FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

ZADÁNÍ DIPLOMOVÉ PRÁCE

Název:	Možnosti využití metodiky DEMO pro modelování informační bezpečnosti
Student:	Bc. Hai Bui Phu
Vedoucí:	Ing. Pavel Náplava
Studijní program:	Informatika
Studijní obor:	Webové a softwarové inženýrství
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	Do konce letního semestru 2018/19

Pokyny pro vypracování

Analyzujte možnosti využití metodiky DEMO v oblasti informační bezpečnosti a na příkladech demonstrujte výhody/nevýhody tohoto přístupu. Postupujte následujícím způsobem:
1. Definujte pojmy informační bezpečnost, bezpečnostní incident.
2. Analyzujte existující normy a specifikace, popisující oblast informační bezpečnosti.
3. Seznamte se s metodikou DEMO a navrhněte způsob jejího použití pro modelování vybraných oblastí informační bezpečnosti.
4. Po dohodě s vedoucím práce vyberte vhodné oblasti informační bezpečnosti a namodelujte je pomocí metodiky DEMO.
5. Na vytvořených modelech demonstrujte různé bezpečnostní incidenty, spojené s chybným použitím modelu a poukažte na možné nevhodně navržené bezpečnostní opatření.
6. Vyhodnoťte smysluplnost využití metodiky DEMO pro navrhování a řízení informační bezpečnosti, pokuste se vyhodnotit přínosy a náročnost využití metodiky DEMO pro tyto účely.

Seznam odborné literatury

Dodá vedoucí práce.

Ing. Michal Valenta, Ph.D.
vedoucí katedry

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
děkan

V Praze dne 26. prosince 2017

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Diplomová práce

Možnosti využití metodiky DEMO pro modelování informační bezpečnosti

Bc. Bui Phu Hai

Katedra softwarového inženýrství
Vedoucí práce: Ing. Pavel Náplava

9. května 2018

Poděkování

Na tomto místě bych rád poděkoval vedoucímu mé práce, Ing. Pavlu Náplavovi, za jeho způsob vedení diplomové práce a volný čas, který mi při vypracování diplomové práce věnoval. Poděkování patří též korektorovi, kamarádovi Jardovi Vašákovi, který přispěl ke zkvalitnění této práce. Poděkování patří i mým přátelům, díky nim bylo studium mnohem zajímavější. V poslední řadě, a hlavně, bych rád poděkoval mé rodině a sestře, kteří mi byli oporou při studiu a při návratu domu mi vždy upekla dort.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval(a) samostatně a že jsem uvedl(a) veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona.

V Praze dne 9. května 2018 .....

Odkaz na tuto práci

Bui Phu, Hai. *Možnosti využití metodiky DEMO pro modelování informační bezpečnosti*. Diplomová práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2018.

Abstrakt

Tato práce se zabývá modelováním informační bezpečnosti a využití doporučeních z norem ČSN ISO/IEC pro informační bezpečnost. Rozšířením o grafické elementy pro modelování procesů a informační bezpečnosti v DEMO metodice jsem demonstroval na modelovém příkladu. Tyto rozšiřující grafické elementy pomáhají uživatelům neopomenout na důležitá bezpečnostní opatření celé organizace.

Klíčová slova procesy, BPMN, DEMO, informační bezpečnost, ISO/IEC 27001, ISO/IEC 27005, GDPR

Abstract

The thesis will present a way of modelling of information security and use recommendations from ISO/IEC standards for information security. By extending graphical elements for process modelling and information security in DEMO methodology I will demonstrate on a model case. These expanding graphical elements help users not to neglect important security measures across the organization.

Keywords processes, BPMN, DEMO, information security, ISO/IEC 27001, ISO/IEC 27005, GDPR

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Motivace

IT technologie zažívá rozmach od poloviny minulého století a současné organizace se bez IT technologií neobejdou. Technologie jsou dnes nedílnou součástí každé fungující a rostoucí organizace, která se chce prosadit na trhu. Organizace musí zpracovávat velké množství dat, které se stávají i nejcennějším aktivem organizace. Těchto citlivých informací není málo a s každým rokem toto množství informací roste exponenciální rychlostí a je potřeba tyto informace chránit. S komplexností množství informací roste i komplexnost zabezpečení IT.

Dnes jsou procesy v organizaci zaznamenávány pomocí různých metodik a notací, počínaje flow charty, BPMN notací, UML notací, až po různé matice rizik a jak následně řešit konkrétní bezpečnostní incidenty. Jsou toho plné kartotéky těchto dokumentací a pro jednoho člověka je nemožné, aby si udržel přehled všech detailů, obzvlášť potom rozeznat, co je podstatné pro tu danou organizaci. Lidská krátkodobá paměť podle nejznámějšího výzkumu G. Millera [13] říká, že jsme schopni si udržet v krátkodobé paměti 7 a +-2 informací, tzn. v rozmezí 5–9 informací. Byť se zdá, že dat, informací – jak jsou si mezi sebou propojené, jaké mají mezi sebou vazby – je hodně, tak toho podstatného, není moc, aby si člověk nedokázal udržet v krátkodobé paměti. Jenom je k tomu potřeba vhodný nástroj nebo model pro zachycení skutečnosti.

Na informační bezpečnost je potřeba pohlížet jako na průběžný inovovaný proces. Informační bezpečnost není pouze o IT technologiích, ale je to také o lidském přístupu k bezpečnosti jako takové. Aby člověk měl přehled, co se vše skrývá v organizaci, potřebuje mít přehledný nástroj nebo model, který mu poukáže na možné faktory, které mohou být příčinou vzniku možných slabých míst v zabezpečení v organizaci. Mít velký přehled[1], co je s čím provázané.

[1] Někdy známý jako *Big Picture*.

Cíle práce

Cílem práce je vybrat vhodné oblasti informační bezpečnosti a namodelovat je pomocí metodiky DEMO. Na vytvořených modelech budu demonstrovat různé případy v transakci (podprocesu), které povedou různým vyhodnocením dopadu na aktivum v organizaci. Tato diplomová práce si neklade za cíl komplexní vyhodnocení bezpečnostních incidentů, ale má poukázat na možnosti identifikace kritických míst, kde může nastat bezpečnostní incident a organizace sama rozhodne, zda-li danou bezpečnostní událost řešit, či ne.

V diplomové práci se pokusím uchopit komplexnost informací a s tím spojená informační bezpečnost do modelu, který mi na první pohled napoví, kde jsou možná kritická bezpečnostní místa dané organizace.

Struktura práce

Celá diplomová práce je tvořená pěti kapitoly, pomocí kterých se pokusím naplnit stabivené cíle.

1. kapitola – vymezení pojmu informační bezepčnost a analýza existujícíc norem a specifikací týkající informační bezpečnosti.
2. kapitola – od propisu procesů k metodice DEMO. Pro navržení něčeho nového je důležité pochopit, jak se přístup k podnikovým procesům vyvíjel.
3. kapitola – popis potřebných konstruktů z norem ČSN ISO/IEC, BPMN notace a metodiky DEMO.
4. kapitola – aplikace potřebných konstruktů popsané ve třetí kapitole na modelovém příkladu týkajícího se informační bezpečnosti.
5. kapitola – shrnutí, co vzešlo z praktické části.

Kapitola 1

Informační bezpečnost

1.1 Proč se zabývat informační bezpečností

Už v minulosti si Julius Caesar [11] uvědomil důležitost doručování zpráv během bitev. Kdyby se důležitá zpráva dostala do rukou nepřítele, celá bitva se mohla stát osudnou pro Caesara. Přenášené zprávy byly potřeba zabezpečit a tak vznikla jedna z prvních bezpečnostních opatření v oblasti komunikace – *šifrování zprávy* pomocí substituční metody. Princip substituční metody spočíval v posunu celé abecedy a k jeho dešifrování jste potřebovali znát číslo, o kolik byla zpráva posunutá.

Tabulka 1.1: Numerický ekvivalent písmenům anglické abecedy pro posun v substituční šifře. Zdroj: [11].

Písmeno	A	B	C	D	E	F	G	H	I	J	K	L	M
Num. ekv.	0	1	2	3	4	5	6	7	8	9	10	11	12
Písmeno	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Num. ekv.	13	14	15	16	17	18	19	20	21	22	23	24	25

IT technologie zažívá velký rozmach od poloviny minulého století a pro prosazení se na trhu se dnešní organizace bez nich neobejdou. Kdo chce jít dopředu, musí jít s dobou. Dnes to znamená investovat do technologií, zejména do těch IT. Uchovávaná data jsou zpracovávaná ve velkém množství a informace z nich získané se pro firmu stává jeho nejcennějším aktivem. Metody zpracování dat jsou neustále zdokonalovány a správné vyhodnocení informací přináší organizacím konkurenční výhody. Z toho plyne, analogie se zasíláním šifrovaných zpráv za dob Juliuse Caesara, že informace jednoho podniku jsou velice užitečné pro jiný podnik a to vyvolává potřebu tyto data chránit.

Obrázek 1.1: Poznávací hierarchie. Zdroj: [1]

1.2 Informační bezpečnost

Přesná definice, co je to informační bezpečnost[1] neexistuje. Každý uživatel, organizace, tento pojem chápe trošku jinak a záleží z jaké disciplíny jsou tito uživatelé, organizace, a podle toho se pak liší vymezení pojmu informační bezpečnost (např. úzké disciplíny zabývající se výhradně bezpečnosti informačních a komunikačních technologií). Pro mojí diplomovou práci zde uvedu dvě převzaté definice:

- *„Informační bezpečnost znamená komplexní pohled, který organizaci pomáhá poznat a chránit své cenná data a také vede praktickými opatřeními k eliminaci či výraznému snížení dopadů v případě mimořádných událostí.“* [18]
- *„Souhrn prostředků a postupů na zabezpečení důvěrnosti, integrity a dostupnosti informací, na zabezpečení autentizace uživatelů a zdrojů, účtovatelnosti operací, jakož i zabezpečení ochrany proti neautorizované manipulaci, modifikaci nebo zničení, resp. poškození informací v informačním systému.“* [10]

[1] V anglickém jazyce se lze setkat se zkratkou *InfoSec* od slovního spojení *Information Security*

Do informační bezpečnosti se zahrnují oblasti jako je problematika datových přenosů, ochrana počítačových sítí, kabelových i bezdrátových propojení, ochrana před vnějšími i vnitřními útoky, autentizace, autorizace, fyzická ochrana budov, proškolování personálu, definice aktiv podniku a jejich zabezpečení, identifikace a analýza rizik, scénáře obnovy dat při nenadálých událostech, zajištění dostupnosti dat, zálohování, definování dodržování bezpečnostních směrnic atd.

Lze vidět, že problém informační bezpečnosti je komplexní záležitost. Každé organizace se od sebe liší a tak se budou lišit i nároky na zavedení informační bezpečnosti do konkrétní organizace. Začlenění informační bezpečnosti se netýká pouze IT technologií. Hraje v něm roli i lidský faktor a je potřeba zapojit celý personál napříč organizací k přispění ucelené bezpečnosti.

1.2.1 Bezpečnostní incident

Při řešení informační bezpečnosti se snažíme zamezit vzniku informačních incidentů. Informační incident je událost, která vede k narušení pravidel bezpečnosti organizace. [12]

Příklady bezpečnostních incidentů: Krádež, neoprávněný přístup k datům nebo informacím, neoprávněné použití informací, neoprávněný vstup do budovy nebo do systému, smazání dat ze systému, selhání infrastruktury nebo připojení, hackerský útok, penetrace do systému, virový útok,přírodní katastrofa, atd.

Podle své povahy lze bezpečnostní incidenty rozdělit na:

- *Informační bezpečnostní incident* – narušení důvěrnosti, celistvosti, dostupnosti nebo neodmítnutelnosti informace.
- *Personální informační incident* – narušení osobního bezpečí.
- *Bezpečnostní incident fyzické povahy* – narušení bezpečí na fyzickém majetku nebo infrastruktuře (např. vloupání).

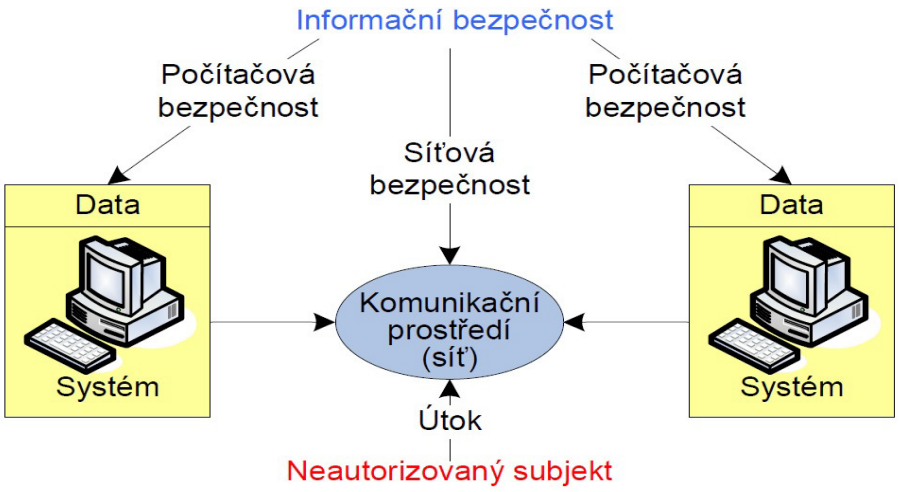
1.2.2 Obecné pojmy informační bezpečnosti

Níže v seznamu jsou uvedeny pojmy týkající se informační bezpečnosti [21][25]:

- *Aktiva (Assets)* – majetek podniku či hospodářské prostředky. Pod pojmem majetek rozumíme souhrn všech věcí, peněz, pohledávek a jiných majetkových hodnot, které patří podnikateli a slouží k podnikání. Aktiva jsou prostředky kontrolované podnikem, u kterých se předpokládá, že přinesou podniku budoucí ekonomický užitek.
- *Autentizace (Authentication)* – Proces k určení identity uživatele nebo jiné entity.

- *Autorizace (Authorization)* – Proces udělování práv subjektům, které jim umožňují přístup k síťovým zdrojům.
- *Bezpečnost informací (Information security)* – zachování důvěrnosti, integrity a dostupnosti informací.
- *Celistvost (Integrity)* – jsou jasně stanoveny pravomoci a práva k pozměňování informací či dat.
- *Data (Data)* – kolekce hodnot přiřazených k základním mírám, odvozeným mírám a/nebo indikátorům.
- *Dostupnost (Availability)* – data jiného zařízení jsou k dispozici v okamžiku jejich potřeby. Vyjadřuje se v procentech dostupného času.
- *Důvěrnost (Confidentiality)* – k informacím či datům mají přístup pouze oprávněné osoby.
- *Kompetence/odborná způsobilost (Competence)* – schopnost použít znalosti a dovednosti k dosažení zamýšlených výsledků.
- *Monitorování (Monitoring)* – určování stavu systému, procesu nebo činnosti.
- *Možnost výskytu (Likelihood)* – možnost, že něco nastane.
- *Neustále zlepšování (Continual improvement)* – opakovaná činnost vedoucí k zvyšování výkonnosti.
- *Rozhodovací kritéria (Decision criteria)* – prahy, cíle nebo vzory, které se používají k určení potřeby akce nebo dalšího zkoumání, nebo k popisu úrovně důvěry v daný výsledek.
- *Spolehlivost (Reliability)* – soulad mezi zamýšleným chováním a výsledky.
- *Událost (Event)* – výskyt nebo změna určité množiny okolností.
- *Útok (Attack)* – pokus o zničení, vystavení hrozbě, změnu, vyřazení z činnosti, zcizení aktiva nebo získání neoprávněného přístupu k aktivu nebo uskutečnění neoprávněného použití aktiva.
- *Úroveň rizika (Level of risk)* – velikost rizika vyjádřená jako kombinace následků a jejich možnosti výskytu.
- *Zainteresovaná strana (Interested party)* – osoba nebo organizace, která může ovlivnit rozhodnutí nebo činnost, nebo může být ovlivněna, popřípadě se může cítit být ovlivněna rozhodnutím nebo činností.
- *Zranitelnost (Vulnerability)* – slabé místo aktiva nebo opatření, které může být využito jednou nebo více hrozbami.

1.3 Komunikační bezpečnost



Obrázek 1.2: Komunikační bezpečnost. Zdroj: [10].

Informační technologie jsou založeny na komunikaci a tato oblast se stává rizikovým místem pro nežádoucí útok s cílem získání informací. Cílem organizace je vytvořit takovou komunikační infrastrukturu, která bude splňovat základní požadavky komunikace mezi systémy. S rostoucí komplexností komunikační infrastruktury rostou nároky na informační bezpečnost.

Atributy bezpečnosti, které by měla komunikační infrastruktura v organizaci splňovat je důvěryhodnost a autenticita přenášených dat (příklad: poslání e-mailové pošty).

Komunikační kanály se stávají potenciální hrozbou stejně jako je tomu u vydobytí citlivých informací z informačních systémů. Zavádění bezpečnosti na komunikačních kanálech je nákladnější než u fyzického zabezpečení. Je to z důvodů větší investice do pravidelného vzdělávání zaměstnanců, provádění pravidelných kontrol komunikační infrastruktury a zavádění nových možností komunikace napříč systémy (př. přechod z fax $\rightarrow$ e-mail: zavedení firewall, vzdělání zaměstnanců, co smějí a nesmějí posílat v e-mailu, pravidelná kontrola e-mailového serveru).

1.4 Riziko

IT riziko

Převzatá definice IT rizika z normy ISO/IEC 27005[23]:

„Riziko bezpečnosti informací je spojeno s možností, že hrozby využijí zranitelnosti informačních aktiv nebo jejich skupin, a tak způsobí škodu organizaci.“

IT riziko lze chápat jako jakákoliv hrozba, která souvisí s informačními technologiemi. Hrozbám je třeba předcházet, protože jejich výskyt má neblahé následky na informační aktiva organizace. Důkladnou a pravidelnou analýzou možných hrozeb v organizaci jsme potom schopni se jim vyhnout, minimalizovat dopady, když nastanou, a popřípadě být připraveni přijmout jejich následky.

Možné dopady hrozeb na organizaci:

- Ztráta výnosů,
- snížení efektivity (produkce)
- poškození reputace,
- zvýšení nákladů,
- právní spory,
- ohrožení cash-flow[1].

Kategorizace hrozeb

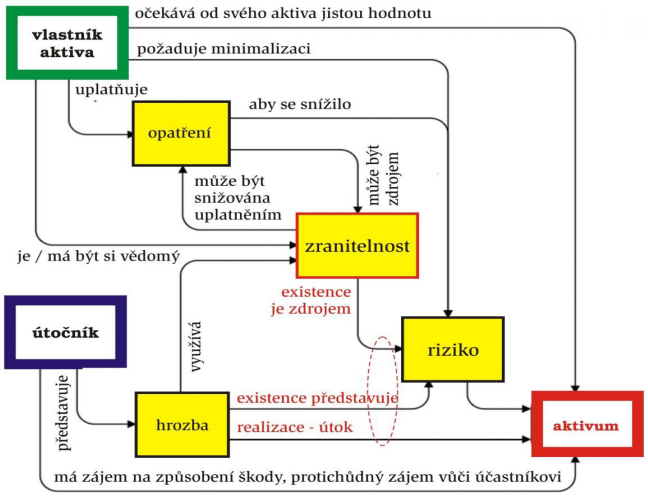
IT technologie jsou nedílnou součástí dnešního fungování organizace a při jejich využívání se nelze vyhnout hrozbám. Hrozby, které ohrožují informační systémy, lze rozdělit do několika skupin. Dle Doucka [3] je dělíme na:

- *Přírodní a fyzické* – živelné pohromy a nehody jako jsou např. poruchy v dodávce elektrického proudu, požáry, povodně, hurikány, vichřice apod.
- *Technické a technologické* – poruchy nosičů dat, počítačů nebo jiných technologických komponent ICT, poruchy sítí, poruchy způsobené programy – nesprávná funkčnost např. nedostatečné otestované programové vybavení, viry, trojské koně, atd.

[1] Cash-flow, česky peněžní tok, je definován jako příjem a výdej peněžních prostředků

- *Lidské* – ty dále dělíme na *úmyslné* a *neúmyslné*.
  - *Neúmyslné* – vyplývají z neznalosti nebo zanedbání plnění povinností.
  - *Úmyslné* – dělíme na působící *zvenku* (hackeři, teroristé, mezi firemní špionáž, ...), nebo *zevnitř* (zlomyslní, zneuznaní, chamtivý zaměstnanci, hosté a návštěvníci organizace, ...).

1.5 Obecný model zabezpečování



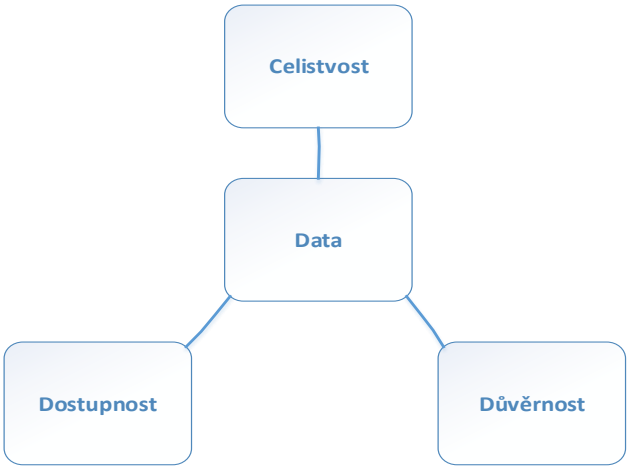
Obrázek 1.3: Obecný model zabezpečování. Zdroj [20].

Zajišťování informační a komunikační bezpečnosti, obecně bezpečnost ICT, je dlouhodobý kontinuální proces zlepšování. Zlepšování v nalézání potenciálního výskytu bezpečnostního incidentu a rozvíjení schopnosti pružně na ně reagovat.

Bezpečnost ICT je globálním problémem, kde je možné na něj nalézt *„kuchařky“*. Tyto kuchařky obsahují nejlepší postupy jak řešit problémy a vycházejí ze zkušenosti ostatních, které už podobný problém řešili. Při jejich aplikování, dodržování a po certifikaci, je možné organizaci považovat za bezpečného partnera v obchodním styku.

Při pohledu na schéma modelu bezpečnosti informačních technologií (viz. Obrázek [1.3]) je třeba si všimnout, že zde nefigurují pouze IT technologie. Model využívaný k řešení informační bezpečnosti totiž obsahuje mnohem více a

zahrnuje mimo bezpečnost IT, také bezpečnost personální, infrastruktury, budov a prostředí, požární a poplašné systémy, kontroly přístupu, atd. Při dbání na informační bezpečnost v organizaci, ať už se jedná o technologické zabezpečení nebo lidský přístup, je potřeba systematicky dodržovat základní atributy – *důvěrnost*, *celistvost* a *dostupnost*[1] informací a relevantních informačních systémů v organizaci (informačních aktiv).



Obrázek 1.4: Základní atributy pro zajištění informační bezpečnosti – celistvost, dostupnost a důvěrnost. Zdroj [Autor].

1.6 Zákony a normy regulující informační bezpečnost

1.6.1 Zákony v legislativě České republiky

V legislativě České republiky lze nalézt několik zákonů, které by mohly mít vliv na oblast informační bezpečnosti. Cílem této práce není podrobný popis jednotlivých zákonů a jejich komentování. Proto v následujících řádcích ve stručnosti uvedu seznam zákonů a zvídavý čtenář si může jejich plné znění dohledat v zákoníku České republiky.

