dostupné z: https://www.atlassian.com/agile/project-management

[33] WHAT IS SCRUM?. *WHAT IS SCRUM?* [online]. Cambridge: scrum.org, 2022 [cit. 2022-05-04]. Dostupné z: https://www.scrum.org/resources/what-is-SCRUM

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ABAC	Attribute-Based Access Control Atributové řízení přístupu
BCP	Business Continuity Plan Plán kontinuity podnikání
BIA	Business Impact Analysis Analýza dopadů na podnikání
BYOD	Bring Your Own Device Přines si své vlastní zařízení
CIA	Confidentiality, Integrity, Availability Důvěrnost, integrita, dostupnost
DAC	Discretionary Access Control Volitelné řízení přístupu
DRP	Disaster Recocery Plan Plánů obnovení po havárií
IDS	Intrusion Detection System Systém detekce průniku
IPS	Intrusion Prevention System Systém prevence průniku
ISMS	Information Security Management System Systém řízení bezpečnosti informací
MAC	Mandatory Access Control Povinné řízení přístupů
MTD	Maximum Tolerable Downtime Maximální přípustní prostoje
MTBF	Mean Time Between Failures Střední meziporuchová doba
MTTR	Mean Time to Recovery Střední doba obnovy
NAKIT	Národní agentura pro komunikační a informační technologie
NDA	Non-disclosure agreement Dohoda o mlčenlivosti
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost

PDCA	Plan-Do-Check-Act Plánuj-Dělej-Kontroluj-Konej
RBAC	Role-Based Access Control Řízení přístupu pomocí rolí Rule-Based Access Control Řízení přístupu na základě pravidel
RPO	Recovery Point Objective Bod obnovení
RTO	Recovery Time Objective Čas obnovy
SLA	Service Level Agreement Smlouva o úrovni služeb
VLAN	Virtual Local Area Network Virtuální počítačová síť
VPN	Virtual private network Virtuální privátní síť
VoKB	Vyhláška o kybernetické bezpečnosti
ZoKB	Zákon o kybernetické bezpečnosti

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: VODÍTKA PRO URČENÍ ZÁVAŽNOSTI DOPADŮ NARUŠENÍ BEZPEČNOSTI INFORMACÍ

Příloha 1

Národní úřad pro kybernetickou a informační bezpečnost — NÚKIB

Regulace odpovídající úrovni dopadu	Úroveň dopadu	Vodítka (kategorie) pro určení závažnosti dopadů narušení bezpečnosti informací (dostupnost, důvěrnost, integrita) - NUKIB v1.0 / 23.02.2018									
		A. Bezpečnost a zdraví osob	B. Ochrana osobních údajů	C. Zákonné a smluvní povinnosti	D. Trestně-právní řízení	E. Veřejný pořádek	F. Mezinárodní vztahy	G. Řízení a provoz organizace	H. Ztráta důvěryhodnosti	I. Finanční ztráty	J. Zajišťování nezbytných služeb
Obalní / ISVS / GDPR / ZKB - VIS, ISZS / ZKB - KII, ISZS / ZůI	1 nízká	*žádné vodítko*	Může způsobit porušení etických, nikoli však právních předpisů vedoucí k negativním osobním dopadům na jednotlivce nebo skupinu osob.	Může zapříčinit porušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností.	*žádné vodítko*	*žádné vodítko*	*žádné vodítko*	Může narušit řádné řízení nebo fungování části nebo celé organizace.	Může negativně ovlivnit vztahy s jinými částmi organizace, jinými organizacemi nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhé trvání.	Může přímo nebo nepřímo vést ke ztrátám menším než 0,05 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	*žádné vodítko*
	2 střední	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) jedné nebo několika osob.	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 10 mil. EUR nebo 2 % celkového ročního obratu - viz čl. 83/4 GDPR).	Může zapříčinit správní nebo občanskoprávní řízení vedoucí k pokutě nebo k náhradě škody.	Může vytvořit podmínky pro páchání trestné činnosti nebo může ztížit její vyšetřování.	Může zapříčinit rozsahem, formou nebo místem omezené protesty (lokální nepokoje).	Může vytvářet negativní obraz ČR v jednom teritoriu, popř. v jednom státě.	Může omezit provádění důležitých činností organizace.	Může negativně ovlivnit vztahy s jinými organizacemi nebo veřejností, negativní publicita se ale bude týkat omezené zájmové skupiny nebo bude široká, avšak krátkodobá.	Může přímo nebo nepřímo vést ke ztrátám mezi 0,05 % a 2 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	Může způsobit závažné omezení či narušení nezbytných služeb pro malé množství osob.
	3 vysoká *	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) větší skupiny osob, nebo ohrožení na životě jednotlivců.	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na velkou skupinu osob (pokuta až 20 mil. EUR nebo 4 % celkového ročního obratu - viz čl. 83/5 GDPR).	Může zapříčinit porušení právních předpisů vedoucí k zahájení trestního stíhání.	Může vést k narušení vyšetřování trestné činnosti nebo soudní řízení (méně závažná kriminalita, krátkodobě, v jednotlivých případech).	Může zapříčinit rozsahem, formou nebo místem omezené protesty na úrovni významné části správního území obce s rozšířenou působností, jejichž řešení si může vyžádat aktivaci krizového řízení na úrovni kraje.	Může vytvářet negativní obraz ČR ve světě.	Může způsobit dočasné zastavení nebo podstatné narušení důležitých činností organizace nebo poškodit rozvoj nebo prosazování cílů a zájmů organizace.	Může závažně ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní negativní publicity.	Může přímo nebo nepřímo vést ke ztrátám vyšším než 2 % a nižším či rovným 10 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace). Pozn. v případě PZS je hranice ztráty stanovena na 0,25 % HDP.	Může způsobit závažné omezení, narušení či nedostupnost nezbytných služeb pro více než 25 000 osob (v rámci kategorie provozovatelů základních služeb se může lišit dle právní úpravy pro jednotlivá odvětví viz vyhláška č. 437/2017 Sb.).
	4 kritická **	Může vést k přímému ohrožení či ztrátě života skupiny osob.	*žádné vodítko*	*žádné vodítko*	Může vést k závažnému, dlouhodobému narušení schopnosti vyšetřovat trestnou činnost, popřípadě zpochybnění soudních řízení a rozhodnutí (závažná kriminalita, celkové zpochybnění systému).	Může zapříčinit hromadné nepokoje, např. generální stávku, nebo jinak závažně narušit veřejný pořádek s celostátními dopady.	Může negativně ovlivnit nebo poškodit diplomatické vztahy a tím způsobit nevýhodu pro zájmy ČR.	Závažným způsobem může zasáhnout do fungování celé organizace a může vést až k ukončení činnosti.	Může závažně a dlouhodobě ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní či nadnárodní negativní publicity, s dlouhodobými účinky a požadavky přijetí politické odpovědnosti.	Může přímo nebo nepřímo vést ke ztrátám přesahujícím 10 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace). Pozn. v případě KII je hranice ztráty stanovena na 0,5% HDP.	Může způsobit rozsáhlé omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.
	ZůI	Narušení bezpečnosti informací v oblasti "důvěrnosti" může způsobit újmu zájmům České republiky anebo nevýhodnost pro zájmy České republiky a zároveň je informace typově uvedena v seznamu utajovaných informací (§ 2 písm. a) zákona č. 412/2005 Sb.). Na základě tohoto dopadu by se za splnění dalších legislativně stanovených podmínek mělo jednat o utajované informace. Pro určení odpovídajícího stupně utajení je třeba postupovat v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. A to za splnění dalších stanovených podmínek, např. uvedených v nařízení vlády č. 522/2005 Sb.									

