Využití metodiky COBIT pro stanovení úrovně informačních technologií v organizaci

Aleš Matějíček

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Aleš Matějíček**
Osobní číslo:	**A13267**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Využití metodiky COBIT pro stanovení úrovně informačních technologií v organizaci.**
Téma anglicky:	**The Use of the COBIT Standard for Assessing the Level of ICT in an Organisation.**

Zásady pro vypracování:

1. **Proveďte liteární rešerši na téma stanovení úrovně informačních technologií v organizaci.**
2. **Analyzujte a navrhněte postupy k dosažení strategických cílů organizace s využitím metodiky COBIT.**
3. **Definujte strategický plán rozvoje ICT organizace s ohledem na architekturu, procesy, vztahy a investice.**
4. **Identifikujte a stanovte technické předpoklady pro dosažení požadovaných výstupů.**
5. **Navrhněte vzdělávací plán pro ICT vzdělávání uživatelů.**
6. **Definujte nástroje pro kontrolu plnění stanovených cílů.**
7. **Vyhodnoťte řešení projektu a stanovte doporučení pro udržení jeho kvality v budoucnu.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **COBIT 5 (Control Objectives for Information and related Technology). ManagementMania [online]. USA: ManagementMania.com, 2016 [cit. 2016-02-04]. Dostupné z: https://managementmania.com/cs/cobit-control-objectives-for-information-and-related-technology.**
2. **DOUCEK, Petr, Luděk NOVÁK, Lea NEDOMOVÁ a Vlasta SVATÁ. Řízení bezpečnosti informací. 2. vydání. Praha: Professional publishing, 2011. ISBN 978-80-7431-050-8.**
3. **DOBDA , Luboš. Ochrana dat v informačních systémech. Praha : Grada, 2001. 288 s. ISBN 8071694797.**
4. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Praga : Computer Press, 2004. 200 s. ISBN 80-251-0106-1.**
5. **Information Systems Audit and Control Association [online]. USA: ISACA, 2016 [cit. 2016-02-04]. Dostupné z: https://www.isaca.org/Pages/default.aspx.**
6. **KOVACICH, Gerald L. Průvodce bezpečnostního pracovníka informačních systémů: zavádění a prosazování bezpečnostní politiky informačních systémů. Brno : UNIS, 2000. 200 s. ISBN 80-86097-42-0.**

Vedoucí bakalářské práce: **Ing. Lukáš Králík**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **14. prosince 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

Ve Zlíně dne 14. prosince 2018

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

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, 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 26.05.2019

Jméno: Aleš Matějíček …….

podpis diplomanta

ABSTRAKT

Bakalářské práce popisuje základní metodické postupy a principy frameworku COBIT 2019, pochopení klíčových principů a terminologii, kterou framework COBIT 2019 používá, obchodní přínos systému, řešení problémů v oblasti řízení a místa, kde se vzájemně ovlivňují v podnikovém řízení. Správné pochopení pěti klíčových principů pro správu a řízení podnikového IT. Schopnost, jak správně řídit a spravovat celostním způsobem podnik, pochopit klíčové koncepty Hodnocení způsobilosti procesu PCA a klíčové vlastnosti PRM. V konečném důsledku, jak procesy COBIT 2019 a PRM pomáhají nastavit pět základních principů a sedm pilířů pro stanovení úrovně informačních technologií v organizaci a správu a řízení podnikového IT. Pochopení konceptu a formátu frameworku COBIT 2019 umožní získat obchodní výhodu, která přinese kvalitu do procesů pro správu a řízení podnikového IT.

Klíčová slova: COBIT, ISMS, PDCA, framework, proces, řízení, ZKB

ABSTRACT

Bachelor thesis is describing the basic methods and principles of the COBIT 2019 framework, understanding the key principles and terminology and the business benefits of using COBIT 2019, solving the IT management issues and challenges that affect enterprises.

Correct understanding the 5 Key Principles of COBIT for the governance and management of Enterprise IT. How COBIT enables IT to be governed and managed in a holistic manner for the entire enterprise, understand the key concepts in a PCA and the key attributes of the PRM. In the End, how the COBIT 2019 processes and the PRM help guide the creation of the 5 Principles for Governance and 7 pillars for Assessing the Level of ICT in an Organization. Understand the concepts relating to the structure and format of the framework, the drivers and business benefits of using the COBIT 2019 framework, provide a renewed and authoritative governance and management framework for enterprise information and related technology

Key word: COBIT, ISMS, PDCA, framework, process, management, ZKB

Dovolte mi touto cestou vyjádřit poděkování Ing. Lukáši Králíkovi, za jeho cenné rady, a především pak za nezměrnou trpělivost, ochotu a vstřícnost při dlouhých konzultacích a vedení mé bakalářské práce. Dále bych rád poděkoval své rodině a svému okolí za trpělivost a absenci v čase kdy jsem vytvářel tuto bakalářskou práci.

OBSAH

ÚVOD

Prevence je hybnou silou k optimalizaci a k hledání systémových řešení složitých situací. Je moudré a určitě je vhodné problematice efektivity v organizaci věnovat pozornost, protože umožňuje strategicky uvažovat a možné úkony odladit na modelových situacích, kde tato řešení mohou ušetřit nejen drahý čas pracovníků, ale také nemalé finanční náklady na prostředky, které jsou do ICT světa vkládány a posuzování výběru dodavatelů. [8]

Žijeme v době, kde jsme prostoupeny informačními technologiemi a ty se pro nás stávají všudypřítomnými. Umožňují nám zefektivnit pracovní procesy, zrychlit a zjednodušit komunikaci. Do ruky se nám dostává stále více komunikačních nástrojů, vznikají nové produkty, technologie, vyvíjejí se nové aplikace, která nám mají usnadnit, či zjednodušit pracovní nebo osobní život.

Permanentní vývoj a inovace v oblasti podnikových informačních systémů (IS) a informačních a komunikačních technologií (ICT) vedou k integraci ICT do činností organizace a tím i na druhou stranu k rostoucí závislosti podniků i organizací na jejich funkčnosti. ICT a jeho důležitost představuje významný potenciál konkurenční výhody ve světě globalizace. [3]

Zde je namístě si otevřeně klást otázky. Které technologie či technologické celky jsou pro nás ty správné? Které aplikace jsou pro nás ty správné? Potřebujeme všechny nástroje, které aktuálně ve firmě využíváme, nebo je možnost se některých zbavit a jak je chránit? [1] Sleduje někdo nákladovost systémů, jejich dlouhodobou udržitelnost, případně rentabilitu. Potřebujeme tolik systémových inženýrů, nebo správců systému, nebo je pro nás efektivnější služby řešit formou outsourcingu případně část služeb nakupovat formou cloudových služeb? V současné době je téměř nepředstavitelné, aby procesy a činnosti organizací nebyly podporovány funkcemi ICT. [3] Je to spousta otázek, které často generují jen spoustu dalších otázek.

Největším rizikem ICT je, že samy nebudou buď vůbec schopny podporovat požadované procesy, nebo je budou podporovat pouze omezeně. Zde nastupuje na scénu potřeba smysluplnosti interních procesů, jejich popis, kvantifikace, začlenění do logických rámců, které zapadají do šablon struktur, které mají definovaný charakter a směr. [3]

Metodiky, které poskytují možnosti řešení, jsou k dispozici, záleží jen preferenci, případně potřebě, kterou definují dodavatelské nebo subdodavatelské vztahy, nejrozšířenější u nás jsou různé variace normy ISO, případě ITIL, TOGAF, atd.]

Dlouhodobě velmi efektivní se jeví kombinace metodik ITIL a COBIT, kde COBIT zajišťuje analýzu a identifikaci prvků pro řízení IT prostředí a ITIL pro vytvoření designu a následně implementaci systému operativně-taktického řízení služeb v souladu s IT strategií vytvořenou dle metodiky COBIT. [2]

I. TEORETICKÁ ČÁST

1 HISTORIE

V dnešní době jsou informace klíčový obchodní nebo podnikový nástroj a je dobré sledovat, případně mapovat jejich tok od vytvoření až po zánik. Informační technologie ze své podstaty mají za úkol tvořit procesy, zavádět a zdokonalovat metody pro sběr, zpracování a využívání dat a informací a hledat možnosti automatizace.

Dnešní, z velké části digitalizovaný svět, poskytuje ohromné množství neselektovaných informací. Pokud chceme mít možnost aktivně a dynamicky ovlivňovat procesy, je třeba dát věcem, informacím řád. Dále je nutné stanovit systém a definovat jednotlivé systémové funkční celky, které nám v neselektovaných informacích vytvoří milníky, které dokážeme lépe kvantifikovat, případně ohodnotit, dát jim prioritu, která v další fázi může znamenat pořádek. [8]

Paralela je také v oblasti řízení firem, podniků a organizací. Zde pracujeme také s velkým množstvím informací, které vyžadují hierarchické členění a následné zpracování. Se zrychlující se dobou je nutné stanovit co nejpřesnější algoritmy, které definují jednoznačnost, a ta informace řadí do fyzických, nebo virtuálních složek. Míra kvality stanovených procesních postupů a jejich smysluplnost definuje následnou rychlost a kvalitu zpracování. Z pohledu uživatele je nutná smysluplnost, která definuje motivaci se kterou úlohu plní a tím i rychlost vyřízení požadavku.

William Edward Deming, americký statistik, průkopník optimalizací, se proslavil tím, že hledal možnosti, jak stále efektivněji a s lepšími výsledky řídit jakost v automobilovém průmyslu. Vytvořil tak základní koncept řízení, kterému se říká Demingův cyklus (PDCA). [19]

Proslul také vyjádřením 7 smrtelných chorob firem:

- Nedostatek vytrvalosti
- Důraz na krátkodobé zisky
- Hodnocení na základě výkonu, zásluh a každoroční hodnocení výkonu
- Vrtkavost managementu
- Řízení firmy jen na základě viditelných čísel
- Nadměrné nálady na zdravotní péči
- Nadměrné náklady na záruční opravy

Demingův cyklus (PDCA z anglického plan-do-check-act tedy naplánuj-proveď-ověř-jednej) je základní popis metody řízení založený na čtyřech krocích, které mají vést ke stálému/cyklickému zdokonalování procesů, výrobků a služeb. Poprvé elementární formu konceptu PDCA zaznamenal ve vědecké práci a následně rozvinul Francis Bacon (Novum Organum, r. 1620) a řešení je možné popsat jako hypotéza-experiment-hodnocení, jinou terminologií tedy naplánuj-proveď-ověř. Jednotlivé fáze PDCA se skládají z: [1]

I. Naplánuj

První krok cyklu, který primárně slouží pro stanovení cílů a hlavně jako náprava k odstranění nedostatků. Definují se úkoly, opatření, nástroje a procesy ke stanovení cílů. Součástí plánu jsou konkretizované návrhy řešení, které budou součástí realizace. Podmínka nutná je v podobě personálního zajištění projektu kvalifikovanými pracovníky.

II. Proveď

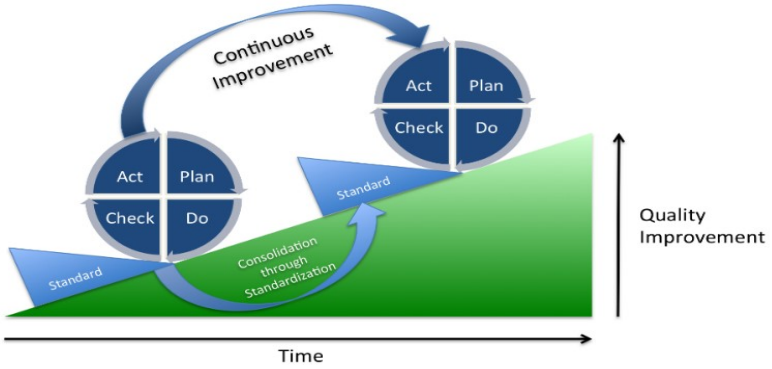
Druhý krok cyklu spočívá v implementaci vytvořeného plánu a následné realizaci řešení, případně zpracovaní nových procesů. Zároveň dochází ke sběru dat a měření dat je zdrojem pro možné další kroky. Každý krok, každá změna je provedena s patřičnou dokumentací.

III. Ověř

Třetí krok je zároveň krokem kontroly. Intenzivně se pracuje s nasbíranými daty a předchozí kroky se podrobně analyzují, dochází k procesu podrobného zkoumání a hledají se odchylky od plánu implementace. Doporučuje se použití grafů, které snáze zobrazí trendy a tím nastavení dalšího vývoje, které je důležitý pro plánovaný záměr a postup

IV. Jednej

Čtvrtý krok je akce, která uzavírá celý cyklus. Pokud fáze, Ověř, prokáže oprávněnost nasazení metodiky a pozitivní dopad procesu, stává se tak nový procesním standardem.



Obrázek 1: PDCA cyklus [19]

PDCA je univerzálním postupem a základním stavebním kamenem pro většinu procesních metodik. [7] Vznikají tak pracovní postupy, které definují normy pro nakládání s procesy a s informacemi. V našich končinách je nejrozšířenější Mezinárodní organizace pro normalizaci (ISO), která byla založena v roce 1947 a v roce 2011 definovala více než 18000 ISO norem ve všech oblastech, kromě elektrotechniky. [2]

Oblast, která je náplní mé bakalářské práce filozoficky vychází z principů Demingova cyklu a patří do části správy a řízení informaticky, tzv. IT Governance, nebo Enterprise Governance, která definuje řízení podnikové informatiky do stavu, aby maximálně podporovala podnikové strategie a cíle. Lze je definovat jako soubor odpovědnostní a činností, které realizují vlastníci nebo vedení organizace, kteří chtějí realizovat strategický rozvoj při zajištění přiměřených rizik a efektivní kontroly průběžné spotřeby zdrojů v organizaci. Zohledňuje se primárně návratnost investic do Informačních a komunikačních technologií (ICT) při realizaci očekávané přidané hodnoty a při vyrovnání rizika s návratností investic do ICT vložených. [8]

V této oblasti dominuje dlouho mezinárodní profesní asociace ISACA (Information Systems Audit and Control Association), která zastřešuje oblasti auditu, řízení, kontroly a bezpečnosti informačních systémů, zajišťuje certifikace, systémovou metodiku a praktické příručky.

Jedna z nejkomplexnějších metodik, kterou vytvořili a která poskytuje ucelenou řadu rámců pro oblast IT Governance je COBIT.

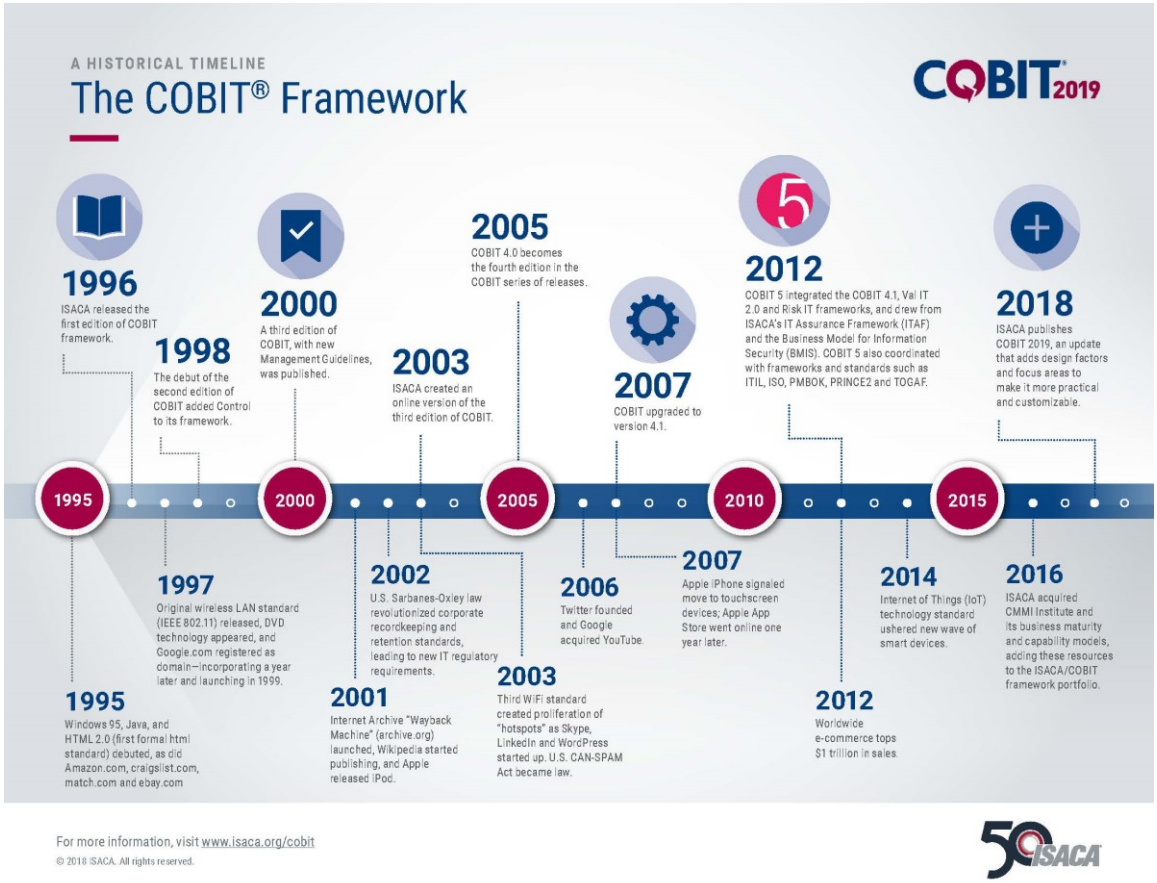
„COBIT (Control Objectives for Information and Related Technology), je framework vytvořený mezinárodní asociací ISACA pro správu a řízení informatiky (IT Governance).