- *Zákon č. 101/2000 Sb., o ochraně osobních údajů* – práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva

[1] CIA – Confidentiality (C), Integrity (I), Availability (A)

a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států. V květnu 2018 bude nahrazen nařízením EU GDPR – General Data Protection Regulation.

- *Zákon č. 181/20114 Sb., o kybernetické bezpečnosti* – upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.
- *Vyhláška ČNB č. 163/2014 Sb. o pravidlech obezřetného podnikání bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry* – upravuje používání Cloudu v bankovním sektoru.
- *Zákon č. 563/1991 Sb., o účetnictví* – upravuje rozsah a způsob vedení účetnictví, požadavky na jeho průkaznost, rozsah a způsob zveřejňování informací z účetnictví a podmínky předávání účetních záznamů pro potřeby státu.
- *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti* – upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.
- *Zákon č. 365/2000 Sb., o informačních systémech veřejné správy* – stanoví práva a povinnosti, které souvisejí s vytvářením, správou, provozem, užíváním a rozvojem informačních systémů veřejné správy spravovaných státními orgány nebo orgány územních samosprávných celků.

1.6.2 Rodina norem ISO/IEC 27000

Obrázek 1.5: Vztahy mezi normami řady ISMS. Převzato [25].

ISO/IEC 27000[1], obecné značení *ISO/IEC číslo normy:xxxx* (xxxx značí rok vydání/aktualizace normy), je rodina mezinárodních norem zaměřená na řízení informační bezpečnosti v organizacích. Všechna série norem ISO/IEC 27000 byly vydány Mezinárodní organizací pro normalizaci v roce 2005.

Normy specifikující požadavky

- *ISO/IEC 27001 Systém řízení bezpečnosti informací – Požadavky* — hlavní norma pro Systém řízení bezpečností informací (ISMS). Tato mezinárodní norma specifikuje požadavky na ustavení, implementaci, provozování, monitorování, přezkoumávání, udržování a zlepšování formalizovaných systémů řízení bezpečnosti informací (ISMS) v kontextu celkových rizik činnosti organizace. Specifikuje požadavky na implementaci opatření bezpečnosti informací upravených podle potřeb jednotlivých organizací nebo jejich částí. Tuto mezinárodní normu mohou používat všechny organizace bez ohledu na typ, velikost a povahu.

- *ISO/IEC 27006 Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací* — specifikuje požadavky a poskytuje pokyny pro orgány provádějící audit a certifikaci ISMS v souladu

[1] Všechny normy jsou dostupné zdarma v Národní technické knihovně v Dejvicích ve 3. patře v tiché studovně.

s ISO/IEC 27001. Je určena především k podpoře akreditace certifikačních orgánů, provádějící certifikaci ISMS podle ISO/IEC 27001.

Normy popisující obecné směrnice

- *ISO/IEC 27002 Soubor postupů pro opatření bezpečnosti informací* —

- *ISO/IEC 27003* — poskytuje seznam obecně akceptovaných cílů opatření a opatření pro doporučené postupy, které mají být použity jako pokyny k implementaci při výběru a provádění opatření, jejich cílem je dosáhnout bezpečnosti informací.

- *ISO/IEC 27004 Řízení bezpečnosti informací – Měření* — je pro organizace pomůckou k měření a prezentaci efektivity jejich systémů řízení bezpečnosti informací (ISMS), zahrnující řídící procesy definované v ISO/IEC 27001 a opatření z ISO/IEC 27002.

- *ISO/IEC 27005 Řízení rizik bezpečnosti informací* — poskytuje směrnice pro řízení rizik bezpečnosti informací. Přístup popsaný v této mezinárodní normě podporuje obecná pojetí specifikovaná v ISO/IEC 27001.

- *ISO/IEC 27007 Směrnice pro audit systémů řízení bezpečnosti informací* — poskytuje pokyny na provádění auditů ISMS a pokyny popisující odbornou způsobilost (kompetenčně) auditorů systémů řízení bezpečnosti informací vedle pokynů obsažených v ISO 19011, který je obecně použitelný na systémy řízení.

- *ISO/IEC 27008 Směrnice pro auditory kontrolních opatření bezpečnosti informací* — poskytuje pokyny na přezkoumávání implementace a provozování opatření včetně kontroly technické shody opatření informačních systémů podle norem bezpečnosti informací ustavených danou organizací.

ISO/IEC 27000 je rodinou norem v seznamu výše uvedených položek. Je patrné, že celkový výčet norem ze seznamu ISO/IEC 27000 je nemalý (zbylé lze nalézt v n. ISO/IEC 27000). V praxi stačí zavést pouze ty, které řeší dané problémy konkrétní organizace.

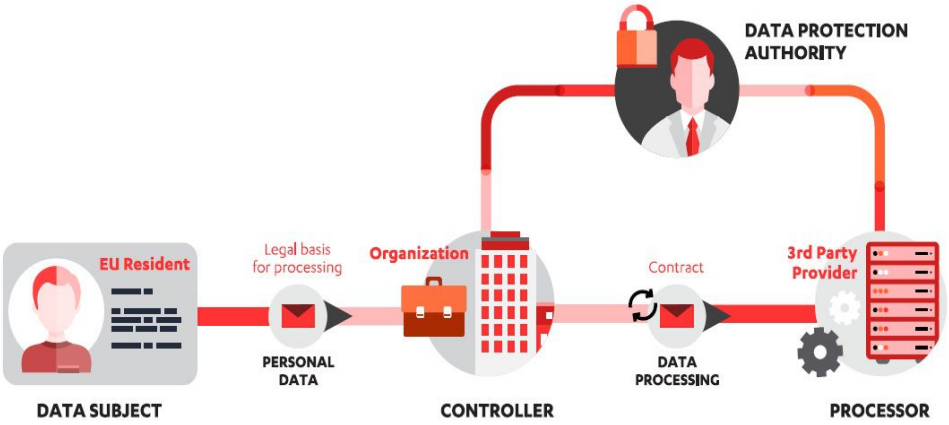
Pro tuto práci jsou klíčové tyto dvě normy: *ISO/IEC 27001:2014 (369790)* a *ISO/IEC 27005:2013 (369790)*.

1.7 GDPR

1.7.1 Nové nařízení o ochraně osobních údajů

Obecné nařízení o ochraně osobních údajů[1] (General Data Protection Regulation, GDPR) [26] je nová legislativa EU, která má chránit osobní údaje uživatelů napříč všemi zeměmi, které jsou členy EU. Nařízení GDPR bylo schváleno už v roce 2016 a v platnost nabude až letos 25. května 2018 a na území České republiky nahradí tím stávající Zákon č. 101/2000 Sb., o ochraně osobních údajů. Všechny dotčené organizace v rámci Evropské unie, které pracují s osobními údaji, dostaly dva roky na přípravu k uplatnění nutných změn ke splnění podmínek nařízení GDPR.

1.7.2 Pojmy



Obrázek 1.6: Hlavní pojmy a vztahy GDPR. Zdroj: [6].

Na obrázku 1.6 jsou znázorněny vztahy mezi jednotlivými pojmy. [5]

- *Subjekt údaje (Data Subject)* – Subjektem údaje se rozumí fyzická osoba, ne právnická, která vlastní osobní údaj. Vždy se musí jednat o žijící fyzickou osobu.

- *Osobní údaj (Personal Data)* – nařízení GDPR se vztahuje pouze na osobní údaje. Osobními údaji se rozumí veškeré informace týkající se identifikování nebo identifikované osoby, přímo či nepřímo, subjektu údajů. Identifikátorem může být jméno, identifikační číslo, údaje o poloze nebo online identifikátor.

[1] Plné znění si lze přečíst na: `http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1501688126470&uri=CELEX:32016R0679`

- *Správce (Controller)* – Správce údajů je ten, který sám nebo společně s ostatními určuje účel a prostředky zpracování osobních údajů. Typicky bývá organizace a správce může být jak fyzická, tak právnická osoba.

- *Zpracování dat (Data Processing)* – podle nařízení GDPR *„je jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.“*

- *Zpracovatel (Processor)* – je fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.

1.7.3 Pověřenec pro ochranu osobních údajů

Důležitým pilířem prokazování souladu s nařízením GDPR je jmenování pověřence pro ochranu osobních údajů (Data Protection Officer, DPO). Hlavním úkolem DPO bude monitorování souladu zpracování osobních údajů s povinnostmi vyplývajícími z nařízení, provádění interních auditů, školení pracovníků a celkové řízení agendy interní ochrany dat. Jmenování pověřence nastává v případech, pokud:

1. zpracování provádí orgán veřejné moci či veřejný subjekt (s výjimkou soudů),

2. hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování občanů,

3. hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

Cílem této diplomové práce není se dopodrobna zabývat, co je to GDPR. Vymezil jsem ty nejpodstatnější informace o obecném nařízení, aby se čtenář seznámil se základními pojmy a konceptem GDPR. Další důvod, proč jsem se zmínil krátkou kapitolou o GDPR je, že v praktické části budu demonstrovat na procesech různé situace, které se týkají informační bezpečnosti a budu brát v potaz i práci s osobními údaji.

Kapitola 2

Od popisu procesů k metodice DEMO

2.1 Procesy

Samotné lidstvo už počátku své existence má tendenci si věci zjednodušovat a dělat vše pro to, aby za co nejméně vynaloženého úsilí dostalo co nejlepší výsledek. Uvědomilo si, že pokud k upečení chleba Josef Pekařů dokáže nahnětat těsto a napéct 150 ks chleba za jeden den a Karel Mlejnek jenom 50 ks, za to Karel dokáže namlít mouku na 150 ks chleba a ten samý Josef Pekařů pouze na 50 ks za den, tak je výhodnější, aby Karel jenom mlel mouku a Josef dělal samotný chléb a výsledek si rozdělili mezi sebou na půl, tzn. 75 chlebů každý. Oba budou mít víc chlebů, když si rozdělí práci na to, kdo je v čem zdatnější, než aby každý dělali celý proces od začátku do konce sami. Chápání dílčích procesu se stalo pro lidstvo denním chlebem.

2.1.1 Historie procesů

Tradičně řízená společnost v 18. století měla pyramidovou organizační strukturu, v níž se každý vedoucí snažil maximalizovat výkon svého oddělení. V dnešní době ještě některé společnosti používají pyramidovou strukturu, ale nefungují tak dobře. Náš svět se změnil a již nestačí čerpat z teorie spontánního řádu Adama Smithe, který ve své knize *O původu bohatství národů* v r. 1776 napsal, že svoboda, konkurence a dělba práce jsou nezbytnými předpoklady bohatství všech členů společnosti, a stal se díky tomu jedním z nejvýznamnějších světových ekonomů svých dob. Mezi základní myšlenky A. Smithe, jak zvýšit efektivitu společnosti [8], patří:

- Specializace dělníka na jednu operaci, což vedlo ke vzniku manufaktur.
- Rozmístění jednotlivých profesí a dodávaného zboží.

- Vztah mezi zaměstnavatelem a zaměstnancem, při kterém zaměstnavatel zajišťuje prostřednictvím zaměstnanců navýšení svého kapitálu, čímž zvyšuje možnost zaměstnávat další zaměstnance, takže tento vztah je oboustranně výhodný.

Další vývojové kroky přinesli jiní významní ekonomové Henry Ford a Alfred Sloan. Tito pánové si uvědomili, že k vytvoření výrobku jako celku se skládá z více menších kroků. Zavedli tzv. *pásovou výrobu*, která spočívala v posloupnost skládaní jednotlivých kroků do většího celku. Každý byl zodpovědný za konkrétní pohyb (část pásu jenom šroubovala, další část jenom tloukla hřebík, atd.). Položili základ složitějšímu systému řízení, jenž se vyznačuje plánovitostí a kontrolou a v podstatě je platný dodnes.

2.1.2 Význam procesů

Proces (někdy též jako business proces) je podle normy 27000 [25] definován jako neustále se opakující činnost, která má vstup a výstup. Každá organizace je v podstatě organizovaná soustava procesů a činností, která na sebe vzájemně navazují, vzájemně komunikují, probíhají napříč organizačními jednotkami, reagují na různé podněty z vnitřního i vnějšího prostředí. V procesech se transformují *vstupy* a *zdroje* na *výstupy*, které zhodnocuje zákazník procesu.

Proč se společnosti stále zabývají procesy, výhody plynoucí ze zavedených procesů, jsou:

- Vyšší spokojenost zákazníků,
- úspora nákladů,
- zvýšená kvalita služeb,
- zvýšená produktivita organizace,
- přehlednější organizace práce.

Obrázek 2.1: Příklad znázornění procesu – doručení zásilky. Zdroj: [22].

2.1.3 Klasifikace procesů

Jedna z možných klasifikací procesů [8] můžeme dělit do tří kategorií:

1. *Řídící procesy* – jsou určeny pro management, který pomocí nich řídí chod organizace a kvalitu výstupu. Jedná se většinou o procesy spojené např. s vytvářením strategie firmy, řízením rizik, ...

2. *Hlavní procesy* – jejichž výstup jsou určeny pro externí zákazníky a jejich cílem je vytvářet hodnotu pro zákazníka. Důležité je mapovat celý řetězec aktivit od identifikace požadavků zákazníků až po dodání služby či produktu zákazníkovi a sledování jeho spokojenosti. Hlavní procesy každé organizace jsou specifické podle jeho předmětu podnikání.

3. *Podpůrné procesy* – podporují realizaci hlavních procesů. Jsou většinou velmi univerzální a podobné v různých organizacích. Z tohoto důvodu jsou často předmětem outsourcingu.

Tabulka 2.1: Klasifikace procesů. Zdroj [9].

Typ procesu	**Charakteristika procesu**			
	Přidává hodnotu?	Probíhá napříč organizací	Má externí zákazníky?	Generuje zisk?
Řídící	Ne	Ano	Ne	Ne
Hlavní	Ano	Ano	Ano	Ano
Podpůrné	Ano	Ne	Ne	Ne

2.1.4 Modelování procesů

Klasifikace přístupů

Existuje mnoho různých přístupů k reprezentování průběhu procesu. Zjednodušeně můžeme klasifikovat všechny tyto přístupy do čtyř kategorií [2] podle hlavního pohledu, který přebírá dynamiku podnikových procesů:

- *Vstupní/výstupní tok (Input/output flow)* – Tento v/v tok může být znázorněn jako diagram (graf). Pořadí napojených aktivit vstupně/výstupním tokem neznázorňuje pořadí vykonávání, ale znázorňuje kauzální pořadí, tj. výsledky jedné aktivity jsou vstupem druhé aktivity. Př. IDEF0 diagram (Icam DEFinition for Function Modeling).

- *Pracovní postup (Workflow)* – Důraz je kladen na pořadí aktivit v čase. Tento tok může být znázorněn jako diagram (graf), kde šipky představují

činnosti. Uzly zobrazují výsledky jedné nebo více činností. Př. UML, Petriho sítě.

- *Pohled aktérů (Agent-related view)* – Pohled, v jakém pořadí se aktéři dostávají a vykonávají svoji část práce. Př. Diagram aktivit.

- *Stavový tok (State flow)* – Každá aktivita po jeho vykonání způsobí nějakou změnu stavu instance procesu. Důraz je více kladen na stav po vykonání procesu než na to, jaké aktivity daný proces obsahuje a kdo má jakou zodpovědnost v dané instanci procesu.

Metodiky pro modelování procesů

Lidé modelovali procesy už po mnoho let, jenom tomu neříkali modelování podnikových procesů, protože často to, co popisovali, nepovažovali za podnikové procesy. To znamená, že modely, postupy, které používali, byly např. k popisu organizace, jak funguje. Tyto modely mohly být také použity pro zaučení nových zaměstnanců k rychlejšímu pochopení fungování organizace, k přepracování[1] stávajících postupů, nebo k simulaci a testování nového postupu. Dnes už se vyvíjejí informační systémy, aby tyto procesy, postupy, mohly být zautomatizovány.

Stephan Haberl vyvinul soubor sedmi kritérií pro hodnocení metodik pro modelování procesů [7]:

1. Možnost modelovat všechny součástí procesu v níže uvedeném seznamu:
   - posloupnost aktivit,
   - větvení,
   - smyčky,
   - paralelní konstrukty – fork a synchronizace,
   - časové lhůty,
   - agregace (spojení do většího celku).
2. Možnost rozlišování rolí a jejich zodpovědností.
3. Musí mít jasnou a srozumitelnou grafickou reprezentaci.
4. Mít transakční model, který umožní popsat případ, kdy může být proces nedokončen.
5. Možnost v celém průběhu procesu specifikovat pořadí spuštění jednotlivých procesů.

[1] V dnešní době se častěji setkáme spíše se slovem reengineering xyz, který znamená rekonstrukci, změnu stávajícího stavu

6. Možnost specifikovat charakteristiky podnikových procesů, které by mohly být zajímavé pro externí uživatele. Např. kvalita služby a cena procesu.

7. Metodika by neměla zahrnovat podrobnosti o komunikačních protokolech.

První tři kritéria jsou důležitá pro získání prvních sedmi výhod procesního modelování. Druhá skupina tří kritérií je nezbytná pro automatizaci provádění procesů mezi spolupracujícími a samostatnými organizacemi. Poslední kritérium uchovává procesní modely na správné úrovni abstrakce.

Existuje mnoho různých metodik, s kterými je možno modelovat pracovní postup v organizaci. Tyto metodiky se od sebe liší podle účelu a způsobu koukání se na problematiku procesu v organizaci. Mezi významnější metodiky k popisu pracovního postupu patří: vývojový diagram (Flow Chart Diagram), diagram datových toků (Data Flow Diagram), Ganttův diagram (Gantt Diagram), IDEF, a mezi ty modernější patří např. UML 2.0, XLANG, XPDL, BPMN, ... a metodika DEMO.

Pro tuto práci jsem si vybral metodiky BPMN a DEMO pro možnost podchycení co možná nejširšího stavové prostoru informační bezpečnosti.

2.2 BPMN

Business Process Modeling Notation (BPMN) je notace pro modelování podnikových procesů, která poskytuje grafické znázornění pro specifikaci podnikových procesů. Jedná se poměrně o novou techniku, která je vyvíjená od roku 2005. Po několika verzích se od roku 2011 označuje jako BPMN 2.0. BPMN je založen na jazyku XML nazývaný jako Business Processing Modeling Language (BPML).

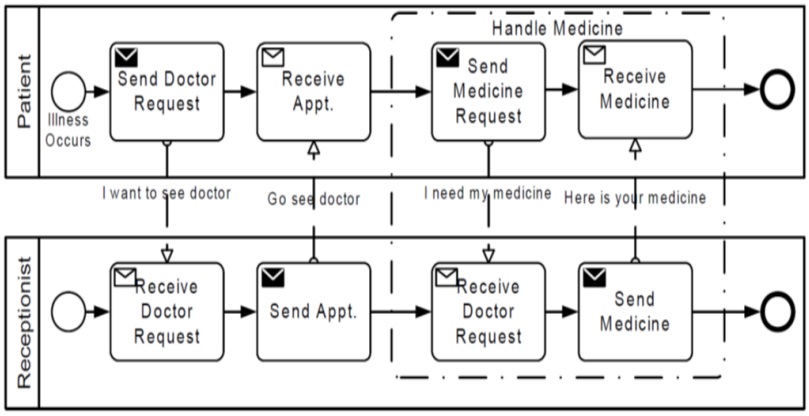
Business Process Modeling Institute (BPMI) se v květnu 2004 spojilo s Object Management Group (OMG). BPMN bylo následně vyvíjeno pod dohledem OMG a v roce 2005 byla uvedena první verze BPMN a následující rok 2006, OMG tuto verzi přijalo jako standard. Kompletní dokumentaci o BPMN lze nalézt na stránkách OMG. [14]

BPMN 2.0 si klade za cíl být jedinou notací pro tvorbu modelů podnikových procesů. Nový formát zachovává vlastnosti z předešlých verzí a díky tomu standard může zůstat pod značkou BPMN. Základními rysy BPMN 2.0 jsou [15]:

- Za pomocí sjednocení definice podnikových procesů BPMN a metamodelu BPDM (Business Process Definition Metamodel) se snaží vytvořit jednotný konzistentní jazyk.

- Vlastnosti BPMN umožňují zorganizovat model tak, aby se mohl vytvořit buď jako nezávislý (samotný), nebo integrovaný model.

- BPMN poskytuje XML schémata sloužící pro transformaci modelů, na základě kterých rozšiřuje vlastnosti BPMN směrem k podnikovému modelovaní.



Obrázek 2.2: Příklad procesu namodelovaný pomocí BPMN. Zdroj: [15].

2.3 Metodika DEMO

Metodika DEMO (Design & Engineering Methodology for Organisation) [16][17] je o návrhu popisu organizace a jejich podnikových procesů. Tato metodika vznikla v 90. letech na půdě univerzity TU Delft v Nizozemí. Autorem je prof. Jan Diedtz a nikdo jiný tomu nerozumí správně jako on sám. Čím se liší DEMO od ostatních notací, tak je založená na standardizovaném a abstraktním modelu komunikace mezi aktéry.

2.3.1 Transakce a transakční axiom

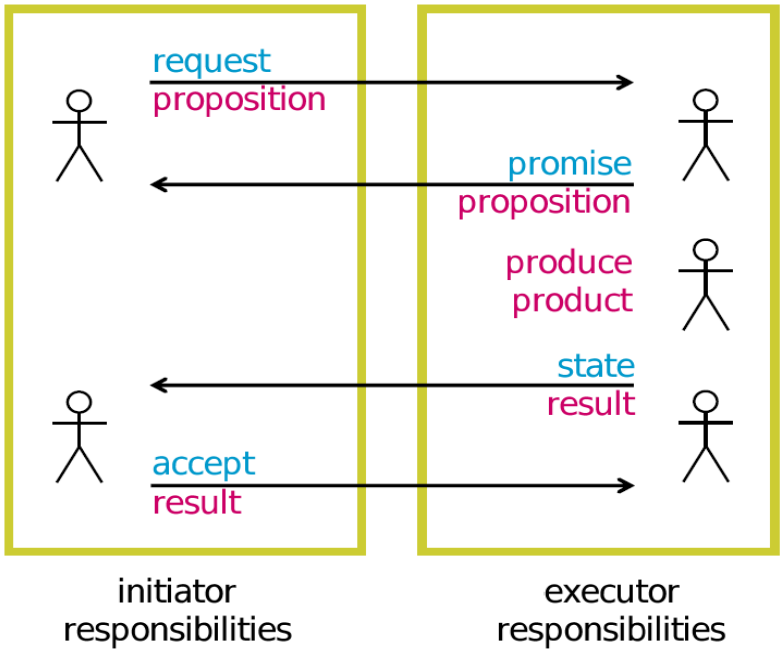
Transakce

Jedním ze stavebních bloků metodiky DEMO je transakce (viz Obrázek 2.3). Jedná se o podnikové procesy, které jsou rozděleny na standardizované menší části. Výstup každé transakce do dodávka nějakého produktu. Např. vytvoření objednávky, prodej rýže, naplánování denního rozvrhu, atd.

Transakce se skládá ze tří fází:

1. *Požadavek a souhlas (Proposition Phase)* – Iniciátor žáda vykonavatele (executor) o dodávku. Dojde k posouzení dodávky vykonavatelem a ten posoudí, zda-li dodávku zamítne, nebo přislíbí.

