Bezpečnostní audit a inovace bezpečnostní politiky informačních technologií ve firmě

Bc. František Podrazil

Diplomová práce
2017

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2016/2017

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. František Podrazil**
Osobní číslo:	**A15220**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Forma studia:	**kombinovaná**
Téma práce:	**Bezpečnostní audit a inovace bezpečnostní politiky informačních technologií ve firmě**
Téma anglicky:	**A Security Audit and the Innovation of the Information Technologies Security Policies in a Company**

Zásady pro vypracování:

1. **Proveďte literární rešerši a zpracujte metodické poznatky z oblasti auditů informačních technologií a procesních rámců pro řízení IS/IT.**
2. **Proveďte analýzu současného stavu bezpečnosti IS/IT v dané firmě.**
3. **Na základě této analýzy vypracujte hodnocení – vycházejte z mezinárodních procesních rámců.**
4. **Navrhněte inovaci bezpečnostní politiky firmy po dohodě s jejím vedením a následně implementujte.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **DOUCEK, Petr, Luděk NOVÁK, Lea NEDOMOVÁ a Vlasta SVATÁ. Řízení bezpečnosti informací. 2. vydání. Praha: Professional publishing, 2011. ISBN 978-80-7431-050-8.**
2. **ISACA. Cobit 5: A business framework for the governance and management of enterprise IT [online]. Rolling Meadows. IL: ISACA, 2012 [cit. 2014-01-27]. ISBN 978-160-4202-373. Dostupné z: http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx.**
3. **DOBDA , Luboš. Ochrana dat v informačních systémech. Praha : Grada, 2001. 288 s. ISBN 8071694797.**
4. **Information Systems Audit and Control Association. Dostupné z: https://www.isaca.org/Pages/default.aspx.**
5. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Praga: Computer Press, 2004. 200 s. ISBN 80-251-0106-1.**

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **3. února 2017**

Termín odevzdání diplomové práce: **16. května 2017**

Ve Zlíně dne 3. února 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne …….

podpis diplomanta

ABSTRAKT

V Teoretické části práce je popsána základní terminologii v oblasti auditů informačních technologií s využitím mezinárodních procesních rámců. Praktická část obsahuje analýzu současného stavu bezpečnosti informačních technologií v konkrétní firmě. Na základě této analýzy jsou identifikovány hrozby, stanovena rizika a ohodnocen systém společnosti z pohledu bezpečnosti. Toto hodnocení bylo předloženo a konzultováno s vedením společnosti dané firmy a následné byla navržena vhodná inovace bezpečnostní politiky firmy.

Klíčová slova: bezpečnostní audit, ISO, COBIT, ITIL, ISMS, analýza, interní směrnice, bezpečnostní politika

ABSTRACT

Theoretical part of the thesis describes the basic terminology in the field of information technology auditing using international process framework. Practical part includes an analysis of the current state of information technology safety in a particular company. On the basis of the analysis, potential threats have been identified, risks assessed and company system evaluated from safety point of view. The evaluation was submitted for consultation with the company related and consequently, after discussion, suitable security policity innovations were suggested.

Keywords: Security Audit, ISO, COBIT, ITIL, ISMS, Analysis, Internal guidelines, Security Policy

Poděkování, motto a čestné prohlášení, že odevzdaná verze bakalářské/diplomové práce a verze elektronická, nahraná do IS/STAG jsou totožné ve znění:

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

OBSAH

ÚVOD

Informační technologie se neustále vyvíjí a stále více a více se stávají součástí každodenního osobního i pracovního života, každého s nás. V současné uspěchané době spousta lidí téměř nedělá, rozdílí mezi služební a soukromím zařízením. Téměř všichni využívají soukromé zařízení pro pracovní účely a služební zařízení pro soukromé. Jen málo kdo nevyužije možnosti okamžitého přístupu k firemním informacím v mobilu nebo nevyužije služební laptop k soukromím účelům někde na služební cestě. Trendy v IT stále více využívají vzdálených přístupů nebo ovládání vědí IoT. Právě proto firmy stále více požadují větší výkonost a transparentnost v oblasti IT. Ve většině malých a středních organizací se snažili vystačit s jedním správcem nebo ideálně zajištěním celého IT externím dodavatelem. V těchto případech ovšem firma jen málo kdy má vůbec nějaký přehled o výkonu nebo o stavu bezpečnosti. Jelikož pracovníci se u těchto externích firem často mění, tak s každou změnou vždy odejdou nějaké zkušenosti a informace. Nastává potencionální možnost úniku informací.

Právě pro kompletní přehled a vyšší kvalitu IT služeb jsou využívány auditní rámce díky, kterým je možné ohodnotit kvalitu, výkon oddělení jako celku nebo konkrétních zaměstnanců. Díky vyšší kvalitě služeb mezi, které je počítána i bezpečnost, která je jedním s klíčových bodů, které se dnes řeší po celém světě. Jelikož únik informací nebo napadení a vyřazení systémů firmy může být pro spoustu firem existenčním. S tohoto důvodu jsou dnes ve všech firmách nastaveny nejrůznější bezpečnostní politiky a nařízení, která mají firmy chránit nejen před útokem zvenčí, ale i před zaměstnanci samotnými. Nejčastějším příčinou narušení bezpečnosti firem jsou právě její zaměstnanci, kteří úmyslně nebo z nedbalosti porušují tyto základní pravidla bezpečnosti a můžou způsobit újmu na majetku svého zaměstnavatele. Bezpečnostní audit může mimo jiné odhalit, která pravidla se nejčastěji porušují a pomoci vytvořit opatření, která tomu budou předcházet.

Právě auditem v oblasti IT se tato práce zabývá, jelikož je to aktuální a přínosné téma v každé firmě. Je zde popsáno několik metodik a rámců, kde každý má své přednosti a nedostatky a na základě analýzy je pak vybrán rámec, který je nejvhodnější pro konkrétní firmu.

I. TEORETICKÁ ČÁST

1 AUDIT IT A JEHO STANDARDY

V dnešní je plošné využívání informačních a telekomunikačních technologií (ICT) ve firmách běžným standardem. Se stoupající modernizací a automatizací ve firmách zároveň i stoupá jejich závislost na kvalitě a funkčnosti a zabezpečení využívaných ICT služeb a procesů. Prosazení vyšší míry spolehlivosti, bezpečnosti a účinností u všech informačních systémů (IS) se tak stává jednou z hlavních odpovědností vedení každé organizace a odpovědných osob v oblasti informatiky.[1]

1.1 Princip a základní pojmy auditu

Pro řízení a kontrolu skutečného stavu bezpečnosti ve firmě je důležité využívat vhodné techniky a nástroje. V praxi jsou využívány různé druhy technik, metodik a rámců pro provádění auditu[1] společností.[1]

1.1.1 Principy auditu

Audity a jejich provádění je spojeno s respektováním řady zásad a pravidel. Spolehlivost a efektivnost auditů je přímo spojena s dodržováním těchto zásad (Obr. 1). Audit je účinný nástroj pro podporu řízení, který poskytuje důležité informace pro zlepšování systému řízení.[1]

Obrázek 1: Zásady a pravidla auditu [1]

[1] Audit - systematický, nezávislý a dokumentovaný proces získání důkazů a jejich hodnocení s cílem stanovit rozsah plnění definovaných kritérií tohoto procesu. [16]

1.1.2 Základní typy auditu

Audity jsou příliš komplexní a z toho důvodu je možné je dělit na několik možných odvětví. Z různého hlediska provádění auditu IS.[1]

Z hlediska použití výsledků

- Audity první stranou, které si provádí organizace sama za účelem sebe ověření.
- Audity druhou stranou jsou prováděny externí firmou, která má vůči auditované organizaci nějaký smluvní vztah a má zájem na auditované organizaci.
- Audity třetí stranou jsou prováděny externí společností za účelem certifikace auditovaného subjektu.[1]

Z hlediska úrovně aplikace auditu

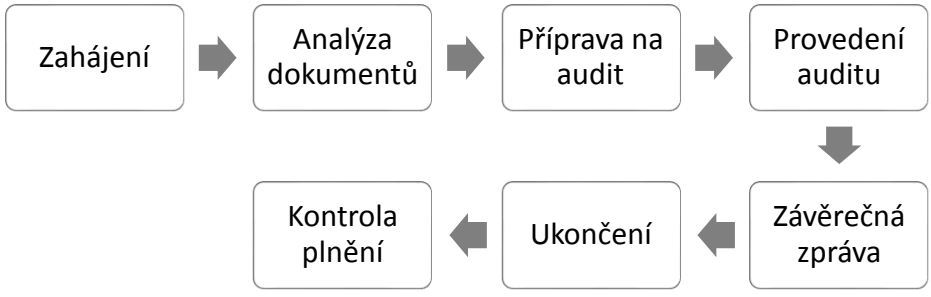
- Technický audit má ověřit shodu mezi objektivní realitou a systémem řízní a je pracováno se správnými a kvalitními informacemi.
- Profesionální audit má ověřit shodu mezi jednotlivými výstupy ze společnosti.[4]

Z hlediska vykonavatele auditu

- Interní audit prováděný v rámci organizace.
- Externí audit prováděný externí společností nebo pracovníkem.[4]

1.1.3 Obecný postup auditu

Auditní fáze systému bezpečnosti informací mají různé posloupnosti a názvy dle použitých metodik a norem. Na níže uvedeném obrázku (Obr. 2) jsou tyto fáze vyobrazeny dle normy ISO/IEC 27007 až 27009.



Obrázek 2: Schéma obecného postupu auditu [4]

V první fázi s názvem zahájení se vytváří tým auditoru a volí vedoucí auditorského týmu, určuje se rozsah, definice cílů a vyhodnocení proveditelnosti auditu. V této fázi nejsou prováděny žádné přímé kroky s prováděním auditu. V následující fázi analýzy dokumentace

se zaobírá převážně dokumentací k systému řízení informační bezpečnosti a provádí se hodnocení všech definovaných kritérií. Fáze přípravy na audit probíhá již přímo v auditované firmě a obsahuje detailní přípravu plánu auditu. Ve fázi provedení auditu spočívá v testování jednotlivých kontrol, které byly analyzovány a vyhodnoceny jako efektivní. Ke všem testům je evidována veškerá dokumentace. Výsledek auditu obsahuje závěrečná zpráva, která je určena převážně pro vedení organizace. V poslední fázi plnění kontroly se vytvoří plán sledování provedených změn.[1, 16]

1.2 Zákony a normy

Informace jsou v dnešní době jedním z nejdůležitějších pilířů, každé společností. Ztráta firemních informací jako jsou know-how, strategického řízení firmy nebo databáze klientů může mít kritické následky jako ztrátu důvěryhodnosti, dobré pověsti a klientů. V souvislosti s tímto nebezpečím se po celém světě zavádějí kybernetické zákony a normy, které mají zajistit bezpečnost informací jednotlivých firem.[1, 19]

1.2.1 Legislativní požadavky

Bezpečnost komunikačních a informačních systémů je stav, kdy je zachována důvěrnost, integrita a dostupnost informací, s nimiž tyto systémy nakládají, integrita a dostupnost systémových služeb a prostředků a odpovědnost uživatelů za jejich činnost v těchto systémech. Od 1. 1. 2015 vstoupil v platnost zákon o kybernetické bezpečnosti. Díky kterému jsou povinné subjekty nuceny zavést požadovaná technická a organizační bezpečnostní opatření. Spolu s vydáním tohoto zákona byly upraveny i další související zákony (tab. 1) Schéma bezpečnostního zákona (příloha P I).[19]

Tabulka 1: Zákony spojené s bezpečností informací

Zákon č.	181/2014 Sb.	O kybernetické bezpečnosti
Zákon č.	148/1998 Sb.	O ochraně utajovaných skutečností
Zákon č.	412/2005 Sb.	O ochraně utajovaných informací a bezpečnostní způsobilosti
Zákon č.	227/2000 Sb.	O elektronickém podpisu
Zákon č.	127/2005 Sb.	O elektronických komunikacích
Zákon č.	365/2000 Sb.	O informačních systémech veřejné správy
Zákon č.	101/2000 Sb.	O ochraně osobních údajů

1.2.2 Bezpečnostní standardy

Systém řízení bezpečnosti informací (Information Security Management System – ISMS) je systém k zajištění bezpečnosti informačních aktiv, řízení rizik bezpečnosti informací a zavedení opatření, která jsou následně kontrolována. ISMS může být zaveden nejen pro specifický informační systém, ale může zahrnout celou organizaci. Pro řadu organizací, jsou informace a informační technologie klíčové a proto se rozhoduje, jak zajistit jejich bezpečnost. Tuto problematiku řeší systémový a komplexní přístup, proto jsou základním vodítkem v této oblasti ISO normy (tab. 2) a jiné mezinárodní normy.[1, 19]

Tabulka 2: ISO/IEC normy

ČSN ISO/IEC 27000	ISMS řízení bezpečnosti informaci
ČSN ISO/IEC 13335	Směrnice pro řízení bezpečnosti IT
ČSN ISO/IEC 15408	Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT

Normy ISO/IEC 27001 a ISO/IEC 27002 spadají do rodiny ISO/IEC 27000 jsou úzce spojeny, každá však plní zcela jinou roli. Norma ISO 27001 specifikuje jak v organizaci nastavit, implementovat, monitorovat, udržovat a zlepšovat ISMS organizace a norma ISO 27002 obsahuje přehled bezpečnostních opatření pro budování ISMS.