** V případě, že je v některém z parametrů bezpečnosti (dostupnost, důvěrnost, integrita) dosaženo max. úrovně dopadu "Vysoká", měl by správce zvážit zařazení informačního systému mezi významné informační systémy (VIS), případně mezi informační systémy základní služby (ISZS).*
- Podmínkou pro zařazení systému mezi VIS je současné naplnění definice v § 2 písm. d) zákona č. 181/2014 Sb., a alespoň jednoho oblastního kritéria podle přílohy č. 2 k vyhlášce č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích a zároveň alespoň jednoho dopadového kritéria uvedeného v § 4 vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.
- Podmínkou zařazení systému mezi ISZS je naplnění definice v § 2 písm. i) a j) zákona č. 181/2014 Sb., a současné naplnění odvětvových kritérií a alespoň jednoho dopadového kritéria uvedeného v příloze vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatelů základních služeb.

*** V případě, že je v některém z parametrů bezpečnosti dosaženo úrovně dopadu "Kritická", měl by správce zvážit zařazení informačního nebo komunikačního systému mezi prvky kritické informační infrastruktury (KII), případně mezi informační systémy základní služby (ISZS).*
- Podmínkou zařazení systému mezi KII je současné naplnění definice v § 2 písm. b) zákona č. 181/2014 Sb., a alespoň jednoho odvětvového kritéria v odvětví VI., oblasti G. Kybernetická bezpečnost podle přílohy k nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury a zároveň alespoň jednoho průřezového kritéria uvedeného v § 1 nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.
- Podmínkou zařazení systému mezi ISZS je naplnění definice v § 2 písm. i) a j) zákona č. 181/2014 Sb., a současné naplnění odvětvových kritérií a alespoň jednoho dopadového kritéria uvedeného v příloze vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatelů základních služeb.

Poznámka ke sloupci „Ochrana osobních údajů":
Požadavky na zpracování osobních údajů v cloudových službách musí dle nařízení GDPR vycházet z hodnocení rizik daného scénáře zpracování pro práva a svobody fyzických osob. V případě zjištění vysokého rizika budou správci povinni provést tzv. „posouzení vlivu zpracování dat na ochranu osobních údajů" (DPIA, viz čl. 35), a zajistit adekvátní bezpečnostní opatření a mechanismy ochrany. Přitom předpokládáme využití některého ze schválených „kodexů chování" (viz čl. 40 GDPR) daným zpracovatelem a jeho cloudovou službou. Regulátor (ÚOOÚ) očekává, že do doby účinnosti nařízení GDPR bude schváleno několik kodexů chování, které vytvoří vhodný rámec standardizace pro vyšší úrovně dopadů zpracování osobních údajů.

Seznam použitých zkratek:
GDPR - nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
ISVS - zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
ISZS - informační systém základní služby podle § 2 písm. j) zákona č. 181/2014 Sb.
KII - kritická informační infrastruktura podle § 2 písm. b) zákona č. 181/2014 Sb.
PZS - provozovatel základní služby podle § 2 písm. k) zákona č. 181/2014 Sb.
ÚOOÚ - Úřad pro ochranu osobních údajů
VIS - významný informační systém podle § 2 písm. d) zákona č. 181/2014 Sb.
ZKB - zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

Převzato z https://www.nukib.cz/download/publikace/podpurne_materialy/Priloha_1_dopadova_tabulka.pdf

PŘÍLOHA P II: HODNOCENÍ AKTIV

Stupnice pro hodnocení důvěrnosti	
Úroveň	**Popis**
Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP:WHITE.
Střední	Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:GREEN nebo TLP:AMBER.
Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:AMBER.
Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:RED nebo TLP:AMBER.

Stupnice pro hodnocení integrity	
Úroveň	**Popis**
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.

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

Převzato z vyhlášky č. 82/2018 Sb.