2. *Vytvoření produktu (Execution Phase)* – Vytvoření produktu.
3. *Dodávka a akceptace (Result Phase)* – dodávka a akceptace produktu iniciátorem.



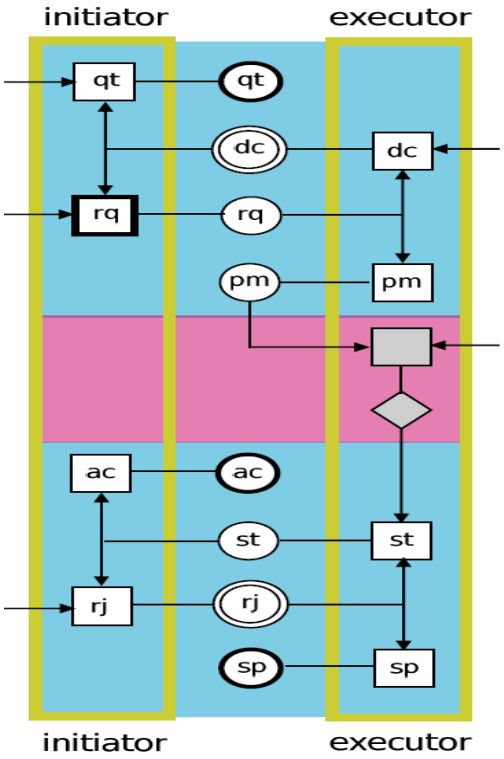
Obrázek 2.3: Průběh transakce. Převzato: [16].

Příklad průběhu transakce z reálného života:

1. Zákazník: Rád bych si koupil jednu modrou růži. (request).
2. Prodavač: Je mi líto, ale modré ruže nemáme. (decline)
3. Zákazník: Dobře, pak mi tedy dejte jednu červenou růži. (request)
4. Prodavač: Ano, červenou ruži Vám mohu dát. (promise)
5. Připraví cervenou ruži.
6. Zde je Vaše růže, pane. (state)
7. Zákazník: Tato růže se mi nelíbí. (reject)
8. Prodavac: Připraví jinou růži. Zde je jiná růže, pane. (state)
9. Zákazník: Ano, tato růže se mi líbí, tu si koupím. (accept)
10. Konec transakce.

Transakční axiom

Ukázali jsme si na příkladě s prodejem růží, jak taková transakce může probíhat. Všecny možné průchody transakcí jak se zákazník nebo prodavač mohl zachovat, lze zachytit do standardního transakčního axiomu (viz Obrázek 2.4)

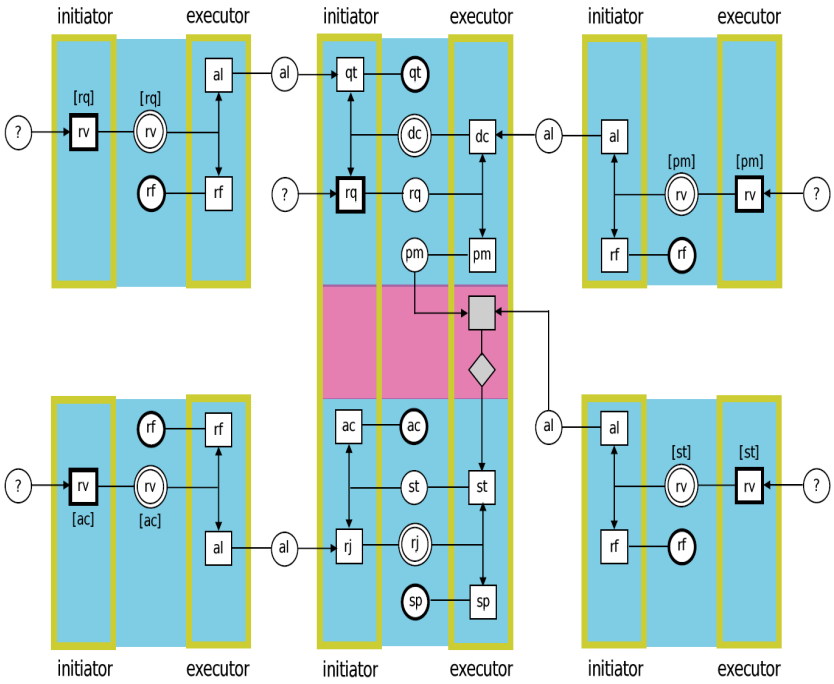


Obrázek 2.4: Stadandardní transakční axiom. Převzato: [16].

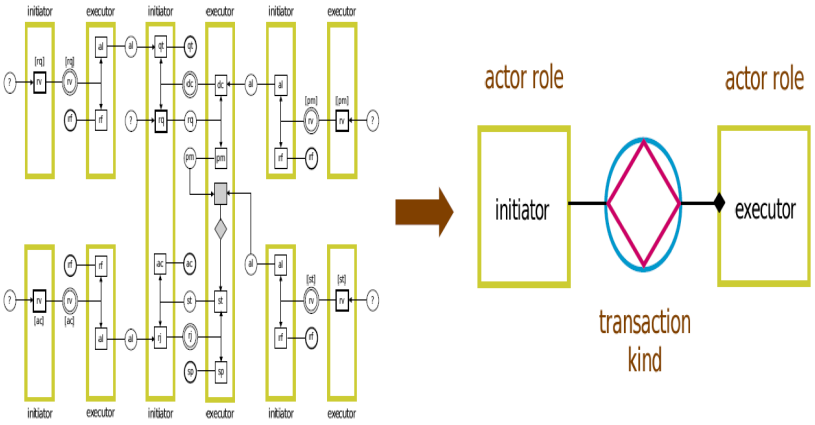
Ne vždy během průběhu transakce (podprocesu) jsme měli ideální podmínky a můžou nastat případy, kdy zákazník je například nespokojen s koupí růže až když opustí květinářství. Takovéto případy jsou v DEMU řešeny tzv. odvoláními (revoke). Potom standardní transakční axiom je rozšířen o tyto odvolání a máme z toho úplný transakční axiom (viz Obrázek 2.5).

Role aktora

Metodika DEMO abstrahuje proces ve všech ohledech a osoba vykonávající určité aktivity nejsou výjimkou. Organizace se v metodice skládá ze subjektů (aktér) zastávající určité role (role aktora). Každá role aktora je zodpovědná vytváření právě jednoho produktu.



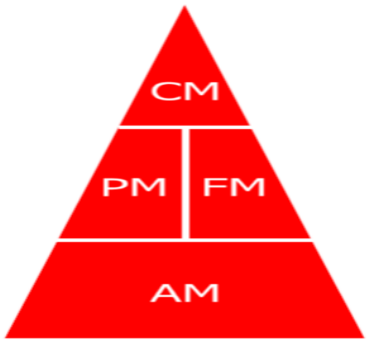
Obrázek 2.5: Úplný transakční axiom. Převzato: [16].



Obrázek 2.6: Úplný transakční axiom překreslena do zjednodušené bloku. Převzato: [16].

2.3.2 Modely a diagramy

Metodika DEMO poskytuje mnoho modelů nejrůznějších úrovní pro popis organizace. Jak jsou si tyto modely provázané je znázorněno na Obrázku 2.7.



Obrázek 2.7: Pyramida modelu metodiky DEMO. Převzato: [16].

- Konstrukční model (CM)
- Procesní model (PM)
- Model faktů (FM)
- Model akčních pravidel (AM)

Pro moji diplomovou práci využiji pouze konstrukční model, který bude podrobněji popsán v 3. kapitole.

Kapitola 3

Konstrukty k praktické části

3.1 ČSN ISO/IEC – tabulky

Z rodiny norem ČSN ISO/IEC 27000 pro moji diplomovou práci použiji normu ČSN ISO/IEC 27001:2014 a normu ČSN ISO/IEC 27005:2013 pro podchycení informační bezpečnosti s pomocí použití BPMN notace a metodiky DEMO.

3.1.1 ČSN ISO/IEC 27001:2014 – Skupiny opatření

Tato norma je o požadavcích, která slouží k opatření bezpečnosti informací upravených podle potřeb organizací nebo jejich částí. V tomto dokumentu nalezneme 114 opatření rozdělených do 14 skupin (viz. Tabulka 3.1).

ČSN ISO/IEC 27001 je pouze seznamem bezpečnostního opatření, které je potřeba jako organizace splnit pro získání certifikace informační bezpečnosti. Tato norma už ale neříká, jakými způsoby se má daná opatření vyhodnotit, aby se (ne)zavedla, revidovala, v organizaci. Z výstupu analyzovaných možných rizik podle doporučení obsažené v normě ČSN ISO/IEC 27005 o pravděpodobnosti výskytu a jeho dopadu na aktiva rozhodnu, v jakém stavu je dané opatření a jaký je další krok pro splnění konkrétního požadavku. Soubor opatření a požadovaný stav z normy 27001 může v mé práci nabývat tří barev (viz. Tabulka 3.2):

- *Zavedeno* – bezpečnostní opatření je již zavedeno a pravděpodobnost výskytu hrozby je minimální. Není potřeba nic provádět.
- *Revidovat* – bezpečnostní opatření je již zavedeno a míra pravděpodobnosti výskytu hrozby je mírná až vysoká. Nutno zkontrolovat současný stav bezpečnostního opatření.
- *Zavést* – opatření je nutné zavést z důvodu, že buď neexistuje, anebo je zastaralé. Míra pravděpodobnosti výskytu hrozby je vysoká.

Tabulka 3.1: Počet jednotlivých opatření z každé skupiny. Zdroj: [24].

Název skupiny opatření	**#opatření**
A.5. Politiky bezpečnosti informací	2
A.6. Organizace bezpečnosti informací	7
A.7. Bezpečnost lidských zdrojů	6
A.8. Řízení aktiv	10
A.9. Řízení přístupu	14
A.10. Kryptografie	2
A.11. Fyzická bezpečnost a bezpečnost prostředí	15
A.12. Bezpečnost provozu	14
A.13. Bezpečnost komunikací	7
A.14. Akvizice, vývoj a údržba systému	13
A.15. Dodavatelské vztahy	5
A.16. Řízení incidentu bezpečnosti informací	7
A.17. Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací	4
A.18. Soulad s požadavky	8
Součet opatření	**114**

Tabulka 3.2: Příklad – Soubor opatření a jeho požadovaný stav. Zdroj [Autor].

Název opatření	**Stav**	**Poznámka**
Název opatření #01	Zavedeno	Cenné papíry, smlouvy, faktury.
Název opatření #02	Revidovat	Zacházení s citlivými daty v transakci T1: Vypůjčka automobilu.
Název opatření #03	Zavést	Databáze klientů.

Soubor všech opatření je velice početný (114 opatření) a použitý příklad v praktické části, na kterém ukáži možnost aplikace této normy, všechna opatření nepokryje. V praktické části práce použiji menší množinu opatření z této normy[1].

[1]Kompletní seznam opatření lze nalézt v Příloze B: Cíle opatření a jednotlivá opatření.

3.1.2 ČSN ISO/IEC 27005:2013 – Přístup k posouzení rizik bezpečnosti informací

Dle doporučení podle normy ČSN ISO/IEC 27005 použiji matici, která vyplývá z úvah o pravděpodobnosti scénáře incidentu namapované proti odhadovanému dopadu na aktivum. Pravděpodobnost scénáře incidentu je dána hrozbou využívající zranitelnosti informační bezpečnosti a může nastat s určitou pravděpodobností. Výsledné riziko se měří na stupnici od 0–8 a může být vyhodnoceno podle kritérií akceptace rizika (viz. Tabulka 3.3). Jedna z možných interpretací škály rizik může být tato:

- Nízké riziko: 0–2
- Střední riziko': 3–5
- Vysoké riziko: 6–8

Tabulka 3.3: Metodika hodnocení rizik. Zdroj: [23].

	Pravděpodobnost scénáře incidentu	Velmi nízká (0)	Nízká (1)	Střední (2)	Vysoká (3)	Velmi vysoká (4)
Dopad na aktivum	Velmi nízká (0)	0	1	2	3	4
	Nízká (1)	1	2	3	4	5
	Střední (2)	2	3	4	5	6
	Vysoká (3)	3	4	5	6	7
	Velmi vysoká (4)	4	5	6	7	8

Stanovení hodnoty dopadu na aktivum

Norma ČSN ISO/IEC 27005:2013 uvádí, že bychom měli vzít v úvahu následující dvě kritéria pro stanovení hodnoty aktiva:

1. *Náklady* – udává částku, která je potřeba pro obnovu aktiva, informací a služeb poskytované organizací. Zpravidla se jedná o náklady na opětovné pořízení HW, SW a infrastruktury z důvodu fyzického poškození nebo zničení.

2. *Následky* – narušení základních atributů informační bezpečnosti aktiva – důvěrnost (confidentiality), celistvost (integrity) a dostupnosti (availability). Většinou se jedná o narušení poskytované služby a její nedostupnosti nebo pokuta za únik informací.

Tabulka 3.4: Dopad na aktivum. Zdroj: [Autor].

Hodnota aktiva	**Popis**
Velmi nízké (0)	Dopad na aktivum je *velmi nízký*. – Škoda je zanedbatelná a není potřeba ji řešit. – Nemá vliv na atmosféru prostředí a neprojevuje se do okolí podniku. – Náklady na odstranění či nápravu nepřesahuje částku xxxx Kč (řádu tisíc korun)
Nízké (1)	Dopad na aktivum je *nízký*. – Případná škoda se neprojevuje do okolí podniku. – Náklady na odstranění či nápravu nepřesahuje částku xxxxx Kč (v řádu desetitisíc).
Střední (2)	Dopad na aktivum je *střední*. – Negativní vliv na organizační celky, ale neprojeví se ve službách poskytovaný navenek. – Mohlo dojít k porušení právních norem a případné správní řízení nebo soudní pře mohou vést k finančnímu postihu do částky xxxxx Kč. (desetitisíce).
Vysoké (3)	Dopad na aktivum je *vysoký*. – Negativní vliv na oddělení podniku a dopad je promítnut do poskytovaných služeb. – Negativní publicita v rámci oboru podnikání. – Správní řízení či soudní pře s postihem přesahujícím xxxxx Kč.
Velmi vysoké (4)	Dopad na aktivum je *velmi vysoký*. – Veřejná negativní publicita. – Ztráta důvěry jednoho nebo více obchodních partnerů. – Potenciální nebezpečí zachování kontinuity podnikání. – Citelná finanční ztráta (miliony, procenta z ročního příjmu).

Je důležité si uvědomit, že hodnota aktiva vyplývající z následků hrozby bude různá vzhledem k původu jejího narušení (důvěrnost, celistvost, dostupnost). Proto u každého aktiva musíme evidovat 3 hodnoty. Jsou hrozby, které mohou narušit pouze jeden z atributů bezpečnosti, anebo taky všechny.

U tří evidovaných hodnot pro každé aktivum je možné udělat aritmetický průměr, tzv. *součtovou metodou*. Všechny tři hodnoty vyhodnocené pro dané aktivum (CIA) sečteme, vydělíme trojkou a zaokrouhlíme směrem nahoru.

Hodnotu zaokrouhlujeme nahoru, protože je lepší počítat s horší variantou řešení, týká-li se to hrozeb a rizik. Vzorec pro součtovou metodu:

$$\sum_{CIA} = \left\lceil \frac{důvěrnost(C) + celistvost(I) + dostupnost(A)}{3} \right\rceil \tag{3.1}$$

Tabulka 3.5: Příklad – Vyhodnocené CIA pro informační aktivum. Zdroj: [Autor].

	Dopad na aktivum			
	C	**I**	**A**	$\sum_{CIA}$
informační aktivum	1	3	4	3

Stanovení hodnoty pravděpodobnosti scénáře incidentu

Pro stanovení hodnoty pravděpodobnosti incidentu mohou být vstupy – seznam identifikovaných scénářů incidentu, identifikace hrozeb, ovlivněná aktiva, seznam všech existujících a plánovaných opatření. Pro identifikaci scénáře incidentu bychom měli používat kvalitativních a kvantitativních ohodnocení pro určení pravděpodobnosti výskytu hrozby.

Při určování pravděpodobnosti výskytu incidentu bysme měli brát v potaz *statistické údaje* o výskytu hrozeb a čerpat ze *zkušeností* (př. vím, že jednou za pět let příjde velká voda, tak nebudu mít servery v přízemí). U úmyslných hrozeb je důležité si zjistit, jakou má útočník *motivaci* a na jaké úrovní jsou jeho schopnosti a dovednosti, aby danou hrozbu mohl zapříčinit. U hrozeb přírodního charakteru bysme se měli dívat na *geografické faktory* – těsná blízkost chemických nebo naftových závodů, možnost extrémních atmosférických podmínek, lidská selhání, funkční poruchy zařízení. [23]

Úplný seznam typických hrozeb z ČSN ISO/IEC 27005 naleznete v Příloze C: Příklady typických hrozeb. Možné typy zdoje: **A** (accidental – náhodný), **D** (deliberate – úmyslný), **E** (environment – přírodní).

Tabulka 3.6: Pravděpodobnost scénáře incidentu. Zdroj: [Autor].

Úroveň hrozby	**Popis**
Velmi nízké (0)	– Malá pravděpodobnost (do 20 %), že může dojít k zanedbatelnému dopadu na činnost podniku nebo oddělení. – Riziko je možné akceptovat.
Nízké (1)	– Nízká pravděpodobnost (20–40 %), že může dojít k zanedbatelnému dopadu na činnost podniku nebo oddělení. – Může dojít k malému dopadu na činnost podniku či oddělení – Riziko je možné akceptovat.
Střední (2)	– Střední pravděpodobnost (40–60 %), že může dojít k zanedbatelnému dopadu na činnost podniku nebo oddělení. – Může dojít k malému dopadu na činnost podniku či oddělení. – Riziko musí být řešeno.
Vysoké (3)	– Vysoká pravděpodobnost (60–80 %), že může dojít k zanedbatelnému dopadu na činnost podniku nebo oddělení. – Riziko musí být řešeno s vysokou prioritou.
Velmi vysoké (4)	– Pravděpodobnost je téměř jistá (80–100 %) a může dojít k vážnému dopadu na činnost podniku či oddělení. – Riziko se musí řešit s největší prioritou.

Tabulka 3.7: Příklad – Hrozba a pravděpodobnost výskytu. Zdroj: [Autor].

Hrozba	**Typ zdroje**	**Úroveň hrozby**	**Komentář**
Požár	A, C, E	Střední (2)	Grill Centrum a erasmáci ze Španělska.
Povodeň	E	Velmi nízké (0)	Budova se nachází 100 m nad řekou Vltavou.
Chybné fungování zařízení	A	Vysoké (3)	Studenti ČVUT.

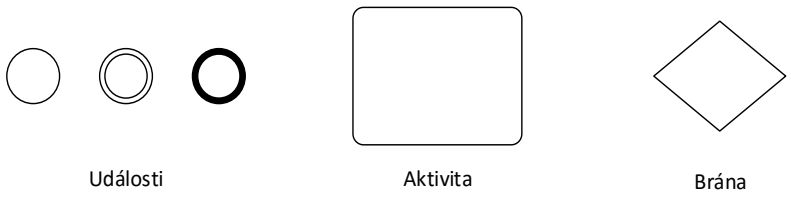
3.2 BPMN – základní modelovací prvky

Tvary elementů BPMN pro modelování byznys procesů se moc neliší od zaběhnutých notací jako je UML (např. rozhodovací blok má tvar kosočtverce, aktivita tvaru obdélníku se zaoblenými hranami, ...). BPMN notace má za cíl poskytnout *byznys uživatelům* jednoduchý a přehledný nástroj, kterému je možné porozumět bez větší odborné znalosti modelování byznys procesů. Tato notace je určena pro analytiky navrhující procesy, vývojáře implementující řešení, až po uživatelé a manažery, kteří tyto procesy spravují, monitorují a řídí.

Základní elementy pro modelování byznys procesů lze rozdělit do 4 základních skupin [19]:

- Plovoucí objekty (Flow Objects),
- propojovací objekty (Connecting Objects),
- plavecké dráhy (Swimlanes),
- artefakty (Artifacts).

3.2.1 Plovoucí objekty (Flow Objects)



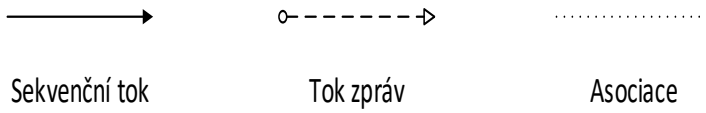
Obrázek 3.1: Notace plovoucích objektů. Zdroj: [Autor].

Kategorie plovoucí objekty obsahuje tři elementy: události (eventy), aktivity (activity) a bránu (gateway).

- *Událost (Event)* – je něco, co se děje v průběhu byznys procesu. Tyto události ovlivňují průběh procesu a obvykle fungují jako spouštěče (trigger) nebo signalizují ukončení byznys procesu s výsledkem (result). Události jsou značeny prázdnou kružnicí, které umožňují interním značkám rozlišovat různé typy událostí. Existují tři typy událostí založené na tom, kdy ovlivňují tok: start (start), přechod (intermediate) a konec (end).

- *Aktivita (Activity)* – obecný termín pro práci, kterou organizace provádí. Aktivita může být atomická, nebo neatomická (sloučení více aktivit). Typy aktivit, které jsou součástí procesního modelu, jsou: procesy, dílčí proces a úkoly.
- *Brána (Gateway)* – se používá k řízení sekvenčního toku, který se buď rozbíhá, nebo sbíhá do brány. Tím určí jejich průběh, větvení a spojování cest. Podle označení uvnitř notace brána lze rozlišit další typy bran – AND, XOR.

3.2.2 Propojovací objekty (Connecting Objects)



Obrázek 3.2: Notace propojovacích objektů. Zdroj: [Autor].

Kategorie propojovací objekty má tři elementy: sekvenční tok (sequence flow), tok zpráv (message flow) a asociace (association).

- *Sekvenční tok (Sequence Flow)* – se používá k zobrazení pořadí provádění aktivit v byznys procesu.
- *Tok zpráv (Message Flow)* – se používá k zobrazení toku zpráv mezi dvouma účastníky, kteří jsou připraveni přijímat a odesílat zprávu. V BPMN, účastníci budou představovat dvě rozdílné dráhy v bazénu.
- *Asociace (Association)* – je určená k propojení datových objektů, textu a dalších artefaktů s plovoucími objekty.

3.2.3 Plavecké dráhy (Swimlanes)

Kategorie plavecké dráhy má dva elementy: bazén (pool), dráha (lane).

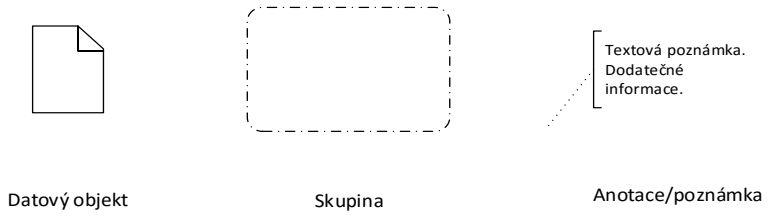
- *Bazén (Pool)* – znázorňuje účastníky procesu. Slouží k rozdělení aktivit, které se účastní procesu v rámci B2B (Business to business) procesů.
- *Dráha (Lanes)* – je součástí bazénu. Dráhy se používají k organizaci a kategorizaci aktivit.

Obrázek 3.3: Notace plaveckých drah. Zdroj: [Autor].