Německá spolková republika má své vlastní standardy (tab. 3) vycházející z ISO 27000 a rozšířené o „best practices“, pro řízení životního cyklu IT společnosti. [1, 4]

Tabulka 3: Německé normy BSI Standard 100

BSI-Standard 100-1	ISMS řízení bezpečnosti informaci
BSI-Standard 100-2	Metodika IT Protection Baseline
BSI-Standard 100-3	Analýza rizik na základě IT Protection Baseline
BSI-Standard 100-4	Business Continuity Management

Další zemí, která má své vlastní specifické standardy, jsou Spojené státy americké (tab. 4). V USA dle federálního zákona o managementu bezpečnosti informací. Je vyžadováno, aby každý úřad zavedl program bezpečnosti informací a to včetně všech služeb poskytovaných nebo řízených jiným dodavatelem. [1, 19]

Tabulka 4: Americké standardy FIPS PUB

FIPS PUB 199	Standardy pro kategorizaci bezpečnosti federálních informací
FIPS PUB 200	Minimální požadavky na bezpečnost informací

2 AUDITNÍ METODIKY A RÁMCE

Normy a postupy si musí každá organizace zvolit tak, aby vyhovovaly jejím požadavkům a potřebám. V tomto případě je možno využít nejrůznější ověřené praktiky, metody a rámce, které jsou ověřeny, vyvíjeny a navržený pro stále se měnící podnikové a informační prostředí. Mezi nejpoužívanější metodiky a nejlepší praktiky patří např. CRAMM, jež je metodikou a současně nástrojem pro analýzu a řízení rizik, COBIT, obsahující praktiky využívané při auditu informačních technologií a ITIL, knihovna nejlepších praktik popisující kompletní vývojový cyklus služeb a další, které jsou vyvíjeny od společností jako Microsoft nebo Hewlett-Packard (HP).[1]

2.1 ISO/IEC 27k

Mezinárodní rodina norem, která poskytuje kompletní přehled systému řízení bezpečnosti informací. ISMS poskytuje šablonu pro nastavení, implementování, ověření a udržování a neustálého zlepšování ochrany firemních aktiv. Je založen na hodnocení rizik a nastavení řešení rizik a jejich řízení. Scháma ISO/IEC 27K Family (viz. Příloha P II). [5]

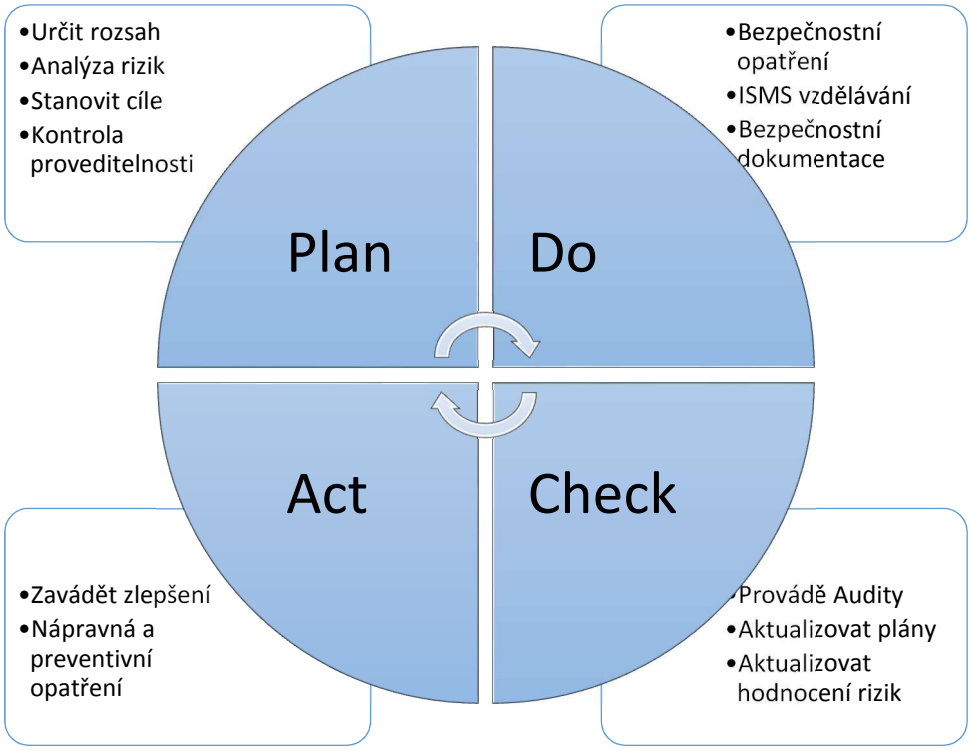
2.1.1 ISO/IEC 27001

ISO 27001 je základní normou celé rodiny ISO 27000, která poskytuje komplexní přístup k informační bezpečnosti v organizaci. Jsou v ní obsažena veškerá aktiva od elektronických dat, přes papírové dokumenty, informační a komunikační technologie až po firemní know-how. Obsahuje také rozvoj kvalifikace zaměstnanců a technickou ochranu proti počítačovým podvodům. [6, 7]

Tři základní principy ochrany informací dle ISO 27001:

- Důvěrnost - informace jsou přístupné pouze vyhrazeným osobám
- Celistvost – informace jsou správné a kompletní
- Dostupnost – uživatelé s oprávněním mají přístup k potřebným informacím

ISO 27001 je v souladu s ostatními systémy řízení, jako ISO 9001, zahrnuje kontinuální proces zlepšování celého systému řízení informační bezpečnosti pomocí integrovaného modelu Demingova cyklu Plan-Do-Check-Act (PDCA).[6, 7]



Obrázek 3: PDCA model

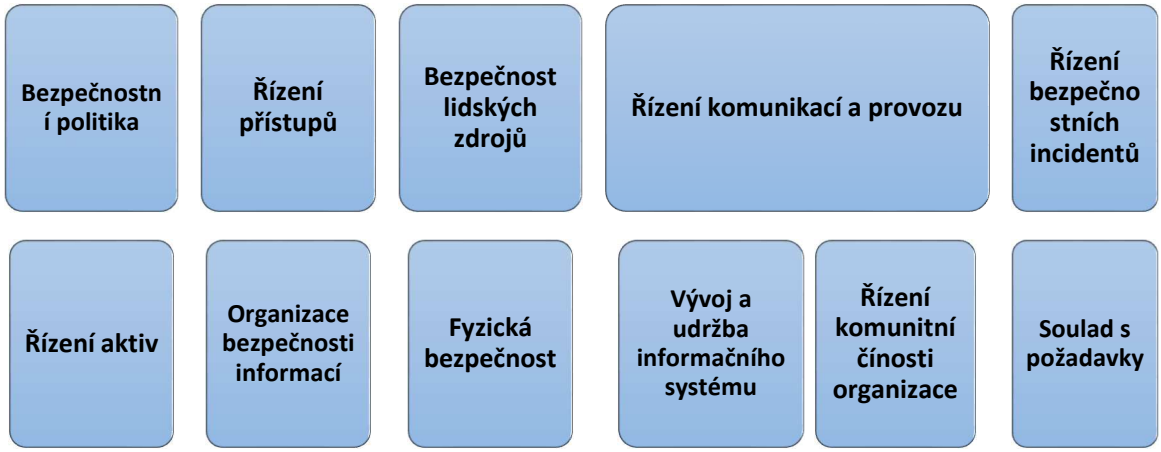
Během zavádění systému řízení bezpečnosti IT je nutné projít celý životní cyklus ISMS, tak jak je definovaný v ISO/IEC 27001:2005. Pro dosažení certifikace ISMS dle této normy je to nezbytné a i v případě, že certifikace není vyžadována, tak to lze jen doporučit.[6, 1]

2.1.2 ISO/IEC 27002

Tato mezinárodní norma je druhým základním pilířem ISMS. Je určena pro organizace jako doporučení pro výběr opatření v rámci procesu zavádění ISMS, založeného na normě ISO/IEC 27001. Jsou v ní obsažená tzv. nejlepší zkušenosti řízení bezpečnosti informací. Tato norma se rovněž využívá při vyvíjení směrnic organizací všech typů a velikostí. Bezpečnost, které může být dosaženo technickými prostředky, je omezená a měla by být podporována vhodným řízením a postupy. Identifikace opatření, která by měla být zavedena, vyžaduje pečlivé plánování a věnování pozornosti detailům. V obecnějším smyslu efektivní bezpečnost informací také zaručuje managementu a dalším zúčastněným stranám, že aktiva organizace jsou rozumně zabezpečena a chráněna proti poškození.[5, 6, 8]

V doporučení normy ISO/IEC 27002 je obsaženo přes 130 bezpečnostních opatření, která se dělí celkem do 11 oblastí (obr. 5). Jednou ze základních oblastí je bezpečnostní politika, která obsahuje definice základních pravidel schválených vedením organizace.

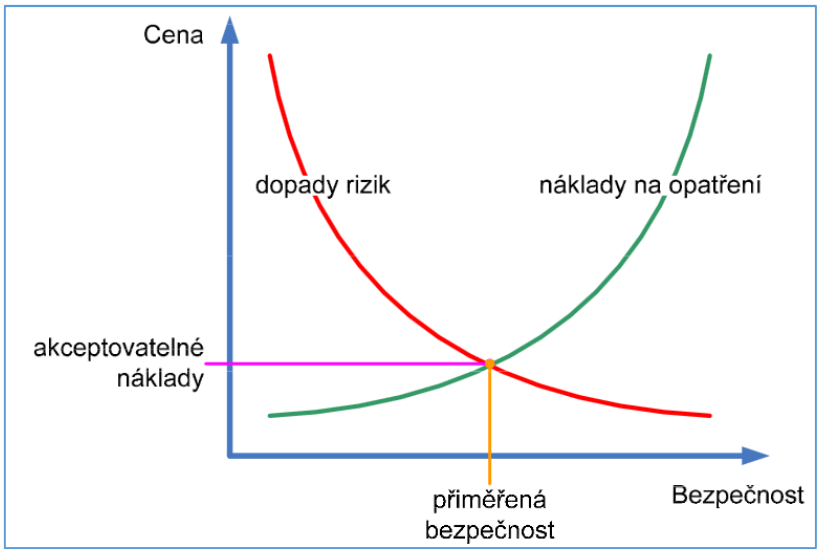
Organizace bezpečnosti upřesňuje řízení bezpečnosti s externími dodavateli. Řízení aktiv udržuje přehled o aktivech organizace. Bezpečnost lidských zdrojů má za úkol vymezení povinností všech pracovníků. Fyzická bezpečnost a řízení přístupu definují pravidla pro přístup do a v rámci organizace. Řízení komunikací zajišťuje spolehlivý a bezpeční chod všech systémů organizace. Vývoj a údržba systémů prosazují principy bezpečnosti do projektů rozvoje ICT. Zvládání bezpečnostních incidentů definuje pravidla pro řešení zvládání bezpečnostních incidentů a sběr všech potřebných dat. Řízení komunity činnosti organizace má za úkol pomocí prevence minimalizovat možné škody v případě havárií. Soulad s požadavky organizace dokazuje plnění právních a smluvních závazků. [15]



Obrázek 4: Dělení oblastí dle ISO/IEC 27002

2.2 CRAMM

Metodika, která byla původně vypracována pro potřeby britské státní správy. V dnešní době patří mezi nejrozšířenější používané metodiky, protože je určena pro všechny fáze životního cyklu systému. Od analýzy až k návrhu protiopatření. Metodika využívá nejnovější trendy v oblasti analýzy a řízení rizik informací. Obsahuje rozsáhlou knihovnu bezpečnostních protiopatření a pomáhá prokázat efektivnost výdajů na bezpečnostní protiopatření. Nástroj CRAMM umožňuje analýzy typu Expert nebo Expres. Velikost celkového úsilí a investic do bezpečnosti IS by mělo odpovídat hodnotě aktiv a míře možných rizik (obr. 6). [9]



Obrázek 5: Přiměřená bezpečnost [9]

2.2.1 Analýza CRAMM Expert

Jedná se o detailní analýzu, která se dělí na tři fáze. Při hodnocení rizik pomocí CRAMM Expert je nezbytné popsat do detailu celý systém, ohodnotit všechna aktiva, hrozby a posoudit zranitelnost. Celkové množství informací je značné a proto je nezbytné tyto činnosti vykonávat v rámci samostatného projektu. Zpravidla trvá několik týdnů i měsíců. [9]

1. V první fázi je třeba identifikovat veškerá aktiva a vytvořit model aktiv a určit hodnoty aktiv
2. Ve druhé fázi se určí míra hrozeb a zranitelnosti systému, stanoví se jejich úrovně a vypočítá míra rizika
3. V poslední třetí fázi se vytvoří návrh opatření na pokrytí identifikovaných rizik a zpracují se podklady pro implementaci těchto opatření

Základním výstupem třetí fáze je databáze opatření a tyto opatření se dělí celkem do pěti hlavních oblastí a to jsou IT bezpečnost, komunikační bezpečnost, personální bezpečnost, administrativní a fyzická bezpečnost.[9]

2.2.2 Analýza CRAMM Express

V analýze CRAMM Expres je umožněno provést analýzu celého systému během několika hodin a přesto jsou původní zásady metodiky CRAMM nedotčeny. Tuto variantu analýzy lze použít například jako rychlou variantu na startu projektu, protože veškeré informace je možné lehce převést do CRAMM Expert a následně provést detailní analýzu.[9]

2.3 COBIT

Rámec COBIT (Control Objectives for Information Technology) je soubor nejlepších praktik a postupů určen především osobám provádějícím audit. COBIT má pomoci dosáhnout cílů organizace pomocí efektivního využití dostupných zdrojů a minimalizací možných rizik. [7]

2.3.1 Historie COBIT

Rámec COBIT byl poprvé vydán organizací ISACA v roce 1996. Toto vydání obsahovalo rámec (framework). Ve druhém vydání z roku 1998 byl rámec rozšířen o auditní postupy (audit guidelines), procesy kontroly (control objectives) a implementační nástroje (implementation tools). Ve třetím vydání z roku 2000 byly přidány manažerské postupy (management guidelines), toto vydání již bylo vydáno institutem ITGI (IT Governance Institute) stejně jako následující verze COBIT 4.0 a 4.1 z roku 2005 a 2007, která byla rozšířena o management rizik (Risk managemant) a šablony procesů (compliance processes). V aktuální verzi COBIT 5 z roku 2012 je dosaženo konsolidace a integrace rámce COBIT 4.1, Val IT 2.0 and Risk IT a významně obsahuje rysy modelu BMIS (Business Model for Information Security) a ITAF (IT Assurance Framework).[2]

2.3.2 Novinky v COBIT 5

Podle definice je COBIT 5 jeden všezahrnující rámec, který obsahu jak ISO 38500, Risk IT a Val IT. Tím pomáhá vytvářet optimální přidanou hodnotu při optimálním riziku a využití IT zdrojů. Od předchozí verze jsou zavedeny nové principy COBIT, tyto principy se vzájemně doplňují a při jejich aplikaci není nutno rozlišovat dle velikosti organizace. Těchto principů je celkem 5. [2, 12]

Zajištění potřeb stakeholderů[2] jako jsou majitel, zaměstnanec nebo zákazník. Každá strana má své požadavky některé jsou shodné a některé protichůdné. Jednotlivé požadavky mají pro konkrétní zainteresovanou stranu hodnotu. Každá organizace se pokusí svých hodnot docílit. Hodnota vzniká ze všech získaných přínosů a pro jejich dosažení je třeba

[2] Stakeholders – v češtině se tomuto pojmu nejvíce přibližují „zainteresované strany.“

vynaložit prostředky a zdroje. To přináší určitá rizika a ta musí být přiměřená získané hodnotě.

Úplné pokrytí orrganizace ve smyslu spolupráce IT a jiných oddělení ve společném snažení a vytváření hodnot pro organizaci. Definování odpovědnosti a určení pravidel pro spolupráci.

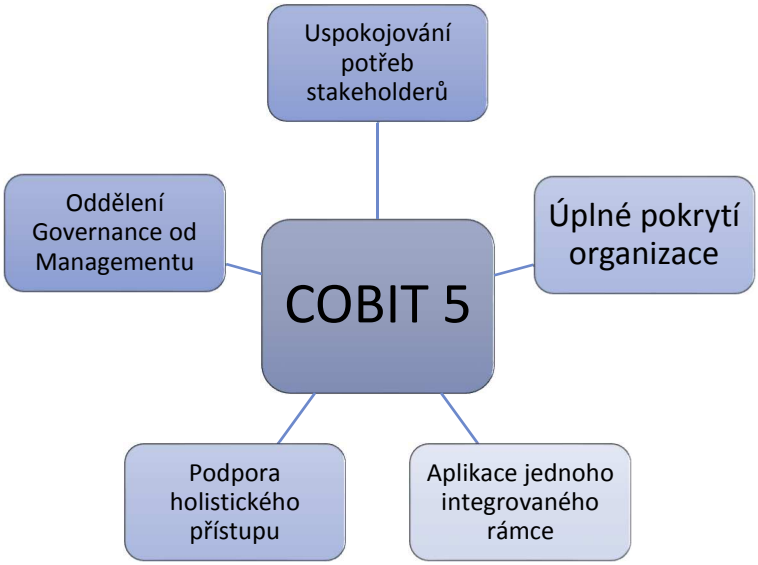
Oddělení Governance od Managementu má rozlišovat mezi každodenním řízením a kontrolování jednotlivých zaměstnanců a směřováním celé organizace neboli vedením společnosti. Toto rozdělení se vztahuje především k procesům, které se podle toho dělí.

