Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

CMMI-SOC: návrh Capability Maturity Modelu pro Security Operations Centra

DIPLOMOVÁ PRÁCE

Studijní program: Aplikovaná informatika

Studijní obor: Informační management

Autor: Bc. Lenka Vrbasová

Vedoucí diplomové práce: doc. Ing. Vlasta Svatá, CSc.

Praha, prosinec 2020

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně. Veškeré použité podklady, ze kterých jsem čerpala informace, jsou uvedeny v seznamu použité literatury a citovány v textu podle normy ČSN ISO 690.

V Praze dne 5. prosince 2020

_____

Podpis

Poděkování

Tímto bych ráda poděkovala své vedoucí diplomové práce doc. Ing. Vlastě Svaté, CSc. za pomoc a užitečné rady, které mi poskytla v průběhu tvorby této práce. Dále chci poděkovat všem zúčastněným lidem z týmu SOC, kteří se zapojili do testování nástroje a poskytli mi zpětnou vazbu. Na závěr bych chtěla poděkovat svým rodičům za jejich podporu a pomoc, kterou mi poskytovali po celou domu mého studia.

Abstrakt

Organizace v posledních letech čelí narůstajícímu počtu kybernetických útoků, které jim způsobují značné ztráty. Jistou obranou proti těmto útokům mohou poskytnou Security Operations Centra (SOCs). Jelikož budování vlastního SOC je docela novou záležitostí, nemají organizace zkušenosti, jak by takový SOC měl fungovat a jak měřit jeho výkonnost. Diplomová práce se zabývá návrhem Capability Maturity Modelu (CMM), který napomůže s měřením výkonosti SOC a zároveň s jeho řízením. Cílem je vytvořit CMM, který bude snadno aplikovatelný v praxi, pomůže organizacím určit úrovně schopnosti a zralosti a umožní identifikovat příležitosti ke zlepšení služeb SOC. CMM byl vytvořen na základě Beckerovy metodiky tvorby modelů zralosti pro řízení IT.

Teoretická část práce se věnuje popisu SOC a jeho komponentám, standardům pro řízení informační bezpečnosti a již existujícím CMM modelům, které se zabývají bezpečností nebo aktivitami SOC. Teoretická část tak odpovídá na první dvě fáze Beckerovy metodiky (definice problému, porovnání stávajících řešení).

Praktická část se věnuje samotné tvorbě hodnoticího modelu a nástroje, který usnadní proces sebehodnocení. Při tvorbě modelu byly využity NIST Cybersecurity Framework a COBIT 2019. Výsledný CMM měří úrovně schopnosti a zralosti napříč devíti doménami: bezpečnostní analýza, vytváření báze znalostí, monitorování, detekční pravidla, řízení přístupových práv, zvládání bezpečnostních incidentů, poincidentní aktivity, údržba bezpečnostních nástrojů a řízení zranitelností. Tento model byl integrován do nástroje umožňujícího snadné sebehodnocení. Nástroj byl následně otestován v jednom českém SOC týmu. Výsledky sebehodnocení a samotný nástroj jsou k dispozici samostatně mimo tento dokument.

Klíčová slova

CMM, COBIT, NIST Cybersecurity Framework, SOC, úrovně schopnosti, úrovně zralosti.

Abstract

Nowadays organizations face an increasing number of cyberattacks that cause them significant losses. Security Operations Center (SOC) could provide some defence against these attacks. Since building your own SOC is quite a new matter, organizations do not know how to manage the SOC and how to measure its performance. The diploma thesis deals with the design of the Capability Maturity Model for Security Operations Center. The aim of the thesis is to develop a CMM that will be efficient in practice, allows organizations to establish the capability and maturity levels of the SOC and identify opportunities to improve SOC services. CMM was designed based on Becker's methodology for developing maturity models for IT Management.

The theoretical part deals with the description of the SOC and its components, standards for Information Security Management and related existing CMM. The theoretical part addresses the first two phases of Becker's methodology (Problem definition, Comparison of existing maturity models).

The practical part addresses development of an evaluation model and o tool, that facilitates the self-assessment process. The model is in alignment with NIST Cybersecurity Framework and COBIT 2019. Capability and maturity levels are measured across nine domains: Security Analysis, Build Cyber & Threat Intelligence, Monitoring, Detection Rules, Identity & Access Management, Incident Response, Post-incident Activities, SOC Tools Maintenance, Vulnerability Management. CMM was integrated into a self-assessment tool, which was subsequently tested in a Czech SOC team. The tool and the results of the self-assessment with recommendations for further SOC growth are available separately outside of this document.

Keywords

CMM, COBIT, NIST Cybersecurity Framework, SOC, capability levels, maturity levels.

Obsah

Seznam obrázků

Seznam zkratek

APT	Advanced Persistent Threat
ARC	Appraisal Requirements for CMMI
C2M2	Cybersecurity Capability Maturity Model
CEO	Chief Enterprise Officer
CISO	Chief Information Security Officer
CIO	Chief Information Officer
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
CMMI-SOC	Capability Maturity Model Security Operations Center
COBIT	Control Objectives for Information and related Technology
CPM	COBIT Performance Management
CTI	Cyber & Threat Intelligence
DDoS	Distributed Denial of Service
DSR	Design Science Research
EDR	Endpoint Detection and Response
EGIT	Enterprise governance of Information Technology
FISMA	Federal Information Security Management Act
GDPR	General Data Protection Regulation
HIDS	Host-based Intrusion Detection System
HIPAA	Health Insurance Portability and Accountability Act
HP SOMM	Hewlett-Packard Security Operations Maturity model
ICT	Information and Communication Technologies
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IM	Incident Management

IOC	Indicators of Compromise
IP	Internet Protocol
IPS	Intrusion Prevention System
IR	Incident Response
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITG	Information Technology Governance
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
MTTD	Mean time to detect
MTTR	Mean time to respond
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
NIST CSF	NIST Cybersecurity Framework
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
O-ISM3	Open Information Security Management Maturity Model
OSINT	Open Source Intelligence
P3M3	Portfolio, Programme and Project Management Maturity Model
PCI-DSS	Payment Card Industry Data Security Standard
SCAMPI	Standard CMMI Appraisal Method for Process Improvement
SEM	Security Event Management
SEI-CMU	Software Engineering Institute - Carnegie Mellon University
SIEM	Security Information and Event Management
SIM	Security Information Management
SOC	Security Operations Center

SOX	Sarbanes-Oxley Act
SSE-CMM	Systems Security Engineering CMM
TLM	Threat Lifecycle Management
TQM	Total Quality Management
VPN	Virtual Private Network

Úvod

It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it.

(Stephane Nappo)

Radikální zvětšení objemu informací ve světě má za následek přetvoření doposud industriální společnosti na společnost informační, ve které kvalita života, sociální změny i ekonomický rozvoj závisí stále více na informacích a na jejich využívání. S tím jde ruku v ruce vývoj informačních a komunikačních technologií (ICT), které lidstvu napomáhají tyto informace sbírat, uchovávat, přenášet a zpracovávat.

Je třeba si uvědomit, že data a informace v sobě zahrnují značný ekonomický i politický potenciál a mohou rozhodovat o samotné existenci jednotlivců, firem či zemí. Kromě pozitivních dopadů informačních a komunikačních technologií přináší i ty negativní. Jelikož se společnost přeorientovala a zdá se, že informace jsou nejcennějším druhem aktiv, vzniká nové pole působnosti pro trestnou činnost zvanou kyberkriminalita.

Podle pravidelných ročních průzkumů společnosti IBM počet kybernetických útoků na společnosti neustále roste. Každý takový útok podniky stojí statisícové částky. Náklady spojené s kybernetickými incidenty sice nominálně poklesly z 3,92 mil. USD v roce 2019 na 3,86 mil. USD v roce 2020, ale při bližším zkoumání bylo odhaleno, že tento pokles byl zapříčiněn společnostmi, které se rozhodly investovat do informační bezpečnosti a obraně proti kyberkriminalitě. Náklady společností, které se rozhodly neinvestovat do rozvoje informační bezpečnosti, byly značně vyšší. Na toto zjištění navazuje statistika, kdy největší náklady na únik informací zaznamenaly sektory zdravotnictví, energie a finančnictví přímo v tomto pořadí. (IBM Corporation, 2020)

Možností, jak minimalizovat únik informací a další negativní působení útočníků, je zvýšit zabezpečení informací a zařízení, která pracují s těmito informacemi, a neustále sledovat podnikové prostředí, zda nedochází k nekalým aktivitám. Možností, jak se bránit kyberkriminalitě, je mít v organizaci oddělení Security Operations Center (SOC). Ten je pověřen sledováním bezpečnostních aktivit v organizaci a při odhalení bezpečnostního incidentu má za úkol zamezit co nejrychleji negativnímu působení a ztrátám.

Cíl práce

Čím kvalitnější a zkušenější SOC tým je, tím je větší pravděpodobnost, že dokáže odvrátit nebezpečné aktivity. Jelikož se bezpečnost začíná teprve v podnicích rozvíjet, existuje jen malé povědomí, jak SOC spravovat a jak si ověřit, že SOC odvádí kvalitní práci. Proto si tato práce klade za cíl vytvořit model hodnocení schopnosti a zralosti SOC (Capability Maturity Model – CMM), který umožní bezpečnostním expertům, auditorům, vedoucím pracovníkům i jiným osobám zhodnotit, jak dobře si SOC ve svém počínání stojí. Aby testování mohla provádět široká veřejnost, která nemá speciální znalosti ohledně metodik hodnocení schopnosti a zralosti, je třeba vytvořit nástroj, který pomůže snadno měřit úrovně schopnosti a zralosti základních aktivit, které by měl SOC vykonávat.

Motivace a očekávané přínosy

Během své práce v oblasti informační bezpečnosti a ve spolupráci s různými SOC týmy jsem narazila na problém, kdy většina bezpečnostních aktivit byla řízena nahodile bez jakýkoliv standardů. Některé společnosti se sice snažily naplňovat podmínky vycházející s různých rámců či standardů typu COBIT, ITIL nebo ISO/IEC27001, ale ty nedefinují specifické aktivity pro týmy SOC, ale spíše se tématům řízení informačních technologií a informační bezpečnosti věnují obšírně. Ve firmách tak často docházelo k nejasnostem, kdo je za co odpovědný.

Dalším problémem byl tlak managementu měřit výkonnost SOC. Při hlubším zkoumání nebyly nalezeny metodiky, které by definovaly, jak výkonnost SOC měřit. Z toho důsledku docházelo ke zcela nesmyslným nastavováním KPI (Key Performance Indicator), která nedokázala napovědět, jak účinné a účelné aktivity SOC jsou.

Třetím problémem byl nesoulad mezi interním auditem a SOC. Interní auditoři často nemají dostatečné znalosti ohledně informační bezpečnosti a ani znalosti technické. Na druhé straně SOC nemá často zkušenosti s hodnoticími rámci či jinými metodikami pro efektivní řízení procesů. To způsobovalo jistou bariéru v komunikaci a kooperace týmů byla značně neefektivní a zbytečně zdlouhavá.

Vytvoření uceleného hodnoticího modelu CMM by mohlo odstranit výše zmíněné problémy. Tým SOC by dostal určitou zpětnou vazbu ohledně kvality svých aktivit. Zároveň na základě měření dokáže navrhnout budoucí vývoj, kam by tým SOC měl směřovat. Vrcholovému vedení CMM měření usnadní sledovat progres SOC napříč jednotlivými aktivitami. V neposlední řadě nástroj může být použit interním auditem pro hodnocení úrovně bezpečnosti. Nástroj staví na bezpečnostním rámci NIST Cybersecurity Framework (NIST CSF), který je čím dál tím častěji používaným rámcem pro hodnocení kybernetické i informační bezpečnosti.

Použité metody a metodiky

Pro vytvoření modelu byla vybrána Beckerova metoda založená na Design Science Research, kterou objasňuje ve své práci Developing Maturity Models for IT Management. V ní definuje několik fází vývoje CMM. Vydefinování jednotlivých aktivit, které CMM měří, bylo prováděno pomocí systematické analýzy literatury. Hlavními zdroji pro vydefinování aktivit se staly knihy *Designing and Building Security Operations Center* od Davida Nathanse a *Ten Strategies of a World-Class Cybersecurity Operations Center* od Carsona Zimmermana. Jednotlivé aktivity byly následně namapovány na NIST CSF. Aktivity značící jednotlivé úrovně schopnosti následně vychází z COBIT 2019. Logika vyhodnocování úrovní schopnosti a zralosti také vychází z COBIT 2019, konkrétně z metody COBIT Performance Management (CPM).

Výsledný CMM byl integrován do nástroje vytvořeného v Microsoft Excel. Kvalita nástroje byla řízena, kontrolována a testována na základě požadavků vydefinovaných v normě ISO/IEC 25010:2011. Finální nástroj byl otestován v praxi.

1 Security Operations Center

Pod pojmem Operations Center si většina osob vybaví obrázek kolosální tmavé místnosti bez oken s velkými obrazovkami připevněnými na zdi, jak je tomu ve společnosti NASA. Lidé sedí naproti těmto velkým obrazovkám se svými počítači za stoly, které jsou postaveny do půlkruhu. Koncept Security Operations Centra (dále jen SOC) je velmi blízký této představě. Jedná se o tým expertů, který pomocí speciálních nástrojů usiluje o prevenci, detekci, analýzu a zvládání bezpečnostních incidentů. Práce bezpečnostních expertů je založena na „day to day" aktivitách, kdy se snaží chránit podniková data a zařízení pracující s těmito daty, jako jsou například servery, databáze, či sítě.

V různých slovnících i v praxi se lze setkat s vícero pojmy, které však často reprezentují stejnou pracovní skupinu, zabývající se bezpečnostním dohledem. Jedná se například o:

- Computer Security Incident Response Team (CSIRT)
- Computer Incident Response Team (CIRT)
- Computer Incident Response Center (or Capability) (CIRC)
- Computer Security Incident Response Center (or Capability) (CSIRC)
- Security Operations Center (SOC)
- Cybersecurity Operations Center (CSOC) (Carson Zimmerman, 2014)

Podle průzkumu společnosti Ernst & Young z roku 2019 bylo zjištěno, že služeb SOC využívá již 72 % velkých společností a 40 % malých společností. (Ernst & Young, 2019)

Některá SOC bývají zakládána, aby byla zajištěna vyšší ochrana firemních dat. Některé organizace zakládají SOC v důsledku vnějšího tlaku. Pro společnosti v českém prostředí se jedná zejména o tyto faktory:

Vnitřní faktory:

- Růstový trend bezpečnostních incidentů
- Ochrana aktiv organizace
- Ucelený přehled informačních aktiv
- Ochrana a kontrola zaměstnanců

Zákonné faktory:

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)
- Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)
- Zákon č. 412/2005 Sb. o ochraně utajovaných informací a bezpečnostní schopnosti

- 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)

Regulatorní požadavky a směrnice:

- Rodina norem ISO/IEC 27000
- Lokální standardy ČSN
- Směrnice GDPR
    - Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
    - Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.
- Směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii
- SOX – Sarbanes-Oxley Act
- JSOX – japonské požadavky stavící na Sarbanes-Oxley Act
- HIPAA – Health Insurance Portability and Accountability Act
- PCI-DSS – Payment Card Industry Data Security Standard

Na SOC lze nahlížet ze tří perspektiv, kterými jsou jednotlivé osoby tvořící systém personálního zajištění, procesy jako jádro provozních aktivit, které SOC pravidelně vykonává, a technologické nástroje, které tyto procesy zajišťují a podporují. Interakcí těchto tří prvků je možné vytvořit bezpečné prostředí.

1.1 Personální obsazení

Tým SOC během své práce komunikuje napříč celou společností doslova se všemi jednotkami, ať už se jedná o vrcholové vedení společnosti, lidské zdroje, právní oddělení, oddělení odpovědné za soulad s předpisy tzv. Compliance, či informační technologie (IT). Tyto útvary se stávají jak objektem monitoringu, tak spolupracujícími jednotkami při řešení jednotlivých bezpečnostních událostí a v neposlední řadě i zákazníky SOC. Kvůli této silné potřebě komunikace se všemi je třeba, aby útvar SOC měl určitou nezávislost na jiných odděleních. Neměl by podléhal tlaku nadřízeného vedení ani jedné ze složek. Díky tomu se vyvaruje střetu zájmů. Zároveň by SOC měl být podporován vedením společnosti a jeho práva a povinnosti by měly být deklarovány shora firemní instrukcí, nejčastěji zakotvením do dokumentu nazvaném Bezpečnostní politika.

Pokud firma chce brát bezpečnost vážně, je zapotřebí, aby oddělení bezpečnosti se SOC týmem bylo co možná nejvýše postavené v organizační struktuře. Ideálně ho mít jako samostatné oddělení, které se přímo zodpovídá nejvyššímu řediteli společnosti (CEO – Chief Executive Officer) či představenstvu společnosti (Board of Directors). Bezpečnost v organi-

zacích není jen otázkou IT problémů, ale má i velký dopad na podnikání, a tím pádem na celou společnost. Proto je nezbytné, aby SOC měl přímou vazbu na vedení společnosti, kterému pravidelně prezentuje zjištěné nedostatky a navrhuje možná protiopatření. Ty vedení společnosti přezkoumává, ohodnocuje míru závažnosti a na základě doporučení zavádí potřebné protiopatření napříč celou organizací. Společnosti v dnešní době musí zajistit dostatečnou bezpečnost, aby došlo ke snížení rizika na přijatelnou úroveň. Pouze vedení společnosti dokáže určit, kde se taková úroveň přijatelnosti nachází. (Nathans, 2014)

Ne vždy se SOC a oddělení bezpečnosti v organizacích vyskytuje jako samostatná entita, ale spadá pod nějaké jiné oddělení. Přidělení je často dáno historií, jak společnost nahlížela na samotnou bezpečnost informací. Zda ji brala jako zabezpečení IT aktiv, zda se jednalo o reakci na působící tlak ze strany legislativních nařízení, či jako určitá nástavba interního auditu, který se rozhodl věnovat bezpečnosti. Pokud je tomu tak, nejčastěji v praxi bývá SOC zařazen pod následující oddělení.

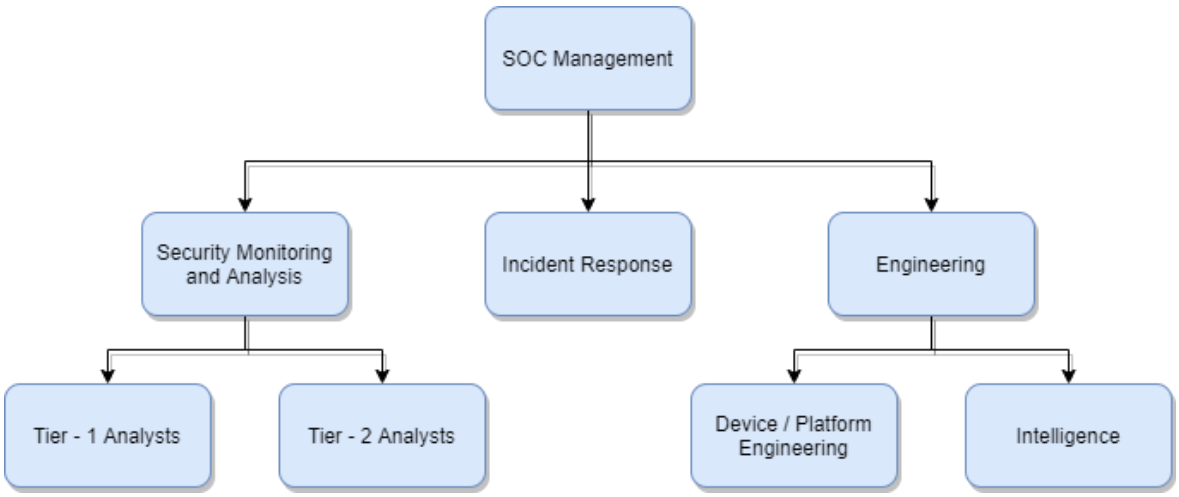
- **Právní oddělení (Legal)** – Mnoho bezpečnostních požadavků plyne přímo ze zákona nebo jiných směrnic. I když vrcholové vedení nevnímá potřebu v podniku budovat informační bezpečnost, působí na něj tlak ze strany zákona, který musí za každou cenu respektovat. To dává SOC vyšší vymáhací pravomoci, protože s nesplněním zákonem daných bezpečnostních požadavků plynou často nejrůznější postihy. Toto prosazování bezpečnosti je ale dosti těžkopádné a nepůsobí dobré vztahy, protože podnik vnímá zavádění bezpečnostních opatření jako nutné zlo, které brzdí podnikání a inovace. Tyto nepříliš dobré vztahy následně mají negativní vliv na efektivnost práce SOC.
- **Oddělení Informačních technologií (IT)** – Hlavním představitelem IT je Chief Information Officer (CIO), který je také členem vrcholového vedení. Vedoucí pracovník za informační bezpečnost (Chief Information Security Officer – CISO) často spadá právě pod něho. Toto zařazení je dáno nejčastěji tím, že IT implementuje technologie, které je třeba sledovat a chránit. Nejdříve se tak o bezpečnost staral jeden člověk v rámci IT a následně došlo na základě potřeby k vytvoření speciálního oddělení, které často už pod IT zůstalo. Tento model zařazení bezpečnosti je také obvyklý u malých organizací. Mezi výhody patří rychlá odezva a včasná komunikace bezpečnostních opatření, kdy odstranění nedostatků nemá za následek tak velké náklady jako v jiných možnostech organizačního začlenění SOC. Zařazení pod IT v mnoha případech může působit problémy plynoucí z odlišnosti cílů. IT je odpovědné za dodávku přidané hodnoty za přesně vymezený čas a daných nákladů. To bohužel jde proti informační bezpečnosti, která vyžaduje neustálé revize, testování a patching informačních aktiv a minimalizaci rizik, což zvyšuje náklady a potřebný čas k nasazení do produkčního prostředí. V takové situaci je třeba s vedením organizace projednávat, co má vyšší prioritu.
- **Oddělení Compliance** – Oddělení se zaměřuje na soulad jednání podniku, zaměstnanců a vedení s právními normami, vnitropodnikovými směrnicemi a různými standardy. Spadá sem často také oddělení auditu. V takovém prostředí je bezpečnost vnímána a brána s nadšením a buduje se proaktivní jednání jednotlivců. Má to však také i své nevýhody. Pokud je společnost teprve ve svých začátcích, zavádí se nové technologie a buduje se IT infrastruktura, je složitější do těchto prvků začle-

nit bezpečnostní opatření. To vzniká v důsledku nepřímé komunikace mezi IT oddělením, které technologie zavádí, a oddělením informační bezpečnosti. Komunikace mezi těmito dvěma odděleními probíhá přes samotné vedení organizace, kdy jakýkoliv bezpečnostní zásah je již často se značným zpožděním.

1.2 Role a odpovědnosti

Každý SOC tým by měl mít sepsán dokument, kde má každá role v týmu SOC přesně vydefinované pravomoci a odpovědnosti. Jelikož práce analytiků je často na pomezí bezpečnostních zákonů a ochrany osobních práv jednotlivců, je třeba mít přímo vydefinované ze strany právníků, co je ještě z hlediska práva akceptováno a naopak, co již je mimo kompetence pracovníka. S těmito odpovědnostmi musí být každý ze zaměstnanců bezpečnostního oddělení před výkonem své práce seznámen. Dalšími vhodnými dokumenty jsou interní OLA (Operational-level agreement), která upravují spolupráci, odpovědnosti a komunikaci dalších oddělení vůči oddělení bezpečnosti.

V malých organizacích se často objevuje problém s řízením bezpečnosti kvůli limitovanému počtu zaměstnanců. Pokud je třeba vybudovat uvnitř organizace SOC, je nezbytné, aby nově vzniklý tým měl alespoň složku analytiků pro monitoring aktivit, incident response tým a bezpečnostní techniky (viz Obrázek 1-1). Pokud kapacity dovolují, je vhodné do týmu SOC zařadit i jednotlivce odpovědné za reporting aktivit různým zainteresovaným stranám a bezpečnostní architekty.



Obrázek 1-1 Základní organizační struktura SOC (Zdroj: Autor na základě (Nathans, 2014))

1.2.1 Vedení SOC

Týmový leader

Jelikož klasický SOC pracuje v režimu 24 hodin 7 dní v týdnu, je třeba tento časový úsek rozdělit do jednotlivých směn. Nezáleží, jestli jde o tři směny po osmi hodinách nebo o dvě směny po 12 hodinách. Každopádně jednotlivé směny musí mít odpovědnou osobu, která zajistí její hladký průběh. Tato osoba musí mít přehled o všem a o všech. Nejčastěji se jedná o nejzkušenějšího člena SOC. Měla by zvládat každou věc lépe než jakýkoliv člen týmu, být odolný vůči stresovým situacím, umět poradit, umět na základě potřeb určovat priority úkolů, mít maximální přehled o procesech a procedurách nejen v rámci SOC, ale i v celé organizaci. Důležité je, aby tato osoba dobře znala jednotlivé členy, protože hodnotí jejich výkon a stanovuje, kam by se jejich kariéra měla ubírat dále. Týmový leadeři přímo reportují události a aktivity, co se odehráli během jednotlivých směn přímo SOC Manažerovi a dalším SOC leaderům.

SOC Manažer

Odpovědnou osobou za chod a výsledky oddělení bezpečnostního dohledu je SOC Manažer. Ručí za monitoring, zlepšování výkonnosti a řízení všech aspektů v rámci SOC. Hlavní náplní je být prostředníkem mezi SOC a zbytkem organizace. Takový člověk by měl mít silný technický základ, být dobrý v komunikaci a ve vyjednávání, protože přímo komunikuje s vrcholovým vedením, či představenstvem. Musí umět přeložit podnikové cíle do jednotlivých dílčích technických cílů, které bude jeho tým následovat. Důležité je také umět komunikovat jednotlivé požadavky podniku na techniky a analytiky. Zároveň musí umět vysvětlit zbytku organizace technické věci takovým způsobem, aby to bylo pro ně srozumitelné. SOC Manažer je kontaktní osobu pro jakéhokoliv externího stakeholdera (jde o zájmové skupiny jako například dodavatelé, policie, NÚKIB, další úřady atd.). V Mnoha organizacích pozici SOC Manažera zastupuje ředitel bezpečnosti, zkráceně CISO, který bývá ve společnostech hlavním představitelem informační bezpečnosti. Záleží často na velikosti týmu bezpečnosti, zda tento tým zahrnuje i jiné úsekové útvary, jako jsou například IT bezpečnostní architekti, tým zabývající se bezpečnostními standardy a jejich dodržováním, tým řešící informační rizika a další.

1.2.2 Bezpečnostní Monitoring a Analytici

Jedná se o jádro celého SOC. Jejich hlavní náplní je monitoring podnikové infrastruktury a prošetřování bezpečnostních událostí zaznamenaných z informačních aktiv organizace. Velikost této skupiny by se měla odvíjet od počtu tiketů (bezpečnostních hlášení), které je třeba na denní bázi odbavit. Proto je nezbytné stanovovat kapacitní metriky oddělení, aby bylo zaručeno, že bude v čas za stanovených podmínek analyzováno vše, co je potřeba. Pro stanovení metrik je třeba započíst i čas zapojených účastníků mimo SOC, protože v některých případech je nutno povolat experty, kteří mohou být z jiných oddělení. Analytiky lze rozdělit do několika úrovní. Dělení podléhá nejčastěji senioritě nebo jsou rozděleni podle expertízy jednotlivých podnikových oblastí (interní x externí perimetr, aplikace, technologie, cloud atd.).

L1 – Junior Analytik

Analytici této úrovně fungují jako první síto bezpečnostních hlášení. Není jim dána žádná flexibilita. Měli by odbavovat jen ty tikety, ke kterým existuje předem vydefinovaný postup v SOC bázi znalostí. Existuje-li postup, tiket vyřeší sami. Avšak pokud žádný postup k danému hlášení neexistuje, eskalují tiket na L2 analytiky. Každý nově příchozí analytik, by měl začínat na této úrovni, i když má potřebné hlubší znalosti na úrovni analytiků vyšších úrovní. Problémem totiž často nejsou technické znalosti, ale procesy, kterými se organizace řídí a je nezbytné, aby se analytik s nimi seznámil. To, co je v jedné organizaci běžnou praxí, může být v jiné bezpečnostním incidentem.

L2 – Senior Analytik

Analytik L2 by měl být více specializovaný pro určitou doménu, než je tomu u Analytika L1. Dále se předpokládá, že Analytik L2 rozumí politice a procesům organizace. Analytici L2 by měli být vybíráni dle aktuálních SOC potřeb, které jsou dány specifickými cíli SOC, strategií informační bezpečnosti a využívanými technologiemi.

L3 – Expert Analytik

Role, která není příliš častá v týmu analytiků. L3 jsou velmi úzce specializovaní v určité oblasti. Jedinci se nachází buď zcela mimo SOC tým, nebo je můžeme najít mezi bezpečnostními techniky. Zkoumají, proč něco nefunguje tak, jak by mělo.

1.2.3 Bezpečnostní technici

Může se jednat o velice specializované osoby s velice úzkým expertním profilem. Měli by být nejvíce technicky zdatnými osobami v týmu. Jejich hlavní odpovědností je zajištění bezpečnostní infrastruktury, nasazování nástrojů pro práci analytiků, jejich údržbu a nastavování pravidel pro monitoring. Nejčastěji se jedná o techniky zajišťující správné fungování nástroje zvaného SIEM (Security Incident and Event Management). (Siemplify, 2017)

Bezpečnostní technici mohou také zastávat roli L3 analytiků pro poslední úroveň eskalace incidentů a problémů. Vyšetřují, proč věci nefungují tak, jak by měly. Mohou také zastávat roli bezpečnostních architektů při implementaci různých technologií. Fungují jako komunikační prostředník mezi bezpečnostními analytiky a oddělením IT, kdy analytici objeví problém, inženýři provedou techničtější analýzu a zakládají požadavek na IT, aby došlo k odstranění chyby. Nachází se zde lidé odpovědní za forenzní analýzu a malware analytici.

1.2.4 Incident Response Manažer

Dojde-li k potvrzení události jako bezpečnostního incidentu, je třeba zahájit neodkladné odstranění chyby a navrácení systému do původního stavu. Jedná-li se o incidenty nižší klasifikace, za incident odpovídají sami analytici. Objeví-li se ale incidenty vyšší úrovně (Major Incidents), dojde k eskalaci incidentů od analytiků na vyšší instanci. Za incidenty vyšší úrovně odpovídá tým Incident Response. V menších SOC se často jedná o jednu osobu, avšak ve větších „dodavatelských“ SOC tuto roli zastává více pracovníků. Kromě zvládání bezpečnostních incidentů odpovídají za vytváření a úpravu procesů a procedur spojených

s Incident Managementem, aby bylo zajištěno, že používané postupy jsou účinné, účelné a jsou co nejaktuálnější.

1.3 Technologické nástroje

Prakticky každý SOC během své práce využívá vícero nástrojů a technologií, které generují, shromažďují, analyzují, ukládají a prezentují pracovní skupině SOC velké množství dat, které jistým způsobem souvisí s bezpečností. Základní funkcí je sledování perimetru a odhalování škodlivých aktivit a anomálií. Takovým nástrojům, které mají za cíl odhalit nežádoucí chování, se říká detekční nástroje. Patří mezi ně nástroje typu SIEM, IDS/IPS systémy a Vulnerability skeny. Zajištění bezpečnosti a následné řešení bezpečnostních událostí na koncových zařízení bývá často problémové kvůli nemožnosti tato zařízení osobně spravovat. Tento problém řeší systémy typu EDR. Jako doplňkové nástroje, které podporují efektivní fungování SOC patří tiketovací nástroj, báze znalostí a sdílená e-mailová schránka.

1.3.1 SIEM

SIEM je zkratkou pro Security Information and Event Management. Z definice vyplývá, že základní schopností SIEM je dlouhodobý sběr dat do centrální databáze, jejich analýza a následné hlášení problémů. Tato aktivita bývá označována jako SIM (Security Information Management). SIM získává informace z logů, které mohou obsahovat mnoho různorodých dat. SIM zajišťuje reportování a vyhledávání trendových anomálií z dlouhodobého hlediska. Kromě této aktivity se SIEM zabývá monitoringem infrastruktury, korelacemi událostí a alertováním v reálném čase, což je označováno jako SEM (Security Event Management). Zde se SEM technologie dívá více do hloubky na specifické druhy událostí (eventů) a to zajišťuje okamžitou reakci SOC na anomálie v systému. Samotnou kategorii bezpečnostního nástroje SIEM, který tak propojuje SIM a SEM v jeden ucelený celek, uvedla na trh společnost Gartner (Gartner Inc., 2020), která SIEM definuje následovně:

„Security information and event management (SIEM) je technologie podporující detekci hrozeb, dodržování souladu s předpisy a řízení bezpečnostních incidentů prostřednictvím shromažďování a analýzy bezpečnostních událostí (jak v reálném čase, tak i historicky), jakož i celé řady dalších zdrojů událostí a kontextuálních dat. Základními schopnostmi jsou široký rozsah sběru a správy logů jednotlivých událostí, jejich analýza a další aktivity jako správa incidentů, dashboardy a reporting.“

SIEM je složen z různých komponent. Aktuální systémy obsahují buď všechny níže uvedené vlastnosti, nebo se jedná o redukovaná řešení, která nabízejí jen některé z nich. (Miller, 2011)

- **Log Management** – Má za úkol shromažďovat standardizované logy ze systémů, nad kterými SIEM následně pracuje. Kolekce logů je základním zdrojem informací o aktivitách uživatelů a systému během forenzní analýzy a auditu. Sběr logů ze systémů se používá jako bezpečnostní standard prokazující věrohodnost systémů, a dokonce jejich analýza je podmínkou udělující většinu bezpečnostních certifikací. (Kahonge et al., 2013) Do systému SIEM je napojeno mnoho zařízení, která nemají

standardizovaný formát logů. Pro korektní práci je třeba tyto logy normalizovat do jednotného formátu.

- **Korelace událostí** – Jde o spojování jednotlivých událostí z vícero zdrojů pro účely monitoringu za použití určitých znalostí podle toho, zda spolu souvisí a do jaké míry. Porovnání se provádí například na základě IP adresy a ID různých prvků. Datovými zdroji mohou být IDS, databáze, servery a další. Korelace může probíhat na základě předem vydefinovaných pravidel. Ty je třeba vydefinovat na základě známých hrozeb a vektorech známých útoků. Dalším typem je korelace založená na statistice. Jde o sledování odchylek od normálního stavu událostí.
- **Aktivní reakce** – Pro co nejefektivnější zvládání bezpečnostních incidentů je potřeba zkracovat délku celého životního cyklu incidentu. SIEM usnadňuje koordinaci incidentů, a tím tak zkracuje délku jejich životního cyklu. Kromě toho lze nastavit automatizované úlohy, které značnou část bezpečnostního hlášení dokáže vyřešit bez asistence bezpečnostního analytika. Jako automatizaci lze považovat také zabudované rozhraní pro tvorbu reportů, které mohou být automaticky distribuovány relevantním osobám.
- **Dlouhodobé uchovávání bezpečnostních událostí** – Podle legislativních požadavků je třeba po určitou dobu provádět archivaci logů takovým způsobem a v takové délce, aby tyto záznamy mohly být použity jako důkazní materiál v trestním řízení. (Kent a Souppaya, 2006)
- **Soulad s legislativou a vnitřními předpisy (Compliance)** – Organizace podléhají čím dál většímu tlaku ze strany nejrůznějších regulací. Nejvíce těchto omezení přichází ze zahraničí. Jedná se například o zákon SOX, GDPR, HIPAA, PCI-DSS, FISMA (BlackStratus, © 2019). V českém prostředí se jedná zejména o zákony č. 101/2000 Sb. o ochraně osobních údajů, č. 227/2000 Sb. o elektronickém podpisu, č. 412/2005 Sb. o ochraně utajovaných informací a bezpečnostní způsobilosti. Největší vliv na technologii SIEM má zákon č. 181/2014 Sb. nesoucí název Zákon o kybernetické bezpečnosti. Ten stanovuje technické požadavky na bezpečnost a konkrétně SIEM zvládá pokrýt 5 z 12 uvedených technických požadavků. Jedná se o:
    - Nástroj pro ochranu integrity komunikačních sítí
    - Nástroj pro ochranu před škodlivým kódem
    - Nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů
    - Nástroj pro detekci kybernetických bezpečnostních událostí
    - Nástroj pro sběr a vyhodnocování kybernetických bezpečnostních událostí (Zákon č. 181/2014 Sb.)
- **Zabezpečení koncových bodů** – Na pracovní stanice uživatelů se uplatňují bezpečnostní kontroly plynoucí z firemní politiky, která jistým způsobem omezuje užití zařízení, jako instalace dalšího software, blokace připojení externích disků a podobně. U serverů se sleduje veškerá komunikace mezi jednotlivými porty, kdy jakékoliv neobvyklé spojení je identifikováno a reportováno.
- **Reporting** – SIEM umožňuje generovat reporty, které poskytují plnohodnotné informace o stavu systému, bezpečnostních událostech i incidentech a zároveň funguje jako měřicí nástroj výkonu SOC týmu. Správný SIEM nástroj by měl být schopen

reporty generovat automaticky nebo ad-hoc dle potřeby. Jelikož příjemci zpráv jsou často netechnické útvary, je třeba, aby reportovaná data byla ve formátu grafů.
- **Podpora správy incidentů** – Kromě detekce bezpečnostních událostí, je nezbytné mít účinnou správu incidentů, kde lze incidenty klasifikovat. Jedná se o integrovaný tiketovací systém v rámci samotného SIEM. Jelikož SOC tým dostává hlášení o možných bezpečnostních incidentech i jiným způsobem než pomocí nástroje SIEM, je třeba mít samostatný tiketovací nástroj, kde se budou sbírat všechny podezřelé události.

Do SIEM je možné napojit další zařízení a na základě korelačních pravidel, signatur či manuálních analýz je následně možné identifikovat mnoho škodlivých aktivit. Mezi zdroji pro napojení lze zařadit: Active directory, různé druhy logů (aplikačních, databází, e-mailů, operačního systému), antivir, proxy servery, web proxy, VPN systémy, firewall, DLP, EDR, honeypoty, vulnerability skenery atd.). (Nathans, 2014)

Ve světě se používají SIEM nástroje jako jsou SolarWinds Security Event Manager, Splunk Enterprise Security, IBM QRadar, RSA Netwitness, LogRhythm NextGen SIEM Platform, McAfee Enterprise Security Manager a další.

1.3.2 IDS/IPS Systém

Základním kamenem pro většinu SOC je detekce incidentů na síťové úrovni. K tomu slouží IDS systémy (Intrusion Detection System). IDS je systém, který se na základě sledování síťového provozu, či chování operačního systému a procesů na koncových zařízení, pokouší odhalit pokusy o útok a další podezřelé činnosti, jako je například exfiltrace dat, skenování portů, či snaha o zneužití zranitelností. IDS se dělí na dva základní typy, kterými jsou HIDS a NIDS.

- **HIDS** (Host-based Intrusion Detection System), který pracuje s daty z konkrétních jednotlivých počítačových systémů. HIDS umožňuje přesně určit, které procesy a uživatelské účty jsou zapojeny do jakého konkrétního útoku na operační systém. Jelikož na rozdíl od NIDS mohou přímo přistupovat a sledovat datové soubory a systémové procesy, mohou snadněji určit zamýšlený výsledek pokusu o útok.
- **NIDS** (Network Intrusion Detection System) bývají umístěny na síťových prvcích nebo jsou v síti umístěny v podobě specializovaných sond. NIDS tak detekuje pokusy o útok pomocí zachycení a analýzy síťových paketů a snaží se hledat známé signatury anomálií. Při odposlechu síťového segmentu či switche, může jeden NIDS sledovat síťový provoz ovlivňující více hostitelů. Dokáže upozornit na odchozí provoz a na odesílání dokumentů, které odpovídají předem zvolené definici. (Committee on National Security Systems, 2015)

IPS (Intrusion Prevention System) je určitou nástavbou IDS, kdy nástroj již sám zasáhne, pokud eviduje podezřelou aktivitu. Nejdříve dojde k identifikaci škodlivých aktivit a zaznamenání informací o jejich průběhu. Následně se tyto aktivity zablokují a jsou nahlášeny bez-

pečnostnímu analytikovi, který následně provede manuální analýzu. IPS pomocí sond kontroluje příchozí a odchozí provoz, řeší ochranu před škodlivým kódem a hledá anomálie chování jednotlivých aplikací přistupujících ze/do sítě. Díky sondám lze tak monitorovat aktivity nebo dokonce blokovat škodlivou komunikaci, protože neprojde přes danou sondu.