3.2.4 Artefakty (Artifacts)

Kategorie artefakty mají tři element: datový object (data object), skupina (group), anotace/poznámka (text annotation).

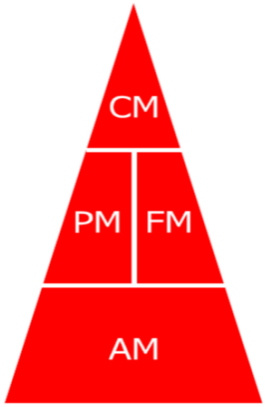
- *Datový object (Data object)* – považují se za artefakty, protože nemají žádný přímý vliv na sekvenční tok nebo tok zpráv procesu. Poskytují informace o tom, jaké činnosti vyžadují provedení a/nebo co vytvářejí.
- *Skupina (Group)* – seskupení činností, které neovlivňuje tok sekvence. Seskupení lze použít pro účely dokumentace nebo analýzy.
- *Anotace/informace (Text Annotation)* – textová poznámka, dodatečné informace pro analytika, vývojáře nebo běžného uživatele.



Obrázek 3.4: Notace artefaktů. Zdroj: [Autor].

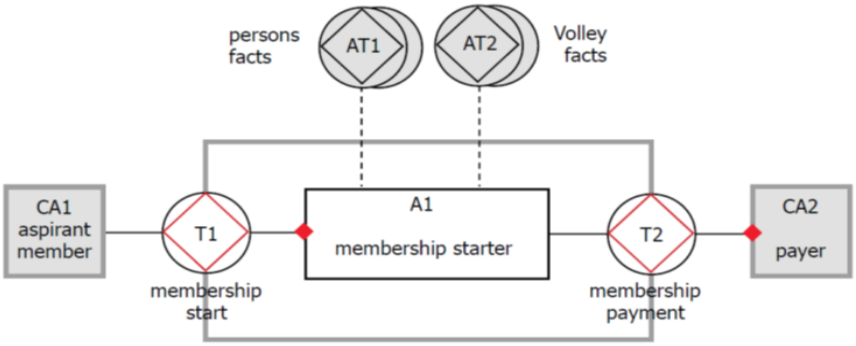
3.3 DEMO metodika – rozšiřující bezpečnostní modul

3.3.1 OCD a TPT



Obrázek 3.5: Pyramida modelů metodiky DEMO. Převzato: [16].

Metodika DEMO poskytuje mnoho modelů nejrůznějších úrovní pro popis organizace. V mé práci využiji pouze jeden model a to konstrukční model (CM). Diagramem konstrukčního modelu je OCD diagram (Organisation Construction Diagram) a TPT tabulka (Transaction Product Table).



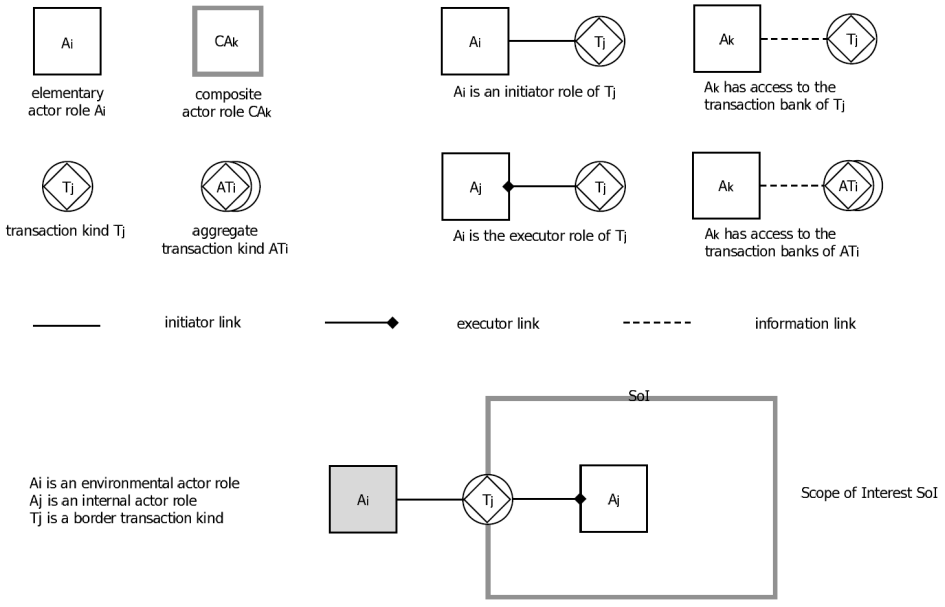
Obrázek 3.6: Příklad OCD diagramu. Převzato: [17].

Tabulka 3.8: Příklad TPT tabulky. Převzato: [17].

Transaction kind	**Product kind**
T1 zřízení členství	P1 členství je zřízeno
T2 zaplacení členského příspěvku	P2 členský příspěvek byl zaplacen

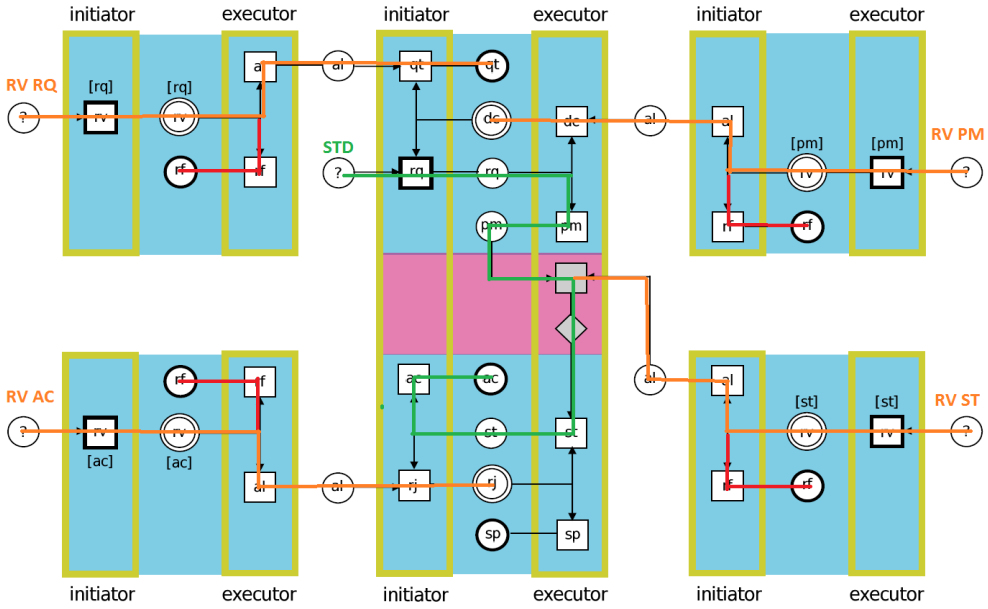
Grafické znázornění OCD diagramu lze rozdělit do skupin:

- *Aktor* – znázorněn obdélníkem. Akorem může být iniciátorem nebo vykonavatelem (executor).
- *Transakce* – znázornění pootočeným čtvercem o 45 stupnů uvnitř kružnice. Výsledkem každé transakce je produkt (P-Fact).
- *Propojovací linky* – definuje, jaký vztah má aktor k dané transakci – iniciátor, vykonavatel, nebo přístup bez možnosti vykonání transakce.
- *SoI (Scope of Interest)* – možno chápat jako rozsah zájmů organizace a co se skrývá pod její střechou z hlediska transakcí a aktorů.



Obrázek 3.7: Modelovací elementy OCD diagramu. Převzato: [16].

3.3.2 Úplný transakční axiom



Obrázek 3.8: Úplný transakční axiom a všechny jeho možné cesty. Převzato: [16].

Každá transakce pracuje s nějakými informačními aktivy organizace. Při standardním průběhu transakčním axiomem (na Obrázku 5.1 vyznačeno zelenou cestičkou STD) informační aktivum nabývá hodnoty rizika podle dopadu na aktivum a pravděpodobnosti výskytu scénáře incidentu (viz. Tabulka 3.3). Tato hodnota rizika se může lišit od standardního průběhu (STD), nastane-li jeden ze čtyř revoků (na Obrázku 5.1 vyznačeno oranžovou cestičkou RV RQ, RV AC, RV PM, RV ST). Mohou nastat až všechny typy revoků, anebo taky žádný.

Tabulka 3.9: Příklad vyhodnocení CIA pro informační aktivum při STD a různých RV. Zdroj: [Autor].

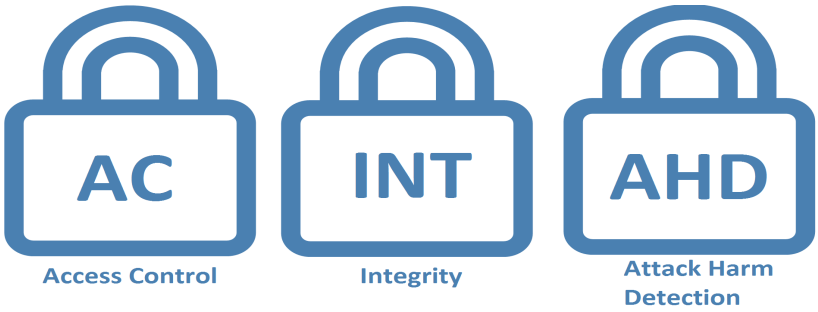
	Dopad na aktivum			
	C	**I**	**A**	$\sum_{CIA}$
informační aktivum, STD	1	3	4	3
informační aktivum, RV RQ	2	2	1	2
informační aktivum, RV PM	3	3	2	3
informační aktivum, RV PM	0	3	1	2
informační aktivum, RV AC	1	0	2	1

3.3.3 Rozšiřující bezpečnostní elementy pro OCD diagram

Metodika DEMO umožňuje popisovat organizaci na všech úrovních, ale chybí jí elementy, které by jí umožňovaly popsat informační bezpečnost. Pro modelování, popisu informační bezpečnosti je důležité myslet na dodržení základních bezpečnostních atributů – *důvěrnost (C)*, *celistvost (I)* a *dostupnost (A)*.

Pro popis organizace je OCD diagram velmi mocný nástroj, protože ukazuje pouze to podstatné, esenciální. Díky tomu na první pohled vidíme, jak konkrétní organizace funguje a jaké jsou její hlavní transakce. V mé diplomové práci jsem se inspiroval prací *A BPMN Extension for the Modeling of Security Requirements in Business Processes* od Alfonsa Rodrígueze [19], který pro BPMN notaci vymyslel rozšíření o elementy pro modelování informační bezpečnosti na základě dodržení CIA[1]. Ve své práci sám autor říká, že tuto myšlenku je možno aplikovat na jiné notace, metodiky. Vybral jsem si tři rozšiřující bezpečnostní elementy a pro OCD diagram lehce modifikoval:

- *Řízení přístupu (Access Control)* – indikuje potřebu zavedení nebo zesílení mechanismu pro přístup k informačním aktivům.
- *Integrita (Integrity)* – indikuje ochranu před úmyslným a neoprávněným vniknutím s cílem poškodit integritu dat.
- *Detekce útoku (Attack Harm Detection)* – indikuje možnost narušení dostupnosti informačního aktiva.



Obrázek 3.9: Rozšiřující bezpečnostní elementy pro OCD diagram. Zdroj: [Autor].

Rozšiřující bezpečnostní elementy v OCD diagramu nám pomůžou neopomenout na důležitá bezpečnostní opatření a může nám taky posloužit jako alarm, že se zde nachází práce s informačními aktivy.

[1]CIA – C (confidentiality – důvěrnost), I (integrity – celistvost), A (availability – dostupnost).

Kapitola 4

Aplikace norem ČSN ISO/IEC, BPMN notace a metodiky DEMO pro návrh a řízení informační bezpečnosti

4.1 Společnost Vypůjči-Si-Automobil (VSA)

V předchozí kapitole jsem popsal konstrukty, které využiji v této kapitole. Jako vzorový příklad jsem si vybral situaci vypůjčení auta z přednášky MI-MEP (modelování ekonomických procesů) [16], na které demonstruji použití norem ČSN ISO/IEC 27001 a ČSN ISO/IEC 27005, DEMO metodiky a BPMN notace pro návrh a řízení informační bezpečnosti.

Vypůjči-Si-Automobil (dále jen VSA) je společnost, která pronajímá automobily jak zákazníkům pro osobní účely, tak i právnickým osobám jakou jsou např. firmy, organizace. Organizace byla založena dvojčaty Janno a Ties v 80. letech. Bratři v počátku začali pronajímat vlastní dvě auta a byli mezi prvními, kteří umožňovali vrátit vypůjčené auto v jiné VSA než kde bylo původně vyzvednuté. Z tohoto důvodu Janno a Ties uzavřeli v několika městech dohodu se studenty. Za malý poplatek si mohl student počkat na příjezd vypůjčeného auta, např. na letišti, a přijet s ním zpět do kanceláří VSA. Potom si student mohl dojet na kolej městskou hromadní dopravou.

V současné době VSA provozuje více než padesát poboček po celé Evropě. Mnoho měst má i několik poboček a nejvíce se nacházejí poblíž letišť. Kde sídlí bratři Janno a Ties dodnes, kde je pobočka kde tato společnost vznikla. Oba jsou vystudovaní jako strojní inženýři a pořád mají v lásce řízení a údržbu automobilů, i přesto, že oba jsou generálními řediteli.

Manažer front office je Chiara. Na tomto oddělení pracují další dva kvalifikovaní zaměstnanci. Zákazník si může vypůjčit automobil několika způsoby: příchod na pobočku VSA, fax, nebo e-mail. Zákazníci, kteří přijdou na pobočku jsou většinou ti, kteří si potřebují ihned vypůjčit automobil. Ostatními způsoby (e-mail, fax) se jedná o rezervaci. Ty mohou být vytvořeny s předstihem až 200 dnů předem. Ať už k vytvoření výpůjčky došlo jakkoliv, je tu pouze jeden elektronický formulář, který vyplňuje kvalifikovaný zaměstnanec do VSAIS (VSA informační systém). Potřebné údaje k vyplnění elektronického formuláře:

- VYPŮJČENÍ: identifikační číslo (automaticky generované), od kdy, do kdy, místo vyzvednutí, místo vrácení, skupina automobilu.
- PŮJČUJÍCÍ: občanský průkaz nebo řidičský průkaz, jméno, příjmení, adresa bydliště, datum narození, místo narození.
- ŘIDIČ: řidičský průkaz (slouží k identifikaci), jméno a příjmení.
- FINANCE: cena za vypůjčení automobilu na den (většinou podle skupiny automobilu).

Ačkoli vyřizování objednávek je úkolem kvalifikovaných zaměstnanců, tuto činnost můžou vykonat i samotní Janno a Ties. Chiaře se toto nelíbí, ale nic s tím nemůže dělat. Problém těchto spontánních činností Janna a Tiese je to, že nedodržují správné postupy vyřízení objednávky a to může vést k nedorozumění, či dokonce ke sporům se zákazníky. Dalším možným problémem může být nabídnutí vypůjčení automobilu za nižší cenu než je stanovená.

Vozy VSA jsou rozděleny do automobilových skupin podle značek a modelu automobilu. Společnou vlastností skupiny automobilů je společná cena za denní pronájem. Správní rada, tj. Janno a Ties, rozhodují, které značky a modely automobilů patří ke které skupině. Stejně rozhodují o cenové sazbě za pronájem. Tuto činnost Janno a Ties provádějí jednou za rok.

Pro začínajícího zákazníka je počáteční den dnem, ve kterém byla smlouva uzavřena. V rezervaci si lze tento den nastavit do budoucna jako počáteční den. VSA uplatňuje maximální dobu pronájmu na deset dní.

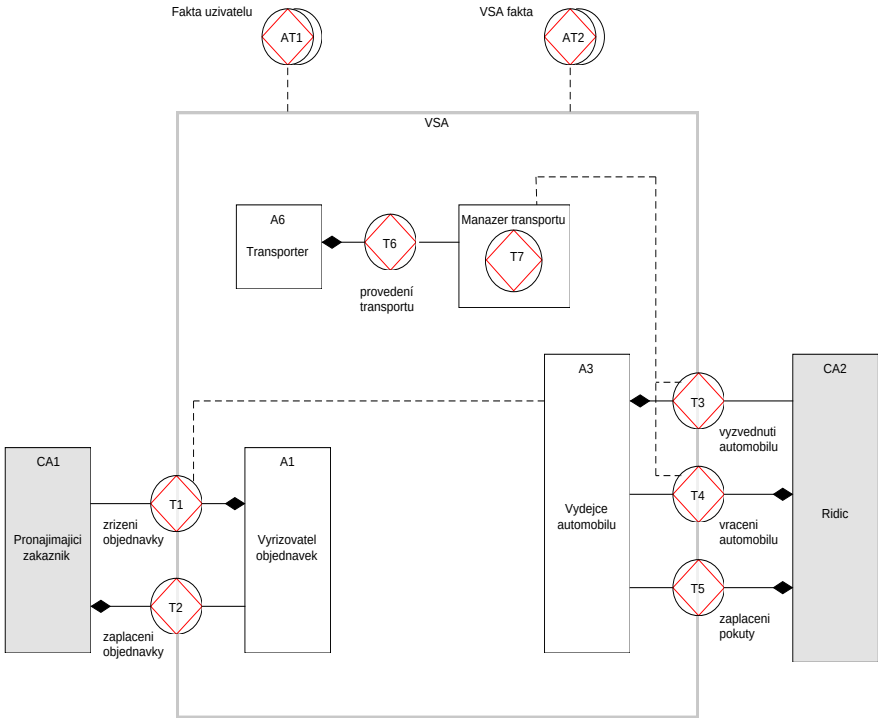
Poté, co zákazník podepíše smlouvu, je smlouva o vypůjčení uzavřena kvalifikovaným zaměstnancem. Vzhledem k tomu, že si zákazník může rezervovat auto a zaplatit zálohu předem, tato platba se může opozdit do dne, kdy nabyde smlouva v platnost, tzn. den, kdy je automobil předán zákazníkovi.

Den, kdy smlouva nabyde v platnost si zákazník po předložení kopie smlouvy může vyzvednout automobil. V oddělení předávání automobilů zákazníkům pracují tři zaměstnanci: Mike, Ferre a Carlo, ale ne všichni tu jsou přítomní.

Tito zaměstnanci zkontrolují zákazníkovu smlouvu a po předání automobilu tuto smlouvu podepíšou jako „předáno“. Pokud v oddělení předávání automobilů není auto ze skupiny napsaná ve smlouvě, zákazník si může vybrat auto z vyšší skupiny a tento automobil z vyšší skupiny mu bude naúčtovaná stejně jako za cenu nižší skupiny uvedená ve smlouvě. Smlouva se aktualizuje na jiný automobil.

Po vrácení automobilů zpět na pobočku, možné vzniklé pokuty musí zákazník uhradit na svůj účet. Může se jednat o pozdní vrácení automobilu po uplynutí smlouvy, nebo auto je vráceno na jinou pobočku, než bylo sjednáno ve smlouvě.

Oddělení předávání automobilů je také zodpovědné za přepravu automobilů mezi pobočkami, protože automobily mohly být vrácený na jiné místo. Každé ráno Mike rozvrhne seznam, kam které auto má být převezeno. Tuto činnost provádějí všichni tři zaměstnanci – Mike, Ferre a Carlo – a proto nemusí být vždy přítomni na pobočce.



Obrázek 4.1: Detailní OCD diagram VSA. Převzato: [16].

Tabulka 4.1: Úplná TPT tabulka VSA. Převzato: [16].

Transaction kind	**Product kind**
T1 zřízení objednávky	P1 objednávka je vytvořená
T2 zaplacení objednávky	P2 objednávka je zaplacená
T3 vyzvednutí automobilu	P3 automobil je vyzvednut
T4 vrácení automobilu	P4 automobil je navrácen
T5 zaplacení pokuty	P5 pokuta je zaplacena
T6 provedení transportu	P6
T7 správa transportu	P7 správa transportu je hotova

4.2 Ohodnocení rizik ve společnosti VSA

Pro ohodnocení rizik potřebujeme nejdříve znát informační aktiva společnosti. Tyto aktiva by měla společnosti přinášet hodnotu a proto má smysl se těmito riziky zabývat. Míru rizik budu hodnotit dle matice pro hodnocení rizik (viz Tabulka 3.3).

4.2.1 Informační aktiva

Pro společnost VSA (Vypůjči-Si-Auto) se jedná o tyto informační aktiva:

- *IA1.Smlouvy o vypůjčení automobilu* – při vytvoření objednávky se zákaznikem.
- *IA2. Osobní údaje zákazníka* – získané po vytvoření objednávky.
- *IA3. VSA informační systém* – systém uchovávající smlouvy v elektronické podobě; znalostní báze problémů.
- *IA4. Databáze formulářů* – při vyplňování údajů pro vytvoření objednávky.
- *IA5. Pracovní stanice* – pracovní stanice sloužítcí k vytvoření objednávky.
- *IA6. Plán na rozmístění automobilů* – pří chybném vrácení automobilu na špatné místo se musí vytvořit plán, kdo a kam zařídí převoz automobilů.

Vyhodnoceni dopadu na aktivum

Informační aktiva společnosti VSA už známe. Pro ohodnocení rizik potřebujeme nadále znát, jaký mají dopad na aktivum nastane-li hrozba. Čím je informační aktivum pro společnost cennější, tím je dopad na aktivum větší.

Tento dopad budu ohodnocovat dle Tabulky 3.4 pro všechny tři bezpečnostní atributy CIA[1].

Tabulka 4.2: Vyhodnocené CIA pro informační aktivum společnosti VSA. Zdroj: [Autor].

	Dopad na aktivum			
	C	**I**	**A**	$\sum_{CIA}$
IA1. Smlouvy o vypůjčení automobilu	3	3	2	3
IA2. Osobní údaje zákazníka	2	3	1	2
IA3. VSA informační systém	3	3	3	3
IA4. Databáze formulářů	3	2	4	3
IA5. Pracovní stanice	2	2	3	3
IA6. Plán na rozmístění automobilů	1	2	0	1

4.2.2 Identifikované a uvažované hrozby

Identifikoval jsem možné hrozby ve společnosti VSA, které uvedu níže v tabulce. Některým hrozbám se nelze úplně vyhnout, např. hrozby přírodní charakteru – povodeň, zemětřesení, atd. Můžeme však učinit preventivní opatření a tím tak úroveň hrozeb snížit na co nejnižší možnou hodnotu. Úroveň hrozeb budu vyhodnocovat dle Tabulky 3.7. Možné typy zdoje: **A** (accidental – náhodný), **D** (deliberate – úmyslný), **E** (environment – přírodní).

Klasifikace hrozeb podle úrovně hrozby

Tabulka 4.3: Hrozba a jeho pravděpodobnost výskytu společnosti VSA. Zdroj: [Autor].

Hrozba	**Typ zdroje**	**Úroveň hrozby**	**Komentář**
Fyzické poškození			
1. Požár	A, C, E	Vysoké (3)	Nedopalky, kouření v zakázaných prostorách, radiátory, ...
2. Poškození vodou	A, D, E	Střední (2)	Není.
3. Zničení zařízení nebo médií	A, D, E	Střední (2)	Není.

[1]CIA – důvěrnost (C – Confidentiality), celistvost (I – Integrity), dostupnost (A – Availability).

Tabulka 4.4: Hrozba a jeho pravděpodobnost výskytu společnosti VSA. Pokračování. Zdroj: [Autor].