Aplikace jednoho integrovaného rámce pro celou organizaci nejen pro oblast IT. Na světě je spousta doporučení, standardů a nejrůznějších rámců. Za Každým z těchto rámců stojí jiná organizace, která využívá jinou terminologii nebo jiný přístup. Některé se vzájemně doplňují a některé dokonce překrývají. Touto různou škálou přístupů a technologií je velice obtížné je vzájemně využívat. Proto se ISACA, snaží v COBITU o sjednocení pod jednou střechou. V prvopočátku se jedná hlavně o sjednocení všech rámců vytvořených sdružením ISACA. Tedy o rámce COBIT, RiskIT a ValIT. Tyto rámce byly vytvořeny, každý v jiném časovém období a každý se specializoval na jinou oblast. Tím se bohužel docílilo toho, že každý z nich měl jinou strukturu a terminologii. Sjednocením těchto rámců do dnešního COBIT 5 se docílilo odstranění těchto nedostatků a snadnější spolupráce. V další části jde o začlenění rámců od dalších organizací. V průběhu vývoje COBIT 5 se jednotlivé rámce vzájemně propojovaly a analyzovaly. Na tomto základě byla vytvořena v COBIT 5 další příloha na propojení jednotlivých procesů z různých rámců a standardů. V COBIT 5 jsou tedy definovány cíle a důvody pro procesy a rámce (obr. 7). Standardy následně určují způsob jejich realizace. [2, 12]

Podpora holistického přístupu každá prosperující firma vždy leží na zdravých základech. Z pohledu firmy je to těchto sedm pilířů (Enablers):

- Principy, politiky a rámce (principles, policies and frameworks) – definují pravidla hry pro každodenní práci.
- Procesy (processes) – definují činnosti jak dosahovat požadovaných výsledků a jednotlivá rozhraní.
- Organizační struktura firmy (organizational structure) – definuje způsob organizace do jednotlivých týmů a rozložení sil.

- Kultura, etika a chování (culture, ethics and behaviour) – určuje způsob chování jaký, je možné očekávat a určuje způsob komunikace v organizaci.
- Informace (information) – tok informací určuje, kde jsou informace potřeba a jakým způsobem se získavájí.
- Služby a infrastruktura (services and infrastructure) – jsou v ní definovány technické prostředky nutné k zajištění informací a jejich logického propojení.
- Lidi a znalosti (people and skills) – definuje, požadavky na lidské zdroje, aby mohli plnit zadané cíle. [2, 12]



Obrázek 6: Pět principů COBIT 5 [2]

Potřeby malý a středních firem, které nemají management zabývající se pouze řízením organizace, ale plní řízení jednotlivých pracovníků. [2, 12]

- Menší počet pracovníků,
- jednodušší organizační struktura,
- větší transparentnost,
- je nutná větší flexibilita,
- role pracovníků se překrývají,
- nedostatek času na plánování,
- méně dostupných prostředků apod.

U implementace IT podle COBIT, je nutno si uvědomit situaci v malých a středních firmách, kde nebude žádný speciální útvar určený pro vedení a směrování organizace. Vrcholové vedení zajišťuje současně i roli středního managementu. Tedy každodenní řízení

výkonných pracovníků organizace. Vedoucí IT nebude pouze řídit a plánovat funkci IT oddělení, ale bude současně zastávat i práci specialisty nebo roli vedoucího na jiných odděleních. Ve značném množství organizací se dokonce s žádným IT oddělení nesetkáte. Bude zde pouze vyčleněný pracovník, který má za úkol směrovat činnost externích dodavatelů zajišťujících IT v organizaci. I přes to je potřeba jasně definovat a krátkodobé i dlouhodobé cíle IT a zajistit jejich realizaci, aby se IT nestalo pouze nákladovou položkou, ale mělo i svojí přidanou hodnotu pro organizaci. [2, 12]

2.3.3 Procesy COBIT 5

COBIT 5 obsahuje celkem 37 procesu a ty jsou rozděleny do dvou oblastí (viz příloha P3). Procesy pro vedení (Governance) jsou zaměřeny na část dlouhodobého plánování a vedení firmy a procesy pro řízení (Management) se zaměřují na každodenní řízení a chod firmy. V popisu každého procesu je vždy obsaženo.[14]

- Označení oblasti, do které proces spadá
- Popis procesu
- Tabulka cílů IT a procesu a souvisejících metrik
- Standardní RACI matici s definicí rolí a vztahů
- Seznam manažerských praktik
- Návazné návody

Governance procesy, někdy označované jako Evaluate, Direct and Monitor (EDM) vyhodnocení, přikazování a sledování, mají na starost zajištění zdrojů, minimalizaci rizik souvisejících s chodem společnosti, nastavení pravidel společnosti, pravidel dodávání a jasnou definice stakeholderů. [12, 14]

Management procesy se dále dělí na čtyři domény. APO (Align, Plan and Organise) roztřídění, plánování a organizace se zaobírá návrhem řešení a doručování služeb. Je v ní obsaženo celkem 13 procesů. BAI (Build, Acquire and Implement) vytváření akvizice a implementace vytváří a implementuje řešení pozdější služby je v ní celkem 10 procesů. DSS (Deliver, Service and Support) dodání, služby a podpora zpřístupňuje služby zákazníkovi a zajištuje podporu chodu služeb. V této doméně je celkem 6 procesů. MEA (Monitor, Evaluate and Assetss) sledování, vyhodnocení a audit sleduje procesy dodávané zákazníkovi a kontroluje plnění sjednaných služeb. [12, 14]

Procesy jsou COBIT 5 mají tzv. hodnoceni úrovně zralosti procesu (Process Capability), které určuje, v jakém stavu se proces v organizaci nachází. Hodnocení je v rozsahu od úrovně 0, kdy proces není implementován nebo nenaplňuje svůj účel po úroveň 5 kdy je proces optimální a neustále se zlepšuje.[14]

2.4 ITIL

Knihovnu ITIL[3] v základní publikaci tvoří celkem pět knih představujících rozsáhlý a všeobecně dostupný návod pro správu služeb IT.

- První kniha Service Strategy (strategie služeb) se zaobírá základním směrování na konkrétní cíle organizace.
- Druhá kniha Service Design (návrh služby) slouží pro navržení a optimalizaci služeb a procesů organizace.
- Třetí kniha Service Transition (přechod služby) obsahuje postupy pro návrh a zavádění nových a vylepšených služeb a procesů do organizace.
- Service operation (provoz služeb) se zavívá kvalitou procesů a služeb.
- V páté knize Continual Service Improvement (neustále zlepšování služeb) je popsáno trvalé a pravidelné zlepšování všech zavedených služeb.

Knihy vycházejí ze zkušeností a doporučení ze, kterých se postupně staly nejlepší praktiky. Každá kniha představuje jednu konkrétní fázi životního služby. [10, 11]

[3] ITIL – v některé literatuře je možno najít jako akronym pro IT Infrastructure Library, ovšem od zavedení aktuální verze se jedná o oficiální obchodní název pro procesně orientovaný rámec.

Obrázek 7: Životní cyklus IT služby [10]

Tento rámec poskytuje dostatečnou flexibilitu a možnost přizpůsobení se vlastním požadavkům a cílům konkrétní organizace. ITIL je dostupný rámec, obsahující celou řadu procesů podporujících chod služeb IT. Jedním ze základních pravidel pro práci s ITIL je adopt and adapt. [10, 11]

V rámci ITIL je nutno se vždy přizpůsobit dle potřeb každé konkrétní firmy a realizovat vše tak, aby bylo dosaženo požadavků a skutečných podmínek. Všechna řešení založená na ITIL odrážejí vždy konkrétní realizaci nebo jednu podpůrnou službu. Příčina spočívá ve struktuře knihovny, která nabízí každé organizaci poskytující služby IT základní orientaci pro jeho organizaci. Nezávisle na činnosti nebo velikosti organizace. Každý pokus převést ITIL z teorie do praxe bez přizpůsobení se je předurčen k neúspěchu. [10, 11]

2.4.1 Audit pomocí ITIL

Knihovna ITIL není auditní nástroj a nedá se podle něj přímo auditovat. Existují sice tzv. self-assessment[4] dotazníky, které posuzují míru shody s „best practice“. V dnešní době je však již ITIL plně kompatibilní s rámcem COBIT. Všechny základní principy se do značné míry shodují. Pouze z hlediska organizačně-procesního se tyto rámce mírně rozchází. V rámci ITIL jsou kladeny čtyři základní otázky, jejichž odpovědi nám určují další postup

[4] Self-assessment – Sebe hodnotící, jelikož mají za cíl ohodnotit své vlastní fungování.

při implementace procesů a neustálé optimalizaci služeb a činností spojených s dodáváním koncovému uživateli. [10, 20]

- Jaký je cíl?
- Jaký je současný stav?
- Co je třeba udělat pro dosažení cíle?
- Kdy budeme skutečně v cíli?

ITIL se zaměřuje převážně na vypracování detailního designu a zavedení procesů a taktického řízení služeb IT. Spojením s IT strategií vypracovanou podle auditního rámce COBIT.COBIT je vhodný pro provedení auditu a specifikace řízení IT částí, které nejsou plně pod kontrolou. Kombinace propojení IT strategie se strategií podniku. [20]

2.5 International Organization of Superme Audit Institutions

International Organization of Superme Audit Institutions (INTOSAI) zastřešuje organizace provádějící externí audity ve státní sféře. Tuto funkci v České republice plní Nejvyšší kontrolní úřad. INTOSAI má rozvětvenou organizační strukturu dělící se na oblastní pracovní skupiny, výbory a pracovní skupiny. Organizace SAI provádějí tři druhy auditů:

- Finanční audit – má za cíl prověřit správnost a úplnost vykazování finančních transakcí
- Výkonnostní audit – má za cíl prověřit efektivitu nakládání s prostředky
- Kvalitativní audit souladu se standardy – kontroluje dodržování norem a zákonů

Kvalitativní audit se většinou provádí společně s finančním auditem. Tento společný audit bývá také označován za audit správnosti. V roce 2007 byl vytvořen pro INTOSAI nový rámec, který má zpřehledňovat a navázat na standardy ISA (International Standards on Audit). Tyto standardy se zabývají převážně finančním auditem a jsou určující pro všechny organizace. Tyto standardy se dělí do několika kategorií jak je možno vidět v následující tabulce (tab. 5).[4]

Tabulka 5: Ogranizace dokumetů INTOSAI

Odpovědnost	
ISA 200	Cíle
ISA 210	Sjednávání podmínek auditních zakázek
ISA 220	Řízení kvality auditu účetní závěrky
ISA 230	Dokumentace

ISA 240	Podvod a chyba
ISA 250	Přihlížení k právním předpisům při auditu účetní závěrky.
Plánování	
ISA 300	Plánování
ISA 310	Znalost podnikání
ISA 320	Významnost při auditu.
Interní kontroly	
ISA 400	Hodnocení rizik a interní kontroly
ISA 401	Audit v prostředí počítačového informačního systému
ISA 402	Zvažované skutečnosti týkající se účetní jednotky
Důkazy auditu	
ISA 500	Důkazy auditu
ISA 501	Důkazní informace specifické aspekty vybraných položek
ISA 510	První auditní zakázka počáteční zůstatky
ISA 520	Analytické postupy
ISA 530	Výběr vzorků
ISA 540	Audit účetních odhadů včetně odhadů reálné hodnoty
ISA 550	Spřízněné strany.
Využívání výstupů práce jiných stran	
ISA 600	Zvláštní aspekty audity účetních závěrek skupiny
ISA 610	Využití práce interních auditorů
ISA 620	Využití práce auditorova experta.
Závěry auditu a reporting	
ISA 700	Formulace výroku a zprávy auditora k účetní závěrce
ISA 710	Srovnávací informace
ISA 720	Odpovědnost auditora ve vztahu s auditovanou účetní závěrku.
Speciální oblasti	
ISA 800	Zvláštní aspekty audity účetních závěrek

Všechny dokumenty vydané v rámci INTOSAI jsou nově označovány jako standardy typu Intrnational Standards of Superme Audit Institutions (ISSAI). Standardy jsou rozděleny celkem do čtyř úrovní.[4]

2. Základní principy
3. Předpoklady fungování
4. Základní auditorské principy
    - Bacis principles
    - General standards
    - Field standards
    - Rreporting standards
5. Auditorské návody

Při porovnání metodiky INTOSAI s jinými rámci je na první pohled zřejmé, že vzhledem k odlišnosti cílů je obtížné a říci, která metodika je lepší nebo horší. Metodika INTOSAI je v porovnání s jinými metodikami jednoduší protože nezahrnuje podnikatelské cíle a strategie, ale z pohledu využití v podnikatelské sféře může působit jako nekompletní.[4]