Jedná se o soubor praktik, které by měly umožnit dosažení strategických cílů organizace díky efektivnímu využití dostupných zdrojů a minimalizaci IT rizik. (Wikipedia, 2019b)

Metodika je primárně určena pro auditory a TOP manažery. Mezi hlavní přednosti patří široký záběr napříč celou organizací. Fokus není kladen pouze na oblast ICT, ale také na oblast auditů a kontrol. COBIT má tendenci vytvořit ucelený systém pravidel, který dokáže zastřešit ostatní systémy, jako ITIL, TOGAF, ISO a které zapadnou do uceleného rámce metodiky, která je z funkčního pohledu zastřešuje. [15]

COBIT byl poprvé publikován roku 1996 ve verzi COBIT 1 jako nástroj pro audit. Druhá verze byla rozšířena o kontrolní postupy a implementační nástroje a procesy rozpracovanosti a detailní cíle (1998), třetí verze v sobě začleňuje manažerské postupy a zároveň inovovanou metodiku auditu (2000). Čtvrtá verze k sobě přiřadila Val IT (řízení přidané hodnoty ICT pro podnik) a Risk IT (řízení nežádoucích událostí) a pátá verze finálně tyto metodiky do sebe zakomponovala. [15]

Verze COBIT 2019, díky akvizici CMMI Institute, aktuálně dceřinou společností ISACA, rozšiřuje možnosti metodiky o stupeň zralosti (maturity model) a úrovně schopností (capability levels) a nabízí tím možnost průběžného vyhodnocování kvalitativního růstu organizace, který je systémově měřitelný. [13]



Obrázek 2: Evoluce COBIT [9]

2 COBIT - ZÁKLADNÍ METODIKA

Information Systems Audit and Control Association (ISACA) je mezinárodní organizace zaměřená na oblast auditu, řízení, kontroly a bezpečnosti informačních systémů a obsahově zastřešuje metodiku COBIT. Organizace má dlouhodobou strategii vytvořit systém v podobě „deštníku“, který začlení pod jednotou metodologii všechny další systémy, jako jsou ITIL, TOGAF nebo ISO. Svým způsobem chce definovat hranice, kde se jednotlivé systémy vzájemně nekanibalizují, ale naopak stanoví rozhraní, kde se definují kompetence navazujících systémů a vytvoří se systém odkazů na spřátelené systémy. [16]

Cílovou skupinou uživatelů metodiky COBIT jsou zainteresované strany (stakeholders) vnitřní (výkonný manažeři, IT manažeři, risk manažeři, vlastníci) a vnější (zákazníci, dodavatelé IT, místní samospráva, vláda). Vnitřní stakeholdeři získávají nástroje pro organizaci a správu IT, možnost sledovat výkonnost, strukturovat oddělení, kontrolovat náklady na IT a sladit strategii IT s obchodními prioritami. Pomáhá řídit závislost na externích poskytovatelích IT služeb, identifikovat a spravovat rizika spojená s provozem IT. Pro vnější stakeholdery pomáhá zajistit správný systém řízení firmy, bezpečnost a soulad s platnými pravidly a předpisy. [15]

COBIT 2019 je vystavěn na dvou základních zásadách:

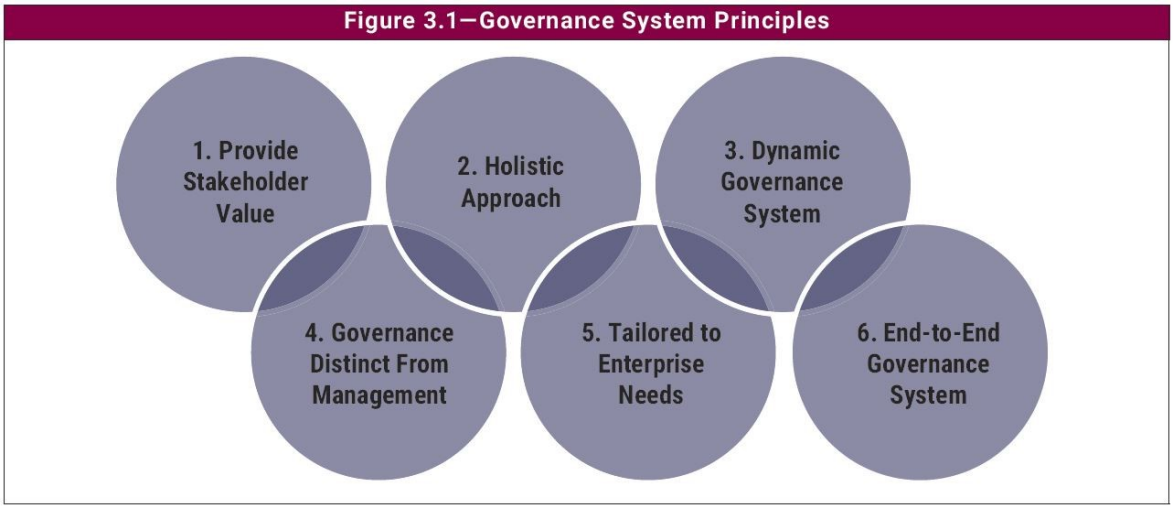
- Popis systému řízení
- Popis cílů organizace

Co to v praxi znamená? Stanovené principy fungují jako referenční příručky pro příslušné obory a role, na kterých jsou pak postavené všechny další součásti. Pro strategické definování cílů společnosti je nutné stanovit oblasti, nebo kategorie, které budou optimalizací zasaženy, případně v jakém pořadí (často se definuje na základě jednotného klíče, který stanovuje priority pro jednotlivé oblasti, jak z pohledu času, tak z pohledu rozsahu realizace). [15]

2.1 Systémy řízení podnikových informací a technologií:

- Zajištění potřeb zainteresovaných stran (Provide Stakeholder Value)
- Umožnit celistvý a systémový přístup (Holistic Approach)
- Dynamický systém řízení (Dynamic Governance System)
- Oddělení vedení od řízení (Governance Distinct From Management)

- Jeden integrovaný rámec (Tailored to Enterprise Needs)
- Pokrytí celé společnosti (End-to-End Governance System)



Obrázek 3: Principy COBIT (systém řízení) [15]

2.1.1 Zajištění potřeb zainteresovaných stran (Provide Stakeholder Value)

Vycházíme z předpokladu, že každá firma má své potřeby a ze zkušenosti víme, že potřeby různých oddělení mohou být až protichůdné. Proto je třeba potřeby přesně identifikovat a v rámci diskuze zajistit rozsah její realizace. K tomu slouží seznam obecných potřeb, ze kterého lze vycházet, jak při diskuzi s interními týmy, tak externími týmy, které se procesu aktivně zúčastňují. Na základě těchto potřeb lze určit firemní cíle, z nich lze definovat cíle IT a finálně jednotlivé cíle pro definované oblasti ICT. [15]

2.1.2 Umožnit celistvý a systémový přístup (Holistic Approach)

Stavíme-li dům, musíme začít stavbou pevných základů, na které můžeme následně začít stavět nosné zdi a na závěr střechu. Z našeho úhlu pohledu je ICT něco jako střecha. Musíme mít business model, potřebujeme znát procesy, zpracované vývojové diagramy. Ale to je málo. Potřebujeme, aby všechny oblasti, v našem případně pilíře, rostli optimálně stejně rychle kvůli stabilitě celého systému. [15]

Pro stabilitu a zdárný růst je nutné, aby se jednotlivé oblasti vzájemně doplňovali a podporovali. Je dobré si znovu projít nastavená očekávání od jednotlivých stran (interní, externí),

kvantitativní stanovené cíle, životní cykly procesů, ale i produktů a z výsledků analýz vyzdvihnout přednosti firmy nebo organizace.

2.1.3 Dynamický systém řízení (Dynamic Governance System)

Systém řízení by měl být dynamický. Znamená to, že každá změna návrhu strategie nebo technologie bude mít dopad na informační systém jako celek a je nutné dopad těchto změn zahrnout do návrhu. Dynamický pohled na podnikové řízení IT garantuje budoucí životaschopný systém, který dokáže reagovat na změny rychle a operativně. [15]

2.1.4 Oddělení vedení od řízení (Governance Distinct From Management)

Cílem každého z nás je rychle a dobře vykonávat svoje každodenní úkoly. Za to jsme v konečném důsledku honorování v horším případě pochvalou a v lepším případě formou bonusu na výplatě, nebo cílovou odměnou. Pokud budeme dobře vykonávat to, co nikdo nepotřebuje, tak se žádné pochvaly nedočkáme. Z tohoto důvodu je potřeba naše každodenní snažení řádně nasměrovat. Potřebujeme vedení. A to je to, co v řadě případů chybí. A právě COBIT 5 zavádí speciální oblast, která se nazývá Governance (vedení/směrování). Tato oblast je zpracovaná do procesního modelu ICT a zajišťuje, že každý účastník týmu bude vědět, co má dělat a hlavně bude vnímat smysluplnost činností, které svou prací naplňuje.

Oddělení řízení firmy od vedení firmy je zdánlivě nesmyslný úkol. Je nutné si uvědomit, jaký je mezi řízením a vedením rozdíl. Řízením lidí se rozumí rozdělování činností tak, aby byli efektivní, dělání věcí správně. (jedná se primárně o krátkodobý horizont). Vedení lidí znamená pěstovat v lidech kompetence, aby svoji práci dělali dobře, tj. dělali správné věci (jedná se primárně o dlouhodobý horizont). [15]

2.1.5 Jeden integrovaný rámec (Tailored to Enterprise Needs)

Dobrá analýza dokáže zajistit vstupy pro popis současného stavu a zároveň doporučení, na základě kterých je možné vytvořit specifická pravidla pro jednotlivé rámce. Při analýze, zpravidla velkých organizací, je možné vidět, že jednotlivá oddělení si mezi sebou „nerozumí“. Že mluví na sebe „jiným jazykem“. Nejčastěji to je právě v oblasti ICT. Cílem je najít „společný jazyk“, kterým se dokáží všechna oddělení domluvit. Terminologii, která propojí pro všechny zúčastněné strany vše dohromady a najde společnou cestu. To je přesně

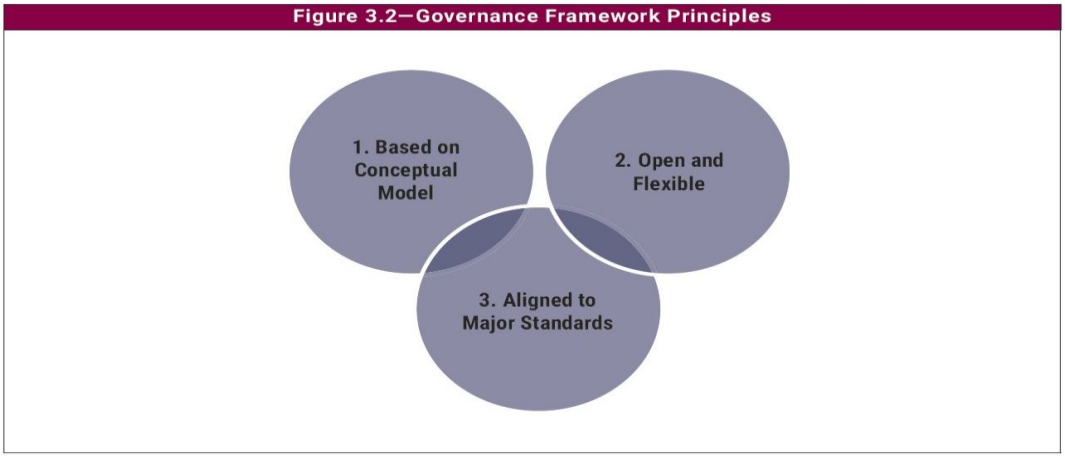
úloha COBIT 5. V rámci jednotné terminologie, srozumitelné pro všechny je možné definovat hranice a zároveň všechna doporučení a standardy používat dohromady. [15]

2.1.6 Pokrytí celé společnosti (End-to-End Governance System)

Doby, kdy se na ICT nahlíželo jako na "temnou skříňku" jsou dávno minulé. Z pohledu firmy nebo organizace je ICT dodavatel, jako každý jiný a cílem je poskytnou ICT jako placenou službu. Viděno touto optikou je rázem jasnější, že nutnost definovat ICT procesy je stejně důležité, jako obchodní procesy. A v kontextu výše uvedeného je patrné, že ICT a obchodní procesy potřebují vzájemný soulad a pro optimálně fungující společnost nemůže existovat jeden bez druhého. A stejné to je z pohledu strategie, kde obchodní strategie nemůže existovat bez strategie ICT. Proto je klíčové vidět ICT v kontextu celé společnosti a nevyčleňovat ho. Tak jako v jiných oblastech i zde je nutné jasně určit oblast, pro kterou se strategie dělá, zajistit potřebné zdroje a určit kompetence a zodpovědnost bez rozdílu, zda se jedná o business nebo ICT. [15]

2.2 Cíle organizace

- Cíle organizace by měli být postaveny na modelu, který popisuje klíčové komponenty a vztahy mezi komponenty při zachování integrity a konzistence
- Cíle organizace by měli být otevřené a pružné a schopné reagovat na nové podněty a zapojit je do procesu probíhající změny
- Cíle organizace by měli být v souladu se standardy, normami a právními předpisy



Obrázek 4: Principy COBIT (cíle organizace) [15]

3 HODNOCENÍ ÚROVNĚ ICT V ORGANIZACI (SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ)

Hodnocení je stav, kdy porovnáváme minimálně dva parametry. Referenční vzorek slouží jako etalon a ostatní poměřujeme ve vztahu k referenci podle předem definovaných kritérií.

Kritéria jsou buď stanovena zákonnou normou, nebo vizí organizace. Sdílená vize je základem dlouhodobě úspěšných projektů a firem, protože lidé se většinou nesoustředí na budoucnost, protože musí, ale proto, že chtějí.