Hrozba	**Typ zdroje**	**Úroveň hrozby**	**Komentář**
Přírodní události			
4. Klimatický jev	E	Velmi nízký(0)	Nehrozí extrémní výkyvy počasí.
5. Sopečný jev	E	Velmi nízké (0)	Řídící pobočka sídlí v ČR.
6. Meteorologický jev	E	Velmi nízké (0)	V ČR tornáda a podobné úkazy nebyly zaznamenány.
7. Povodeň	E	Velmi nízké (0)	Město je bez řeky.
Ztráta základních služeb			
8. Selhání telekomunikačního zařízení	A, D	Nízká (1)	Lze fungovat i na mobilních telefonech.
9. Selhání klimatizace nebo dodávky vody	A, D	Střední (2)	Nepravidelná údržba.
10. Přerušení dodávky elektřiny	A, D, E	Nízký (1)	Řídící pobočka sídlí v ČR.
Ohrožení důvěrnosti			
11. Neoprávněné získání přístupových údajů	D	Střední (2)	Není.
12. Chyba v nastavení přístupových práv	A, D	Střední (2)	Není.

Tabulka 4.5: Hrozba a jeho pravděpodobnost výskytu společnosti VSA. Pokračování. Zdroj: [Autor].

Hrozba	**Typ zdroje**	**Úroveň hrozby**	**Komentář**
13. Krádež technického vybavení	D	Střední (2)	Není.
14. Škodlivý software	A, D	Nízké (1)	Přístup k nainstalováního nového SW mají pouze IT specialisté.
Ohrožení informací			
15. Vzdálená špionáž	D	Střední (2)	Vyzjištění cenové politiky, pronajímané typy aut, ...
16. Odposlech	D	Nízké (1)	Není.
17. Krádež médií nebo dokumentů	D	Střední (2)	Vyzjištění cenové politiky, pronajímané typy aut, ...
18. Vyzrazení know how	A, D	Střední (2)	Konkurence.

4.2.3 Tabulka rizik – dopad na aktivum a úroveň hrozby

V podkapitole 4.2.1 jsem vyhodnotil dopad na informační aktiva společnosti VSA a v další podkapitole 4.2.2 jsem vyhodnotil úroveň hrozeb. Tabulka pro hodnocení rizik (viz Tabulka 3.3) je připravená s menší obměnou, že jsem prohodil vstupní proměnné oproti původní tabulce kvůli rozvržení stránky, tzn. dopad na aktivum za pravděpodobnost scénáře incidentu. Z důvodu A4 papírového formátu nebudu značit informační aktiva celými názvy, ale pouze jejich číselným označením.

Legenda:

- *IA1., IA2., ..., IA7.* – informační aktivum 1, informační aktivum 2, ..., informační aktivum 7.
- $\sum_{CIA}$ – součtová metoda vypočítaná z analyzovaných hodnot CIA pro informační aktivum.
- *%* – pravděpodobnost scénáře incidentu vycházející z úrovně hrozby.

Tabulka 4.6: Kompletní tabulka ohodnocení rizik společnosti VSA. Zdroj: [Autor].

		IA1. $\sum_{CIA}$	IA2. $\sum_{CIA}$	IA3. $\sum_{CIA}$	IA4. $\sum_{CIA}$	IA5. $\sum_{CIA}$	IA6. $\sum_{CIA}$
1. Požár	%	6	5	6	6	6	4
2. Poškození vodou	%	5	4	5	5	5	3
3. Zničení zařízení nebo médií	%	5	4	5	5	5	3
4. Klimatický jev	%	3	2	3	3	3	1
5. Sopečný jev	%	3	2	3	3	3	1
6. Meteorologický jev	%	3	2	3	3	3	1
7. Povodeň	%	3	2	3	3	3	1
8. Selhání telekomunikačního zařízení	%	4	3	4	4	4	2
9. Selhání klimatizace nebo dodávky vody	%	5	4	5	5	5	3
10. Přerušení dodávky elektřiny	%	4	3	4	4	4	2
11. Neoprávněné získání přístupových údajů	%	5	4	5	5	5	3
12. Chyba v nastavení přístupových práv	%	5	4	5	5	5	3
13. Krádež technického vybavení	%	5	4	5	5	5	3
14. Škodlivý SW	%	4	3	4	4	4	2
15. Vzdálená špionáž	%	5	4	5	5	5	3
16. Odposlech	%	4	3	4	4	4	2
17. Krádež médií nebo dokumentů	%	5	4	5	5	5	3
18. Vyzrazení know how	%	5	4	5	5	5	3

4.3 Možné změny v dopadech na aktivum

Metodika DEMO říká, že každá část podprocesu v organizaci lze namapovat na standardní transakční axiom. Občas daný proces neprobíhá podle ideálního scénáře a aktor nebo vykonavatel transakce mají možnost se odvolat (revoke) na standardní průchod transakčním axiomem. Pomocí těchto odvolání lze namodelovat všechny možné případy, které mohou nastat v konkrétní transakci. Podle Obrázku 5.1 jsou možné tyto průchody: STD (STanDarní – zelená cestička), RV – RQ, PM, ST, AC (Revoke **R**e**Q**uest, Revoke **P**ro**M**ise, Revoke **ST**ate a Revoke **AC**cept – oranžová cestička).

Tabulka 4.7: Práce s informační aktivy v jednotlivých transakcích. Zdroj: [Autor].

	Transakce						
	T1	T2	T3	T4	T5	T6	T7
IA1. smlouvy o vypůjčení automobilů	✓	✓	✓	✓	✓	x	x
IA2. osobní údaje zákazníků	✓	x	✓	x	x	x	x
IA3. VSA informační systém	✓	✓	✓	✓	✓	x	x
IA4. databáze formulářů	✓	x	x	x	x	x	x
IA5. pracovní stanice	✓	✓	x	✓	✓	x	✓
IA6. plán na rozmístění automobilů	x	x	x	x	x	✓	✓

4.3.1 Transakce T1: zřízení objednávky

Zákazník si může vypůjčit automobil několika způsoby: příchod na pobočku VSA, fax, nebo e-mail. Zákazníci, kteří přijdou na pobočku jsou většinou ti, kteří si potřebují ihned vypůjčit automobil. Ostatními způsoby (e-mail, fax) se jedná o rezervaci. Ty mohou být vytvořeny s předstihem až 200 dnů předem. Ať už k vytvoření výpůjčky došlo jakkoliv, je tu pouze jeden elektronický formulář, který vyplňuje kvalifikovaný zaměstnanec do VSAIS (VSA informační systém).

Možné scénáře odvolání pro transakci T1:

- RV RQ – zákazník si až po zřízení objednávky rozmyslí, že potřeboval větší automobil. Bude vyžadovat zrušení staré rezervace/objednávky a bude chtít vytvořit místo ní novou. Žádný dopad na aktivum.
- RV PM – tuto situaci nebudeme uvažovat.
- RV ST #01 – VSA zaměstnanec zjistí, že zákazník je trestně stíhaný a bude ho bohužel muset odmítnout. Dopad na aktivum IA2.
- RV ST #02 – VSA zaměstnanec zjistí, že zákazník není schopen zaplatit objednávku. Taktkně ho poprosí o výběr levnějšího automobilu, nebo odstoupení od objednávky/rezervace. Dopad na aktivum IA2.
- RV AC – tuto situaci nebudeme uvažovat. Zákazník je s výběrem vždy šťastný. To, že si uvědomí, že si vybral špatný typ automobilu, tak je to RV RQ.

Tabulka 4.8: Znovuvyhodnocení CIA pro informační aktivum při STD a různých RV v transakci T1. Zdroj: [Autor].

	Dopad na aktivum			
	C	**I**	**A**	$\sum_{CIA}$
IA2. Osobní údaje zákazníka, STD	2	3	1	2
IA2. Osobní údaje zákazníka, RV PM #01	3	3	1	3
IA2. Osobní údaje zákazníka, RV PM #02	3	3	1	3

Tabulka 4.9: Kompletní tabulka ohodnocení rizik pro T1 při možných odvolání. Zdroj: [Autor].

		IA2., STD	**IA2., RV PM #01**	**IA2., RV PM #02**
		$\sum_{CIA}$	$\sum_{CIA}$	$\sum_{CIA}$
1. Požár	%	5	6	6
2. Poškození vodou	%	4	5	5
3. Zničení zařízení nebo médií	%	4	5	5
4. Klimatický jev	%	2	3	3
5. Sopečný jev	%	2	3	3
6. Meteorologický jev	%	2	3	3
7. Povodeň	%	2	3	3
8. Selhání telekomunikačního zařízení	%	3	4	4
9. Selhání klimatizace nebo dodávky vody	%	4	5	5
10. Přerušení dodávky elektřiny	%	3	4	4
11. Neoprávněné získání přístupových údajů	%	4	5	5
12. Chyba v nastavení přístupových práv	%	4	5	5
13. Krádež technického vybavení	%	4	5	5
14. Škodlivý SW	%	3	4	4
15. Vzdálená špionáž	%	4	5	5
16. Odposlech	%	3	4	4
17. Krádež médií nebo dokumentů	%	4	5	5
18. Vyzrazení know how	%	4	5	5

4.3.2 Transakce T2: zaplacení objednávky

Poté, co zákazník podepíše smlouvu, je smlouva o vypůjčení uzavřena kvalifikovaným zaměstnancem. Vzhledem k tomu, že si zákazník může rezervovat auto a zaplatit zálohu předem, tato platba se může opozdit do dne, kdy nabyde smlouva v platnost, tzn. den, kdy je automobil předán zákazníkovi.

Možné scénáře odvolání pro transakci T2:

- RV RQ – tuto situaci nebudeme uvažovat. Předpokládejme, že zákazníci neplatí padělanými penězy.
- RV PM – tuto situaci nebudeme uvažovat. Zákazník zaplatí.
- RV ST – tuto situaci nebudeme uvažovat. Zákazník zaplatil.
- RV AC – tuto situaci nebudeme uvažovat. Zákazník nemá špatné úmysly a vždy platí správně.

V transakci T2 neuvažujeme žádné možné odvolání.

4.3.3 Transakce T3: vyzvednutí automobilu

Den, kdy smlouva nabyde v platnost si zákazník po předložení kopie smlouvy může vyzvednout automobil. V oddělení předávání automobilů zákazníkům pracují tři zaměstnanci: Mike, Ferre a Carlo, ale ne všichni tu jsou přítomní. Tito zaměstnanci zkontrolují zákazníkovu smlouvu a po předání automobilu tuto smlouvu podepíšou jako „předáno“. Pokud v oddělení předávání automobilů není auto ze skupiny napsaná ve smlouvě, zákazník si může vybrat auto z vyšší skupiny a tento automobil z vyšší skupiny mu bude naúčtovaná stejně jako za cenu nižší skupiny uvedená ve smlouvě. Smlouva se aktualizuje na jiný automobil.

Možné scénáře odvolání pro transakci T3:

- RV RQ – tuto situaci nebudeme uvažovat.
- RV PM – výdejce automobilů zjistí, že v garáži nemají konkrétní automobil z dané kategorie. Nabídnou řidiči vyšší řadu automobilu za tu samou cenu jako je ta nižší. Dopad na aktivum IA3.
- RV ST – výdejce automobilů zjistí, že konkrétní automobil není ve stavu, který by mohl být předán řidiči. Nabídnou zákazníkovi vyšší řadu automobilu za tu samou cenu jako je ta nižší. Žádný dopad na aktivum.
- RV AC – řidič automobilu zjistí, že konkrétní automobil není ve stavu, který by mohl řídit. Výdejce automobilů nabídne řidiči vyšší řadu automobilu za tu samou cenu jako je ta nižší. Žádný dopad na aktivum.

Tabulka 4.10: Znovuvyhodnocení CIA pro informační aktivum při STD a různých RV v transakci T3. Zdroj: [Autor].

	Dopad na aktivum			
	C	**I**	**A**	$\sum_{CIA}$
IA3. VSA informační systém, STD	3	3	3	3
IA3. VSA informační systém, RV PM	3	4	3	4

Tabulka 4.11: Kompletní tabulka ohodnocení rizik pro T3 při možných odvolání. Zdroj: [Autor].

		IA6., STD	**IA6., RV AC**
		$\sum_{CIA}$	$\sum_{CIA}$
1. Požár	%	6	7
2. Poškození vodou	%	5	6
3. Zničení zařízení nebo médií	%	5	6
4. Klimatický jev	%	3	4
5. Sopečný jev	%	3	4
6. Meteorologický jev	%	3	4
7. Povodeň	%	3	4
8. Selhání telekomunikačního zařízení	%	4	5
9. Selhání klimatizace nebo dodávky vody	%	5	6
10. Přerušení dodávky elektřiny	%	4	5
11. Neoprávněné získání přístupových údajů	%	5	6
12. Chyba v nastavení přístupových práv	%	5	6
13. Krádež technického vybavení	%	5	6
14. Škodlivý SW	%	4	5
15. Vzdálená špionáž	%	5	6
16. Odposlech	%	4	5
17. Krádež médií nebo dokumentů	%	5	6
18. Vyzrazení know how	%	5	6

4.3.4 Transakce T4: vrácení automobilu

Po vrácení automobilů zpět na pobočku, možné vzniklé pokuty musí zákazník uhradit na svůj účet. Může se jednat o pozdní vrácení automobilu po uplynutí smlouvy, nebo auto je vráceno na jinou pobočku, než bylo sjednáno ve smlouvě.

Možné scénáře odvolání pro transakci T4:

- RV RQ – tuto situaci nebudeme uvažovat. Předpokládejme, že auta se vždy vrátí zpět ať už včas, nebo pozdě.
- RV PM – tuto situaci nebudeme uvažovat.
- RV ST – tuto situaci nebudeme uvažovat.
- RV AC – tuto situaci nebudeme uvažovat. Výdejce automobilů příjme automobil, ať už je automobil vrácen včas, nebo se zpožděním.

V transakci T4 neuvažujeme žádné možné odvolání.

4.3.5 Transakce T5: zaplacení pokuty

Po vrácení automobilů zpět na pobočku, možné vzniklé pokuty musí zákazník uhradit na svůj účet. Může se jednat o pozdní vrácení automobilu po uplynutí smlouvy, nebo auto je vráceno na jinou pobočku, než bylo sjednáno ve smlouvě.

Možné scénáře odvolání pro transakci T5:

- RV RQ – výdejce automobilů VSA mohl špatně vypočítat částku pokuty. Po zákazníkovi se vyžaduje buď o dorovnání peněz, nebo výdejce automobilů vrátí zákazníkovi přeplatek ze zaplacené pokuty. Dopad na aktivum IA1.
- RV PM – řidič nepřijímá pokutu, protože zjistí, že jsou tam špatně vypočítané údaje na zaplacení pokuty. Dopad na aktivum IA1., IA3.
- RV ST – tuto situaci nebude uvažovat. Předpokládejme, že zákazníci vždy zaplatí, pokud jim byla vystavena pokuta a oni už ji přijmuli ve stavu Promise.
- RV AC – tuto situaci nebude uvažovat. Předpokládejme, že zákazníci vždy zaplatí, pokud jim byla vystavena pokuta a oni už ji přijmuli ve stavu Promise. Výdejce automobilů dostal peníze a transakce je STD uzavřená.

Tabulka 4.12: Znovuvyhodnocení CIA pro informační aktivum při STD a různých RV v transakci T5. Zdroj: [Autor].

	Dopad na aktivum			
	C	**I**	**A**	$\sum_{CIA}$
IA1. Smlouvy o vypůjčení automobilu, STD	3	3	2	3
IA1. Smlouvy o vypůjčení automobilu, RV RQ	3	4	2	3
IA1. Smlouvy o vypůjčení automobilu, RV PM	3	4	2	3
IA3. VSA informační systém, STD	3	4	2	3
IA3. VSA informační systém, RV PM	4	4	2	4

Tabulka 4.13: Kompletní tabulka ohodnocení rizik pro T5 při možných odvolání. Zdroj: [Autor].

		IA1., STD	**IA1., RV RQ**	**IA1., RV PM**	**IA3., STD**	**IA3., RV PM**
		$\sum_{CIA}$	$\sum_{CIA}$	$\sum_{CIA}$	$\sum_{CIA}$	$\sum_{CIA}$
1. Požár	%	6	6	6	6	7
2. Poškození vodou	%	5	5	5	5	6
3. Zničení zařízení nebo médií	%	5	5	5	5	6
4. Klimatický jev	%	3	3	3	3	4
5. Sopečný jev	%	3	3	3	3	4
6. Meteorologický jev	%	3	3	3	3	4
7. Povodeň	%	3	3	3	3	4
8. Selhání telekomunikačního zařízení	%	4	4	4	4	5
9. Selhání klimatizace nebo dodávky vody	%	5	5	5	5	6
10. Přerušení dodávky elektřiny	%	4	4	4	4	5
11. Neoprávněné získání přístupových údajů	%	5	5	5	5	6
12. Chyba v nastavení přístupových práv	%	5	5	5	5	6
13. Krádež technického vybavení	%	5	5	5	5	6
14. Škodlivý SW	%	4	4	4	4	5
15. Vzdálená špionáž	%	5	5	5	5	6

Tabulka 4.14: Kompletní tabulka ohodnocení rizik pro T5 při možných odvolání. (Pokračování). Zdroj: [Autor].

		IA1., STD	IA1., RV RQ	IA1., RV PM	IA3., STD	IA3., RV PM
		$\sum_{CIA}$	$\sum_{CIA}$	$\sum_{CIA}$	$\sum_{CIA}$	$\sum_{CIA}$
16. Odposlech	%	4	4	4	4	5
17. Krádež médií nebo dokumentů	%	5	5	5	5	6
18. Vyzrazení know how	%	5	5	5	5	6

4.3.6 Transakce T6: provedení transportu

Každé ráno Mike rozvrhne seznam, kam které auto má být převezeno. Tuto činnost provádějí všichni tři zaměstnanci – Mike, Ferre a Carlo – a proto nemusí být vždy přítomni na pobočce.

Možné scénáře odvolání pro transakci T6:

- RV RQ – Mike zjistí, že špatně naplánoval seznam na rozvoz. Je možnost, že auto ze skupiny xyz bylo převezeno na špatné místo. Dopad na aktivum IA6.
- RV PM – tuto situaci nebudeme uvažovat. Očekává se od zaměstnanců, že co Mike přerozdělil, to Carlo a Ferre vykonají.
- RV ST – Řidiči zjistí, že dostali špatný seznam (např. starý) a požádají Mika, aby jim vyhotovil nový. Starý seznam se zahodí a Mike musí vytvořit nový, jinak dneska nikdo nikam nepojede. Může se stát, že starý seznam nebyl důkladně odstraněn a někdo cizí se mohl zmocnit tohoto seznamu. Nový zmocněnec zahozeného seznamu může naplánovat krádež drahého automobilu. Dopad na aktivum IA6.
- RV AC – řekněme, že Mike je nenáročnej a pokud to auto ten den dorazilo tam kam mělo, přijme to jako za hotovou práci. RV AC nebudeme předpokládat pro transakci T6.

Tabulka 4.15: Znovuvyhodnocení CIA pro informační aktivum při STD a různých RV v transakci T6. Zdroj: [Autor].

	Dopad na aktivum			
	C	**I**	**A**	$\sum_{CIA}$
IA6. Plán na rozmístění automobilů, STD	1	2	0	**1**
IA6. Plán na rozmístění automobilů, RV AC	1	2	1	**2**
IA6. Plán na rozmístění automobilů, RV RQ	1	2	2	**2**

Tabulka 4.16: Kompletní tabulka ohodnocení rizik pro T6 při možných odvolání. Zdroj: [Autor].

		IA6., STD	**IA6., RV AC**	**IA6., RV RQ**
		$\sum_{CIA}$	$\sum_{CIA}$	$\sum_{CIA}$
1. Požár	%	4	5	5
2. Poškození vodou	%	3	4	4
3. Zničení zařízení nebo médií	%	3	4	4
4. Klimatický jev	%	1	2	2
5. Sopečný jev	%	1	2	2
6. Meteorologický jev	%	1	2	2
7. Povodeň	%	1	2	2
8. Selhání telekomunikačního zařízení	%	2	3	3
9. Selhání klimatizace nebo dodávky vody	%	3	4	4
10. Přerušení dodávky elektřiny	%	2	3	3
11. Neoprávněné získání přístupových údajů	%	3	4	4
12. Chyba v nastavení přístupových práv	%	3	4	4
13. Krádež technického vybavení	%	3	4	4
14. Škodlivý SW	%	2	3	3
15. Vzdálená špionáž	%	3	4	4
16. Odposlech	%	2	3	3
17. Krádež médií nebo dokumentů	%	3	4	4
18. Vyzrazení know how	%	3	4	4

4.3.7 Transakce T7: správa transportu

Oddělení předávání automobilů je také zodpovědné za přepravu automobilů mezi pobočkami, protože vypůjčené automobily mohly být vrácené na jiné místo než bylo sjednáno ve smlouvě. Každé ráno Mike rozvrhne seznam, kam které auto má být převezeno.

Možné scénáře odvolání pro transakci T7:

- RV RQ – tento případ může nastat právě tehdy, když si Mike uvědomí, že naplánoval omylem znovu včerejší seznam na rozmístění aut. Tento starý seznam musí zahodit a vytvořit znovu nový. Může se stát, že starý seznam nebyl důkladně odstraněn a někdo cizí se mohl zmocnit tohoto seznamu. Nový zmocněnec zahozeného seznamu může naplánovat krádež drahého automobilu automobilu. Dopad na aktivum IA6.
- RV PM – pouze Mike připravuje seznam vozidel k přepravě na konkrétní místa. Situace RV PM nemůže nastat pro transakci T7.
- RV ST – Mike zjistí, že nevypočítal optimální cestu. Nelíbí se mu to, tak jde znovu přepočítat a vytvoří nový seznam. Na informační aktiva to nebude mít žádný nový dopad.
- RV AC – tento případ neuvažujeme.

Tabulka 4.17: Znovuvyhodnocení CIA pro informační aktivum při STD a různých RV v transakci T7. Zdroj: [Autor].

	Dopad na aktivum			
	C	**I**	**A**	$\sum_{CIA}$
IA5. Pracovní stanice	2	2	3	**2**
IA6. Plán na rozmístění automobilů, STD	1	2	0	**1**
IA6. Plán na rozmístění automobilů, RV RQ	1	2	2	**2**

Tabulka 4.18: Kompletní tabulka ohodnocení rizik pro T7 při možných odvolání. Zdroj: [Autor].