II. PRAKTICKÁ ČÁST

3 ANALÝZA FIREMNÍHO STAVU IT

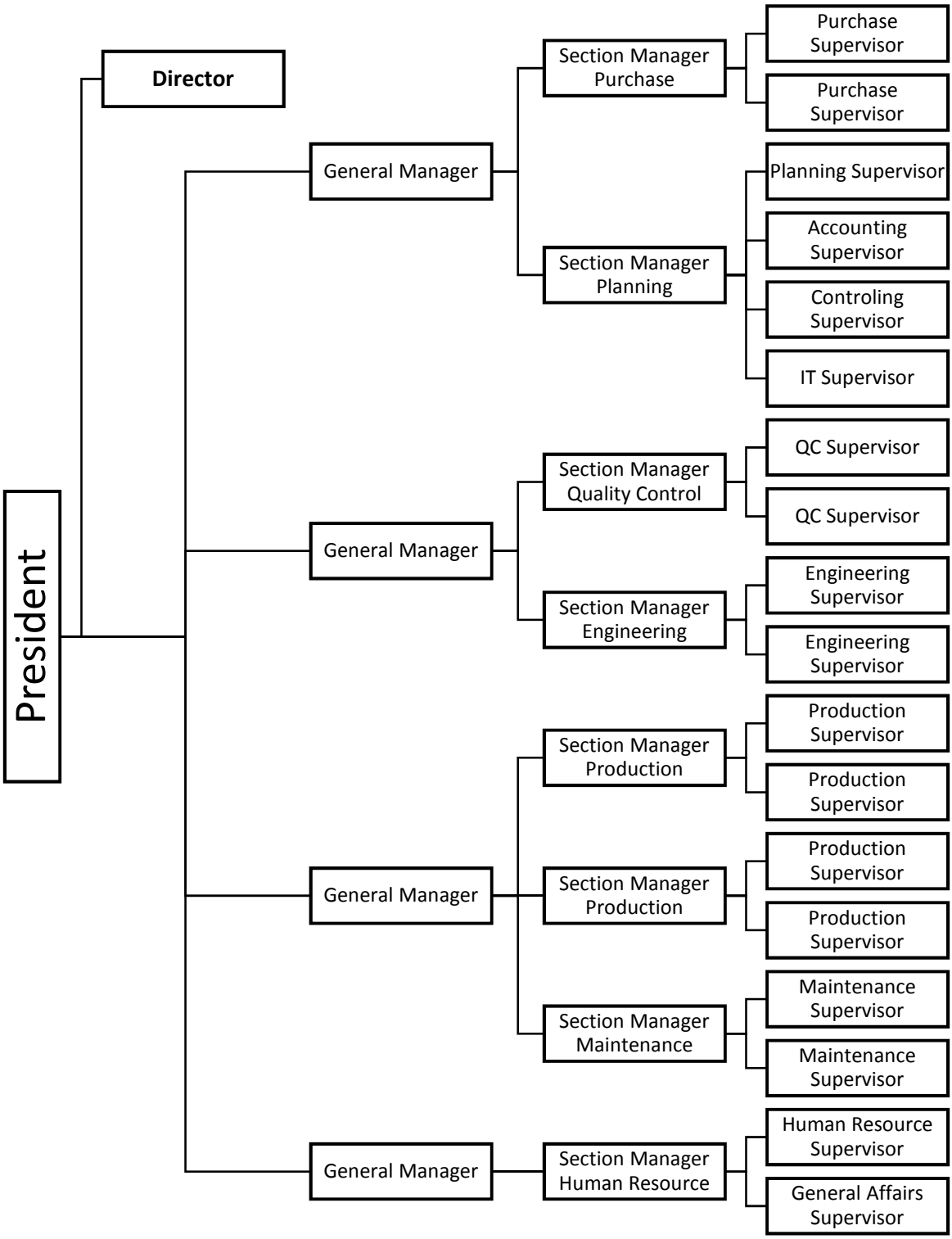
Auditovaná společnost dále jen firma je jednou z dceřiných spolčeností nadnárodního koncernu působícího po celém světě. Na každém kontinentě se pak nachází centrála pro daný kontinent, která působí jako mateřská firma pro dceřiné firmy působící v jednotlivých státech. Tyto dceřiné firmy se dále dělí na obchodní a výrobní společnosti a výrobní pak dále na výrobní firmy finálního produktu a subdodavatelské, které dodávají a předpřipravují materiál pro výrobní firmy. Auditovaná firma je jednou s těchto subdodavatelských společností umístěná v České republice. Firma jako taková musí splňovat nejen všechny legislativní předpisy České republiky, ale také všechny předpisy a nařízení vydaná evropskou a světovou centrálou organizace. Společnost je razí moto „Kvalita na prvním místě." Je proto jasným cílem dodávat zákazníků kvalitní, efektivní a ekologické výrobky. Požadavky kladené na efektivnost a výkon veškerých služeb a systému firmy jsou každým rokem náročnější. Je proto třeba nejen vyvíjet a zefektivňovat nová opatření a procesy, ale také kontrolovat a dodržovat zavedené již osvědčené procesy a nařízení vydané evropskou nebo světovou centrálou. Firemní IT je pravidelně auditováno externí organizací v rámci finančního auditu a evropskou centrálou v rámci bezpečnosti IT.

3.1 Analýza prostředí firmy

Firma působí na českém trhu již přes deset let. Její top management tvoří převážné cizinci, kteří jsou v české republice vždy na období 3, 5 nebo 7 let. Z tohoto důvodu je celý top management obměněn a i cíle společnosti se v průběhu let vyvíjeli. Současné vedení se snaží více spolupracovat s evropskou centrálou a přizpůsobit se evropským standardům.

V minulých letech byly do firmy úspěšně implementovány části knihovny ITIL a jsou zde snahy neustále vyvíjet a zavádět „best practice", která můžou firmě pomoci v dodávání kvalitních služeb zákazníkům. S ohledem na předchozí úspěšnou implementaci ITIL s jejíž pomocí se práce IT nejen zefektivnila, ale také se stala více transparentní pro management firmy. Po úspěšné implementaci ITIL bylo vedením a evropskou centrálou požadováno, také zavedení interních auditů IT v rámci firmy.

Firmě byla z evropské centrály zaslána na doporučení několika konkrétních rámců. Konečné rozhodnutí bylo ovšem učiněno až ve firmě samotné.



Obrázek 8: Organizační struktura firmy

3.1.1 Firemní struktura

Struktura firmy je trochu odlišná od klasické české organizace (obr. 9). Nejvyšší úroveň vedení ve firmě zastává prezident následován ředitelem společnosti, kde oba zastávají post jednatele společnosti. Další úrovní vedení jsou pozice generálních manažerů (GM). GM

zastávají nejvyšší vedení ve svěřených oblastech působení. Následující úrovní vedení je sekční manažer, který řídí supervisory oddělení pod něj spadající. V sekcích s THP pracovníky je supervisor nejnižší pozice vedení. Ve výrobní části firmy ještě následují úrovně Foreman a Team Leader.

Na první pohled je zřejmé, že ve společnosti se nenachází obchodní oddělení nebo jakákoliv sekce, která by s obchodem byla jakkoliv související. Toto je způsobeno tím, že firma dodává výrobky pouze v rámci firem spadajících pod evropskou centrálu organizace. Funkci obchodu nebo v tomto případě spíše přijímání zakázek zastává oddělení plánování, které přijme zakázky od evropské centrály a na základě těchto zakázek naplánuje výrobu v rámci firmy.

IT oddělení firmy spadá, také pod oddělení plánování jelikož plánování zakázek a rozvoje firmy úzce souvisí s rozvojem firemního IT. Oddělení IT se skládá celkem ze tří členů. Supervior a dva specialisti, kde každý zodpovídá za svěřenou část práce, ale je také nutná vzájemná zastupitelnost.

3.2 Výběr auditního rámce

Hlavním cílem auditu je splnění požadavků evropské centrály, která klade důraz především na správu majetku (Manage Assets), správu bezpečnosti (Manage Security), správu dodavatelů (Manage Suppliers), správu servisních smluv (Manage Service Agreements) a správu problémů (Manage Problems)(tab. 6). Tyto části jsou klíčové a díky výsledům auditu z těchto části může evropská centrála dále vyvodit, jestli není vhodnější mít společné dodavatele, jestli jsou dodržovány firemní předpisy na obnovu majetku atd. Další části auditu byly také doporučeny, ale nebyly označeny jako klíčové pro provádění v rámci interního auditu.

Tabulka 6: Rozdělení zodpovědnosti firmy

Rizika			**Kdo to dělá**					
Význam	**Kvalita**	Kvalita = Jak dobře se provádí Dokumentace = Existence smlouvy Auditováno = Ano, nebo Ne? Odpovědnost = jméno nebo "nevím" Hodnocení 1 až 5 nejlepší	**IT**	**EU centrála**	**Někdo jiný**	**Dodavatel**	**Není známo**	**Auditováno**
2	3	Resource Optimisation	x					ano
3	2	Stakeholder Transparency	x					ano
3	1	Manage the IT Management Framework	x					ne
2	2	Manage Strategy		x				ne
4	2	Manage Service Agreements			x			ano
4	2	Manage Suppliers	x					ano
2	3	Manage Risk						ano
4	3	Manage Security	x	x		x		ano
4	3	Manage Knowledge	x					ne
4	3	Manage Assets	x					ne
2	1	Manage Service Requests and Incidents	x					ne
4	3	Manage Problems	x					ne

Jednotlivým odvětvím se přiřadil význam s pohledu firmy. Na přiřazení byla použita prioritizační metoda MoSCoW[5]. Priority podle MoSCoW se dělí právě podle jejich významu pro firmu.

Tabulka 7: Hodnocení dle MOSCOW

Hodnota	**Význam**
4	Musí být obsaženo
3	Mělo by být obsaženo
2	Mohlo by být obsaženo
1	Nemusí být obsaženo nyní

[5] MoSCoW – Metoda agilniho projektového managementu pro stanovení priorit; **M**ust have, **S**hould have, **C**ould have, **W**ont have.

Ve výsledné tabulce hodnocení jsou doplněny ještě další speciální položky, které zahrnují nejdůležitější část z pohledu firmy a tou jsou náklady a doporučení z evropské centrály..

Tabulka 8: Normované váhy

	Význam	**Normované váhy**
Správa IT Framework	3	0,0750
Správa Strategie	1	0,0250
Správa služeb	4	0,1000
Správa dodavatelů	4	0,1000
Správa rizik	3	0,0750
Správa bezpečnosti	4	0,1000
Správa vědomostí	4	0,1000
Správa majetku	4	0,1000
Správa incidentů	2	0,0500
Správa problémů	3	0,0750
Náklady	4	0,1000
Doporučení	4	0,1000
Celkem	**40**	1,0000

Hodnocení jednotlivých kritérií je v rozmezí 0-5 a výpočet celkového hodnocení se provádí vynásobením hodnocení kritéria nástroje (rámce, standardu) a normované váhy kritéria. Součet hodnot všech kritérií je následně vydělen maximálním dosažitelným počtem bodů a vynásoben stem, aby byla hodnota udávána v procentech. Vztah v následující rovnici (1)[17][18].

$$H = \left[\frac{\sum_{i=1}^{n} K_i \cdot V_i}{10}\right] * 100 \ [\%] \tag{1}$$

Kde:

H Celkové hodnocení

K_i i-té kritérium

V_i váha i-tého kritéria

n počet kritérií

3.2.1 Hodnocení ISO/IEC 27k

rodina norem ISO/IEC 27k kompletně pokrývá oblast správy bezpečnosti a rizik. Z nákladového hlediska stačí nastudovat samotné normy nebo popřípadě zaplati proškolení

zaměstnanců. Je v ní obsažena ISMS šablona pro nastavení, implementování, ověření a udržování a neustálého zlepšování ochrany firemních aktiv.

Tabulka 9: Hodnocení ISO/IEC 27k

Název	Splňuje
Správa IT Framework	8
Správa Strategie	10
Správa služeb	0
Správa dodavatelů	0
Správa rizik	10
Správa bezpečnosti	10
Správa vědomostí	0
Správa majetku	0
Správa incidentů	0
Správa problémů	0
Náklady	10
Doporučení	6
Celkem	43%

3.2.2 Hodnocení CRAMM

Metodika CRAMM řeší oblasti analýzy a řízení rizik informací. Ve všech ostatních oblastech by nebyla příliš užitečná. Bylo by třeba ji zkombinovat s nějakou další metodikou.

Tabulka 10: Hodnocení CRAMM

	Splňuje
Správa IT Framework	0
Správa Strategie	0
Správa služeb	0
Správa dodavatelů	0
Správa rizik	10
Správa bezpečnosti	0
Správa vědomostí	0
Správa majetku	0
Správa incidentů	0
Správa problémů	0
Náklady	8
Doporučení	2
Celkem	16%

3.2.3 Hodnocení ITIL

Knihovna ITIL se dotýká všech zasažených oblastí, ale řeší je převážně z pohledu řízení a plánování než kontroly. Z pohledů nákladů by byl sice vhodný, jelikož prostředí firmy je s ním již seznámeno, ale využití jako auditního nástroje by nebylo nejvhodnější, jak jde vidět v tabulce z hlediska doporučení z evropské centrály.

Tabulka 11: Hodnocení ITIL

	Splňuje
Správa IT Framework	7
Správa Strategie	7
Správa služeb	8
Správa dodavatelů	6
Správa rizik	7
Správa bezpečnosti	6
Správa vědomostí	8
Správa majetku	8
Správa incidentů	8
Správa problémů	8
Náklady	10
Doporučení	4
Celkem	72%

3.2.4 Hodnocení INTOSAI

INTOSAI je vhodný pro audity všeho druhu. Zahrnuje, spává rizik, bezpečnosti a majetku a všechny klíčové části pro firmu potřebné. Jediná chybějící část je správa služeb a obchodní strategie jelikož původně pochází ze státní sféry. Další nevýhodou je nízké hodnocení ze strany evropské centrály.

Tabulka 12: Hodnocení INTOSAI

	Splňuje
Správa IT Framework	8
Správa Strategie	4
Správa služeb	7
Správa dodavatelů	6
Správa rizik	8
Správa bezpečnosti	4
Správa vědomostí	6
Správa majetku	8
Správa incidentů	7
Správa problémů	7
Náklady	8
Doporučení	4
Celkem	64%

3.2.5 Hodnocení COBIT

COBIT byl evropskou centrálou doporučen nejvíce. Z pohledu nákladů je na tom také výrazně lépe než ostatní z důvodu možnosti inertního zaškolení z evropské centrály. Jsou v něm obsaženy všechny klíčové části.

Tabulka 13: Hodnocení COBIT

	Splňuje
Správa IT Framework	7
Správa Strategie	7
Správa služeb	7
Správa dodavatelů	6
Správa rizik	7
Správa bezpečnosti	7
Správa vědomostí	8
Správa majetku	7
Správa incidentů	8
Správa problémů	7
Náklady	10
Doporučení	10
Celkem	77%

3.2.6 Celkové hodnocení

V porovnání všech rámců mají nejlepší hodnocení COBIT, INTOSA a ITIL, které pokrývají všechny klíčové části na rozdíl od CRAMM nebo ISO/IEC 27k. Celkové hodnocení v následující tabulce.

Tabulka 14: Hodnocení rámců

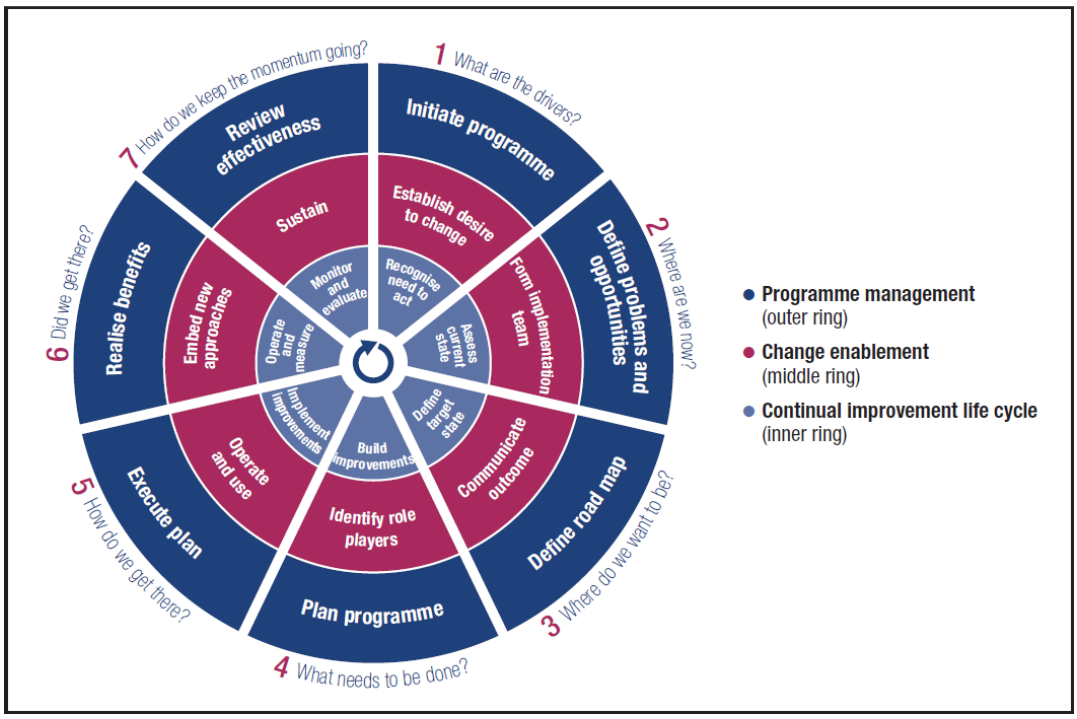
RÁMEC	**Hodnocení**
ISO/IEC 27k	43%
CRAMM	16%
ITIL	72%
INTOSAI	64%
COBIT	***77%***

4 AUDIT V ORGANIZACI

Ve firmě bude probíhat pouze implementace ICT části COBIT. V možnostech COBIT je samozřejmě pokrytí všech částí společnosti. Z důvodu již nastavených standardů ze strany evropské a světové centrály v jiných odděleních firmy, proto zde zmíněná implementace bude aplikována pouze na části IT firmy. Jelikož implementace COBIT stejně jako ITIL není přímo závazná a nelze ji provádět podle předpisu. Vždy je nutné implementaci přizpůsobit organizaci a jejím možnostem a potřebám, které ne vždy jsou identické.

4.1 Implementace

V rámci COBIT 5 je proces implementace rozdělen celkem na 7 po sobě jdoucích fázi. Jednotlivé fáze jsou přímo popsány v samostatné publikaci „COBIT 5 Implementation“, která je zaměřena implementaci COBIT ve firemním prostředí. Seznamuje s pojmem GEIT[6] a vysvětluje důležitost vytvoření vhodného prostředí pro implementaci a následný audit podle COBIT.



Obrázek 9: Fáze implementace

[6] GEIT - Governance of Enterprise IT jedná se mezinárodně uznávaný program se zaměřením na vzdělávání a strategické řízení IT.

4.1.1 Sumarizace důvodů k implementaci

V první fázi implementace bylo třeba vedení organizace seznámit s rámcem COBIT a se všemi výhodami, které jeho zavedení firmě přinese. Zpřehlednění IT vybavení a pravidelné reportování stavu IT do evropské a světové centrály. Vedení bylo již dříve seznámeno s požadavkem evropské centrály firmy na zavedení některého z auditních rámců pro potřeby IT a provádění interních auditů ve firmě jako přípravou na audit s evropské centrály nebo audit externí. V rámci prezentace byly zobrazeny i výsledky analýzy výběru vhodného rámce, které jsou součástí této práce. Tato prezentace byla klíčovým bodem celé implementace, jelikož bylo třeba, aby vedení pochopilo důležitost a přínosy implementace. Bez dostatečné podpory ze strany vedení firmy by byl další postup značně problematický možná dokonce nemožný. Během prezentace bylo také rozhodnuto o způsobu implementace. Za využití vlastního IT, které bude proškoleno a za spolupráce a podpory evropské centrály.

4.1.2 Analýza stavu IT před implementací

Ve druhé fázi bylo třeba posoudit současný stav IT, aby bylo možno lokalizovat nedostatky a určit rozsah potřebné implementace. Rozsah by již předem stanoven pouze na oblast IT. V rámci COBIT se této fázi řeší následující body.

- Identifikace klíčových podnikový a IT podporujících cílů
- Zjištění významu IT pro další oddělení
- Identifikace slabých stránek pro budoucí rozvoj
- Identifikace procesů pro předcházení klíčových rizik
- Posouzení rizik procesů souvisejících s poskytováním služeb
- Seznámení vedení společnosti se současnými riziky
- Definice metod posouzeni
- Dokumentace současných procesů
- Analýza úrovně schopností
- Definice hodnocení způsobilosti procesu

Klíčovou složkou pro veškeré služby IT ve firmě byl určen provoz ESX serverů na platformě VMware a HP LeftHand StoreVirtual, které zajišťují provoz všem virtuálním serverů a služeb provozovaných v rámci interní sítě. Tato zařízení a jejich kapacity jsou také klíčové pro další rozvoj IT ve firmě.

Základním cílem IT ve firmě je zajištění plynulého provozu služeb poskytovaných ostatním oddělením a zajištěním jejich plynulého provozu. Hlavním cílem firmy je výroba a včasné dodávky kvalitních výrobků sesterským firmám v rámci koncernu.

Tabulka 15: Služby provozované interně

1.	ERP systém Helios využívám jako hlavní ERP
2.	MES systémy - několik specializovaných systémů rozděleno dle druhu výroby
3.	QC systém - uchovává informace z oddělení kvality převážně výsledky měření a testů výrobků
4.	Docházkový systém – napojený na ERP Helios HR modul
5.	AD – doménový server
6.	Telefonní ústředna CISCO
7.	Služební Intranet – Helpdesk IT, Webové přístupy k dalším službám
8.	Zálohovací server

Tabulka 16: Služby zajišťované externě

1.	SAP využíván převážně pro výměnu dat v rámci koncernu
2.	MES systém
3.	VPN systém

Byla prozkoumána firemní dokumentace, která byla značně nekompletní v rámci změn na stávajících službách a implementaci nových někdy úplně chyběla.

4.1.3 Určení cílů, prirorit.

Hlavním cílem bylo stanoveno zajistit jasný a přehledný výsledek auditu, který bude vypovídat o skutečném stavu věcí v rámci IT. Zajistí se tak přehlednost nad všemi službami a procesy a jejich nedostatky. Současně bude působit jako příprava na audit s evropské centrály. Podle COBIT se cíle dělí na podnikové cíle a cíle týkající se informačních technologií. Ke každému cíli jsou přiřazeny metriky, které lze použít k měření a analýze

výkonosti. Vzorky těchto metrik jsou uvedeny jako příklady knize „COBIT 5 Enabling Processes“. Tyto metriky musí každý podnik pečlivě přezkoumat a vytvořit seznam relevantních a dosažitelných metrik pro vlastní prostředí a navrhnout vlastní systém jejich hodnocení. Níže uvedené cíle a metriky procesu jsou obsaženy v podrobných popisech procesů.

Tabulka 17: Zvolené metriky pro nasledující audit

Metriky cílů informačních technologií		
BSC	IT cíle	Metriky
FINANČNÍ	Správa IT souvisejících rizika	Procento kritických IT služeb a programů Počet nezmapovaných IT incidentů. Perioda aktualizací rizik.
	Transparentnost nákladů	Procento investic do rozvoje IT Procento IT služeb se zaevidovanými náklady.
INTENÍ	IT agility	Počet výrobních aplikací závislých na IT Úroveň spokojenosti s reakcí na IT požadavky
	Bezpečnost informací, procesů a aplikací	Počet bezpečnostních incidentů Počet IT služeb se zvýšenou bezpečností Reakční doba na vytvoření, změnu, zrušení oprávnění Počet zařízení s vyšším bezpečnostním režimem
	Optimalizace IT majetku, zdrojů a schopností	Frekvence obnovy majetku Frekvence kontrol softwarových licencí Počet evidovaných a schválených dodavatelů
	Dodržování vnitřních politiky IT	Počet incidentů souvisejících s nedodržováním politiky Frekvence obnovy politiky Procento politiky podporované systémem

ROZVOJ	Znalosti, odbornost a iniciativa	Počet pravidelných školení IT Počet dalších vzdělávacích aktivit Procento zdokumentovaných procesů

4.1.4 Sestavení bodů pro implementaci

Body pro implementaci byly doporučeny z evropské centrály. Jejich účelem, jak již je řečeno v předchozí fázi bylo zajistit hlavně zpřehlednění a zkvalitnění a synchronizaci služeb s evropskou centrálou společnosti. Bylo nám doporučeno implementovat následující procesy. Cíle v tabulce jsou stanoveny na maximum tj. 5 protože vždy být co nejlepší i když to je samozřejmě nedosažitelný cíl. Reálně bude považováno za úspěch jakékoli zlepšení.

Tabulka 18: body k implementaci

Název	Označení	Zabývá se	Hodnocení	Cíl
	EDM03			
Risk Optimisation	EDM03.01	Evaluate risk management.	1	5
Risk Optimisation	EDM03.02	Direct risk management.	2	5
Risk Optimisation	EDM03.03	Monitor risk management.	2	5
	EDM04			
Resource Optimisation	EDM04.01	Evaluate resource management.	2	5
Resource Optimisation	EDM04.02	Direct resource management.	2	5
Resource Optimisation	EDM04.03	Monitor resource management.	1	5
	APO10			
Manage Suppliers	APO10.01	Identify and evaluate supplier.	1	5
Manage Suppliers	APO10.02	Select suppliers.	2	5
Manage Suppliers	APO10.03	Manage supplier contracts.	1	5
Manage Suppliers	APO10.04	Manage supplier risk.	0	5
Manage Suppliers	APO10.05	Monitor supplier performance	1	5
	APO13			
Manage Security	APO13.01	Establish and maintain an ISMS.	2	5
Manage Security	APO13.02	Manage an IT security risk plan.	2	5
Manage Security	APO13.03	Monitor and review the ISMS.	1	5
	BAI08			
Manage Knowledge	BAI08.01	Nurture knowledge-sharing.	3	5
Manage Knowledge	BAI08.02	Classify sources of information.	3	5
Manage Knowledge	BAI08.03	Organise information into knowledge.	4	5
Manage Knowledge	BAI08.04	Use and share knowledge.	4	5
Manage Knowledge	BAI08.05	Evaluate and retire information.	2	5

	BAI09			
Manage Assets	BAI09.01	Identify and record current assets.	4	5
Manage Assets	BAI09.02	Manage critical assets.	4	5
Manage Assets	BAI09.03	Manage the asset life cycle.	3	5
Manage Assets	BAI09.04	Optimise asset costs.	3	5
Manage Assets	BAI09.05	Manage licences.	4	5

4.1.5 Stanovení postupu implementace

Některé zmíněné body byly již implementovány v minulosti, a proto jejich implementace již není nutná. V následujícím postupu implementace zbylých procesů na základě informací získaných v knize COBIT Implementation.

- EDM03 Risk Optimisation – Nejvyššími riziky pro firmu bylo vyhodnoceno, přerušení výrobních procesů, ztráta dat, přerušení komunikace s evropskou centrálou. Byl vytvořen havarijní plán pro přesun systému na záložní server umístěný v jiné budově firmy. Na tento server se pravidel kopírují zálohy všech SQL serverů a jsou zde uloženy i veškeré záložní data a server, který může dočasně nahradit servery aplikační. Byl určen rozvrh a frekvence všech záloh. Komunikace s evropskou centrálou je zajišťována externími dodavateli. Po dvou nezávislých linkách.
- EDM04 Resource Optimisation - Správa zdrojů byla nastavena v ERP systému Helios, kde zodpovědné osoby při vytváření objednávek na služby nebo materiál musí vybrat nákladové středisko a rozpočet ze kterého má práva čerpat. Při nedostatečných zbrojích je třeba vytvořit RINGI[7], které zajišťuje navýšení zdrojů nebo jednorázový výdej na požadovanou objednávku. Veškerý postup byl zdokumentován ve firemní dokumentaci.
- APO10 Manage Suppliers – Správa dodavatelů byla, také nastavena v systému Helios. Byla nastavena pravidla pro výběr nového dodavatele, zanesení do systému. Hodnocení dodavatele a nastavena perioda kontrol z oddělení General Affairs.
- APO13 Manage Security – Správa bezpečnosti je z velké části zajištována evropskou centrálou. Veškerý tok komunikace jde přes VPN do evropské centrály a dále přes jejich firewall a proxi server do sítě internet. Ve firmě je zajišťována převážně bezpečnost uniku, ztráty informací nebo zavirováním sítě. Ve firmě bylo metodickým pokynem zakázáno používat soukromé USB flash disky nebo připojovat telefony k PC. Byl, také nainstalován

[7] RINGI – Jedná se podání návrhu nadřízeným, které čeká na jejich projednání a rozhodnutí.

software pro zprávu USB na všech PC, který zamezuje tyto flash disky připojovat z výjimkou schválených krytovaných firemních USB flash disků.

- BAI08 Manage Knowledge – Správa vědomostí byla implementována již dříve, proto její implementace nebyla nutná. Veškeré informace evidovány v databázi software Správce IT a rozděleny na veřejné pro všechny uživatele a soukromé pouze pro správce IT.
- BAI09 Manage Assets – Správa majetku byla, také implementována již dříve spolu se správcem vědomosti. Informace o majetku jsou všechny uloženy v databázi „Správce IT“, kam jsou odesílány veškeré informace o změnách na majetku z jeho klientů nainstalovaných na všech PC. Pouze majetek jako síťové prvky, telefony, kopírky atd. je přidáván ručně.

4.1.6 Ověření stavu po implementaci

Implementace zvolených procesů proběhla úspěšně. Zbývá vyhodnotit, do jaké míry jsme splnili cíle, které jsme si stanovili a hlavně implementované součásti dále udržovat a neustále zlepšovat a přizpůsobovat potřebám firmy. Stav procesů po implementaci byl předložen managementu firmy k posouzení, zda bylo splněno jejich očekávání.

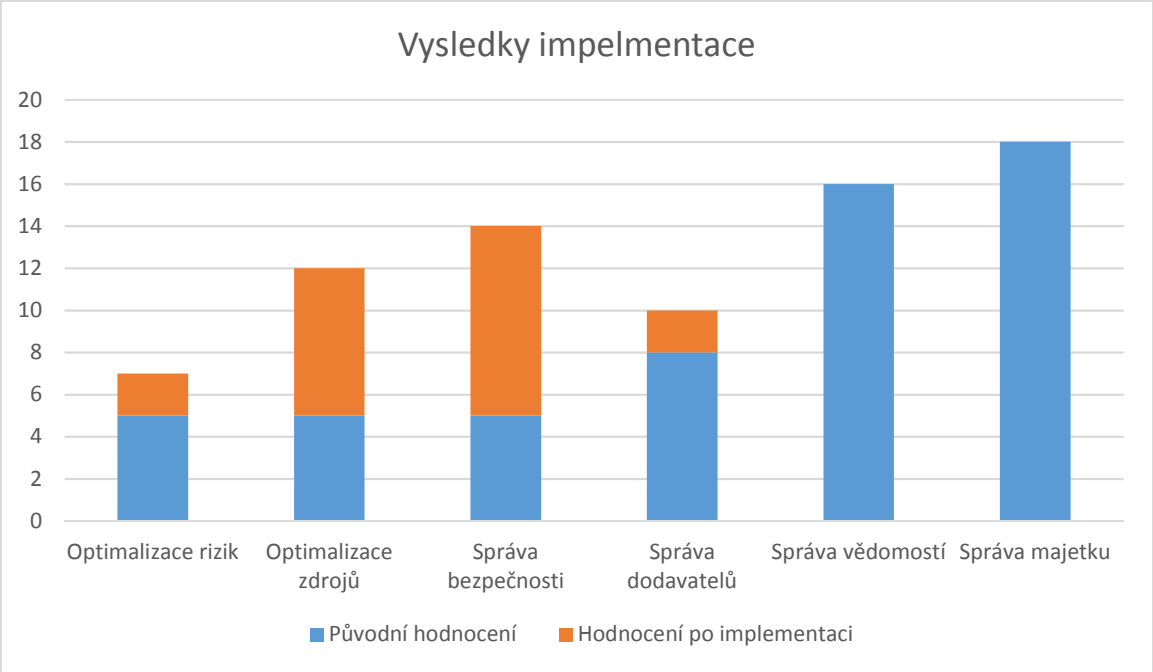
Tabulka 19: Vysledné hodnocení implementace

Název	Označení	Zabývá se	Hodnocení	Změna	Cíl
EDM03					
Risk Optimisation	EDM03.01	Evaluate risk management.	1	1	5
Risk Optimisation	EDM03.02	Direct risk management.	2	3	5
Risk Optimisation	EDM03.03	Monitor risk management.	2	3	5
			5	**7**	
EDM04					
Resource Optimisation	EDM04.01	Evaluate resource management.	2	4	5
Resource Optimisation	EDM04.02	Direct resource management.	2	4	5
Resource Optimisation	EDM04.03	Monitor resource management.	1	4	5
			5	**12**	
APO10					
Manage Suppliers	APO10.01	Identify and evaluate supplier.	1	4	5
Manage Suppliers	APO10.02	Select suppliers.	2	3	5
Manage Suppliers	APO10.03	Manage supplier contracts.	1	3	5
Manage Suppliers	APO10.04	Manage supplier risk.	0	2	5
Manage Suppliers	APO10.05	Monitor supplier performance	1	4	5
			5	**14**	
APO13					

Manage Security	APO13.01	Establish and maintain an ISMS.	2	3	5
Manage Security	APO13.02	Manage an IT security risk plan.	3	4	5
Manage Security	APO13.03	Monitor and review the ISMS.	3	3	5
			8	**10**	
BAI08					
Manage Knowledge	BAI08.01	Nurture knowledge-sharing.	3	3	5
Manage Knowledge	BAI08.02	Classify sources of information.	3	3	5
Manage Knowledge	BAI08.03	Organise information into knowledge.	4	3	5
Manage Knowledge	BAI08.04	Use and share knowledge.	4	4	5
Manage Knowledge	BAI08.05	Evaluate and retire information.	2	2	5
			16	**16**	
BAI09					
Manage Assets	BAI09.01	Identify and record current assets.	4	4	5
Manage Assets	BAI09.02	Manage critical assets.	4	4	5
Manage Assets	BAI09.03	Manage the asset life cycle.	3	3	5
Manage Assets	BAI09.04	Optimise asset costs.	3	3	5
Manage Assets	BAI09.05	Manage licences.	4	4	5
			18	**18**	

4.1.7 Správa o výsledcích implementace

Na závěr implementace bylo třeba sepsat správu o jejích výsledných datech a vytvořit plán kontrol a návrhů na možná další zlepšení, protože implementace není konce, ale naopak start. Je třeba všechno co jsme zavedli nejen udržovat, ale také neustále vylepšovat, aby se dosáhlo požadovaných výsledků. Ve všech procesech došlo po implementaci ke zlepšení s výjimkou Správy znalostí a majetku, které byli implementovány dříve a měli dostatečnou úroveň. Hlavním cílem jako takovým bylo mít procesy zavedené, aby je bylo možné auditovat a odesílat výsledky auditu evropské centrále. V následujícím obrázku je porovnání původních výsledků hodnocení a výsledků po implementaci.

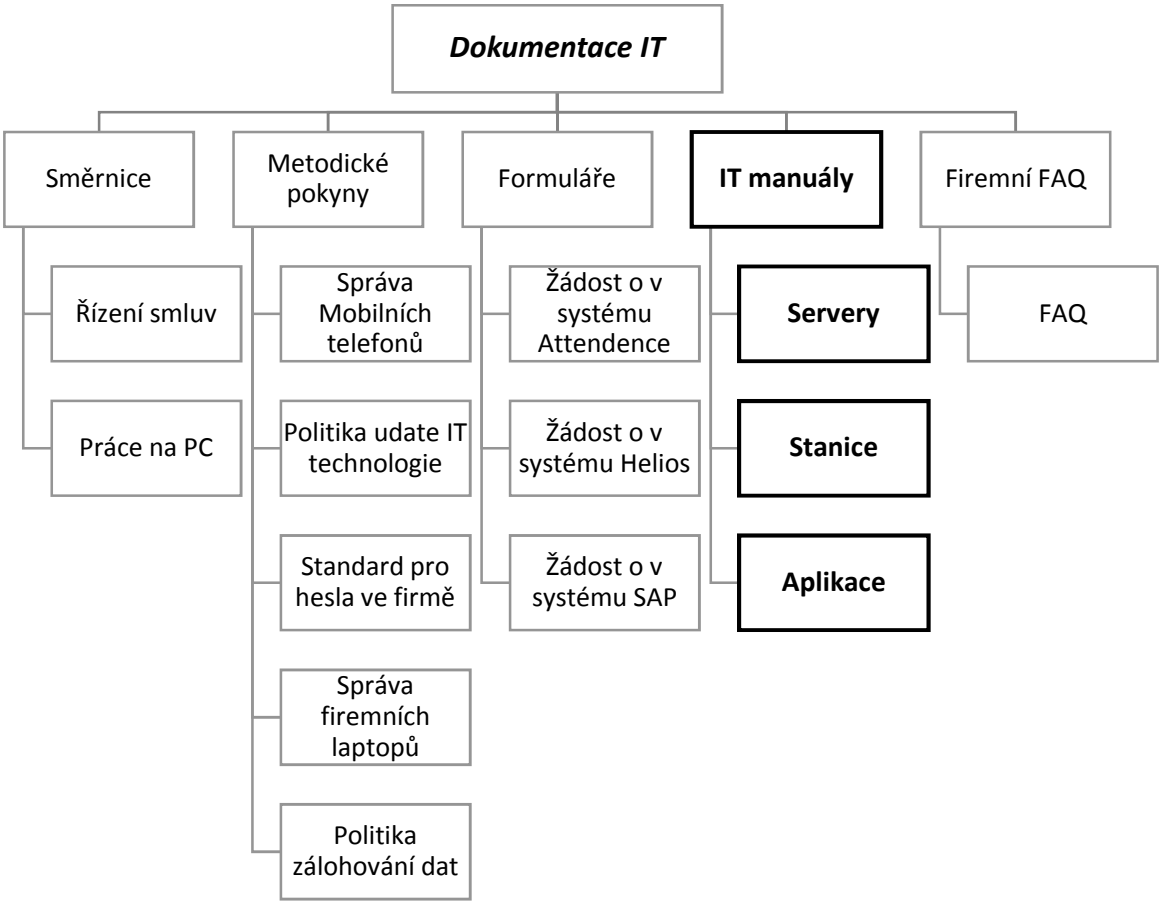


Obrázek 10: Přehled výsledků implementace

4.2 Audit

V rámci auditu IT ve firmě bylo zaměřeno nejen na metriky, které byly již dříve zvoleny, ale i na celkovou analýzu problémů a nedostatků ve firmě. Byl sestaven tým interních auditorů. Tento tým musel být vybrán ze spolehlivých a důvěryhodných zaměstnanců firmy, jelikož se v průběhu auditu pracovalo s velmi citlivými údaji a informacemi z oblasti IT, které mohou mít vážný dopad na chod celé firmy.

V první fázi auditu bylo třeba projít firemní dokumentaci. V rámci úseku IT je dokumentace rozdělena do 5 části jak je možno vidět na následujícím obrázku (obr. 10.). Z toho čtyři veřejné a jeden neveřejný. Veřejné části jsou dostupné všem zaměstnancům firmy pomocí intrawebu nebo prostřednictvím sdílených složek na datovém serveru. Práva přístupu pro čtení mají všechny skupiny v rámci AD. V případě pracovníků, kteří nemají v rámci AD vlastní účet, tak přístup zajišťuje PC dostupné na oddělení HR. Neveřejnou část (zvýrazněno tučně) tvoří IT manuály, které jsou dostupné pouze pracovníkům IT a část metodických pokynů, které se vztahují k neveřejným informacím jako perioda zálohování atd.



Obrázek 11: Rozdělení firemní dokumentace

Dokumentace seznamuje uživatele s prostředím firmy a také se všemi možnostmi a nařízení s toho plynoucími. Firemní FAQ dále radí v případě konkrétních problémů, které můžou nastat. Dokumentace IT ve firmě obsahuje celkem 14 oficiálních souborů, které podléhají kontrole a schvalování. Výsledky v následujících tabulkách jsou v rozmezí minulého fiskálního roku firmy.

V následujících tabulkách metrik je vždy zobrazen výsledek hodnocení a stav jaký tento výsledek má v rámci firmy, který nabývá hodnot OK, pokud je firma spokojena se současným výsledkem měření nebo NG[8], kdy výsledek neodpovídá hodnotám, které firma požaduje.

[8] NG – výraz z prostředí asijských firem představující zkratku "NO GOOD"

4.2.1 Audit správy vědomostí

Firemní rozpočet má vyčleněnou část na vzdělávání a rozšiřování vědomostí vlastního IT oddělení. Plán školení počítá se dvěma školeními na osobu ročně v případě běžného školení v hodnotě cca 15 000 Kč v případě nákladnějšího nebo levnějšího školení je možné počet ročních školení upravit.

V rámci rozpočtu IT je také počítáno s cca dvěma kolektivními školeními např. formou semináře nebo v dnešní době již spíše webináře z důvodu nutné přítomnosti v případě incidentů na firmě. Dále nákup potřebné literatury v rámci sebevzdělávání IT pracovníků.

V rámci kontroly dokumentace byla prověřována metrika zdokumentovaných procesů ve firmě. Ke zmiňované dokumentaci bylo nutné dále prověřit data obsažená v databázi počítačové programu na evidenci informací a manuálů, která jsou přímo napojená na firemní helpdesk a v případě opakovaného problémů z něj můžou čerpat i běžný zaměstnanci. V rámci toho byli zjištěni rozdíly ve schválené dokumentaci a informacím uložených v databázi. Jelikož v rámci nastavených metrik tato kontrola nebyla nastavena, tak následující tabulce není evidována. Tato informace byla pouze přidána jako poznámka pro další audit.

Tabulka 20: Výsledky metrik správy vědomostí

Metrika	Výsledek	Stav
Počet pravidelných školení IT	**2x ročně**	**OK**
Počet dalších vzdělávacích aktivit	**2x ročně**	**OK**
Procento zdokumentovaných procesů	**68%**	**OK**

4.2.2 Audit správy rizik

Kritickými službami jsou ty služby, které jsou zásadní pro chod firmy. Jejich určení může byt velice složitá záležitost. Ve firmě je více ERP systémů a tak výpadek jednoho nebo druhého ovlivní pouze část pracovníků. Jediným kritickým bodem by byl výpadek sítové infrastruktury. Z toho důvodu jme, vyhodnotili jako kritické všechny procesy, jejichž výpadek by ovlivnil jakoukoli část firmy. Tyto služby jsme zmiňovali již dříve v Tabulce 15 a 16. Služby na sebe vzájemně navazují a podporují se. Výpadek jedné ovlivní další např. SQL server nebo VPN jsou služby, které podporují další programy a z toho důvodů je pro ně v případě výpadku připraveno alternativní řešení pro zajištění chodu navazujících služeb.

Incidenty, které nejsou evidované v rámci aplikace Helpdesk jsou převážně drobné incidenty, které jsou odstraněny v rámci řešení jiných zaevidovaných incidentů na pracovišti nebo incidentů, tak závažní, že jejich řešení probíhá automaticky nezávisle na jejich evidenci v systému.

Aktualizace rizik původně probíhala pouze jednou ročně v rámci auditu evropskou centrálou. Nyní díky zavadění vlastních interních auditů bude tato aktualizace probíhat minimálně dvakrát ročně v případě auditu externí firmou dokonce třikrát.

Podobně jako v předchozím případě byly nalezeny nedostatky, které nesouvisí s nastavenými metrikami. V rámci optimalizace rizik bylo zjištěno, že přístupy do místnosti se servery nejsou nikde evidovány. Klíče od této místnosti mají pouze pracovníci IT, ale existuje i několik univerzálních klíčů v rámci celé firmy např. správci budovy, bezpečnostní technik a několik výše postavených manažerů. Z toho důvodu bylo navrhnuto zavézt přístup na čipové karty jako je v celém areálu firmy a který bude evidovat veškeré přístupy do těchto střežených prostor.

Tabulka 21: Výsledky metriky správy rizik

Metrika	Výsledek	Stav
Procento kritických IT služeb a programů	**72%**	**NG**
Počet nezmapovaných IT požadavků.	**17%**	**OK**
Perioda aktualizací rizik.	**2x ročně**	**OK**

4.2.3 Audit správy zdrojů

Rozvoj a vylepšení IT služeb je pro firmu zásadní, proto je vždy minimálně 30% celkového rozpočtů určeno na rozvoj nových nebo vylepšení stávajících zařízení. Nejnákladnější projekt minulého roku byl částečně hrazen z investic do rozvoje a investic do obnovy. Jednalo se o výměnu a modernizaci stávající telefonní ústředny za novou CISCO PBX[9] ústřednu, která se dokáže připojit na centrální ústřednu v evropské centrále.

[9] PBX - (Private Branch Exchange) telefonní ústředna se správou interní komunikace uživatel

Veškeré služby a náklady jsou evidovány v systému. Bez jejich zaevidování není možné je zakoupit. Systém to nedovoluje. Jedinou možností jak by něco takového nastat je zakoupení z vlastních nákladů a dodatečné zaevidování a proplacení ze strany firmy.

Tabulka 22: Výsledky metrik pro spává zdrojů

Metrika	Výsledek	Stav
Procento investic do rozvoje IT	**33%**	**OK**
Procento IT služeb se zaevidovanými náklady	**99%**	**OK**

4.2.4 Audit správy bezpečnosti

Incidenty související s narušením bezpečnosti jsou minimální, bohužel ne nulové, jak by si nejspíše všichni přáli. Většinou se jednalo o nedodržení předpisů a stažení infikovaných souborů z mailu nebo internetu. Byl zde také jeden evidovaný případ úmyslného smazání dat zaměstnancem, který již byl ve výpovědní lhůtě. Právě z toho důvodu byla vytvořena metrika pro zjištění reakční doby.

Systémy se zvýšenou bezpečností jsou dva hlavní ERP systémy SAP a Helios, ve kterých jsou obsaženy důležité informace firmy. Dalším takovým systémem je docházkový systém, který uchovává citlivé informace o zaměstnancích. Posledním s těchto čtyř systémů je doménový AD, který zajišťuje přístupy v rámci sítě a sdílených datový serverů. Přístup do všech těchto systémů je zabezpečen helem. Tyto hesla podléhají nařízením firemní politiky.

Reakční doba na změnu oprávnění byla původně 48 hodin. Ta z důvodu již dříve zmíněného bezpečnostního incidentů, byla změněna. Byl přednesen návrh na její změnu na co možná nejkratší dobu. Po dohodě bylo schváleno 24 hodin. V systému Helpdesk byla těmto požadavků zvýšena priorita.

Ve firmě je evidováno celkem 57 zařízení, která mají nastavené zvýšené bezpečnostní opatření. Jedná se o laptopy manažérů a jiných klíčových zaměstnanců firmy. Veškerá výpočetní technika, která opouští areál firmy má nainstalovanou rozšířenou verzi antivirového software McAfee a kryptovací software od firmy Pointsec. Na serverové konzole bylo ověřeno všech 57 instalací na koncových zařízeních včetně jejich posledního

přihlášení a aktualizace. Tyto zařízení se pak dále můžou pouze připojovat pomocí VPN k firemnímu mailu, ale ne k firemním datům.

Tabulka 23: Výsledky metrik pro správu bezpečnosti

Metrika	Výsledek	Stav
Počet bezpečnostních incidentů	**2%**	**OK**
Počet IT služeb se zvýšenou bezpečností	**4**	**OK**
Reakční doba na vytvoření, změnu, zrušení oprávnění	**48h**	**NG**
Počet zařízení s vyšším bezpečnostním režimem	**57**	**OK**

4.2.5 Audit správy majetku

Analýzu stavu majetku proběhla s využitím software Správce IT, který veškerý majetek v kompetenci IT oddělení spravuje. Jsou v něm obsaženy veškeré informace od zakoupení, čísla faktury přes uvedení do provozu až po dobu vyřazení. Na základě vyexportovaných dat s tohoto programu byla provedena kontrola se skutečným stavem a počtem majetku na firmě. Data v následujícím obrázku (obr. 11) slouží jako příklad tohoto exportu. Data byla změněna a názvy zařízení nahrazeny názvem procesoru v zařízení obsaženém. Počítače se ve firmě standardně obměňují po pěti letech, pokud není jiný důvod pro změnu. Laptopy se standardně obměňují po třech letech. Veškeré potřebné informace byly obsaženy v metodickém pokynu.

Popisky řádků	12	13	14	15	16	Celkový součet
Intel Core i3-4005 1 700 MHz				3		3
Intel Core i3-4130 2 900 MHz			20			20
Intel Core i3-6100 3 200 MHz				10	14	24
Intel Core i5-3210 2 500 MHz	3	1				4
Intel Core i5-3230 2 600 MHz		11				11
Intel Core i5-4200 1 600 MHz			1			1
Intel Core i5-4210 1 700 MHz			7			7
Intel Core i5-4210 2 600 MHz				1		1
Intel Core i5-5200 2 200 MHz				2		2
Intel Core i5-6200 2 300 MHz				1	13	14
Intel Core i5-6300 2 400 MHz					1	1
Pentium IIIC 3 000 MHz	29	15				44
Celkový součet	**32**	**27**	**28**	**17**	**28**	**132**

Obrázek 12: Ukázka exportu HW dat pro obnovu majetku

Softwarová kontrola probíhala, také za pomocí již zmíněného software, který je nainstalován na všech PC ve firmě a pravidelně skenuje, zda na PC není nějaký nový software, který pak zaeviduje do databáze Správce IT a následně upozorní na neexistující licenci. Data byla z programu vyexportovaná a proběhla náhodná kontrola PC, zda je opravdu všechno v databázi, také obsaženo na PC a naopak zda v databázi něco nechybí. Data na následujícím obrázku (obr. 12) byla opět z bezpečnostních důvodů pozměněna a slouží pouze jako ukázka daného exportu. V případě záporné balance je software zvýrazněn a označen jako nelegální. K veškerým licencím software je připojena faktura ve formátu PDF, která slouží jako ověření pravosti SW.

SW name	SW version	Edition	License	Installed	Balanc
Acronis TrueImage	2013	Home	2	0	**2**
Aktivity	2015		250	57	**193**
Autodesk AutoCAD LT	2012		10	2	**8**
MS Access	2013		2	2	**0**
MS Excel	2016		15	15	**0**
MS InfoPath	2016		15	15	**0**
MS Office	2016	Standard	35	25	**10**
MS OneNote	2016		15	15	**0**
MS Outlook	2016		15	15	**0**
MS PowerPoint	2016		15	15	**0**
MS Project	2010	Standard	8	6	**2**
MS Project	2013	Standard	1	1	**0**
MS Visual Studio	2015		2	1	**1**
MS Windows Server	2008 R2	Enterprise x64	8	7	**1**
MS Windows Server	2008 R2	Standard x64	3	3	**0**
MS Windows Server	2003 R2	Standard x64	3	0	**3**
MS Windows Server	2012 R2	Standard x64	4	2	**2**
MS Word	2016		15	15	**0**
Polycom Telepresence m100			5	0	**5**
Správce IT	2015		250	44	**206**
Správce IT	2016		250	43	**207**

Obrázek 13: Ukázka exportu SW balance

Ze zmíněných metrik je v tabulce označena perioda obnovy majetku 5 let, která se vztahuje na většinu majetku s výjimkou laptopů. Frekvence kontrol SW, byla navýšena z kontroly jednou ročně na dvakrát ročně, díky zavedení vlastních interních auditů. V rámci kontroly majetku, byly jako zásadní nedostatek označeny PC se systémem XP, které firma stále využívá na některých nový PC ve výrobním procesu. Tyto počítače sice nejsou připojeny do firemní sítě, ale i tak je třeba vytvořit plán náhrady těchto zastaralých systémů.

Tabulka 24: Výsledky metrik pro správu majetku

Metrika	Výsledek	Stav
Frekvence obnovy majetku	**5 let**	**OK**
Frekvence kontrol softwarových licencí	**2x ročně**	**OK**
Počet evidovaných a schválených dodavatelů	**99%**	**OK**

4.2.6 Audit vnitřních politiky IT

Ve firmě bylo evidováno několik nedodržení firemní politiky. Nejčastějším případem je sdílení uživatelského ID a hesla. K této situaci nastává výtečně a jedná se převážně o improvizované řešení absence některého uživatele nebo nutné vypomoci. Z kritických systémů pouze systém SAP je proti tomuto nedodržení politiky částečně zajištěn, jelikož nedovoluje současné přihlášení dvou stejných uživatelských ID.

Bezpečnostní politika zavedená ve firmě byla, zavedena na začátku fungování firmy a od té doby se téměř nezměnila. V rámci dřívějších auditů se vůbec neřešila a neaktualizovala. Až v rámci implementace COBIT, byla evidována potřeba její pravidelné kontroly a aktualizace. Aktualizace byly nastaveny na 2x ročně v rámci přípravy na interní audity.

Velkou část firemní politiky není možné porušit díky její podpoře v rámci nastavení programů a systémů. Například politika hesel je nastavena v rámci AD, kde je nastavena periodická obnova hesla na dobu několika měsíců a po uplynutí, této doby je uživatel automaticky vyzván ke změně. Dále je kontrolováno, jestli heslo nebylo použito již dříve nebo není příliš podobné se stávajícím heslem.

Tabulka 25: Výsledky metrik pro vnitřní politiku

Metrika	Výsledek	Stav
Počet evidovaných nedodržení firemní politiky.	**7**	**OK**
Frekvence obnovy politiky	**2x ročně**	**OK**
Procento politiky podporované systémem	**78%**	**OK**

4.3 Zhodnocení auditu

V rámci auditu bylo objeveno několik nedostatků a špatně nastavených nebo nedostačujících metrik. Nicméně přinesl cenné informace jak pro tým auditorů, tak pro oddělení IT a firmu celkově. V následujících by se mělo zvážit implementovat ještě několik dalších procesů, které doporučuje evropská centrála. Většinu cílů se podařilo naplnit dle požadavků evropské centrály, ale některé části zůstali nesplněni.

Vedení firmy přijalo výsledky pozitivně, jelikož ke všem nesplněným částem byla navržena opatření, která by zjištěné nedostatky měla do dalšího auditu odstranit. Dále bylo navrženo dodatečné proškolení auditního týmu externí firmou, které by mělo v budoucnu zajistit ještě lepší a kompaktnější výsledky. V následující tabulce můžete vidět sumarizaci všech metrik a výsledek jejich hodnocení.

Tabulka 26: Souhrn hodnocení výsledných metrik

BSC	IT cíle	Metriky	Výsledky
FINANČNÍ	Správa IT souvisejících rizika	Procento kritických IT služeb a programů	NG
		Počet nezmapovaných IT incidentů.	OK
		Perioda aktualizací rizik.	OK
	Transparentnost nákladů	Procento investic do rozvoje IT	OK
		Procento IT služeb se zaevidovanými náklady.	OK
INTENÍ	IT agility	Počet výrobních aplikací závislých na IT	OK
		Úroveň spokojenosti s reakcí na IT požadavky	OK
	Bezpečnost informací, procesů a aplikací	Počet bezpečnostních incidentů	OK
		Počet IT služeb se zvýšenou bezpečností	OK
		Reakční doba na vytvoření, změnu, zrušení oprávnění	NG
		Počet zařízení s vyšším bezpečnostním režimem	OK

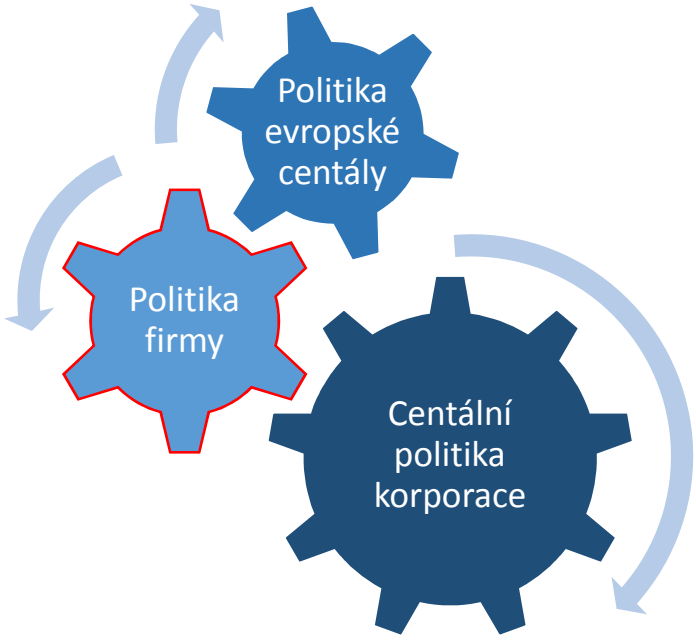
	Optimalizace IT majetku, zdrojů a schopností	Frekvence obnovy majetku Frekvence kontrol softwarových licencí Počet evidovaných a schválených dodavatelů	OK OK OK
	Dodržování vnitřních politiky IT	Počet incidentů souvisejících s nedodržováním politiky Frekvence obnovy politiky Procento politiky podporované systémem	OK OK OK
ROZVOJ	Znalosti, odbornost a iniciativa	Počet pravidelných školení IT Počet dalších vzdělávacích aktivit Procento zdokumentovaných procesů	OK OK OK

Ze zvolených metrik nebyli dostačující výsledky pouze metrice „Procento kritických IT služeb a programů“, kde bylo zjištěno velké procento programů bez zajištění náhrady v případě poruchy zařízení. Bylo navrženo řešení záložním serverem, kam by se replikovala data klíčových aplikací. Další nevyhovující výsledek byl u metriky „Reakční doba na vytvoření, změnu, zrušení oprávnění“. Tato doba byla zkrácena, ale dle požadavku vedení by měla být téměř minimalizována. Byl zaslán požadavek na evropskou centalu zda by synchronizace lokálního AD serveru a centrálním evropského AD serveru mohla býti spouštěna manuálně a ne jen ve stanovené termíny. Popřípadě zda by perioda synchronizace mohla být zkrácena na 12h. V poznámkách pro další audit bylo připsáno několik návrhů na nové metriky.

- Celková hodnota nevyužitých licencí firmy
- Počet přístupů do mistrnosti se servery
- Počet PC se systémy bez podpory

5 INOVACE BEZPEČNOSTNÍ POLITIKY

Bezpečnostní politika firmy byla nastavena na začátku fungování firmy a vychází z původní bezpečnostní politiky celé korporace. Bohužel politiky a z bezpečnostních důvodů bohudík se tato politika neustále mění a vyvíjí. Do současné politiky firmy je nutné zabudovat nejen aktualizace korporátní politiky, ale také politiku evropské centrály. Jak je vidět na obrázku všechny politiky jsou vzájemně propojené a musejí spolupracovat.



Obrázek 14: Spolupráce bezpečnostních politik

5.1 Aktuální bezpečnostní politika firmy

Současná firemní bezpečnostní politika IT je rozdělena do několika části, kde ke každé části je několik nařízení a kdo za jejich dodržování zodpovídá. Toto rozdělení je shodné s evropskou centrálou i korporátní politikou. Jednotlivé časti, jsou:

- Uživatelské jméno a heslo
- Přenos dat a přístupy
- Připojení na internet
- Vzdálené připojení
- Osobní omezení
- Zabezpečení počítače
- Systémová nastavení

V rámci firemních nařízení je zde nemůžu všechny vypsat a rozepsat co přesně obsahují. V následujících tabulkách je několik obecných politik, která jsou využívaná ve firmě spolu s rozdělením zodpovědnosti.

Tabulka 27: Příklad politiky uživatelské přihlášení a hesla

	Zodpovídá		
	IT Manažer	IT oddělení	Každý sám
Uživatelské ID nesmí být sdíleno mezi více uživateli			X
Pravidelné změny hesla v rozmezí X měsíců			X
Heslo musí mít minimální délku X znaku musí obsahovat číselné i alfanumerické znaky.			X
Smazání neaktivních ID účtů		X	

Politiky pro uživatelské jméno a heslo v předchozí tabulce jsou jedny z nejzákladnějších a jsou využívány téměř v každé firmě, které na bezpečnosti, alespoň trochu záleží. Příklady v následující tabulce jsou souhrnem z více dříve zmíněných částí bezpečnostní politiky. Jsou trochu konkrétnější, ale jsou také zmiňovány již v předchozích částech práce.

Tabulka 28: Přístup k internetu a bezpečnost

	Zodpovídá		
	IT Manažer	IT oddělení	Každý sám
V případě nutnosti vzdáleného přístupu do firemní sítě je zažádat u manažera IT oddělení.	**X**		
Přidělení přístupu na internet pro nové uživatele je třeba zažádat u manažera IT oddělení.	**X**		

Na firemních PC je zakázáno využívat síť internet k přístupu na soukromé mail klienty, internet, hry.			**X**
Je zakázáno otevírat neznáme a podezřelé e-maily			**X**
Je zakázáno připojovat soukromá USB zařízení k firemním PC			**X**
Je zakázáno instalovat software z neznámých zdrojů		**X**	
Veškeré zařízení, jež obsahuje firemní data a opouští areál firmy, musí obsahovat kryptovací software.		**X**	
Data na firemních laptopech musí být periodiky zálohována		**X**	

5.2 Navržené změny

Po analýze stávajících politiky bylo zjištěno několik neshod se současnými politikami korporace a evropské centrály. První čtyři položky v následující tabulce byly navrženy na základě zjištění těchto neshod. Poslední dva body byly navrženy na základě zkušeností IT oddělení. Kdy v mnoha případech uživatelé měli nalepené heslo od PC na monitoru nebo klávesnici.

Tabulka 29: Nově navržené politiky

	Zodpovídá		
	ID Manažer	IT oddělení	Každý sám
Soukromé mobilní zařízení můžou mít přístup pouze do Wi-Fi sítě pro hosty firmy.		X	
Mobilní zařízení smí využívat firemní mail pouze přes firemní VPN klienta.			X
V případě odprodeje zařízení firmy po jeho vyřazení je třeba firemní HDD bezpečně naformátovat a přepsat, aby nemohlo dojít k obnovení firemních dat.		X	
Vývojové a testovací zařízení nesmí být propojeno do firemní sítě			X

Uživatelské heslo nesmí být nikde zapsáno na místě, kde může být nalezeno jiným uživatelem.			X
Je zakázáno připojovat soukromé PC do firemní sítě.			X

ZÁVĚR

V teoretické části, této práce je zpracována literární rešerše na téma auditů obecně a dále auditů IT. Jsou zde popsány legislativní požadavky na firmy dle nového kybernetického zákona a je zde popsáno několik rámců, které jsou s touto problematikou spojeny. Je zde popsáno jejich nejčastější využití, dále silné slabé stránky a rozsah pokrytí ve společnosti.

V praktické části probíhá analýza současné stavu a řešení na firmě. Je zde rozebírána organizační struktura firma a vedení. Řešena oblast a procesy, které by se měli auditovat. Tyto procesy byly dodány evropskou centrálou firmy a byli jedním z prvotních důvodů auditu. Na základě této analýzy je vyhodnocen rámec COBIT, který nejlépe vyhovuje této konkrétní firmě.

Dále je řešena implementace některých procesů, které jsou součástí COBIT a po jejichž implementování bude audit jednodušší. Jedná se o implementaci optimalizace rizik, optimalizace zdrojů, správa dodavatelů, správa bezpečnosti, další auditované součásti správa vědomostí a správa majetku byli ve firmě implementovány již dříve. Po dokončení implementace bylo provedeno hodnocení výkonosti neboli audit. Byla zkontrolována veškerá stávající dokumentace a nastavené procesy. Byly vyhodnoceny všechny nastavené metriky, které jsme si zvolili již během implementace. Po jejich vyhodnocení bylo zjištěno několik nedostatků a bylo přidáno několik poznámek pro vytvoření nových metrik do dalšího auditu. Ke zjištěným nedostatkům byla nevržena opatření na jejich odstranění.

Závěr práce je věnován revizi bezpečnostní politiky firmy, která byla součástí firemního auditu. Firemní politika byla doplněna o několik chybějících bodů, které byli nastaveni politikou korporace a evropské centrály firmy. Dále bylo vedení firmy navrženo několik pravidel do bezpečnostní politiky IT oddělením na základě zkušenosti s uživateli firmy.

SEZNAM POUŽITÉ LITERATURY

[1] DOUCEK, Petr, Luděk NOVÁK, Lea NEDOMOVÁ a Vlasta SVATÁ. Řízení bezpečnosti informací. 2. vydání. Praha: Professional publishing, 2011. ISBN 978-80-7431-050-8.

[2] COBIT 5 (Control Objectives for Information and related Technology). ManagementMania. USA: ManagementMania.com, 2016 Dostupné z: https://managementmania.com/cs/cobit-control-objectives-for-information-and-related-technology.

[3] DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Praga : Computer Press, 2004. 200 s. ISBN 80-251-0106-1.

[4] SVATÁ, Vlasta: Audit informačního systému. Oeconomica, Praha, 2005. ISBN 978-80-7431-034-8.

[5] ČSN ISO/IEC 27000:2010. Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník.

[6] ČSN ISO/IEC 27001:2006, Informační technologie – Bezpečnostní techniky – Systém managementu bezpečnosti informací – Požadavky.

[7] *ISO-27001* [online]. 2015 [cit. 2017-05-09]. Dostupné z: https://managementmania.com/cs/iso-27001

[8] ČSN ISO/IEC 27002:2006, Informační technologie – Soubor postupů pro management bezpečnosti informací.

[9] ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, 2013. ISBN 978-80-7204-872-4.

[10] ITIL 2011. 1. vyd. Brno: Computer Press, 2012, 216 s. ISBN 978-80-251-3732-1.

[11] ITIL FOUNDATION: Přípravný kurz na základní certifikaci ITIL. Praha: Telefónica Czech Republic a.s, 2012

[12] ISACA. Cobit 5: A business framework for the governance and management of enterprise IT [online]. Rolling Meadows. IL: ISACA, 2012. ISBN 978-160-4202-373. Dostupné z: http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx.

[13] ISACA. COBIT 5: Implementation. Rolling Meadows (Ill.): ISACA, 2012. ISBN 978-160-4202-380.

[14] ISACA. *COBIT 5: Enabling processes*. Rolling Meadows (Ill.): ISACA, 2012. ISBN 978-160-4202-397.

[15] ISO-27002 [online]. 2015 [cit. 2017-05-09]. Dostupné z: http://cybersecurity.cz

[16] Komora auditorů České republiky [online]. 2015 [cit. 2017-05-09]. Dostupné z: http://www.kacr.cz/prirucka-pro-provadeni-auditu

[17] KRÁLÍK, Lukáš, LUKÁŠ, Luděk. Proposal of Evaluation ITIL® Tools. In Proceedings of the 2014 International conference on Applied Mathematics, Computational Science and Engineering. Craiova : Europment, 2014, s. 142-146. ISSN 2227-4588. ISBN 978-1-61804-246-0.

[18] KRALIK, Lukas, SENKERIK, Roman, JASEK Roman. Proposal of Evaluation Criteria for Free and Open Source Tools for Modeling and Support of IT Service Management According to ITIL. In Proceedings of the 29th Europen Conference on Modeling and Simulation (ECMS 2015).Germany: Digitaldruck, 2015, s.537-542. ISBN 978-0-9932440-0-1.

[19] Národní centrum kybernetické bezpečnosti [online]. [cit. 2017-05-09]. Dostupné z: https://www.govcert.cz/

[20] Best Practice [online]. [cit. 2017-05-09]. Dostupné z: http://www.bestpractice.cz

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Active directory
ASP	Active Server Pages
BSC	Balanced Scorecard
CCTA	Central Computer and Telecommunications Agency
COBIT	Control Objectives for Information and related Technologies
ERP	Enterprise Resource Planning
ESX	Enterprise Server Virtualization Platform
HDD	Hard Disk Drive
HP	Hewlett-Packard
HR	Human-Resources
HW	HardWare
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IS	Informační systém
ISACA	Information Systéms Audit and Control Association
ISO	International Organization for Standardization
IT	Information Technology
ITSM	IT Service Management
MS	Microsoft
MES	Manufacturing Execution Systems
NG	No Good
OEM	Original Equipment Manufacturer
OGC	Open Geospatial Consortium
PBX	Private Branch Exchange

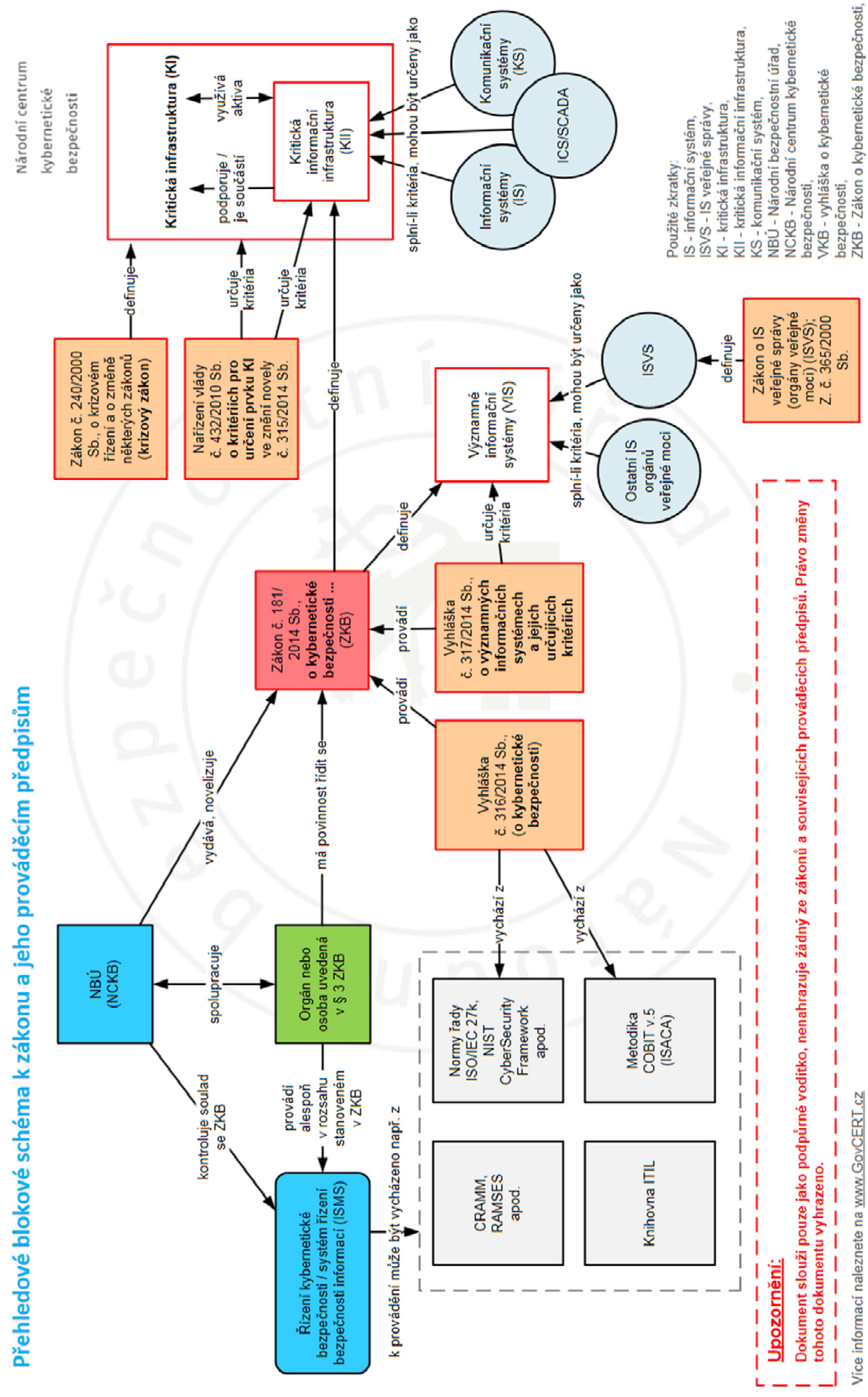
PC	Personal computer
PING	Packet InterNet Grope
QC	Quality Control
RDP	Microsoft Remote Desktop
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SW	SoftWare
USB	Universal Serial Bus
VPN	Virtual Private Network

SEZNAM OBRÁZKŮ

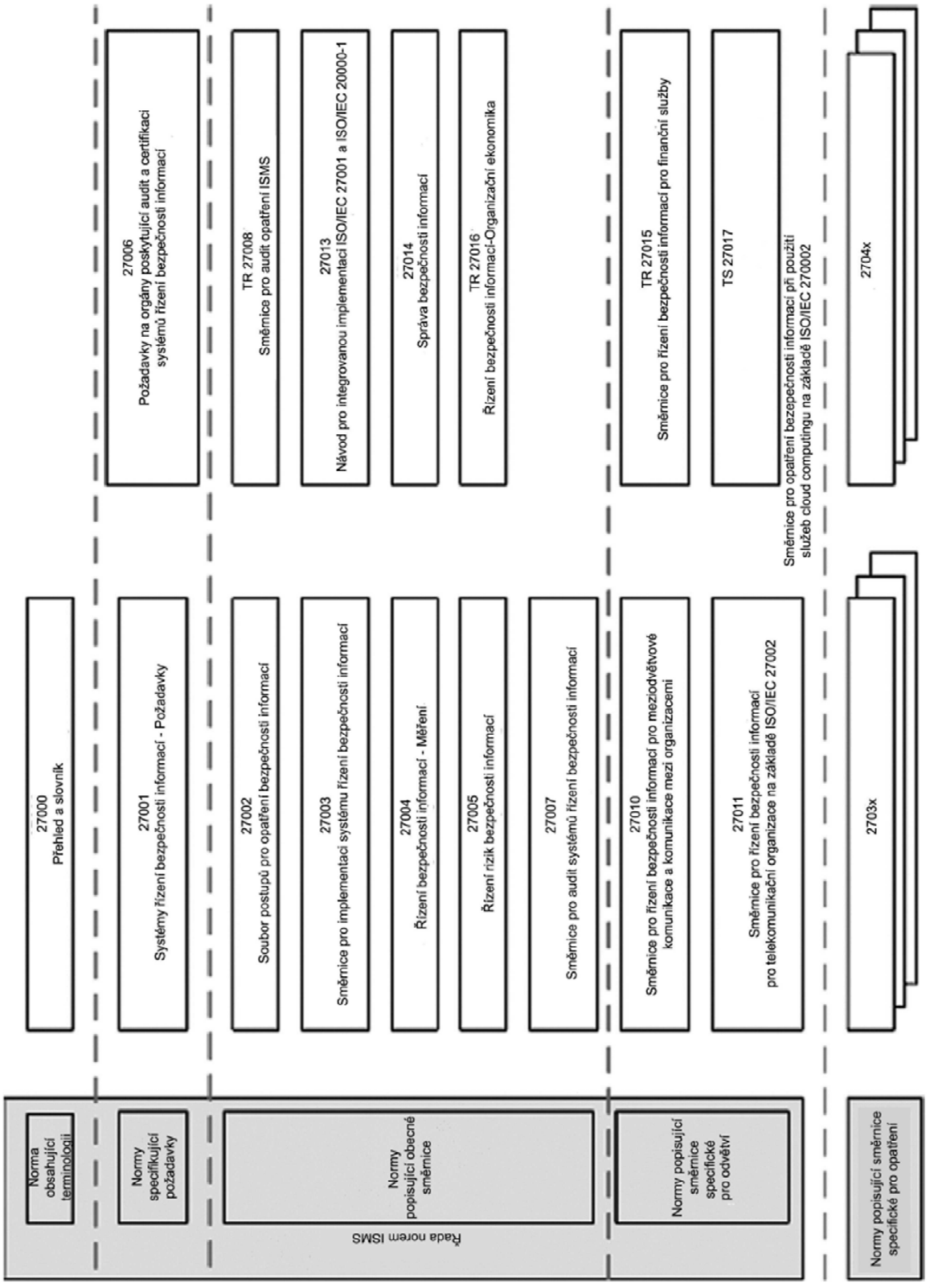
SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: SCHÉMA KE KYBERNETICKÉMU ZÁKONU



PŘÍLOHA P II: SKUPINA NOREM ISO/IEC 27K



PŘÍLOHA P III: ROZDĚLENÍ PROCESŮ DLE COBIT 5