Tyto nástroje však slouží spíše k prevenci před dobře známými typy útoků. Analýza často probíhá automaticky bez lidského zásahu, což je jejich slabina. Výstupy ze systémů IDS/IPS mohou ale být napojeny do systému SIEM, kdy při kombinaci s dalšími událostmi a analýze SOC analytiků mohou detekovat sofistikovanější typy útoků.

Mezi nejznámější IDS/IPS systémy se řadí Snort (open source), McAfee Network Security Platform a Trend Micro TippingPoint.

1.3.3 Skenery zranitelností

Při snaze minimalizovat počet bezpečnostních incidentů je se třeba zaměřit i na preventivní opatření. Mezi preventivní aktivity patří zejména řízení zranitelností (Vulnerability Management), které má za cíl identifikovat slabá místa v systémech, která mohou být zneužita pro průnik útočníků do prostředí společnosti. Nejčastěji se jedná o veřejné servery, které pomocí internetu umožňují komunikaci a výměnu dat s okolním světem. Pro identifikaci těchto slabin/zranitelností se používají tzv. skeny zranitelností (Vulnerability scans). Jedná se o nástroje, které identifikují a vytváří mapu sítě, což tvoří jakýsi inventář všech systémů. Identifikuje prvky jako jsou servery, databáze, notebooky, desktopové počítače, virtuální stroje, tiskárny, firewally a switche, které jsou v podnikové síti. Následně ke každému zařízení dokážou identifikovat konfigurační informace. Skenování zranitelností může být externí nebo interní. (Paul Rubens, 2019)

- **Externí skeny zranitelností**, které jak již napovídá název probíhají zvenčí sítě a jejich účelem je odhalit zranitelnosti, které mohou způsobit průnik do vnitřního systému. Jedná se například o identifikaci otevřených portů.
- **Interní skeny zranitelností** se provádí uvnitř sítě. Účelem je odhalení slabých míst, která mohou být zneužita útočníky, kteří se do vnitřní sítě už dostali. Nemusí se však jednat jen o útočníky zvenčí. Zranitelnosti systémů mohou být často zneužity podnikovými dodavateli nebo nespokojenými zaměstnanci.

Po zmapování síťových prvků dochází k automatizovanému otestování, zda se na těchto prvcích nepotvrdí nějaké známé zranitelnosti. Výsledkem kontroly je seznam všech systémů nalezených v dané síti a k nim identifikované známé zranitelnosti, kterým je třeba věnovat pozornost. Tyto zranitelnosti je třeba následně záplatovat (Patching), což má často na starosti Patch Management, který může vykonávat IT provoz nebo oddělení IT bezpečnosti.

Známými zástupci vulnerability skenů jsou Qualys Vulnerability Management, Tenable Nessus, Rapid7 Nexpose, Burp a Metasploit.

1.3.4 Endpoint Detection and Response

EDR je ochrana koncových stanic před škodlivým kódem a průnikem útočníka. Tento pojem se používá pro velkou paletu nástrojů, které se primárně zaměřují na detekci a investigaci

na koncových stanicích. Od běžných antivirových produktů se liší logováním důležitých aktivit. Sbírá informace ohledně změn v registrech a v souborových systémech, stažených souborech, vykonaných příkazech pomocí příkazové řádky nebo powershell, či DNS requestech. Analytik se může díky EDR vzdáleně připojit ke koncové stanici a dokáže tak vynutit ukončení škodlivého procesu, smazat soubory nebo je stáhnout pro detailnější analýzu. Vzdáleně také může zablokovat síťovou komunikaci infikovaného zařízení. (Anton Chuvakin, 2013)

Mezi EDR zástupce patří produkty jako CarbonBlack, RSA ECAT, CounterTack nebo CrowdStrike.

1.3.5 Tiketovací nástroj

Tým SOC se o incidentech dozvídá z mnoha zdrojů, jako je například hlášení HelpDesku, oznámení do společné schránky pro nahlašování incidentů, SIEM, nástroje pro skenování zařízení a zranitelností, ad-hoc manuální analýzy a mnohé další. Všechny tyto nálezy je třeba spravovat na jednom místě. K tomu slouží tiketovací nástroje. Analytik v nástroji pro daný incident vytvoří tiket s unikátním ID. Následně se provádí klasifikace a prioritizace incidentu, eviduje se průběh řešení a výstupy analýzy. Je možné vkládat přílohy jako například výpis logů, screen shoty a další. Pokud je potřeba participace jiných stran, zasílá se samotný tiket na dané oddělení/ osobu, Pokud tiket putuje mimo SOC a druhá strana by neměla znát veškeré detaily, správný tiketovací nástroj by měl umožnit skrýt tyto informace.

1.3.6 Knowledge base - WIKI

Samotná práce týmu SOC je dosti specifická a často vyžaduje hluboké znalosti různých problematik. Kromě technických znalostí je třeba znát podnikové normy, kulturu, architekturu infrastruktury a mnohé další. Tyto informace je třeba někde uchovávat a sdílet mezi jednotlivými členy týmu. Proto je vhodné budovat bázi znalostí, kde budou všechny aspekty práce popsány. Správná báze znalostí by měla obsahovat manuál pro nově příchozí, popis bezpečnostních nástrojů, popis podnikové infrastruktury a pracovní postupy.

Důležitou složkou báze znalostí je popis pravidel systému SIEM, který by měl obsahovat informace o tom, jak bezpečnostní pravidlo funguje, jak má probíhat analýza a popis, kdy se jedná o false positive hlášení a kdy naopak o true positive hlášení. V neposlední řadě je třeba vydefinovat procedury a procesy SOC při hlášení bezpečnostních událostí, zvládání bezpečnostních incidentů, zajištění zařízení, zajištění kontinuity činností a další.

1.3.7 Mailová schránka SOC

Pro komunikaci mezi SOC týmem a zbytkem organizace slouží mailová schránka, kam přichází důležité a zajímavé informace. Kromě hlášených bezpečnostních incidentů sem chodí informace o nových zranitelnostech, bezpečnostní reporty, výsledky virus skenů a další zajímavé informace, které SOC zpracovává. Dále pomocí týmové emailové adresy SOC komunikuje jak na interní uživatele, tak i na externí zájmové skupiny, jako jsou vládní úřady, policie, NÚKIB a další.

Společná e-mailová schránka také může sloužit jako informační kanál pro celý SOC tým, kde každý člen vidí, co se aktuálně řeší a jak. To napomáhá sdílení informací během řízení bezpečnostních incidentů.

1.4 Procesy a služby

Mise SOC by se dala shrnout následovně. SOC je odpovědný za monitoring, analýzu a mírnění dopadu významných bezpečnostních událostí pro zajištění dostupnosti, důvěrnosti a integrity informací. S tím souvisí zajištění ochrany dalších aktiv, které pracují s těmito informacemi. (Sundaramurthy et al., 2014)

Mít vlastní dohledové centrum se pojí s nemalými investicemi. Proto společnosti nejčastěji využívají kombinovaný model, kdy základní nezbytné aktivity jsou prováděny vlastními silami podniku. Ostatní aktivity jsou outsourcingovány u jiných specializovaných firem. Mezi nejčastější aktivity interního SOC patří zvládání bezpečnostních incidentů a skenování bezpečnostních zranitelností. Naproti tomu nejčastěji outsourcingovanými službami jsou provádění penetračních testů, vytváření Threat Intelligence, real-time security monitoring sítí, digitální forenzní analýza a analýza malware. (Ernst & Young, 2019)

Jak již bylo nastíněno výše, SOC poskytuje mnoho bezpečnostních služeb, které se často odvíjí od mise, účelu a konzumentů jejich služeb. Všechny tyto služby pro přehlednost lze rozdělit do tří kategorií. (West-Brown et al., 2003)

- **Reaktivní služby** – Tyto služby jsou poskytovány na základě reakce na určitý spouštěč, kterým může být nějaká událost či požadavek. Například identifikace škodlivého kódu v e-mailové zprávě jdoucí na představenstvo společnosti. Reaktivní služby jsou základní součástí práce SOC. Patří sem aktivity jako zvládání bezpečnostních incidentů, monitoring a ohlašování podezřelých aktivit, či bezpečnostní analýza.
- **Proaktivní služby** – tyto služby poskytují pomoc a informace pro přípravu, ochranu a zabezpečování systémů proti škodlivým aktivitám jako je útok na systémy. Výkon těchto služeb může v budoucnu značně snížit počet incidentů. Jedná se zejména o služby jako jsou řízení zranitelností, vývoj, údržba a nastavování bezpečnostních nástrojů, bezpečnostní audit a assessment, ladění bezpečnostních pravidel a tvorba scénářů, sledování dění mimo organizaci týkající se bezpečnosti a další.
- **Bezpečnostní služby řízení kvality** – Tyto služby rozšiřují stávající a zavedené služby, které jsou nezávislé na řešení incidentů a jsou často prováděny ve spolupráci s jinými pracovními jednotkami organizace, jako jsou například oddělení IT, Audit či oddělení starající se o školení zaměstnanců. Expertní pohled a participace SOC u těchto aktivit může poskytnout přehled, který pomůže zlepšit celkovou bezpečnost organizace a identifikovat rizika, hrozby a slabá místa systému. Jedná se o služby obecně proaktivní, ale přímo nepřispívají ke snížení počtu incidentů. Jejich návrh je řešen tak, aby se v nich odrážely zkušenosti získané při reakci na bezpečnostní incidenty, zranitelnosti a útoky. SOC tak může přispět k aktivitám jako jsou analýza

rizik, plánování kontinuity podnikání a zotavení po katastrofě, bezpečnostní konzultace, školení a vzdělávání zaměstnanců, hodnocení produktů/ technologií při výběrovém řízení a další.

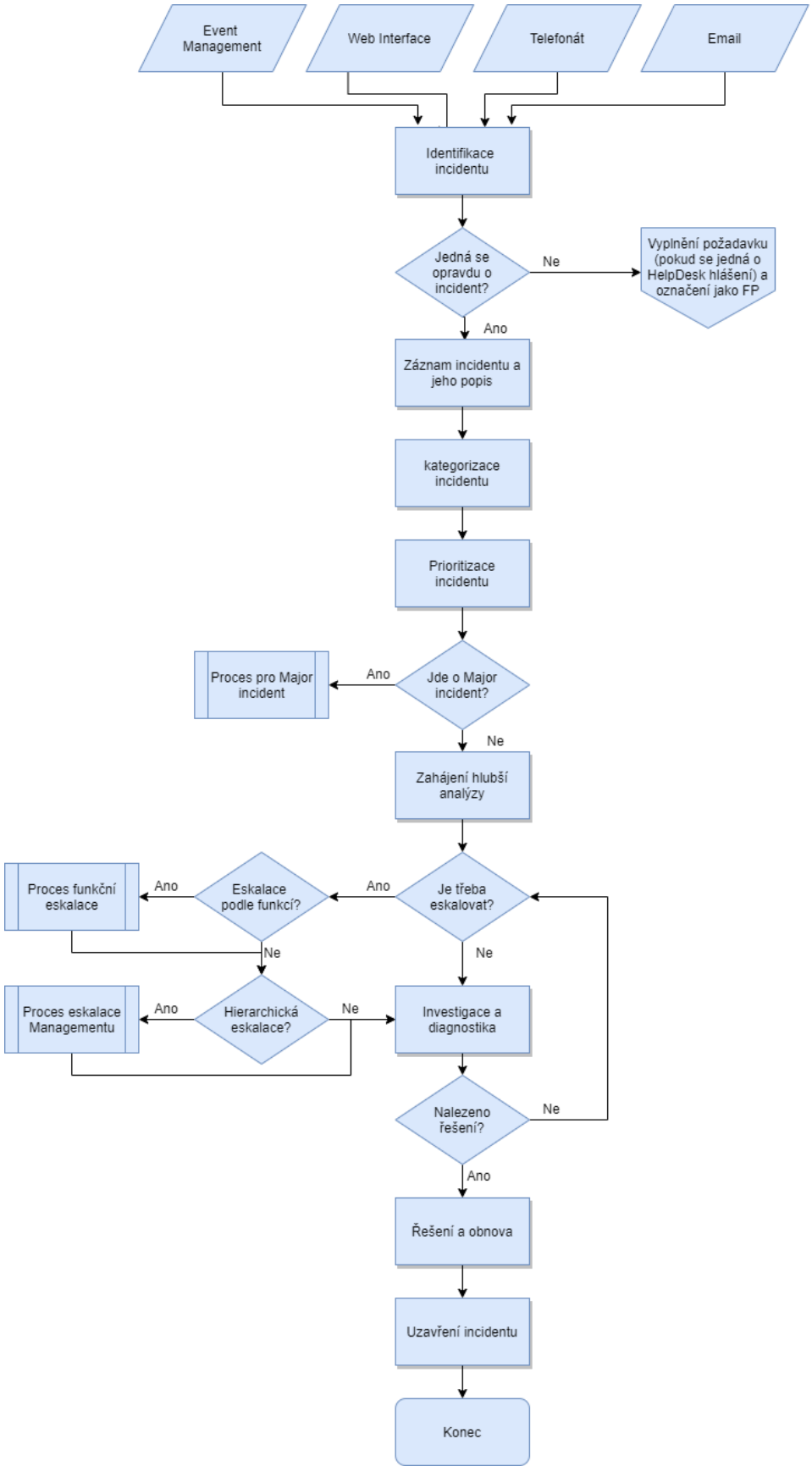
V následujícím textu jsou rozebrány procesy, které generují výše uvedené služby. Jako zástupce reaktivních služeb byl vybrán proces Zvládání bezpečnostních incidentů. Za zástupce proaktivních služeb byly vybrány procesy Řízení zranitelností a Budování báze znalostí o kybernetických hrozbách.

1.4.1 Incident Response

Hlavním důvodem, proč vůbec SOC v organizacích existuje, je zajištění odhalování bezpečnostních incidentů a jejich zvládání. Incident Response (IR) plán se liší podle typu organizace a také podle toho, kterým rámcem se řídí. Jeden z možných rámců, který se detailněji věnuje řízení incidentů, je ITIL v3. Ten proces pojmenovává Incident Management (IM) a detailněji ho znázorňuje Obrázek 1-3.

Základními aspekty, které definují celý proces Incident Managementu lze shrnout do šesti na sebe navazujících fází, které znázorňuje Obrázek 1-2

Obrázek 1-2 Návaznost fází procesu Řízení incidentů (Zdroj: Autor)



Obrázek 1-3 Proces Incident Management podle ITIL v3 (Zdroj: Autor na základě (Steinberg et al., 2013))

Detekce (Detection)

Výchozím bodem procesu IR je zachycení potenciálně škodlivých událostí (eventů). Tyto události lze identifikovat z různých zdrojů. Nejčastěji se zdroje zachycení incidentů rozdělují do dvou kategorií. Prvním zdrojem je identifikace událostí všemi zaměstnanci v organizaci, kteří nahlašují podezřelé události pomocí e-mailu, telefonátu či jiných nástrojů na HelpDesk nebo přímo oddělení bezpečnosti. Druhou možností je pomocí samotného monitoringu SOC týmu za použití různých nástrojů pro detekci, jako je třeba SIEM či nástroje pro skenování zranitelností.

Je často nepřijatelné čekat, až dojde k nějakému nežádoucímu dopadu na uživatele a ten se obrátí na HelpDesk. Proto je třeba zajistit monitoring klíčových komponent, aby došlo k odhalení chyby co nejdříve. Ideálně by měl být incident vyřešen dříve, než chyba bude mít nějaký dopad na uživatele. (Steinberg et al., 2013)

Potvrzení (Confirmation)

Nahlášenou událost je třeba přeformovat do tiketu, který se dostane do rukou bezpečnostního analytika. Ten má za úkol provést prvotní analýzu a na základě toho kategorizovat událost a určit, co tuto událost způsobilo. Na základě analýzy může následně událost označit jako false positive a celý proces IR je u konce, nebo ho označit jako true positive a dále je tato událost vnímána jako bezpečnostní incident. Následuje kategorizace a prioritizace bezpečnostního incidentu. Od těchto parametrů se dále odvíjí, jakým způsobem bude incident řešen, do kdy má být vyřešen a zda incident zůstane čistě v řešení SOC týmu nebo bude zapotřebí další spolupráce jiného oddělení.

Analýza a investigace (Analysis and Investigation)

Po potvrzení, že se opravdu jedná o bezpečnostní incident je třeba provést důkladnější analýzu. Nastínit bližší pohled na to, co se stalo, jak moc byl útok účinný, jaké všechny systémy byly postihnuty, jakým způsobem a jaká data byla narušena či odcizena. Je zapotřebí také průběžně monitorovat vektor incidentu. Jelikož incidenty jsou silně dynamickou záležitostí a při hlubších analýzách mohou být odhaleny další skutečnosti, je někdy potřeba incident překlasifikovat či změnit jeho prioritu řešení.

Zvládání (Containment)

Všechny škodlivé aspekty incidentu je třeba dostat pod kontrolu. To obnáší izolaci systému od sítě, aby nedošlo k dalšímu šíření škodlivých souborů, monitorování trafiku aktivit a případně blokace komunikace. Fáze zvládání a analýza často probíhá souběžně, protože úkolem IR je co nejdříve nastolit bezproblémový stav a není prostor čekat na důkladnou analýzu a až na základě ní se teprve rozhodovat. SOC musí okamžitě jednat s vlastníkem zasaženého aktiva a obeznámit ho s nálezem. SOC bez schválení vlastníka by neměl podnikat žádné další kroky, protože by mohl napáchat více škody než užitku. Není vhodné ihned při dostání hrozby pod kontrolu incident uzavírat. Je třeba po určitou dobu monitorovat situaci, zda klidový stav byl opravdu nastolen.

Obnova (Recovery)

Když se podaří vektor incidentu dostat pod kontrolu a již nehrozí další šíření hrozby, je třeba dostat službu či aktivum do původního stavu, do tzv. bodu obnovy. Aktivity provádí buď samotný SOC tým nebo dle potřeby specializovaný tým, který má za úkol zajistit kontinuitu činností organizace. Tato aktivita stojí na preventivních opatření IT oddělení, které pravidelně vytváří zálohy dat jednotlivých systémů. V případě havárie dojde k obnově technického zařízení a následně k obnově dat z uložených záloh.

Ponaučení (Lessons learned)

Uzavřením incidentu aktivita SOC nekončí. Je třeba vytvořit poincidentní dokumenty pro vrcholové vedení, zákazníky, vládní úřady a další zainteresované osoby. Závěrečná zpráva by měla obsahovat základní popis a klasifikaci incidentu, časovou osu řešení incidentu, zapojené osoby, vyhodnocení kvality řešení, analýzu spouštěče incidentu, zda byl zaznamenán dopad na jiné služby/ aktiva. Zpráva se vyhodnocuje až u závažnějších typů incidentu (Major Incident nebo Critical Incident). Následně tato zpráva slouží SOC týmu pro ponaučení se ze situace. Cílem je snaha predikce daného typu incidentu do budoucna.

Napříč všemi etapami IM probíhají administrativní procesy, které jsou jistou nezbytností. Patří sem vyplňování formulářů, sestavování zpráv o průběhu řešení a zvládání incidentů (nejčastěji zaznamenávání timeline průběhu), průběžné informování vedení a zainteresovaných stran. (Doucek, 2011)

Podle průzkumu společnosti IBM prováděného v roce 2020 bylo zjištěno, že správně fungující proces zvládání bezpečnostních incidentů se projevilo jako neúčinnější úsporné opatření vůči nákladům vzniklých v důsledku úniku dat. Průměrné náklady na únik dat pro společnosti s vlastním týmem na zvládání bezpečnostních incidentů, které také průběžně testovaly své plány na zvládání incidentů, byly 3,29 mil. US, ve srovnání s 5,29 mil. USD u společností, které nemají tým na zvládání bezpečnostních incidentů. Jedná se o rozdíl 2 mil. USD za rok 2020. V roce 2019 tento rozdíl byl pouze 1,23 mil. USD. (IBM Corporation, 2020)

1.4.2 Vulnerability Management

Neboli řízení zranitelností spadá mezi nejčastější aktivity interních týmů SOC proaktivního typu. Cílem je mít přehled o zranitelnostech systémů v podniku a následně jednotlivé zranitelnosti vyhodnocovat a adresovat k příslušným rizikům. Důležitou prerekvizitou, aby bylo vůbec možné řídit zranitelnosti, je mít dobře zavedený Asset Management, tedy přehled o zařízeních, která společnost vlastní. Tuto aktivitu je možné zastřešit pomocí mapování sítě (Network Mapping) pomocí tzv. discovery skenů, které mnoho nástrojů pro řízení zranitelností poskytuje. Na těchto zařízení běží v pravidelných intervalech automatizované skeny, které testují známé zranitelnosti evidované v nějaké externí databázi. Objevené zranitelnosti jsou klasifikovány dle závažnosti nejčastěji na stupnici od 1 do 5 a je k ní přiřazeno příbuzné riziko. Poté je třeba naplánovat akce, jak se se zranitelností a rizikem vypořádat. Nejčastěji se jedná o nasazení záplaty tzv. patche, která danou zranitelnost odstraní a zvýší tak zabezpečení systému. Každá záplata by měla být před nasazením otestována. Je třeba evidovat všechny aktivity ohledně průběhu záplatování. Řízení zranitelností se často odvíjí

podle předem vydefinovaných časů na reakci a zvládání, které je založené na úrovni závažnosti dané zranitelnosti. Řízení zranitelností je třeba často spojovat s dalšími aktivitami jako jsou Incident Management a Change Management. Vulnerability Management lze zároveň považovat za určitou subfunkci Change Managementu. (ISO/IEC 27002, 2013) Průzkum společnosti IBM odhalil, že zneužití zranitelností se řadí mezi nejčastější metodou útočníků, jak prolomit zabezpečení firemních systémů. Řadí se tak hned za zneužitím špatně konfigurovaného cloudu a za kompromitací přihlašovacích údajů. (IBM Corporation, 2020)

1.4.3 Cyber & Threat Intelligence

Vytvoření báze znalostí o kybernetických hrozbách nazývanou Cyber & Threat Intelligence (CTI) je mocným nástrojem, který se používá k ochraně podnikové sítě. Informace pro CTI mohou pocházet z nejrůznějších zdrojů. Jedná se o proces shromažďování informací, jejich vyhodnocování, korelace a interpretace. SOC ITC používá při tvorbě pravidel, která jsou nastavena pro detekční nástroje, aby zachytila nežádoucí aktivitu odehrávající se na podnikových systémech. SOC často vytváří vhodná doporučení, jak možné riziko plynoucí z identifikovaných hrozeb snížit a tato doporučení reportuje subjektům s rozhodovací pravomocí, které mohou rozhodnout o nasazení opatření, díky kterým je následně možné odhalovat sofistikované útoky. (Nathans, 2014)

V posledních letech se rozšířily sofistikované hackerské techniky, které cílí přímo na konkrétní cíl. Takovým útokům se říká Advanced Persistent Threat (APT). Útočníci nechtějí, aby jejich snažení bylo lehce vysledovatelné, a proto vytváří co možná nejméně nápadné scénáře útoků a snaží se tak obejít bezpečnostní systémy jednotlivých společností. Při takových druzích útoků klasické bezpečnostní nástroje jako jsou antiviry, IPS systémy, Next-Generation firewally selhávají. Aby takové typy útoků mohly být identifikovány, je třeba vytvořit strategii, která bude založená na porozumění aktuálním hrozbám.

CTI lze dělit na dva typy podle toho, jak SOC získává dané informace pro její budování. První možností je budování CTI na základě reaktivních aktivit. CTI je založena na vlastních zkušenostech s řešením kompromitovaných podnikových systémů, forenzním zkoumáním, analýzou škodlivého kódu a v neposlední řadě s nastavováním metrik odhalující určité trendy a vzorce aktivit. Pokud existuje nějaká zkušenost s problémem na jednom systému, je vhodné otestovat také zbytek systémů, zda nečelily podobným útokům. Na základě poučení se z incidentů je vhodné vytvářet detekční pravidla a nastavovat bezpečnostní nástroje, aby takové aktivity mohly být v budoucnu efektivněji zaznamenány, popřípadě odvráceny. Druhou možností jsou proaktivní indikátory, které jsou často získávány z externích zdrojů, protože náklady pro jejich získání jsou vysoké. Tyto informace lze získat zdarma jako součást OSINT (Open Source Intelligence). Lze je také zakoupit nebo získat tím, že se organizace nebo SOC stane součástí komunity, která mezi sebou sdílí informace o hrozbách a incidentech. Takové informace z identifikovaných hrozeb lze shromažďovat, analyzovat a přijímat na základě nich opatření k prevenci a zmírnění bezpečnostních rizik.

CTI může zahrnovat IP adresy, doménová jména, řetězce kódu uvnitř spustitelného souboru a jednotlivé hashe souborů. Tyto prvky mohou být vysoce volatilní. Ať už zdroje dat pro CTI SOC generuje sám nebo je získává z externích zdrojů, je třeba mít na paměti, že čím obec-

nější data jsou, tím více falešných upozornění na nevyžádané aktivity bude generováno. Zároveň však příliš konkrétní data v CTI, založená převážně jen na blacklistech či whitelistech, nebudou dostatečně pružná na to, aby na aplikovaných datech zaznamenala drobné odchylky. Cílem je vytvořit takovou CTI, která vyváží oba faktory a poskytovala co nejefektivnější podkladovou bázi pro vylepšování bezpečnostních nástrojů. (Nathans, 2014)

Podkladové informace pro CTI je nutno podrobit detailnějším analýzám. Sagar Samtani a kolektiv (Samtani et al., 2019) definují sedm hlavních typů analýz, kterými mohou být:

- **Proaktivní služby** – Tyto služby poskytují pomoc a informace pro přípravu na bezpečnostní incidenty a ochranu proti nim.
- **Souhrnné statistiky** – Jedná se o vyšší pohled na data pomocí statistik, jako je například počet blokovaných IP adres, lokace, ze kterých byl veden útok, vyšší tok dat.
- **Korelace událostí** – Cílem je analýza událostí z vícero zdrojů a odhalování jejich vzájemných vazeb. Příkladem může být identifikace stroje, který šíří škodlivý traffic, na základě kontroly logů z firewallu.
- **IP reputace** – Existují databáze hodnotící reputaci IP adres na základě detekovaných historických aktivit vícero detekčních týmů či jednotlivců. Takové adresy mohou být použity pro sledovací listy, které budou napojeny do detekčních nástrojů a dojde-li z takové IP adresy k nějaké komunikaci, bude tým SOC ihned upozorněn.
- **Analýza škodlivého kódu** – Analýza může být statická nebo dynamická. Cílem je určit, co spustitelný soubor dělá a na základě analýzy vytvořit vhodné protiopatření.
- **Detekce anomálií** – Nové bezpečnostní nástroje tuto aktivitu již zvládají samy a při detekci nestandardních aktivit dochází k odeslání upozornění SOC analytiků. Tyto detekce jsou vhodné například při boji proti DDoS útokům (Distributed Denial of Service).
- **Forenzní analýza** – Analýza jednotlivých artefaktů, pro zajištění důkazů a odhalení, jakým způsobem došlo k útoku. Příkladem může být analýza operační paměti napadeného systému.
- **Strojové učení** – Jedná se o podskupinu umělé inteligence, která je schopna učit se na základě dat, se kterými pracuje, pomocí nejrůznějších algoritmů. Toto učení může být zprostředkováno datovým analytikem, který učí algoritmus, jaké závěry má učinit, nebo nezávisle, kdy se systém sám učí rozpoznávat složité vzorce.

2 Standardy řízení informační a kybernetické bezpečnosti

Cílem informační bezpečnosti je zabezpečení všech zařízení, která jsou nositeli nebo jinak zachází s informacemi. Takové objekty lze nazývat informačními aktivy. Základním konceptem pro zajištění bezpečnosti informací je ochrana informačních aktiv proti působení nejrůznějších hrozeb. Mezi základní hrozby patří vyzrazení informací, porušení integrity informací, jejich zničení či zamezení jejich dostupnosti. Hrozby se snaží zneužít zranitelnosti systému, čímž se rozumí slabé místo informačního aktiva. Pro zajištění bezpečnosti je třeba zavádět nejrůznější opatření. Tato opatření jsou jistým procesem řízení rizika včetně vytváření politik, postupů, směrnic, která umožní snížit či zcela zabránit působení hrozby. (Doucek, 2011)

Vývoj bezpečnosti informací nemá dlouhou tradici. První snahy o řízení bezpečnosti vznikaly v 80. letech, kdy se bezpečnost a její řízení omezovaly spíš na zabezpečení IS/IT než na systematické, holistické řízení informační bezpečnosti. V roce 1983 ve Spojených státech Amerických vznikla doporučení nazvaná Trusted Computer Security Evaluation Criteria – TCSEC. V Evropě v roce 1990 vznikla také norma věnující se bezpečnosti IS/IT nazvaná Information Technology Security Evaluation Criteria – ITSEC. Ani Kanada nezůstala pozadu a publikovala kritéria pro hodnocení počítačových produktů nazvaná Canadian Trusted Computer Product Evaluation Criteria – CTCPEC. Nedostatky kritérií v americké normě TCSEC vedly k její přepracování, kterého se roku 1990 ujaly organizace National Institute of Standards and Technology (NIST) a National Security Agency (NSA). Vydaly tak kritéria pro bezpečnost IT, kterou nazvaly Federal Criteria (FC). (Doucek, 2011)

Bohužel tyto normy se nevěnují řízení celkové bezpečnosti informací a požadavky z nich vyplývající, které vznikly na základě kooperace vlády a armády, nejsou zrovna aplikovatelné pro komerční organizace. To se změnilo roku 1995, kdy ve Spojeném království byla vydána norma BS 7799. V roce 2000 byl první díl této normy schválen jako mezinárodní standard ISO/IEC 17799:2000 a v roce 2001 se tato norma stala součástí českých technických norem označovaná ČSN ISO/IEC 17799:2001. (Doucek, 2011) Začátek nového tisíciletí došlo k rozvoji nejrůznějších standardů pro řízení bezpečnosti. Mezi nejznámější patří rodina norem ISO/IEC 27000, DCI-DSS, SOX, HIPAA, GDPR, NIST Cybersecurity Framework a mnoho dalších. V posledních letech se potřeba řízení informační bezpečnosti dostává i do lokálních standardů, nařízení a zákonů. Příkladem může být zákon o kybernetické bezpečnosti vydaný v České republice v roce 2014.

2.1 ISO 27000

Tato řada norem vydaná Mezinárodní organizací pro standardizaci (International Organization for Standardization – ISO) se zaměřuje na řízení informační bezpečnosti. Organizace ISO vyhlásila v roce 2005 vydání nové rodiny norem, která ustanoví pravidla pro

systém řízení bezpečnosti informací (Information Security Management System – ISMS). ISMS je systematický přístup, který pomáhá vytvořit opatření pomáhající udržet data organizace v bezpečí. Ideově vychází z konceptu Demingova cyklu PDCA, který řízení bezpečnosti rozděluje do čtyř na sebe navazujících činností – plánování, realizace plánu, ověření výsledků realizace oproti požadovaným cílům a úprava provedení, které povede ke zlepšení ISMS.

Jádrem normalizace je považována norma ISO/IEC 27001:2005[1], která specifikuje požadavky na ISMS. Zahrnuje soubor požadavků pro kontrolu a zmírnění rizik spojených s informačními aktivy, která chce organizace pomocí ISMS ochránit. Vychází z britského standardu BS 7799-2. Požadavky definované v této normě jsou obecné, tzn. použitelné pro všechny organizace bez ohledu na typ, velikost či povahu, a jsou zároveň závazné, což znamená, že musí být splněny. Druhou nejčastěji používanou normou této řady je ISO/IEC 27002:2005[2] a vychází z britského standardu BS 7799-1. Obsahuje výklad vhodných bezpečnostních opatření. Obě normy se dočkaly druhé verze vydané v roce 2013. Jedná se zatím o jejich poslední aktualizované vydání. Vyspecifikované požadavky v ISO/IEC 27002 oproti ISO/IEC27001 nejsou závazné a jsou jen jistým doporučením. Norma slouží také pro potřeby SOC. Některé požadavky jsou specifikovány přímo jako například požadavky na logování a monitorování infrastruktury, řízení zranitelností systému, ochrana před malwarem, řízení bezpečnostních incidentů a zajištění kontinuity informační bezpečnosti. (ISO/IEC 27002, 2013) Jiné požadavky se protínají napříč všemi dalšími kategoriemi. Díky komplexnímu pohledu norem ISO, není tato norma zcela nejvhodnějším rámcem pro účely hodnocení účinnosti a účelnosti SOC jako celku. Pro zajištění kvality jednotlivých aktivit, které SOC vykonává je možné využít normy ISO/IEC 27032:2012[3] pro kybernetickou bezpečnost, ISO/IEC 27031:2011[4] pro zachování kontinuity podnikání, ISO/IEC 27035:2016[5] pro zvládání bezpečnostních incidentů, která je rozdělena na tři části a ISO/IEC 27043:2015[6] pro analýzu a vyšetřování bezpečnostních incidentů.

[1] ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements

[2] ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management

[3] ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity

[4] ISO/IEC 27031:2011
Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

[5] ISO/IEC 27035:2016 Information technology — Security techniques — Information security incident management
Part 1: Principles of incident management (ISO/IEC 27035-1:2016)
Part 2: Guidelines to plan and prepare for incident response (ISO/IEC 27035-2:2016)
Part 3: Guidelines for ICT incident response operations (ISO/IEC 27035-3:2020)

[6] ISO/IEC 27043:2015 Information technology — Security techniques — Incident investigation principles and processes

ISO neustále aktualizuje své stávající normy a také vytváří normy nové. Následující výčet zobrazuje poslední aktualizace nejpoužívanějších z nich. (ISO, 2020)

- ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary
- ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements
- ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls
- ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance
- ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation
- ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management
- ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007:2020 Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing
- ISO/IEC TS 27008:2019 Information technology — Security techniques — Guidelines for the assessment of information security controls
- ISO/IEC 27009:2020 Information security, cybersecurity and privacy protection — Sector-specific application of ISO/IEC 27001 — Requirements

Jak je z názvů patrné, tak v posledních letech se normy pod hlavičkou ISO 27000 začínají věnovat více kybernetické bezpečnosti. V blízké budoucnosti se chce ISO zaměřit na takové aspekty, jako jsou například zabezpečení internetu věcí (IoT), big data, cloud computing, kybernetická bezpečnost, biometrická autentizace na mobilních zařízení, či zabezpečení virtualizovaných kořenů důvěry. (Risk Analysis Consultants, 2020)

2.2 NIST CSF

Dne 12. února 2013 vydal americký prezident Barack Obama nařízení č. 13636 nazvané *Improving Critical Infrastructure Cybersecurity* jako reakci na alarmující počet kybernetických útoků mířící na kritickou infrastrukturu Spojených států amerických. To vyvolalo potřebu jednotného rámce pro kybernetickou bezpečnost, který poskytne přístup pro řízení rizik souvisejících s kybernetickou bezpečností a kritickou infrastrukturou. Kritickou infrastrukturou se míní všechny systémy a aktiva, ať už fyzická nebo virtuální, pro Spojené státy americké tak zásadní, že nezpůsobilost nebo zničení takových systémů a aktiv by mohla mít oslabující dopad na národní bezpečnost, ekonomiku, zdraví a bezpečnost veřejnosti nebo na jakoukoliv kombinaci těchto vytyčených záležitostí. (Executive Order no. 13636, 2013)

Jelikož rizika z oblasti kybernetické bezpečnosti jsou silně závislá na faktorech jednotlivých organizací a informačních technologií, které využívají, bylo třeba vytvořit tak obecný rámec, aby dokázal pokrýt všechny potřeby pro řešení těchto rizik. Rok od vydání nařízení vznikla první verze (verze 1.0) rámce nazývaná *Framework for Improving Critical Infrastructure Cybersecurity* (NIST CSF) vydanou pod záštitou National Institute of Standards and Technology (NIST). Na jeho vzniku spolupracovali bezpečnostní experti z veřejného sektoru, soukromého sektoru a z akademické sféry. Poslední vydanou verzí NIST CSF je verze 1.1 vydaná 16. dubna 2018. (NIST, 2018)

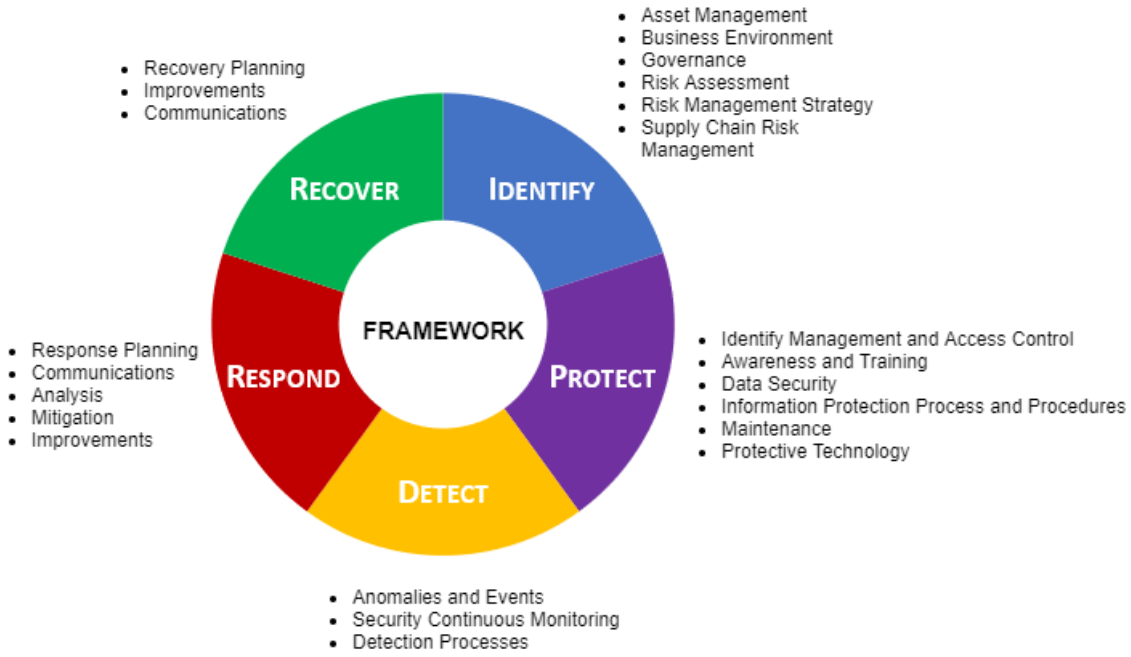
I když byl původně rámec primárně zamýšlen pro vlastníky kritické infrastruktury ve Spojených státech amerických, se jeho uživatelská základna rozrostla i o komunity a organizace po celém světě. Podle průzkumu společnosti Gartner, zabývající se výzkumem v oblasti bezpečnostních technologií, NIST CSF pro řízení kybernetické bezpečnosti využívalo v roce 2015 až 30 % amerických organizací. Sice ještě nebyly publikovány statistiky za rok 2020, ale předpokládá se, že se počet amerických organizací využívající NIST CSF zvedne na 50 %. Dále tato společnost predikuje, že ISO 27001 a NIST CSF až do roku 2024 budou převládajícími bezpečnostními rámci pro organizace, které budou doplněny o lokalizované a oborové standardy a předpisy. (Verve Industrial, 2019; Hanacek, 2017)

NIST CSF se skládá ze tří částí, kterými jsou jádro rámce, úrovně implementace a rámcové profily.

Jádro rámce

Základem rámce je sada činností v oblasti kybernetické bezpečnosti, která je společná pro všechna odvětví kritické infrastruktury. Skládá se z pěti funkcí, kterými jsou identifikace, ochrana, detekce, reakce a obnova. Tyto funkce poskytují strategický pohled na řízení rizik spojených s kybernetickou bezpečností během jejich celého životního cyklu. Funkce se následně člení na jednotlivé kategorie a podkategorie (viz Obrázek 2-1).

- **Identifikace (Identify) –**Základem pro efektivní využívání rámce je porozumět, jak řídit kybernetická bezpečnostní rizika. Je třeba pochopit podnikový kontext, zdroje, které budou podporovat jednotlivé funkce.
- **Ochrana (Protect) –** Cílem je mít taková ochranná opatření, která omezí nebo zcela potlačí dopad potenciálních incidentů souvisejících s kybernetickou bezpečností.
- **Detekce (Detect) –** Pro odhalování potenciálních incidentů souvisejících s kybernetickou bezpečností je třeba nepřetržitě sledovat bezpečnostní události.
- **Reakce (Respond) –** Po odhalení bezpečnostního incidentu je třeba vykonat určité aktivity, které zamezí šíření incidentu a zmírní jeho dopad na organizaci.
- **Obnova (Recover) –** Poslední funkcí je obnova běžného chodu organizace. Aktivity obnáší tvorbu plánů pro zachování činností organizace (Business Continuity Plan – BCP) a plánů obnovy po havárii (Disaster Recovery Plan – DRP). (National Institute of Standards and Technology, 2018)



Obrázek 2-1 NIST CSF, funkce a jeho kategorie (Zdroj: Autor na základě: (ISACA, 2019))

Úrovně implementace

Poskytují kontext o tom, jak organizace vnímá kybernetické bezpečnostní riziko a procesy zavedené k jeho řízení. Úrovně popisují, do jaké míry jednotlivé postupy pro řízení kybernetických bezpečnostních rizik odpovídají vydefinovaným standardům v NIST CSF. S vyšší úrovní roste stupeň přísnosti a propracovanosti postupů pro řízení rizik kybernetické bezpečnosti.

- **Částečná (Partial) –** Postupy pro řízení rizik spojených s kybernetickou bezpečností nejsou formalizovány a jednotlivá rizika jsou řízena ad hoc, někdy dokonce jen reaktivním způsobem. Povědomí o kybernetických bezpečnostních rizicích není na celopodnikové úrovni zavedeno.
- **Založená na riziku (Risk Informed) –** Aktivity pro řízení kybernetických bezpečnostních rizik mohou být schváleny vedením, ale nejsou implementovány do celopodnikových standardů a norem. Stanovení priorit pro řízení těchto rizik je přímo založeno na cílech pro řízení rizik a na prostředí daným identifikovanými hrozbami. Na celopodnikové úrovni existuje povědomí o rizicích souvisejících s kybernetickou bezpečností, ale nebyl zaveden celopodnikový přístup k řízení těchto rizik.
- **Opakovatelná (Repeatable) –** Postupy pro řízení rizik jsou formálně schváleny a ustanoveny v celopodnikových standardech a normách. Tyto postupy jsou pravidelně aktualizovány na základě změn požadavků podnikové funkce, změn prostředí daného identifikovanými hrozbami a změn technologií. K řízení rizik existuje celopodnikový přístup. Jsou definovány zásady, procesy a postupy založené na znalos-

tech o rizicích. Jsou také zavedeny konzistentní metody, které umožňují účinně reagovat na změny rizika. Pracovníci mají potřebné znalosti a dovednosti pro výkon činností stanovenými jejich rolí a odpovědnostmi.

- **Adaptivní (Adaptive) –** Postupy pro řízení rizik jsou založeny na základě lessons learned a na základě prediktivních ukazatelů odvozených z předchozích a současných aktivit v oblasti kybernetické bezpečnosti. Do procesů jsou zapojovány nové technologie. Organizace se aktivně přizpůsobuje měnícímu se prostředí dané kybernetickou bezpečností a včas reaguje na sofistikované vznikající hrozby. K řízení rizik kybernetické bezpečnosti existuje celopodnikový přístup, který pro řešení používá zásady, procesy a postupy založené na znalosti rizika. Řízení těchto rizik se stalo součástí organizační kultury a odvíjí se ze získaných zkušenostech z dřívějších aktivit a z informací, které organizace sdílí s jinými organizacemi. (National Institute of Standards and Technology, 2018)

Rámcové profily

Jedná se o jednotlivé výstupy tohoto rámce založených na podnikových potřebách, které organizace vybrala z různých kategorií a jejich podkategorií. Profil lze charakterizovat jako sladění standardů, pokynů a postupů z jádra rámce NIST CSF v konkrétních scénářích implementace do konkrétní organizace. Lze je použít pro identifikaci příležitostí ke zlepšení aktuální pozice v oblasti kybernetické bezpečnosti, kdy se aktuální stav porovnává s chtěným stavem. Na základě profilů tak dochází k sebehodnocení.

3 Hodnocení vyspělosti procesů

Procesní řízení organizace sebou nese otázku, jak zjistit, zda prováděné aktivity jsou vykonávány účinně a účelně. Pro tyto potřeby slouží hodnocení vyspělosti procesů. Celkem má společnost tři možnosti, jak hodnotit své implementované procesy.

První možností je zkusit si individuálně ohodnotit úroveň procesů pomocí tzv. sebehodnocení (self-assessment). K tomu se často používají různé hodnoticí modely jako je například CMMI (Capability Maturity Model Integration). Bohužel použití těchto obecných modelů přináší obecné výsledky, které neodpovídají specifickým požadavkům pro řízení bezpečnosti. Často se lze také setkat se specializovanými hodnoticími nástroji, které umožňují provádění sebehodnocení již podle specifičtějších kritérií, což do značné míry usnadňuje práci. Tyto nástroje jsou součástí nejrůznějších metodik nebo existují samostatné hodnoticí nástroje vytvořené různými organizacemi.

Druhou možností, jak určit vyspělost procesů je použití služeb externích společností, které mají jisté zkušenosti s hodnocením procesů. Takové poskytování služeb hodnocení třetí stranou se nazývá audit. Jedná se o objektivní ověření aktuálního stavu se stavem žádoucím (norma, model), které provádí nezávislá strana. Výsledkem je pak komplexní názor ve formě výroku auditora. (Svatá, 2012)

Níže v textu jsou představeny hodnoticí modely CMM a CMMI jako reprezentanti všeobecných hodnoticích modelů a PAM, CPM modely využívané v rámci COBIT pro řízení IS/IT služeb. V neposlední řadě se kapitola věnuje nejvíce zaměřujícím se modelům pro hodnocení SOC, které jsou často komerčního typu nebo projekty jednotlivců.

3.1 Historie CMM

Capability Maturity modely (CMM) jsou určitou zjednodušenou reprezentací světa a obsahují prvky založené na koncepcích vyvinutých Philip B. Crosby, W. Edwards Deming, Humphey a Radice. Skládá se ze sledu úrovní zralosti určitých tříd objektů a představuje očekávanou, žádanou nebo typickou cestu evoluce těchto objektů. Objekty jsou nejčastěji jednotlivé procesy.

První pokusy o zlepšování procesů probíhalo již ve 30. letech, kdy Walter Shewhart začal pracovat na principech statistické kontroly procesů. Tyto principy byly dále rozpracovávány v 80. letech Demingem v jeho knize s názvem *Out of the Crisis*, kde popisuje teorii Managementu založenou na jeho 14 bodech Managementu, a Philipem Crosbym v knize *Quality is Free*, kde definoval Maturity Grid matici, která se stala ideovým základem dalších CMM. Watts Humphrey a Ron Radlice dále rozšířili jejich principy a začali je aplikovat na software při jejich práci ve společnosti IBM. Humpreyho kniha *Managing the Software Process* z roku 1989 popisuje základní principy a pojmy, na kterých mnoho dnešních CMM stojí. (CMMI Product Team, 2010b)

3.2 CMMI

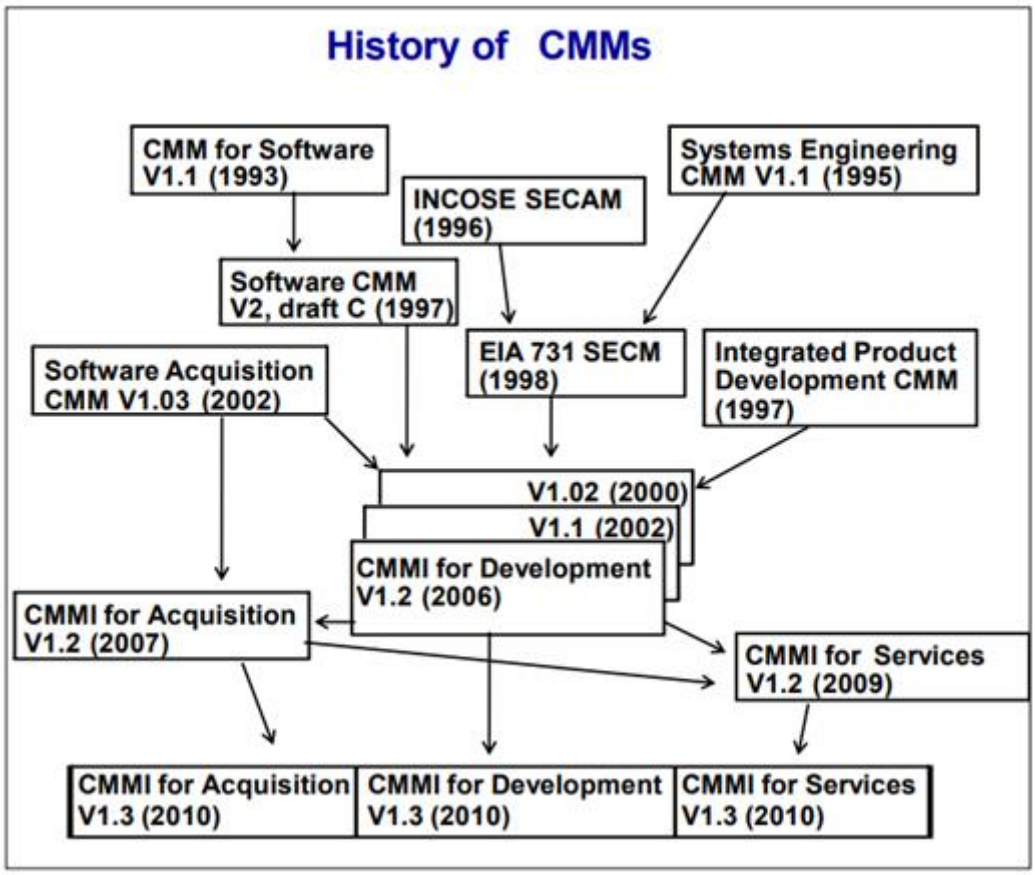
Model se opírá o tři kritické faktory, kterými jsou lidé, technologie a procedury. Tyto tři prvky následně propojují procesy. Základní myšlenkou bylo vytvoření nástrojů pro hodnocení zralosti procesů, hlavně procesů týkající se tvorby software. Postupem času byly začleněny i další procesy jako pořízení software a poskytování služeb. Mezi hlavní benefity zavedení hodnoticího modelu CMMI do organizací je, že umožňuje redukovat náklady na proces zlepšování napříč podniky, u kterých dosažení jejich cílů závisí na vícero funkcích a skupinách. (Chrissis et al. 2011; Kulpa a Johnson, 2003)

První aktivity související se vznikem CMMI modelu se datují k 80. létům 20. století, kdy několik amerických vojenských projektů zahrnující softwarové dodavatele skončilo značným překročením stanoveného rozpočtu a s velkým časovým zpožděním. Jako reakci na tyto neúspěchy se United States Air Force rozhodlo finančně podpořit studii, která měla za cíl vytvořit abstraktní model pro objektivní hodnocení dodavatelů softwaru v rámci rozsáhlých vládních programů zadávání státních armádních zakázek. Tento výzkum byl zadán společnosti Carnegie Mellon University Software Engineering Institute (SEI-CMU) v Pittsburgu. Výsledkem byl model pro vojenské použití, který sloužit jako objektivní posouzení schopnosti softwarových subdodavatelů. SEI při vytváření CMM převzala premisy, že kvalita systému či produktu je vysoce ovlivněna kvalitou procesu použitého k jeho vývoji a údržbě. V tuto premisy také věří i mnoho dalších organizací. Svědčí o tom i skupina norem ISO/IEC – International Organization/ international Electrotechnical Commission body of standards a další modely stavící na TQM – Total Quality Management. Koncepce úrovně zralostí se objevila třeba v P3M3, Cobit, ISO/IEC 15504 a ISO/IEC 21827. Model vycházel z již výše představené koncepce od Philipa B. Crosbyho v knize *Quality is free*. (Kevin Roebuck, 2012)

Vývoj modelu začal v roce 1986 a sedm let na to vznikl první Capability Maturity Model for Software, který byl publikován v knize *The Capability Maturity Model: Guidelines for Improving the Software Process*. První integrovaný model CMMI byl vytvořen roku 2000 pod názvem CMMI v1.02 (CMMI for Software) a zahrnoval 3 modely. Jednalo se o Capability Maturity Model for Software (SW-CMM), Systems Engineering Capability Model (SECM) a Integrated Product Development Capability Maturity Model (IPD-CMM). V roce 2002 vyšla druhá a následně v roce 2006 třetí aktualizace modelu. SEI si uvědomila, že pro postihnutí všech procesů vázaných k software je model velice komplexní, tak se rozhodla pozměnit název na CMMI for Development, jak je již známý dnes. Komplexita stále však narůstala, a proto vznikly další dva modely CMMI for Acquisition a CMMI for Services, které vychází z třetí aktualizace CMMI for Development v1.2 z roku 2006. Také tyto modely dostaly přívlastek v1.2. Poslední vývojový zásah do rámce byl proveden v listopadu 2010, kdy došlo k synchronizaci tří modelů tak, aby je bylo možné používat společně. Tak vznikla stávající verze, která obsahuje 3 modely:

- Capability Maturity Model Integration for Acquisition v1.3 (CMMI-ACQ)
- Capability Maturity Model Integration for Development v1.3 (CMMI-DEV)
- Capability Maturity Model Integration for Services v1.3 (CMMI-SVC)

Celý časový vývoj CMMI je graficky znázorněn na obrázku níže (viz Obrázek 3-1).



Obrázek 3-1 Historie CMMI (Zdroj: (CMMI Product Team, 2010c))

CMMI-ACQ se zabývá řízením dodavatelsko-odběratelského řetězce. Nejdříve vedení SEI schválilo malou úvodní sbírku osvědčených postupů akvizice nazvanou „Acquisition Module (CMMI-AM)“, která byla založena na CMMI rámci. Tento model však neměl sloužit pro účely hodnocení a zlepšování procesů akvizice. Až ve spolupráci se společností General Motors na základě tohoto modelu byl vytvořen model, jak ho známe dnes. (CMMI Product Team, 2010a)

CMMI-DEV se zabývá procesy vývoje produktů a služeb. Model mimo hardwarových či softwarových firem využívají i další odvětví jako jsou například letectví, bankovnictví, automobilový průmysl, telekomunikace, či obrana. Zahrnuje praktiky z projektového managementu, procesního řízení, systémového inženýrství, hardwarového a softwarového inženýrství a další podpůrné aktivity, které jistým způsobem souvisí s vývojem a údržbou produktů a služeb. (CMMI Product Team 2010b; Chrissis et al., 2011)

CMMI-SVC se zabývá poskytováním služeb jak v rámci organizace, tak i externím subjektům. Cílem je pokrýt činnosti související s dodávkou služeb jako jsou zavedení služby, dodání služby a samotné jejich řízení. Model staví na dalších konceptech jako jsou ITIL, COBIT, ISO/IEC 2000, ITSCMM. (CMMI Product Team, 2010c)

Je nutno brát v úvahu, že CMMI není popis jednotlivých procesů, protože každá organizace má jiné potřeby a finální proces ovlivní mnoho faktorů jako je třeba velikost podniku, organizační struktura, odvětví podnikání, normy a právní prostředí.

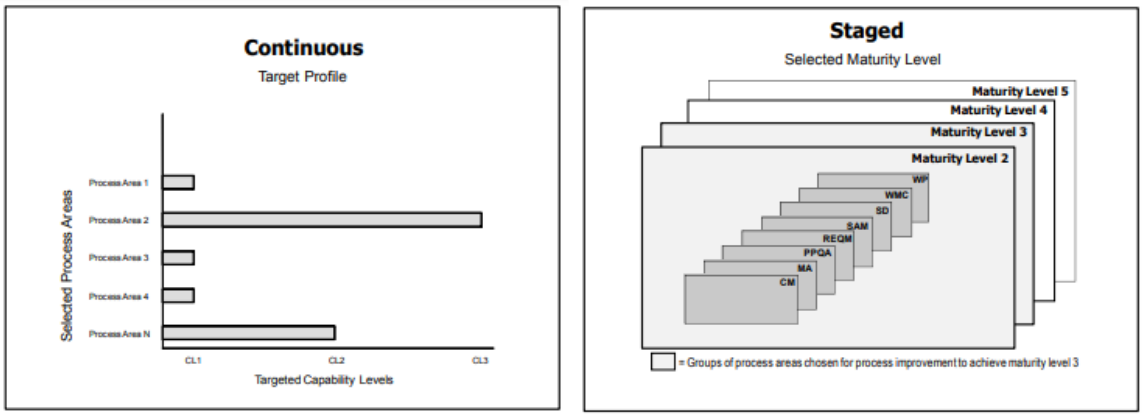
CMMI se skládá ze tří základních komponent, kterými jsou:

- **Požadované komponenty** – Jsou nezbytné pro dosažení zlepšení daného procesu. Sem spadají specifické a obecné cíle. Specifické cíle (Specific Goals) jsou jedinečné charakteristiky, které musí být přítomny, aby došlo k uspokojení procesní oblasti. Obecné cíle (Generic Goals) platí pro více procesních oblastí a jde o charakteristiky, které musí být přítomny k institucionalizaci procesů implementující danou procesní oblast. Je to požadovaná součást modelu a používá se při hodnocení k určení, zda je procesní oblast splněna. (Kulpa a Johnson, 2003)
- **Očekávané komponenty** – Jedná se o aktivity důležité pro dosažení požadované komponenty CMMI. Jsou vodítkem pro ty, kteří implementují zlepšení nebo provádí hodnocení. Aktivity lze opět rozdělit na specifické a obecné. Specifické postupy (Specific Practices) popisují činnosti nutné pro dosažení specifických cílů a obecné postupy (Generic Practices) popisují činnosti, které jsou považovány za důležité pro dosažení obecných cílů a přispívají k institucionalizaci procesů souvisejících s danou procesní oblastí.
- **Informativní komponenty** – Jejich účelem je poskytnutí informací nezbytných pro dosažení správného pochopení cílů a postupů v CMMI. Tím pomáhají porozumět požadovaným a očekávaným komponentám. Může tím být podrobné vysvětlení či jiné užitečné informace (reference, subpraktiky, poznámky, zdroje). (Chrissis et al., 2011)

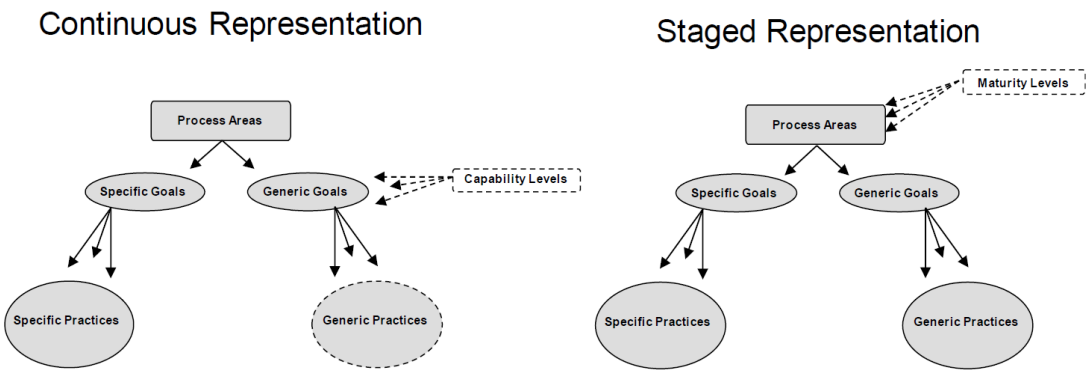
CMMI využívá dvě cesty, jak docílit zlepšení procesů. Dochází k tomu na dvou úrovních, kterými jsou úrovně schopnosti (capability levels) a úrovně zralosti (maturity levels). Každý druh úrovní je použit pro jinou reprezentaci zlepšování procesů.

- **Kontinuální reprezentace** (continuous representation) – používá úrovně schopnosti k charakterizaci stavu procesů organizace ve vztahu k jednotlivé oblasti procesu. Jedná se o postupné zlepšování jednoho konkrétního procesu. Obsahuje čtyři úrovně schopnosti (0-3), kdy pro dosažení konkrétní úrovně je třeba naplnit všechny obecné cíle. Toho se docílí pomocí aplikace obecných postupů.
- **Stupňovitá reprezentace** (staged representation) – používá úrovně zralosti k charakterizaci celkového stavu procesů organizace ve vztahu k modelu jako celku. Umožňuje tak vylepšit sadu souvisejících procesů napříč různými procesními oblastmi. Existuje 5 úrovní zralosti (1-5), které reprezentují určitou výkonnost. Měří se dosahování jak obecných cílů, tak i specifických cílů spojených s každou předdefinovanou sadou procesních oblastí. Toho lze docílit obecnými a specifickými postupy.

Odlišnosti a provázanost mezi těmito dvěma typy reprezentace a dvěma typy úrovní hodnocení zobrazují obrázky níže (viz Obrázek 3-2 a Obrázek 3-3).



Obrázek 3-2 Vztah mezi kontinuální a stupňovitou reprezentací (zdroj: (CMMI Product Team, 2010c))



Obrázek 3-3 Vztah úrovní schopnosti a úrovní zralosti (Zdroj: (CMMI Product Team, 2010c))

3.2.1 Úrovně schopnosti (Capability levels)

0. úroveň – Neúplný (Incomplete)

Takové úrovně dosahuje proces, který se neprovádí nebo je prováděn jen částečně. Jeden nebo více specifických cílů dané procesní oblasti nejsou splněny. Pro tuto úroveň neexistují žádné obecné cíle, protože není důvod institucionalizovat takový proces, který je vykonáván jen z části. (CMMI Product Team, 2010c)

1. úroveň – Vykonávaný (Performed)

Vykonávaný proces je takový proces, který dokončí potřebnou práci k výrobě požadovaného výstupu procesu. Všechny specifické cíle jsou splněny. Tato úroveň sice vede k důležitým

zlepšením, avšak tato zlepšení mohou být časem ztracena, pokud nejsou institucionalizována, což je záležitostí vyšších úrovních. (CMMI Product Team, 2010c)

2. úroveň – Řízený (Managed)

Proces má oproti vykonávanému procesu již jistý řád. Proces je plánován a prováděn v souladu s vyhláškami/normami, zaměstnává kvalifikované lidi, kteří mají adekvátní zdroje k produkci požadovaných výstupů a proces také zahrnuje relevantní zúčastněné strany. Vykonávání procesu je neustále monitorováno, kontrolováno a dochází k jeho hodnocení z hlediska dodržování popsaného postupu. Proces má jasně stanoveny účel, vstupy, vstupní kritéria, aktivity, role, opatření, ověřovací kroky, výstupy a výstupní kritéria. Takové procesy pomáhají zajistit, aby byly stávající postupy během stresových situacích stále zachovávány. Při dosažení této úrovně je možné konstatovat, že existují normy, které dokládají vykonávání procesu. Existuje plán pro jeho provedení, zdroje jsou poskytovány, jsou přiřazeny odpovědnosti a lidem zapojeným do procesu bylo poskytnuto školení k danému výkonu. (CMMI Product Team, 2010c)

3. úroveň – Definovaný (Defined)

Definovaný proces je řízený proces, který je šitý na míru dle zásad procesních standardů organizace a je tak v souladu s požadavky definovanými organizací. Popis procesu je neustále udržován aktuální. Rozdílem mezi 2. úrovní a 3. úrovní je rozsah popisů procesů a postupů. Na 2. úrovni mohou být standardy/ procesy/ postupy v každé konkrétní instanci procesu (používané konkrétní pracovní skupinou) zcela odlišné, avšak již na 3. úrovni jsou standardy/ procesy/ postupy přepracovány a přizpůsobeny ze souboru standardních procesů, které definovala organizace tak, aby vyhovovaly konkrétní pracovní skupině. Přizpůsobení procesů by se mělo řídit také pokyny organizace, která stanoví, jakým způsobem je možné dané postupy přizpůsobovat vlastním potřebám. Dalším rozdílem je, že procesy na 3. úrovni jsou obvykle popsány přísněji než na 2. úrovni. Při dosažení nejvyšší úrovně lze konstatovat, že proces je spojen se standardním procesem definovaným organizací, který byl přizpůsoben potřebám oddělení. Pokud se podaří dosáhnout 3. úrovně, je možné pokračovat na zlepšení tím, že se hodnocení zaměří na procesní oblasti s vysokou vyspělostí (Organizational Process Performance, Quantitative Work Management, Causal Analysis and Resolution, Organizational Performance Management). (CMMI Product Team, 2010c)

3.2.2 Úrovně zralosti (Maturity levels)

1. úroveň – Počáteční (Initial)

Procesy jsou prováděny nahodile (ad-hoc) a převážně chaoticky. Organizace většinou neposkytuje stabilní prostředí pro podporu procesního řízení. Úspěch v těchto organizacích závisí na kompetencích jednotlivců a jejich dovednostech, nikoli na použití osvědčených procesů. Navzdory tomuto chaosu společnosti na této úrovni maturity poskytují služby, které často fungují, ale překračují rozpočet a časový plán dokumentovaný v jejich plánech. Organizace s touto úrovní maturity jsou charakterizovány tendencí během krizových situací

opouštět od svých procesů a nejsou schopnosti opakovat své úspěchy. (CMMI Product Team, 2010c)

2. úroveň – Řízený (Managed)

Pracovníci různých oddělení definují strategii poskytovaných služeb, vytváří pracovní plány, monitorují a kontrolují práci, aby zajistili, že služba bude dodána podle plánu. Řízení konfigurace a proces pro zajištění kvality výstupů jsou institucionalizovány. Pracovní skupiny, pracovní aktivity, procesy, výstupy a služby jsou řízeny. K vykonání procesu, poskytuje poskytovatel služeb odpovídající zdroje a přiřazuje odpovědnosti za provádění procesu a školí jednotlivé pracovníky zapojené do procesu. Je pravidelně vyhodnocováno, zda je proces dodržován a výkon procesu je řešen s vedením. Procesní disciplína na této úrovni pomáhá zajistit, aby byly stávající postupy zachovány ve stresových obdobích. (CMMI Product Team, 2010c)

3. úroveň – Definovaný (Defined)

Do procesů jsou zakomponovány již zažité principy a postupy z projektů a prací. Postupy, potřebné nástroje a metody jsou popsány a standardizovány. Standardní sada procesů je definována napříč celou organizací a je kontinuálně revidována a upravována dle stávajících potřeb. Jednotlivé týmy si tuto sadu standardních organizačních procesů mohou přizpůsobit vlastním potřebám dle pokynů pro přizpůsobení, které stanovuje organizace. Toto je zásadní rozdíl oproti 2. úrovni, kde se jednotlivé procesy mohly v organizaci zcela lišit, protože nevycházely z nějakého předem definovaného setu standardů definovaného organizací. Proces jasně stanovuje účel, vstupy, vstupní kritéria, činnosti, role, opatření, ověřovací kroky, výstupy a výstupní kritéria. (CMMI Product Team, 2010c)

4. úroveň – Kvantitativně řízený (Quantitatively Managed)

Poskytovatel služeb na této úrovni zralosti definuje kvantitativní cíle (kvalita, výkonnost) a používá je jako kritéria pro řízení procesů. Tyto kvantitativní cíle jsou založeny na potřebách zákazníků, koncových uživatelů, organizace a procesních implementátorů. Kvalita a výkonost jsou měřeny pomocí statistik po dobu celého procesu. U konkrétních podprocesů jsou shromažďována a statisticky analyzována konkrétní měřítka výkonnosti procesu. Oproti 3. úrovni lze predikovat, jakou bude mít proces výkonnost. Zde je totiž výkonnost řízena pomocí statistických a kvantitativních technik a z nich se pak odvíjí predikce vývoje výkonu jednotlivých procesů, což napomáhá dalšímu plánování aktivit, rozpočtu a zdrojů. (CMMI Product Team, 2010c)

5. úroveň – Optimalizovaný (Optimizing)

Organizace kontinuálně zlepšuje své procesy podle kvantitativního porozumění business cílům a výkonnostním potřebám. Zlepšování je inkrementální na základě inovacích a technických zlepšeních. Cíle kvality a výkonnosti procesů jsou stanoveny, neustále revidovány, zda stále splňují měnící se business cíle a výkonnost organizace. Efekt zlepšování procesů je měřen pomocí statistických a jiných kvantitativních technik Ve 4. úrovni je výkonnost vnímána jako podproces a výsledky jsou použity pro řízení projektů. Na 5. úrovni se organizace

zabývá celkovým výkonem organizace pomocí dat shromážděných z více pracovních skupin. (CMMI Product Team, 2010c)

3.2.3 SCAMPI

SCAMPI (Standard CMMI Appraisal Method for Process Improvement) je metoda poskytující měřítko kvality hodnocení procesů založený na modelu CMMI. Používá se k identifikaci silných a slabých míst stávajících procesů, odhaluje rizika vývoje či akvizice a určuje úrovně schopnosti a zralosti. Často se výsledky tohoto hodnocení používají jako součást aktivit vedoucích ke zlepšení procesů nebo získané výsledky jsou použity pro hodnocení potenciálních dodavatelů. CMMI obsahuje specifické požadavky nazývané Appraisal Requirements for CMMI, které jsou zkráceně označovány jako ARC. Ty definují tři třídy hodnocení, které se vyznačují stupněm přísnosti použité metody. (SCAMPI Upgrade Team, 2011)

- **Třída A** je ze všech tří tříd nejpřísnější. Metody třídy A musí splňovat všechny požadavky ARC a jsou jedinými metodami považovanými za vhodné pro poskytování měřítek pro benchmarking.
- **Třída B** je méně formální než třída A. Pomáhá identifikovat příležitosti pro zlepšení. Některé požadavky, které jsou pro metody třídy A povinné jsou v metodách třídy B volitelné. Metody této kategorie neprodukují měřítko hodnocení. Tyto metody jsou vhodné pro počáteční hodnocení v organizacích, které právě začínají používat CMMI modely pro zlepšování jejich procesů.
- **Třída C** je méně formální než třída A. Pomáhá identifikovat příležitosti pro zlepšení. Metody hodnocení třídy C jsou podmnožinou požadavků ARC pro metody třídy B, kdy u metod třídy C je vyžadován pouze jeden ze dvou typů objektivních důkazů oproti metodám třídy A a B. Stejně jako metody třídy B, ani metody této úrovně neprodukují měřítko hodnocení. Tyto metody jsou vhodné při rychlém náhledu nebo pravidelném hodnocení projektů a podpůrných organizačních skupin.

3.3 COBIT

Pro řízení informatiky v organizacích se používají dvě koncepce. První z nich je IT Governance (ITG), která je logickým rozšířením koncepce Corporate Governance a Enterprise Governance. ITG se zabývá odpovědným řízením a chováním vlastníků a vedení organizace ve vztahu k IT, kdy cílem je zajistit propojení IT s celkovou strategií a kulturou organizace. Druhou koncepcí je IT Service Management (ITSM), která se zaměřuje na nižší úroveň řízení podnikové informatiky. Každá z těchto dvou koncepcí má svůj vlastní rámec, který napomáhá manažerům podniku s jejich zaváděním do praxe. I když obě koncepce mají mnoho společného, lze říci, že ITG se zaměřuje spíše na strategické řízení organizace a ITSM se orientuje na taktické a operativní řízení. Koncepce ITG je podporována standardem COBIT a koncepce ITSM standardem ITIL. (Svatá, 2012)

Metodika COBIT (Control Objectives for Information and Related Technologies) je komplexní rámec od společnosti ISACA (Information Systems Audit and Control Association),

který napomáhá manažerům, auditorům a všem vedoucím pracovníkům porozumět IT systémům a jaké postupy navrhovat a implementovat pro jejich řízení.

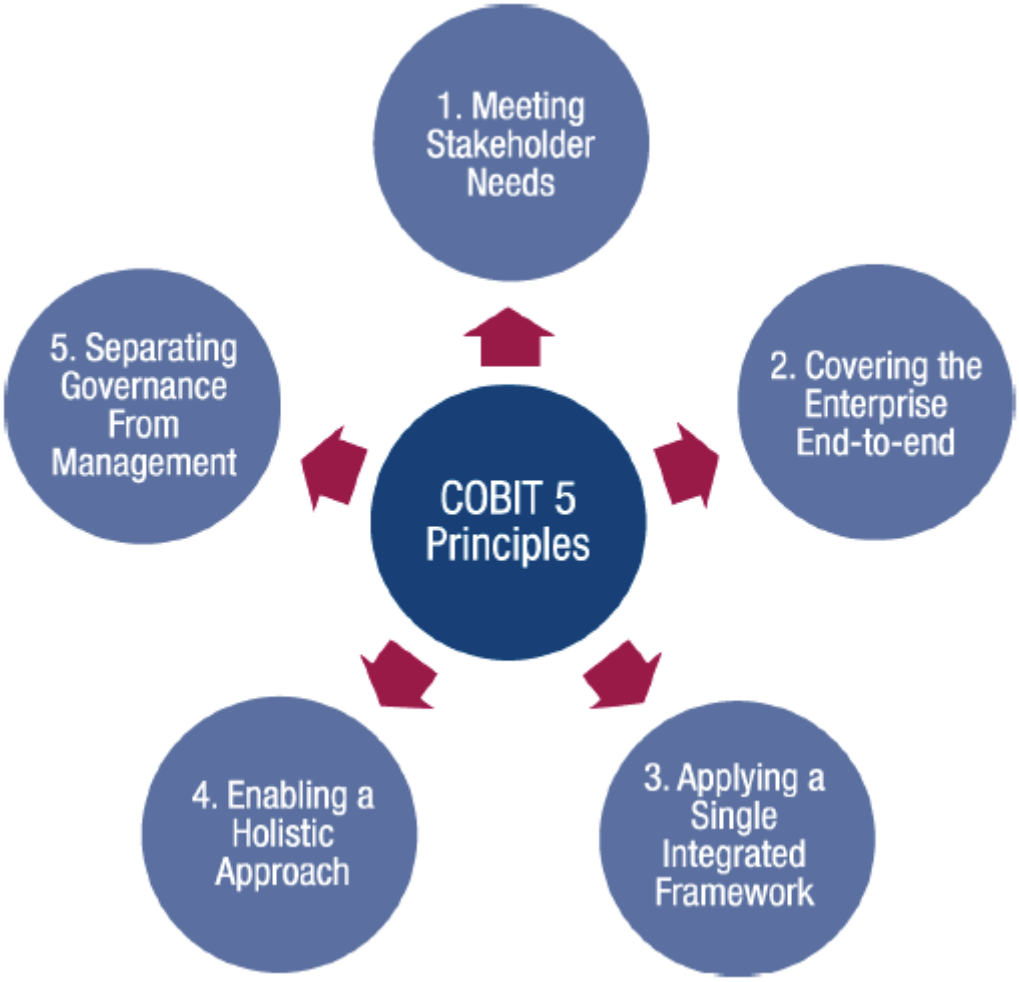
V roce 1996 byla vydána první verze, která obsahovala metodiky čistě zaměřené na audit. O dva roky později byla společností ISACA založena nezisková organizace s názvem IT Governance Institute (ITGI), která převzala odpovědnost za metodiku, a tak v roce 1998 vznikla druhá verze. Druhá verze oproti první byla rozšířena o auditní postupy (Audit Guidelines), sadu implementačních nástrojů (Implementation Toolset) a o rozpracovanější procesy a detailnější cíle (Control Objectives). Třetí verze nazvaná COBIT 3rd Edition byla vydána v roce 2000 a byla rozšířena o manažerské postupy (Management Guidelines). Těchto několik dokumentů bylo sloučeno a v roce 2005 přichází ITGI s COBIT verzí 4.0. V roce 2007 došlo k vydání COBIT verze 4.1, která rozděluje IT do 4 domén. Jsou jimi plánování a organizace (PO – Plan and Organise), pořízení a implementace (AI – Acquire and Implement), dodávka a podpora (DS – Deliver and Support), monitorování a hodnocení (ME – Monitor and Evaluate). Následovaly ještě dvě verze a to COBIT 5 a COBIT 2019, kterým se detailněji věnuje text níže. (Čermák, 2010)

3.3.1 COBIT 5

COBIT 5 byl vydán roku 2005. Váže a posiluje všechna znalostní aktiva společnosti ISACA, jako je COBIT 4.1, Val IT, Risk IT, BMIS, ITAF, TGF a Board Briefing on IT Governance, 2nd Edition. (ISACA, 2012)

COBIT jasně rozlišuje mezi správou (Governance) a řízením (Management). Ve většině podnicích je za správu odpovědné představenstvo, které specifické odpovědnosti za správu může delegovat na zvláštní organizační útvary. Za řízení pak většinou bývá odpovědné výkonné vedení pod vedením výkonného ředitele. Management plánuje, stanovuje, provozuje a monitoruje aktivity v souladu se směrem, který byl dán Governance, za účelem dosažení cílů podniku. Proto jsou tyto cíle také rozděleny do dvou kategorií, a to pro Management a pro Governance, což je posun od COBIT 4.1, který se zaměřuje jen na cíle managementu.

COBIT 5 rozšiřuje dosavadní koncepci pro řízení IT v podnicích zvanou ITG na GEIT (Governance Enterprise of IT), která zdůrazňuje potřebu propojení řízení IT s řízením organizace jako celku. Pro podporu tohoto nového směru, byl COBIT 5 vybudován na pěti základních principech znázorněných na obrázku níže (viz Obrázek 3-4).



Obrázek 3-4 Pět principů COBIT 5 (Zdroj: (ISACA 2014))

- **Uspokojení potřeb zájmových skupin** – Hlavním účelem GEIT je dosažení strategického souladu informací a informačních technologií s cíli podniku. Tyto podnikové cíle a potřeby zainteresovaných stran se v čase mění a udržení souladu je obtížné. Pomocí kaskádování COBIT 5 překládá potřeby zainteresovaných stran do podoby konkrétních cílů podniku a následně do IT cílů.
- „**End-to-end" pokrytí podniku** – GEIT se bezproblémově integruje do jakéhokoli systému správy a řízení organizace. Již nedochází k čistému pokrytí jen funkcí IT, jak tomu bylo zvykem u dřívějších verzí COBIT, ale jsou pokryty všechny funkce a procesy v rámci organizace. Nově jsou informace a související informační technologie považovány za aktiva a zároveň za zdroje, což vyžaduje, aby obchodní manažeři převzali odpovědnost za správu a řízení informačních aktiv v rámci svých organizačních jednotek. Tímto krokem se IT aktiva zařazují na stejnou úroveň správy a řízení jako jsou například majetek a vybavení organizace, lidské zdroje a finanční prostředky.
- **Aplikace jednoho integrovaného rámce** – Organizace se v čase vyvíjí a pro své vnitřní řízení používají mnoho koncepcí, které během své existence zvládly adoptovat. Často se stává, že organizační jednotky v jedné firmě mohou používat rozdílné

koncepce a standardy. Někteří pro zajištění kvality využívají ISO/IEC 9000. IT oddělení může mít zavedeny procesy na základě ITIL rámce a projekty jsou řízeny pomocí uznávaných metodik jako jsou PMBOK či PRINCE2. Na organizace jsou vyvíjeny tlaky i ze stran statutárních orgánů pro plnění nejrůznějších nařízení. (Zora Říhová a Vlasta Svatá, 2019) Vzniká tak potřeba propojit vícero rámců a standardů, které usnadní správu a řízení IT. Proto pátá verze je plně v souladu i s mnoho dalšími uznávanými standardy a rámci a může tak sloužit jako zastřešující rámec pro GEIT. COBIT 5 je tak sladěn s: (ISACA 2014)

    - Risk IT
    - Val IT
    - ISO/IEC 38500:2008[7]
    - ISO/IEC 27001:2013[8]
    - ISO/IEC 20000[9]
    - ISO 31000 series[10]
    - ISO 9001:2008[11]
    - Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control—Integrated Framework
    - IT Infrastructure Library® (ITIL® V3)
    - Project Management Body of Knowledge (PMBOK®)
    - Data Management Body of Knowledge (DMBOK)
    - The Open Group Architecture Framework (TOGAF® 9)
    - Projects in Controlled Environments (PRINCE2®)
- **Podpora holistického přístupu** – účinná a účelná implementace GEIT bere v úvahu několik vzájemně se ovlivňujících složek či mechanismů. COBIT 5 je nazývá aktivátory (enablers). Lze je chápat jako faktory, které jednotlivě či společně ovlivňují, zda bude něco fungovat či nikoliv. Existuje celkem sedm kategorií aktivátorů:
    - Principy, politiky a rámce
    - Procesy
    - Organizační struktury
    - Kultura, etika a chování
    - Informace
    - Služby, infrastruktura a aplikace
    - Lidé, znalosti a kompetence
- **Oddělení úrovně řízení Governance od úrovně řízení Management** – Jak již bylo nastíněno výše, COBIT 5 rozlišuje mezi správou a řízením, které vychází z pokynů ISO/IEC 38500:2008, kdy ředitelé by měli řídit IT prostřednictvím tří hlavních úkolů. Prvním je vyhodnocování současného a budoucího využívání IT. Druhým je

[7] ISO/IEC 38500:2008 Corporate governance of information technology
[8] ISO/IEC:27001:2013 Information technology — Security techniques—Information security management systems – Requirements
[9] ISO/IEC 20000-1:2011 Information technology — Service management — Part 1: Service management system requirements
[10] ISO 31000:2009 Risk management – Principles and guidelines
[11] ISO 9001:2008 Quality management systems — Requirements

přímá příprava a implementace plánů a politik k zajištění toho, aby užívání IT splňovalo obchodní cíle. Posledním úkolem je průběžně sledovat, zda dodržování zásad a samotný výkon je v souladu s vydefinovanými plány. Tato potřeba oddělit úrovně řízení Governance od úrovně řízení Managementu se odrazila na skladbě referenčního procesního modelu. Je definováno 37 procesů, které jsou rozděleny do pěti domén. Jedna doména je čistě vyhrazena procesům Governance a zbylé čtyři jsou určeny pro procesy Management.

- Evaluate, Direct and Monitor (EDM) – Jedná se o správní cíle, kdy správní orgán hodnotí strategické možnosti, řídí vrcholový management nad vybranými strategickými možnostmi a sleduje dosahování cílů.
- Align, Plan and Organize (APO) – Jsou cíle řízení řešící celkově organizaci, strategii a podpůrné aktivity pro IT.
- Build, Acquire and Implement (BAI) – Jsou cíle řízení zpracovávající definici, akvizici a implementaci IT řešení a jejich integraci do podnikových procesů.
- Deliver, Service and Support (DSS) – Cíle řízení, které řeší provozní dodávku a podporu IT služeb, včetně řízení bezpečnosti.
- Monitor, Evaluate and Assess (MEA) – Cíle řízení, které řeší monitorování výkonu a soulad IT s interními cíli a externími požadavky.

Process Assessment Model

Dosavadní hodnoticí model zralosti procesů Capability Maturity Model (CMM) známý z COBIT 4.1, Val IT a Risk IT byl nahrazen novým modelem zvaným Process Assessment Model (PAM). Nové schéma je založené na mezinárodním standardu ISO/IEC 15504 Software Engineering — Process Assessment standard. Detailní popis hodnoticího rámce je zahrnut v samostatné publikaci *COBIT Process Assessment Model (PAM) Using Cobit 5*. Hodnocení probíhá ve dvou dimenzích.

První dimenze se zaměřuje na procesy (The Process Dimension). Procesní dimenzi používá COBIT 5 jako referenční procesní model (PRM), který je složen z 37 procesů v 5 doménách. Druhou dimenzí je hodnocení schopnosti (The Capability Dimension), která poskytuje měřítko, jak daný proces je schopen splňovat současné či předpokládané podnikové cíle. Dimenze schopnosti využívá pro měření 6 úrovní značených od 0 do 5. (ISACA, 2013a)

- **0 – Neúplný proces (Incomplete)** – Proces není implementován nebo selhává při dosahování svého procesního účelu. Na této úrovni je malá nebo žádná evidence o systematickém dosahování účelu procesu.
- **1 – Vykonávaný proces (Performed)** – Implementovaný proces dosahuje svého procesního účelu.
- **2 – Řízený proces (Managed)** – Vykonávaný proces je nyní implementován řízeným způsobem (plánovaný, monitorovaný a upravovány) a jeho pracovní produkty jsou náležitě zavedeny, řízeny a udržovány.
- **3 – Zavedený proces (Established)** – Řízený proces je nyní implementován pomocí definovaného procesu, který je schopen dosáhnout svých procesních výstupů.

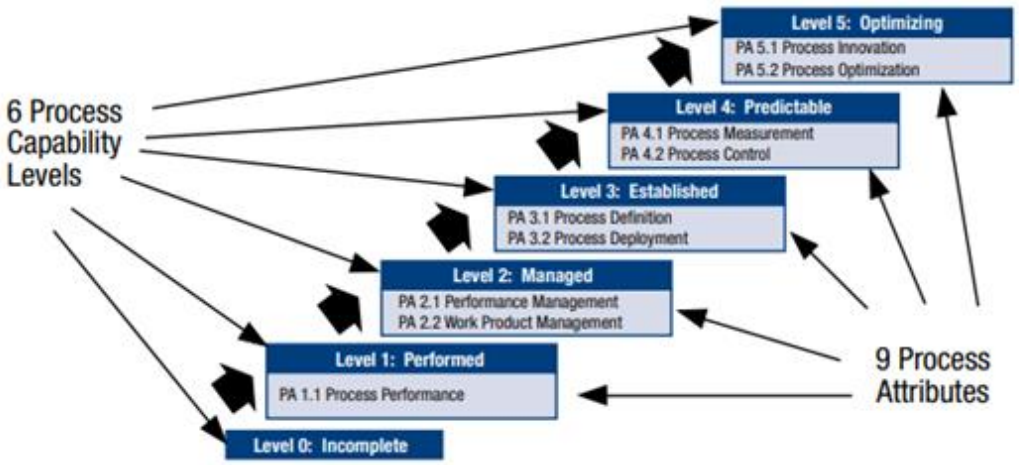
- **4 – Předvídatelný proces (Predictable)** – Zavedený proces nyní funguje v definovaných mezích, aby mohl dosahovat svých procesních výstupů.
- **5 – Optimalizovaný proces (Optimizing)** – Předvídatelný proces se neustále zdokonaluje, aby splňoval relevantní současné a předpokládané obchodní cíle.

Pro posouzení, zda proces dosáhl dané schopnosti, se používají devět procesních atributů. Vzájemnou vazbu mezi úrovněmi schopnosti, procesními atributy znázorňuje Obrázek 3-5.

PAM dále pracuje s hodnoticími ukazateli, které poskytují základ pro určení, zda bylo dosaženo atributů procesu. Existují dva druhy ukazatelů: (ISACA, 2013b)

- **Ukazatele výkonnosti procesu** (Process Performance Indicators), které se vztahují pouze pro posouzení, zda proces dosáhl první úrovně schopnosti. Ukazatele jsou specifické pro každý proces a hodnotí, zda bylo dosaženo první úrovně. Tedy zda implementovaný proces dosahuje svého účelu.
- **Ukazatele procesní schopnosti atributu** (Process Capability Attribute Indicators), které se vztahují k úrovním schopnosti 2-5. Hodnocení je založeno na obecných procesních ukazatelích. Tyto ukazatele platí pro všechny procesy, ale liší se od jedné úrovně schopnosti k druhé. Obecně se rozumí, že čím vyšší úroveň schopnosti je dosaženo, tím nižší je riziko, že proces nesplní svůj zamýšlený účel. Rovněž se obecně rozumí, že čím vyšší je schopnost, tím nákladnější je provozování procesu.

Pro ohodnocení každého atributu se používá hodnoticí stupnice, která je také převzata z normy ISO/IEC 15504. Při rozhodování o tom, jaké hodnocení se má přiřadit, je třeba zajistit konzistentní stupeň interpretace. Tabulka 3-1 popisuje hodnocení založené na základě čtyř hodnot a jejich procentuálního naplnění.



Obrázek 3-5 Úrovně schopnosti a procesní atributy COBIT PAM (zdroj: (ISACA, 2013b))

Tabulka 3-1 Hodnoticí stupnice COBIT PAM (Zdroj: (ISACA 2013b))

Zkratka	Hodnota dosažení	Popis hodnoty	Procentuální dosažení
N	Not Achieved (nedosaženo)	Existují jen malé nebo žádné důkazy o dosažení definovaného atributu v hodnoceném procesu.	0 % - 15 %
P	Partially achieved (částečně dosaženo)	Existují určité důkazy o přístupu (a o dosažení) k definovanému atributu v hodnoceném procesu. Některé aspekty dosažení atributu mohou být nepředvídatelné.	15 % - 50 %
L	Largely achieved (z větší části dosaženo)	Existují důkazy o systematickém přístupu (a o značném dosažení) k definovanému atributu v hodnoceném procesu. V procesu mohou existovat určité slabiny související s tímto atributem.	50 % - 85 %
F	Fully achieved (plně dosaženo)	Existují důkazy o úplném a systematickém přístupu (a o úplném dosažení) k definovanému atributu v hodnoceném procesu. V procesu neexistují žádné významné slabiny související s tímto atributem.	85 % - 100 %

Úroveň schopnosti procesu je určena tím, zda atributy procesu na dané úrovni byly z velké části nebo zcela (L nebo F) dosaženy a zda atributy procesu nižší úrovně byly zcela (F) dosaženy.

3.3.2 COBIT 2019

Poslední verzí je COBIT 2019 a aktuálně zahrnuje tyto publikace:

- *COBIT® 2019 Framework: Introduction and Methodology* představující hlavní koncept COBIT 2019.
- *COBIT® 2019 Framework: Governance and Management Objectives*, který popisuje 40 hlavní cílů pro správu a řízení IT, procesy v nich obsažené a další související komponenty.
- *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution* zkoumá návrhové faktory, které mohou ovlivnit správu a zahrnuje pracovní postupy pro plánování a přizpůsobeného systému pro podnikovou správu.

- *COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance* představuje evoluční vývoj starší verze COBIT5.

COBIT 2019 již není postaven na pěti základních principech, které vydefinoval jeho předchůdce COBIT 5. Nově zavádí celkem 11 principů, které jsou rozděleny do dvou skupin. Principy pro Governance systém (Governance Systems Principles), které popisují základní požadavky Governance systému na informace a technologie v organizaci, a principy pro Governance rámec (Governance Framework Principles), které lze použít k vybudování Governance systému v organizaci. (ISACA, 2018b)

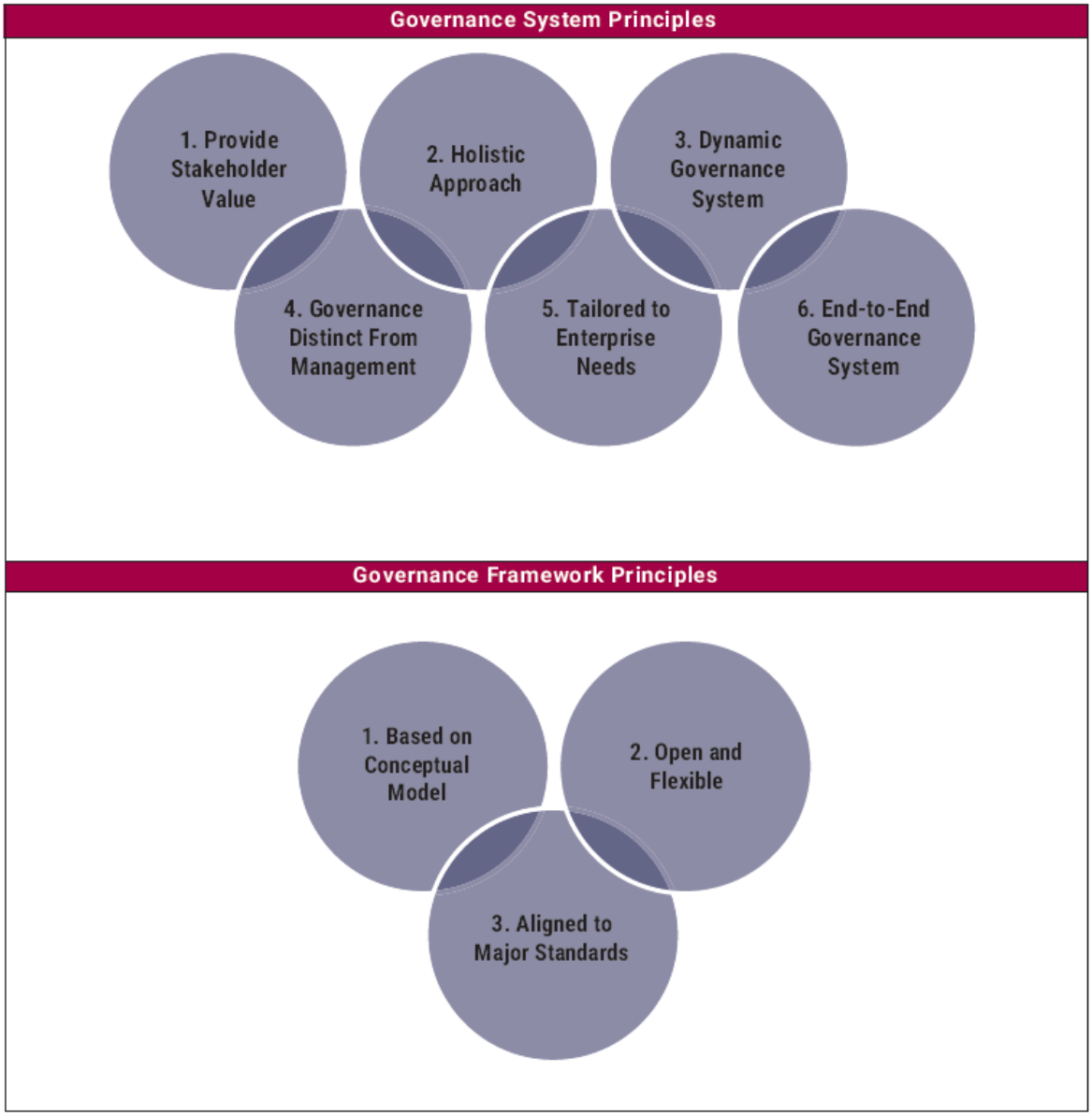
Principy pro Governance systém

- Každý podnik potřebuje systém Governance pro uspokojování potřeb zúčastněných stran a vytvářel tak určitou hodnotu za použití IT.
- Governance systém je tvořen řadou různých komponent, které spolupracují holistickým způsobem.
- Governance systém musí být natolik dynamický, aby při každé změně v návrhu, došlo ke zvážení dopadu těchto změn na EGIT systém a na základě toho se vytvořil životaschopný nový EGIT systém.
- Je třeba jasně rozlišovat mezi aktivitami a strukturami, které spadají pod Management a jaké naopak pod Governance.
- Systém Governance by měl být šitý na míru podnikovým potřebám. Toho lze docílit pomocí sady návrhových faktorů jako parametrů k přizpůsobení a se stanovením priorit komponent systému Governance.
- Governance systém by měl pokrývat podnik od jeho začátku až do konce. Tzn. nezaměřovat se nejen na funkci IT, ale na veškeré technologie a zpracování informací, které organizace používá k dosahování svých cílů.

Principy pro rámec Governance

- Rámec Governance je třeba založit na konceptuálním modelu, který identifikuje klíčové komponenty a vztahy mezi nimi. To vše tak, aby došlo k maximální konzistenci a byla umožněna automatizace.
- Rámec Governance by měl být otevřený a flexibilní, aby bylo umožněno přidávání nového obsahu a řešit nově vzniklé problémy co možná nejflexibilnějším způsobem při zachování integrity a konzistence.
- Rámec Governance by měl být v souladu s hlavními relevantními standardy, rámci a předpisy.

Grafické znázornění všech těchto 11 principů je zobrazeno na následujícím obrázku (viz Obrázek 3-6).



Obrázek 3-6 Principy COBIT 2019 (Zdroj: (ISACA, 2018b))

Komponenty systému správy

Pro uspokojení Governance cílů a Management cílů, potřebuje každá organizace zavést, přizpůsobit a udržovat takový Governance systém, který je složený z řad komponent. Tyto komponenty samy nebo společně přispívají k dobrému fungování podniku. COBIT 2019 identifikuje celkem 7 komponent znázorněných níže (viz Obrázek 3-7).

Obrázek 3-7 COBIT komponenty pro Governance Systém (Zdroj: (ISACA, 2018a))

- **Procesy** – Popisují sadu postupů a činností potřebných k dosažení určitých cílů a tvoří soubor výstupů, které podporují dosažení celkových IT cílů.
- **Organizační struktura** – Je předpisem klíčových entit, které mají rozhodovací pravomoci.
- **Principy, pravidla, rámce** – Převádí požadované chování do praktických pokynů pro každodenní řízení.
- **Informace** – Jedná se o všechny informace produkované a používané podnikem. COBIT se zaměřuje na informace potřebné pro efektivní fungování systému správy (Governance System).
- **Kultura, etika a chování** jednotlivců a podniků – Jedná se často o podceňovaný faktor úspěchu aktivit Governance a Managementu.
- **Lidí, dovednosti a kompetence** – Jde o důležitý prvek, který je vyžadován pro správná rozhodnutí, provedení nápravných opatření a úspěšné dokončení všech činností.
- **Služby, infrastruktura a aplikace** – Poskytují podniku systém správy pro zpracování informací a technologií.

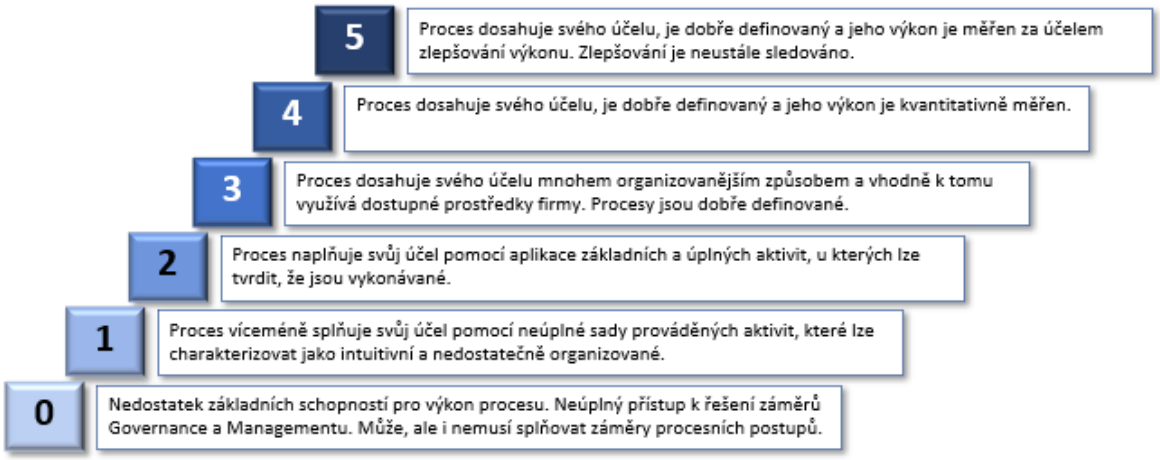
COBIT Performance Management

Řízení výkonu vyjadřuje, jak dobře funguje systém správy a řízení a všechny komponenty a jak je možné jejich aktivity zlepšit, aby dosahovaly požadovaných úrovní. COBIT Performance Management (CPM) zahrnuje měření jak úrovní schopnosti, tak úrovní zralosti. Z velké části tak odpovídá konceptu CMMI Development v2.0, kdy jednotlivé činnosti

procesu jsou spojeny s úrovněmi schopnosti a úrovně zralosti jsou spojeny s oblastmi zaměření. V COBIT 2019 jsou explicitní procesní výstupy a procesní cíle nahrazeny samotnými procesními postupy, což znamená, že hodnocení procesů probíhá podle nové řady norem ISO/IEC33000[12], která reviduje starší řadu norem ISO/IEC 15504[13].

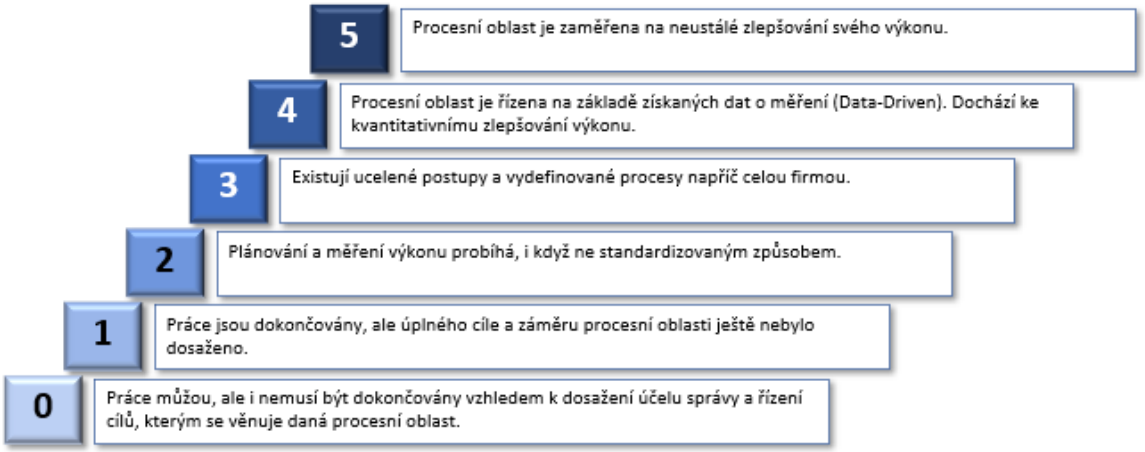
- **Úrovně schopnosti (Capability levels)** – Úrovně schopnosti reprezentují postupné zlepšování jednotlivých konkrétních procesů v organizaci. Je měřítkem toho, jak dobře je proces implementován do prostředí organizace a jaké dosahuje výkonnosti. Vedení společnost by si mělo předem vydefinovat, jaké úrovně pro daný proces chtějí dosáhnout, protože ne vždy snaha dosáhnout 5. úrovně je za jistých podmínek produktivní. Obecně se rozumí, že čím vyšší úrovně schopnosti je dosaženo, tím nižší je riziko, že tento proces nesplní svůj zamýšlený účel. Bohužel s růstem úrovně schopnosti se také navyšují náklady spojené s vykonáváním daného procesu. Úroveň schopnosti každého procesu je vyjádřena pomocí úrovní 0-5.
- **Úrovně zralosti (Maturity levels)** – Úrovně zralosti slouží k charakterizaci celkového stavu procesů pro určitou stanovenou oblast. Tyto oblasti jsou hodnoceny jako celek, i když se skládají z vícero procesů. Toto chápání napomáhá vylepšit sadu souvisejících procesů napříč různými procesními oblastmi. Úrovně zralosti je možné stejně jako úrovně schopnosti rozdělit vzestupně pomocí úrovní 0-5. Pro dosažení konkrétní úrovně zralosti, musí všechny jednotlivé procesy dané procesní oblasti dosahovat minimálně stejné úrovně schopnosti.

Obrázek 3-8 a Obrázek 3-9 znázorňují jednotlivé úrovně schopnosti a zralosti na základě COBIT 2019. Takto definované úrovně byly následně použity pro hodnocení v rámci navrženého nástroje v praktické části.



Obrázek 3-8 Úrovně schopnosti podle COBIT 2019 (Zdroj: (ISACA, 2018b))

[12] ISO/IEC 33000 Information technology — Process assessment
[13] ISO/IEC 15504 Information technology — Process assessment (Software Process Improvement and Capability Determination (SPICE))



Obrázek 3-9 Úrovně zralosti podle COBIT 2019 (Zdroj: (ISACA, 2018b))

3.4 Modely pro hodnocení procesů bezpečnosti IS/IT

Kromě všeobecných modelů a COBIT modelů pro hodnocení vyspělosti procesů uvedených výše, existují i další modely/ nástroje, které se snaží hodnotit procesy spojené s informační bezpečností nebo přímo spojené s aktivitami SOC. Podle průzkumu Rob Van Os (Rob Van Os, 2016) lze mezi ně zahrnout:

- **CMM bezpečnosti informací** – Všechny tyto modely se věnují ať už z části nebo přímo bezpečnostními tématy, jako jsou řízení bezpečnosti či řízení rizik.
    - Software Assurance Maturity Model (OpenSAMM)
    - Cybersecurity Capability Maturity Model (C2M2)
    - ISA-CMM
    - Gartner ITScore for Security & Risk Management
    - Risk Management Process Maturity
    - (Im)-Maturity Capability Model
    - ISO/IEC 21827:2008 (SSE-CMM)[14]
    - Open Information Security Management Maturity Model (O-ISM3)
- **CMM specializující se přímo na aktivity SOC** – Existují i přímo se zaměřující modely, které byly vytvořeny soukromým sektorem a nejsou volně dostupné veřejnosti nebo vytvořené v rámci školních prací.
    - HP Security Operations Maturity model (HP SOMM)
    - IBM SOC consulting services – part Maturity Measurement
    - LogRhythm's Security Operations Maturity Model (SOMM)
    - Security Operations Center Capability Maturity Model (SOC-CMM)

[14] ISO/IEC 21827:2008 Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model (SSE-CMM)

Bohužel využití těchto modelů/ nástrojů je časově náročnější a vyžaduje určitou znalost samotných modelů a jejich metodik nebo jak již bylo zmíněno, jsou poskytovány v rámci externích služeb za úplatu, tudíž se nejedná o sebehodnocení.

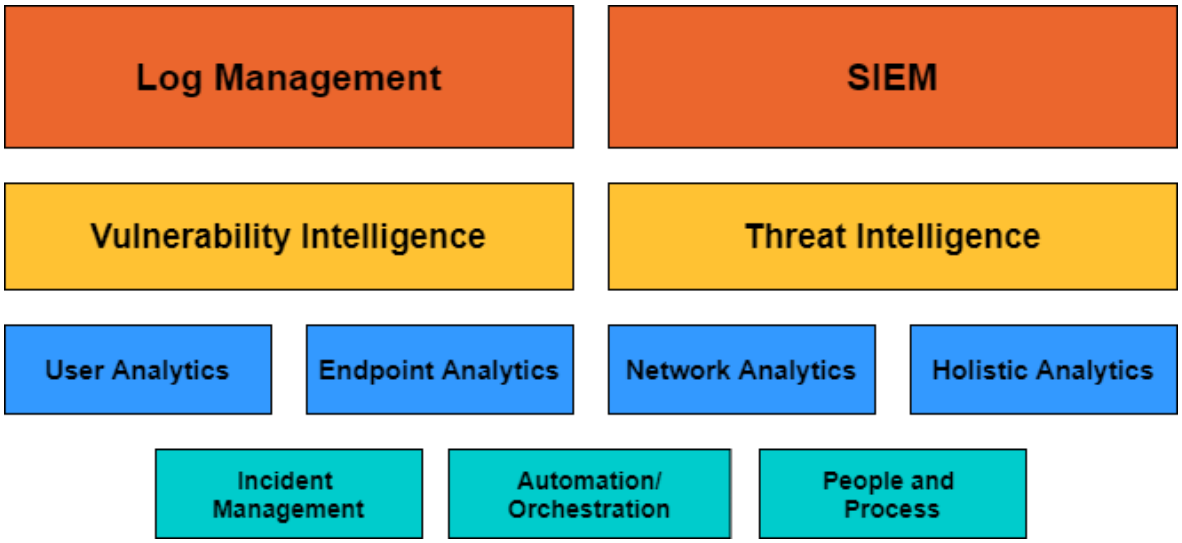
3.4.1 LogRhythm's SOMM

Společnost LogRhythm vyvinula rámec životního cyklu hrozby (Threat Lifecycle Management — TLM), který má organizacím napomáhat sladit technologie, lidi a procesy za účelem dodávek služeb týmů SOC, mezi které patří sledování hrozeb, jejich odhalování, analýza a zvládání bezpečnostních incidentů vzniklých v důsledku těchto hrozeb. Rámec pomáhá měřit efektivitu bezpečnostních SOC operací a pomáhá je posouvat na vyšší úroveň. Model se opírá o vytyčení životního cyklu hrozby, který definuje šest fází – průzkum, počátek kompromitace, převzetí kontroly, postranní aktivity, dosažení cíle a exfiltrace. Pro identifikaci a zvládání takových hrozeb je třeba určitých operativních schopností a procesních postupů. SOMM se opírá o čtyři základní principy každého SOC. Jedná se o sledování hrozeb, jejich odhalování, investigaci a následné řešení incidentů. (Petersen et al., 2019)

Model používá dva druhy metrik, kterými jsou průměrný čas pro detekci (mean time to detect — MTTD) a průměrný čas pro zvládání (mean time to respond — MTTR). S růstem vyspělosti SOC se tyto časy snižují, což zároveň snižuje riziko dopadu kybernetických bezpečnostních incidentů. SOMM specifikuje pět úrovní zralosti (0-4), které na sebe navazují a s každou další vyšší úrovní přichází určité vylepšení technologií a procesů, které napomáhají snižování MTTR a MTTD. Pro splnění určité úrovně zralosti není klíčové, jakým způsobem došla organizace k naplnění dané podmínky, ale pouze to, zda byla daná podmínka splněna.

- Level 0 – Blind
- Level 1 – Minimally compliant
- Level 2 – Securely compliant
- Level 3 – Vigilant
- Level 4 – Resilient

SOMM hodnotí určité aktivity a aspekty SOC, kterým říká bloky. Celkově specifikuje 11 takových bloků, které znázorňuje obrázek níže (viz Obrázek 3-10).



Obrázek 3-10 Jednotlivé stavební bloky modelu SOMM (Zdroj: (Cathey, 2019))

Jednotlivé úrovně zralosti jsou pro každý blok vydefinovány zvlášť. Malou ukázku pro hodnocení jednotlivých bloků nastiňuje Tabulka 3-2.

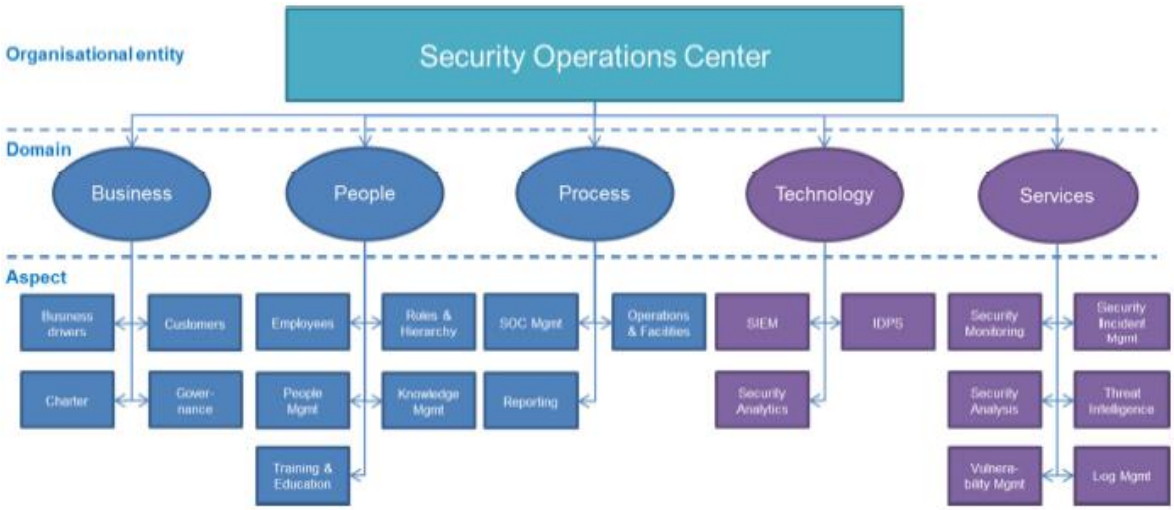
Tabulka 3-2 Hodnocení SOC bloků pomocí SOMM (Zdroj: (Cathey, 2019))

Blok	Úrovně SOMM
Log Management	0 – Logy nejsou centrálně sbírány. 1 – Sbírání logů je primárně řízeno požadavky auditu. 2 – Sběr logů se provádí ze všech bezpečnostních nástrojů, síťové infrastruktury, produkčních serverů, aplikací a databází. 3 – Sběr logů se zaměřuje i na systémy fyzického zabezpečení a nějaká osobní zařízení. 4 – Sběr logů se provádí ze všech systémů generující logy a auditní záznamy.
SIEM	0 – Organizace nepoužívá SIEM. 1 – SIEM je zaveden hlavně kvůli požadavku auditu. 2 – SIEM se používá k monitorování a reakci hrozeb a zda dochází k dodržování předpisů. 3 – SIEM se používá pro pochopení kybernetického bezpečnostního rizika napříč celým produkčním prostředím. 4 – SIEM se používá k pochopení kybernetického bezpečnostního rizika napříč logickým, fyzickým a sociálním prostředí.
Vulnerability Intelligence	0 – Organizace nepoužívá žádný systém pro řízení zranitelností. 1 – Skenují se jen ty systémy, které jsou vyspecifikovány nějakými požadavky (audit, zákon, …). 2 – Skeny pro odhalování zranitelností probíhají pravidelně v obvodovém perimetru nebo na jiných vysoce rizikových systémech. 3 – Existuje určitá holistická báze znalostí (intelligence) se základními korelacemi a integrací workflow. 4 – Existuje určitá holistická báze znalostí (intelligence) s pokročilou korelací a integrací automatizovaného workflow.
Threat Intelligence	0 – Organizace nesbírá žádné informace o hrozbách. 1 – Organizace používá informace jen omezeně, a to jen z volně dostupných zdrojů. 2 – Pracovní postupy související s hrozbami jsou spíše reaktivní a manuální. 3 – Znalosti získané o hrozbách jsou založeny na IOC. Tyto získané znalosti jsou integrovány do pracovních postupů a do prováděných analýz. 4 – Hrozby jsou založeny na IOC a TTP dle odvětvové specifikace a jsou integrované do pracovních postupů a do prováděných analýz.
User & Entity Behaviour Analytics	0 – Aktivity uživatelů nejsou monitorovány. 1 – Monitorování pouze privilegovaných uživatelů typu admin a administrátor. 2 – Monitoring aktivit uživatelů je založen na scénářích, které definují „nežádané“ aktivity. 3 – Monitoring uživatelských aktivit probíhá v reálném čase na základě získaných informací z trendů a vzorů jednotlivých aktivit. 4 – Monitoring na všech produkčních serverech a pracovních stanicích je monitorován v kombinaci s monitoringem aktivit jednotlivých uživatelů.

3.4.2 SOC-CMM

Model vznikl v roce 2016 jako magisterská závěrečná práce, kdy autorem je Rob Van Os z Technické univerzity Luleå ve Švédsku. Model je sladěn s normou NIST CSF. Úroveň zralosti je zde měřena napříč pěti doménami, kterými jsou podnikání, lidé, procesy, technologie a služby. První tři domény jsou hodnoceny pouze z hlediska úrovně zralosti (maturity levels) a domény technologie a služby jsou hodnoceny z hlediska úrovně zralosti i schopnosti. Přehled domén a k nim navázaných 25 aspektů znázorňuje obrázek níže (viz Obrázek 3-11).

Jednotlivé domény a aktivity, o které se model opírá byly vyspecifikovány na základě dotazníkového šetření, do kterého se zapojilo 16 organizací. Dotazník byl rozdělen do několika částí. Otázky se týkaly ohledně aktuálně vnímané úrovně zralosti služeb SOC, outsourcingu, možnosti rozpočtu, velikosti SOC, jednotlivých rolí a používaných technologií.



Obrázek 3-11 SOC Capability Maturity Assessment Model (Zdroj: (Rob Van Os, 2016))

Model zralosti byl navržen na základě výzkumu nazvaném *Inductive Design of Maturity Models: Applying the Rasch Algorithm for Design Science Research* od Lahrmanna a kolektivu. (Lahrmann et al., 2011). Úroveň zralosti je zde hodnocena jako kontinuální veličina. Zde se model odkloňuje od běžné praxe CMMI, kdy úrovně zralosti jsou hodnoceny jako stupňovitá reprezentace dat (staged representation) na místo kontinuální reprezentace dat (continuous representation). Nástroj pro určení úrovně zralosti používá pro každou doménu pět základních otázek vycházejících z CMMI-SVC.

- Je požadovaný aspekt (služba, role, technologie, …) identifikován?
- Byl aspekt formalizován, aby bylo zajištěno stejně kvalitních výstupů při vícero opakování?
- Je aspekt plně zdokumentován a formalizován?
- Je aspekt měřen za účelem optimalizace procesu?
- Je aspekt měřen, zda dosahuje podnikových cílů a na základě toho optimalizován?

Každá jednotlivá otázka reprezentuje jednu úroveň zralosti (1-5).

Úroveň schopnosti je měřena pouze pro služby a technologie. Výpočet úrovně je dán výsledky počátečního dotazníkového šetření, kdy jednotlivé služby a technologie byly na základě výsledků rozděleny na základní, podpůrné a neobvyklé. Výpočet je primárně dán určením úrovně zralosti a na základě této naměřené úrovně byly dodatečně vybrány technologie a služby, které budou spadat pod tuto úroveň. Pokud podnik například dosahoval 3. úrovně zralosti pro technologie, bylo dle dotazníku zjištěno, že společnosti této úrovně používají určitý typ nástrojů a poskytují určité služby. Pokud organizace takovou službu nebo technologii využívá, ale nedosahuje patřičné úrovně zralosti, nepočítá se do konečného hodnocení. (Rob Van Os, 2016)

4 Návrh capability maturity modelu

Pro tvorbu modelu byla vybrána metodologie inspirovaná prací Beckera *Developing Maturity Models for IT Management*, kde se svými kolegy předkládá doporučení pro tvorbu modelů hodnoticí úroveň zralosti. Metodologie staví na Design Science Research (návrhový typ výzkumu – DSR) a na výzkumné práci Hevnera. Jedná se o metodologický přístup k navrhování artefaktů, které slouží k rozvíjení znalostí ohledně problémových situací. Artefaktem se rozumí symbolická reprezentace nebo fyzická instance navrhovaného konceptu. (Hevner et al., 2004) Artefakt musí být zhodnocen, zda je užitečný pro řešení daného problému, který doposud nebyl vyřešen nebo poskytuje jeho efektivnější řešení. Z toho důsledku může být pro účely práce CMM chápán jako artefakt, který slouží k měření úrovní zralosti a schopnosti SOC.

Hevner a kolektiv (Hevner et al., 2004) představují sedm pokynů pro DSR, které jsou inspirací pro následný postup návrhu CMM.

- **Návrh jako artefakt** – DSR musí produkovat životaschopný artefakt ve formě konstrukce, modelu, metody či instance.
- **Relevance problému** – Cílem DSR je vytvoření technologického řešení důležitých a relevantních problémů.
- **Hodnocení návrhu** – Užitečnost, kvalita a účinnost artefaktu musí být důsledně prokázána pomocí dobře provedených metod hodnocení.
- **Příspěvky výzkumu** – Efektivní DSR musí poskytnout jasné a ověřitelné příspěvky v oblastech návrhu artefaktu, základů návrhu a metodik návrhu.
- **Rigoróznost výzkumu** – Výzkum v oblasti návrhu se spoléhá na použití rigorózních (přísných) metod jak při konstrukci, tak při hodnocení návrhu artefaktu.
- **Návrh jako proces hledání** – Hledání efektivního artefaktu vyžaduje využití dostupných prostředků k dosažení požadovaných cílů při splnění zákonů v problémovém prostředí.
- **Komunikace výzkumu** – Výzkum v oblasti návrhu musí být efektivně prezentován jak technickým pracovníkům, tak managementu.

Becker a kolektiv (Becker et al., 2009) na základě specifikovaných DSR pokynů od Hevnera vydefinoval osm požadavků, které jsou pro tvorbu CMM zásadní. Logiku osmi požadavků založených na Hevnerových sedmi postupech znázorňuje následující tabulka (viz Tabulka 4-1).

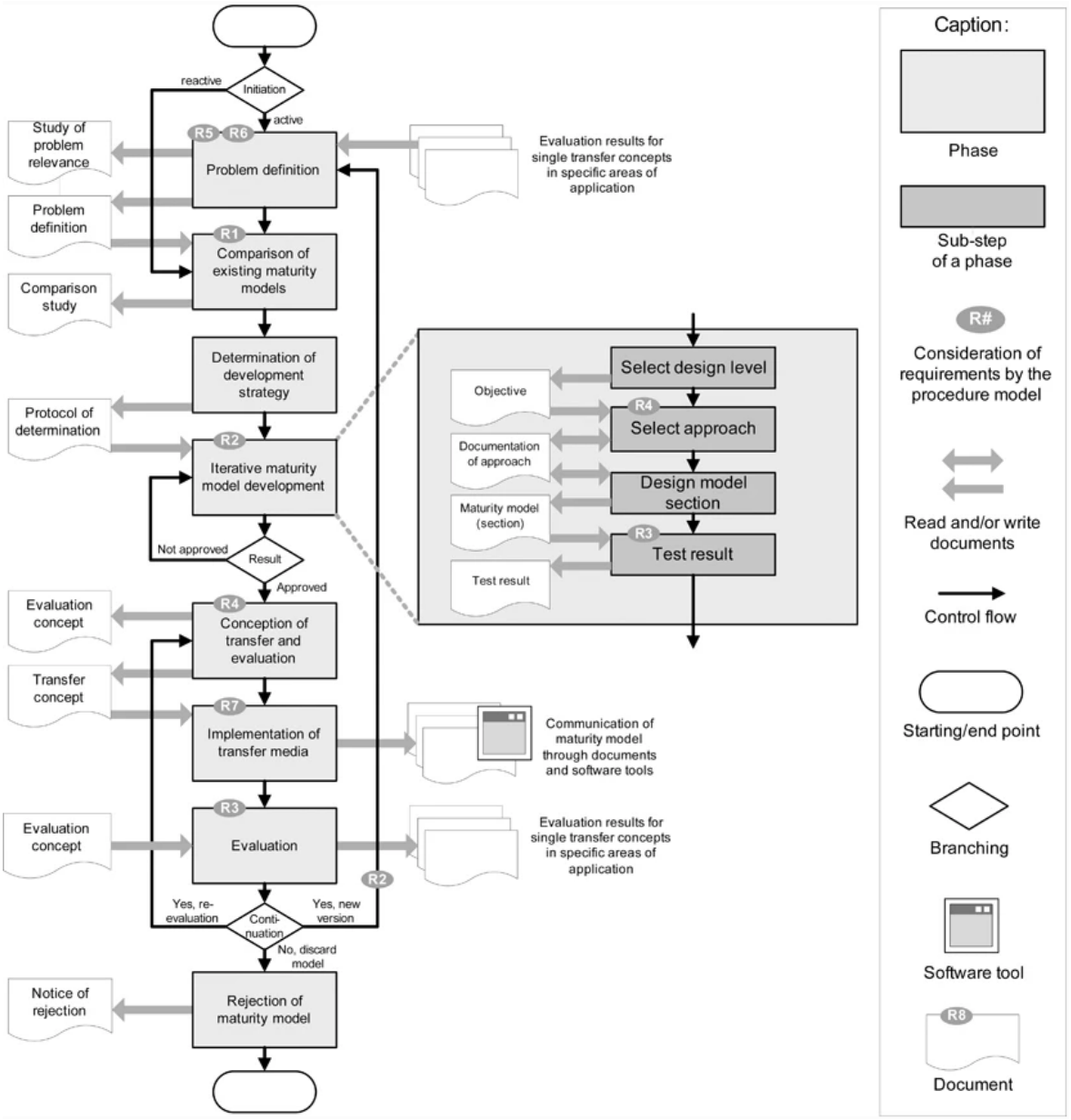
Tabulka 4-1 Provázanost požadavků na vývoj CMM a pokynů pro DSR (Zdroj: Autor na základě (Becker et al., 2009))

7 pokynů pro Design Science Research	**8 požadavků pro vytvoření CMM**
G1 – Návrh jako artefakt	• R1 – Srovnání se stávajícími modely zralosti
G2 – Relevance problému	• R5 – Identifikace relevance problému • R6 – Definice problému
G3 – Hodnocení návrhu	• R3 – Hodnocení
G4 – Příspěvky výzkumu	• R1 – Srovnání se stávajícími modely zralosti
G5 – Rigoróznost výzkumu	• R4 – Multi-metodologické postupy
G6 – Návrh jako proces hledání	• R2 – Iterativní postupy • R3 – Hodnocení
G7 – Komunikace výzkumu	• R7 – Cílená prezentace výsledků • R8 – Vědecká dokumentace

- **R1 – Srovnání se stávajícími modely zralosti** – Cílem DSR je vyvinutí inovativního artefaktu pro řešení problémové situace, který zároveň jistým způsobem přispěje současnému výzkumu. Proto je třeba vývoj CMM podložit srovnáním se stávajícími modely. Nový model může být pouze zdokonalením již existujícího modelu.
- **R2 – Iterativní postupy** – Modely zralosti musí být vytvářeny iterativním způsobem, což znamená krok po kroku.
- **R3 – Hodnocení** – Všechny principy a předpoklady pro vývoj modelu zralosti, stejně jako užitečnost, kvalita a účelnost artefaktu musí být iterativně vyhodnocovány. Zároveň hodnocení musí být prováděno pomocí vhodné vědecké metody, kdy DSR přijímá multi-metodologické postupy.
- **R4 – Multi-metodologické postupy** – Vývoj modelu zralosti využívá řadu výzkumných metod, jejichž využití musí být opodstatněné a vzájemně provázané, což zajistí určitou úroveň rigoróznosti.
- **R5 – Identifikace relevance problému** – Pro výzkumné pracovníky a odborníky z praxe musí být prokázána relevance řešení problému projektovaného do modelu zralosti. Relevance může být zajištěna pomocí dotazování potenciálních uživatelů CMM.
- **R6 – Definice problému** – Před návrhem je třeba určit doménu potenciálního použití modelu zralosti, jakož i podmínky pro jeho aplikaci a zamýšlené výhody.

- **R7 – Cílená prezentace výsledků** – Prezentace modelu zralosti musí být cílená s ohledem na podmínky jeho aplikace a potřeby uživatelů. Prezentace musí být zaměřena na konkrétní skupiny uživatelů.
- **R8 – Vědecká dokumentace** – Proces návrhu modelu zralosti je třeba podrobně zdokumentovat s ohledem na každý krok procesu, zapojené strany, použité metody a získané výsledky.

Model rozlišuje osm fází vývoje CMM. Jednotlivé prvky modelu staví na výše vyspecifikovaných požadavcích. Požadavky R1-R7 jsou v modelu graficky znázorněny. Požadavek R8 byl začleněn pomocí dokumentů generovaných v průběhu celkového návrhu CMM. Vývojový model vytvořený Beckerem je znázorněn na obrázku níže (viz Obrázek 4-1).



Obrázek 4-1 Model vývoje CMM (zdroj: (Becker et al., 2009))

4.1 Definice problému

Před zahájením modelování artefaktu je nezbytné vydefinování samotného problému, proč je zapotřebí vůbec model vytvářet. Zároveň je třeba prokázat relevantnost řešení, zda existuje skutečná poptávka po modelu.

Problém byl vydefinován v samotném úvodu této práce (viz kapitola Úvod), který nastiňuje problematický růst kybernetických útoků mířených na veřejné i soukromé organizace. Jen za rok 2019 bylo detekováno více než 7 000 narušení, kdy uniklo 15,1 bilionu záznamů. Nejčastějším terčem útoků jsou klientská data. Útočníci jsou stále chytřejší a rychlejší, avšak průměrný čas na identifikaci a řešení kybernetického bezpečnostního incidentu je 280 dní. Což zcela nahrává dalšímu šíření kyberkriminality. Dle průzkumu se náklady spojené s kyberkriminalitou neustále zvyšují. (IBM Corporation, 2020) Bohužel středoevropské organizace se ještě zcela nenaučily finančně řídit IT útvary, na tož aby dokázaly finančně řídit útvary zaměřující se na informační bezpečnost.

Možnou odpovědí, jak zvládat kybernetické útoky, snižovat reakční čas na incidenty, a tím i redukovat náklady, je vybudovat kvalitní SOC. Často bývá problém určit, zda SOC opravdu dosahuje potřebné kvality. Zda organizace dostává na zpět potřebnou přidanou hodnotu nebo naopak, zda je třeba SOC více rozvíjet. Pro měření kvality slouží CMM (Capability Maturity Model). Bohužel praxe nedisponuje adekvátními modely pro měření výkonnosti SOC. Stávající modely se buď nespecifikují do takové hloubky, jako jsou jednotlivé aktivity SOC, což znamená, že osoba provádějící testování musí mít rozsáhlé zkušenosti s aplikací obecných hodnoticích modelů. Sice existují modely pro hodnocení kvality SOC, ale jsou jistým příjmem konzultantských firem, tedy není běžně možné za nízkých nákladů otestovat kvalitu SOC. To může být pro mnoho neziskových organizací značným problémem. Podle průzkumů společnosti IBM je nejvíce postiženým sektorem v oblasti úniku dat zdravotnictví, kdy náklady na únik jednoho záznamu byly vyčísleny na 429 dolarů. (IBM Corporation, 2020)

Dle výše zmíněného lze problém definovat následovně: Absence modelu pro hodnocení zralosti a schopností SOC, který je volně k dispozici a jeho použití je snadno aplikovatelné.

4.2 Porovnání stávajících řešení

Dalším krokem je zkoumání, zda již nedošlo k vyřešení identifikovaného problému. Existující řešení nemusí přinášet nejlepší výsledky, což může být hnacím motorem pro vylepšení stávajících modelů. Komplexní srovnání je nutné pro odůvodnění návrhové strategie CMM.

Průzkumu jednotlivých modelů je věnována třetí kapitola (viz kapitola Hodnocení vyspělosti procesů). Nejvíce použitelnými modely pro vyřešení nadefinovaného problému jsou Security Operations Maturity Model (SOMM) od společnosti LogRhythm a Capability Maturity Model – Security Operations Center (CMM-SOC) od Rob Van Os.

SOMM model je velice široký. Skládá se z 11 bloků, které popisují základní i podpůrné aktivity SOC. Základním nedostatkem je, že tento model není běžně k dostání. Volně dostupný je jen koncept hodnocení a vysvětlení jednotlivých úrovní zralosti.

Druhý model CMM-SOC je ze všech prozkoumaných možností pro řešení problému nejvhodnější. Ale i tento model má pár svých nedostatků. Model staví na aktivitách definovaných praxí, ale tato praxe je dána pouze na základě dotazování 16 společností. Model by měl být v souladu s NIST CSF, ale tento rámec definuje pouze co je třeba dělat, ale již neříká, jak toho docílit. V neposlední řadě jsou úrovně zralosti testovány pouze pomocí pěti otázek, kdy každá z nich určuje jednu úroveň zralosti.

4.3 Stanovení strategie rozvoje

Předcházející fáze *Porovnání stávajících řešení* je nutná pro odůvodnění návrhové strategie, kterou je třeba podle požadavku R8 nutno zdokumentovat.

Vybranou strategií je vytvoření nového modelu CMM, který se bude opírat o relevantní standardy a rámce tak, aby byl vytvořen co nejúčinnější a nejúčelnější model pro hodnocení SOC. Prvním krokem bude vybrání aktivit, které budou podléhat měření kvality. Následně budou vytvořeny hodnoticí úrovně schopnosti a zralosti SOC a k nim příslušné hodnoticí podmínky, které bude třeba splnit, aby bylo dosaženo určité úrovně. Podmínky budou formulovány pomocí testových otázek, na které bude respondent odpovídat. Veškeré testování bude probíhat v softwarovém nástroji. Úrovně schopnosti a zralosti budou vyhodnocovány automaticky po vyplnění všech příslušných otázek v daném nástroji. Nástroj musí být jednoduchý na ovládání i pro netechnickou veřejnost.

4.4 Iterativní vývoj CMM

Jedná se o ústřední fázi návrhu CMM. Pro vytvoření v praxi použitelného modelu je třeba získat dostatečné informace o vlastnostech SOC. Proto bylo třeba odpovědět na základní otázky.

- Jaké jsou běžné modely pro SOC?
- Jaké služby SOC poskytuje a na jaké procesy se vážou?
- Jaké je personální obsazení SOC a jaké role a odpovědnosti zastupují jeho jednotliví členové?
- Jaké technologie pro práci SOC využívá?

Na všechny tyto čtyři otázky bylo odpovězeno v úvodu práce, která se věnuje představení SOC (viz kapitola Security Operations Center). Vzhledem k tomu, že publikací věnující se SOC je omezený, hlavními zdroji odpovědí byly knihy *Designing and Building Security Operations Center* od Davida Nathanse (Nathans, 2014) a *Ten Strategies of a World-Class Cybersecurity Operations Center* od Carsona Zimmermana (Carson Zimmerman, 2014). Tato literatura byla vybrána na základě toho, že se jedná o komplexní publikace věnující se problematice bezpečnosti, jak vybudovat fungující SOC na základě potřeb podniku a jakým

jednotlivým aktivitám by se SOC měl věnovat. Oba autoři jsou v praxi uznávanými konzultanty v oblasti budování bezpečnostních programů pro firmy a mají mnohaleté zkušenosti. Tyto dva zdroje byly porovnány a jednotlivé aktivity byly vzájemně provázány. Tak došlo k vytyčení základních oblastí, kterým by se SOC měl věnovat. Tyto aktivity byly následně napasovány na NIST CSF, který je uznávaným rámcem pro řízení kybernetické bezpečnosti. Byly tak vytyčeny jednotlivé aktivity definované v NIST CSF, které by měly jednotlivé SOC splňovat. Toto mapování je dostupné v příloze (viz Příloha A: Mapování aktivit SOC na NIST CSFMapování aktivit SOC na NIST CSFMapování aktivit SOC na NIST CSF). Díky tomuto mapování vyvstalo 8 domén pro měření úrovně schopnosti a zralosti. Jedná se o:

- Bezpečnostní analýzy (Analysis)
- Budování znalostní o kybernetických hrozbách (Build Cyber & Threat Intelligence)
- Správa bezpečnostních nástrojů a jejich ladění (Tooling)
- Správa přístupových práv (Identity & Access Management)
- Řízení bezpečnostních incidentů (Incident Response)
- Poincidentní aktivity (Post-incident Activities)
- Řízení zranitelností (Vulnerability Management)
- Bezpečnostní monitoring (Monitoring)

Následně bylo třeba vytvořit pro tyto domény úrovně schopnosti. Během průzkumu již existujících modelů, který proběhl v kroku dvě, bylo zjištěno, že ISACA ve spolupráci s NIST vydala dokument, který namapovává jednotlivé aktivity NIST CSF na COBIT 5 i na COBIT 2019. Jelikož COBIT 2019 standardně definuje úroveň schopnosti u aktivit jednotlivých procesů, byl pro účely další tvorby CMM využit právě tento framework. Dokument pro mapování pod *názvem NIST Cybersecurity Framework V1.1/COBIT 2019 Mapping* je dostání na oficiální stránkách ISACA. (ISACA, 2019)

Mapování mezi NIST CSF a COBIT 2019 vyvolal značné úpravy v návrhu modelu. Pro určení vzájemných závislostí mezi NIST CSF a COBIT 2019 jsou v dokumentu používány čtyři možnosti návazností.

- Equal to (odpovídá procesu) – Element v NIST CSF přímo odpovídá danému procesu v COBIT 2019 a všem jeho aktivitám.
- Intersects with (protíná výčet procesů) – Výčet procesů v COBIT 2019 může napříč jednotlivými aktivitami obsahovat požadovaný element specifikovaný v NIST CSF.
- Superset of (nadmnožina procesů) – Na výčet procesů v COBIT 2019 je třeba nahlížet z nadhledu a širšího kontextu, aby bylo možné daný element z NIST CSF namapovat.
- Subset of (podmnožina procesu) – Pouze část přiděleného procesu COBIT 2019, či jen některé aktivity procesu odpovídají elementu z NIST CSF.

Jednotlivé aktivity tak musely být modifikovány, vypuštěny nebo sloučeny. Vznikaly také duplicitní aktivity nebo velmi podobné aktivity, které bylo třeba odstranit. Při mapování byly odhaleny i další nedostatky. Domény Incident Response a Post-incident Activities při plném dodržení mapování neodpovídaly potřebám praxe. Proto bylo zvětší části odstoupeno od kritérií NIST CSF a tyto domény byly nově vydefinovány čistě na základě COBIT 2019 tak, aby pokryly aktivity vydefinované literaturou výše. Některé aspekty NIST CSF byly

začleněny do těchto domén. Kvůli nevyrovnanosti a překryvu aktivit napříč výše specifikovanými doménami došlo k úpravě domén. Doména Tooling, která měla zastřešovat správu bezpečnostních nástrojů a jejich ladění, se rozdělila do dvou domén. První z nich se nazývá Detection Rules (detekční pravidla), která z části obsahuje některé aktivity dříve vedených pod doménou monitoring. Druhá se jmenuje SOC Tools Maintenance (údržba SOC technických nástrojů).

Při několika iteracích, úpravách a následného testování bylo vytvořeno celkem 9 domén, 33 subdomén a 309 aktivit, které jsou definovány testovými dotazy. Finální strukturu pro účely testování demonstruje tabulka níže (viz Tabulka 4-2). Celkový výpis vytvořených otázek k subdoménám a návrh jednotlivých úrovní schopnosti je přiložen v příloze (viz Příloha B: Architektura CMM).

Tabulka 4-2 Finální návrh testovaných oblastí pro CMM (Zdroj: Autor)

Doména	Subdoména
Vulnerability Management	• Identifikace, detekce, klasifikace zranitelností • Zvládání zranitelností a patchování • Používání scénářů • Strategie, procesy, postupy • Znalosti personálu • Reporting • Měření
Monitoring	• Monitoring infrastruktury • Bezpečnostní monitoring
Post-incident Activities	• Převedení incidentu do problému • Tvorba BCP a DRP • Testování a cvičení BCP a DRP
Build Cyber & Threat Intelligence	• Identifikace a klasifikace informací • Uspořádání informací a vzájemné propojování dat • Použití a šíření znalostí • Nástroj pro uchování dat
Analysis	• Investigace a diagnostika • Schopnosti analytiků
Identity & Access Management	• Řízení identit uživatelů a logického přístupu • Řízení rolí, odpovědností, přístupových oprávnění a úrovně oprávnění • Ověření, schválení a plnění požadavků ohledně přístupových práv
Incident Response	• Identifikace Incidentu • Klasifikace/kategorizace incidentu • Řešení incidentů • Uzavírání incidentů • Sledování stavu a vytváření reportů
Detection Rules	• Logování a korelace událostí • Návrh řešení • Vývoj řešení • Testování a úprava řešení
SOC Tools Maintenance	• Dodávka třetích stran • Provoz a údržba nástrojů • Pořizování a implementace nástrojů

Úroveň schopnosti je počítána pro všechny subdomény a úroveň zralosti je počítána jen pro jednotlivé domény.

Úrovně schopnosti subdomén vychází z jednotlivých aktivit, které je nutno splnit, aby bylo dosaženo dané úrovně. Pro tyto účely metodika testování a měření úrovní je založena na metodice CPM a PAM v COBIT5 a COBIT2019, které byly detailněji vysvětleny v textu výše (viz COBIT Performance Management a Process Assessment Model). Na každou testovou otázkou je třeba odpovědět, na kolik procent je dané tvrzení pravdivé a daná aktivita se v SOC vykonává. Aby došlo k dosažení dané úrovně, musí být všechny aktivity hodnoceny minimálně úrovní Largely. Metodický klíč hodnocení znázorňuje obrázek níže (viz Obrázek 4-2).

Úrovně zralosti jednotlivých domén jsou dány podmínkou, že pro dosažení dané úrovně zralosti je nezbytné dosáhnout minimálně stejné úrovně schopnosti nebo maximálně možné úrovně schopnosti ve všech subdoménách dané domény.

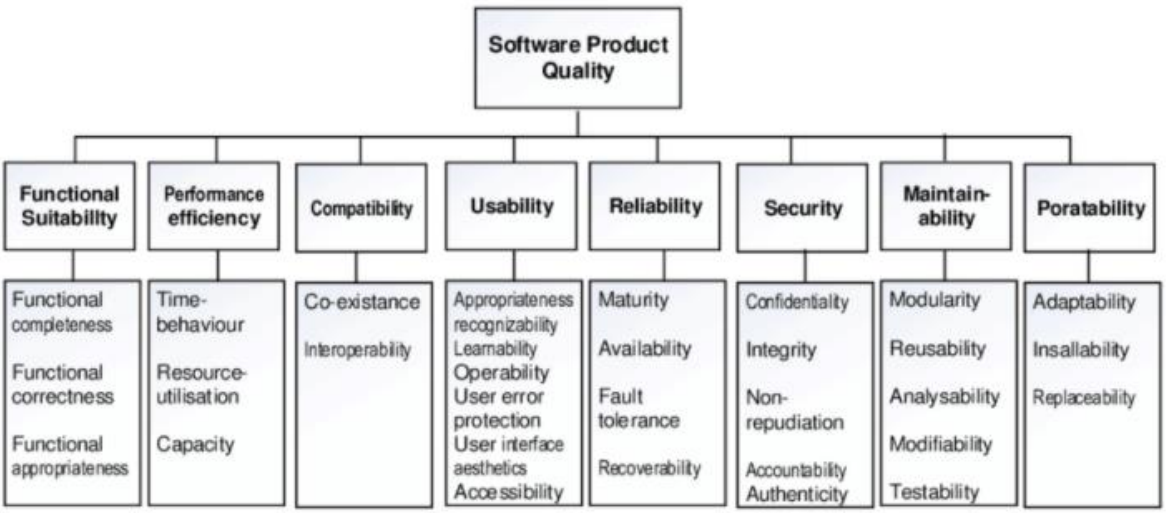
Figure 5—Levels and Necessary Ratings

Scale	Process Attributes	Rating
Level 1	Process Performance	Largely or fully
Level 2	Process Performance Performance Management Work Product Management	Fully Largely or fully Largely or fully
Level 3	Process Performance Performance Management Work Product Management Process Definition Process Deployment	Fully Fully Fully Largely or fully Largely or fully
Level 4	Process Performance Performance Management Work Product Management Process Definition Process Deployment Process Measurement Process Control	Fully Fully Fully Fully Fully Largely or fully Largely or fully
Level 5	Process Performance Performance Management Work Product Management Process Definition Process Deployment Process Measurement Process Control Process Innovation Process Optimization	Fully Fully Fully Fully Fully Fully Fully Largely or fully Largely or fully

Obrázek 4-2 Hodnoticí klíč pro určení úrovně schopnosti (Zdroj: (ISACA, 2013b))

4.5 Koncepce přenosu a implementace přenosového média

Pro uživatelskou komunitu mimo akademickou sféru byl vytvořen nástroj určený k sebehodnocení. Nástroj má tak usnadnit hodnocení bez hlubších znalostí metodik hodnocení. Pro jednoduchou reprezentaci následných výsledků pomocí grafů a snadný sběr testových odpovědí bylo rozhodnuto, že nástroj bude vytvořen pomocí programu Microsoft Excel. Pro zajištění kvalitního nástroje pro sebehodnocení úrovní schopnosti a zralosti SOC, byl použit model kvality SQuaRE. Jedná se o ucelenou soustavu norem řady ISO/IEC 250xx, která se zaobírá kvalitou softwarových produktů. Nástroj byl ověřován na základě osmi charakteristik vydefinovaných v ISO/IEC 25010:2011, které by měl softwarový produkt splňovat. Tyto požadavky znázorňuje Obrázek 4-3.



Obrázek 4-3 Požadavky kvality na softwarové produkty (Zdroj: (ISO/IEC 25010:2011))

- **Funkční přiměřenost** — Navržený nástroj musí obsahovat funkce, které zabezpečí předpokládané nebo stanovené potřeby uživatelů při používání systému za stanovených podmínek. Cílem nástroje bylo umožnit jednoduché měření úrovně schopnosti a zralosti. Toho je docíleno po vyplnění testových otázek. Výsledky jsou reprezentovány pomocí grafických znázornění, která zobrazují jak dosažené úrovně, tak i maximálně možnou úroveň, které lze pro danou doménu a subdoménu dosáhnout. Přesnost a správnost výsledků je zajištěna díky využití ověřených postupů vycházejících z rámce COBIT.
- **Výkonnost** — Nástroj musí poskytovat potřebný výkon vzhledem k množství použitých prostředků. Výkonnost je dána samotnou aplikací Microsoft Excel. Nástroj byl několikrát odzkoušen na různých prostředí a nebyly nalezeny žádné výkonnostní problémy.
- **Kompatibilita** — Určuje, jakým způsobem si může produkt vyměňovat informace s jinými produkty či systémy. Kompatibilita nástroje je dána verzí Microsoft Excel. Při testování bylo zjištěno, že některé komponenty se načítají pouze v nové verzi pro Microsoft Office 365. Na určení úrovní schopnosti a zralosti však tyto komponenty nemají vliv. Co se týče logické kompatibility, tak navržený CMM staví na COBIT 2019, a zároveň je v souladu s rámcem NIST CSF.
- **Použitelnost** — Nástroj byl navržen s ohledem na snadné použití. Pro zajištění jednoduché obsluhy nástroj obsahuje sekci návod, jak nástroj používat. Při ověřování v praxi nebyly zaznamenány od respondentů žádné výtky ke složitosti nástroje či problematičnosti užívání. Nástroj se jevil jasně popsaný, jednoduchý a přehledný.
- **Spolehlivost** — Nástroj by měl být odolný vůči chybám tím, že došlo k omezení vkládání nahodilých vstupů. Uživateli jsou povoleny jen nezbytné předdefinované funkce. Pokud by došlo k jakýmkoliv problémům, Microsoft Excel umožňuje obnovení dat.
- **Bezpečnost** — Uživatel má povoleny jen nezbytné funkce pro vyplnění dotazníku. Ostatní funkce jsou kvůli bezpečnosti uzamčeny. Dojde-li k jakékoliv modifikaci v nástroji, je tato aktivita zaznamenána.
- **Udržitelnost** — Tato charakteristika představuje míru účinnosti a efektivity, s jakou lze produkt nebo systém upravit, aby se zlepšil, opravil nebo přizpůsobil změnám prostředí a požadavků. Jelikož aktivity SOC spadají mezi rychle se měnící odvětví, lze předpokládat, že časem bude třeba nějaké aktivity upravit nebo přidat. Nástroj byl navržen tak, aby integrace nových SOC aktivit do nástroje byla co možná nejsnadnější.
- **Přenositelnost** — Jelikož je nástroj vybudován v Microsoft Excel, který je základním vybavením všech počítačů, nebo alespoň obsahují alternativní programy, které podporují soubory typu .xlsx, není přenositelnost velkým problémem. Avšak při testování v praxi bylo odhaleno, že některé funkce nástroje jsou kompatibilní pouze s verzí Microsoft Office 365. Jedná se o jednu z funkcí, kdy sám nástroj dokáže identifikovat aktivity, které dokážou SOC posunout o úroveň schopnosti/ zralosti výše. Pro plnou podporu nástroje je třeba modifikovat nástroj a využít syntaxi podporovanou i nižšími verzemi Microsoft Excel.

Pro detailnější specifikaci hodnocení pomocí SQuaRE požadavků byla vytvořena tabulka, která je přiložena níže v příloze (viz Příloha C: Požadavky na kvalitní software dle SQuaRE).

4.5.1 Popis hodnoticího nástroje

Nástroj se skládá ze čtyř hlavních sekcí, kterými jsou Návod, Testové otázky, Výsledky testu a Interpretace výsledků.

- **Návod** — První sekce seznamuje uživatele, jak hodnoticí nástroj ovládat. Obsahuje postupy pro vyplnění jednotlivých testovacích otázek napříč všemi doménami. Uživatel zde najde informace ohledně dalších dvou sekcí, kterými jsou Výsledky testu a Interpretace výsledků.
- **Testové otázky** — Jedná se o stěžejní sekci nástroje. Zde se nachází testové otázky všech devíti domén. Pro úspěšné měření úrovní schopnosti a zralosti je nezbytné vyplnit všechny uvedené otázky.
- **Výsledky testu** — Tato sekce se dělí na dvě části. První z nich Úrovně schopnosti hodnotí jednotlivé procesy v rámci dané domény. Pokud uživatel zcela vyplnil sekci Testové otázky, měl by dostat celkem 33 naměřených úrovní schopnosti pro 33 procesů. Ke každému procesu jsou následně sepsány aktivity, které je třeba splnit, aby se dosáhlo vyšší úrovně schopnosti. Druhou částí je Úrovně zralosti, která hodnotí úrovně zralosti jednotlivých domén. Pokud uživatel zcela vyplnil sekci Testové otázky, měl by dostat celkem 9 naměřených úrovní zralosti pro 9 domén. I zde nástroj vypisuje procesy, které je třeba zlepšit, aby bylo dosaženo vyšší úrovně zralosti dané domény.
- **Interpretace výsledků** — Poslední sekce nástroje poskytuje uživateli informace o tom, jak správně interpretovat jednotlivé naměřené úrovně schopnosti a zralosti.

Grafické znázornění hodnoticího nástroje je zachyceno v příloze této práce (viz Příloha D: Grafická prezentace hodnoticího nástroje).

4.6 Hodnocení

Vytvořený CMM a nástroj byly na závěr otestovány v praxi. Pro tento účel byl vybrán SOC tým jedné české společnosti. Nástroj byl distribuován celkem sedmi zaměstnancům SOC a ti měli za úkol na základě svých specializací vyplnit dotazníkové šetření. Výsledky měření a doporučení pro další rozvoj jednotlivých SOC aktivit je shrnuto v samostatném dokumentu vysledky_mereni.pdf.

Po skončení procesu hodnocení, byly dotazované osoby požádány o zpětnou vazbu ohledně zhodnocení kvality CMM a nástroje, s kterými se setkaly. Při hodnocení klasifikačního modelu CMM se shodly, že výsledné úrovně odpovídají reálné situaci v týmu. Nástroj hodnotily jako uživatelsky přívětivý s lehkým ovládáním. Při zpětné vazbě byl identifikován jeden závažnější problém, kdy osoby používající nižší verzi než Microsoft Office 365 nebyly schopny zobrazit soupis aktivit, které je třeba splnit pro zlepšení úrovně schopnosti a zralosti. Dále byly odhaleny drobné chyby v logických propočtech, které byly následně opraveny. Kromě

logických chyb uživatelé identifikovali i gramatické chyby. I na nich bylo zapracováno a došlo k jejich opravě.

Závěr

Informační a kybernetická bezpečnost je v posledních letech ve veřejném i soukromém sektoru silně diskutovaným tématem. Zvyšující se kyberkriminalita nutí organizace, aby se začaly starat o bezpečnost svých i klientských dat. Zajištění operativní bezpečnosti v mnoha společnostech mají na starost týmy SOC. Jelikož se týmy SOC v posledních letech teprve do společností zavádí, nejsou v praxi dostatečné zkušenosti, jak by takový SOC měl fungovat a jak zjistit, zda SOC vykonává kvalitní práci. Cílem práce bylo vytvořit model pro hodnocení úrovně schopnosti a zralosti (CMM).

Problém chybějících metod pro hodnocení efektivity SOC byl řešen pomocí metodik Design Science Research. Konkrétně byl použit Beckerův model, jak vytvářet modely pro hodnocení zralosti. Ten zahrnuje sedm kroků od vydefinování problému, přes průzkum stávající situace, tvorby modelu, až po samotné otestování modelu. Na základě odborné literatury byly vydefinovány aktivity, kterým by se měl SOC tým věnovat. Pro zajištění profesionality a exaktnosti byly tyto aktivity sladěny s NIST Cybersecurity Frameworkem, který je v praxi uznávaným rámcem pro informační kybernetickou bezpečnost. Následně tyto aktivity byly namapovány na COBIT 2019. Ten měl zajistit snadné škálování aktivit do jednotlivých úrovní schopnosti a zralosti. Pro zajištění použitelnosti v praxi prošel CMM během iterativního vývoje vícero úpravami. Konečný hodnoticí model obsahuje 8 domén (hlavní aktivity SOC), 33 subdomén a 309 aktivit.

Aby byl model co možná nejsnadněji využitelný v praxi, byl navržen nástroj, který na základě vyplnění dotazníkového šetření dokáže změřit úrovně schopnosti a zralosti SOC a zároveň dokáže identifikovat příležitosti, jak jednotlivé SOC aktivity posunout na vyšší úroveň. Nástroj byl vytvořen, testován a upravován na základě normy ISO/IEC 25010:2011, která definuje sadu požadavků pro dodávku kvalitního softwarového produktu.

Na úplný závěr byl nástroj otestován v praxi. Bylo osloveno sedm zaměstnanců jednoho českého SOC týmu, kteří měli zkusit provést sebehodnocení svých denních pracovních aktivit za pomocí hodnoticího nástroje. Následně proběhla schůzka se SOC manažerem, na které se blíže zhodnotily výsledky testování a použitelnost nástroje. Dle vyjádření SOC manažera, naměřené výsledky odpovídají reálným nedostatkům, kterých si je vědom a již se zavádí nápravná opatření. Kvůli citlivosti informací jsou tyto výsledky k dispozici ve speciálním dokumentu vysledky_mereni.pdf.

Po tomto testování proběhl rozhovor i s jednotlivými lidmi ze SOC s žádostí o zpětnou vazbu k testovému nástroji. Ti nástroj shledali jako lehce ovladatelný a srozumitelný. Měli jisté výhrady spíše ke kompatibilitě a chybám, které však neznemožňovaly správné fungování nástroje. Všechny jejich podněty byly zapracovány a opraveny.

Výsledkem práce je snadno použitelný nástroj pro hodnocení aktivit SOC, který dokáže měřit úrovně schopnosti a zralosti SOC a dokáže identifikovat příležitosti pro další rozvoj.

Použitá literatura

ANTON CHUVAKIN, 2013. Named: Endpoint Threat Detection & Response. *Gartner Blog Network* [online]. [vid. 2020-10-01]. Dostupné z: https://blogs.gartner.com/anton-chuvakin/2013/07/26/named-endpoint-threat-detection-response/

BECKER, Jörg, Ralf KNACKSTEDT a Jens PÖPPELBUSS, 2009. Developing Maturity Models for IT Management: A Procedure Model and its Application. *Business & Information Systems Engineering* [online]. **1**(3), 213–222. ISSN 1867-0202. Dostupné z: doi:10.1007/s12599-009-0044-5

BLACKSTRATUS ©, 2019. IT Compliance | IT Security Regulations & Compliance Management. *BlackStratus* [online] [vid. 2020-02-23]. Dostupné z: https://www.blackstratus.com/compliance/

CARSON ZIMMERMAN, 2014. *Ten Strategies of a World-Class Cybersecurity Operations Center*. B.m.: The MITRE Corporation. ISBN 978-0-692-24310-7.

CATHEY, Darren, 2019. Security Operations Maturity Model. In: *ISSA Central Maryland Chapter - Monthly Meeting October 16, 2019* [online]. The National Electronics Museum, Linthicum, Maryland, USA. Dostupné z: https://issa-centralmd.org/wp-content/uploads/LogRhythm-ISSA-SOMM-Presentation-101619.pdf

CMMI PRODUCT TEAM, 2010a. CMMI for Acquisition, Version 1.3 [online]. 3507391 Bytes. Dostupné z: doi:10.1184/R1/6572306.V1

CMMI PRODUCT TEAM, 2010b. CMMI for Development, Version 1.3 [online]. 4037844 Bytes. Dostupné z: doi:10.1184/R1/6572342.V1

CMMI PRODUCT TEAM, 2010c. CMMI for Services, Version 1.3 [online]. 4315959 Bytes. Dostupné z: doi:10.1184/R1/6572375.V1

COMMITTEE ON NATIONAL SECURITY SYSTEMS, 2015. *CNSSI 4009 Committee on National Security Systems (CNSS) Glossary* [online] [vid. 2020-09-29]. Dostupné z: https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Resources-Tools-and-Publications/Resources-and-Tools-Files/CNSSI-4009-Committee-on-National-Security-Systems-CNSS-Glossary

ČERMÁK, Miroslav, 2010. COBIT tajemství zbavený. *CleverAndSmart Management Consulting* [online]. [vid. 2020-11-20]. ISSN 2694-9830. Dostupné z: https://www.cleverandsmart.cz/cobit-tajemstvi-zbaveny/

DOUCEK, Petr, 2011. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. Praha: Professional Publishing. ISBN 978-80-7431-050-8.

ERNST & YOUNG, 2019. *EY Global Information Security Survey 2018–19*.

GARTNER INC., 2020. Security Information And Event Management (siem). *Gartner* [online] [vid. 2020-02-09]. Dostupné z: https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

HANACEK, Natasha, 2017. Cybersecurity Framework. *NIST* [online] [vid. 2020-11-24]. Dostupné z: https://www.nist.gov/industry-impacts/cybersecurity-framework

HEVNER, Alan R., Salvatore T. MARCH, Jinsoo PARK a Sudha RAM, 2004. Design Science in Information Systems Research. *MIS Quarterly* [online]. **28**(1), 75–105. ISSN 02767783. Dostupné z: doi:10.2307/25148625

CHRISSIS, Mary Beth, Mike KONRAD a Sandy SHRUM, 2011. *CMMI for development: guidelines for process integration and product improvement*. 3rd ed. Upper Saddle River, NJ: Addison-Wesley. SEI series in software engineering. ISBN 978-0-321-71150-2.

IBM CORPORATION, 2020. *Cost of a Data Breach Report 2020* [online] [vid. 2020-10-14]. Dostupné z: https://www.ibm.com/security/digital-assets/cost-data-breach-report/

ISACA, ed., 2012. *COBIT 5: a business framework for the governance and management of enterprise IT: an ISACA® framework*. Rolling Meadows, IL 60008 USA: ISACA. ISBN 978-1-60420-237-3.

ISACA, 2013a. *COBIT Process Assessment Model (PAM): Using COBIT® 5*. Rolling Meadows, IL 60008 USA: ISACA. ISBN 978-1-60420-271-7.

ISACA, 2013b. *Self-assessment Guide: Using COBIT® 5*. Rolling Meadows, IL 60008 USA: ISACA. ISBN 978-1-60420-266-3.

ISACA, ed., 2014. *COBIT 5 Principles: Where Did They Come From?* [online]. Rolling Meadows, IL 60008 USA: ISACA. Dostupné z: https://www.isaca.org/

ISACA, ed., 2018a. *COBIT® 2019 Framework: Governance and Management Objectives*. Schaumburg, IL: ISACA. ISBN 978-1-60420-764-4.

ISACA, ed., 2018b. *COBIT® 2019 Framework: Introduction and Methodology*. Schaumburg, IL: ISACA. ISBN 978-1-60420-763-7.

ISACA, 2019. Implementing the NIST Cybersecurity Framework Using COBIT 19. *ISACA* [online] [vid. 2020-11-28]. Dostupné z: https://www.isaca.org/bookstore/bookstore-cobit_19-digital/wcb19nist

ISO, 2020. ISO - 35.030 - IT Security. *Standards catalogue ICS 35.030* [online] [vid. 2020-11-27]. Dostupné z: https://www.iso.org/ics/35.030/x/p/1/u/0/w/0/d/0

ISO/IEC 25010, 2011. *ISO/IEC 25010:2011 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models*. 2011.

ISO/IEC 27002, 2013. *ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls*. 2013.

KAHONGE, Andrew Mwaura, William OKELLO-ODONGO, Evans K. MIRITI a Elisha ABADE, 2013. Web Security and Log Management: An Application Centric Perspective. *Journal of Information Security* [online]. **04**(03), 138–143. ISSN 2153-1234, 2153-1242. Dostupné z: doi:10.4236/jis.2013.43016

KENT, K a M P SOUPPAYA, 2006. *Guide to computer security log management* [online]. NIST SP 800-92. Gaithersburg, MD: National Institute of Standards and Technology [vid. 2020-02-14]. Dostupné z: doi:10.6028/NIST.SP.800-92

KEVIN ROEBUCK, 2012. *ISO/IEC 15504 (SPICE): High-impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors*. [online]. Dayboro: Emereo Pub. [vid. 2020-10-11]. ISBN 978-1-74333-358-7. Dostupné z: http://public.ebookcentral.proquest.com/choice/publicfullrecord.aspx?p=1063036

KULPA, Margaret K a Kent A JOHNSON, 2003. *Interpreting the CMMI: a process improvement approach* [online]. Boca Raton, Fla.: Auerbach/CRC Press [vid. 2020-12-06]. ISBN 978-0-203-50461-1. Dostupné z: http://www.books24x7.com/marc.asp?isbn=0849316545

LAHRMANN, Gerrit, Frederik MARX, Tobias METTLER, Robert WINTER a Felix WORTMANN, 2011. Inductive Design of Maturity Models: Applying the Rasch Algorithm for Design Science Research. In: Hemant JAIN, Atish P. SINHA a Padmal VITHARANA, ed. *Service-Oriented Perspectives in Design Science Research* [online]. Berlin, Heidelberg: Springer Berlin Heidelberg, Lecture Notes in Computer Science, s. 176–191 [vid. 2020-11-27]. ISBN 978-3-642-20632-0. Dostupné z: doi:10.1007/978-3-642-20633-7_13

MILLER, David, 2011. *Security information and event management (SIEM) implementation*. New York: McGraw-Hill. ISBN 978-0-07-170109-9.

NATHANS, David, 2014. *Designing and Building Security Operations Center* [online]. Rockland, MA, UNITED STATES: Elsevier Science & Technology Books [vid. 2019-09-21]. ISBN 978-0-12-801096-9. Dostupné z: http://ebookcentral.proquest.com/lib/vsep/detail.action?docID=1834659

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2018. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* [online]. NIST Cybersecurity White Paper. Gaithersburg, MD: National Institute of Standards and Technology [vid. 2019-09-21]. Dostupné z: doi:10.6028/NIST.CSWP.04162018

PAUL RUBENS, 2019. *Vulnerability Scanning: What It Is and How to Do It Right* [online] [vid. 2020-09-30]. Dostupné z: https://www.esecurityplanet.com/network-security/vulnerability-scanning.html

PETERSEN, Chris, Andrew HOLLISTER a James CARDER, 2019. *Security Operations Maturity Model A practical guide to assessing and improving the maturity of your security operations through Threat Lifecycle Management* [online]. Dostupné z: https://logrhythm.com/uk-security-operations-maturity-model-white-paper/

RISK ANALYSIS CONSULTANTS, 2020. *Řada norem ISO/IEC 27000* [online] [vid. 2020-11-26]. Dostupné z: https://www.iso27000.cz/rac/homepage.nsf/CZ/ISO27000

ROB VAN OS, 2016. *SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers* [online]. B.m. Master Thesis. Luleå University of Technology Department of Computer Science, Electrical and Space Engineering. Dostupné z: http://www.soc-cmm.com/

ŘÍHOVÁ, Zora a Vlasta SVATÁ, 2019. IT Governance a změny v řízení IT organizací. *IT Systems* [online]. **2019**(4) [vid. 2020-11-21]. Dostupné z: https://www.systemonline.cz/sprava-it/it-governance-a-zmeny-v-rizeni-it-organizaci.htm

SAMTANI, Sagar, Maggie ABATE, Victor BENJAMIN a Weifeng LI, 2019. Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective. In: [online]. s. 1–20. ISBN 978-3-319-90307-1. Dostupné z: doi:10.1007/978-3-319-90307-1_8-1

SCAMPI UPGRADE TEAM, 2011. Appraisal Requirements for CMMI® Version 1.3 (ARC, V1.3) [online]. [vid. 2020-10-11]. Dostupné z: doi:10.1184/R1/6571994.v1

SIEMPLIFY, 2017. Understanding The SOC Team Roles And Responsibilities. *Siemplify* [online] [vid. 2020-02-05]. Dostupné z: https://www.siemplify.co/blog/understanding-the-soc-team-roles-and-responsibilities/

STEINBERG, Randy, AXELOS LIMITED, STATIONERY OFFICE a GROSSBRITANNIEN, ed., 2013. *ITIL: IT service management practices. 4: Service operation*. 2011 edition, 2. impr. London: TSO, The Stationery Office. AXELOS - global best practice. ISBN 978-0-11-331307-5.

SUNDARAMURTHY, Sathya Chandran, Jacob CASE, Tony TRUONG, Loai ZOMLOT a Marcel HOFFMANN, 2014. A Tale of Three Security Operation Centers. In: *the 2014 ACM Workshop*: *Proceedings of the 2014 ACM Workshop on Security Information Workers - SIW '14* [online]. Scottsdale, Arizona, USA: ACM Press, s. 43–50 [vid. 2019-09-21]. ISBN 978-1-4503-3152-4. Dostupné z: doi:10.1145/2663887.2663904

SVATÁ, Vlasta, 2012. *Audit informačního systému*. Praha: Professional Publishing. ISBN 978-80-7431-106-2.

THE WHITE HOUSE - OFFICE OF THE PRESS SECRETARY, 2013. *Executive Order 13636: Improving Critical Infrastructure Cybersecurity* [online]. 12. únor 2013. Dostupné z: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

VERVE INDUSTRIAL, 2019. What is the NIST Cybersecurity Framework? *Verve* [online]. [vid. 2020-11-24]. Dostupné z: https://verveindustrial.com/resources/blog/what-is-the-nist-cybersecurity-framework/

WEST-BROWN, Moira, Don STIKVOORT, KLAUS-PETER KOSSAKOWSKI, Georgia KILLCRECE, Robin M. RUEFLE a Mark T. ZAJICEK, 2003. Handbook for Computer Security Incident Response Teams (CSIRTs) [online]. 1673727 Bytes. Dostupné z: doi:10.1184/R1/6574055.V1

ZÁKON Č. 181/2014 SB., 2020. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). *Zákony pro lidi* [online] [vid. 2020-09-28]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

Přílohy

Příloha A: Mapování aktivit SOC na NIST CSF

Vzniklá doména	NIST CSF	Ten Strategies of a World-Class Cybersecurity Operations Center	Designing and Building Security Operations Center
Vulnerability Management	• Zranitelnosti zařízení jsou identifikovány a dokumentovány • Hrozby, zranitelnosti, pravděpodobnosti a dopady jsou použity pro určení rizika • Je vyvinut a implementován plán na řízení zranitelností • Provádí se skenování zranitelností • Jsou stanoveny procesy pro příjem, analýzu a reakci na zranitelnosti odhalené z interních a externích zdrojů • Nově identifikované zranitelnosti jsou mitigovány (mírněny) nebo zdokumentovány jako přijatá (accepted) rizika	• Network mapping • Vulnerability scanning • Vulnerability assessment • Penetration testing	• Network mapping • Threat and vulnerability management • Host hardening/configuration monitoring • Patch management • Penetration testing

Monitoring	• Síť je monitorována, aby detekovala potenciální kybernetických bezpečnostních událostí • Aktivity zaměstnanců jsou monitorovány za účelem detekce potenciálních kybernetických bezpečnostních událostí • Detekce škodlivého kódu • Detekce škodlivého mobilního kódu • Sleduje se aktivita externího poskytovatele služeb, aby se detekovaly potenciální kybernetických bezpečnostních události • Je prováděno monitorování neoprávněného personálu, připojení, zařízení a softwaru • Fyzické prostředí je monitorováno za účelem detekce potenciálních kybernetických bezpečnostních událostí	• Real-time monitoring and triage • Audit data collection and distribution • Audit content creation and management	• Wireless monitoring/management • Behavioural monitoring • Web application malware monitoring • Mobile device management/ monitoring • Database monitoring • Unauthorized scanning • Device monitoring and management • Real-time monitoring • Surveilance • File integrity monitoring • Host intrusion monitoring • Host hardening/configuration monitoring • Log management • Audit data distribution • Content creation, management and auditing • Fraud detection • Internet misuse • Phishing detection
Post-incident Activities	• Plány zvládání a obnovu (incident response, continuity plan, incident recovery, disaster recovery) jsou zavedeny a spravovány	• Countermeasure implementation	• Disaster recovery • Business continuity

	• Plány pro zvládání a obnovu jsou testovány • Response plan je vykonáván během nebo po incidentu • Response plány zahrnují lessons learned • Plány obnovy jsou vykonávány během nebo po bezpečnostním kybernetickém incidentu • Do plánů obnovy jsou implementovány lessons learned • Recovery strategie jsou aktualizovány • Recovery strategie jsou aktualizovány • Recovery aktivity jsou komunikovány interním, externím stakeholderům a managementu		
Build Cyber & Threat Intelligence	• Informace o kybernetických hrozbách jsou přijímány z fór a zdrojů pro sdílení informací • Hrozby interní i externí jsou identifikovány a dokumentovány • Zjištěné události jsou analyzovány za účelem pochopení cílů a metod útoku • Data událostí jsou shromažďována a korelována z více zdrojů a senzorů • Dobrovolné sdílení informací s externími stakeholdery za účelem dosažení širšího situačního povědomí o kybernetické bezpečnosti • Jsou stanoveny procesy pro příjem, analýzu a reakci na zranitelnosti	• Cyber intelligence collection and analysis • Cyber intelligence creation • Cyber intelligence distribution • Cyber intelligence collection and analysis • Trending • Threat assessment	• Intelligence collection and analysis • Binary whitelisting • Application whitelisting • Emerging threat research • Risk evaluation

	odhalené z interních a externích zdrojů • Dopad incidentu je chápán		
Analysis	• Zjištěné události jsou analyzovány za účelem pochopení cílů a metod útoku • Data událostí jsou shromažďována a korelována z více zdrojů a senzorů • Notifikace z detekčních systémů jsou investigovány • Forenzní analýza je prováděna • Jsou stanoveny procesy pro příjem, analýzu a reakci na zranitelnosti odhalené z interních a externích zdrojů	• Incident analysis • Tradecraft analysis • Forensic artifact handling • Malware and implant analysis • Forensic artifact analysis	• Incident analysis, coordination, and response • Tradecraft analysis • Forensic artifact collection • Rogue device detection • Rogue wireless device detection • Ediscovery • Malware analysis, reverse engineering • File whitelist management • Malware impact analysis • Unknown binary analysis • Netflow analysis
Identity & Access Management	• Response plány (incident response, continuity plan) a plány obnovy (incident recovery, disaster recovery) jsou zavedeny a spravovány • Identity a pověření jsou vydána, řízena, ověřována, obnovována a auditována pro autorizovaná zařízení, uživatele a procesy • Fyzický přístup k aktivům je řízen a chráněn • Odebrání přístupů je řízeno		• Endpoint identity • Authentication management • User administration/identity management

	• Přístupová oprávnění a autorizace jsou řízeny, zahrnuje principy nejmenších potřebných privilegií • Integrita sítě je chráněna (segregace sítě, síťová segmentace) • Identity jsou prokazovány a vázány na pověření a uplatňovány v interakcích • Uživatelé, zařízení, a další aktiva jsou autentifikována (jednofaktorově, vícefaktorově) přiměřeně dle rizika transakce		
Tooling	• Zdroje (hw, sw, zařízení, data, čas, lidi) mám priority na základě klasifikace, kritičnosti a obchodní hodnoty • Účelnost ochranných technologií je sdílena • Data událostí jsou shromažďována a korelována z více zdrojů a senzorů • Trashholds pro upozornění na incidenty jsou stanoveny • Trashholds pro upozornění na incidenty jsou stanoveny • Detekční aktivity splňují všechny příslušné požadavky • Detekční procesy jsou testovány • Komunikují se informace o detekovaných událostech • Detekční procesy se neustále zlepšují	• Border protection device operation and maintenance • Soc infrastructure operation and maintenance • Sensor tuning and maintenance • Custom signature creation • Tool engineering and deployment • Tool research and development	• Web proxy policy management • Scripting and automation • Security device tuning • Signature creation • Rule creation • Security tool engineering and development

Incident Response	• Response plan je vykonáván během nebo po incidentu • Koordinace se zúčastněnými stranami probíhá v souladu s response plány • Incidenty jsou kategorizovány v souladu s response plány • Jsou stanoveny procesy pro příjem, analýzu a reakci na zranitelnosti odhalené z interních a externích zdrojů • Incidenty jsou omezovány • Incidenty jsou mírněny • Response plány zahrnují lessons learned • Response strategie je aktualizována • Dopad incidentu je chápán • Zaměstnanci znají svou roli a pořadí operací, které jsou nutné při reakci	• Incident analysis • Tradecraft analysis • Incident response coordination • On-site incident response • Remote incident response	• Risk evaluation • Incident analysis, coordination, and response • Tradecraft analysis • Ddos mitigation • Emergency announcements and communications • Remote incident response

Příloha B: Architektura CMM

oblast hodnocení	úroveň zralosti	otázka	zdroj	Typ
Vulnerability Management	1	SOC se zabývá identifikací zranitelností.	-	Identifikace, detekce a klasifikace
	2	Metoda pro sběr, klasifikaci a analýzu zranitelností je zavedena a udržována.	APO12.01	
	2	Nástroje na detekci zranitelností jsou implementovány.	DSS05.01	
	2	Identifikovat a hlásit zranitelnosti může kdokoli v podniku.	EDM03.02	
	3	Informace o rizikovosti jednotlivých zranitelností jsou pravidelně aktualizovány.	APO12.03	
	3	Existuje taxonomie (klasifikace, kategorizace) zranitelností, která napomáhá definovat rizikové scénáře a kategorizovat dopad a pravděpodobnost zneužití zranitelnosti.	APO12.01	
	3	Zranitelnosti jsou evidovány podle kategorií dopadů definovaných v taxonomii zranitelností.	APO12.01	
	4	Informace o nových zranitelnostech na systémech jsou pravidelně kontrolovány a vyhodnocovány, zda nedošlo ke změnám klasifikace, rizika, či samotného výskytu.	DSS05.01	
	4	U podobných kategorií zranitelností (dle taxonomie) jsou hledány společné přispívající faktory. Tyto rizikové faktory jsou pravidelně analyzovány za účelem identifikace nových rizik.	APO12.01	
	4	Na základě rizikového profilu zranitelnosti jsou definovány sady indikátorů, které umožňují rychlou identifikaci a sledování aktuálních zranitelností a jejich trendy.	APO12.03	
	4	Informace o detekovaných zranitelnostech jsou přezkoumávány vůči informacím získaných z externích zdrojů (reporty, trendy, business partneři, dodavatelé, nezávislé organizace). Zkoumá se, zda byla zranitelnost zneužita, jaká je pravděpodobnost zneužití, náklady spojené s neužitím a možné dopady na podnikání.	APO12.01	
	4	Jsou identifikovány konkrétní podmínky, které by musely nastat, aby došlo ke zneužití zranitelnosti.	APO12.01	
	4	Do rizikového profilu zranitelnosti jsou zvažovány/zahrnovány výsledky objektivních hodnocení třetích stran a interních auditů a kontrol, kteří se ve svých závěrech vyjadřují k zajištění kvality Vulnerability Managementu a jednotlivým zranitelnostem. Na základě takového rizikového faktoru se plánují reakce na danou zranitelnost.	APO12.04	

Vulnerability Management	1	Detekované zranitelnosti jsou opravovány.	-	Patching a zvládání
	2	Plán pro opravu zranitelností je vypracován a prováděn.	BAI03.10	
	3	Distribuce patchů je prováděna centrálně pomocí centralizovaného Configuration&Change Managementu.	DSS05.01	
	3	Navrhované akce pro odstranění zranitelností jsou posuzovány na základě rizika, dopadu na uživatele a dostupnosti zdrojů pro odstranění zranitelnosti.	BAI03.10	
	3	V případě závažných (major) změn při zvládání zranitelností, je postupováno podle vývojového procesu používaného pro nové systémy. Pro updaty se používají procesy Change Managementu.	BAI03.10	
	4	Protiopatření pro zvládání zranitelností jsou před použitím kontrolována a ověřena, zda nedošlo ke zkreslení informací.	APO12.02	
	5	Při návrhu protiopatření pro zvládání zranitelností je zvážena analýza nákladů a přínosů potenciálních možností, jak reagovat na zranitelnost.	APO12.02	
	1	SOC se zabývá identifikací zranitelností.	-	Použití scénářů
	2	Jsou vytvářeny rizikové scénáře, které usnadňují rozpoznání a pochopení pravděpodobnosti a dopadu zranitelnosti.	DSS05.07	
	2	Aktuální rizikové scénáře jsou agregovány podle kategorie, obchodní linie a funkční oblasti.	APO12.03	
	3	Na základě scénářů je identifikována míra rizika zneužití zranitelnosti. Toto riziko je porovnáváno vůči risk apetitu podniku. Pro zranitelnosti, překračující tento risk apetit jsou navrhována protiopatření, jak riziko spojené se zranitelností dostat na akceptovatelnou toleranci danou risk apetitem.	APO12.02	
	1	SOC se zabývá identifikací zranitelností.	-	Strategie, procesy, postupy
	2	Existuje strategie řízení zranitelností, která je rozpracována do jednotlivých postupů řízení zranitelností.	EDM03.02	
	3	Existují plány, které dokumentují konkrétní kroky, které je třeba podniknout, když dojde ke zneužití zranitelnosti.	APO12.06	
	1	Lidé vykonávající procesy související s Vulnerability Managementem disponují potřebnými znalostmi pro výkon práce.	-	Znalosti personálu
	2	Management stanovil očekávání ohledně znalostí personálu pro vykonávání Vulnerability Managementu a užitečnost znalostí a potřeba sdílení znalostí ohledně zranitelností byly prokázány.	BAI08.03	

Vulnerability Management	2	Při nalezení zranitelnosti na aktivu, personál má možnost zjistit, jakou službu zranitelnost ovlivňuje, a s jakými dalšími aktivy kooperuje (aplikace, servery, databáze, služby, počítače, …).	APO12.03	Znalosti personálu
	2	Je určeno, které IT služby infrastruktury jsou nezbytné pro udržení provozu obchodních procesů (kritické služby).	APO12.03	
	2	Potenciální uživatelé znalostí byli identifikováni podle klasifikace jednotlivých znalostí (kdo jaké znalosti bude potřebovat).	BAI08.03	
	3	Personál Vulnerability Managementu získává znalosti na základě efektivního vzdělávacího systému (účelně a účinně). Bylo nastaveno prostředí, nástroje a artefakty, které podporují sdílení a přenos znalostí. Je zajištěno, že k daným znalostem mají přístup pouze pověření lidé.	BAI08.03	
	4	Personál používá nástroj pro zachycení/šíření/získávání znalostí. Nástroj umožňuje měřit využívání těchto informací (znalostí) a je na základě toho vyhodnocován dopad na procesy správy a řízení Vulnerability Managementu.	BAI08.03	
	5	Znalosti a informovanost personálu Vulnerability Managementu jsou neustále zlepšovány a rozšiřovány o nové poznatky a trendy.	BAI08.03	
	1	SOC se zabývá identifikací zranitelností.	-	Reporting
	2	Hlášení o zranitelnostech je předáváno příslušným osobám.	EDM03.02	
	2	Existují plány, jak reportovat a komunikovat aktivity Vulnerability Managementu napříč všemi úrovněmi podniku.	EDM03.02	
	2	Mechanismy pro reakci na zranitelnosti jsou implementovány. Tyto mechanismy zahrnují i podávání zpráv příslušným úrovním řízení, na základě dohodnutých zásad eskalace (co hlásit, kdy, kde a jak).	EDM03.02	
	4	Výsledky a metriky Vulnerability Managementu jsou reportovány všem dotčeným zúčastněným stranám v dohodnutých termínech a formátech.	APO12.04	
	4	Aktuální rizikový profil je reportován všem zúčastněným stranám. V reportu jsou zahrnuty informace o účinnosti procesů Vulnerability Managementu, identifikovaných mezerách, nesrovnalostech, stavu nápravy a jejich dopadech na rizikový profil.	APO12.04	
	4	Osobám s rozhodovací pravomocí jsou poskytovány informace k pochopení nejhorších a nejpravděpodobnějších scénářů, možných ztrát, právních a regulačních postihů a dalších negativních dopadů.	APO12.04	

Vulnerability Management	5	Příslušným osobám s rozhodovací pravomocí je reportována hlavní příčina zranitelnosti, další doporučení, jak reagovat na zranitelnosti a jak zefektivňovat procesy Vulnerability Managementu.	APO12.06	Reporting
	1	SOC se zabývá identifikací zranitelností.	-	Měření
	3	Jsou identifikovány klíčové cíle a metriky pro správu a řízení zranitelností (pro procesy Vulnerability Managementu), a jsou schváleny přístupy, metody, techniky a procesy pro sběr a vykazování informací o měření.	EDM03.02	
	4	Management určil výkonnostní cíle a jejich metriky týkající se toho, čeho se chce dosáhnout v oblasti Vulnerability Managementu. Metriky zahrnují měření jednotlivých aktivit a zda se daří dosahovat cílů. Měření zahrnuje jak finanční, tak i nefinanční ukazatele.	EDM02.04	
	4	Shromažďují se relevantní, včasná, úplná, důvěryhodná a přesná data, aby se mohl hlásit pokrok v dosahování hodnoty oproti cílům.	EDM02.04	
	4	Zprávy o výkonnosti procesů Vulnerability Managementu jsou pravidelně získávány. Prověřuje se pokrok vzhledem k dosahování cílů a v jaké míře byly cíle dosaženy.	EDM02.04	
	4	Provádí se pravidelná kontrola účinnosti Vulnerability Managementu pomocí penetračního testování či jiného testování zabezpečení systému.	DSS05.02	
	5	Po přezkoumání reportů, dochází k zahájení vhodných nápravných/zlepšujících opatření, které optimalizuje přidanou hodnotu Vulnerability Managementu.	EDM02.04	
Monitoring	1	Infrastruktura podniku je monitorována a logována.	-	Monitoring infrastruktury
	2	Dochází k logování událostí. Je určena úroveň informací, která má být zaznamenávána na základě zvážení rizika a výkonu.	DSS01.03	
	3	Infrastrukturní aktiva, která je třeba monitorovat, jsou identifikována a zaznamenána. Při výběru aktiv byla zvážena jejich kritičnost.	DSS01.03	
	3	Jsou definována a implementována pravidla, která identifikují a zaznamenávají porušení nastavených prahových hodnot (treshholdů) a porušení podmínek událostí. Aby logy nebyly přetíženy zbytečnými informacemi, dochází k objevování rovnováhy mezi generovanými rušivými vedlejšími událostmi a významnými událostmi. Loguje se jen to nezbytné.	DSS01.03	
	3	Při zjištění odchylek od definovaných prahových hodnot jsou včas vytvořeny upozornění na incidenty.	DSS01.03	
	3	Logy událostí jsou po určitou dobu uchovávány, aby pomohly při budoucím vyšetřování.	DSS01.03	

Monitoring	4	Jsou zavedeny postupy pro monitorování logů událostí. Tyto postupy jsou pravidelně revidovány.	DSS01.03	Monitoring infrastruktury
	1	V rámci podniku dochází k monitorování bezpečnostních událostí.	-	Bezpečnostní monitoring
	2	Jsou implementovány mechanismy filtrování sítě, jako jsou brány firewall a software pro detekci narušení.	DSS05.02	
	2	Sleduje se příchozí a odchozí provoz (traffic).	DSS05.02	
	2	Logy událostí jsou pravidelně procházeny a vyhodnocovány, zda neobsahují potenciální incident. Dojde-li k identifikaci možného incidentu, je včas vytvořen tiket incidentu a dojde k upozornění personálu.	DSS05.07	
	3	Z logů událostí jsou vytvářeny bezpečnostní logy událostí, které jsou zaznamenávány a archivovány po příslušnou dobu.	DSS05.01	
	3	Bezpečnostní události jsou zaznamenávány a tyto data jsou archivována po příslušnou dobu.	DSS05.07	
	3	Informace související s incidenty jsou také logovány.	DSS03.05	
	3	U privilegovaných uživatelských účtů jsou monitorovány veškeré aktivity.	DSS05.04	
	4	Na základě citlivosti a regulatorních požadavků je přístup k informacím auditován (evidován a ukládán).	DSS05.04	
Poincidentní aktivity	1	Firma má zavedeny procesy typu Problem Management.	-	Převedení incidentu do problému
	2	Pokud související problém nebo známá chyba související s incidentem ještě neexistuje a pokud incident splňuje dohodnutá kritéria pro registraci problému, vytvoří se nový problém.	DSS02.04	
	2	Záznamy problémů jsou uzavírány buď po potvrzení úspěšného odstranění známé chyby, nebo po dohodě, jak alternativně problém řešit.	DSS03.04	
	2	Servisní středisko IT (Service Desk) je informováno o harmonogramu pro uzavření problému (např. Harmonogram opravy známých chyb, možné řešení nebo skutečnost, že problém přetrvává, dokud nebude implementována změna) a o důsledcích zvoleného přístupu k řešení problému. Podle potřeby jsou informováni dotčení uživatelé.	DSS03.04	
	3	V průběhu celého procesu řešení problému jsou získávány pravidelné zprávy od IT Change Managementu (nebo jiné strany odpovědné za řešení problémů) o pokroku při řešení problémů a chyb.	DSS03.04	

	4	Pokračující dopad problémů a známých chyb na služby je monitorován.	DSS03.04	Převedení incidentu do problému
Poincidentní aktivity	4	Úspěšnost řešení hlavních (Major) problémů je přezkoumávána a potvrzována.	DSS03.04	
	5	Znalosti získané z kontroly úspěšně vyřešených problémů jsou začleňovány do podmínek služeb při revizi SLA nebo OLA s obchodním zákazníkem či v rámci společnosti.	DSS03.04	
	1	SOC je zapojen do plánů obnovy podnikání (Business Continuity Plan, Disaster Recovery Plan) po incidentu.	-	Obnova podnikových procesů
	2	Pokud je po incidentu potřeba, provádí se aktivity spojené s obnovou.	DSS02.05	
	2	Je stanoven minimální čas potřebný k obnovení obchodního procesu na základě přijatelné délky přerušení podnikání a maximálního tolerovatelného výpadku.	DSS04.02	
	2	Jsou známy podmínky a osoby s rozhodovací pravomocí, které aktivují procesy pro zachování kontinuity podnikání.	DSS04.02	
	2	Jsou vytvářeny scénáře, které pravděpodobně způsobí bezpečnostní události. Na jejich základě se pak tvoří odpovídající plány kontinuity.	DSS04.02	
	3	Požadavky na kontinuitu podnikání jsou analyzovány a jsou identifikovány možné strategické obchodní a technické možnosti.	DSS04.02	
	3	Jsou stanoveny požadavky na zdroje a náklady pro každou strategickou technickou možnost a na základě toho je vydáno strategické doporučení.	DSS04.02	
	3	Posuzuje se pravděpodobnost hrozeb, které by mohly způsobit ztrátu kontinuity podnikání a existují opatření, která sníží pravděpodobnost a dopad prostřednictvím lepší prevence a zvýšené odolnosti.	DSS04.02	
	1	SOC je zapojen do plánů obnovy podnikání (Business Continuity Plan, Disaster Recovery Plan) po incidentu.	-	Tvorba BCP a DRP
	1	Jsou vytvořeny plány pro zachování kontinuity podnikání (BCP - Business Continuity Plan) a plány na obnovu (DRP – Disaster Recovery Plan).	-	
	2	Jsou definovány podmínky pro BCP a DRP. Do plánů jsou zahrnuty aktualizace a rekonciliace informačních databází k zachování integrity informací.	DSS04.03	
	2	BCP a DRP jsou udržovány aktuální a obsahují postupy, které je třeba dodržovat, aby bylo možné pokračovat v provozu důležitých obchodních procesů nebo dočasných ujednání o zpracování.	DSS04.03	
	2	Do BCP a DRP jsou zahrnuty odkazy na plány externích poskytovatelů služeb.	DSS04.03	

	2	Jsou definovány a zdokumentovány zdroje potřebné k podpoře zachování kontinuity a obnovy po havárii s ohledem na lidi, zařízení a IT infrastrukturu.	DSS04.03	
Poincidentní aktivity	2	Požadavky na zálohování informací požadované pro podporu BCP a DRP jsou definovány a dokumentovány. Plány a papírové dokumenty i datové soubory jsou zahrnuty do BCP a DRP.	DSS04.03	Tvorba BCP a DRP
	2	Požadované dovednosti pro jednotlivce zapojené do provádění BCP a DRP jsou určeny.	DSS04.03	
	2	Provádí se analýza dopadu na podnikání. Tato analýza je zvážena při tvorbě BCP a DRP.	DSS04.02	
	3	BCP, DRP a k nim podpůrná dokumentace je dostatečně bezpečně distribuována oprávněným zúčastněným stranám. Plány a dokumentace jsou přístupné ve všech možných scénářích katastrof.	DSS04.03	
	3	Noví i stávající zaměstnanci jsou školeni, trénováni a informováni o změnách v BCP a DRP.	BAI05.07	
	4	Po obnově chodu podniku se provádí kontroly, zda byl v praxi dodržen dokumentovaný BCP a DRP. Pro účely měření jsou definovány jasné metriky.	DSS04.08	
	5	Po obnově dochází k revizi BCP a DRP a hledají se slabiny nebo opomenutí. Na základě toho se vydá doporučení pro zlepšení plánů a předává se odpovědným osobám s rozhodovací pravomocí k posouzení, zda je možné tato doporučení zahrnout do BCP a DRP.	DSS04.08	
	1	BCP a DRP jsou testovány.	-	Testování a cvičení BCP a DRP
	1	SOC je zapojen do plánů obnovy podnikání po incidentu.	-	
	2	Role a odpovědnosti za provádění cvičení BCP a DRP byly přiřazeny.	DSS04.04	
	2	K ověření úplnosti BCP a DRP jsou definovány cíle pro jejich provádění a testování.	DSS04.04	
	2	Došlo k definování a dohodnutí se na cvičeních zúčastněných stran, která jsou realistická, a ověřují postupy BCP a DRP. Byly zahrnuty role a odpovědnosti a opatření k uchovávání dat, které způsobí minimální narušení obchodních procesů.	DSS04.04	
	3	Cvičení a testování BCP a DRP probíhá přesně podle definovaných kroků uvedených v těchto plánech.	DSS04.04	
	4	Po testování BCP a DRP se provádí rozbor a analýza s cílem posoudit jejich úspěšnost.	DSS04.04	
	4	Metriky pro měření úspěchu byly vydefinovány a konzultovány s vlastníky podnikových procesů a týmem SOC.	BAI07.08	
	4	Po obnově chodu podniku se prošetřuje účinnost plánů z hlediska schopnosti kontinuity, rolí a odpovědností, kompetencí, odolnosti vůči incidentu, technické infrastruktury a organizačních struktur.	DSS04.08	

	4	Kontrola BCP a DRP probíhá podle potřeb s vlastníky obchodních procesů a dalšími zainteresovanými stranami.	BAI07.08	
Poincidentní aktivity	5	Na základě výsledků kontroly jsou vypracovávány doporučení pro zlepšení stávajících BCP a DRP.	DSS04.04	Testování a cvičení BCP a DRP
	5	Poznatky získané při kontrole BCP a DRP jsou zachyceny. Získané ponaučení je sdíleno se zainteresovanými stranami.	BAI05.07	
	5	Získané poznatky jsou implementovány do plánů zvládání incidentů a do plánů BCP s DRP.	BAI07.08	
Budování Cyber & Threat Intelligence	1	SOC disponuje vlastní CTI (Cyber & Threat Intelligence - báze znalostí pro SOC) a data využitá pro její tvorbu pochází z externích i interních zdrojů informací a znalostí.	-	Identifikace a klasifikace informací
	2	Pro budování CTI jsou od jejích uživatelů zjišťovány požadavky na potřebné znalosti a jsou hledány zdroje informací odkud lze tyto znalosti čerpat.	BAI08.01	
	2	Existují metody/postupy pro sběr, klasifikaci a analýzu informací, které pomáhají budovat interní CTI.	APO12.01	
	2	Z externího i interního prostředí jsou zaznamenávány relevantní data související s hrozbami, incidenty, monitoringem a dalšími prvky, které mohou podpořit účelnost a účinnost CTI.	APO12.01	
	3	Zdroje informací pro CTI jsou tříděny a klasifikovány podle zařazení aplikovatelnosti.	BAI08.01	
	4	Zdroje informací pro CTI jsou shromažďovány, porovnávány a ověřovány na základě kritérií pro ověřování informací (např. Srozumitelnost, relevance, důležitost, integrita, přesnost, konzistence, důvěryhodnost, spolehlivost).	BAI08.01	
	1	CTI obsahuje znalosti pro vykonávání činností pro různé SOC role.	-	Uspořádávání informací a vzájemné propojování dat
	2	Požadavky na znalosti od uživatelů CTI a tvůrců CTI jsou sladěny, aby získané znalosti z CTI byly účinné a účelné pro práci SOC.	APO14.08	
	3	Pro budování CTI se vytváří nové znalosti na základě získávání dat z více zdrojů, které jsou vzájemně propojovány.	BAI08.02	
	3	Vlastní i sdílená data v CTI jsou namapována do jednotlivých kroků procesů tak, aby osoba vykonávající daný proces vždy věděla, jaké znalosti/data potřebuje a kde je najde.	APO14.08	
	3	Procesy detekce, monitoringu, analýzy, řešení incidentů a další jsou mapovány na získaná data pro CTI. Dochází ke kontrolám, zda procesy a data jsou stále aktuální a vhodně navázaná. Dochází ke vzájemnému podporování, kdy na základě CTI se zlepšují jednotlivé procesy a naopak, při analýze procesů se zlepšuje obsah CTI.	APO14.08	

Budování Cyber & Threat Intelligence	3	Změny sdílených dat, které jsou zahrnuty do CTI, jsou prováděny ve spolupráci s relevantními zúčastněnými stranami (vlastníky dat, konzumentů dat, uživatelů, na které změna má dopad, …).	APO14.08	Uspořádávání informací a vzájemné propojování dat
	3	Existují různé pohledy na související datové sady s ohledem na požadavky uživatelů CTI a dalších zainteresovaných stran. (analytik, IR manažer, technik, architekt, manažer pro zvládání rizik, …).	BAI08.02	
	3	Pro nestrukturované znalosti, které nejsou k dispozici prostřednictvím formálních zdrojů (např. Odborné znalosti jednotlivců) existuje systém, jak takové znalosti sbírat, formalizovat je (převést do písemné/audio podoby) a dále je šířit zainteresovaným stranám.	BAI08.02	
	5	Informace a znalosti, které neodpovídají potřebám personálu jsou neustále zlepšovány a rozšiřovány.	BAI08.03	
	1	Tým SOC a další zainteresované osoby disponují nebo získávají potřebné znalosti pro výkon své práce.	-	Použití a šíření znalostí
	2	Očekávání managementu SOC ohledně znalostí personálu bylo stanoveno. Požadované znalosti jsou adekvátní na základě prokázané užitečnosti znalostí.	BAI08.03	
	2	Potenciální uživatelé znalostí byli identifikováni podle klasifikace jednotlivých znalostí (kdo jaké znalosti bude potřebovat).	BAI08.03	
	3	Uživatelé znalostí CTI získávají znalosti na základě efektivního vzdělávacího systému (účelné a účinné). Bylo nastaveno jednotné prostředí, nástroj a artefakty, které podporují sdílení a přenos znalostí. Je zajištěno, že k daným znalostem mají přístup pouze pověřené osoby.	BAI08.03	
	3	Sdílení informací z CTI se provádí na základě uzavřených dohod o spolupráci a sdílení dat v rámci obchodních a partnerských procesů v i mimo podnik.	APO14.08	
	4	CTI je sdílena se zainteresovanými stranami tak, aby se nevytvářely zbytečně duplicitní nebo nadbytečné informace či procesy.	APO14.08	
	1	Je implementován nástroj (aplikace) pro CTI.	-	Uchovávání dat (nástroj)
	2	Nástroj používaný pro CTI umožňuje správu historických dat a splňuje požadavky na uchování, zničení dat organizace.	APO14.09	
	2	Existuje metoda, jak mít přístup k historickým datům nezbytných pro podporu potřeb zainteresovaných stran (audit, management, IT, …).	APO14.09	

Budování Cyber & Threat Intelligence	2	Existují postupy a pravidla pro kontrolu přístupu, přenosu, úpravu historických a archivovaných dat v CTI.	APO14.09	Uchovávání dat (nástroj)
	3	SOC má předepsané datové úložiště, které poskytuje přístup k historickým datům pro splnění analytických potřeb a budování CTI.	APO14.09	
	3	CTI je zpřístupněna všem zainteresovaným stranám na základě rolí a přístupových oprávnění.	BAI08.02	
	4	Je měřeno používání CTI pro získávání/šíření znalostí (jak často jsou používány nástroje, kde je CTI uložena) a na základě toho je vyhodnocován dopad na kvalitu vykonávání procesů SOC.	BAI08.03	
Analýza	1	Analytici SOC provádí analýzu bezpečnostních událostí a incidentů.	-	Investigace, diagnostika
	2	Hlášení o bezpečnostních událostech jsou pravidelně kontrolována, zda neobsahují potenciální incidenty.	DSS05.07	
	2	Pro účely analýzy se využívá vícero podporovaných technologií, služeb a aktiv (např. Skenery zranitelností, fuzzery, sniffery, IDS, SIEM, analyzátory protokolů).	DSS05.07	
	2	Aby se zjistily nejpravděpodobnější možné příčiny incidentů, jsou při analýze identifikovány a popsány všechny relevantní symptomy. Tyto informace a jednotlivé kroky analýz jsou popsány v CTI (Cyber & Threat Intelligence – báze znalostí pro SOC).	DSS02.04	
	2	Pro analýzu bezpečnostních událostí se používají všechny možné zdroje znalostí/dat (včetně známých chyb a problémů).	DSS02.04	
	2	Pro získání hlubších odborných znalostí jsou k analýze a řešení incidentů přizvány i osoby mimo SOC.	DSS02.04	
	2	Pro zajištění hlubší analýzy různých artefaktů (sítě, databáze, aplikace, OS, …) jsou identifikovány skupiny podpory a kontakty na ně.	DSS03.01	
	3	Na základě analýzy incidentů dochází k hledání problémů či chyb v systému, které je třeba opravit/odstranit.	DSS03.02	
	3	Jsou připraveny, udržovány a testovány plány, které dokumentují konkrétní kroky analýz, které je třeba podniknout, když riziková událost způsobí významný incident se závažným dopadem na podnikání.	APO12.06	
	3	Během analýzy využívají analytici znalosti z CTI.	APO14.08	
	3	Pro šíření znalostí jsou postupy běžných analýz zaznamenávány do CTI. Již popsané analýzy jsou pravidelně revidovány kvůli aktuálnosti dat.	APO14.08	

Analýza	4	Incidenty jsou analyzovány podle kategorie a typu. Jsou stanoveny trendy a identifikovány vzorce opakujících se incidentů, problémů a poruch.	DSS02.07	Investigace, diagnostika
	4	Minulé nepříznivé události/ztráty a zmeškané příležitosti jsou zpětně analyzovány a jsou hledány jejich hlavní příčiny.	APO12.06	
	4	Zdroje dat pro analýzu jsou shromažďovány, porovnávány a ověřovány na základě kritérií pro ověřování informací (např. srozumitelnost, relevance, důležitost, integrita, přesnost, konzistence, důvěrnost, měna a spolehlivost).	BAI08.01	
	4	Jsou zavedeny postupy pro pravidelné manuální procházení a analýzu logů událostí, zda se neobjevují nějaké anomálie, které detekční systémy doposud neznají a nedovedou na ně reagovat.	DSS01.03	
	5	Příslušným osobám s rozhodovací pravomocí jsou sdělovány výsledky analýz, hlavní příčiny incidentů a doporučení na vylepšení procesů a zvýšení bezpečnosti. Výstupy z analýz jsou zohledněny při řízení rizik.	APO12.06	
	5	Informace a znalosti potřebné pro provádění analýz, které neodpovídají potřebám personálu, jsou neustále rozšiřovány a zlepšovány.	BAI08.03	
	1	Analytici mají dostatečné znalosti a dovednosti pro analýzu bezpečnostních událostí.	-	Schopnosti analytiků
	2	Lidé v týmu SOC mají určené kompetence dle jejich znalostí a na základě toho se tito lidé zaměřují na ten druh analýz, který jim je vlastní.	APOI07.03	
	2	Jsou známy mezery mezi požadovanými a dostupnými znalostmi pro vykonávání analýz. Existují plány, které se snaží tyto mezery vyplnit. Jedná se například o použití externích zdrojů buď z jiného oddělení nebo jiné firmy, plánovaný nábor, školení atd.	APOI07.03	
	3	Dochází k přezkoumávání potřebných znalostí pro vykonávání analytických činností. Které analýzy se provádí nejčastěji, zda znalosti a schopnosti analytiků jsou přiměřené vůči měnícímu se prostředí a požadavkům firmy.	APOI07.03	
	3	Analytici vedou návody a postupy běžných analýz v CTI.	APOI07.03	
	3	Pokud znalosti a schopnosti nepokrývají potřeby SOC, je zajištěno školení či jiný způsob, jak získat potřebné znalosti a schopnosti.	APOI07.03	
	4	Dochází k pravidelným kontrolám a hodnocení posunu ve znalostech a dovednostech interních i externích analytiků. Během revize se přezkoumává, zda jednotliví analytici jsou vzájemně zastupitelní.	APOI07.03	

Identity and Access Management	1	Všichni uživatelé mají přiřazena přístupová práva k potřebným informacím a systémům pro vykonávání jejich práce.	-	Řízení identit uživatelů a logického přístupu
	2	Přístupová práva uživatelů jsou udržována v souladu s obchodními funkcemi, požadavky na procesy a bezpečnostními zásadami. Správa identit a přístupových práv je sladěna s definovanými rolemi a odpovědnostmi na základě tří principů. Mít co nejméně privilegovaných přístupů. Mít jen nezbytné přístupy k funkcím, které jsou třeba pro vykonání práce. Mít přístup jen k potřebným informacím.	DSS05.04	
	3	Všechny změny přístupových práv (vytváření, úpravy a mazání) jsou včas spravovány pouze na základě schválených a zdokumentovaných požadavků a autorizovanými určenými osobami odpovědnými za správu identit.	DSS05.04	
	3	Privilegované uživatelské účty jsou odděleny, redukovány na minimální nezbytné množství a jsou aktivně spravovány.	DSS05.04	
	3	Všechny aktivity privilegovaných uživatelských účtů jsou monitorovány.	DSS05.04	
	3	Tyto aktivity jsou zaznamenávány a archivovány po příslušnou dobu danou zákonem nebo organizací.	DSS05.04	
	3	Jsou identifikovány všechny činnosti zpracování informací podle funkčních rolí. Všechny role jsou konzistentně definovány ve spolupráci se všemi obchodními jednotkami, včetně rolí, které jsou definovány samotným podnikáním jednotlivých procesů v aplikacích.	DSS05.04	
	3	Veškerý přístup k informačním aktivům na základě role jednotlivce nebo obchodních pravidel je ověřován. Ve spolupráci s obchodními jednotkami, které spravují ověřování v různých aplikacích, se kontroluje, zda procesy ověřování probíhají správně.	DSS05.04	
	3	Všichni uživatelé (interní, externí a dočasní) i jejich aktivita v systémech IT (obchodní aplikace, infrastruktura IT, provoz systému, vývoj a údržba) jsou jednoznačně identifikovatelní.	DSS05.04	
	4	Přístup k informacím na základě citlivosti a regulatorním požadavkům je auditován (evidován a ukládán).	DSS05.04	
	4	Pravidelně dochází ke kontrolám všech účtů a souvisejících oprávnění.	DSS05.04	
	1	Role, odpovědnosti, úrovně autorit a přístupová práva jsou spravovány.	-	Řízení rolí, odpovědností, přístupových oprávnění a úrovně oprávnění
	2	Role a odpovědnosti jsou přiřazovány na základě schválených popisů pracovních pozic a podnikových procesních činností.	DSS06.03	

Identity and Access Management Identity and Access Management	2	Úrovně oprávnění pro schvalování různých rozhodnutí týkající se obchodního procesu (transakce, transakční limity, …) jsou alokovány na základě schváleného popisu pracovní pozice.	DSS06.03	Řízení rolí, odpovědností, přístupových oprávnění a úrovně oprávnění
	2	Jsou alokovány role pro speciální, citlivé činnosti, aby došlo k jasnému oddělení povinností.	DSS06.03	
	3	Přidělování přístupových práv probíhá na základě minima, které je vyžadováno k vykonání pracovních činností. Toto minimum je předem vydefinováno v popisu pracovní role.	DSS06.03	
	3	Přístupová práva jsou okamžitě odebírána, pokud dojde ke změně pracovní role (role změní rozsah práv) nebo pracovník opustí vykonávaný proces (změna pracovní pozice, zaměření).	DSS06.03	
	3	Přístupová práva jsou v pravidelných intervalech přezkoumávána, zda je přístup stále potřeba.	DSS06.03	
	3	Pravidelně se poskytuje školení a šíří se povědomí týkající se rolí a odpovědností, aby každý v organizaci rozuměl svým odpovědnostem, důležitosti kontrol, bezpečnosti a ochraně podnikových dat.	DSS06.03	
	3	Aby se předešlo zneužití práv, jsou oprávnění administrátorů dostatečně zabezpečena, sledována a kontrolována.	DSS06.03	
	4	Pravidelně se kontrolují definice řízení přístupů (access control definitions), logy souvisejících událostí a udělované výjimky.	DSS06.03	
	4	Kontroluje se, zda všechna přístupová oprávnění jsou platná a sladěna s aktuálními zaměstnanci a jejich přidělenými rolemi.	DSS06.03	
	1	Správa rolí a přístupových práv je řízena na základě požadavků.	-	Ověření, schválení a plnění požadavků ohledně přístupových práv
	2	Ověřuje se oprávněnost požadavků (založení/zrušení/změna přístupů/role) pomocí předdefinovaných po sobě jdoucích akcí v procesu.	DSS02.03	
	2	Je vynucováno schválení manažera, popřípadě, kde je to třeba, další potřebná schválení na druhé úrovni.	DSS02.03	
	3	Pro často se opakující žádosti existují svépomocné automatizované nabídky a předdefinované modely požadavků.	DSS02.03	
Incident Response	1	Dochází k identifikaci incidentů ať už automatizovaně nebo manuálně.	-	Identifikace incidentů
	2	Incidenty jsou identifikovány pomocí monitorovacích nástrojů, hlášení zaměstnanců, bezpečnostních analýz, a dalších zdrojů.	DSS03.01	

Incident Response	2	Incidenty jsou řešeny analytiky, kteří mají přístup ke všem relevantním datům.	DSS03.01	Identifikace incidentů
	2	Jsou definovány vhodné skupiny podpory, které mohou pomoci s identifikací incidentu, analýzou hlavních příčin a při samotném řešení incidentu. Skupiny podpory jsou určeny na základě předdefinovaných kategorií, jako je server, databáze, síť, software, aplikace a podpůrný software.	DSS03.01	
	2	Je-li potřeba, hlásí se stav identifikovaných incidentů servisnímu oddělení (HelpDesk, ServiceDesk), aby zákazníci a správa IT mohli být průběžně informováni.	DSS03.01	
	2	Existuje jednotný nástroj/místo pro správu incidentů, který umožňuje registraci a hlášení zjištěných incidentů. V tomto nástroji/místě se vedou záznamy o jednotlivých krocích při řešení incidentů, včetně aktuálního stavu (tj. otevřený, znovuotevřený, probíhající nebo uzavřený).	DSS03.01	
	2	Incidenty (i potencionální) a k nim relevantní informace jsou zaznamenávány, aby je bylo možné efektivně zpracovat a udržovat tak úplný historický záznam.	DSS02.02	
	1	Incidenty jsou klasifikovány/kategorizovány.	-	Klasifikace/kategorizace incidentů
	2	Incidenty jsou klasifikovány podle typu incidentu (spoofing, tampering, repudiation, DOS, information disclosure, …).	DSS02.02	
	2	Incidentům se přiřazují úrovně priority a dopadu, aby se zajistilo, že identifikace incidentu a analýza hlavních příčin budou zpracovány včas. Úrovně priorit jsou definovány na základě dopadu a naléhavosti.	DSS03.01	
	3	Existují jasná schémata pro klasifikaci a prioritizaci incidentů, která zajistí jednotnou klasifikaci napříč SOC.	DSS02.01	
	3	Existují pravidla, jak registrovat jednotlivé incidenty.	DSS02.01	
	3	Pro známé incidenty existují postupy řešení, aby byla zajištěna co největší efektivita.	DSS02.01	
	3	Existují pravidla pro eskalaci incidentů, zejména pro závažné incidenty.	DSS02.01	
	3	Postupy a podpůrné materiály pro řešení incidentů jsou dostupné oprávněným osobám v CTI (Cyber & Threat Intelligence – báze znalostí pro SOC).	DSS02.01	
	1	SOC je odpovědný za zvládání bezpečnostních incidentů.	-	Řešení incidentů
	2	Jsou vybírána a používána nejvhodnější možná řešení incidentů (dočasné řešení nebo trvalé řešení).	DSS02.05	
	2	Pokud je k řešení incidentů použito alternativní řešení, existuje o tom záznam.	DSS02.05	

Incident Response	2	Řešení incidentů je dokumentováno.	DSS02.05	Řešení incidentů
	2	Po uzavření incidentu je posuzováno, zda lze řešení incidentu použít jako budoucí vzor pro další řešení podobných incidentů.	DSS02.05	
	3	Jsou připraveny, udržovány a testovány postupy dokumentující konkrétní kroky, které je třeba podniknout, když riziková událost způsobí incident. Tyto postupy zahrnují cesty eskalace a komunikace napříč podnikem.	APO12.06	
	3	Plány reakce na incident obsahují postupy pro minimalizaci dopadu incidentu.	APO12.06	
	4	Incidenty jsou dle potřeb rekategorizovány a dochází k vyčíslování dopadu a ztrát.	APO12.06	
	4	Dopady incidentu jsou oznamovány zainteresovaným osobám s rozhodovací pravomocí.	APO12.06	
	4	Incidenty jsou zpětně analyzovány a jsou hledány jejich hlavní příčiny.	APO12.06	
	5	Příslušným osobám je sdělována hlavní příčina incidentu, další požadavky na očekávanou reakci na vzniklé riziko a návrhy pro vylepšení zabezpečení.	APO12.06	
	1	Po vyřešení incidentů, dochází k jejich uzavření.	-	Uzavírání incidentů
	2	Incidenty jsou uzavírány až po kontrole, že došlo k zamezení škodlivého působení incidentu a vše bylo obnoveno do stavu před incidentem.	DSS02.06	
	2	Kontroluje se, zda incident byl uzavřen v dohodnutém/přijatelném termínu dle klasifikační matice dané naléhavostí a dopadem.	DSS02.06	
	3	Incident je uzavřen až osoba s rozhodovací pravomocí udělí souhlas pro uzavření. Ověřují se výstupy a probíhá komunikace na zúčastněné strany, zda skutečně byl incident vyřešen. Práce na řešení incidentu jsou tak zastaveny.	BAI01.09	
	4	Po uzavření incidentu probíhá sumarizace získaných poznatků (lessons learned). Tyto poznatky jsou písemně zdokumentovány.	BAI01.09	
	4	Probíhají kontroly, zda byl dodržen dokumentovaný postup pro řešení incidentů.	DSS04.08	
	4	Účinnost procesu pro řešení incidentů se prošetřuje z hlediska úspěšnosti vyřešení incidentu, rolí a odpovědností, dovedností a kompetencí, technické infrastruktury a organizační struktury.	DSS04.08	
	5	Je zavedena odpovědnost (accountability), že ponaučení z incidentů (lessons learned) bude zapracováno do CTI (Cyber & Threat Intelligence) a procesů SOCu i celého podniku.	BAI01.09	
	1	Sleduje se progres zvládání incidentů.	-	Sledování stavu a vytváření reportů
	2	Průběžně se sleduje řešení incidentů a dle potřeb se vymáhají postupy vedoucí k vyřešení incidentu.	DSS02.07	

Incident Response	3	Jsou známy osoby, které potřebují získávat informace ohledně incidentů a je známo, o jaké konkrétní informace se jedná.	DSS02.07	Sledování stavu a vytváření reportů
	3	Těmto osobám je dle potřeb pravidelně zasílán report o stavu incidentů.	DSS02.07	
	4	Je zajištěno, že osoby s informační potřebou dostanou informace o incidentech včas buď pomocí včasného reportingu nebo přímého přístupu k online datům o incidentech.	DSS02.07	
	4	Incidenty jsou analyzovány dle typu/kategorie a na základě těchto analýz se identifikují trendy a opakující se vzorce chování.	DSS02.07	
	5	Analýzy trendů a opakujících se vzorů v incidentech se následně používají jako vstup pro zlepšování detekčních nástrojů, procesů a bezpečnostních opatření.	DSS02.07	
Detekční pravidla	1	Do detekčních nástrojů vstupují logy z více IT aktiv/služeb.	-	Logování a korelace událostí
	2	Požadavky na zdroje dat/logů, které budou zapojeny do procesu monitoringu jsou zjištěny. Od zúčastněných stran (vlastník monitorované služby/aktiva, SOC analytik, SOC vývojář, …) se zjišťuje, co je cílem detekce, jaké jsou požadavky na detekční pravidla, a nad jakými logy se pravidla budou spouštět. Je známo, kde dané logy sbírat.	BAI08.01	
	3	Zdroje dat/logů pro vytváření detekčních pravidel jsou tříděny a klasifikovány podle jejich zdrojů.	BAI08.01	
	3	Při tvorbě pravidel se zohledňují různé prahové hodnoty (thresholdy), kdy při jejich překročení dojde k okamžitému upozornění na možný bezpečnostní incident. Příkladem je maximálně 5 pokusů pro zadání bezpečnostního hesla, když stahování překročí 500 MB, a další.	DSS01.03	
	4	Jsou zavedeny postupy pro monitorování logů událostí a dochází k pravidelným manuálním kontrolám.	DSS01.03	
	4	Zdroje dat/logů jsou shromažďovány, porovnávány a ověřovány. Hledají se společné atributy, které pomohou vytvářet složitější detekční pravidla.	BAI08.01	
	1	Jsou vytvářena bezpečnostní pravidla, která pomáhají detekovat bezpečnostní události.	-	Návrh řešení
	2	Návrhy detekčních pravidel jsou zpracovávány tak, aby splňovaly požadavky bezpečnostního monitoringu.	BAI03.01	
	2	Pravidla se vytváří na základě vydefinovaných rizikových scénářů, které mohou nastat. Vytváří se tzv. Use Case.	DSS05.07	

Detekční pravidla	2	Návrhy jsou předkládány všem zúčastněným stranám zapojených do procesu monitoringu. (vlastník monitorované služby/aktiva, bezpečnostní analytici, IT experti, risk konzultanti, …). Pravidla jsou navrhována na základě shody mezi SOC a vlastníkem monitorované služby/aktiva.	BAI03.01	Návrh řešení
	2	Detailní návrhy pravidel (Use Case) obsahují informace o tom, jaká data se budou sbírat, kde se budou sbírat, kde se budou shromažďovat, na jak dlouho se budou ukládat, jaká je vyhodnocovací logika pravidel, zda se budou vytvářet nové bezpečnostní logy.	BAI04.02	
	3	Již během návrhů pravidel se bere v úvahu možné vznikající false positive hlášení a výkonnostní problémy.	BAI04.02	
	3	Návrhy jsou proaktivně vyhodnocovány, aby se identifikovaly slabiny/nedostatky návrhu detekčních pravidel ještě před tím, než dojde k jejich vývoji. Na základě těchto hodnocení se vytváří vylepšení návrhů.	BAI04.02	
	1	Jsou vytvářena bezpečnostní pravidla, která pomáhají detekovat bezpečnostní události.	-	Vývoj řešení
	2	Úpravy i tvorba detekčních pravidel se provádí na neprodukčním prostředí.	BAI03.03	
	2	Pokud jsou do vývoje zapojeny poskytovatelé třetí strany, je zajištěno, že údržba, podpora, vývojové standardy a licence jsou řešeny ve smluvních závazcích.	BAI03.03	
	2	Během vývoje se nezapomínají sledovat požadavky na změny, které se dle potřeb zapracovávají.	BAI03.03	
	2	Všechna pravidla jsou dokumentována dle definovaných standardů. Eviduje se a kontroluje vydávání verzí a k nim příslušné dokumentace.	BAI03.03	
	2	Existuje metoda, jak mít přístup k historickým záznamům všech detekčních pravidel a k jejich dokumentaci. Tyto historické záznamy slouží dalším stranám (audit, management, IT, …).	APO14.09	
	2	Existují postupy a pravidla pro kontrolu přístupu, přenosu, úpravu pravidel a související dokumentace.	APO14.09	
	3	Při vývoji pravidel se posuzuje dopad na výkonost a efektivitu řešení.	BAI03.03	
	3	Pokud se manipuluje s bezpečnostně citlivými komponentami/daty, jsou s tím odpovědné osoby za vývoj detekčních pravidel detailně obeznámeny a rozumí odpovědnostem, které se pojí s manipulací takových komponent/dat.	BAI03.03	

Detekční pravidla	3	Procesy tvorby bezpečnostních pravidel a k nim potřebná dokumentace jsou zaznamenávány do CTI (Cyber & Threat Intelligence – báze znalostí pro SOC). Dochází ke kontrolám, zda zaznamenané procesy pro tvorbu a dokumentaci pravidel jsou stále aktuální.	APO14.08	Vývoj řešení
	3	Dokumentace k pravidlům se sdílí podle uzavřených dohod v rámci spolupráce na bezpečnostním monitoringu.	APO14.08	
	3	Pro každé vytvořené pravidlo existují v CTI postupy k analýze bezpečnostního hlášení a reakční plán.	APO14.08	
	4	Dokumentace pravidel je sdílena dle potřeb se zúčastněnými stranami tak, aby se nevytvářely zbytečné duplicitní dokumenty. Předchází se tak chybám způsobenými zastaralými informacemi.	APO14.08	
	1	Jsou vytvářena bezpečnostní pravidla, která pomáhají detekovat bezpečnostní události.	-	Testování a úprava řešení
	2	Testování probíhá dle předem vytvořených testovacích plánů, které simulují podmínky pro ověření funkčnosti detekčních pravidel.	BAI03.08	
	2	Testování probíhá na testovacím nebo vývojovém prostředí, které je odděleno od produkčního prostředí.	BAI03.08	
	2	Objevené chyby při testování se zaznamenávají. Testy jsou prováděny do té doby, až se nevyřeší všechny významné chyby.	BAI03.08	
	2	Výsledky testů a objevené chyby se zapracovávají do změn detekčních pravidel.	BAI03.08	
	2	Při akceptačních testech se kontroluje, zda byly všechny chyby a nedostatky odstraněny.	BAI07.05	
	3	Postupy testování a použitá nastavení jsou ukládány pro budoucí testování detekčních pravidel.	BAI03.07	
	3	Akceptační testy provádí jedinec nebo skupina osob, která je nezávislá na vývojovém týmu.	BAI07.05	
	3	Do testování jsou zapojeni i vlastníci monitorované služby/aktiva.	BAI07.05	
	3	Po akceptačních testech vytváří testující osoby závěr, který se prezentuje vlastníkům monitorovaných služeb/aktiv.	BAI03.05	
	3	Akceptace se stvrzuje písemným souhlasem SOC vývojáře, SOC analytika a vlastníka monitorované služby/aktiva.	BAI03.05	
	3	Bezpečnostní pravidla/vylepšení se i po nasazení do produkce po předem určenou dobu revidují. Kontroluje se, v jakém rozsahu došlo ke splnění očekávání všech zúčastněných stran a zda lze řešení považovat za použitelné.	BAI07.08	

Detekční pravidla	4	Revize naimplementovaných pravidel se dle potřeb provádí s vlastníky monitorovaných služeb/aktiv a dalšími osobami zapojených do řešení bezpečnostních události vyvolané tímto pravidlem.	BAI07.08	Testování a úprava řešení
	4	Metriky pro měření úspěchu a dosažení požadavků jsou určeny SOC analytiky, vlastníky monitorované služby/aktiva a dalšími zúčastněnými stranami.	BAI07.08	
	5	Odhalené nedostatky jsou sepsány ve formě nových požadavků či změn a vrací se na vývojový tým k zapracování.	BAI07.08	
	1	Jsou vytvářena bezpečnostní pravidla, která pomáhají detekovat bezpečnostní události.	-	Provoz, údržba, zlepšování
	3	Pokud pravidla generují mnoho false positive hlášení, je informován vlastník monitorované služby/aktiva a pravidlo je na základě vzájemných dohod upraveno.	DSS01.03	
	3	Pokud detekční pravidlo vykazuje odchylky od plánů, analytik tuto skutečnost hlásí vývojovému týmu a ten dané pravidlo přezkoumá a popřípadě upraví.	BAI03.09	
	3	Všechny požadavky na změny jsou zaznamenávány.	BAI03.09	
	3	Změny pravidel jsou prováděny jen pokud změnu odsouhlasí všechny zainteresované strany.	BAI03.09	
	4	Kontinuálně se vedou záznamy o false positive upozornění, trendech, společných znacích bezpečnostních incidentů. Nad takovými daty se provádí analýza a výsledky jsou zaznamenávány a reportovány zúčastněným stranám do procesu monitoringu.	APO08.05	
	4	Pravidla jsou pravidelně kontrolována, zda stále dosahují potřebné kvality. Zda pravidlo stále splňuje požadavky pro detekci anomálií, zda se nevyskytují nové skutečnosti, které je třeba zohlednit. Po přezkumu se vytváří doporučení ke zlepšení daného pravidla.	APO14.07	
	4	Vytváří se zpráva o měření kvality pravidel, do které se přikládají návrhy na zlepšení. Tato zpráva je distribuována všem zúčastněným stranám.	APO14.07	
	5	Na základě analýz dochází k hledání možných vylepšení detekčních nástrojů, která jsou následně implementována.	APO08.05	
	5	Dochází ke spolupráci mezi vlastníky objektů pod monitoringem, techniky bezpečnostních detekčních nástrojů a analytiků SOC, aby se zajistilo, že detekční pravidla jsou neustále vylepšována a byly tak redukovány false positive nálezy a docházelo k nalezení skutečných incidentů.	APO08.05	
	5	Na základě zprávy o měření kvality pravidel dochází mezi zúčastněnými stranami k diskusi a návrhu zlepšení pravidel, která jsou následně implementována.	APO14.07	

Správa SOC nástrojů	1	Existují SOC nástroje a související podpora, které dodávají třetí strany.	-	Dodávka třetích stran
	2	Dodávky od externích firem se řídí podle dohodnutých smluvních podmínek.	BAI09.03	
	3	Požadavky na zabezpečení informačních procesů u dodávek třetích stran jsou v souladu se smlouvami a SLA.	DSS01.02	
	3	Kritické interní procesy správy nástrojů SOC jsou integrovány do procesů externích poskytovatelů služeb. Jedná se například o plánování výkonu a kapacity, správu změn, správu konfigurace, správu požadavků na služby a incidenty, správu problémů, správu zabezpečení, kontinuitu podnikání a monitorování výkonu procesů a podávání zpráv.	DSS01.02	
	3	Smlouvy o údržbě zahrnují přístupy třetích stran k SOC nástrojům pro činnosti údržby na místě i mimo něj (on-site vs. Off-site). Smlouvy obsahují nebo odkazují na všechny nezbytné podmínky zabezpečení a ochrany soukromí, včetně postupů povolení přístupu, aby byl zajištěn soulad se zásadami a normami zabezpečení a ochrany soukromí.	BAI09.02	
	4	Existují plány nezávislého auditu a přezkoumání provozního prostředí externích poskytovatelů, který potvrdí, že dohodnuté požadavky ve smlouvách a SLA jsou adekvátně řešeny.	DSS01.02	
	1	SOC nástroje jsou spravovány lidmi ze SOC.	-	Provoz a údržba nástrojů
	2	Jsou vytvořeny a udržovány provozní postupy a související aktivity na podporu SOC nástrojů.	DSS01.01	
	2	Údržba nástrojů se provádí dle stanoveného harmonogramu.	DSS01.01	
	2	Plány údržby nástrojů SOC zahrnují pravidelné kontroly podle SOC potřeb a provozních požadavků, jako je správa oprav, strategie upgradu, rizika, soukromí, hodnocení zranitelností a bezpečnostní požadavky.	BAI03.10	
	2	Odpovědné osoby za správu nástrojů využívaných v SOC berou v potaz riziko selhání nebo potřeby výměny každého daného nástroje. Všechny možná rizika s tím spojená jsou komunikována postiženým zákazníkům a uživatelům těchto nástrojů.	BAI09.02	
	3	Existují mechanismy pro ověření, že všechna očekávaná data (logy) ke zpracování byla přijata přesně a včas. Je zajištěno, že SOC analytici přijímají správná data z nástrojů bezpečně a včas.	DSS01.01	
	3	Plánované odstávky jsou zahrnuty do celkového plánu údržeb. Činnosti údržby jsou plánovány tak, aby se minimalizovaly nepříznivé dopady na SOC aktivity.	BAI09.02	

Správa SOC nástrojů	3	Provádí se pravidelná preventivní údržba, monitoruje se výkon a v případě potřeb se poskytují alternativní a/nebo další prostředky za účelem minimalizace pravděpodobnosti selhání nástrojů SOC.	BAI09.02	Provoz a údržba nástrojů
	3	Plán preventivní údržby se stanovuje s ohledem na analýzu nákladů a přínosů, doporučení prodejců, riziko výpadku, kvalifikovaný personál a další relevantní faktory.	BAI09.02	
	3	Před navrhovanou činností údržby nástroje se posuzuje její význam pro aktuálně implementované řešení, jeho funkčnost a stávající procesy. Zvažuje se riziko, dopad na uživatele a dostupnost zdrojů. Vlastníci SOC nástrojů jsou obeznámeni s dopady dané údržby a se souvisejícími změnami.	BAI03.10	
	3	V případě zásadních změn stávajících řešení, které vedou k významným úpravám současných návrhů a/nebo funkčnosti a/nebo obchodních procesů, se postupujte podle vývojového procesu používaného pro nové systémy. Pro aktualizace údržby se používá proces správy změn.	BAI03.10	
	3	Je zajištěno, aby služby vzdáleného přístupu a uživatelské profily (nebo jiné prostředky používané k údržbě nebo diagnostice) byly aktivní pouze v případě potřeby.	BAI09.02	
	4	Spravuje se výkonost a propustnost (performance&throughput) naplánovaných aktivit.	DSS01.01	
	4	Typy a objemy činností údržby jsou pravidelně analyzovány na abnormální trendy, které mohou naznačovat základní problémy s kvalitou nebo výkonem. Mohou také odhalovat možné výhody/nevýhody významného upgradu/výměny namísto údržby.	BAI03.10	
	4	Provádí se analýza spokojenosti SOC analytiků a poskytovatelů SOC nástrojů. Je zajištěno, že nalezené nedostatky jsou řešeny a stav údržby a její výsledky jsou reportovány zúčastněným stranám.	APO08.05	
	4	Sleduje se výkon SOC nástrojů pomocí zkoumání trendů incidentů, výpadků a problémů. V případě potřeby se provádí oprava či výměna nástroje.	BAI09.02	
	5	Sledují se poruchy a problémy spojené se SOC nástroji a na základě nich se přijímají vhodná opatření ke zlepšení spolehlivosti SOC nástrojů.	DSS01.01	
	5	SOC analytici a poskytovatelé SOC nástrojů vzájemně spolupracují na identifikaci, komunikaci a implementaci zlepšení SOC nástrojů a byly identifikovány a vyřešeny hlavní příčiny problémů s nástroji.	APO08.05	

Správa SOC nástrojů	1	SOC nástroje jsou spravovány lidmi ze SOC.	-	Pořizování a nasazení nástrojů
	2	Dochází k zaznamenávání aktivit spojených s vytvářením, obstaráváním, implementováním, testováním, údržbou a vyřazováním SOC nástrojů.	BAI09.03	
	3	Nástroje jsou nasazovány podle standardního životního cyklu implementace, včetně správy změn a akceptačního testování.	BAI09.03	
	3	Jednotlivým nástrojům jsou přiřazeni vlastníci, kteří za daný nástroj nesou odpovědnost.	BAI09.03	
	3	Vyřazování bezpečnostních nástrojů je předem plánováno a schvalováno. Všechny kroky spojené s vyřazováním nástrojů je dokumentováno.	BAI09.03	
	3	Likvidace nástrojů probíhá bezpečným způsobem (například s ohledem na trvalé odstranění veškerých zaznamenaných dat na mediálních zařízeních a potenciální poškození životního prostředí).	BAI09.03	

Příloha C: Požadavky na kvalitní software dle SQuaRE

Funkční přiměřenost	Funkční úplnost	Míra splnění všech zadaných úkolů a cílů pro vydefinovaný SW.	Nástroj na základě vyplnění dotazníku dokáže určit úrovně schopnosti a zralosti. Dokáže také vyspecifikovat aktivity, které napomohou dosažení vyšší úrovně schopnosti a zralosti.
	Funkční správnost	Míra, do jaké software poskytuje správné výsledky s potřebnou mírou přesnosti.	Pro zajištění přesnosti při určování úrovní schopnosti a zralosti byla využita metoda hodnocení CPM, kterou využívá COBIT 2019.
	Funkční přiměřenost	Do jaké míry jednotlivé funkce usnadňují plnění stanovených úkolů a cílů. Je ukazatelem toho, jak dobře je nástroj schopen vykonávat svou primární funkci.	Primární funkcí je určování úrovní schopnosti a zralosti aktivit SOC a identifikace silných a slabých stránek SOC. Nástroj plně automatizuje vyhodnocování dotazníku a určuje jednotlivé úrovně schopnosti a zralosti, a to vše za plné vizualizace pomocí grafů.
Výkonnost	Časové chování	Časová odezva a doba pro zpracování dat při plnění jeho funkcí.	Data jsou vyhodnocována v celém průběhu odpovídání na testové otázky. Po dokončení testu, jsou výsledky ihned k dispozici. Výkonnost však také závisí na výkonnosti zařízení, kde je nástroj pomocí Microsoft Excel spouštěn. Nástroj však nepoužívá žádné složité výpočty, tedy by nemělo docházet k problémům při zpracovávání dat. Tento fakt byl otestován na osmi zařízení a nebyly shledány žádné výkonnostní problémy.
	Využití zdrojů	Množství a typy zdrojů použitých produktem nebo systémem při plnění jeho funkcí.	Nástroj nevyužívá žádné externí zdroje. Logická struktura je plně integrována do dvou pomocných listů, kde dochází k propočtům výsledků na základě vyplněných dotazníků. Nástroj používá jednoduché matematické, statistické, logické a vyhledávací funkce, které nemají nikterak vliv na výkonnost nástroje.

	Kapacita	Jak maximální limity jednotlivých parametrů produktu či systému splňují dané požadavky.	Kapacitu nástroje není třeba řešit, protože došlo k omezení počtu vstupních hodnot, které může uživatel do nástroje zadat. Z toho důsledku nemůže dojít k přečerpání kapacit. Při testování nástroje bylo ověřeno, že aktuální kapacita nástroje je dostačující, aby zajistila hladký provoz.
Kompatibilita	Koexistence	Do jaké míry může produkt efektivně vykonávat požadované funkce při sdílení společného prostředí a zdrojů s jinými produkty, aniž by to mělo negativní dopad na jakýkoliv jiný produkt.	Nástroj není uzpůsoben na kooperaci s jinými softwarovými produkty.
	Interoperabilita	Do jaké míry si mohou dva a více systémů či komponent vyměňovat informace.	Z technického hlediska je interoperabilita zajištěna samotnou aplikací Microsoft Excel a podporou formátu .xlsx. Z logického hlediska je kompatibilita výstupu nástroje dána rámcem užití. Pro určení úrovní schopnosti a zralosti byl využit rámec COBIT 2019. Tedy jednotlivé aktivity je možné následně v tomto rámci dohledat. Uvedené hodnocené aktivity jsou dále v souladu s rámcem NIST CSF, kdy výstup sebehodnocení může být využit k posudku, zda SOC naplňuje požadavky tohoto rámce.
Použitelnost	Rozpoznatelnost přiměřenosti	Míra, do jaké mohou uživatelé rozpoznat, zda je produkt nebo systém vhodný pro jejich potřeby.	Hodnocený SOC by měl být rychle schopen určit, zda je nástroj vhodný pro jejich potřeby. To vyžaduje vysvětlení účelu nástroje a definici oboru, která organizaci umožňuje určit, zda nástroj odpovídá potřebám sebehodnocení.
	Schopnost učit se	Do jaké míry se mohou uživatelé naučit daný produkt používat účinně, účelně a bez rizika.	Jelikož se jedná o nástroj pro sebehodnocení je třeba, aby nástroj byl jednoduchý na pochopení a následně jednoduchý na používání. Kvůli tomu je v nástroji popsán návod, jak daný nástroj používat.
	Provozuschopnost	Do jaké míry je produkt nebo systém atributy, které usnadňují ovládání.	Nástroj by měl být snadno použitelný. Za tímto účelem je nástroj vybaven grafickými navigačními prvky pro snadné ovládaní a

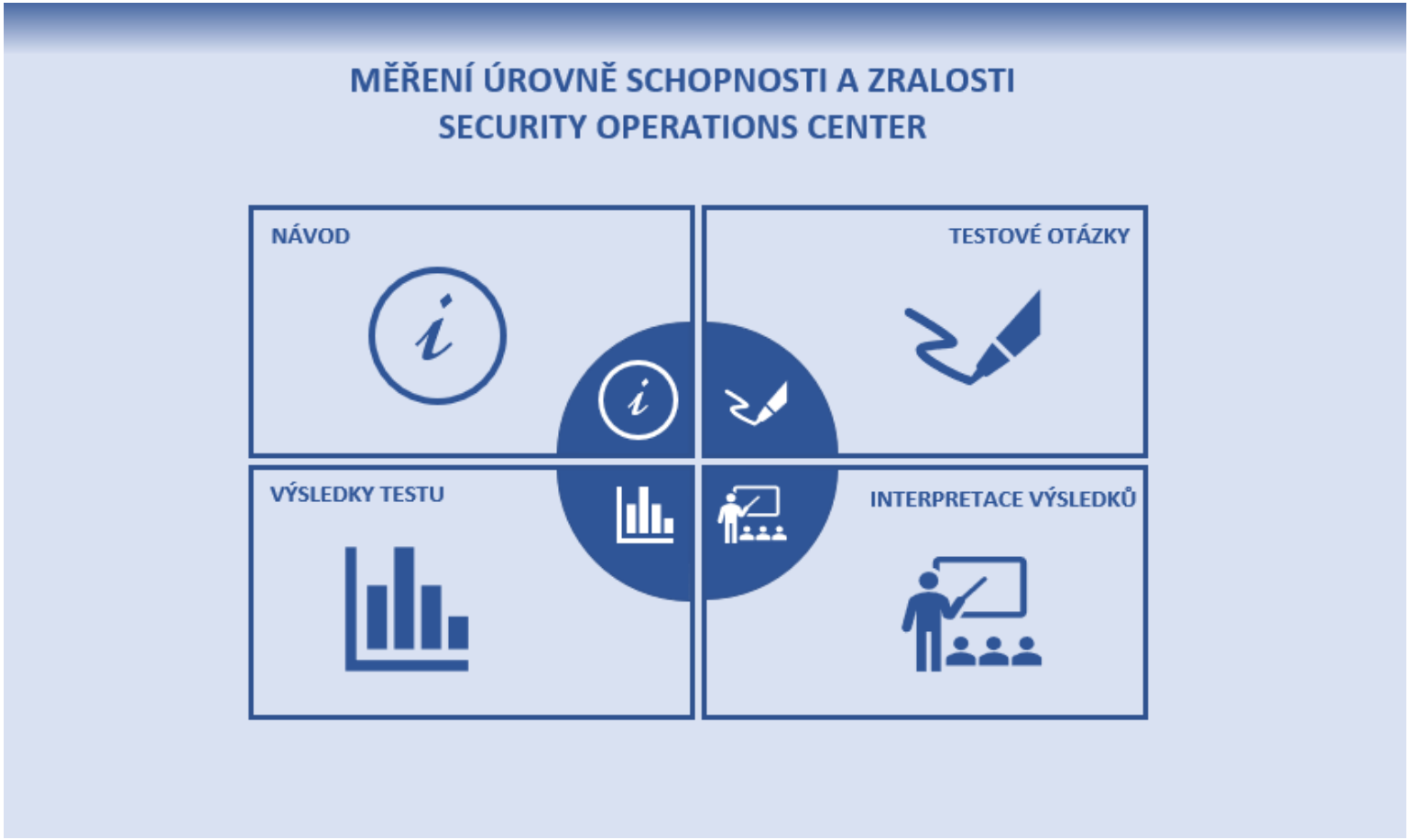
			testové otázky mají předem vydefinované možnosti pro výběr odpovědi.
	Ochrana před chybou uživatele	Míra, do jaké systém chrání uživatele před chybami.	Nástroj automaticky rozpozná, pokud nedojde k úplnému vyhodnocení dotazníkového šetření a při načítání výsledků je uživatel na tuto skutečnost upozorněn. Nástroj je také uzamčen pro běžné uživatele, tedy nelze vykonávat jiné funkce než předem povolené funkce, což zamezuje vznik chybám.
	Estetika uživatelského rozhraní	Do jaké míry uživatelské rozhraní umožňuje uživateli příjemnou a uspokojivou interakci.	Při testování v praxi bylo ověřeno, že designové řešení napomáhá snadné orientaci napříč celým nástrojem.
	Přístupnost	Do jaké míry mohou produkt používat lidé s nejširší škálou znalostí a schopností k dosažení stanovených cílů v konkrétním kontextu použití.	Nástroj je jednoduchý na používání a nevyžaduje žádné technické znalosti. Problémy mohou nastat, když nástroj pro sebehodnocení použije osoba, která nezná činnosti týmu SOC, což celkově postrádá význam pro „sebehodnocení“ vyspělosti SOC.
Spolehlivost	Zralost	Do jaké míry systém, produkt nebo komponenty splňují požadavky na spolehlivost za normálního provozu.	Při testování nebyly nalezeny žádné závažnější nedostatky, které by znemožnily vykonávat základní funkce nástroje. Při testování praxi bylo zjištěno, že generovaná doporučení pro dosažení vyšší úrovně schopnosti a zralosti jsou kompatibilní pouze s verzí Microsoft Office 365. Starší verze bohužel tato doporučení nenavrhují. Z toho plyne návrh na zlepšení rozšířit podporu i starší verze Microsoft Office.
	Dostupnost	Do jaké míry je produkt či systém funkční a přístupný, je-li to pro použití nutné.	Nástroj je vytvořen pomocí Microsoft Excel a funguje v offline režimu. Jelikož softwarové kancelářské balíky od společnosti Microsoft jsou základní výbavou počítačů s OS Windows, je nástroj kdykoliv k dispozici.
	Odolnost proti chybám	Do jaké míry systém, produkt nebo komponenty fungují, jak bylo zamýšleno, navzdory přítomnosti hardwarových nebo softwarových chyb.	Nástroj by měl být odolný vůči chybám tím, že omezí možnost vstupu a kontroluje zadané vstupy uživateli, kteří provádí sebehodnocení. Při testování v praxi bylo odhaleno, že některé

			funkce nástroje jsou kompatibilní pouze s verzí Microsoft Office 365.
	Obnovitelnost dat	Do jaké míry může produkt nebo systém v případě přerušení nebo poruchy obnovit přímo ovlivněná data a obnovit požadovaný stav systému.	Microsoft Excel nabízí možnost obnovení dat v případě neočekávaného ukončení programu. Kromě toho poskytuje možnost verzování dokumentů.
Bezpečnost	Důvěrnost	Do jaké míry produkt nebo systém zajišťuje, že k údajům mají přístup pouze osoby oprávněné k přístupu.	Dokument je možné zašifrovat pomocí standardní funkce aplikace Microsoft Excel.
	Integrita	Do jaké míry systém, produkt nebo komponenta brání neoprávněnému přístupu nebo úpravám počítačových programů nebo dat.	Nástroj je uzamčen pro běžné uživatele, tím pádem je zamezeno neoprávněnému přístupu nebo úpravám samotného nástroje či dat. Aplikace Microsoft Excel zaznamenává změny dokumentu, a tedy pokud dojde ke změně dat, je možné tyto informace získat. Pokud organizace používají funkce digitálních podpisů (certifikáty), tak je zajištěna autenticita, integrita a nepopiratelnost.
	Nepopiratelnost	Do jaké míry lze prokázat, že došlo k různým akcím nebo událostem, takže události nebo akce nelze později zapřít.	Microsoft Excel zaznamenává aktivity jednotlivých uživatelů a ukládá je do historie. Pokud organizace používají funkce digitálních podpisů (certifikáty), tak je zajištěna autenticita, integrita a nepopiratelnost.
	Odpovědnost	Do jaké míry lze jedinečně vysledovat akce entit.	Microsoft Excel zaznamenává aktivity jednotlivých uživatelů a ukládá je do historie. Pokud organizace používají funkce digitálních podpisů (certifikáty), tak je zajištěna autenticita, integrita a nepopiratelnost.
	Autenticita	Do jaké míry lze prokázat totožnost subjektu nebo zdroje.	Aplikace Microsoft Excel umožňuje zapnout funkci „Sledovat Změny“.
Udržitelnost	Modularita	Do jaké míry je systém nebo počítačový program složen z diskrétních	Aktivity SOC se neustále rozšiřují a aktuálně nástroj postihuje jen ty nejzákladnější, které jsou praxí vydefinovány. Pokud nastane

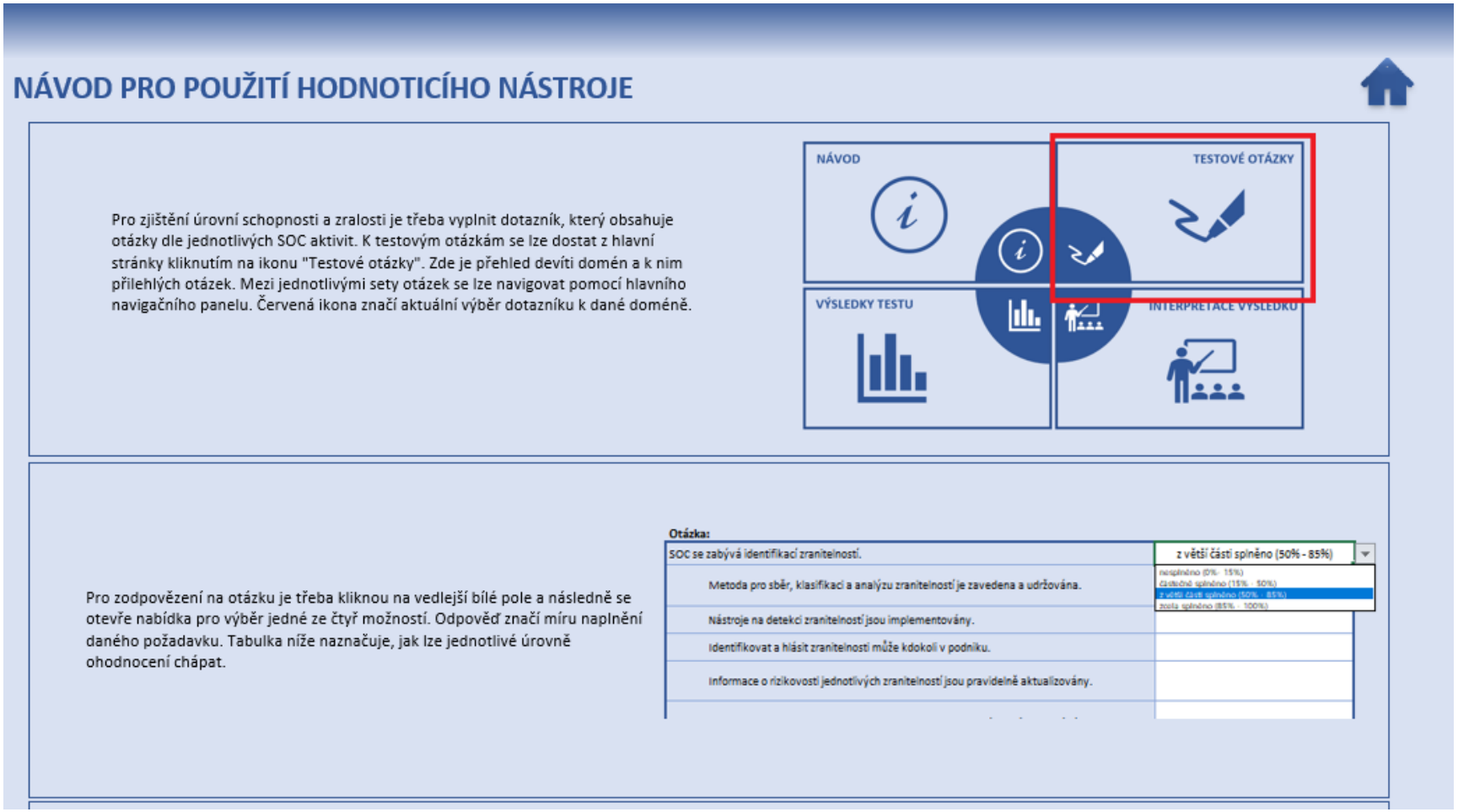
		komponent. To znamená, že změna jedné komponenty by měla mít minimální dopad na ostatní komponenty.	potřeba přidat do nástroje novou sadu aktivit pro sebehodnocení, nemělo by to činit technické komplikace.
	Opakovaná použitelnost	Do jaké míry lze aktivum použít ve více než v jednom systému.	Opakovanou použitelnost pokrývá samotný Microsoft Excel. Vytvořením kopie dokumentu lze sebehodnocení použít vícekrát.
	Analyzovatelnost	Míra účinnosti a efektivity, s níž je možné posoudit dopad zamýšlené změny na jednu nebo více jejích částí na produkt nebo systém, nebo diagnostikovat u produktu nedostatky nebo příčiny poruch, nebo identifikovat součásti k úpravě.	Při testování bylo odhaleno, že pokud by bylo třeba měnit některé komponenty, musela by se upravit i logika vyhodnocování. Jedná se hlavně v případě změn názvů zvolených parametrů pro rozhodovací bloky, zda bylo dosaženo dané úrovně zralosti. Tento podnět byl zapracován a nyní by změna jednoho logického bloku neměla mít negativní dopad na další logické bloky.
	Modifikovatelnost	Do jaké míry lze produkt nebo systém efektivně modifikovat, aniž by docházelo k vadám nebo zhoršování stávající kvality produktu.	Požadavek souvisí s modularitou, kdy není problém daný nástroj rozvíjet. Co se týče přizpůsobení potřebám jednotlivých SOC, tak tyto zásahy nejsou pro účely objektivního sebehodnocení vítány. Nástroj byl vyvinut na základě požadavku obecného hodnocení SOC týmů vycházející z NIST CSF a COBIT 2019. Pro potřeby vyhodnocení jednotlivých aktivit a domén je na vedení, aby zhodnotilo dosažené výsledky hodnocení s požadovanými úrovněmi. Na tuto skutečnost jsou uživatelé v nástroji upozorněni v sekci „interpretace výsledků“.
	Testovatelnost	Stupeň účinnosti a účelnosti, s nimiž lze stanovit testovací kritéria pro systém, produkt nebo komponenty, a lze provést testy, aby se zjistilo, zda byla tato kritéria splněna.	Možnost tvorby testových scénářů je snadno proveditelná, protože díky provázanosti nástroje s metodikami COBIT jsou známy cílené hodnoty, kterých má být dosaženo po vyplnění dotazníkového šetření. Tyto scénáře byly také použity při testování, zda nástroj generuje správné výsledky.

Přenositelnost	Přizpůsobivost	Do jaké míry lze produkt nebo systém efektivně přizpůsobit různému HW, SW či jinému uživatelskému prostředí.	Nástroj je vytvořen pro aplikaci Microsoft Excel. To udává míru přizpůsobení pro různá prostředí.
	Instalovatelnost	Míra účinnosti a účelnosti s jakou lze produkt či systém instalovat či odinstalovat ve specifickém prostředí.	Jelikož je nástroj vytvářen na platformě Microsoft Excel, instalace podléhá faktu, zda uživatel disponuje Microsoft Excel či jiným softwarem, který umožňuje spouštět soubory formátu .xlsx. Pokud uživatel používá software splňující tuto podmínku, další instalace není potřeba.
	Vyměnitelnost	Do jaké míry může produkt nahradit jiný určený softwarový produkt pro stejný účel ve stejném prostředí.	Při testování v praxi bylo odhaleno, že některé funkce nástroje jsou kompatibilní pouze s verzí Microsoft Office 365. Pokud by se nástroj chtěl použít pro nižší verze, je třeba pozměnit logickou strukturu nástroje a nahradit jisté komponenty novými, které budou vybudovány na základě podporovaných funkcí dané verze.

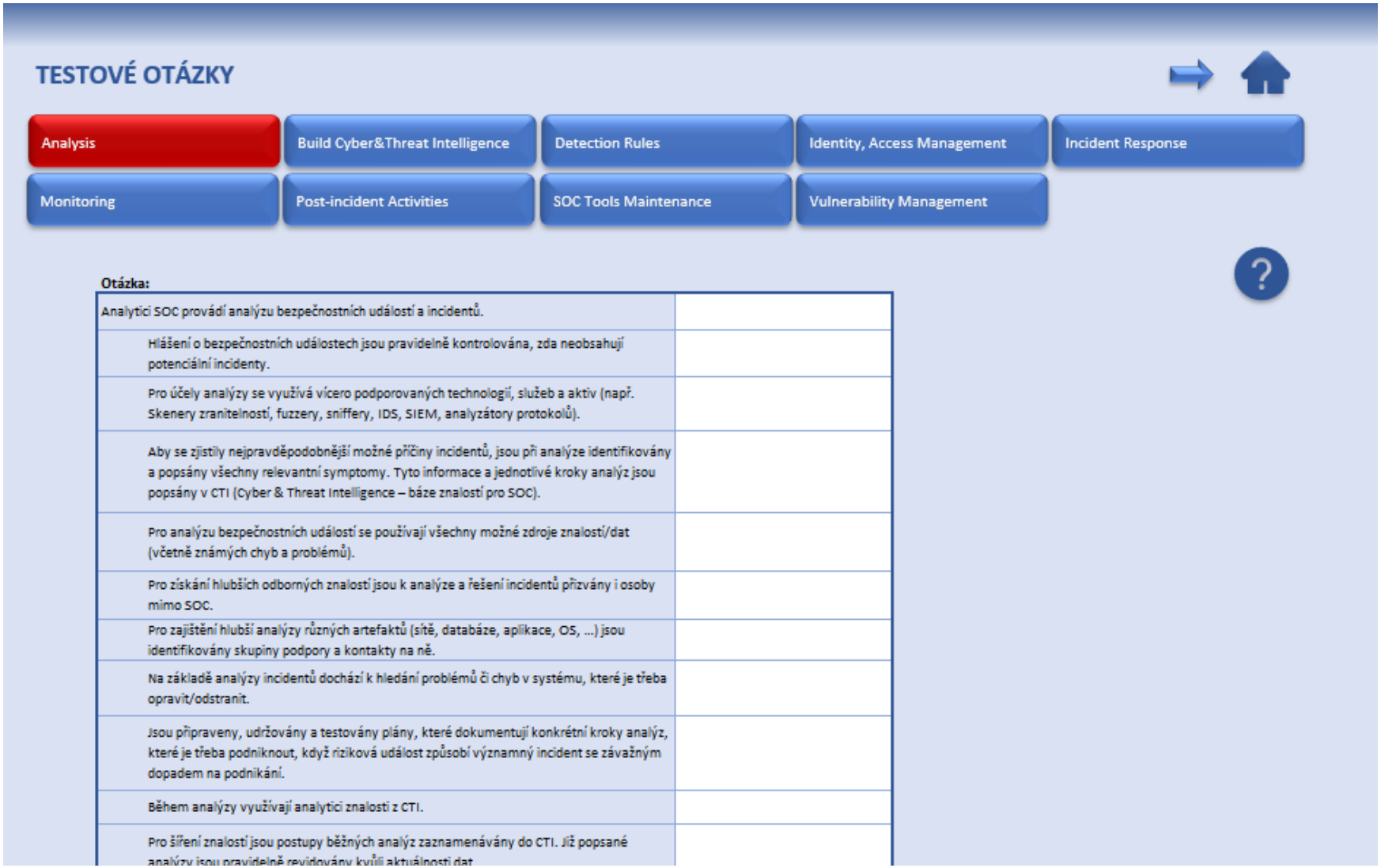
Příloha D: Grafická prezentace hodnoticího nástroje



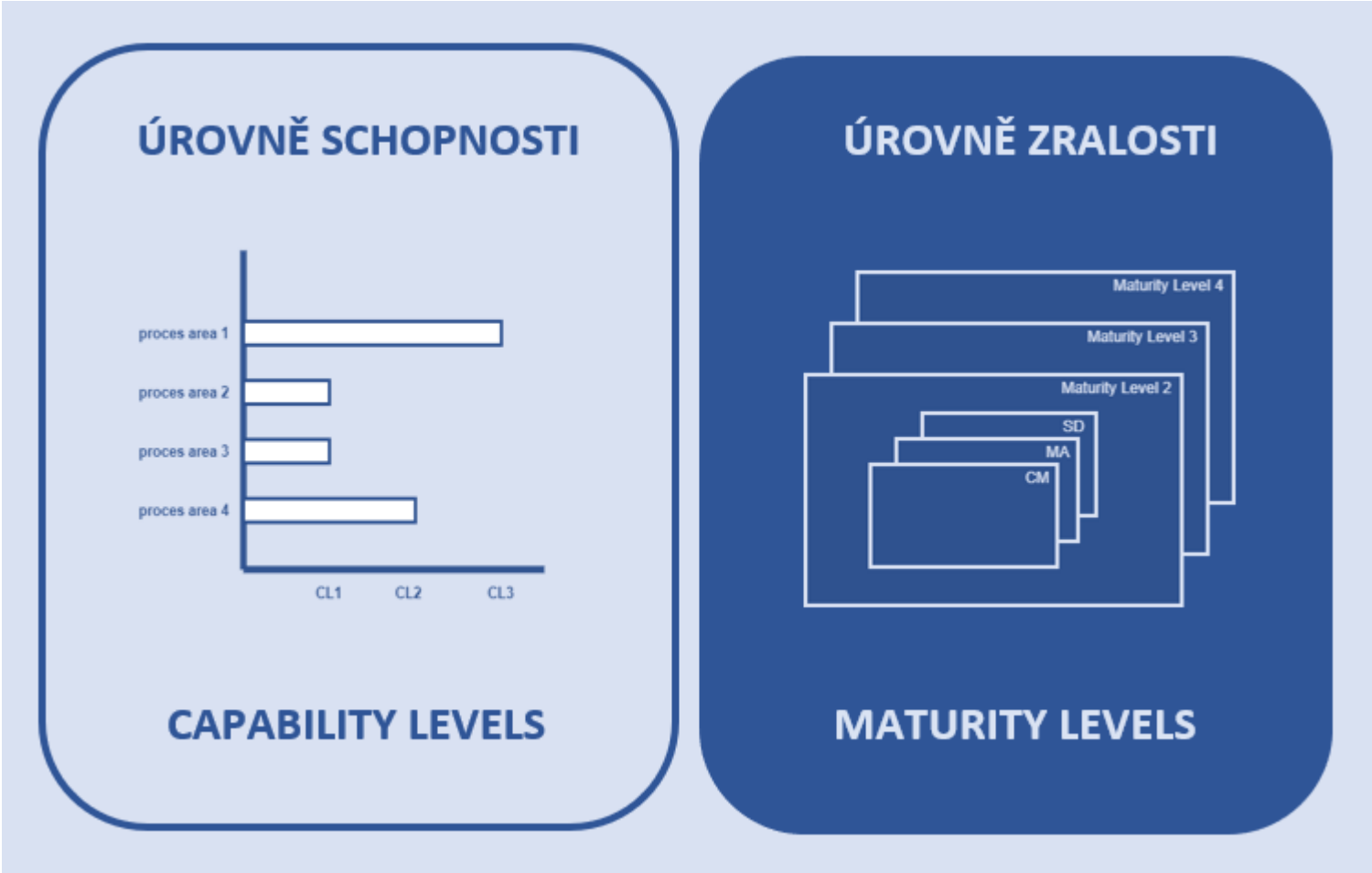
Obrázek D-1 Úvodní navigační stránka hodnoticího nástroje (Zdroj: Autor)



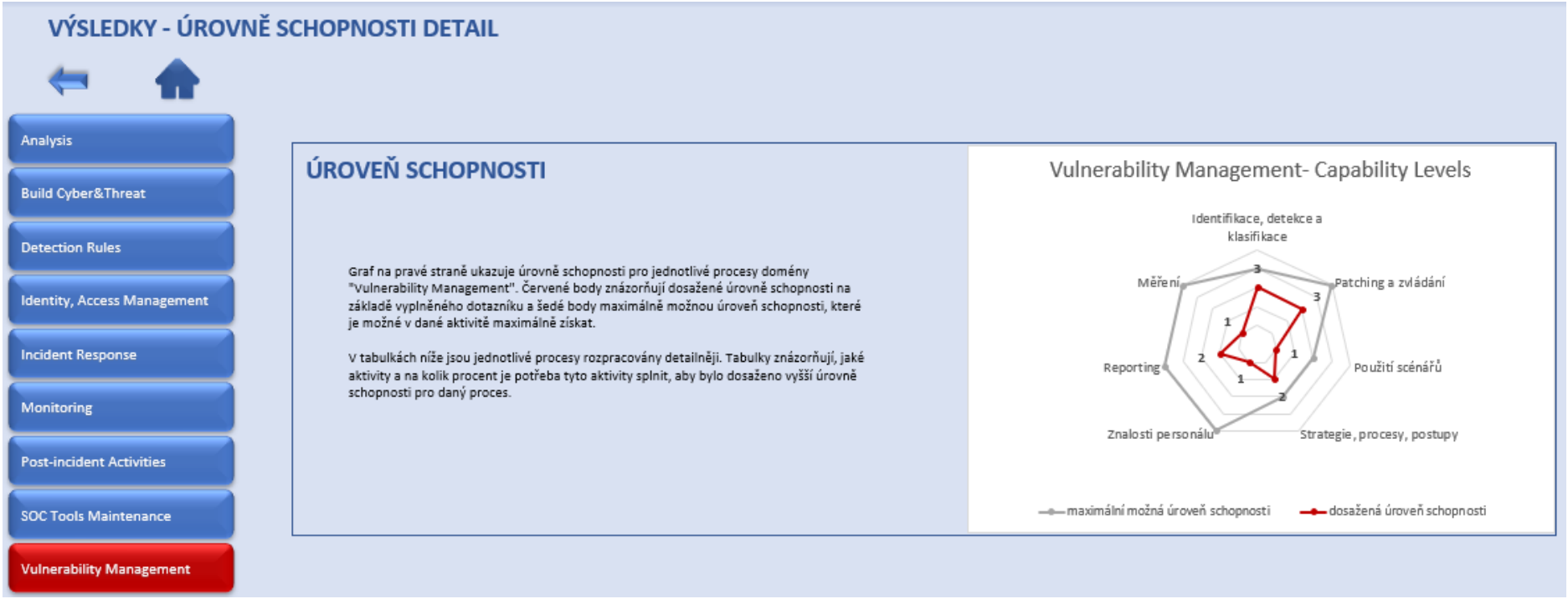
Obrázek D-2 Návod, jak pracovat s nástrojem (Zdroj: Autor)



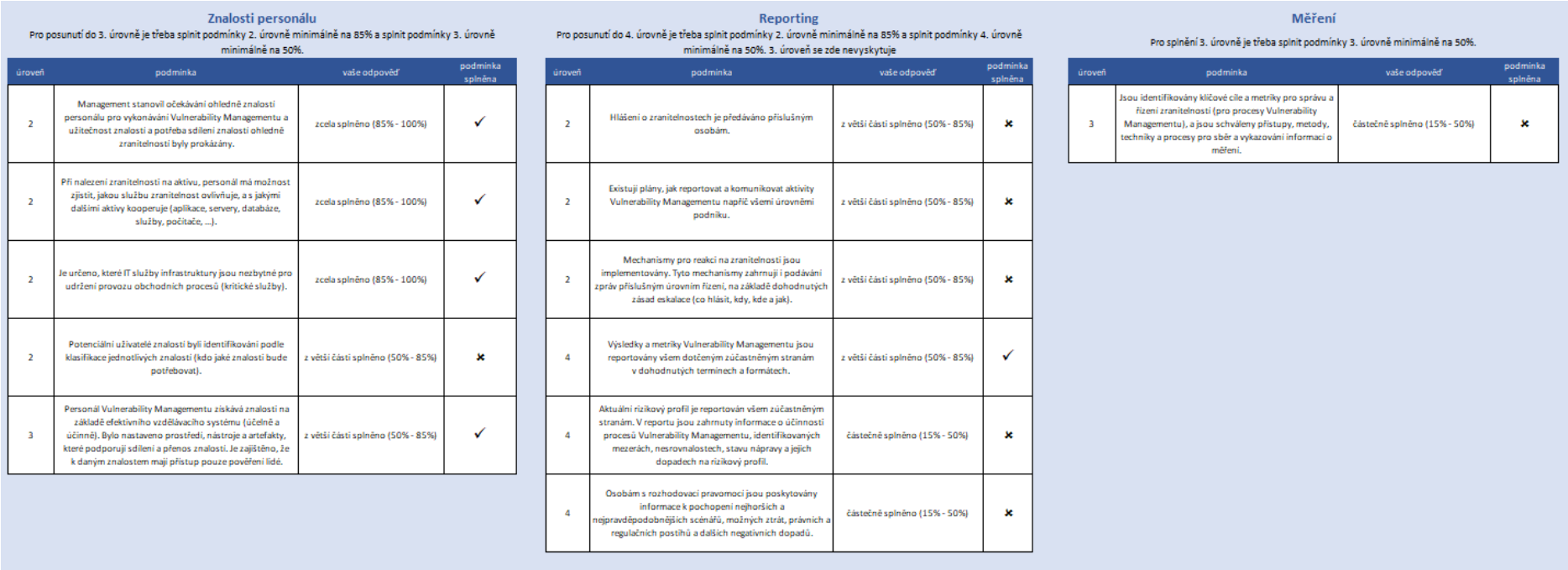
Obrázek D-3 Testové otázky domény Analysis (Zdroj: Autor)



Obrázek D-4 Dva druhy výsledků – rozcestník (Zdroj: Autor)



Obrázek D-5 Výsledné úrovně schopností domény Vulnerability Management (Zdroj: Autor)



Znalosti personálu

Pro posunutí do 3. úrovně je třeba splnit podmínky 2. úrovně minimálně na 85% a splnit podmínky 3. úrovně minimálně na 50%.

úroveň	podmínka	vaše odpověď	podmínka splněna
2	Management stanovil očekávání ohledně znalostí personálu pro vykonávání Vulnerability Managementu a užitečnost znalostí a potřeba sdílení znalostí ohledně zranitelností byly prokázány.	zcela splněno (85% - 100%)	✓
2	Při nalezení zranitelnosti na aktivu, personál má možnost zjistit, jakou službu zranitelnost ovlivňuje, a s jakými dalšími aktivy kooperuje (aplikace, servery, databáze, služby, počítače, ...).	zcela splněno (85% - 100%)	✓
2	Je určeno, které IT služby infrastruktury jsou nezbytné pro udržení provozu obchodních procesů (kritické služby).	zcela splněno (85% - 100%)	✓
2	Potenciální uživatelé znalostí byli identifikováni podle klasifikace jednotlivých znalostí (kdo jaké znalosti bude potřebovat).	z větší části splněno (50% - 85%)	✗
3	Personál Vulnerability Managementu získává znalosti na základě efektivního vzdělávacího systému (účelně a účinně). Bylo nastaveno prostředí, nástroje a artefakty, které podporují sdílení a přenos znalostí. Je zajištěno, že k daným znalostem mají přístup pouze pověření lidé.	z větší části splněno (50% - 85%)	✓

Reporting

Pro posunutí do 4. úrovně je třeba splnit podmínky 2. úrovně minimálně na 85% a splnit podmínky 4. úrovně minimálně na 50%. 3. úroveň se zde nevyskytuje

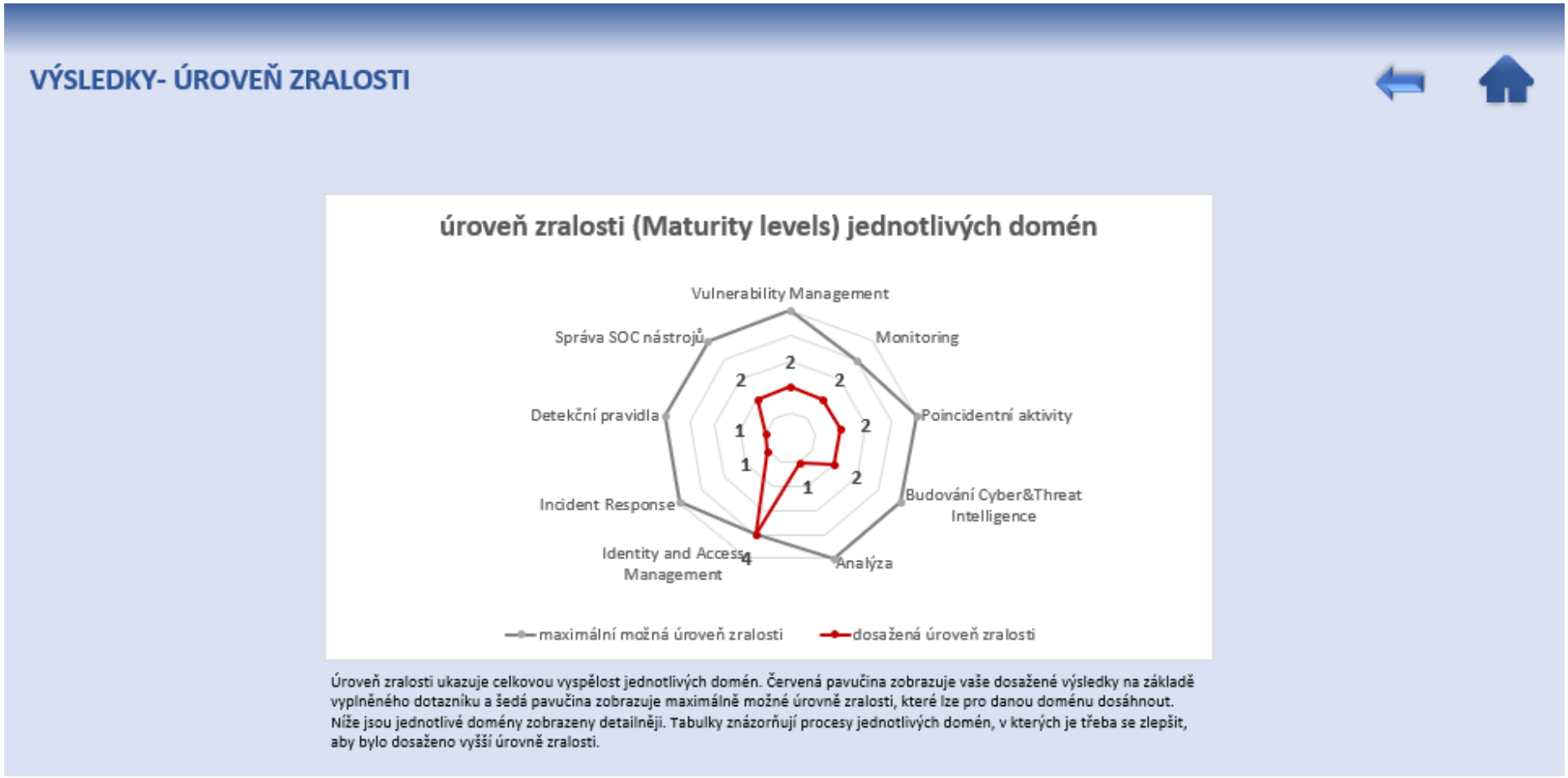
úroveň	podmínka	vaše odpověď	podmínka splněna
2	Hlášení o zranitelnostech je předáváno příslušným osobám.	z větší části splněno (50% - 85%)	✗
2	Existují plány, jak reportovat a komunikovat aktivity Vulnerability Managementu napříč všemi úrovněmi podniku.	z větší části splněno (50% - 85%)	✗
2	Mechanismy pro reakci na zranitelnosti jsou implementovány. Tyto mechanismy zahrnují i podávání zpráv příslušným úrovním řízení, na základě dohodnutých zásad eskalace (co hlásit, kdy, kde a jak).	z větší části splněno (50% - 85%)	✗
4	Výsledky a metriky Vulnerability Managementu jsou reportovány všem dotčeným zúčastněným stranám v dohodnutých termínech a formátech.	z větší části splněno (50% - 85%)	✓
4	Aktuální rizikový profil je reportován všem zúčastněným stranám. V reportu jsou zahrnuty informace o účinnosti procesů Vulnerability Managementu, identifikovaných mezerách, nesrovnalostech, stavu nápravy a jejích dopadech na rizikový profil.	částečně splněno (15% - 50%)	✗
4	Osobám s rozhodovací pravomocí jsou poskytovány informace k pochopení nejhorších a nejpravděpodobnějších scénářů, možných ztrát, právních a regulačních postihů a dalších negativních dopadů.	částečně splněno (15% - 50%)	✗

Měření

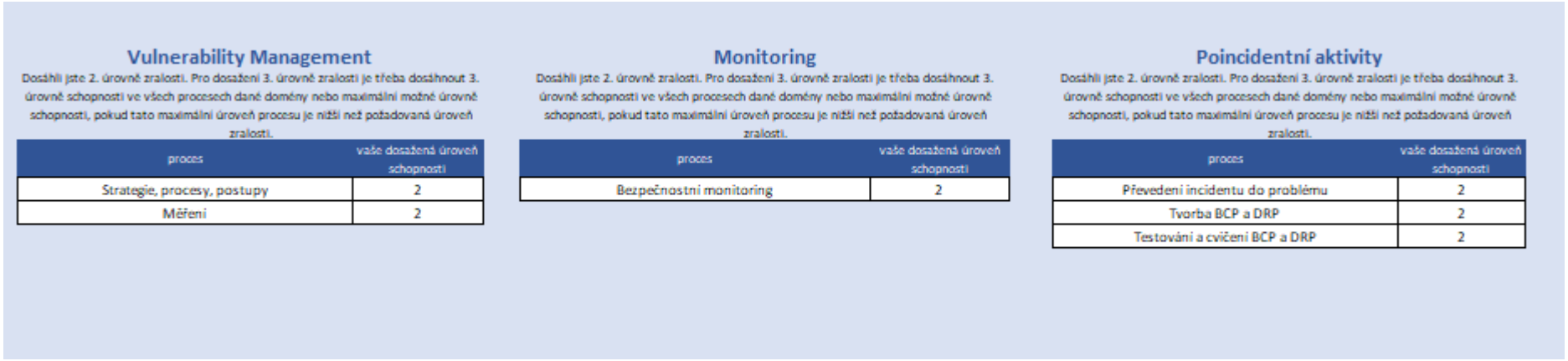
Pro splnění 3. úrovně je třeba splnit podmínky 3. úrovně minimálně na 50%.

úroveň	podmínka	vaše odpověď	podmínka splněna
3	Jsou identifikovány klíčové cíle a metriky pro správu a řízení zranitelností (pro procesy Vulnerability Managementu), a jsou schváleny přístupy, metody, techniky a procesy pro sběr a vykazování informací o měření.	částečně splněno (15% - 50%)	✗

Obrázek D-6 Přehled aktivit nutných pro dosažení vyšší úrovně schopnosti (Zdroj: Autor)



Obrázek D-7 Výsledky naměřených úrovní zralosti (Zdroj Autor)



Vulnerability Management

Dosáhli jste 2. úrovně zralosti. Pro dosažení 3. úrovně zralosti je třeba dosáhnout 3. úrovně schopnosti ve všech procesech dané domény nebo maximální možné úrovně schopnosti, pokud tato maximální úroveň procesu je nižší než požadovaná úroveň zralosti.

proces	vaše dosažená úroveň schopnosti
Strategie, procesy, postupy	2
Měření	2

Monitoring

Dosáhli jste 2. úrovně zralosti. Pro dosažení 3. úrovně zralosti je třeba dosáhnout 3. úrovně schopnosti ve všech procesech dané domény nebo maximální možné úrovně schopnosti, pokud tato maximální úroveň procesu je nižší než požadovaná úroveň zralosti.

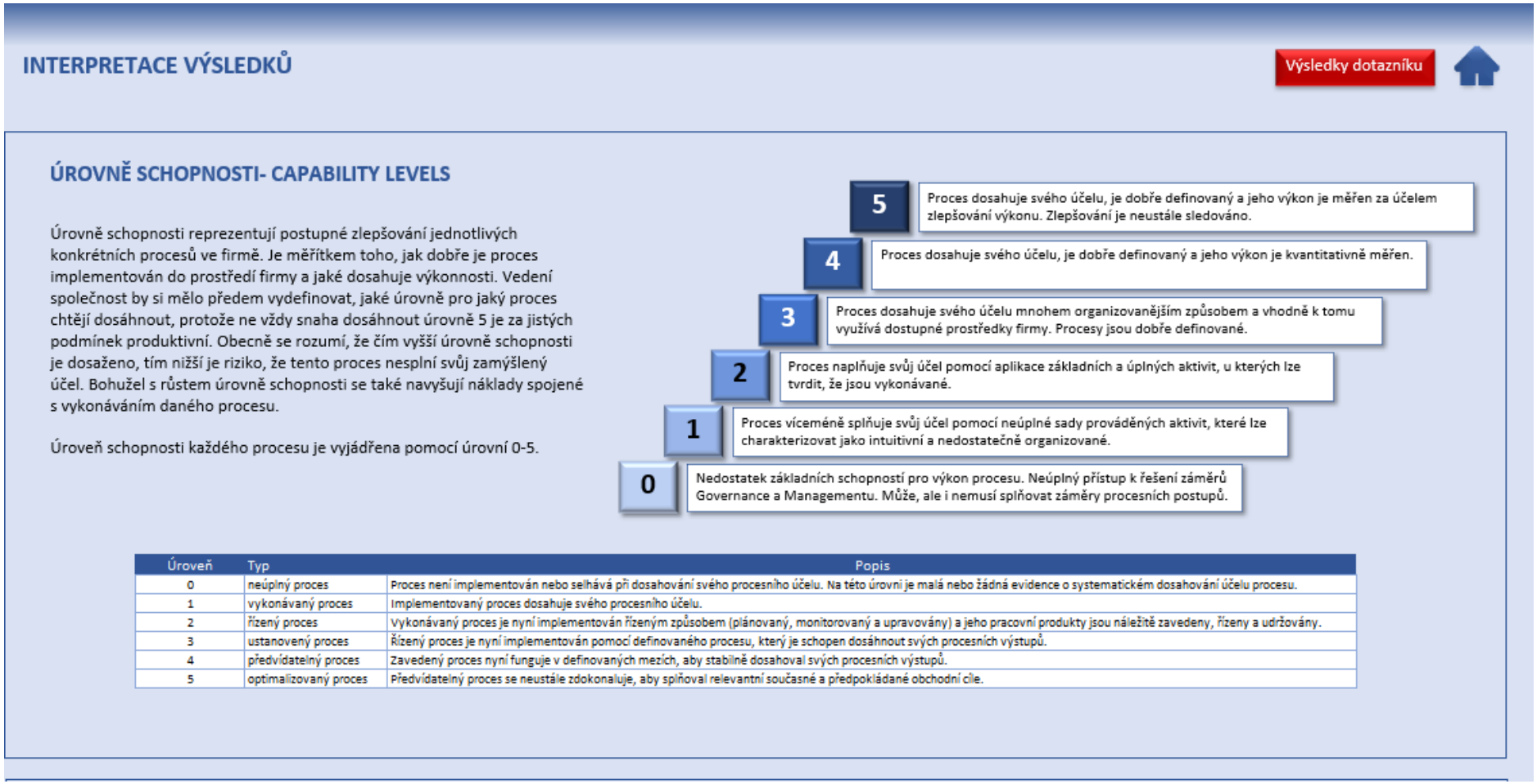
proces	vaše dosažená úroveň schopnosti
Bezpečnostní monitoring	2

Poincidentní aktivity

Dosáhli jste 2. úrovně zralosti. Pro dosažení 3. úrovně zralosti je třeba dosáhnout 3. úrovně schopnosti ve všech procesech dané domény nebo maximální možné úrovně schopnosti, pokud tato maximální úroveň procesu je nižší než požadovaná úroveň zralosti.

proces	vaše dosažená úroveň schopnosti
Převedení incidentu do problému	2
Tvorba BCP a DRP	2
Testování a cvičení BCP a DRP	2

Obrázek D-8 Domény, které je třeba zlepšit pro získání vyšší úrovně zralosti (Zdroj: Autor)



Úroveň	Typ	Popis
0	neúplný proces	Proces není implementován nebo selhává při dosahování svého procesního účelu. Na této úrovni je malá nebo žádná evidence o systematickém dosahování účelu procesu.
1	vykonávaný proces	Implementovaný proces dosahuje svého procesního účelu.
2	řízený proces	Vykonávaný proces je nyní implementován řízeným způsobem (plánovaný, monitorovaný a upravovány) a jeho pracovní produkty jsou náležitě zavedeny, řízeny a udržovány.
3	ustanovený proces	Řízený proces je nyní implementován pomocí definovaného procesu, který je schopen dosáhnout svých procesních výstupů.
4	předvídatelný proces	Zavedený proces nyní funguje v definovaných mezích, aby stabilně dosahoval svých procesních výstupů.
5	optimalizovaný proces	Předvídatelný proces se neustále zdokonaluje, aby splňoval relevantní současné a předpokládané obchodní cíle.

Obrázek D-9 Informace k interpretaci úrovní schopnosti a zralosti (Zdroj: Autor)