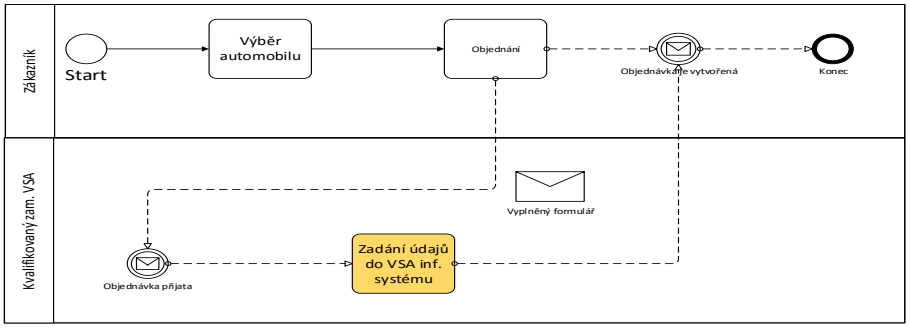
		IA5., STD	IA6., STD	IA6., RV RQ
		$\sum_{CIA}$	$\sum_{CIA}$	$\sum_{CIA}$
1. Požár	%	5	4	5
2. Poškození vodou	%	4	3	4
3. Zničení zařízení nebo médií	%	4	3	4
4. Klimatický jev	%	2	1	2
5. Sopečný jev	%	2	1	2
6. Meteorologický jev	%	2	1	2
7. Povodeň	%	2	1	2
8. Selhání telekomunikačního zařízení	%	3	2	3
9. Selhání klimatizace nebo dodávky vody	%	4	3	4
10. Přerušení dodávky elektřiny	%	3	2	3
11. Neoprávněné získání přístupových údajů	%	4	3	4
12. Chyba v nastavení přístupových práv	%	4	3	4
13. Krádež technického vybavení	%	4	3	4
14. Škodlivý SW	%	3	2	3
15. Vzdálená špionáž	%	4	3	4
16. Odposlech	%	3	2	3
17. Krádež médií nebo dokumentů	%	4	3	4
18. Vyzrazení know how	%	4	3	4

4.4 GDPR

EU legislativa GDPR nabyde v platnosti už 25.5.2018. GDPR a informační bezpečnost jako téma je na samostatnou bakalářskou nebo diplomovou práci. V mé práci pouze nastíním, jaké jsou možnosti k odhalení míst, aktivit, v již existujícím procesu, které se budou týkat GDPR.

Ve společnosti VSA jsem vyhodnotil, že pouze ve dvou transakcích (podprocesech) dochází k práci s osobními údaji. Jsou to transakce T1 (viz Podkapitola 4.3.1) a transakce T3 (viz Podkapitola 4.3.3). Rozhodl jsem se pro BPMN notaci k zachycení toku aktivit jednotlivých transakcí a označit ty aktivity, který pracují s osobními údaji, protože GDPR je celé o osobních údajích.

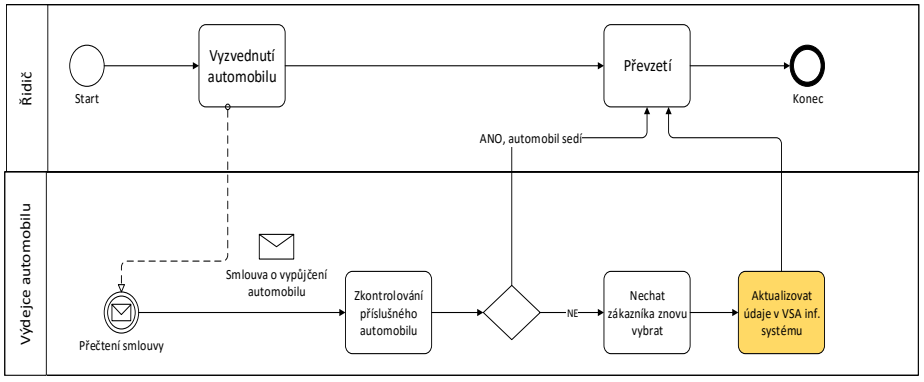
4.4.1 BPMN – T1: zřízení objednávky



Obrázek 4.2: Transakce T1 namodelovaná pomocí BPMN notace. Zdroj: [Autor].

Transakci T1 jsem si překreslil pomocí BPMN notace, abych viděl konkrétní aktivity a mohl následně identifikovat místa pracující s osobními údaji. Pro tuto transakci je to aktivita, kdy kvalifikovaný zaměstnanec zadává údaje zákazníka do VSA informačního systému. Jedná se o aktivitu *Zadání údajů do VSA inf. systému* a na Obrázku 4.2 lze tuto aktivitu vidět jako plně vybarvený obdélník.

4.4.2 BPMN – T3: vyzvednutí automobilu



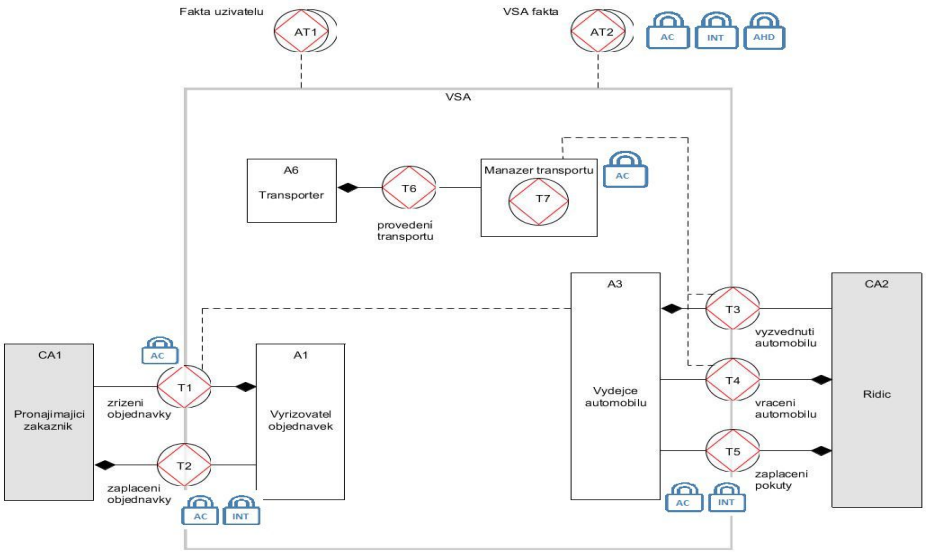
Obrázek 4.3: Transakce T3 namodelovaná pomocí BPMN notace. Zdroj: [Autor].

Podobně jako transakci T1 jsem překreslil transakci T3 pomocí BPMN. Zde dochází k práci s osobními údaji až tehdy, kdy daný automobil není na skladě a zákazníkovi se musí nabídnout jiné. Po vybrání jiného auta musí výdejce automobilů aktualizovat údaje do VSA informačního systému. Jedná se o aktivitu *Aktualizovat údaje v VSA inf. systému* a na Obrázku 4.3 lze tuto aktivitu vid2t jako plně vybarvený obdélník.

4.5 Znázornění informační bezpečnosti v OCD diagramu

Grafické bezpečnostní elementy (viz. Kapitola 3.3.3) jsem použil na původní OCD diagram společnosti VSA. Podle ohodnocení dopadu na aktivum (viz. Tabulka 4.2) jsem použil příslušné bezpečnostní elementy, aby u těchto informačních aktiv byla zvýšená bezpečnost s cílem dodržení základních bezpečnostních atributů CIA.

Spolu s OCD diagramem vidíme pouze z jednoho diagramu, jaké jsou klíčové transakce společnosti, ještě k tomu víme, na jakých místech bychom měli dbát zvýšené bezpečnosti informací.



Obrázek 4.4: OCD diagram rozšířený o grafické bezpečnostní zámky. Zdroj: [Autor].

4.6 Seznam bezpečnostního opatření

Úplný seznam opatření z normy ČSN ISO/IEC 27001 lze najít v Příloze B, která se skládá ze 114 opatření rozdělena do 14 skupin. Pro diplomovou práci nevyužiji všechna opatření a vyberu pouze ty, které se hodí pro modelovou společnost VSA. Cílem je si ukázat, jak je možné přistupovat k takovéto tabulce opatření.

Tabulka 4.19: Soubor opatření a jeho požadovaný stav. Zdroj [Autor].

Název opatření	**Stav**	**Poznámka**
6. Organizace bezpečnosti informací		
6.1.2 Koordinace bezpečnosti informací	zavést	
6.1.3 Přidělení odpovědnosti v oblasti informačních bezpečnosti	revidovat	
6.1.6 Kontakt s orgány veřejné správy	zavedeno	
6.2.1 Identifikace rizik vyplývajících z přístupu externích subjektů		VSA nespolupracuje s externími subjekty
6.2.2 Bezpečnostní požadavky pro přístup klientů		Klienti nemají přístup k informačním aktivům společnosti.
7. Řízeni aktiv		
7.1.3 Přípustné použití aktiv	zavést	ohrožení důvěrnosti
7.1.4 Doporučení pro klasifikaci	zavést	ohrožení důvěrnosti
8. Bezpečnost lidských zdrojů		
8.1.1 Role a odpovědnosti	revidovat	neoprávněné činnosti
8.1.3 Podmínky výkonu pracovní činnosti	revidovat	neoprávněné činnosti
8.2.1 Odpovědnosti vedoucích zaměstnanců	zavedeno	neoprávněné činnosti, lidská selhání
8.2.2 Bezpečnostní povědomí, vzdělávání a školení v oblasti bezpečnosti informací	zavést	lidská selhání
8.3.2 Navrácení zapůjčených prostředků	zavedeno	
8.3.3 Odebrání přístupových práv	revidovat	ohrožení důvěrnosti, neoprávněné činnosti

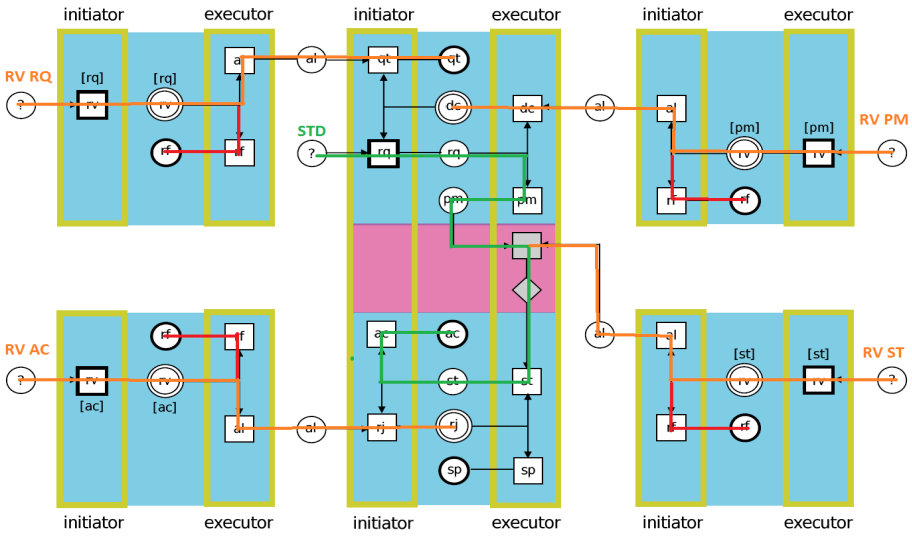
Tabulka 4.20: Soubor opatření a jeho požadovaný stav. Zdroj [Autor].

Název opatření	**Stav**	**Poznámka**
9. Fyzická bezpečnost a bezpečnost prostředí		
9.1.1 Fyzický bezpečnostní perimetr	zavést	ztráta služeb, ohrožení důvěrnosti
9.1.2 Fyzické kontroly vstupu osob	revidovat	ztráta služeb, neoprávněné činnosti
9.1.3 Zabezpečení kanceláří, místností a prostředků	zavést	ohrožení důvěrnosti, neoprávněné činnosti
9.1.5 Práce v zabezpečených oblastech	zavést	lidská selhání
9.2.2 Podpůrná zařízení	revidovat	
9.2.3 Bezpečnost kabelových rozvodů		VSA využívá síť, která je zabudovaná v budově
9.2.4 Údržba zařízení	revidovat	ytráta služeb, technická selhání
13. Zvládání bezpečnostních incidentů		
13.1.1 Hlášení bezpečnostních selhání	zavést	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
13.1.2 Hlášení bezpečnostních slabin	zavést	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
13.2.1 Odpovědnosti a postupy reakce na incidenty	zavést	ohrožení důvěrnosti, neoprávněné činnosti, lidská selhání
13.2.2 Ponaučení z bezpečnostních incidentů	zavést	

Kapitola 5

Vzešlé výstupy z praktické části

Přibližně před osmi měsíci, kdy jsem ještě neměl zadání diplomové práce, jsem se stavil za vedoucím práce, jestli tam v „šuplíku“ by pro mě něco neměl. Neměl. Napadlo nás zkusit použít metodiku DEMO pro podchycení problematiky informační bezpečnosti. Z jednoho prostého důvodu – DEMO říká, že je schopna pokrýt celý stavový prostor řešeného problému na poli modelování procesu. Úplný transakční axiom se k tomu úplně nabízel a jedna z možných způsobu použití tohoto axiomu lze vidět v praktické části práce v Kapitole 4.3.



Obrázek 5.1: Úplný transakční axiom a všechny jeho možné cesty. Převzato: [16].

Metodika DEMO je abstraktnější nástroj než je např. BPMN pro modelování procesů. Díky jeho abstraktnějšímu pojetí problému na té nejvyšší úrovni jsme schopni namodelovat celou organizaci na jednu A4. Přístup k informační bezpečnosti není pouze o zajištění bezpečné komunikační infrastruktury, firewallů, fyzického bezpečnostního opatření, atd. Je to taky o přístupu, jak se díváme na bezpečnost jako takovou. K tomu nám posloužil esenciální model OCD diagram.

Na žádné úrovni svého modelu DEMO neobsahuje elementy, které by umožnily podchytit informační bezpečnost. Pro modelování bezpečnosti jsem potřeboval takové elementy vymyslet nebo najít, jestli se tím už někdo nezabýval. Narazil jsem na práci *A BPMN Extension for the Modeling of Security Requirements in Business Processes* od Alfonsa Rodrígueze [19], který už takový problém pro BPMN řešil. Idea nebyla vázána na konrétní notaci, či metodiku. Inspiroval jsem se a vybral jsem si tři rozšiřující bezpečnostní elementy a pro OCD diagram lehce modifikoval (viz Kapitola 3.3.3). Díky těmto bezpečnostním elementům máme větší přehled, s jakým typem dopadu na aktivum lze očekávat v konkrétní transakci (podprocesu). Grafické elementy nám pomůžou neopomenout na klíčové bezpečnostní opatření a může nám taky posloužit jako alarm, že se zde nachází práce s informačními aktivy. Bezpečnostní grafické elementy s kombinací OCD diagramem nám umožní se na podnik koukat z velké perspektivy s přehledem o bezpečnost informace (viz. Kapitola 4.5).

Obrázek 5.2: Rozšiřující bezpečnostní elementy pro OCD diagram. Zdroj: [Autor].

Snažil jsem se vycházet z norem pro informační bezpečnost a v mé práci jsem použil normy ČSN ISO/IEC 27001 a ČSN ISO/IEC 27005 z rodiny norem ČSN ISO/IEC 27000[1]. Norma ČSN ISO/IEC 27001 je seznamem požadavků na bezpečnost informace a ČSN ISO/IEC 27005 je o řízení rizik bezpečnosti informací, která obsahuje doporučení, jak přistupovat k analýze rizik v organizaci. V první fázi jsem zanalyzoval informační aktiva společnosti a na základě toho jsem mohl dále posoudit možná rizika (viz. Kapitola 4.2). Když už jsem

[1]Všechny ČSN ISO/IEC normy jsou zdarma dostupné v NTK v Dejvicích, Praha 6, ve třetím patře v tiché studovně.

znal zranitelná místa v bezpečnosti informací, tak na základě identifikovaných rizik jsem byl schopen určit jaký opatření podle normy ČSN ISO/IEC 27001 bych měl použít (viz. Kapitola 4.6).

Tabulka 5.1: Metodika hodnocení rizik. Zdroj: [23].

	Pravděpodobnost scénáře incidentu	Velmi nízká (0)	Nízká (1)	Střední (2)	Vysoká (3)	Velmi vysoká (4)
Dopad na aktivum	Velmi nízká (0)	0	1	2	3	4
	Nízká (1)	1	2	3	4	5
	Střední (2)	2	3	4	5	6
	Vysoká (3)	3	4	5	6	7
	Velmi vysoká (4)	4	5	6	7	8

Neopomenul jsem taky na nastupující legislativu o ochraně osobních údajů – GDPR. Problematika GDPR a informační bezpečnost je kapitola sama o sobě. V mé práci jsem se pouze za pomocí BPMN notace pokusil identifikovat možné aktiva, které souvisí s prací s osobními údaji. Tyto aktiva jsem vyznačil v diagramu. Cílem bylo poukázat na možnost, jak je možné identifikovat místa v procesech, které se týkají GDPR (viz. Kapitola 4.4).

Závěr

Cíle práce

Hlavním cílem diplomové práce bylo vymyslet způsob, jak lze využit metodiku DEMO pro modelování informační bezpečnosti. Tento hlavní cíl se skládal z podcílů – definovat informační bezpečnost; analyzovat existující normy a specifikace, popisující oblast informační bezpečnosti; seznámit se s metodikou DEMO a navrhnout způsob použití pro modelování vybraných oblastí informační bezpečnosti; demonstrovat na vhodných oblastech informační bezpečnosti. Hlavní cíl a podcíle stanovené pro mou diplomovou práci se mi podařily naplnit v pěti kapitolách.

V první kapitole jsem popsal informační bezpečnost, jak je chápána v této práci. Problematika informační bezpečnosti nesouvisí pouze se zajištěním bezpečné komunikační infrastruktury, firewallů, fyzického bezpečnostního opatření, silné šifrovací algoritmy, atd. Je potřeba pochopit, že vedle „železa“, které zajištují vyšší informační bezpečnost, je informační bezpečnost taky o tom lidském přístupu, jak k informačním aktivům přistupujeme. Ke zvýšení bezpečnosti je potřeba zavést opatření, které jsou popsané v normách ČSN ISO/IEC a zákonech ČR, který již budou brzy nahrazeny legislativou GDPR. Jedná se konkrétně o celosvětově certifikované technické normy z rodiny ČSN ISO/IEC 27000.

Ve druhé kapitole jsem nastínil, co to je podnikový proces a jak jej již dnes chápeme. Kapitola začíná od podnikových procesů z důvodu, že je důležité pochopit, jak se takové procesy vyvíjely, abychom mohli vymyslet nový přístup k modelování informační bezpečnosti v procesech za použití metodiky, která neobsahuje elementy pro modelování informační bezpečnosti. Pro tuto práci jsem využil BPMN notaci a DEMO metodiku pro zachycení podnikových procesů a identifikace míst týkající se informační bezpečnosti.

Ve třetí kapitole popisuji potřebné konstrukty z norem ČSN ISO/IEC, BPMN notace a DEMO metodiky, jak je použiji v praktické části práce. Z normy ČSN ISO/IEC 27001 jsem použil seznam opatření informační bez-

pečnosti; z normy ČSN ISO/IEC 27005 metodiku, jak vyhodnocovat rizika v organizaci; z BPMN notace základní elementy pro modelování procesů; a z metodiky DEMO úplný transakční axiom, který mi umožní zachytit celý stavový prostor možných případů při modelování transakce (podprocesu), a OCD diagram, který je rozšířen o grafické elementy pro zachycení informační bezpečnosti

Čtvrtá a pátá kapitola je praktická část práce. Zde uplatňuji konstrukty, které jsem popsal v předchozí kapitole. Po dohodě s vedoucím práce jsem tyto konstrukty aplikoval na modelovém případu Vypůjči-Si-Automobil, který jsem si vypůjčil z předmětu MI-MEP (Modelování ekonomických procesů). V následující v páte kapitole jsem shrnul, co vzešlo z praktické části – na informační bezpečnost je potřeba se koukat z větší perspektivy a ne pouze z té technické. K hardwarovým inftrastukturám, antivirům, firewallům, algoritmům pro šifrování, ... musí být zahrnut i lidský faktor. Potom můžeme říci, že informační bezpečnost je úplná splňující na maximální úrovni základní bezpečnostní atributy CIA.

Přínosy

Problematikou bezpečnost informace a modelováním podnikového procesu pomocí metodiky DEMO se ještě nikdo nezabýval k datu, kdy jsem psal tuto diplomovou práci (zima 2017–jaro 2018). Pro vědeckou obec zabývající se DEMO metodikou nebo obecně modelováním podnikových procesů, může být má práce zajímavá z pohledu, že se nám s vedoucím práce podařilo vymyslet jednu z možných využití metodiky DEMO pro podchycení bezpečnosti informací v organizaci.

S přibližujícím nástupem legislativy GDPR je umět se koukat na problematiku týkající se informační bezpečnosti dvakrát tak vhodná. DEMO metodika umožňuje se koukat na věc koncepčně a ne jenom, jak jednotlivé aktivity jdou za sebou jako je tomu např. u BPMN. Proto vidím přínos mé práce i pro konzultanty, kteří denně modelují a analyzují různé problémy, a jiný úhel pohledu na věc by jim mohlo přijít vhod.

Tato diplomová práce je takovou průkopnickou prací týkající se modelováním bezpečnosti informací pomocí metodiky DEMO. Studenti, kteří se zajímají o modelování bezpečnosti v jakékoliv metodice, notaci, mohou na tuto práci navázat bakalářskou nebo diplomovou prací.

Za osobní přínos považuji to, že jsem se během práce se naučil dívat na věc z jiného úhlu pohledu. Bylo to kvůli metodice DEMO, která se kouká na problém jako na celek. Tato diplomová práce byla z velké části rešeršní prací, protože jsem hledal způsoby, jak lze přistupovat k modelování podnikových procesů a tak následně mohl rozšířit model v DEMU. Tato práce mě přesvědčila o tom, že není problém, který by se nedal vyřešit, když se vhodně rozdělí na menší stravitelné části a kousek po kousku se řeší.

Literatura

[1] ALMER, L.; BŘEŇ, J.; BEŇOVÁ, P.; aj.: Nové přístupy k zajištění bezpečnosti státu. (Konference). 2017, [cit. 2018-04-04]. Dostupné z: https://www.unob.cz/fvl/vyzkum_vyvoj/Documents/Konference/Conference%20Proceedings%202017.pdf

[2] BIDER, I.: *Choosing Approach to Business Process Modeling – Practical Perspective. (Online)*. 2007, [cit. 2018-05-05]. Dostupné z: http://ibissoft.se/publications/Howto.pdf

[3] DOUCEK, P.; NOVÁK, L.; NEDOMOVÁ, L.; aj.: *Řízení bezpečnosti informací*. Průhonice: Professional Publishing, 2017, ISBN 978-80-7431-050-8, 289 str. s., [cit. 2018-04-05].

[4] Enterprise Engineering Institute: CHARACTERISTICS OF DEMO. (Online). [cit. 2018-05-05]. Dostupné z: http://www.ee-institute.org/en/demo/characteristics

[5] Evropská unie: *NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679. (Online)*. Evropská unie, duben 2016, [cit. 2018-04-23]. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1501688126470&uri=CELEX:32016R0679

[6] F-Secure Inc., Taija: A Quick Guide to GDPR Concepts. (Online). Poslední aktualizace: 23.01.2018. [cit. 2018-04-23]. Dostupné z: https://business.f-secure.com/quick-guide-to-gdpr-concepts

[7] HABERL, S.: Business Process Desciption Languages. (Online). [cit. 2018-05-05]. Dostupné z: http://www.cis.unisa.edu.au/~cissh/research/webflow/bpdl.html

[8] JANIŠOVÁ, D.; KŘIVÁNEK, M.: *Velká kniha o řízení firmy*. Grada Publishing a.s., 2013, ISBN 978-80-247-4337-0, 400 str. s., [cit. 2018-05-05].

[9] KLUG Solution: Klasifikace business procesů. (Online). [cit. 2018-05-05]. Dostupné z: http://www.klugsolutions.cz/znalostni-baze/klasifikace-procesu.htm

[10] LÓRENCZ, R.: Informační bezpečnost. (Přednáška). 2013, [cit. 2018-04-04].