Dnešní doba nám nabízí různé nástroje. COBIT umožňuje začlenit, jak zákonné normy, tak vize organizace pod jeden hodnotící systém. Vlivy prostředí, tj. geopolitická situace, technologická evoluce, environmentální evoluce, působí na rozhodování vedoucích pracovníků společností. Hovoříme o interních a externích zainteresovaných stran (stakeholders). Stakeholder je definovaný jako jednotlivec nebo skupina, která může ovlivnit, nebo přímo ovlivňuje dosažení cílů podniku. Jedná se o vlastníky/investory, zákazníky, dodavatele, zaměstnance, lokální komunity, odbory, spolky, média, ochránci životního prostředí, vládu. Při realizaci nám udává směr kaskádování cílů. Na počátku procesu definujeme potřeby zainteresovaných stran, tj. které lze pro náš případ volně přeložit jako vizi pro organizaci v daném místě a čase, které se zhmotní přes jeden integrovaný rámec, tj. benefity z optimalizace rizik a zdrojů, se následně rozpadají na zájmy společnosti, zájmy ICT a zájmy jednotlivců. Z principu jsou požadavky jednotlivých skupin protichůdné a cílem je najít řešení a výslednou rovnováhu. Abychom dokázali cíle hodnotit, musíme je v první řadě umět změřit. [13]

3.1 COBIT Core Model

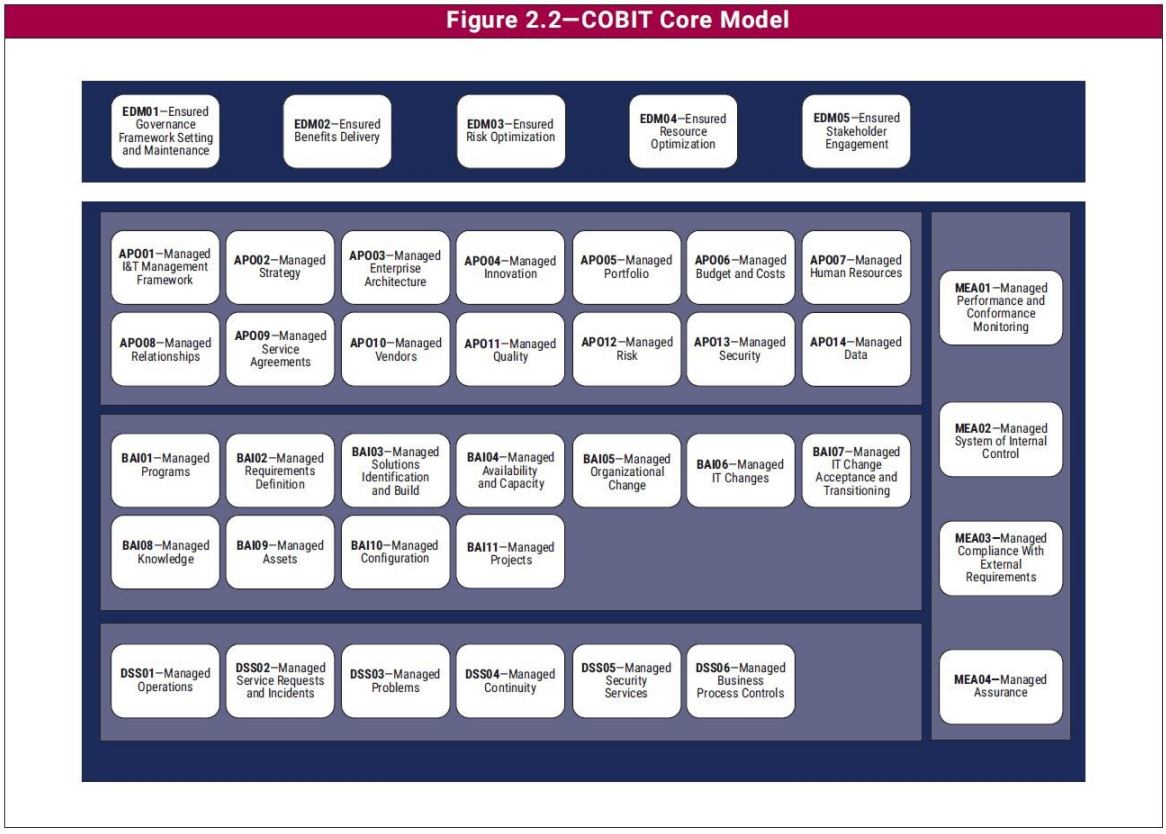
COBIT Core Model je soubor cílů správy a řízení organizace a tvoří dohromady pět oblastí.

Cíle správy jsou tvořeny:

- Ohodnoť, Řiď, Ohodnoť (EDM) – vrcholový management hodnotí strategické možnosti a dohlíží na plnění strategických cílů.

Cíle řízení jsou seskupeny do čtyř oblastí:

- Setřiď, Plánuj, Uspořádej (APO) – řeší celkovou strategií, portfolia inovací, rozpočtů, lidských vztahů, kvality, rizika a bezpečnosti.
- Buduj, Osvoj si, Uskutečni (BAI) - řeší řízení projektů, programů, organizačních změn.
- Dodej, Spravuj, Podporuj (DSS) – řízení provozu, servisních požadavků, incidentů, bezpečnostních služeb, firemních procesů.
- Kontroluj, Ohodnoť, Posuď (MEA) – kontrola a dohled, hodnocení výkonu, vnitřní kontroly a vnějších požadavků.



Obrázek 5: Core model COBIT [13]

Podnikové řízení informačních technologií musí organizace zavést, upravit a udržet. Se správou nám může pomoct systém složek. Každá složka definuje sadu kvalit, které v čase porovnáváme s výchozím stavem a porovnáním určujeme míru kvalitativního posunu podniku. Dělíme je na generické složky, které jsou obecné a mutace, které upravíme ke specifickému

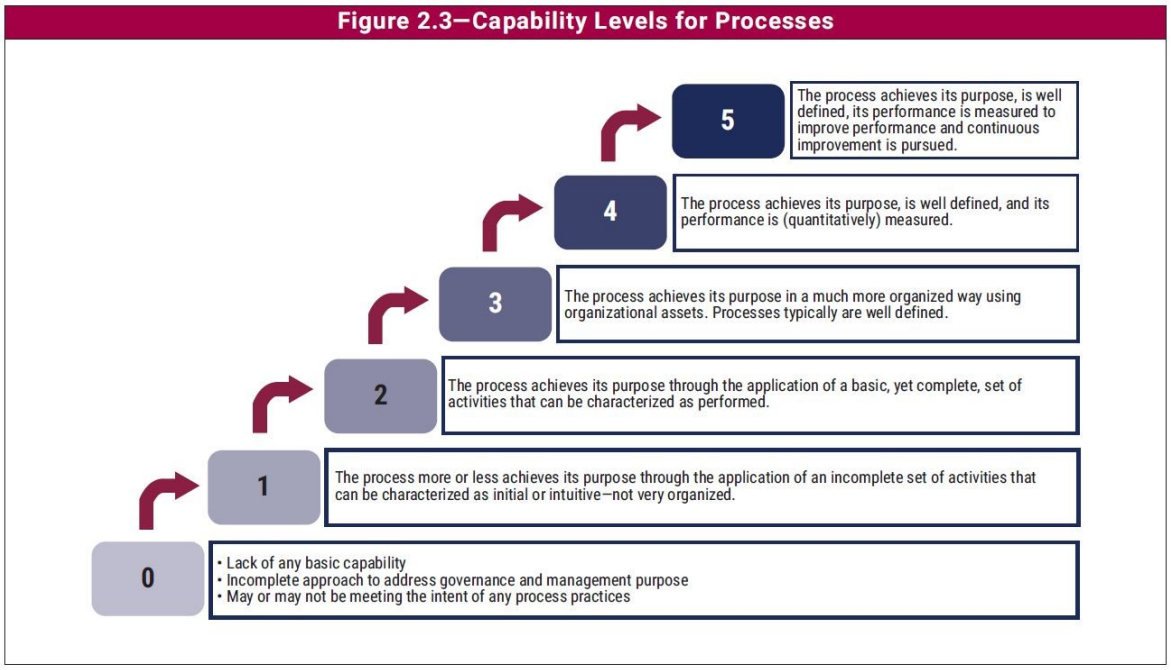
účelu nebo kontextu sboru prioritních oblastí dle zadání zákazníka. Pro stanovení konkrétních nápravných opatření je dobré generické složky přizpůsobit specifickému účelu nebo v kontextu řešeného problému zákazníka (Informační bezpečnost, DevOps, apod.)

Soubor prioritních oblastí může být prakticky neomezený. Z praxe je patrné, že generické složky a jejich mutace se volně kombinují podle potřeb daného projektu a požadavkům zákazníka. To nám umožňuje obohatit stávající otevřený model metodiky COBIT. [13]

3.2 Stupňovitý model zralosti

„Stupňovitý model zralosti“(CMMI) je systém pravidel a cílů, které určují, co by měly týmy dělat, aby jejich práce byla dobře udělaná, bylo ji možné plánovat a byla efektivní. Vytvořeny jsou 3 varianty modelu, každá se zaměřuje na samostatnou oblast práce: vývoj technologií, poskytování služeb a nákup. [13]

CMMI model, stejně jako ostatní soudobé standardy kvality, se zaměřuje především na důslednou organizaci, plánování a sledování postupů. Jeho největším rozdílem oproti většině jiných podobných standardů (např. ISO 9001) je, že definuje 5 úrovní zralosti a tým může podle modelu svou procesní dokonalost postupně zlepšovat. [13]



Obrázek 6: Kaskádování cílů [13]

COBIT Core Model přiřazuje úroveň pro všechny činnosti a umožňuje definovat procesy úrovně zralosti. Pro zjednodušení rozdělujeme úroveň 0-2 na „nižší“ a 3-5 na „vyšší“

3.2.1 COBIT procesy jsou následující:

- Zainteresované strany interní, externí (Stakeholders);
- Cíle, metriky ekonomické, kvalitativní cíle, metriky;
- Životní cyklu naplánuj, proveď, ověř, jednej;
- Ověřené praktiky prostupy, interní a externí;
- Atributy vstupy, výstupy, RACI tabulka.

3.2.2 Hodnocení procesů:

0 – Incomplete – proces není implementovaný, nebo selhal
1 – Performed – proces je implementovaný, ale nahodile a neorganizovaně
2 – Managed – proces je v základu aplikovaný, zajištěný a řízený
3 – Established – proces je zařazen a nasazen a dobře definovaný
4 – Predictible – proces je kvantitativně měřitelný, dobře definovaný a řízený
5 – Optimizing - proces lze inovovat, optimalizovat a pokračovat v dalším zlepšování

Stav procesu v bodě 0-2 znamená přímé riziko, body 3-5 poukazují na kvalitu

3.2.3 Hodnocení atributů:

N – nesplněno 0-15%;
P – částečně splněno 15-50%;
L – většinou splněno 50-85%;
F – splněno 85-100%.

3.2.4 Metriky

- Výsledkové metriky – outcome measures, tzv. lag indikátor, měření dosažené hodnoty, tzv. KGI (Key Global Indicators)
- Výkonnostní metriky – performance indicators, tzv. lead indikátor, měření pravděpodobnosti dosaženého výsledku pro dílčí subjekty, tzv. KPI (Key Performance Indicator).

3.2.5 Balanced Score Card (BSC)

- Finanční - často hlavní ukazatel výkonnosti organizace;
- Zákaznická - Image, konkurenceschopnost, zákaznická spokojenost;
- Interní podnikové procesy - kvalita služeb, zboží;
- Inovace a vzdělávání - kompetence a kvalifikace zaměstnanců.

3.2.6 Rizika hodnocení ICT

Měření úrovně ICT má rizika ve špatně definovaných požadavcích na měření, špatně definované metriky, v komunikaci mezi ICT a obchodní částí firmy, nedostatečné komunikaci mezi auditory a zaměstnanci, nedostatečné dokumentaci, apod.

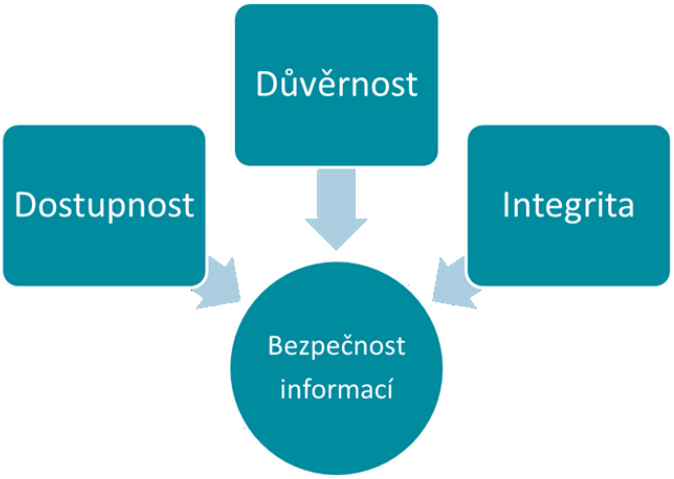
Řešením je při tvorbě metrik v dodržení principů SMART

- Specific specifické;
- Measurable měřitelné;
- Actionable dosažitelné;
- Relevant realistické;
- Timely časově ohraničené.

3.3 Hodnocení bezpečnosti ICT

Klíčovým faktorem pro hodnotu Informačních a komunikačních technologií (ICT), jako podpůrného nástroje určujícího kvalitu našeho života je škála vlastností a optimální provoz ICT služeb. Aby ICT podávalo požadovaný výkon a nedošlo tak ke snížení kvality lidského života, je potřeba chránit všechny procesy, nad kterými je ICT postaveno.

Hodnota bezpečnosti vždy závisí na hodnotě služeb ICT, respektive na ztrátách vyplývajících z důsledků bezpečnostních incidentů. Porozumění této závislosti umožňuje řídit provoz ICT efektivně. Řízení bezpečnosti informací je tak nedílnou součástí služeb ICT. [4]



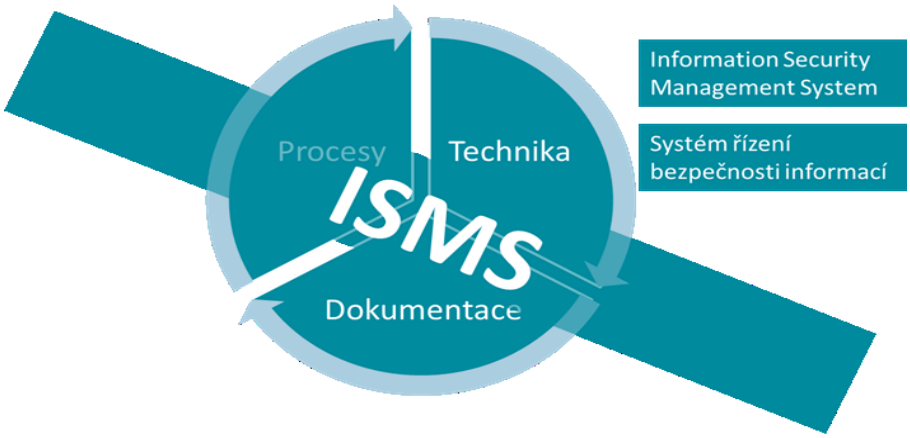
Obrázek 7: Hodnocení bezpečnosti informací

Řízení bezpečnosti informací představuje vzhledem k robustnosti ICT dnešní doby celou řadu činností, z čehož vyplývá potřeba zavedení systematického přístupu. Systematické řízení bezpečnosti informací tak vede k vytvoření Systému řízení bezpečnosti informací (dle normy ISO/IEC 27001:2013 Information Security Management System - ISMS). Kvalitní ISMS je nakonec přesně tím, co pomáhá každé organizaci (a civilizaci obecně) těžit z ICT služeb plánovaný efekt. [2]

Obrázek 8: ISMS procesy

Pro lepší porozumnění vztahu kvality života a důsledku, který incident může způsobit, rozdělujeme na tři body, a to:

1. uvědomění si hodnoty majetku (hodnocení aktiv);
2. systematického přístupu k rizikům (vztah hrozeb, zranitelností a dopadu);
3. zajištění takových opatření, která minimalizují rizika na rozumnou úroveň.



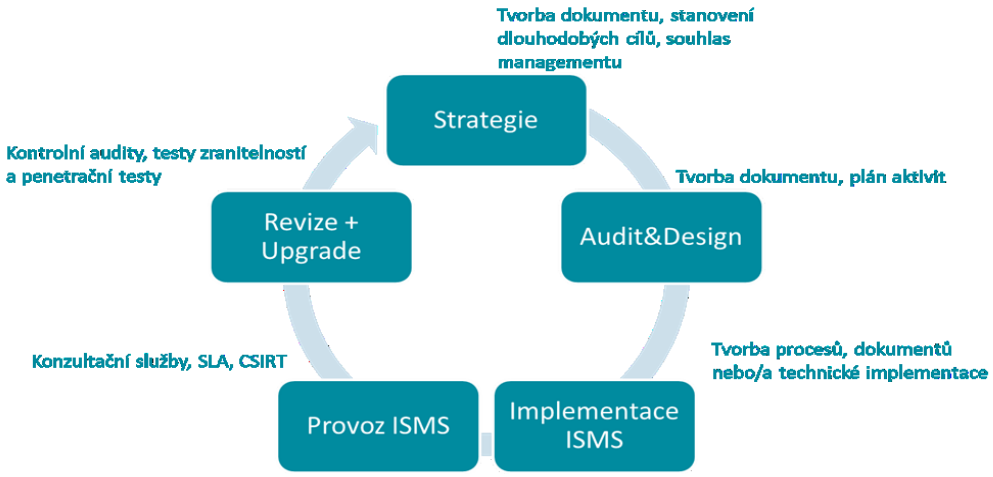
Obrázek 9: ISMS

Aktuálním trendem je usměrňování úrovně bezpečnosti informací z pohledu Evropské Unie – postižení skupiny kritických systémů jako poskytovatelů základních služeb s výraznou regulací a zavedení minimalistické verze ochrany pro všechny státní organizace. ČR již dnes reguluje oblast bezpečnosti informací na základě zákona č. 181/2014 Sb. Evropská Unie dále výrazně reguluje oblast osobních údajů nařízením GDPR, které bude účinné bez ohledu na legislativu členských států od května 2018. Je nutné dát zvýšenou pozornost na všechny parametry, které jsou základem ucelené dokumentace jednotlivých činností. [5]

3.4 Systém řízení bezpečnosti informací

ISMS se skládá z několika prvků, které tvoří jeho jasnou strukturu:

- Bezpečnostní strategie;
- Bezpečnostní audit a návrh;
- Implementace ISMS (organizačních a technických bezpečnostních opatření);
- Funkční dokumentace;
- Zajištění povozu ISMS, jeho kontrola, testování a zlepšování.

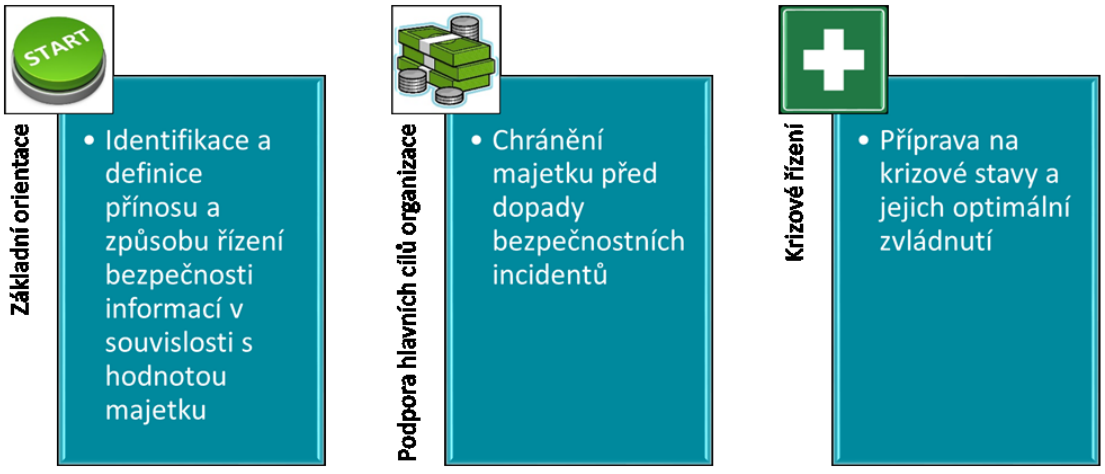


Obrázek 10: Systém řízení bezpečnosti informací

3.5 Bezpečnostní strategie

Bezpečnostní strategií definujeme a dokumentujeme strategické cíle pro předem odsouhlasené období. Vedeme k porozumění bezpečnosti informací všechny klíčové úrovně organizace, včetně nejvyššího managementu. [2]

Plnění jednotlivých strategických cílů popisujeme pomocí plánu úkolů bezpečnostní strategie. Úkoly musí obsahovat jasný popis, termíny splnění a určení odpovědnosti za jeho splnění.



Obrázek 11: Bezpečnostní strategie

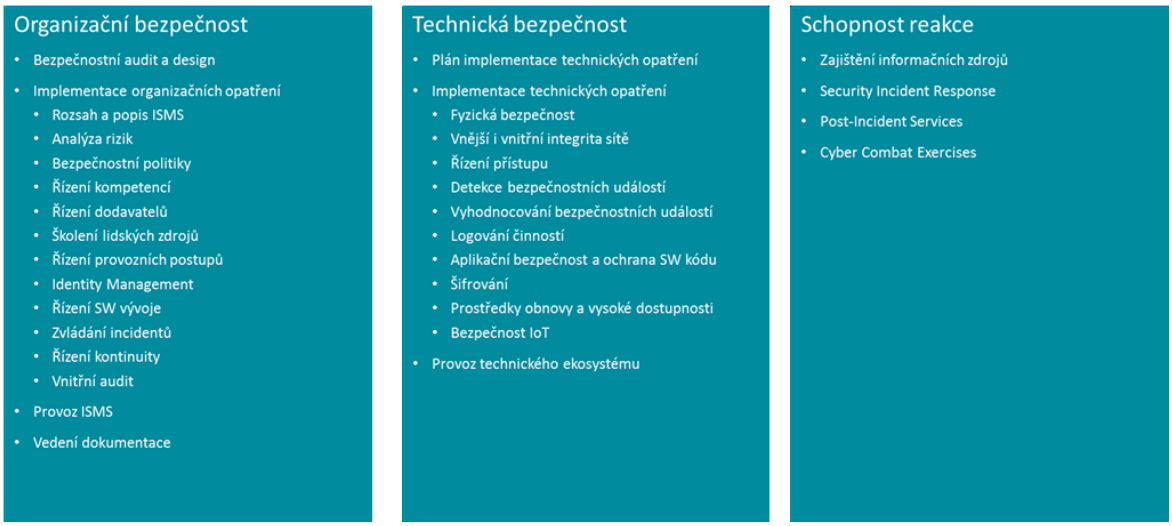
Plnění strategických cílů sledujeme, vyhodnocujeme a případně aktualizujeme.

Bezpečnostní strategií pomáháme nejvyššímu managementu sledovat stav řízení bezpečnosti informací ve vazbě hlavní cíle organizace.

3.6 Bezpečnostní audit a návrh

Základem každé úspěšné činnosti je dobrý plán. Dobré plánování závisí na dobrých informačních zdrojích. Bezpečnostní audit pomáhá určit vstupy pro bezpečnostní design, na jehož výstupech se top management organizace rozhoduje o podobě řízení bezpečnosti informací.

Implementaci ISMS musí předcházet posouzení využitelnosti všech zdrojů ze stávajícího prostředí (audit) a podrobný plán, jak bude implementace ISMS probíhat (návrh) – assesment. Ekonomickým cílem auditu i návrhu je úspora zdrojů nutných k vybudování odolného prostředí ICT. Technickým cílem auditu zjištění skutečného stavu a podle jeho úrovně nastavení dalšího vývoje. Audit musí být proveden podle předem dohodnuté metodiky. [2]



Obrázek 12: Assessment

Provedení auditu závisí na zvolené metodice. Podrobný audit je třeba vždy na začátku před implementací ISMS a v případě velkých pochybností o kvalitě ISMS je potřeba podrobný audit opakovat. Audit zasahuje celou řadu organizačních složek organizace:

- ICT oddělení;
- Oddělení informační bezpečnosti (existuje-li);
- Oddělení fyzické bezpečnosti;
- Právní oddělení;
- Investiční oddělení (Procurement);
- Personální oddělení (HR);
- Top management, úsekoví řídicí pracovníci, garanti aktiv.

Výstupem z auditu a návrhu je soubor dokumentů:

- Podrobné výsledky měření auditu pro bezpečnostní role;
- Souhrnné výsledky auditu s vazbou na podrobné výsledky;
- Auditní zpráva – text shrnující výsledky auditu doplněná o část návrhu;
- Prezentace pro technickou skupinu podílející se na auditu a návrhu;
- Prezentace pro top management.

Posuzujeme využitelnost všech zdrojů ze stávajícího prostředí (bezpečnostní audit) a podrobně plánujeme, jak bude implementace ISMS probíhat (bezpečnostní návrh). [2]

Stanovujeme si 2 základní cíle:

1. Šetříme zdroje nutných k vybudování odolného prostředí ICT (ekonomický cíl);
2. Zjišťujeme skutečný stav a podle jeho úrovně doporučujeme další rozvoj (technický cíl).

3.7 Implementace ISMS

ISMS potlačuje chaotické jednání při ochraně informačních aktiv a přináší systematický postup. Pro nastavení ISMS platí, že je vhodné použít jako etalon některou z norem (ISO/IEC 27001:2013 nebo zákon č. 181/2014 Sb. nebo speciální normy pro specifické oblasti, např. vojenská oblast). Implementace ISMS probíhá podle bezpečnostního návrhu. Základem implementace ISMS je realizace bezpečnostních opatření: [6]

- Organizační opatření – soubor procesů a dokumentace
- Technická opatření – soubor technických nástrojů

3.7.1 Organizační opatření

Organizačním opatřením se rozumí ovlivnění procesů, dokumentace stavu, která zároveň obsahuje možné budoucí scénáře incidentů. Procesy se rozumí zejména:

- Řízení rizik;
- Bezpečnostní politiky;
- Nastavení kompetencí a odpovědnosti rolí;
- Řízení dodavatelů;
- Řízení lidských zdrojů;
- Řízení dokumentace;
- Identity Management;
- Zvládání bezpečnostních incidentů;
- Plán kontinuity;
- Posouzení externích i interních vlivů.

3.7.2 Technická opatření

Návrh, implementace, správa a podpora technických bezpečnostních opatření musí vždy vycházet z organizačních opatření. Návrh technického opatření musí respektovat cíle vytyčené organizačními opatřeními a musí stanovit měřitelné hodnoty přínosu. Kvalita implementace, správy a podpory je závislá jednak na kvalitě lidských zdrojů a know-how, jednak na stavu ISMS, tedy v obou případech na organizačních opatřeních, které mají tyto oblasti řešit. Technická opatření tvoří ekosystém technických automatizovaných nástrojů, mezi které patří zejména:

- Prostředky fyzické bezpečnosti;
- Ochrana integrity sítě;
- Řízení autentizačních údajů a přístupu;
- Ochrana proti škodlivému kódu;
- Detekce bezpečnostních událostí;
- Sběr událostí, archivace a vyhodnocování bezpečnostních událostí a incidentů;
- Ochrana SW kódu, řízení kryptografické ochrany;
- Implementace technických prostředků pro naplnění plánu kontinuity.

Pro limity výběru technických nástrojů slouží Katalog bezpečnostních technických opatření, který je vhodné vytvořit za účelem ujasnění si schopnosti vzájemné integrace do technického ekosystému. [17]

3.8 Dokumentace

Funkční dokumentace spočívá v rozumném nakládání a prezentaci dokumentovaných informací, což představuje řešení 2 zásadních problémů:

- Rozumná úroveň hloubky informací pro roli, která bude dokumentaci číst, za předpokladu velmi komplexního postižení všech možných situací bezpečnosti informací;
- Rozumný formát pro snadnou aktualizaci dokumentace.

3.9 Zajištění povozu ISMS, jeho kontrola, testování a zlepšování

Po implementaci ISMS musí proběhnout přezkoumání odolnosti prostředí kvůli ověření funkčnosti bezpečnosti. To představuje méně podrobnou variantu auditu, kdy se používají například vzorkovací technicky. Po přezkoumání je možné libovolně přistoupit k certifikaci celého ISMS nezávislou stranou. [17]

Obrázek 13: Poměr počtu incidentů a významu škod

Obrazem kvality ISMS jsou bezpečnostní incidenty, zejména úroveň jejich kategorizace. Při implementaci procesů a technologií ISMS se buduje prostředí schopné si s bezpečnostními incidenty poradit bez následků, nebo jejich dopad minimalizovat. Zvládání bezpečnostních incidentů by mělo být opřeno o 4 hlavní pilíře: [17]

- Prevence – zajištění kvalitních informačních zdrojů pro preventivní zásahy do ISMS před hrozbou bezpečnostního incidentu nebo zranitelností ISMS;
- Reakce – zajištění činnosti s přímo probíhajícím bezpečnostním incidentem;
- Prošetření incidentu – prošetření bezpečnostního incidentu po zvládnutí škod vzniklých jeho působením a návrh nápravných opatření;
- Ověřování odolnosti ISMS – testy zranitelností, penetrační testy, vzdělávání a cyber combat cvičení IT administrátorů, vlastníků privilegovaných účtů, operátorů dohledových pracovišť SOC a členů týmů CSIRT;

3.10 Kompetence a odpovědnost lidí

Člověk je rozhodující prvek odolnosti ISMS. Každá role musí znát možné důsledky svého chování.

Obrázek 14: Rovnice ochrany informací

Znalost důsledků nebezpečného chování předchází incidentům ve všech úrovní organizace:

- Potřeba rozšířit a ověřit vědomosti bezpečnostních rolí odpovědných za řízení ISMS;
- Trénink bezpečnostního povědomí privilegovaných rolí a ICT administrátorů;
- Řízení bezpečnostního povědomí uživatelů.

Kvalitní ochrana informaci umožňuje plnění primární cílů každé organizace. Z pohledu digitalizace globálního světa, kdy jsou informace přístupné přes komunikační systém odkudkoliv, není možné bezpečnost těchto informací podceňovat. [6]

II. PRAKTICKÁ ČÁST

4 REALIZACE PROJEKTU ZA POUŽITÍ METODIKY COBIT

4.1 Popis prostředí organizace a řešený projekt

V praktické části své práce řeším nastavení IT prostředí v rámci organizace, která je zaměřena na aktivity a procesy nesouvisející přímo s IT technologiemi a IT řešeními.

Dalším specifickým rysem je skutečnost, že se jedná o subjekt státní správy a to definuje některá omezení a aspekty ve srovnání s běžnou komerční organizací. Jedná se především o velmi striktní regulaci a požadavky o naplnění legislativního rámce, minimální tlak na inovace a tlak na financování pouze zákonem definované funkcionality.

4.1.1 Vzorový případ: Zpoplatnění provozu na pozemní komunikaci

V tomto konkrétním případě, který je v práci řešen, realizuje organizace zavedení zcela nového systému Zpoplatnění provozu na pozemní komunikaci pro vozidla nepřesahující 3,5tuny. Za tímto účelem definuje potřebné procesy, organizaci a informační systém tak, aby v maximální míře naplnila dva základní cíle projektu:

I. **Spolehlivý a efektivní výběr poplatku**

Vysoce dostupný, elektronický nástroj pro zajištění platby a evidence vozidel s provedenou úhradou, dále potom kontrolu všech výjimek a slev na jejich oprávněnost vazbou na existující zdroje informací (tj. registry a evidence státu).

II. **Podporu kontroly uhrazeného poplatku vykonávanou na komunikacích**

Poskytnutí nástroje pro rychlé a automatizované ověření, zda konkrétní vozidlo (podle jeho Registrační Značky) má uhrazen poplatek.

4.2 Další postup řešení

S ohledem na uvedené specifické rysy organizace a priority, uvedené v tomto odstavci, je dále zpracováno rozdělení jednotlivých oblastí činností a procesů do 3 základních skupin:

- Činnosti **klíčové (zelená)**
    - přímo souvisí se statutem a posláním organizace

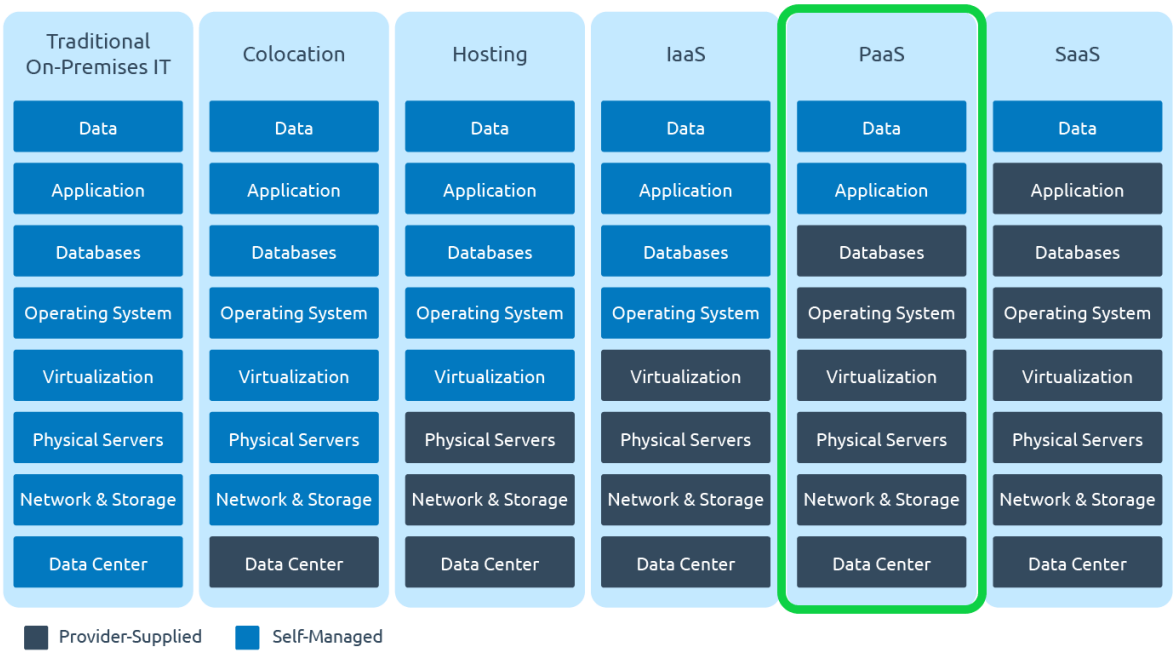
  - jsou kritické pro kontinuitu provozu systému
  - předáním výkonu této činnosti se snižuje kontrola nad procesem a plněním zákonné povinnosti
  - obsahují specifické know-how spojené s projektem
  - **budou vykonávány přímo organizací**
- Činnosti **důležité (bílá)**
  - Jsou podpůrné pro naplnění procesu provozu systému
  - nesouvisí přímo se statutem a posláním organizace
  - jedná se o standardně dostupné činnosti, které jsou poskytovány specializovanými společnostmi
  - je možné změnit poskytovatele s ohledem na potřebu kvality a efektivity
  - **budou vykonávány externím poskytovatelem služby**
- Činnosti **nepodstatné (červená)**
  - nejsou nezbytně nutné pro naplnění procesu provozu systému
  - je možné jejich potřebu zvážit na základě první fáze provozu systému a následně, v případě potřeby, doplnit
  - **v první fázi projektu a nastavení organizace nebudou realizovány**

4.3 Mapování – strategie organizace do modelu

Pro nastavení IT prostředí v rámci organizace můžeme využít různé koncepty definované jako Anything as a Service (XaaS). Mezi základní patří Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), fyzická infrastruktura sdílená poskytovatelem služby (Hosting), kompletní vlastní zařízení umístěné v pronajatých objektech, nejčastěji u poskytovatelů datové konektivity (Collocation), a poslední, kdy celé/kompletní řešení je provozováno v prostorách zákazníka (On-Premises IT).

Následující obrázek číslo 15 níže ukazuje možné alternativy rozdělení kompetencí při realizaci projektu z pohledu zdrojů, vlastní (modrá) a externího poskytovatele (černá). S ohledem na rozhodnutí organizace, věnovat se pouze vlastím agendám, vychází nejlépe model PaaS . V modelu PaaS udržuje organizace plnou kontrolu nad svými daty a také aplikací specifickou pro její činnost. Ostatní, nespecifické, činnosti ponechává na externím poskytovateli služby.

Samostatná kapitola je mapování na bezpečnostní standardy a politiky. Jak už jsem zmiňoval výše, hodnota bezpečnosti vždy závisí na hodnotě služeb ICT, respektive na ztrátách vyplývajících z důsledků bezpečnostních incidentů. Porozumění této závislosti umožňuje nastavit prostředí pro provoz IT efektivně. Řízení bezpečnosti informací je tak nedílnou součástí služeb IT. Komplexní správa IT a kvalitní ochrana informaci tvoří páteř moderní organizace, kde progresivní hráči dokážou efektivně využívat příležitosti, které elektronická komunikace, jako nedílná nadstavba tržního prostředí, nabízí.



Obrázek 15: Platform as a service [18]

4.3.1 Základní mapování

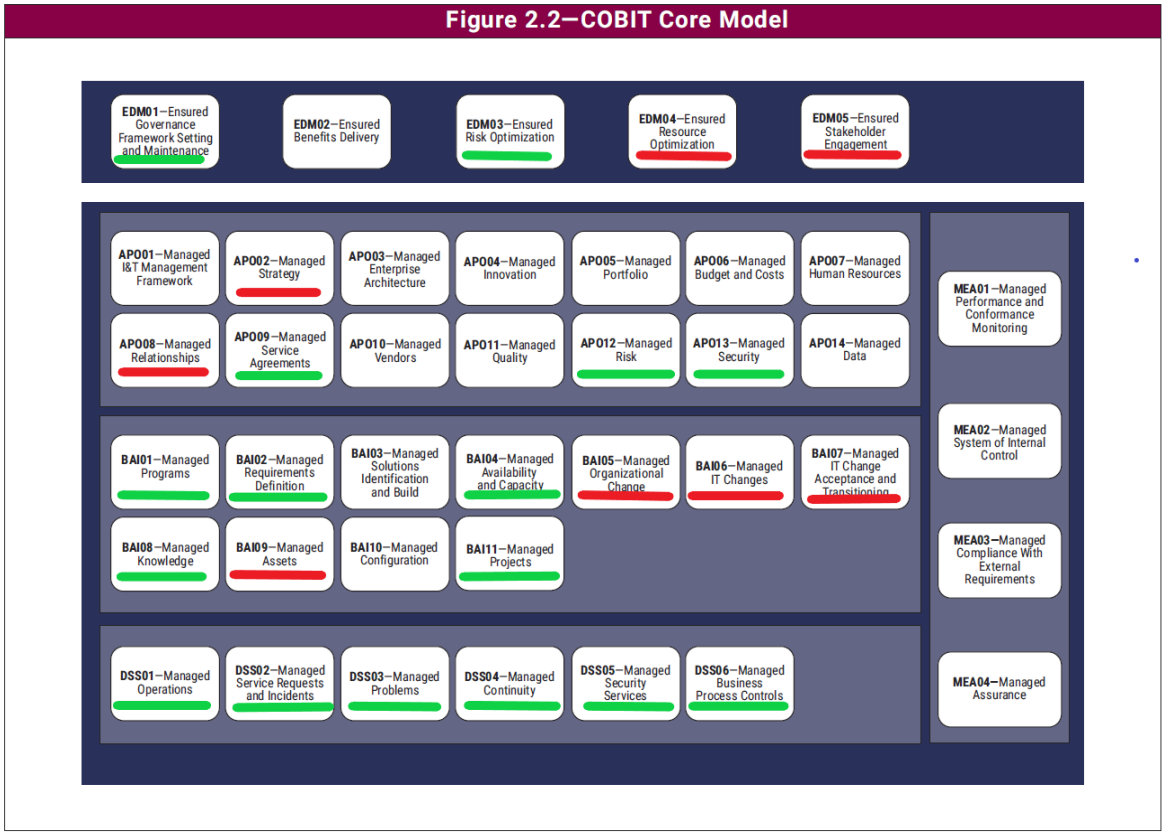
Celkový pohled na Core model metodiky COBIT je využit k základnímu rozčlenění odpovědností za jednotlivé části. Legendu ke zpracování následujících schémat a tabulek demonstruje tabulka 1 a rozdělena barevně, dle výběru aktivit.

Tabulka 1: Vzor sady otázek …[13]

		Explanation	**Action**
		činnost kritická, bude v projektu zajištěno přímo organizací	
		činnost potřebná, možno zajistit externě	
		činnost nepotřebná pro stávající fázi projektu	

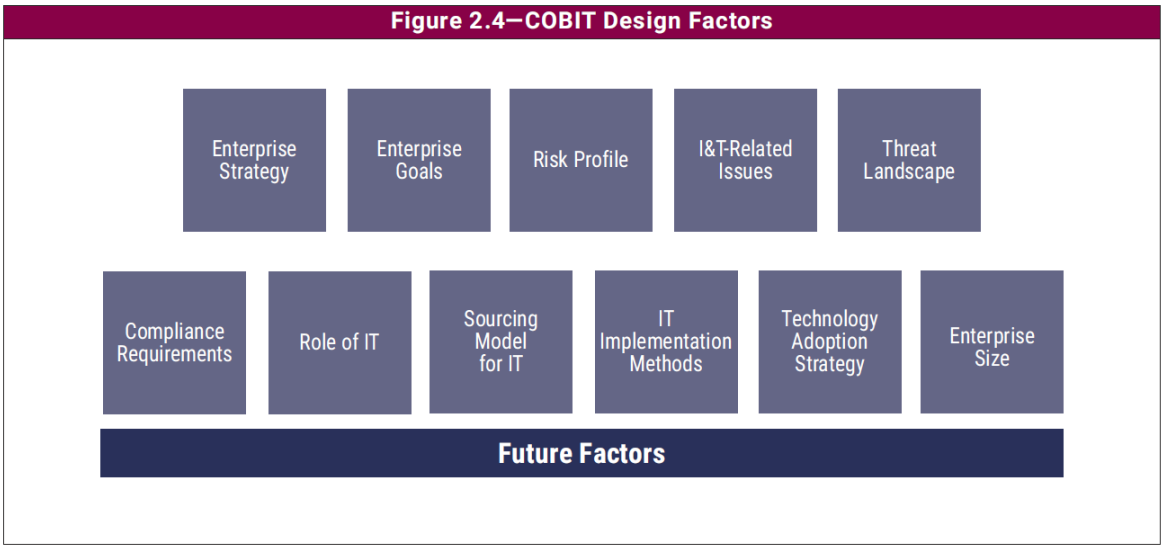
Základní rozčlenění odpovědnosti je jedna z metod, kde přiřadíme odpovědnosti jednotlivých činností nebo osob ke konkrétnímu úkolu. V úvodu si musíme vydefinovat jednotlivé oblasti a k nim přiřadit nějaký měřitelný parametr, který dokážeme sledovat a progres nebo stagnaci zaznamenat a v časové přímce vyhodnotit. Pro definovaný případ jsem využil vzorové sady otázek z COBIT rámce, který je pro mou práci signifikantní, jenž můžeme vidět na obrázku č.16. Pro vyhodnocování je možné využívat různé nástroje, jako Matice odpovědností, RACI matice, nebo kompetenční model. Pro zpracování je důležité stanovit hloubku, resp. úrovně, které v průběhu měření chceme zkoumat a jak detailního výsledku chceme dosáhnout.

Obrázek 16: COBIT Core Model [13]



Níže popsané aktivity jsou hlavní silou, která řídí nastavení ideální konstrukce IT prostředí v organizaci. Jednotlivé faktory z obrázku 17 mohou ovlivnit návrh systému řízení podniku a tím rozhodnout o úspěchu nebo neúspěchu a zmapovat potenciální dopad řešení na systém řízení. COBIT 2019 pracuje s níže uvedenými prvky a je možné využít libovolnou kombinaci.

Obrázek 17: Faktory ovlivňující návrh systému řešení [13]



4.3.2 Detailní mapování

Podniková strategie - Podniky mohou mít různé strategie, které lze vyjádřit jako jeden nebo více archetypů znázorněných v tabulce 2, která je barevně doplněna. Organizace mají obvykle primární strategii a nanejvýš jednu sekundární strategii.

Tabulka 2: Enterprise Strategy Design Factor [13]

Enterprise Strategy Design Factor			
	Strategy Archetype	**Explanation**	**Action**
	Growth/Acquisition	Portfolio of competitive products and services	
	Innovation/Differentiation	Managed business risk	
	Cost Leadership	Compliance with external laws and regulations	
	Client Service/Stability	Quality of financial information	

Podnikové cíle podporující podnikovou strategii - Podniková strategie je realizována dosažením (souboru) podnikových cílů z tabulky číslo 3. Tyto cíle jsou součástí COBIT rámce a jsou definovány ve strukturované podobě ve skóre kartách (BSC) a zahrnují následující. Tabulka rozdělena dle barev aktivit.

Tabulka 3: Podnikové cíle [13]

Enterprise Goals Design Factor			
Reference	**Balanced Scorecard (BSC) Dimension**	**Enterprise Goal**	**Action**
EG01	Financial	Portfolio of competitive products and services	
EG02	Financial	Managed business risk	
EG03	Financial	Compliance with external laws and regulations	
EG04	Financial	Quality of financial information	
EG05	Customer	Customer-oriented service culture	
EG06	Customer	Business-service continuity and availability	
EG07	Customer	Quality of management information	
EG08	Internal	Optimization of internal business process functionality	
EG09	Internal	Optimization of business process costs	
EG10	Internal	Staff skills, motivation and productivity	
EG11	Internal	Compliance with internal policies	
EG12	Growth	Managed digital transformation programs	
EG13	Growth	Product and business innovation	

Profil rizik podniku a aktuální problémy ve vztahu k IT — Rizikový profil identifikuje druh rizika, kterému je podnik v současné době vystaven, a poukazuje na oblasti, kde rizika překračují bezpečnou/akceptovatelnou mez. Vyznačené rizikové kategorie jsou uvedené na tabulce číslo 4.

Tabulka 4: Profil rizik podniku [13]

Risk Profile Design Factor (IT Risk Categories)			
Reference		**Risk Category**	**Action**
1		IT investment decision making, portfolio definition and maintenance	
2		Program and projects lifecycle management	
3		IT cost and oversight	
4		IT expertise, skills and behavior	
5		Enterprise/IT architecture	
6		IT operational infrastructure incidents	
7		Unauthorized actions	
8		Software adoption/usage problems	
9		Hardware incidents	
10		Software failures	
11		Logical attacks (hacking, malware, etc.)	
12		Third party/supplier incidents	
13		Noncompliance	
14		Geopolitical issues	
15		Industrial action	
16		Acts of nature	
17		Technology-based innovation	
18		Environmental	
19		Data and information management	

Problémy související s IT – pro výběr vhodné techniky pro posouzení rizik IT v podniku je třeba vzít v úvahu více faktorů a zaměřit se na ty klíčové, které mohou způsobit největší problémy a ty začít řešit. Vzor nejpoužívanějších otázek shrnuje tabulka číslo 5.

Tabulka 5: Problémy související s IT [13]

IT-Related Issues Design Factor			
Reference		Description	Action
A		Frustration between different IT entities across the organization because of a perception of low contribution to business value	
B		Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business value	
C		Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT	
D		Service delivery problems by the IT outsourcer(s)	
E		Failures to meet IT-related regulatory or contractual requirements	
F		Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems	
G		Substantial hidden and rogue IT spending, that is, IT spending by user departments outside the control of the normal IT investment decision mechanisms and approved budgets	
H		Duplications or overlaps between various initiatives, or other forms of wasted resources	
I		Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction	
J		IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget	
K		Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT	
L		Complex IT operating model and/or unclear decision mechanisms for IT-related decisions	
M		Excessively high cost of IT	
N		Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems	
O		Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages	
P		Regular issues with data quality and integration of data across various sources	
Q		High level of end-user computing, creating (among other problems) a lack of oversight and quality control over the applications that are being developed and put in operation	
R		Business departments implementing their own information solutions with little or no involvement of the enterprise IT department16	
S		Ignorance of and/or noncompliance with privacy regulations	
T		Inability to exploit new technologies or innovate using I&T	

Přehled hrozeb – Míra rizika prostředí, které mohou působit na podnik, lze v základním rozdělení klasifikovat podle tabulky č. 6. Vzhledem k lokaci technologií a jejich primárního využití hodnotím stav jako normální.

Tabulka 6: Míra rizika prostředí [13]

Threat Landscape Design Factor			
	Threat Landscape	**Explanation**	**Action**
	Normal	The enterprise is operating under what are considered normal threat levels.	
	High	Due to its geopolitical situation, industry sector or particular profile, the enterprise is operating in a high-threat environment.	

Požadavky na shodu – dodržování požadavků na shodu jsou v této úloze velmi striktní, jedná se o státní subjekt, kde část systémů je vedena jako kritická infrastruktura. Příklad požadavků na shodu demonstruje tabulka číslo 7.

Tabulka 7: Příklad požadavků na shodu [13]

Compliance Requirements Design Factor			
	Regulatory Environment	**Explanation**	**Action**
	Low compliance requirements	The enterprise is subject to a minimal set of regular compliance requirements that are lower than average.	
	Normal compliance requirements	The enterprise is subject to a set of regular compliance requirements that are common across different industries.	
	High compliance requirements	The enterprise is subject to higher-than-average compliance requirements, most often related to industry sector or geopolitical conditions.	

Role IT jsou definovány jejich úlohami. Úloha IT je klasifikována a dopodrobna rozebrána v tabulce č. 8. IT je kritickou infrastrukturou a rozhodující složkou, která ovlivňuje jak chod businessu, tak i inovace služeb zákazníkům a celkový chod firmy. Role IT ve firmě se zdá být motorem businesových procesů a dalších aspektů, jež nejsou na první pohled viditelné.

Tabulka 8: Role IT [13]

Role of IT Design Factor			
	Role of IT	**Explanation**	**Action**
	Support	IT is not crucial for the running and continuity of the business process and services, nor for their innovation.	
	Factory	When IT fails, there is an immediate impact on the running and continuity of the business processes and services. However, IT is not seen as a driver for innovating business processes and services.	
	Turnaround	IT is seen as a driver for innovating business processes and services. At this moment, however, there is not a critical dependency on IT for the current running and continuity of the business processes and services.	
	Strategic	IT is critical for both running and innovating the organization's business processes and services.	

Model pro sdílení zdrojů v IT - Nastavení formy sdílení služeb pro IT v organizaci vychází ze strategického záměru využít službu Platforma as a Service (PaaS).

Tabulka 9: Možnosti využití zdrojů v IT [13]

Sourcing Model for IT Design Factor			
	Sourcing Model	**Explanation**	**Action**
	Outsourcing	The enterprise calls upon the services of a third party to provide IT services.	
	Cloud	The enterprise maximizes the use of the cloud for providing IT services to its users.	
	Insourced	The enterprise provides for its own IT staff and services.	
	Hybrid	A mixed model is applied, combining the other three models in varying degrees.	

Metody implementace v IT - Metody, které podnik používá, lze klasifikovat tak, jak je uvedeno v tabulce č.10. Hlavní rozdělení metod dělíme na tradiční a hybridní, které jsou popsány v tabulce pro lepší pochopení

Tabulka 10: Metody implementace v IT [13]

IT Implementation Methods Design Factor			
	IT Implementation Method	Explanation	Action
	Agile	The enterprise uses Agile development working methods for its software development.	
	DevOps	The enterprise uses DevOps working methods for software building, deployment and operations.	
	Traditional	The enterprise uses a more classic approach to software development (waterfall) and separates software development from operations.	
	Hybrid	The enterprise uses a mix of traditional and modern IT implementation, often referred to as “bimodal IT.”	

Strategie zavádění technologie - Strategii přijetí technologie lze klasifikovat, jak je uvedeno v tabulce číslo 11. Strategie se dělí dle typu/rychlosti klienta na 3 části.

Tabulka 11: Strategie zavádění technologie do organizace [13]

Technology Adoption Strategy Design Factor			
	Technology Adoption Strategy	Explanation	Action
	First mover	The enterprise generally adopts new technologies as early as possible and tries to gain first-mover advantage.	
	Follower	The enterprise typically waits for new technologies to become mainstream and proven before adopting them.	
	Slow adopter	The enterprise is very late with adoption of new technologies.	

Velikost podniku – Podniky dělíme do různých kategorií dle velikosti a počtu zaměstnanců. Pro návrh systému řízení podniku jsou identifikovány dvě kategorie, jak je znázorněno v tabulce číslo 12.

Tabulka 12: Segmentace dle velikosti podniku [13]

Enterprise Size Design Factor			
	Enterprise Size	Explanation	Action
	Large enterprise (Default)	Enterprise with more than 250 full-time employees (FTEs)	
	Small and medium enterprise	Enterprise with 50 to 250 FTEs	

4.4 Implementace do organizace

Na základě strategie z kapitoly 4.2 a mapování v kapitole 4.3 vycházíme při definici požadavků na vlastní realizační tým a na zadání pro externího poskytovatele. Vzhledem k důležitosti celého systému by součástí projektu měla být realizace bezpečnostního auditu.

4.4.1 Bezpečnostní audit

Významnou metodikou v ČR je zákon o kybernetické bezpečnosti [21], kterým je v současné době regulována celá řada organizací. Protože existuje potenciálně silné riziko budoucí regulace zadavatele tímto zákonem, bude součástí navrhovaného řešení bezpečnostní audit.

Metodika se zakládá na zjišťování stavu bezpečnostních opatření proti požadavkům jednotlivých § nové vyhlášky. [22] V rámci těchto tematických okruhů bude sledována sada dílčích hledisek pro plný soulad se zněním ZKB vč. vyhlášky.

Celé vypracování bezpečnostního auditu lze rozdělit do tří základních fází:

V první fázi probíhá rekognoskace prostředí zadavatele, jejímž cílem je získání potřebných informací pro zpracování bezpečnostního auditu. V této fázi probíhá intenzivní spolupráce zadavatele s dodavatelem.

Ve druhé fázi jsou vytěžená data porovnávána z požadavky ZKB a dodavatel identifikuje a hodnotí zjištěné rozdíly.

Ve třetí fázi dodavatel vytváří výstupní dokumentaci a seznamuje s výsledky zadavatele.

Během auditu je použitá vzorkovací metodika při určení rozsahu auditu. Obsahově audit postihuje maximální možnou hloubku pro zjištění správného a úplného stavu odolnosti prostředí informační bezpečnosti zadavatele. Zkoumá kvalitu stávajícího systému řízení bezpečnosti informací (dále jen „ISMS“) ve vzájemné vazbě hodnoty aktiv, hodnoty dopadů rizik a incidentů a hodnoty bezpečnostních opatření.

Orientační harmonogram projektu:

Zadavatel požaduje po dodavateli vedení implementace ISMS dle normy ISO/IEC 27001:2013 v prostředí zákazníka, přípravu na certifikační audit dle ISO/IEC 27001:2013 a podporu při certifikačním auditu ISO/IEC 27001:2013.

4.4.2 Postup plnění

Dodavatel je povinen při implementaci ISMS respektovat normu ISO/IEC 27001:2013. Dále si dodavatel musí být vědom, že některé systémy spravované zadavatelem spadají pod regulaci ZKB a přizpůsobit veškerou činnost výstupy v souladu s tímto zákonem. [21]

Postup plnění charakterizuje následující plán implementace:

- Kontext organizace
- Vůdčí role a závazek
- Plánování
- Podpora
- Provozování
- Hodnocení výkonnosti
- Zlepšování

4.4.3 Požadavky na vlastní tým

Struktura týmu a role. Vhodné je spojení vedoucího týmu s vedením projektu. Toto spojení je výhodné z pohledu sloučení odpovědnosti za výsledek práce týmu, vedení týmu a s tím spojenou možnost definice hodnotících kritérií, rozvoje a odměňování jednotlivých pracovníků. Toto vyplývá i ze [21].

Definovaný tým musí zajistit kompletní pokrytí aktivit a činností dle výše uvedených požadavkům dle tabulek číslo 2-12.

Pro každou roli v týmu definujeme

- Aktuální znalosti pracovníka
    - Předpoklady v oblasti vzdělání a znalostí
    - Předpoklady v oblasti zkušeností – osobní reference
    - Osobnostní předpoklady – očekávání růstu a dalšího vzdělávání
- Měření a hodnotící kritéria
    - Vazba na výsledky – tzv. „tvrdé“ metriky (SLA pro roli)

  - Spolupráce v týmu, osobnostní rozvoj – tzv. „soft“ metriky (subjektivní ohodnoceni)
  - Vliv jednotlivých metrik na ohodnocení
- Další rozvoj
  - Možnost karierního růstu
  - Plán školení a certifikací (senior vs. junior, Lead, apod.)

Na závěr definice týmu a jednotlivých rolí je nutné provedení kontroly, že veškeré definované požadavky jsou pokryty právě jednou rolí v týmu. Požadavek naplňuje zákonné požadavky a doplňuje další potřebné role k nim. [21] V případě, že bude požadavek naplňován dvěma a více rolemi, musí být definována jedna konkrétní – vedoucí role pro zabránění konfliktů a jednoznačnou odpovědnost / kompetence.

Příkladem technických požadavků na jednotlivé role je následující popis:

- Manažer kybernetické bezpečnosti
  - Minimálně 5 let praxe v oblasti metodického řízení systémů řízení bezpečnostních informaci
  - Zkušenosti s návrhem a implementací bezpečnostních opatření
  - Znalost technických norem zabývající se problematikou bezpečnosti informací

- Architekt kybernetické bezpečností
  - Minimálně 3 let praxe v oblasti metodického řízení systémů řízení bezpečnostních informaci
  - Zkušenosti s návrhem a implementací bezpečnostní architektury
  - Odborná znalost a orientace v informačních a komunikačních technologiích

- Projektový manažer:
  - ukončené vysokoškolské vzdělání;
  - minimálně 5 let praxe v oblasti řízení projektů implementace informačních systémů;
  - zkušenost s pozicí projektového manažera nebo obdobné roli alespoň na jakémkoliv 1 projektu, který naplní všechny znaky (předmět, počet uživatelů

a finanční objem) „významné dodávky“ v oblasti vytvoření/dodávky informačních systémů dle ustanovení **ad 1) níže**;
    - certifikace PRINCE 2, IPMA nebo obdobná.

- Architekt informačního systému:
    - ukončené vysokoškolské vzdělání;
    - minimálně 5 let praxe v oblasti činnosti architekta informačních systémů, kterou se rozumí zejména návrhy architektury řešení, návrh způsobu integrace řešení s okolními systémy apod.;
    - zkušenost s pozicí architekta informačního systému na jakémkoliv 1 projektu, který naplňuje všechny znaky (předmět, počet uživatelů a finanční objem) „významné dodávky“ v oblasti vytvoření/dodávky informačních systémů dle ustanovení **ad 1) níže**;
- Analytik:
    - ukončené vysokoškolské vzdělání;
    - minimálně 5 let praxe v oblasti analýz agend zahrnující správní a finanční procesy;
    - zkušenost s alespoň jakýmkoliv 1 projektem, který naplňuje všechny znaky (předmět, počet uživatelů a finanční objem) „významné dodávky“ v oblasti vytvoření/dodávky informačních systémů dle ustanovení **ad 1) níže**;
- Databázový specialista:
    - minimálně 5 let praxe v oblasti činnosti databázového specialisty, kterou se rozumí instalace, konfigurace a údržba databází informačních systémů;
    - minimálně 3 roky praxe v oblasti činnosti datových analýz a integrací, DWH, OLAP;
    - zkušenost s alespoň jakýmkoliv 1 projektem, který naplňuje všechny znaky (předmět, počet uživatelů a finanční objem) „významné dodávky“ v oblasti vytvoření/dodávky informačních systémů dle ustanovení **ad 1)** nebo v oblasti uživatelské podpory a provozu informačních systémů **ad 2) níže**.
- Migrační specialista:
    - ukončené vysokoškolské vzdělání;

  - minimálně 5 let praxe v oblasti metodického, organizačního a věcného zajištění migrace dat mezi informačními systémy;
  - zkušenost s alespoň jakýmkoliv 1 projektem, který naplňuje všechny znaky (předmět, počet uživatelů a finanční objem) „významné dodávky“ v oblasti vytvoření/dodávky informačních systémů dle ustanovení **ad 1) níže**.

- Manažer servisní podpory
  - ukončené vysokoškolské vzdělání;
  - minimálně 3 roky praxe v oblasti poskytování IT podpory a souvisejících služeb;
  - zkušenost s pozicí manažera servisní podpory na alespoň i 1 projektu, který naplňuje všechny znaky (předmět, počet uživatelů a finanční objem) „významné dodávky (služby)“ v oblasti podpory a provozu informačních systémů dle ustanovení **ad 2) níže**.
  - Požadavky na externího dodavatele

4.4.4 Požadavky na externího dodavatele PaaS

Definici požadavků na externího dodavatele lze shrnout jako soubor technických kvalifikačních předpokladů. Požadavky dělíme do dvou oblastí, funkční požadavky a nefunkční požadavky. Funkční požadavky jsou definovány především monitorováním výkonu poskytované služby (SLA), které je možné zastřešit řízením úrovně služeb (SLM), kde jsou vyjednány obecně dohody o úrovni služeb se zákazníky a navrhované služby jsou v souladu dohodnutými cíli na úrovni služeb. Nefunkční požadavky definují vlastnosti sytému jako celku a musí být ověřitelné. Pro výběr externího dodavatele jsou nefunkční požadavky často důležitější, protože jsou zárukou pro dlouhodobou stabilní a kvalitní práci. Implementace procesů ISO 20000 a ISO 27000 vypovídají o potřebě udržitelného rozvoje a dlouhodobé firemní strategii na udržení standardu kvality služeb. Stejně tak důležité jsou certifikace dodavatele, nebo osobní certifikace zaměstnanců. Další důležitý parametr je pozitivní reference na provozování Významného informačního systému veřejné správky.

Příkladem pro prokázání kvalifikačního předpokladu do projektu, kde musí předpokládaný externí dodavatel doložit níže uvedené parametry, kde v posledních 3 letech realizoval. Příklad je veden z praxe a tyto předpoklady byly požadovány v rámci výběrového řízeni.

Ad 1)

- významné dodávky v oblasti vytvoření/dodávky informačních systémů,
    - Zadavatel v této souvislosti stanoví, že za významné dodávky v oblasti vytvoření/dodávky informačních systémů se pro účely prokázání splnění kvalifikace v tomto zadávacím řízení považují dodávky v oblasti vytvoření/dodávek informačních systémů zpracovávajících agendy zahrnující správní a finanční procesy v součtu minimálně pro 10 tis. aktivních klientů (klientů, u nichž jsou reálně prováděny předmětné správní a finanční procesy), pokud předmětem každé z těchto významných dodávek byla komplexní dodávka informačního systému (tj. analýza, návrh, realizace, testování a uvedení do provozu). Správními a finančními procesy se pro účely vymezení pojmu významných dodávek rozumí zejména správa klientského portfolia, zpracování a vyhodnocení procesů žádostí klientů.
    - Za vytvoření/dodávku informačního systému ve výše uvedeném smyslu se považuje i významný rozvoj již implementovaného informačního systému, pokud výsledkem takového rozvoje je významné rozšíření původních funkcionalit implementovaného informačního systému a v rámci významného rozvoje byla provedena analýza, návrh, realizace, testování a uvedení do provozu takto nově vytvořených funkcionalit.
    - Finanční objem všech významných dodávek v oblasti dodávky informačních systémů (ad 1) musí celkově dosáhnout v posledních 3 letech minimálně 150 mil. Kč bez DPH.
- Pro vyloučení pochybností zadavatel uvádí, že poskytnutí významných dodávek v oblasti vytvoření/dodávky informačních systémů může dodavatel prokázat jednou či více dodávkami, pokud:
    - veškeré tyto dodávky budou svým předmětem spadat do významných dodávek požadovaných zadavatelem (vytvoření/dodávka informačních systémů zpracovávajících agendy zahrnující správní a finanční procesy) a pokud předmětem každé z těchto významných dodávek byla komplexní dodávka informačního systému;

- předmětem těchto dodávek bylo vytvoření/dodávka informačních systémů zpracovávajících agendy zahrnující správní a finanční procesy (zejména evidence, provedení finanční operace) v součtu minimálně 10 tis. aktivních klientů (klientů, u nichž jsou reálně prováděny předmětné správní a finanční procesy), u každé však minimálně 5 tis. aktivních klientů; a současně;
- objem těchto významných dodávek dosáhl v součtu v posledních 3 letech v součtu minimálně 150 mil. Kč bez DPH, u každé však minimálně 50 mil. Kč bez DPH.

Ad 2)

- významné dodávky (služby) v oblasti uživatelské podpory a provozu informačních systémů
  - Zadavatel v této souvislosti stanoví, že za významné dodávky (služby) v oblasti uživatelské podpory a provozu informačních systémů se pro účely prokázání splnění kvalifikace v tomto zadávacím řízení považují dodávky (služby), jejichž předmětem bylo provozování a rozvoj informačních systémů (tj. dodávky (služby) zahrnující zajištění provozu software a jeho rozvoj, řešení incidentů, zajištění maintenance (údržby) a legislativního souladu) zpracovávajících agendy zahrnující správní a finanční procesy (zejména evidence, provedení finanční operace) v součtu minimálně pro 10 tis. aktivních klientů (klientů, u nichž jsou reálně prováděny předmětné správní a finanční procesy), a to po dobu nejméně 12 měsíců.
  - Finanční objem těchto významných dodávek (služeb) v oblasti uživatelské podpory a provozu informačních systémů (ad 2) musí celkově dosáhnout v posledních 3 letech minimálně 50 mil. Kč bez DPH.
  - Pro vyloučení pochybností zadavatel uvádí, že poskytnutí významné dodávky (služby) v oblasti uživatelské podpory a provozu informačních systémů může dodavatel prokázat jednou či více dodávkami (službami), pokud:
  - veškeré tyto dodávky (služby) budou svým předmětem spadat do významných dodávek (služeb) požadovaných zadavatelem (uživatelská podpora a provoz informačních systémů zpracovávajících agendy zahrnující správní a finanční procesy), pokud předmětem každé z těchto významných dodávek

(služeb) bylo zajištění provozu software a jeho rozvoj, řešení incidentů, zajištění maintenance (údržby) a legislativního souladu, a to po dobu nejméně 12 měsíců;

- předmětem těchto dodávek (služeb) byly dodávky (služby) uživatelské podpory a provozu informačních systémů zpracovávajících agendy zahrnující správní a finanční procesy v součtu minimálně pro 10 tis. aktivních klientů (klientů, u nichž jsou reálně prováděny předmětné správní a finanční procesy), u každé však minimálně 5 tis. aktivních klientů; a současně;

5 VZDĚLÁVÁCÍ PLÁN PRO ICT VZDĚLÁVÁNÍ UŽIVATELŮ

Kontinuální periodické vzdělávání zaměstnanců je v oblasti bezpečnosti v souladu s plánem rozvoje bezpečnostního povědomí a plní požadavky vyhlášky. [22] Vzdělávání má zahrnovat tyto oblasti:

- Zasílání zpráv z oblasti obecné uživatelské bezpečnosti o aktuálních hrozbách a zranitelnostech v týdenní periodě
- Vzdělání vedoucích pracovníků a administrátorů zákazníka o aktuálních trendech kybernetické bezpečnosti v rozsahu cca 60 minut v periodě 6 měsíců prezenční formou.
- Vzdělávání vedoucích pracovníků, administrátorů a bezpečnostních rolí o aktuálních trendech kybernetické bezpečnosti v rozsahu cca 60 minut v periodě 3 měsíce prezenční formou.

V rámci programu zvyšování bezpečnostního povědomí (tzv. cybersecurity awareness) nabízí společnost zákazníkům zajištění kontinuálního vzdělávání zaměstnanců v oblasti kybernetické bezpečnosti. Podrobnější popis kurzů je přidán v seznamu příloh.

5.1 Cybersecurity awareness

Zaměstnanci zákazníka procházejí v rámci tohoto programu periodicky komplexním školením zaměřeným na problematiku kybernetické bezpečnosti se zvláštním důrazem na zásady bezpečného chování a interní směrnice dané organizace. Uvedené školení může být doplněno o vzdělávací akce s užším zaměřením, které slouží k připomenutí nejdůležitějších bezpečnostních konceptů a shrnutí vývoje v oblasti kybernetických hrozeb za poslední kvartál. Uvedená školení mohou být realizována různou formou (prezenčně, pomocí webinářů či e-learningu). Aby byly zaměstnanci schopní úspěšně čelit všem aktuálním hrozbám, jsou jim navíc s vybranou periodou (v závislosti na požadavcích zákazníka) zasílány zprávy Security News obsahující shrnutí nejdůležitějších událostí a doporučení pro ochranu před nejnovějšími hrozbami. V případě výskytu zvláště nebezpečné nové hrozby je zaměstnancům mimo tuto periodu navíc zasláno varování s popisem hrozby a doporučením pro její eliminaci.

Popsaný víceúrovňový systém, formulovaný na základě mnohaletých zkušeností v oblasti bezpečnostního vzdělávání uživatelů, zaručuje neustálé zvyšování bezpečnostního povědomí zaměstnanců a poskytuje tak nezbytný základ pro zajištění informační bezpečnosti v rámci organizace.

Pro organizace regulované zákonem č. 181/2014 Sb. (zákon o kybernetické bezpečnosti) je takový systém zvyšování bezpečnostního povědomí vyhovující povinnostem vyplývajícím z vyhlášky. [21]

V rámci vyhlášky je uvedena povinnost vytvoření dokumentu Plán rozvoje bezpečnostního povědomí a zajištění procesu, který je s tímto dokumentem v souladu. Služba zvyšování bezpečnostního povědomí může být doplněna o kompletní plnění této legislativní povinnosti, kdy je navíc specifikován vzdělávací plán pro všechny role v organizaci a zajištěna evidence pravidelných školení. To vše s přihlédnutím k nástrojům a povaze zákazníka. [21]

V souvislosti s povinnostmi stanovenými výše uvedenou vyhláškou je rovněž možné zajišťovat kontrolu dodržování bezpečnostní politiky všech rolí v organizaci. Formou kontroly mohou být nejrůznější scénáře ověření kvality bezpečnostního povědomí.

V zájmu maximálního pokrytí potřeb cílové organizace se nabízí také možnost zajištění jednorázových nebo periodických bezpečnostních školení uživatelů mimo komplexní program zvyšování bezpečnostního povědomí. Tato školení jsou obsahově plně přizpůsobena zákaznické organizaci a mohou být realizována libovolnou níže uvedenou formou.

5.1.1 Formy školení

Vzdělávací kurzy seznamující uživatele se zásadami bezpečného chování, s odpovídajícími pravidly a předpisy a aktuálními hrozbami jsou standardně poskytovány ve 3 variantách (prezenčně, pomocí webinářů či e-learningu), pro potřeby navrhuji následující formy školení:

- Prezenční školení — všichni uživatelé jsou s obsahem relevantních interních předpisů seznámeni formou přednášky, realizované specialisty.
- Školení formou webinářů či videopřednášek — uživatelé jsou se zásadami a obsahem relevantních interních předpisů seznámeni pomocí webinářů či videozáznamů,

v rámci nichž je materiál promítán za doprovodného komentáře přednášejícího specialisty. Uživatelé se mohou účastnit webináře v čase jeho konání, nebo shlédnout záznam z něj v době, která jim nejvíce vyhovuje.

2 Struktura školení

Struktura a obsah školení jsou vždy uzpůsobeny prostředí a požadavkům organizace, obecně jsou však v jeho průběhu zaměstnanci vždy seznámeni se zásadami informační bezpečnosti a interními standardy a směrnicemi, které tuto oblast upravují. Primárně bývá obsah školení determinován politikami a směrnicemi, zaměřenými na používání informačních a komunikačních technologií v organizaci a zabezpečení informací a informačních a komunikačních technologií. Do školení je vždy rovněž zahrnuta problematika obecných zásad bezpečného chování v organizační síti i mimo ní. V zájmu maximálního osvětlení a zafixování látky jsou probírané koncepty doplňovány o praktické příklady aktuálních hrozeb a korektní postupy v případě styku s nimi.

Jak je uvedeno výše, semináře svou strukturou vždy reflektují specifika konkrétní organizace, obecně však odpovídají následující osnově:

- Úvod do problematiky informační bezpečnosti
- Seznámení s relevantními interními normami
- Seznámení s užívanými pojmy
- Klasifikace informací užívaná v organizaci a požadavky na jejich ochranu
- Odpovědnosti a povinnosti uživatelů při práci v informačních systémech
- Politika hesel a řízení přístupu
- Zabezpečení přístupů do infrastruktury
- Povolené způsoby výměny informací a zacházení s médii
- Politika zálohování a zabezpečení dat
- Fyzická bezpečnost a zabezpečení přístupů
- Nakládání s informačními technologiemi a odpovědnosti uživatelů za ně
- Bezpečnostní kontroly a monitoring
- Události a incidenty související s informační bezpečností a jejich řešení
- Seznámení s konceptem plánů kontinuity a souvisejícími povinnostmi uživatelů
- Seznámení s aktuálními hrozbami a způsobem reakce na ně

5.1.3 Vzdělávání manažerů IB

Pro manažery informační bezpečnosti, kteří již mají vytvořené vlastní vzdělávací programy, a také možnost revize a úpravy těchto materiálů svými specialisty tak, aby bylo zajištěno pokrytí všech oblastí nutných pro soulad s požadavky norem řady ISO 27000 i zákona 181/2014 Sb.

5.1.4 Vzdělávání zaměstnanců

Vzdělávání vybraných zaměstnanců ve stanovené periodě o aktuálních trendech kybernetické bezpečnosti v souvislosti s řízením ISMS podle zákona č. 181/2014 Sb. prezenční formou.

Vzhledem k interaktivní formě výuky doporučujeme maximálně 15 účastníků na kurz.

6 VYHODNOCENÍ PROJEKTU A STANOVENÍ DOPORUČENÍ PRO UDRŽENÍ KVALITY V BUDOUCNU

Správnému vyhodnocení systému řízení podniku předchází pečlivé prověření všech vstupů, které k vyhodnocení používáme. Je nutné si uvědomit, že některé z parametrů se mohou vzájemně prolínat a některé mohou být dokonce ve vzájemném konfliktu. Pracovní postup popsaný výše lze aplikovat na různé situace, což ve výsledku vyžaduje různé strategie pro dosažení cíle. Stručně řečeno, podnik musí analyzovat data a výsledky po aplikaci všech faktorů návrhu v kontextu svých cílů pro implementaci řízení kvality. Máme vydefinovanou významnou investici do podnikové aplikace a tím nastaven posun do digitální transformace. V našem případě, pro zpoplatnění provozu na pozemní komunikaci pro vozidla nepřesahující 3,5tuny. Kromě vlastní problematiky výběru je současně nutné zajistit sled požadavků na bezpečnost transakcí, protože nedílnou součástí řešení je přímá komunikace s Významnými informačními systémy státu. Nemusíme uplatňovat v plném rozsahu všechny kroky v navrženém pracovním postupu, můžeme se zaměřit na konkrétní oblast zájmu s nejvyšší prioritou.. V případě významných investic do rozvoje může podnik vyhodnotit své činitele tvorby podnikové strategie za inovační / diferenciační a následně se rozhodnout pracovat pouze na cílech správy a řízení, které jsou pro tento návrh zdůrazněny. V případě nových nařízení o ochraně osobních údajů se podnik může zaměřit na cíle správy a řízení, které odpovídají vysokým požadavkům na dodržování předpisů a zákonných norem. Tyto cíle jsou v obecné rovině uvedeny v rámci COBIT Core Model, konkrétně v Zajištění nastavení a údržby rámce správy (EDM01), Zajištění optimalizace rizika (EDM03), Řízení rizika (APO12). Důležitá součást projektu je tzv. exit plán, pro případ ukončení spolupráce a zajištění kontinuity provozu. Exit strategie je důležitá proto, že všechny zúčastněné strany mají jasno, co se stane a co bude probíhat, když se zúčastněné strany nedohodnou na pokračování spolupráce. V exit strategii tak mohou být obsažena důležitá ujednání, jako je například vrácené poskytnutých licencí nebo technologií, předání dat, migrace na nové systémy, kompetence a finanční vyrovnání nákladů spojených s přechodem na novou platformu.

6.1 Nástroje pro udržení kvality

Cílem podniku je vytvořit a udržovat takový systém řízení kvality, kde společnost i její pracovníci dodržují profesní standardy a požadavky právních norem a předpisů.

Podnik nastavuje systém řízení kvality, který obsahuje zásady a postupy, které vedou k odpovědnosti vedení společnosti za kvalitu, etiku, dostatečně dimenzované lidské zdroje, provedení zakázky a její monitorování. Podnik je povinen stanovit takové zásady a postupy, kde výkonný ředitel nebo vedení společnosti přidělí provozní odpovědnost za systém řízení kvality pouze osobám, které mají schopnosti a potřebné pravomoci k převzetí této odpovědnosti.

Podnik stanovuje zásady a postupy, které mu poskytnou jistotu, že má dostatečný počet pracovníků s potřebnými schopnostmi, způsobilostí, aby zakázky byly provedeny v souladu se standardy a požadavky příslušných právních předpisů.

Podnik stanovuje zásady a postupy pro dokumentaci kontroly kvality zakázky, která je zdokumentování toho, že postupy byly provedeny a v požadované kvalitě zakázky a v řádném termínu.

Podnik vyhodnocuje dopad nedostatků, které vyplynuly z monitorovacího procesu, a stanovit, zda jde o případy, kde systém sice vykazoval nedostatky, ale poskytoval přiměřenou jistotu a odpovídá profesním standardům. A pak systémové, opakující se nebo jiné významné nedostatky, které vyžadují okamžitá nápravná opatření.

Doporučení nápravných opatření o zjištěných nedostatcích obsahuje následující:

Přijetí nápravných opatření ve vztahu ke konkrétní zakázce nebo ke konkrétnímu pracovníkovi a informování osob, které odpovídají za školení a odborný rozvoj.

Zajištění změny zásad a postupů řízení kvality a disciplinární řízení s těmi, kteří nedodržují zásady a postupy společnosti, zvláště s těmi, kteří je porušují opakovaně.

Podnik stanovuje zásady a postupy, které definují potřebu uchovat dokumentaci z projektů, nebo auditních zpráv po dobu dostatečně dlouhou dle standardů podniku, nebo déle, pokud to vyžaduje zákonná norma.

ZÁVĚR

Tato práce měla za cíl ukázat COBIT jako nástroj, který dokáže najít cestu pro řešení složitých a komplexních požadavků na správu IT. Jen z krátkého náhledu možností, které rámec COBIT poskytuje je patrné, jak mocný nástroj to je. Autoři jsou si vědomi, že má-li efektivně fungovat tak složitý mechanizmus, kterým podnik, nebo organizace bezesporu jsou, je nutné strukturovaně vidět, jak celek, tak i všechny dílčí podčásti, a ke každé přistupovat s ucelenou metodikou, která na jedné straně dokáže vytěžit maximum z kvalit, které podnik, nebo organizace má, a používá, a zároveň dokáže ukázat na slabiny systému, či jednotlivých procesů a ty zafixovat, aby celý systém stál na pevných nohách a smysluplnost byla nejen v nastavených procesech, ale hlavně ve vědomí lidí, kteří činnost naplňují svoji prací.

Schopnost vidět kriticky nedostatky ve vnitrofiremní kultuře je pro vedoucí pracovníky velmi komplikované a často až nemožné, protože veškerá pozornost je směřována k dílčím úkolům v oblasti, nebo v odvětví, kde působí a získat nadhled nad procesy celé firmy nebo organizace často vyžaduje větší úsilí než pročíst výroční zprávu, případě si prohlédnout konsolidované výsledky firmy.

Hlavní přidaná hodnota rámce COBIT v případě implementace běžících projektů dovoluje zmapovat a zafixovat stávající nevyhovující stav a po měřitelných krocích ho postupně měnit, aniž by došlo k přerušení činností zákazníka nebo k ohrožení běžících služeb.

Použitý vzorový případ, Zpoplatnění provozu na pozemních komunikacích, patří do kategorie nových projektů, které při vhodné aplikací rámce umožní zachytit proces v okamžiku generování poptávky po službě a tím ho zafixovat a nastavit v optimální podobě na začátku vývojového cyklu a řešení tak navrhnout v souladu se všemi zúčastněnými stranami.

Odměnou za kvalitní analytickou přípravu v předprojektové fázi je výrazné zkrácení realizační fáze, minimální korekce během projektu, jak po obsahové stránce, tak především z pohledu časových milníků projektu. Pokud použijeme obecné pravidlo, kde čas = peníze, tak hlavní argument pro aplikaci rámce COBIT je úspora finančních prostředků. Díky komplexnímu přístupu k problematice a definovaným sofistikovaným nástrojům umožňujícím detailně zmapovat problematiku zákazníka, jak v podobně hloubkové analýzy požadavků, jejich kvantifikaci a nastavení priorit pro jejich vyřešení, tak požadavků systémových a kvalitativních.

Obsahem práce bylo ukázat možnosti, které COBIT nabízí a na příkladu mapování podnikové strategie na projekt Zpoplatnění provozu na pozemních komunikacích demonstrovat ideové možnosti rámce, který v Evropě zatím není příliš rozšířený. Z mého pohledu není na místě otázka, zda k většímu rozšíření rámce COBIT vůbec dojde, ale kdy se tak stane.

Vzhledem k rostoucím nárokům na administrativu v podobě různých forem nařízení z EU, které je nutné integrovat a implementovat, z počátku pouze formálních, a následně právně vymahatelných, bude komplexní metodika, kterou COBIT bezesporu je, pro fungující a prosperující podnik nebo organizaci nepostradatelná. Framework COBIT nabízí možnost celostního pohledu na procesy uvnitř firmy, nebo organizace, a dokáže nabídnout nástroje, které umožní tak specifickou oblast jako je IT, začlenit do smysluplného celku, který má nejen motivaci táhnout za jeden provaz, ale zároveň ví, který se směrem se bezpečně ubírat dál.

SEZNAM POUŽITÉ LITERATURY

Knižní zdroje:

[1] DOBDA, Luboš. *Ochrana dat v informačních systémech*. Praha: Grada, 2001. ISBN 80-716-9479-7.

[2] DOUČEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. *Řízení bezpečnosti informací*. Praha: Professional Publishing, 2008. ISBN 978-80-86946-88-7.

[3] DOUČEK, Petr a Luděk NOVÁK. *Když ICT nefungují - řízení kontinuity činnosti organizace*. 2010,10.

[4] KEŘKOVSKÝ, Miloslav a Miloš DRDLA. *Strategické řízení firemních informací: teorie pro praxi*. Praha: C.H. Beck, 2003. C.H. Beck pro praxi. ISBN 80-717-9730-8.

[5] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.

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

[7] SOKOVIC, M., D. PAVLETIC a K. KERN PIPAN. Quality Improvement Methodologies – PDCA Cycle, RADAR Matrix, DMAIC and DFSS. *JAMME*. OCSCO World Press, 2010, **2010**(43), 8.

[8] TVRDÍKOVÁ, Milena. *Aplikace moderních informačních technologií v řízení firmy: nástroje ke zvyšování kvality informačních systémů*. Praha: Grada, 2008. ISBN 80-247-2728-5.

Elektronické zdroje:

[9] COBIT Timeline. In: *ISACA* [online]. 2019b [cit. 2019-05-26]. Dostupné z: http://www.isaca.org/COBIT/PublishingImages/COBIT-2019/COBIT-Timeline-2019.jpg

[10] COBIT. *Wikipedia* [online]. 2019b [cit. 2019-03-01]. Dostupné z: https://cs.wikipedia.org/wiki/COBIT

[11] CORRINE N., Johnson. *The benefits of PDCA* [online]. Milwaukee: Quality Progress, 2002 [cit. 2019-03-04]. Dostupné z: https://search.proquest.com/openview/6fb24b731a9c0c8bafd90096fd751e76/1?pq-origsite=gscholar&cbl=34671

[12] ISACA. *COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution* [online]. ISACA, 2018d. ISBN 978-1604207620.

[13] ISACA. *COBIT® 2019 Design Guide: Designing an Information and Technology Governance Solution* [online]. ISACA, 2018b. ISBN 978-1-60420-765-1.

[14] ISACA. *COBIT® 2019 Framework: Governance and Management Objectives* [online]. ISACA, 2018a. ISBN 978-1-60420-764-4.

[15] ISACA. *COBIT® 2019 Framework: Introduction and Methodology* [online]. ISACA, 2018c. ISBN 978-1-60420-763-7.

[16] ISACA. *ISACA* [online]. 2019a [cit. 2019-03-22]. Dostupné z: https://www.isaca.org

[17] NOVÁK, Luděk a Josef POŽÁR. Systém řízení informační bezpečnosti. *Cybersecurity.cz* [online]. 2011 [cit. 2019-04-10]. Dostupné z: https://www.cybersecurity.cz/data/srib.pdf

[18] PAAS. *ISPSYSTEM* [online]. 2019 [cit. 2019-4-12]. Dostupné z: https://www.ispsystem.com/news/xaas

[19] PDCA. *Wikipedia* [online]. 2019a [cit. 2019-02-13]. Dostupné z: https://cs.wikipedia.org/wiki/PDCA

[20] SANTE, Tom van a Jeroven ERMERS. *ITIL® and TOGAF® 9.1: two frameworks* [online]. 2013, 12 [cit. 2019-05-03]. Dostupné z: https://www.tsoshop.co.uk/gempdf/ITIL_and_TOGAF_White_Paper_v0_3.pdf

Právní předpisy:

[21]Zákon č. 181/2014 Sb. ze dne 29. srpna 2014, o Zákon o kybernetické bezpečnosti,

ve znění pozdějších předpisů. In: Zákony pro lidi [online]. [cit. 2019-02-20]. Dostupný z: https://www.zakonyprolidi.cz/cs/2014-181

[22] Vyhláška č. 82/2018 Sb. ze dne 28. května 2018, o vyhlášce o kybernetické bezpečnosti, ve znění pozdějších předpisů. In: Zákony pro lidi [online]. [cit. 2019-04-11]. Dostupný z: https://www.zakonyprolidi.cz/cs/2018-82

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

APO - Setřiď, Plánuj, Uspořádej

BAI - Buduj, Osvoj si, Uskutečni

BS - Business continuity

CCIE - Cisco Certified Internetwork Expert

CCTV - Closed-circuit television

CISSP - Certified Information System Security Professional

CMMI – Capability Maturity Model Integration

COBIT Control Objectives for Information and related Technology

CSIRT - Cyber Security Incident Response Team

DDOS - Distributed denial of service

DevOPs - Development and operations

DI - Detekce Insiderů

DMZ - Demilitarizovaná zóna

DSS - Decision support system

HR - Oddělení lidských zdrojů

ICT - Informační a komunikační technologie

IPS - Intrusion prevention system

ISACA - Information Systems Audit and Control Association

ISMS - Information Security Management System

ISO - International Organization for Standardization

IT - Informační technologie

ITIL- Information Technology Infrastructure Library

KGI - Key Global Indicator

KU - kybernetický útok

MEA - Kontroluj, Ohodnoť, Posuď

PDCA - Plan-do-check-act

RACI - Responsibility Matrix

SIEM - Security Information and Event Management

SLA - Service-level agreement

SMART - Analytická technika pro navrhování cílů v řízení a plánování

SNORT - Network Intrusion Detection & Prevention System

SOC - Security operation centrum

TOGAF - The Open Group Architecture Framework

UCS - Unified Computing Server

VPIR - Validace procesů a incident response

VPN - Virtual private network

ZKB - Zákon Kybernetické bezpečnosti

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Příloha 1: Katalogový list navrhovaných školení

Základy kybernetické bezpečnosti

Délka školení: 1 den

Stručný popis školení: Úvod do bezpečnosti informací. Kurz slouží k pochopení řízení informační bezpečnosti a vysvětlení jednotlivých technických nástrojů.

Obsah:

- Popis a smysl řízení bezpečnosti informací
- Základní stavební kameny ISMS
- Procesy a dokumentace
- Ekosystém technických nástrojů
- Životní cyklus přístupu k bezpečnosti informací
- Problematika kybernetických hrozeb

Implementace zákona kybernetické bezpečnosti

Délka školení: 1 den

Stručný popis školení: Praktické shrnutí zákona o kybernetické bezpečnosti (ZKB) a jeho dopadů na regulované subjekty. Zaměříme se na praktickou stránku, jak požadavky ZKB implementovat a představíme Vám ověřené postupy implementace ISMS a upozorníme Vás na kritická nebo komplikovaná místa. Předáváme tak znalosti o bezpečnostních trendech a bezpečnostních incidentech, získaných zejména díky ALEF CSIRT, další přidanou hodnotou je získání přístupu pro tvorbu bezpečnostní strategie pro budoucí období a proces zlepšování ISMS v budoucnu. Ve školení představíme nové požadavky v novele ZKB a implementační postupy pro jednotlivé povinnosti vyplývající ze zákona.

Obsah:

- Důvody vzniku právní regulace
- ZKB České republiky v prostředí aktuální geopolitické situace
- Podrobný rozbor zákona a vyhlášek

- Plán implementace ZKB
- Představení principu auditu ISMS, příprava na státní dozor

Manager kybernetické bezpečnosti

Délka školení: 2 dny

Stručný popis školení: Seznámení manažerů kybernetické bezpečnosti s podstatou bezpečnostních opatření a efektivními přístupy k jejich zajištění.

Obsah:

- koncept regulace kybernetické bezpečnosti v ČR
- zákon č. 181/2014 Sb., o kybernetické bezpečnosti,
- nařízení vlády č. 315/2014 Sb., o kritériích pro určení prvku kritické infrastruktury,
- vyhláška č. 316/2014 Sb., vyhláška o kybernetické bezpečnosti
- vyhláška č. 317/2014 Sb., o významných informačních systémech
- normy ISO/IEC 27001:2013 a ISO/IEC 27002:2013 jako základní východiska pro regulaci kybernetické bezpečnosti
- praktické a efektivní přístupy k řízení rizik, vhodné pro splnění požadavků kybernetické bezpečnosti
- organizační a technická opatření kybernetické bezpečnosti a účelné přístupy k jejich účinnému splnění
- bezpečnostní dokumentace jako nástroj efektivního řízení kybernetické bezpečnosti
- techniky vyhodnocení účinnosti systému řízení bezpečnosti informací a plánování jeho rozvoje

Auditor kybernetické bezpečnosti

Délka školení: 5 dnů

Stručný popis školení: Tento intenzivní 5denní kurz připraví účastníky na to, jakým způsobem vykonávat audity pro certifikační orgány a napomáhá registračnímu procesu podle ISO/IEC 27001:2013. Cvičení a přednášky o auditování jsou založeny na normě ISO 19011:2012 (návod na auditování systémů řízení pro kvalitu a environment). Účastníci též získají vědomosti a zručnosti potřebné k tomu, aby byli způsobilí poskytnout praktickou pomoc a informace ostatním jednotlivcům a organizacím, které se snaží o dosažení souladu

s touto normou. Školení je zakončeno testem, při jeho úspěšném absolvování obdrží účastník mezinárodně uznávaný certifikát „Information Security Management Systems Auditor/Lead Auditor Course ISO 27001:2013“.

Obsah:

- Co je informační bezpečnost
- Důležitost informační bezpečnosti
- Výklad požadavků normy ISO/IEC 27001:2013
- Přehled o hrozbách a zranitelnosti informační bezpečnosti
- Řízení rizik informační bezpečnosti
- Výběr řízení informační bezpečnosti
- Jak vybudovat systém řízení informační bezpečnosti (ISMS)
- Techniky auditování ISO/IEC 27001:2013
- Řízení a vedení auditního týmu při auditu ISO/IEC 27001:2013
- Plánování auditů a sestavení programu auditu
- Příprava na vykonání auditu, sestavení kontrolního seznamu
- Zjištění z auditu, definice neshod, kategorizace neshod
- Dokumentace výsledků auditu, vypracování závěrečné zprávy z auditu
- Řešení neshod, opatření k nápravě
- Schopnosti pro efektivní vedení externího auditu
- Psychologické aspekty auditu
- Příprava na závěrečnou písemnou zkoušku
- Vykonání závěrečné písemné zkoušky

Architekt kybernetické bezpečnosti

Délka školení: 3 dny

Stručný popis školení: Tento intenzivní 3 denní kurz poskytne bezpečnostní přehled přes jednotlivé části ICT s vazbou na zákon o kybernetické bezpečnosti č. 181/2014 Sb. Náplň kurzu poskytuje podstatné informace pro plnění role architekta kybernetické bezpečnosti.

Obsah:

- Procesy zajištění bezpečnosti informací
- Způsob zajištění kvality procesů v celém životním cyklu

- Základní principy vytvoření strategie bezpečnostních opatření
- Základní principy vytvoření návrhu bezpečnostních opatření
- Základní principy implementace bezpečnostních opatření
- Základní principy provozu bezpečnostních opatření
- Základní principy prověřování a zlepšování bezpečnostních opatření
- Fyzická bezpečnost
- Klasifikace chráněných informací / parametry prvků fyzické bezpečnosti
- Řízení přístupu
- Elektronické Zabezpečovací Signalizace
- Prostředky omezující působení požárů nebo záplav.
- CCTV
- Bezvýpadkové napájení
- Zařízení pro zajištění optimálních provozních podmínek
- Aplikační bezpečnost
- Bezpečný SW design
- System Development Life Cycle
- Využívání jednotných šablon
- Řízení identity uživatelů
- Logování
- Testování
- Základní pravidla pro L2 a L3 design sítě
- Principy L2 a L3 segmentace sítě
- Principy vytváření DMZ
- Slučování a určování aplikací do VLAN
- SPT (Spanning Tree)
- Principy L2 útoků
- Doporučení pro konfiguraci přepínačů
- Řízení přístupů
- Síťový pohled
- Aplikační pohled
- Správa Hesel
- VPN

- Next Generation Firewally a Next Generation Intrusion Prevention Systémy
- DDoS - podstata útoků a způsoby ochrany
- Behaviroální analýza síťového provozu
- Zabezpečení emailové komunikace
- Zabezpečení webové komunikace
- Antivirus a AntiMalware ochrana sítě a uživatelů
- Data Lost Prevention
- Nástroje pro zaznamenávání činností
- Typické logovací mechanismy
- Definice požadavků na zaznamenávání činností dle ZKB
- Požadavky na přesný čas
- Logování přístupu a práce se síťovými prvky
- Logování na úrovni operačních systémů
- Logování na úrovni aplikací
- Centrální nástroje pro sběr logů
- Nástroje pro sběr a vyhodnocování událostí
- Popis základní funkcionality SIEMu
- Požadavky na nepřetržité vyhodnocování KBU
- Analýza zjištěných KBU
- Kontinuita
- Vysoká dostupnost
- Návaznosti na analýzy rizik
- Support / Servis
- SLA
- Náhradní díly

Lead Implementer ISO/IEC 27001:2013

Délka školení: 5 dní

Stručný popis školení: Na kurzu získáte komplexní znalosti nastavení ISMS podle normy ISO/IEC 27001:2013, pokrytí a hodnocení jednotlivých požadavků normy ISO/IEC 27001:2013 v přípravě na certifikační proces. Při složení testu na konci školení získáte certifikát ISO/IEC 27001 Lead Implementer v akreditaci BSI.

Školení je v anglickém jazyce.

Obsah:

- Porozumění rámci normy ISO/IEC 27001:2013 a principům správy ISMS podle této normy
- Zvládnutí tvorby bezpečnostních politiky, řízení procesů a postupů ISMS
- Vedení projektu implementace ISMS

Kybernetický útok a obrana v praxi

Délka školení: 3 dny

Stručný popis školení: Školení zaměřené na praktický výcvik v oblasti technik kybernetického útoku a obrany v prostředí kybernetického polygonu. V rámci „obranné“ části kurzu jsou probírány základy bezpečnostního monitoringu sítě, vyhledávání škodlivého provozu v síti a škodlivého kódu na koncových stanicích a další témata pokrývající ochranu informačních systémů před moderními hrozbami. „Útočná“ část kurzu je věnovaná základním technikám penetračního testování a praktickému vyzkoušení postupů užívaných při reálných kybernetických útocích.

Obsah:

- Základy kybernetické obrany
- Bezpečnostní monitoring
- Analýza síťového provozu
- Analýza potenciálně škodlivého kódu
- Základy kybernetických útoků
- Metodiky užívané pro penetrační testy
- Základní typy kybernetických útoků