[11] LÓRENCZ, R.: Základní pojmy v kryptologii, substituční, blokové a transpoziční šifry. (Přednáška). 2013, [cit. 2018-04-04].

[12] Management Mania: Bezpečnostní Incident (Security Incident). (Online). Poslední aktualizace: 17.02.2018. [cit. 2018-04-04]. Dostupné z: https://managementmania.com/cs/bezpecnostni-incident

[13] MILLER, G. A.: *The Magical Number Seven, Plus or Minus Two Some Limits on Our Capacity for Processing Information.* May 1955, [cit. 2018-04-04]. Dostupné z: http://www.idi.ntnu.no/emner/tdt60/papers/Cloud_Computing_Security_Risk.pdf

[14] Object Management Group: ABOUT THE BUSINESS PROCESS MODEL AND NOTATION SPECIFICATION VERSION 2.0. (Online). [cit. 2018-05-05]. Dostupné z: https://www.omg.org/spec/BPMN/2.0/

[15] Object Management Group: Business Process Model and Notation (BPMN), version 2.0. (Online). [cit. 2018-05-05]. Dostupné z: https://www.omg.org/spec/BPMN/2.0/PDF

[16] PERGL, R.: DEMO Bachelor – Introduction and Overview. (Přednáška). 2015, [cit. 2018-05-04].

[17] PERINFORMA, A.: *The Essence of Organisation – An Introduction to Enterprise Engineering, 2nd revised edition.* Perinforma, A.P.C., 2013, ISBN 978-90-815449-4-8, [cit. 2018-05-05].

[18] POŽÁR, J.: Vybrané hrozby informační bezpečnosti organizace. (Online). [cit. 2018-04-04]. Dostupné z: https://www.cybersecurity.cz/data/pozar2.pdf

[19] RODRÍGUEZ, A.; FERNÁNDEZ-MEDINA, E.; PIATTINI, M.: *A BPMN Extension for the Modeling of Security Requirements in Business Processes. (Online).* 2007, [cit. 2018-05-05]. Dostupné z: https://pdfs.semanticscholar.org/d634/a8851766ca540210eff15b143b83be62a6a6.pdf

[20] STAUDEK, J.: Koncept informační bezpečnosti I. (Přednáška). 2017, [cit. 2018-04-04].

[21] TULLOCH, M.: *Microsoft Encyklopedia of Security.* Washington: Microsoft Press, July 2003, ISBN 0-7356-1877-1, 480 str. s., [cit. 2018-04-05].

[22] Česká pošta: Track and Trace. (Online). [cit. 2018-05-05]. Dostupné z: `https://www.postaonline.cz/trackandtrace`

[23] Český normalizační institut: *ISO/IEC 27005:2013 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací.* Praha: Český normalizační institut, 2013, [cit. 2018-04-05].

[24] Český normalizační institut: *ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky.* Praha: Český normalizační institut, 2014, [cit. 2018-04-05].

[25] Český normalizační institut: *ISO/IEC 27000:2014 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník.* Praha: Český normalizační institut, 2017, [cit. 2018-04-05].

[26] ŠKORNIČKOVÁ, E.: Obecné nařízení o ochraně osobních údajů prakticky. (Online). [cit. 2018-04-23]. Dostupné z: `https://www.gdpr.cz/gdpr/`

Příloha **A**

Seznam použitých zkratek

BPMN Business Process Model and Notation

DEMO Design & Engineering Methodology for Organizations

ICT Information and Communication Technologies

IT Informační technologie

GDPR General Data Protection Regulation

OCD Organisation Construction Diagram

STD STanDard

FM Facts Model

PM Process Model

CM Construction Model

AM Action Model

RV RQ Revoke Request

RV PM Revoke Promise

RV ST Revoke State

RV AC Revoke Accept

Příloha B

Cíle opatření a jednotlivá opatření

Tabulka cílů opatření s 114 jednotlivými opatřeními rozdělený do 14 skupin z normy 27001:2013. [norma 27001]

Tabulka B.1: Metodika hodnocení rizik. Zdroj: [norma 27001].

A.5 Politiky bezpečnosti informací		
A.5.1 Směřování bezpečnosti informací vedením organizace		
Cíl: Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky týkající se činnosti organizace, příslušnými zákony a směrnicemi.		
A.5.1.1	Politika pro bezpečnost	*Opatření* Soubor politik pro bezpečnost informací musí být definována, schválen vedením organizace, vydán a dán na vědomí všem zaměstnancům a relevantním externím stranám.
A.5.1.2	Přezkoumání politik pro bezpečnost informací	*Opatření* Pro zajištění neustálé vhodnosti, přiměřenosti a efektivnosti musí být politiky pro bezpečnost informací přezkoumávány v plánovaných intervalech a vždy, když nastane významná změna.
A.6 Organizace bezpečnosti informací		
A.6.1 Interní organizace		
Cíl: Ustavit rámec řízení pro zahájení a řízení implementace a provozování bezpečnosti informací v organizaci.		
A.6.1.1	Role a odpovědnosti bezpečnosti informací	*Opatření* Musí být definovány a přiděleny odpovědnosti v oblasti bezpečnosti informací.

A.6.1.2	Princip oddělení povinností	*Opatření* Pro snížení příležitostí k neoprávněné nebo neúmyslné modifikaci nebo zneužití aktiv organizace musí být zajištěno oddělení neslučitelných povinností a odpovědností.
A.6.1.3	Kontakt s příslušnými orgány a autoritami	*Opatření* Musí být udržovány přiměřené vztahy s příslušnými orgány a autoritami.
A.6.1.4	Kontakt se zájmovými skupinami	*Opatření* Musí být udržovány přiměřené vztahy s odbornými zájmovými skupinami nebo ostatními odbornými fóry na bezpečnost a profesními sdruženími.
A.6.1.5	Bezpečnost informací v řízení projektů	*Opatření* Bezpečnost informací musí být zohledněna v řízení projektů nezávisle na typu projektu.
A.6.2 Mobilní zařízení a práce na dálku		
Cíl: Zajistit bezpečnost při použití mobilních zařízení a pro práci na dálku.		
A.6.2.1	Politika mobilních zařízení	*Opatření* Musí být přijata politika a relevantní bezpečnostní opatření pro zvládání rizik spojených s používáním mobilních zařízení.
A.6.2.2	Práce na dálku	*Opatření* Musí být implementována politika a relevantní bezpečnostní opatření na ochranu informací, které jsou přístupné, zpracované nebo ukládané v místech pro práci na dálku.
A.7 Bezpečnost lidských zdrojů		
A.7.1 Před vznikem pracovního vztahu		
Cíl: Zajistit, aby zaměstnanci a smluvní strany byli srozuměni se svými povinnostmi a aby pro jednotlivé role byli vybráni vhodní kandidáti.		
A.7.1.1	Prověřování	*Opatření* Všichni uchazeči o zaměstnání musí být prověřeni podle platných zákonů, předpisů a v souladu s etikou. Prověření musí být prováděna na základě požadavků týkajících se činností organizace, dále s ohledem na klasifikaci informací, ke kterým by měli získat přístup, a také z hlediska potenciálních rizik.
A.7.1.2	Podmínky pracovního vztahu	*Opatření* Pracovní smlouvy uzavřené se zaměstnanci a smluvními stranami musí obsahovat ustanovení o jejich odpovědnostech a odpovědnostech organizace za bezpečnost informací.

A.7.2 Během pracovního vztahu		
Cíl: Zajistit, aby si zaměstnanci a smluvní strany byli vědomi a plnili si svoje povinnosti v oblasti bezpečnosti informací.		
A.7.2.1	Odpovědnosti vedení organizace	*Opatření* Vedení organizace musí po všech zaměstnancích a smluvních stranách požadovat dodržování bezpečnosti informací v souladu s ustavenými politikami a postupy v organizaci.
A.7.2.2	Povědomí, vzdělávání a školení bezpečnosti informací	*Opatření* Všichni zaměstnanci organizace, a je-li to relevantní i smluvní strany musí s ohledem na svou pracovní náplň dostávat odpovídající vzdělávání a školení pro zvyšování povědomí bezpečnosti informací a musí být pravidelně informováni o změnách v politikách a postupech bezpečnosti informací.
A.7.2.3	Disciplinární řízení	*Opatření* Musí existovat formální proces disciplinárního řízení k přijetí opatření vůči zaměstnancům, kteří se dopustili narušení bezpečnosti informací.
A.7.3 Ukončení a změna pracovního vztahu		
Cíl: Chránit zájmy organizace v rámci procesu změny nebo ukončení pracovního vztahu.		
A.7.3.1	Odpovědnosti při ukončení nebo změně pracovního vztahu	*Opatření* Odpovědnosti a povinnosti v oblasti bezpečnosti informací, které zůstávají platné po ukončení nebo změně pracovního vztahu, musí být definovány, komunikovány se zaměstnanci nebo smluvními stranami a prosazovány.
A.8 Řízení aktiv		
A.8.1 Odpovědnost za aktiva		
Cíl: Identifikovat aktiva organizace a definovat odpovědnosti k jejich přiměřené ochraně.		
A.8.1.1	Seznam aktiv	*Opatření* Aktiva související s informacemi a vybavení pro zpracování informací musí být identifikována a seznam těchto aktiv musí být vytvořen a udržován aktuální.

A.8.1.2	Vlastnictví aktiv	*Opatření* Aktiva udržovaná v seznamu musí mít určeného vlastníka.
A.8.1.3	Přípustné použití aktiv	*Opatření* Musí být určena, dokumentována a implementována pravidla pro přípustné použití informací a aktiv souvisejících s informacemi a vybavením pro zpracování informací.
A.8.1.4	Navrácení aktiv	*Opatření* Při ukončení pracovního vztahu, smluvního vztahu nebo dohody musí zaměstnanci a pracovníci externích stran odevzdat veškerá jim svěřená aktiva, která jsou majetkem organizace.
A.8.2 Klasifikace informací		
Cíl: Zajistit, aby informace získaly odpovídající úroveň ochrany v souladu s jejich důležitostí pro organizaci.		
A.8.2.1	Klasifikace informací	*Opatření* Informace musí být klasifikovány s ohledem na zákonné požadavky, jejich hodnotu, kritičnost a citlivost vůči neoprávněnému prozrazení nebo modifikaci.
A.8.2.2	Označování informací	*Opatření* Pro označování informací musí být vytvořen a implementován vhodný soubor postupů, které jsou v souladu se schématem klasifikace informací přijatým organizací.
A.8.2.3	Manipulaci s aktivy	*Opatření* Pro manipulaci s aktivy musí být vytvořeny a implementovány postupy v souladu se schématem klasifikace informací přijatým organizací.
A.8.3 Manipulace s médii		
Cíl: Předcházet neoprávněnému vyzrazení, modifikací, odstranění nebo zničení informací uložených na médiích.		
A.8.3.1	Správa výměnných médií	*Opatření* Musí být implementovány postupy pro správu výměnných médií v souladu se schématem klasifikace informací přijatých organizací.
A.8.3.2	Likvidace médií	*Opatření* Média, pokud nejsou dále upotřebitelná, musí být bezpečně zlikvidována v souladu s formalizovanými postupy.

A.8.3.3	Přeprava fyzických médií	*Opatření* Média obsahující informace musí být během přepravy chráněna proti neoprávněnému přístupu, zneužití nebo narušení.
A.9 Řízení přístupu		
A.9.1 Požadavky organizace na řízení přístupu		
A.9.1.1	Politika řízení přístupu	*Opatření* Musí být ustavena, dokumentována a přezkoumávána politika řízení přístupu v závislosti na požadavcích na činnosti organizace a bezpečnosti informací.
A.9.1.2	Přístup k sítím a síťovým službám	*Opatření* Uživatelé musí mít přístup pouze k těm sítím a síťovým službám pro jejich použití byli zvlášť oprávněni.
Cíl: Omezit přístup k informacím a vybavení pro zpracování informací.		
A.9.2 Řízení přístupu uživatelů		
Cíl: Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k systémům a službám.		
A.9.2.1	Registrace a zrušení registrace uživatele	*Opatření* Pro přidělování přístupových práv musí být implementován proces formalizované registrace uživatele včetně jejího zrušení.
A.9.2.2	Správa uživatelských přístupu	*Opatření* Pro přidělování a odebírání přístupových práv všem typům uživatelů ke všem systémům a službám musí být implementován formalizovaný proces správy uživatelských přístupů.
A.9.2.3	Správa privilegovaných přístupových práv	*Opatření* Musí být omezeno a řízeno přidělování a používání privilegovaných přístupových práv.
A.9.2.4	Správa tajných autentizačních informací uživatelů	*Opatření* Přidělování tajných autentizačních informací musí být řízeno formalizovaným procesem.
A.9.2.5	Přezkoumání přístupových práv uživatelů	*Opatření* Vlastníci aktiv musí v pravidelných intervalech přezkoumávat přístupová práva uživatelů.
A.9.2.6	Odebrání nebo úprava přístupových práv	*Opatření* Při ukončení nebo změně pracovního vztahu, smluvního vztahu nebo dohody musí být všem zaměstnancům a externím stranám odejmuta nebo pozměněna přístupová práva k informacím a vybavení pro zpracování informací.

A.9.3 Odpovědnosti uživatelů		
Cíl: Učinit uživatele odpovědné za ochranu jejich autentizačních informací.		
A.9.3.1	Používání tajných autentizačních informací	*Opatření* Při používání tajných autentizačních informací musí být po uživatelích vyžadováno, aby dodržovali postupy stanovené organizací.
A.9.4 Řízení přístupu k systémům a aplikacím		
Cíl: Předcházet neautorizovanému přístupu k systémům a aplikacím.		
A.9.4.1	Omezení přístupu k informacím	*Opatření* V souladu s politikou řízení přístupu musí být omezen přístup k informacím a funkcím aplikací.
A.9.4.2	Bezpečné postupy přihlášení	*Opatření* Pokud to politika řízení přístupu vyžaduje, musí být přístup k systémům a aplikacím řízen postupy bezpečného přihlášení.
A.9.4.3	Systém správy hesel	*Opatření* Systémy správy hesel musí být interaktivní a musí zajišťovat použití kvalitních hesel.
A.9.4.4	Použití privilegovaných programových nástrojů	*Opatření* Musí být omezeno a přísně kontrolováno použití programových nástrojů, které mohou být schopné překonat systémové nebo aplikační kontroly.
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	*Opatření* Musí být omezen přístup ke zdrojovým kódům programů.
A.10 Kryptografie		
A.10.1 Kryptografická opatření		
Cíl: Zajistit řádné a efektivní používání kryptografie k ochranně důvěrnosti, autentičnosti a/nebo integrity informací.		
A.10.1.1	Politika pro použití kryptografických opatření	*Opatření* Musí být vytvořena a implementována politika pro používání kryptografických opatření na ochranu informací.
A.10.1.2	Správa klíčů	*Opatření* Politika pro používání, ochranu a dobu existence kryptografických klíčů musí být vytvořena a implementována po celou dobu jejich životního cyklu.

A.11 Fyzická bezpečnost a bezpečnost prostředí		
A.11.1 Bezpečné oblasti		
Cíl: Předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace.		
A.11.1.1	Fyzický bezpečnostní perimetr	*Opatření* Bezpečnostní perimetr musí být definovány a používány k ochraně oblastí, které obsahují citlivé nebo kritické informace a vybavení pro zpracování informací.
A.11.1.2	Fyzické kontroly vstupu	*Opatření* Aby bylo možno zajištěno, že je přístup do bezpečných oblastí povolen pouze oprávněným osobám, musí být tyto oblasti chráněny vhodným systémem vstupních kontrol.
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	*Opatření* Musí být navržena a aplikována fyzická bezpečnost kanceláří, místností a vybavení.
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	*Opatření* Musí být navržena a aplikována fyzická ochrana proti přírodním katastrofám, úmyslnému útoku nebo haváriím.
A.11.1.5	Práce v bezpečných oblastech	*Opatření* Musí být navrženy a aplikovány postupy pro práci v bezpečných oblastech.
A.11.1.6	Oblasti pro nakládku a vykládku	*Opatření* Přístupové body, jako oblasti pro nakládku a vykládku a další místa, kde se mohou neoprávněné osoby dostat do prostor organizace, musí být kontrolovány a pokud je to možné, izolovány od vybavení pro zpracování informací, aby se zabránilo neoprávněnému přístupu k nim.
A.11.2 Zařízení		
Cíl: Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činností organizace.		
A.11.2.1	Umístění zařízení a jeho ochrana	*Opatření* Zařízení musí být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup.
A.11.2.2	Podpůrné služby	*Opatření* Zařízení musí být chráněno před selháním napájení a před dalšími výpadky způsobenými selháním podpůrných služeb.

A.11.2.3	Bezpečnost kabelových rozvodů	*Opatření* Silové a telekomunikační kabelové rozvody, které jsou určeny pro přenos dat nebo podporu informačních služeb, musí být chráněny před odposlecehm, rušením či poškozením.
A.11.2.4	Údržba zařízení	*Opatření* Zařízení musí být správně udržováno pro zajištění jeho stálé dostupnosti a integrity.
A.11.2.5	Přemístění aktiv	*Opatření* Zařízení, informace nebo software nesmí být přemisťováno mimo prostory organizace bez předchozího schválení.
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace	*Opatření* Aktiva mimo prostory organizace musí být zabezpečena s přihlédnutím k rozdílným rizikům, která vyplývají z jejich použití mimo organizace.
A.11.2.7	Bezpečná likvidace nebo opakované použití zařízení	*Opatření* Všechny prvky zařízení obsahující paměťová média musí být zkontrolovány tak, aby bylo zajištěno, že před jejich likvidací nebo opakovaným použitím budou jakákoliv citlivá data a licencovaný software odstraněny nebo bezpečně přepsány.
A.11.2.8	Uživatelská zařízení bez obsluhy	*Opatření* Uživatelé musí zajistit přiměřenou ochranu zařízení bez obsluhy.
A.11.2.9	Zásada prázdného stolu a prázdné obrazovky monitoru	*Opatření* Musí být přijata zásada prázdného stolu ve vztahu k dokumentům výměnným paměťovým médiím a zásada prázdné obrazovky monitoru u vybavení pro zpracování informací.
A.12 Bezpečnost provozu		
A.12.1 Provozní postupy a odpovědnosti		
Cíl: Zajistit správný a bezpečný provoz vybavení pro zpracování informací.		
A.12.1.1	Dokumentované provozní postupy	*Opatření* Provozní postupy musí být dokumentovány a musí být dostupné všem uživatelům podle potřeby.
A.12.1.2	Řízení změn	*Opatření* Změny v organizaci a jejich procesech, v prostředních pro zpracování informací a systémech, které ovlivňují bezpečnost informací, musí být řízeny.

A.12.1.3	Řízení kapacit	*Opatření* Pro zajištění požadovaného výkonu systému, s ohledem na budoucí kapacitní požadavky, musí být monitorováno, nastaveno a předvídáno využití zdrojů.
A.12.1.4	Princip oddělení prostředí vývoje, testování a provozu.	*Opatření* Pro snížení rizika neoprávněného přístupu nebo změn provozního prostředí musí být odděleno prostředí vývoje, testování a provozu.
A.12.2 Ochrana proti malwaru		
Cíl: Zajistit, aby informace a vybavení pro zpracovávání informací byly chráněny proti malwaru.		
A.12.2.1	Opatření proti malwaru	*Opatření* Na ochranu proti malwaru musí být implementována opatření na jeho detekci, prevenci a obnovu, a to ve spojení s odpovídajícím bezpečnostním povědomím uživatelů.
A.12.3 Zálohování		
Cíl: Chránit proti ztrátě dat.		
A.12.3.1	Zálohování informací	*Opatření* Záložní kopie informací, softwaru a binárních obrazů systému musí být pořizovány a testovány v pravidelných intervalech v souladu se schválenou politikou zálohování..
A.12.4 Zaznamenávání formou logů a monitorování		
Cíl: Zaznamenávat události a vytvářet záznamy.		
A.12.4.1	Zaznamenávání událostí formou logů	*Opatření* Musí být pořizovány, uchovány a pravidelně přezkoumávány logy událostí zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací.
A.12.4.2	Ochrana logů	*Opatření* Prostředky pro zaznamenávání formou logů a logy musí být chráněny proti zfalšování a neoprávněnému přístupu.
A.12.4.3	Logy o činnosti administrátorů a operátorů	*Opatření* Aktivity systémového administrátora a systémového operátora musí být logovány a logy chráněny a pravidelně přezkoumávány.
A.12.4.4	Synchronizace hodin	*Opatření* Hodiny všech důležitých systémů pro zpracování informací musí být v rámci organizace nebo bezpečnostních domén synchronizovány s jediným referenčním zdrojem času.

A.12.5 Správa provozního softwaru		
Cíl: Zajistit integritu provozních systémů.		
A.12.5.1	Instalace softwaru na provozní systémy	*Opatření* Musí být implementovány postupy řízené instalace softwaru na provozních systémech.
A.12.6 Řízení technických zranitelností		
Cíl: Zabránit využívání technických zranitelností.		
A.12.6.1	Řízení technických zranitelností	*Opatření* Musí být zajištěno včasné získání informací o existenci technických zranitelností provozovaných informačních systémů, vyhodnocena úroveň ohrožení organizace vůči těmto zranitelnostem a přijata příslušná opatření na zvládání souvisejících rizik.
A.12.6.2	Omezení instalace softwaru	*Opatření* Musí být ustavena a implementována pravidla ohledně instalace softwaru uživateli.
A.12.7 Hlediska auditu informačních systémů		
Cíl: Minimalizovat dopady auditních činností na provozní systémy.		
A.12.7.1	Opatření k auditu informačních systému	*Opatření* Požadavky auditu a činnosti zahrnující verifikaci provozních systémů musí být pečlivě naplánovány a schváleny, aby se minimalizovalo narušení procesů organizace.
A.13 Bezpečnost komunikace		
A.13.1 Správa bezpečnost sítě		
Cíl: Zajistit ochranu informací v sítích a jejich podpůrných prostředcích pro zpracování informací.		
A.13.1.1	Opatření v sítích	*Opatření* K ochraně informací v systémech a aplikacích musí být sítě řízeny, spravovány a kontrolovány.
A.13.1.2	Bezpečnost síťových služeb	*Opatření* Musí být identifikovány a do dohod o poskytování síťových služeb zahrnuty bezpečnostní mechanismy, úroveň poskytovaných služeb a požadavky na správu všech síťových služeb, ať už jsou zajišťovány interně nebo cestou outsourcingu.
A.13.1.3	Princip oddělení v sítích	*Opatření* V sítích musí být odděleny skupiny informačních služeb, uživatelů a informačních systémů.

A.13.2 Přenos informací		
Cíl: Zajistit Zajistit bezpečnost informací při jejich přenosu v rámci organizace a s externími subjekty.		
A.13.2.1	Politiky a postupy při přenosu informací	*Opatření* Musí existovat formalizované politiky, postupy a opatření k ochraně přenosu informací pomocí jakéhokoliv typu komunikačního vybavení.
A.13.2.2	Dohody o přenosu informací	*Opatření* Dohody se musí zabývat zabezpečeným přenosem informací týkající se činností organizace mezi organizací a externími stranami.
A.13.2.3	Elektronické předávání zpráv	*Opatření* Musí být vhodným způsobem chráněny elektronicky přenášené informace.
A.13.2.4	Dohody o utajení nebo o mlčenlivosti	*Opatření* Musí být identifikovány, pravidelně přezkoumávány a dokumentovány požadavky na dohody o utajení nebo na dohody o mlčenlivosti reflektující potřeby organizace na ochranu informací.
A.14 Akvizice, vývoj a údržba systémů		
A.14.1 Bezpečnostní požadavky informačních systémů		
Cíl: Zajistit, aby se bezpečnost informací stala nedílnou součástí informačních systémů v jejich celém životním cyklu. To zahrnuje i požadavky na informační systémy, které poskytují služby ve veřejných sítích.		
A.14.1.1	Analýza a specifikace požadavků bezpečnosti informací	*Opatření* V požadavcích na nové informační systémy nebo na rozšíření existujících systémů musí být obsaženy také požadavky týkající se bezpečnosti informací.
A.14.1.2	Zabezpečení aplikačních služeb ve veřejných sítích	*Opatření* Informace přenášené ve veřejných sítích v rámci aplikačních služeb musí být chráněny před podvodnými aktivitami, zpochybňováním smluv, neoprávněným vyzrazením a modifikací.
A.14.1.3	Ochrana transakcí aplikačních služeb	*Opatření* Musí být zajištěna ochrana informací přenášených při transakcích aplikačních služeb tak, aby se zabránilo neúplnému přenosu informací, chybnému směrování, neoprávněné změně zpráv, neoprávněnému vyzrazení, neoprávněné duplikaci nebo opakování přenosu zpráv.

A.14.2 Bezpečnost v procesech vývoje a podpory		
Cíl: Zajistit, aby bezpečnost informací byla navrhována a implementována v životním cyklu vývoje informačních systémů.		
A.14.2.1	Politika bezpečného vývoje	*Opatření* Musí být ustavena a v rámci organizace aplikována pravidla pro vývoj softwaru a systému.
A.14.2.2	Postupy řízení změn systémů	*Opatření* Pomocí formalizovaných postupů řízení změn musí být řízeny změny systémů v rámci jejich životního cyklu vývoje.
A.14.2.3	Technické přezkoumání aplikací po změnách provozní platformy	*Opatření* V případě změny provozní platformy musí být přezkoumány a otestovány aplikace kritické pro činnost organizace, aby se zajistilo, že změny nemají nepříznivý dopad na provoz nebo bezpečnost organizace.
A.14.2.4	Omezení změn softwarových balíků	*Opatření* Modifikace softwarových balíků musí být omezeny na nezbytné změny a veškeré prováděné změny musí být přísně řízeny.
A.14.2.5	Principy budování bezpečných systémů	*Opatření* Principy budování bezpečných systémů musí být ustaveny, dokumentovány, udržovány a aplikovány při implementaci informačních systémů.
A.14.2.6	Prostředí bezpečného vývoje	*Opatření* Pro vývoj systémů a jejich integraci, pokrývající celý životní cyklus vývoje systémů, musí organizace vytvořit a přiměřeně chránit prostředí bezpečného vývoje systémů.
A.14.2.7	Outsourcovaný vývoj	*Opatření* Organizace musí dohlížet a monitorovat činnosti outsourcovaného vývoje systémů.
A.14.2.8	Testování bezpečnosti systémů	*Opatření* během vývoje musí být prováděno testování funkčnosti bezpečnosti.
A.14.2.9	Testování akceptace systémů	*Opatření* Pro nové informační systémy, aktualizace a nové verze musí být ustaveny testovací postupy a odpovídající kritéria akceptace.
A.14.3 Data pro testování		
Cíl: Zajistit ochranu dat používaných pro testování.		
A.14.3.1	Ochrana dat pro testování	*Opatření* Data pro testování musí být pečlivě vybrána, chráněna a kontrolována.

A.15 Dodavatelské vztahy		
A.15.1 Bezpečnost informací v dodavatelských vztazích		
Cíl: Zajistit ochranu aktiv organizace, ke kterým mají dodavatelé přístup.		
A.15.1.1	Politika bezpečnosti informací pro dodavatelské vztahy	*Opatření* Požadavky bezpečnosti informací na snížení rizik spojených s přístupem dodavatelů k aktivům organizace musí být odsouhlaseny s dadavateli a dokumentovány.
A.15.1.2	Bezpečnostní požadavky v dohodách s dodavateli	*Opatření* Všechny požadavky relevantní bezpečnosti informací musí být ustaveny a odsouhlaseny s každým dodavatelem, který může přistupovat k informacím organizace, zpracovávat je, ukládat, komunikovat nebo je zajišťovat prvky IT infrastruktury.
A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	*Opatření* Dohody s dodavateli musí zahrnovat požadavky na rizika bezpečnosti informací spojená s dodavatelským řetězcem služeb a produktů informačních a komunikačních technologií.
A.15.2 Řízení dodávek služeb dodavatelů		
Cíl: Udržovat dohodnutou úroveň bezpečnosti informací a dodávky služeb ve shodě s dodavatelskými dohodami.		
A.15.2.1	Monitorování a přezkoumávání služeb dodavatelů	*Opatření* Organizace musí pravidelně monitorovat, přezkoumávat a auditovat dodávky služeb dodavatelů.
A.15.2.2	Řízení změn ve službách dodavatelů	*Opatření* Změny v poskytování služeb dodavateli, včetně změn v udržování a zlepšování existujících politik, postupů a opatření bezpečnosti informací, musí být řízeny s ohledem na kritičnost informací, systému a procesů organizace, které jsou součástí těchto změn, a s ohledem na opakované posouzení rizik.
A.16 Řízení incidentů bezpečnosti informací		
A.16.1 Řízení incidentů bezpečnosti informací a zlepšování		
Cíl: Zajistit odpovídající a efektivní přístup ke zvládání incidentů bezpečnosti informací zahrnujícímu komunikaci ohledně bezpečnostních událostí a slabých míst.		
A.16.1.1	Posouzení a rozhodnutí o událostech bezpečnosti informací	*Opatření* Události bezpečnosti informací musí být posouzeny a musí být rozhodnuto, zda mají být klasifikovány jako incidenty bezpečnosti informací.

A.16.1.2	Hlášení událostí bezpečnosti informací	*Opatření* Události bezpečnosti informací musí být co nejrychleji hlášeny příslušnými řídícími kanály.
A.16.1.3	Hlášení slabých míst bezpečnosti informací	*Opatření* Po zaměstnancích a smluvních stranách používající informační systémy a služby musí být vyžadováno, aby si všímali a hlásili jakákoliv slabá místa bezpečnosti informací v systémech nebo službách nebo podezření na ně.
A.16.1.4	Odpovědnosti a postupy	*Opatření* Pro zajištění rychlé, efektivní a systematické reakce na incidenty bezpečnosti informací musí být ustaveny odpovědnosti a postupy pro zvládání incidentů bezpečnosti informací.
A.16.1.5	Reakce na incidenty bezpečnosti informací	*Opatření* Reakce na incidenty bezpečnosti informací musí být v souladu s dokumentovanými postupy.
A.16.1.6	Ponaučení z incidentů bezpečnosti informací	*Opatření* Znalosti získané z analýzy a řešení incidentů bezpečnosti informací musí být použity ke snížení pravděpodobnosti nebo dopadu následných incidentů.
A.16.1.7	Shromažďování důkazů	*Opatření* Organizace musí definovat a aplikovat postupy pro identifikaci, sběr, získání a uchování informací, které můžou sloužit jako důkazy.
A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací		
A.17.1 Kontinuita bezpečnosti informací		
Cíl: Kontinuita bezpečnosti informací musí být součástí systémů řízení kontinuity činností organizace.		
A.17.1.1	Plánování kontinuity bezpečnosti informací	*Opatření* Organizace musí určit svoje požadavky na bezpečnost informací a kontinuitu řízení bezpečnosti informací při nepříznivých situacích, například během krizí, katastrof nebo havárií.
A.17.1.2	Implementace kontinuity bezpečnosti informací	*Opatření* Organizace musí ustavit, dokumentovat, implementovat a udržovat procesy, postupy a opatření k zajištění požadované úrovně kontinuity pro bezpečnost informací během nepříznivých situací.

A.17.1.3	Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací	*Opatření* Organizace musí v pravidelných intervalech verifikovat ustavená a implementovaná opatření kontinuity bezpečnosti informací, aby zajistila, že jsou dostatečná a efektivní během nepříznivých situací.
A.17.2 Redundance		
Cíl: Zajistit dostupnost vybavení pro zpracování informací.		
A.17.2.1	Dostupnost vybavení pro zpracování informací	*Opatření* Vybavení pro zpracování informací musí být implementováno s dostatečnou redundancí, aby byly splněny požadavky na dostupnost.
A.18 Soulad s požadavky		
A.18.1 Soulad s právními a smluvními požadavky		
Cíl: Vyvarovat se porušení zákonných, předpisových nebo smluvních povinností týkající se bezpečnosti informací a jakýchkoliv bezpečnostních požadavků.		
A.18.1.1	Identifikace odpovídající legislativy a smluvních požadavků	*Opatření* Pro každý informační systém a organizaci musí být jednoznačně identifikovány, dokumentovány a udržovány aktuální veškeré relevantní zákonné, předpisové a smluvní požadavky a způsob, jakým se organizace dodržuje.
A.18.1.2	Ochrana duševního vlastnictví	*Opatření* Pro zajištění souladu se zákonnými, předpisovými a smluvními požadavky, které jsou relevantní ochraně duševního vlastnictví a používání proprietárních softwarových produktů, musí být implementovány vhodné postupy.
A.18.1.3	Ochrana záznamů	*Opatření* Záznamy musí být chráněny proti ztrátě, zničení padělání a neautorizovanému přístupu a zveřejnění, a to v souladu se zákonnými, předpisovými a smluvními požadavky a požadavky týkající se činností organizace.
A.18.1.4	Soukromí a ochrana osobních údajů	*Opatření* Soukromí a ochrana osobních údajů musí být zajištěny v souladu s odpovídající legislativou a s předpisy, pokud je to použitelné.
A.18.1.5	Regulace kryptografických opatření	*Opatření* Kryptografická opatření musí být používána v souladu s příslušnými úmluvami, legislativou a předpisy.

A.18.2. Přezkoumání bezpečnosti informací		
Cíl: Zajistit, že bezpečnost informací je implementována a provozována v souladu s politikami a postupy organizacemi.		
A.18.2.1	Nezávislá přezkoumání bezpečnosti informací	*Opatření* Přístup organizace k řízení a implementaci bezpečnosti informací (tj. cílů opatření, jednotlivých opatření, politik, procesů a postupů bezpečnosti informací) musí být nezávisle přezkoumáván v plánovaných intervalech, nebo když nastane významná změna.
A.18.2.2	Shoda s bezpečnostními politikami a normami	*Opatření* Vedoucí pracovníci musí pravidelně přezkoumávat shodu zpracování informací a postupů v rozsahu jejich odpovědnosti s odpovídajícími bezpečnostními politikami, normami a dalšími požadavky na bezpečnost.
A.18.2.3	Přezkoumání technické shody	*Opatření* Informační systémy musí být pravidelně přezkoumávány, zda jsou v souladu s politikami a normami bezpečnosti informací organizace.

Příloha C

Příklady typických hrozeb

Seznam typických hrozeb může být využit v rámci procesu posouzení hrozeb. Typy zdroje: **A** (accidental – náhodný), **D** (deliberate – úmyslný), **E** (environment – přírodní). [23]

Tabulka C.1: Příklady typických hrozeb. Zdroj [norma 27005].

Typ	**Hrozby**	**Zdroj**
Fyzické hrozby	Požár	A, D, E
	Poškození vodou	A, D, E
	Znečištění	A, D, E
	Závažná nehoda	A, D, E
	Zničení zařízení nebo médií	A, D, E
	Prach, koroze, zamrznutí	A, D, E
Přírodní události	Klimatický jev	E
	Seizmický jev	E
	Sopečný jev	E
	Meteorologický jev	E
	Povodeň	E
Ztráta základních služeb	Selhání klimatizace nebo dodávky vody	A, D
	Přerušení dodávky elektřiny	A, D, E
	Selhání telekomunikačního zařízení	A, D
Poruchy způsobené zářením	Elektromagnetické záření	A, D, E
	Termální záření	A, D, E
	Elektromagnetické impulzy	A, D, E
Technické selhání	Selhání zářením	A
	Chybné fungování zařízení	A
	Přetížení informačního systému	A, D
	Chybné fungování aplikačního programového vybavení	A
	Chyba údržby	A, D

Typ	**Hrozby**	**Zdroj**
Ohrožení informací	Zachycení kompromitujících interferenčních signálů	D
	Vzdálená špionáž	D
	Odposlech	D
	Krádež médií nebo dokumentů	D
	Krádež zařízení	D
	Zprovoznění recyklovaných nebo vyřazených médií	D
	Vyzrazení	A, D
	Data pocházející z nedůvěryhodných zdrojů	A, D
	Falšování pomocí technického vybavení	D
	Falšování pomocí aplikačního programového vybavení	A, D
	Odhalení pozice	D
Neoprávněné činnosti	Neoprávněné použití zařízení	D
	Podvodné kopírování aplikačního programového vybavení	D
	Použití padělaného nebo zkopírovaného aplikačního programového vybavení	A, D
	Poškození dat	D
	Nezákonné zpracování dat	D
Ohrožení funkčnosti	Chyba v používání	A
	Zneužití oprávnění	A, D
	Falšování práv	D
	Odepření činnosti	D
	Nedostatek personálu	A, D, E

Tabulka C.2: Možné hrozby, jeho motivace a důsledky. Zdroj [norma 27005].

Zdroj hrozby	**Motivace**	**Možné důsledky**
Hacker, cracker	Výzva Ego Rebelie Prestiž Peníze	• Hacking • Sociální inženýrství • Narušení a prolomení systému • Neoprávněný přístup do systému
Počítačová kriminalita	Zničení informací Nezákonné prozrazení informací Finanční prospěch Neoprávněné vyzrazení dat	• Počítačový zločin (např. kybernetické pronásledování) • Podvodné jednání (např. odpovídání, imitace, zachycení) • Získání informace za úplatu • Spoofing • Průnik do systému
Terorismus	Vydírání Zničení Vykořisťování Odplata Politický prospěch Zviditelnění v médiích	• Bombové útoky/Terorismus • Informační válka • Útok na systém (např. útok odmítnutí služby, DoS) • Průnik do systému • Porušení systému
Průmyslová špionáž (zpravodajské služby, společnosti, zahraniční vlády, ostatní vládní zájmy)	Ekonomická špionáž Konkurenční výhoda	• Vojenské zvýhodnění • Politická zvýhodnění • Ekonomické zneužití • Krádež informací • Průnik do soukromí • Sociální inženýrství • Průnik do systému • Neoprávněný přístup do systému (přístup ke klasifikovaným aktivum a technologickým informacím)

Zdroj hrozby	**Motivace**	**Možné důsledky**
Interní pracovníci (špatné zaškolení, nespokojení, škodolibí, nedbalí, nečestní nebo zaměstnanci s ukončeným pracovním poměrem)	Zvědavost Ego Vyzvědačství Finanční prospěch Odplata Neúmyslné chyby a opomenutí (např. chybné vložení dat, chyba při programování	• Napadení zaměstnance • Vydírání • Prohlížení chráněných informací • Zneužití počítačů • Podvod a krádež • Získání informace za úplatu • Vložení falešných nebo upravených dat • Narušení komunikace • Škodlivý kód (např. virus, logická bomba, trojský kůň) • Prodej osobních údajů • Chyby systému • Průnik do systému • Sabotáž systému • Neoprávněný přístup do systému

Příloha D

Příklady zranitelnosti

Následující tabulka ukazuje příklady zranitelnosti pro různé oblasti bezpečnosti, včetně příklady hrozeb, které dané zranitelnosti mohou využít. Tento podklad slouží pro posouzení hrozeb a zranitelnosti a k určení relevantních scénářů incidentů. [norma 27005]

Tabulka D.1: Příklady zranitelnosti. Zdroj [norma 27005].

Skupiny	**Příklady zranitelnosti**	**Příklady hrozeb**
Hardware	Nedostatečná údržba/chybná instalace záznamových médií	Chyba údržby systému
	Nedodržení pravidelné výměny	Zničení zařízení nebo médií
	Citlivost na vlhkost, prach, zašpinění	Prach, koroze, zamrznutí
	Citlivost na elektromagnetickou radiaci	Elektromagnetické záření
	Nedostatek v účinném nastavení změnového řízení	Chyba použití
	Citlivost na změny napětí	Přerušení dodávky elektřiny
	Citlivost na změny teploty	Meteorologický jev
	Nechráněné uskladnění	Krádež médií nebo dokumentů
	Nedostatečné postupy likvidace	Krádež médií nebo dokumentů
	Nekontrolovatelné kopírování	Krádež médií nebo dokumentů

Skupiny	Příklady zranitelnosti	Příklady hrozeb
Software	Žádné nebo nedostatečné testování programu	Zneužití oprávnění
	Známé chyby v programech	Zneužití oprávnění
	Neodhlášení se při opouštění pracovní stanice	Zneužití oprávnění
	Vyřazení nebo opětovné použití záznamových médií bez důkladného vymazání	Zneužití oprávnění
	Neprovádění logování událostí	Zneužití oprávnění
	Chybné přiřazení přístupových práv	Zneužití oprávnění
	Široce rozšířené programy	Poškození dat
	Použití aplikačních programů na špatná data z hlediska času	Poškození dat
	Složité uživatelské rozhraní	Chyba použití
	Nedostatečná dokumentace	Chyba použití
	Špatná nastavení parametrů	Chyba použití
	Nesprávný datum	Chyba použití
	Nedostatečná identifikace a autentizace, např. autentizace uživatele	Falšování práv
	Nechráněné tabulky s hesly	Falšování práv
	Špatná správa hesel	Falšování práv
	Spuštění nepotřebných služeb	Nezákonné zpracování dat
	Neodladěný nebo nový program	Chybné fungování aplikačního programového vybavení
	Nejasné nebo neúplné zadání pro vývojáře	Chybné fungování aplikačního programového vybavení
	Nedostatečné řízení změn	Chybné fungování aplikačního programového vybavení
	Nekontrolované stahování a užívání programů	Chybné fungování aplikačního programového
	Nedostatečné zálohování	Falšování pomocí aplikačního programového vybavení
	Nedostatečná fyzická ochrana budov, dveří a oken	Krádež médií nebo dokumentů
	Chyba v produkci reportů pro management	Neoprávněné použití zařízení

Skupiny	Příklady zranitelnosti	Příklady hrozeb
Sítě	Nedostatečné ověřování posílání a přijímání zpráv	Odepření činností
	Nechráněné komunikační linky	Odposlech
	Nechráněný citlivý provoz přenosu	Odposlech
	Nekvalitní kabelové spojení	Selhání telekomunikačního zařízení
	Bod totálního selhání	Selhání telekomunikačního zařízení
	Nedostatečná identifikace a autentizace, např. Autentizace uživatele	Falšování práv
	Nedostatečná bezpečná síťová architektura	Vzdálená špionáž
	Přenos odkrytých hesel	Vzdálená špionáž
	Nedostatečné řízení sítí (odolnost směrování)	Přetížení informačního systému
	Nechráněné připojení do veřejné sítě	Neoprávněné použití zařízení
Zaměstnanci	Nepřiměřená nebo nedbalá kontrola fyzického přístupu do budov, místností a kanceláří	Nedostatek personálu
	Nedostatečné postupy pro nábor pracovníků	Zničení zařízení nebo médií
	Nedostatečné bezpečnostní školení	Chyba použití
	Nesprávné použití aplikačního programového a technického vybavení	Chyba použití
	Nedostatek povědomí o bezpečnosti	Chyba použití
	Nedostatek kontrolních mechanizmů	Nezákonné zpracování dat
	Nedostatečná kontrola práce externích zaměstnanců nebo zaměstnanců zabezpečujících úklid	Krádež médií nebo dokumentů
	Nedostatek politik pro použití telekomunikačních prostředků a posílání zpráv	Neoprávněné použití zařízení

Skupiny	Příklady zranitelnosti	Příklady hrozeb
Lokality	Nepřiměřená nebo nedbalá kontrola fyzického přístupu do budov, místností a kanceláří	Zničení zařízení nebo médií
	Poloha v zátopové oblasti	Povodeň
	Nestabilní elektrická síť	Přerušení dodávky elektřiny
	Nedostatečná fyzická ochrana budov, dveří a oken	Krádež zařízení
Organizace	Nedostatečný formální postup při registraci a zrušení registrace uživatele	Zneužití oprávnění
	Nedostatečný formální postup při revizi uživatelských práv	Zneužití oprávnění
	Nedostatečné nebo neúplné zajištění (bezpečnosti) ve smlouvách se zákazníky a/nebo třetími stranami	Zneužití oprávnění
	Nedostatky v postupech pro monitorování prostředků pro zpracování informací	Zneužití oprávnění
	Nedostatečné provádění pravidelných auditů (dohledu)	Zneužití oprávnění
	Nedostatky v postupech pro identifikaci a posouzení rizik	Zneužití oprávnění
	Nedostatečné chybové záznamy v logu evidujícím činnosti správců a administrátorů	Zneužití oprávnění
	Nedostatečná odezva pracovníků údržby systému	Chyba údržby systému
	Nedostatečná nebo neúplná smlouva o úrovni služeb	Chyba údržby systému
	Nedostatky v postupech pro řízení změn	Chyba údržby systému
	Nedostatky v postupech pro řízení dokumentace ISMS	Poškození dat
	Nedostatky ve formálních postupech pro revizi záznamů ISMS	Poškození dat
	Nedostatky ve formálním procesu pro autorizaci veřejně přístupných informací	Data pocházející z nedůvěryhodných zdrojů
	Nedostatky ve vhodném přidělení odpovědností za bezpečnost informací	Odepření činností

Skupiny	Příklady zranitelnosti	Příklady hrozeb
Organizace	Nedostatky v plánech kontinuity	Selhání zařízení
	Nedostatky v politice pro používání e-mailu	Chyba použití
	Nedostatečné postupy pro instalaci softwaru do operačních systémů	Chyba použití
	Nedostatečné záznamy v logu evidujícím činnosti správců a administrátorů	Chyba použití
	Nedostatky v postupech pro zacházení s klasifikovanými informacemi	Chyba použití
	Nedostatečně definované povinnosti informační bezpečnosti v popisu pracovních pozic	Chyba použití
	Nedostatečné nebo neúplné zajištění (bezpečnosti) ve smlouvách se zaměstnanci	Nezákonné zpracování dat
	Nedostatečně definované disciplinární řízení v případě vzniku incidentu týkajícího se bezpečnosti informací	Krádež zařízení
	Nedostatky ve formální politice pro používání mobilních zařízení	Krádež zařízení
	Nedostatečné kontroly zařízení mimo lokalitu	Krádež zařízení
	Nedostatečné dodržování pravidel prázdného stolu a prázdné obrazovky monitoru	Krádež médií nebo dokumentů
	Nedostatečný schvalovací proces prostředků pro zpracování informací	Krádež médií nebo dokumentů
	Nedostatečně definované monitorovací mechanizmy při narušení bezpečnosti	Krádež médií nebo dokumentů
	Nedostatek v přezkoumáních managementem	Neoprávněné použití zařízení
	Nedostatečné postupy hlášení bezpečnostních slabin	Neoprávněné použití zařízení
	Nedostatečné postupy pro zajištění souladu se zákony na ochranu duševního vlastnictví	Použití padělaného nebo zkopírovaného aplikačního programového vybavení

Příloha **E**

Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `src`
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF