Ekonomická fakulta
Faculty of Economics

Jihočeská univerzita v Českých Budějovicích
University of South Bohemia in České Budějovice

Jihočeská univerzita v Českých Budějovicích

Ekonomická fakulta

Katedra aplikované matematiky a informatiky

Diplomová práce

IT audit jako podpora finančního auditu

Vypracoval: Bc. Jakub Giertl

Vedoucí práce: Ing. Petr Hanzal Ph.D.

České Budějovice 2016

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
Fakulta ekonomická
Akademický rok: **2015/2016**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jakub GIERTL**
Osobní číslo:	**E14729**
Studijní program:	**N6209 Systémové inženýrství a informatika**
Studijní obor:	**Ekonomická informatika**
Název tématu:	**IT audit jako podpora finančního auditu**
Zadávající katedra:	**Katedra aplikované matematiky a informatiky**

Zásady pro vypracování:

Cílem práce je prověřit nastavení informačních systémů a IT infrastruktury společnosti, které mají vliv na finanční data. Na základě prověření zhodnotit efektivitu a navrhnout změnu u případných nedostatků.

Metodický postup:

1. Studium odborné problematiky, vyhledávání literárních zdrojů souvisejících se studovanou problematikou, sběr dat.
2. Ověření nastavení IS, IT struktury a hlavních IT procesů ve společnosti.
3. Závěr.

Rozsah grafických prací: **dle potřeby**

Rozsah pracovní zprávy: **50 - 60 stran**

Forma zpracování diplomové práce: **tištěná**

Seznam odborné literatury:

1. **Gála, L. (2009).** *Podniková informatika.* **(2. přepracované a aktualizované vyd.). Praha: Grada Publishing.**
2. **Basl, J., & Blatíček, R. (2008).** *Podnikové informační systémy: podnik v informační společnosti.* **(Vyd. 2.) Praha: Grada Publishing.**
3. **ISACA org. (2013). COBIT 5 for Assurance. USA: ISACA.**
4. **Malone, T., & Wedemeyer, M. (2009).** *ITIL V3 Foundation Complete Certification Kit: 2009 edition.*
5. **Stanek, R. W. (2013).** *Microsoft SQLServer 2012: Kapesní rádce administrátora.* **Praha: Computer Press.**

Vedoucí diplomové práce: **Ing. Petr Hanzal, Ph.D.**
Katedra aplikované matematiky a informatiky

Datum zadání diplomové práce: **12. července 2016**

Termín odevzdání diplomové práce: **15. dubna 2017**

doc. Ing. Ladislav Rolínek, Ph.D.
děkan

JIHOČESKÁ UNIVERZITA
V ČESKÝCH BUDĚJOVICÍCH
EKONOMICKÁ FAKULTA
Studentská 13 (26)
370 05 České Budějovice

v.z. prof. RNDr. Pavel Tlustý, CSc.
vedoucí katedry

V Českých Budějovicích dne 13. července 2016

Prohlašuji, že jsem svoji diplomovou práci vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47 zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své diplomové práce, a to - v nezkrácené podobě/v úpravě vzniklé vypuštěním vyznačených částí archivovaných Ekonomickou fakultou - elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích dne …… …….

Bc. Jakub Giertl

Poděkování

Rád bych poděkoval panu Ing. Petru Hanzalovi Ph.D za ochotu a rady poskytované na konzultacích a také kolegům, který mi cennými diskuzemi pomohli k usměrnění záměru práce.

Obsah

1. ÚVOD

Diplomová práce se zabývá IT částí finančního auditu. Finanční audit je pro určité společnosti povinný ze zákona a musí být prováděný výlučně externí auditorskou společností. Hlavní úlohou IT auditorů je ujištění se o správném fungování systémů. Tím je zajištěna bezpečnost a integrita finančních dat.

Cílem této práce, je ověřit nastavení IT infrastruktury a procesů společnosti důležitých z pohledu finančního auditu. Ty budou ověřovány proti good practice (ověřené praxi) z oboru. Na základě výsledků a zhodnocení ověření, budou poté u případných nedostatků navrhnuta doporučení na nastavení procesů a jednotlivých systémů v souladu s good practice.

Při vypracovávání práce budu čerpat z vědomostí získaných ze studia oboru ekonomická informatika a další teorie, která bude rozpracována v teoretické části. Obsah celé práce bude koncipován tak, že jako autor počítám u čtenáře se základnou znalostí informačních technologií.

V první části práce bude čtenář napříč kapitolami postupně seznámen s důležitými oblastmi od poučení o samotném auditu, přes metodiky auditu IS/IT až po good practice a popis informačního systému.

Po shrnutí teorie bude následovat stanovení metodiky a samotná praktická část, ve které bude nejdříve připraven plán auditu, na jehož základě se bude dále postupovat. Následně bude provedeno ověření a poté na základě objevených nedostatků vydána doporučení k nápravě.

2. AUDIT

Na úvod této kapitoly bych rád citoval následující definici auditu z normy ISO 19011.

„Audit je systematický, nezávislý a dokumentovaný proces získání důkazů z auditu a jejich hodnocení s cílem stanovit rozsah splnění kritérií auditu."[1]

V České republice se začal audit rozvíjet až po roce 1989. První zákon o auditorech a Komoře auditorů České republiky byl zákon č.524/1992 Sb., který byl později v roce 2000 nahrazen zákonem č.254/2000. Následné úpravy proběhly ještě v roce 2009 zákonem č.93/2009 a poté v roce 2014 úpravou č.334/2014.

[3][9][10]

2.1 Druhy auditů

Audit je možné dělit podle kritéria předmětu auditu a to například na cenový, procesní, jakosti, legislativní, energetický, finanční, systému řízení, ekologický, bezpečnostní, informační, výkonnostní, provozu IS/IT, programový, daňový a další.

Audit je také možné rozdělit dle několika dalších kritérií jako například:

- interní x externí,
- průběžný x roční,
- předběžný x následný,
- selektivní x komplexní,
- pravidelný x jednorázový,
- povinný x povinný za určitých podmínek x nepovinný (doporučený).

[15]

[1] Citováno z ISO19011

2.2 Finanční audit

Základným cílem externího finančního auditu je posouzení spolehlivosti a kvality finančních výkazů organizace. Z tohoto důvodu je externí auditor zaměřený primárně na spolehlivost finančních informací.

Zákon o účetnictví:

„§ 20 Ověřování účetní závěrky auditorem

(1) Řádnou nebo mimořádnou účetní závěrku jsou povinny mít ověřenou auditorem, kterého účetní jednotka určí způsobem stanoveným v zákoně upravujícím činnost auditorů, účetní jednotky, kterým tuto povinnost stanoví zvláštní právní předpis, a dále

a) velké účetní jednotky s výjimkou vybraných účetních jednotek, které nejsou subjekty veřejného zájmu,

b) střední účetní jednotky,

c) malé účetní jednotky, pokud jsou akciovými společnostmi nebo svěřenskými fondy podle občanského zákoníku a k rozvahovému dni účetního období, za nějž se účetní závěrka ověřuje, a účetního období bezprostředně předcházejícího, překročily nebo již dosáhly alespoň jednu z uvedených hodnot

1. aktiva celkem 40 000 000 Kč,

2. roční úhrn čistého obratu 80 000 000 Kč,

3. průměrný počet zaměstnanců v průběhu účetního období 50,

d) ostatní malé účetní jednotky, pokud k rozvahovému dni účetního období, za nějž se účetní závěrka ověřuje, a účetního období bezprostředně předcházejícího, překročily nebo již dosáhly alespoň 2 hodnoty uvedené v písmeni c) bodech 1 až 3.

(2) Účetní jednotky uvedené v odstavci 1 nejsou povinny mít auditorem ověřenou účetní závěrku

a) sestavenou v průběhu konkursu, a to po dobu nepřetržitě po sobě jdoucích 36 kalendářních měsíců, počínaje prvním dnem kalendářního měsíce následujícího po dni, kterým nastaly účinky prohlášení konkursu, pokud o jejím ověření auditorem nerozhodne věřitelský výbor,

b) sestavenou ke dni předcházejícímu dni, kterým nastanou účinky schválení reorganizačního plánu, pokud o jejím ověření auditorem nerozhodne věřitelský výbor,

c) pokud došlo ke zrušení konkursu z důvodu, že majetek dlužníka je pro uspokojení věřitelů zcela nepostačující.“ [2]

„Posláním a smyslem auditu účetní závěrky je vyjádřit názor nezávislé, kvalifikované osoby na věrohodnost účetní závěrky zveřejněné vedením účetní jednotky. Auditor ověřuje, zda údaje v účetní závěrce podávají věrný a poctivý obraz finanční pozice a výsledků hospodaření a peněžních toků v souladu s pravidly předepsanými českými nebo jinými účetními předpisy, často s Mezinárodními standardy účetního výkaznictví (IFRS). Názor auditora má dostatečnou vypovídací schopnost pouze a jenom ve spojení s určitou úplnou účetní závěrkou, ke které se auditor vyjadřuje. Názor auditora vytržený ze souvislosti s konkrétní účetní závěrkou je zmatečný."[3]

2.3 Audit informačních systémů

Audit informačních systémů (dále také jako IS) se v České republice začal prosazovat v roce 1996, k čemuž dopomohly nově vytvořené vazby na mezinárodní organizaci ISACA®. Nejdříve byl v České republice vytvořen Czech Chapter a následně, o rok později, jsme se stali plnohodnotným členem organizace ISACA®. Od té doby je možné skládat v České republice mezinárodní certifikační zkoušku CISA (Certified Information Systems Auditor).

Auditor IT přidává k úloze auditu rozšíření pro oblast nasazení a využívaní informačních technologií (dále také jako IT) bez ohledu na to, zda jde o externí nebo interní audit. Potřeba IT auditora v souvislosti se stále více komplexnějšími informačními systémy pořád roste. V mnohých organizacích je hlavním zaměřením IT auditora posuzování rizik a ověřování kontrolních mechanizmů v IS.

[3][9][10]

---

[2] Citováno z §20 zákon o účetnictví kapitola Ověřování účetní závěrky auditorem
[3] Citováno z Komory auditorů CR (http://www.kacr.cz/poslani-a-smysl-auditu)

2.4 Metodiky auditu IS/IT

Metodik pro audit IS existuje celá řada. Jedno z hlavních postavení mezi mezinárodně uznávanými metodikami pro audit a ujištění správnosti procesů má COBIT®. Další metodikou může být INTOSAI, které jsou příkladem základu, co by taková metodika měla obsahovat.

[3]

2.4.1 INTOSAI

INTOSAI neboli International Organization of Supreme Audit Institutions sdružuje organizace, které provádí externí audity vládních organizací, tzv. SAI - Supreme Audit Institutions. V České republice je takovou organizací Nejvyšší kontrolní úřad. Pro audity ve státních organizacích byl vytvořen rámec pro standardy, které jsou v souladu s mezinárodními standardy ISA (International Standards on Auditing). Podobným procesem prošly i další instituce zabývající se finančním auditem, jako například Komora auditorů České republiky.

Pro nastínění základních standardů této metodiky v souvislosti s auditem IS se odkazuji na standardy ISA 315 a ISA 330.

ISA 315 - Identifikace a vyhodnocení rizik významné (materiální) nesprávnosti na základě znalosti účetní jednotky a jejího prostředí uvádí v odstavci 21 následující.

„*Při seznamování se s kontrolními činnostmi je auditor povinen zjistit především to, jakým způsobem účetní jednotka řeší rizika plynoucí z použití informačních technologií (IT). (viz odstavce A103–A105)*“ [4]

A následující odstavce, na které je odkazováno výše:

A103

„Použití IT ovlivňuje způsob implementace kontrolních činností. Z hlediska auditora jsou kontroly nad IT systémy účinné, pokud z nich vyplývá zachování integrity informací

[4] Citováno z ISA 315 [13]

a bezpečnost dat, které tyto systémy zpracovávají, a pokud zahrnují účinné obecné kontroly IT a aplikační kontroly.“ [5]

A104

„Obecnými kontrolami IT se rozumí pravidla a postupy, které se týkají mnoha aplikací a podporují účinnou funkci aplikačních kontrol. Týkají se prostředí serverů (mainframe, miniframe) a koncových uživatelů. K obecným kontrolám IT, které zajišťují integritu informací a bezpečnost dat, obvykle patří kontroly v následujících oblastech:

- *provoz datového centra a sítě,*
- *nákup, změny a údržba systémového softwaru,*
- *změny počítačových programů,*
- *zabezpečení přístupu,*
- *nákup, vývoj a údržba aplikačních systémů.*

Obvykle jsou implementovány za účelem řešení rizik uvedených výše v odstavci A63.“[6]

A105

„Aplikačními kontrolami se rozumí manuální nebo automatizované postupy, které obvykle fungují na úrovni podnikových procesů a týkají se zpracování transakcí jednotlivými aplikacemi. Aplikační kontroly mohou mít preventivní nebo zjišťovací charakter a slouží k zajištění integrity účetních záznamů. Proto se aplikační kontroly týkají postupů iniciace, zaznamenání, zpracování a vykázání transakcí nebo jiných finančních dat. Tyto kontroly poskytují ujištění, že se transakce vyskytly, byly schváleny a byly úplně a správně zaznamenány a zpracovány. Mezi příklady těchto kontrol patří editační kontrola vstupních dat a kontrola správnosti nepřetržité numerické řady, po nichž následuje manuální dořešení vykázaných výjimek nebo oprava při vkládání dat.“[7]

[5] Citováno z ISA 315 [13]
[6] Citováno z ISA 315 [13]
[7] Citováno z ISA 315 [13]

ISA 330 – reakce auditora na vyhodnocení rizika, které však pro větší pochopení je potřeba chápat v souvislosti s ISA 200 (Obecné cíle nezávislého auditora a provádění auditu v souladu s mezinárodními auditorskými standardy)

„Tento mezinárodní auditorský standard (ISA) upravuje povinnost auditora navrhnout a provést reakce na riziko významné (materiální) nesprávnosti údajů uvedených v účetní závěrce, které auditor v souladu s ISA 315 identifikoval a vyhodnotil při auditu účetní závěrky.“ [8]

V podstatě se však ISA 330 zabývá dvěma základními typy testů:

- Testy věcné správnosti, které zahrnují auditorské postupy navržené tak, aby pomohly k odhalení významných nesprávností. Úroveň nesprávnosti se dělí na dvě úrovně a to jak na testy detailních údajů jako skupin transakcí, zůstatků účtů a zveřejněných údajů, tak i na analytické testy věcné správnosti.
- Testy kontrol, které slouží k posouzení provozní účinnosti kontrol při prevenci nebo odhalovaní a opravách významných nesprávnosti na úrovni tvrzení.

Mezi odstavce související s auditem IS patří také odstavec A29.

„U automatizovaných kontrol nemusí být nutné zvětšovat rozsah testování, protože zpracování údajů prostřednictvím informačních technologií je svou podstatou konzistentní. U automatizované kontroly lze předpokládat, že funguje konzistentně, dokud nedojde ke změně programu (včetně tabulek, souborů nebo dalších trvalých dat programem užívaných). Jakmile auditor rozhodne, že automatizované kontroly fungují správně (k čemuž může dojít v okamžiku zavedení kontroly nebo k některému pozdějšímu datu), může zvážit provedení dalších testů, jejichž prostřednictvím bude ověřováno, že kontrola i nadále účinně funguje. Tyto testy zahrnují např. ověření toho, že:

• změny programu není možné provádět bez příslušných kontrol zaměřených na změny programů,

• pro zpracování transakcí se používá autorizovaná verze programu,

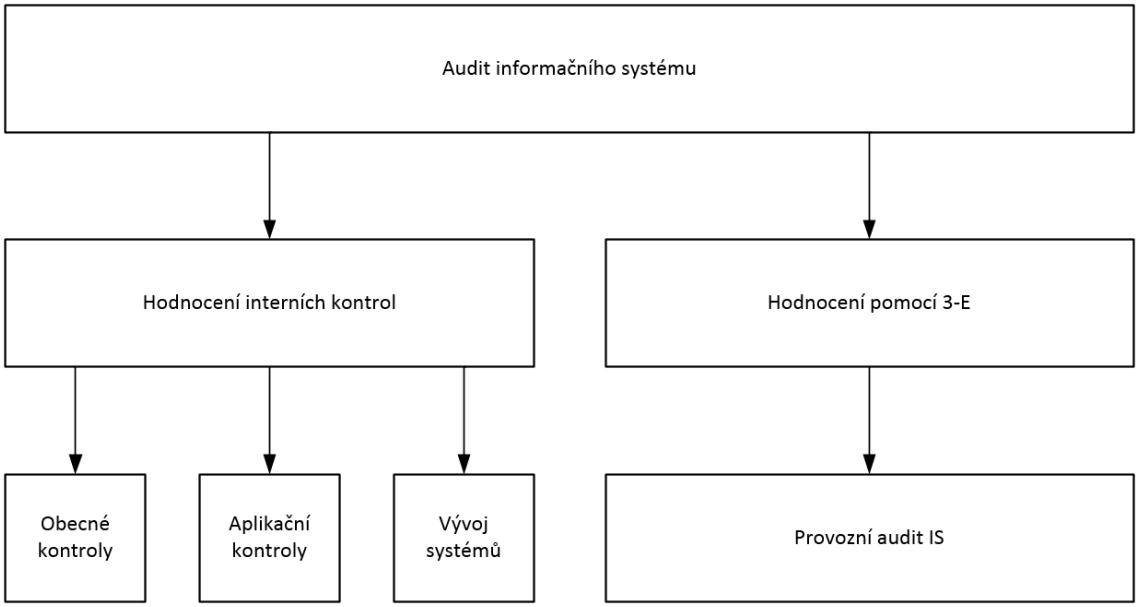
[8] Citováno z ISA 330 [14]

• také ostatní relevantní všeobecné kontroly jsou účinné.

Součástí těchto testů může být i určení toho, že nebyly provedeny změny programů, což může být případ účetní jednotky, která používá běžné softwarové aplikace, aniž by je sama modifikovala nebo udržovala. Auditor může například prověřit zprávu od oddělení zabezpečení informačních technologií, aby získal důkazní informace o tom, že se během daného účetního období neuskutečnil žádný neautorizovaný přístup.“[9]

Jak je možné vidět na obrázku 2.1, audit IS se dá dle INTOSAI rozdělit do více skupin.

Obrázek 2.1: Rozdělení kontrol dle INTOSAI



Zdroj: Vlastní tvorba

Audit obecných kontrol IS (General Controls) by měl procházet třemi etapami a to analýzou, testováním a hodnocením obecných kontrol IS.

Při analýze by se měl auditor zaměřit na následovné:

- odpovědné osoby za informační systém,
- řízení IT procesů v organizaci,
- realizace interního auditu informačních systémů v organizaci,

[9] Citováno z ISA 330 [14]

- hodnocení rizik spojených s IS a případná existence metodologie a dokumentace,
- existence politik, rámců, postupů týkajících se bezpečnosti informací, jejich dokumentace a dodržování politik v praxi,
- soulad IS se zákony,
- jiné významné skutečnosti s ohledem na IS.

U etapy testování bychom se neměli spoléhat jenom na dokumentaci, ale měli bychom si ověřit, jak se jednotlivé IT procesy realizují v praxi. Pro každý proces (přidělování přístupových oprávnění, změnové řízení atd.) bychom měli vybrat samostatný vzorek na testování.

Etapa hodnocení obecných kontrol by se měla zaměřit na kontrolu, zda interní kontroly zajišťují bezpečnost informací, důvěryhodnost, integritu a dostupnost.

Dalším typem auditu dle INTOSAI je audit aplikačních kontrol. Skládá se ze stejných etap jako předchozí audit a je zaměřen na hodnocení kontrol vstupu, zpracování, ochrany a prezentace dat specifických aplikací. Ve fázi testování bychom měli provést jedno až dvě podrobná testování celého životního cyklu dat v aplikaci od vstupu až po prezentaci. Současně bychom měli sledovat, zda aplikace v průběhu testování pracuje spolehlivě a bez problémů. Hodnocení se zaměřuje především na hodnocení spolehlivosti aplikace.

Audit kontrol vývoje systému zastřešuje kontroly životního cyklu jednotlivých IS včetně řízení změn. Dle Svaté [3] by tento audit mohl porušit nezávislost auditora a proto, by měl být prováděn jiným auditorem, než který provádí audit vývoje aplikace a ostatní druhy auditu. Separátní audit by se měl zaměřit na řízení projektu IS, řízení implementace IS do provozu a řízení změn.

Hodnocením účelnosti, účinnosti a úspornosti se zabývá audit provozu IS. Pro tento typ auditu jsou doporučeny tři etapy a důležité jsou výstupy z předchozích auditů.

První fází je hodnocení tvorby a pořízení IS ve všech fázích, za kterou následuje fáze hodnocení využívání a kvality poskytovaných informací tedy řízení IS. Třetí fáze se zaměřuje na hodnocení kvality služeb IS neboli hodnocení dopadu IS na společnost.

Pro každý typ auditu a jednotlivé etapy jsou dostupné přílohy, které můžou upřesňovat auditorské postupy (např. checklisty).

[3][13][14]

2.4.2 COBIT®

Pro řízení informačních technologií v organizacích se v dnešní době využívají hlavně dvě koncepce ITSM a IT Governance. Obě tyto koncepce pro řízení IS/IT vychází ze všeobecně přijímaných rámců, které mají usnadnit manažerům a dalším profesionálům v podniku (jako například vlastníkům byznys procesů, auditorům atd.) jejich zavádění do praxe.

První koncepce je IT Service Management neboli ITSM, která je podporována standardem ITIL® neboli Information Technology Infrastructure Library, kterým se budu zaobírat v pozdější kapitole a také ji budu používat jako good practice pro praktickou část. Koncepce ITSM je zaměřena na nižší úroveň řízení informatiky s cílem poskytování kvalitních služeb IT.

Druhá koncepce je IT Governance, která je rozšířením koncepce Enterprise a Corporate Governance. Tato koncepce je podporována standardem COBIT® neboli Control Objectives for Information and Related Technology.

Standard COBIT® je od verze 4 plně kompatibilní se standardem ITIL®. Základní principy řízení IT jsou v určitých oblastech shodné (jako například řízení incidentů, požadavků na službu atd.), ale principiálně nejsou v rozporu ani když jsou pohledy pojaty mírně odlišným způsobem (jako například životní cyklus IT, informační bezpečnost).

[3][11]

Na začátek je potřeba si vysvětlit pojmy Governance a Management, které oba mohou být v této oblasti přeloženy jako řízení anebo vedení.

Governance

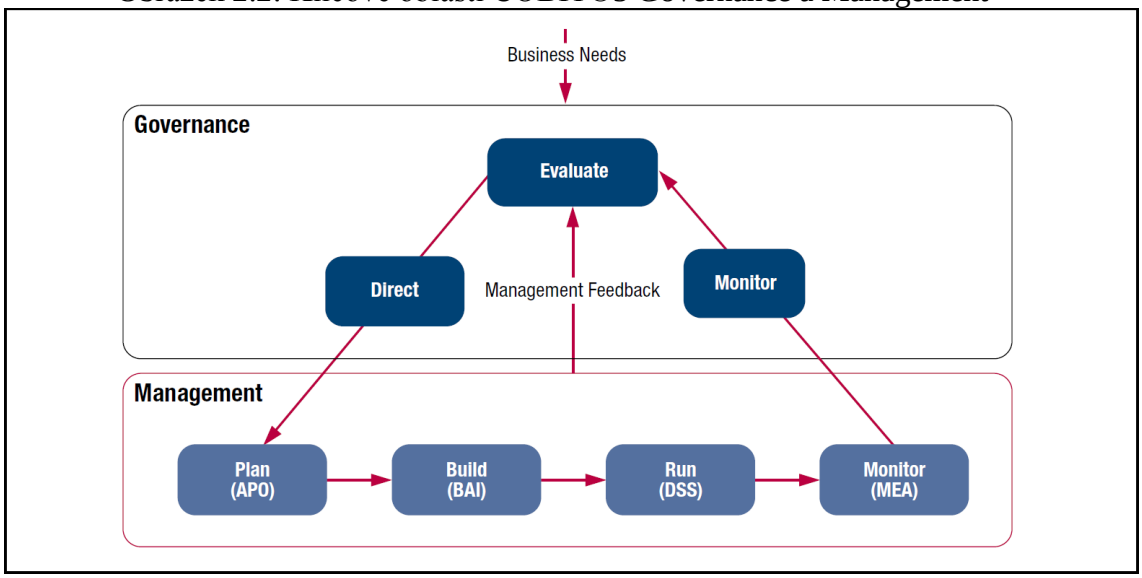
Governance zajišťuje, že potřeby, podmínky a možnosti klíčových osob společnosti jsou vybalancovány tak, aby došlo k odsouhlasení podnikových cílů, které mají být dosaženy. Dále zajišťuje nastavení směru prostřednictvím stanovení priorit a rozhodování a také monitorování výkonnosti a hodnocení proti předem odsouhlaseného směru a cílů.

Management

Management plánuje, sestavuje, řídí a monitoruje aktivity v souladu se směrem nastaveným governance pro dosažení podnikových cílů.

Po ujasnění termínů governance a management je jasné, že se každá oblast zakládá na odlišných činnostech. Základními rolemi pro governance je zhodnotit (Evaluate), nařizovat (Direct), a monitorovat (Monitor) avšak pro fungování efektivního governance systému je důležitá také interakce s managementem. Vztah mezi jednotlivými aktivitami je možné vidět na obrázku 2.2.

Obrázek 2.2: Klíčové oblasti COBIT®5 Governance a Management



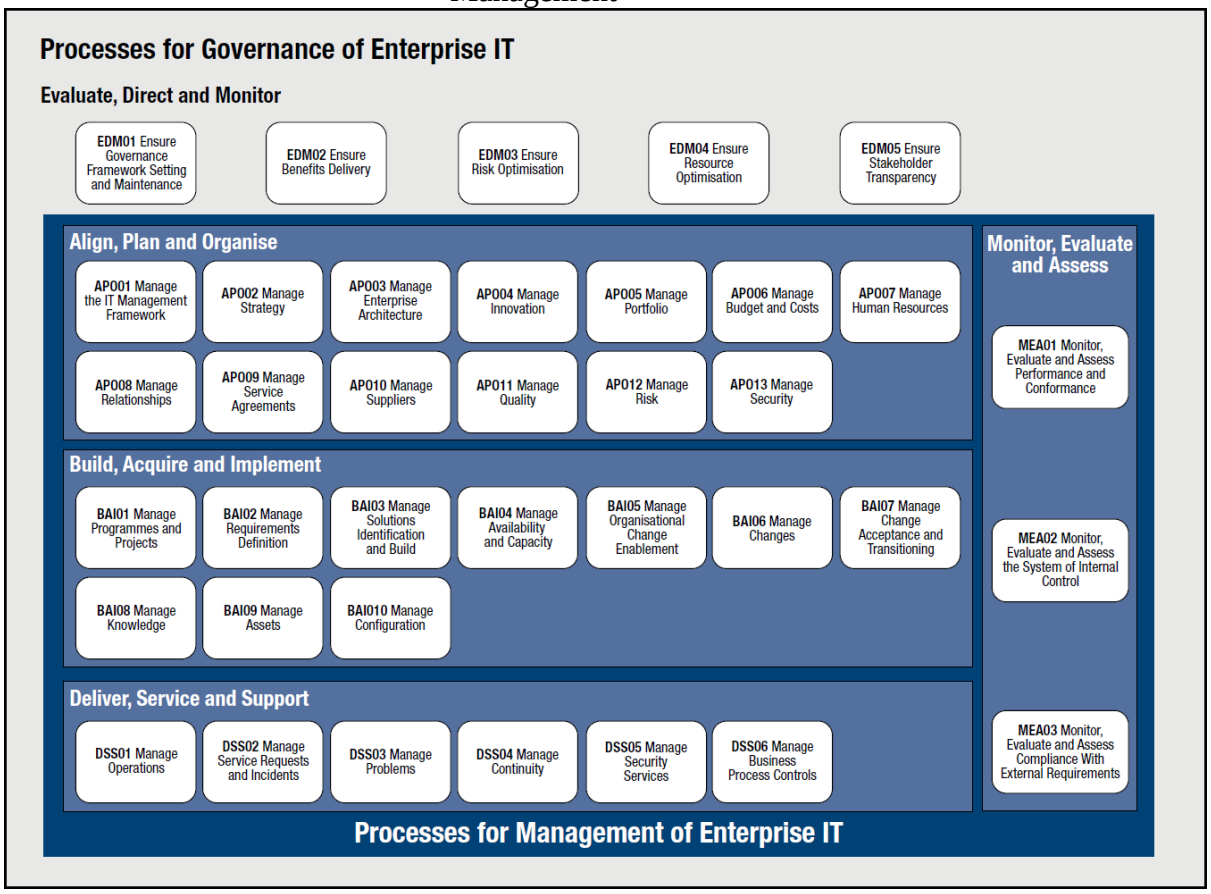
Zdroj: COBIT® 5 Framework [8]

Jednotlivé zkratky u oblasti management na obrázku 2.2 jsou tvořeny z jejich celého názvu, a tedy:

- Align, Plan and Organize (APO) tedy seřadit, naplánovat a organizovat.
- Build, Acquire and Implement (BAI) tedy sestavit, pořídit, implementovat.
- Deliver, Service and Support (DSS) tedy doručit, provozovat, podporovat.
- Monitor, Evaluate, Access (MEA) tedy monitorovat, zhodnotit, přistupovat.

Na obrázku 2.3 je možné vidět detailní pohled na oblasti, ve kterých má každá oblast specifikované procesy, které obsahují.

Obrázek 2.3: Procesy v jednotlivých oblastech COBIT®5 Governance a Management

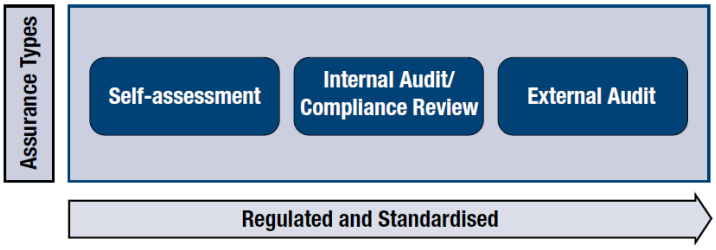


Zdroj: COBIT®5 Framework [8]

Pro každý jednotlivý proces je v metodice dále přesně rozepsaný doporučený detailní postup, metrika, RACI matice, cíle i potřebné vstupy a výstupy.

COBIT® Assurance, tedy metodika, která se zabývá ujištěním neboli auditem, se rozděluje na tři typy. Na obrázku 2.4 je možné vidět zmíněné rozdělení. Na ose X je zobrazeno, do jaké míry je dle názoru autorů daný typ regulován a standardizován. Za nejvíce regulovaný a standardizovaný je považován externí audit.

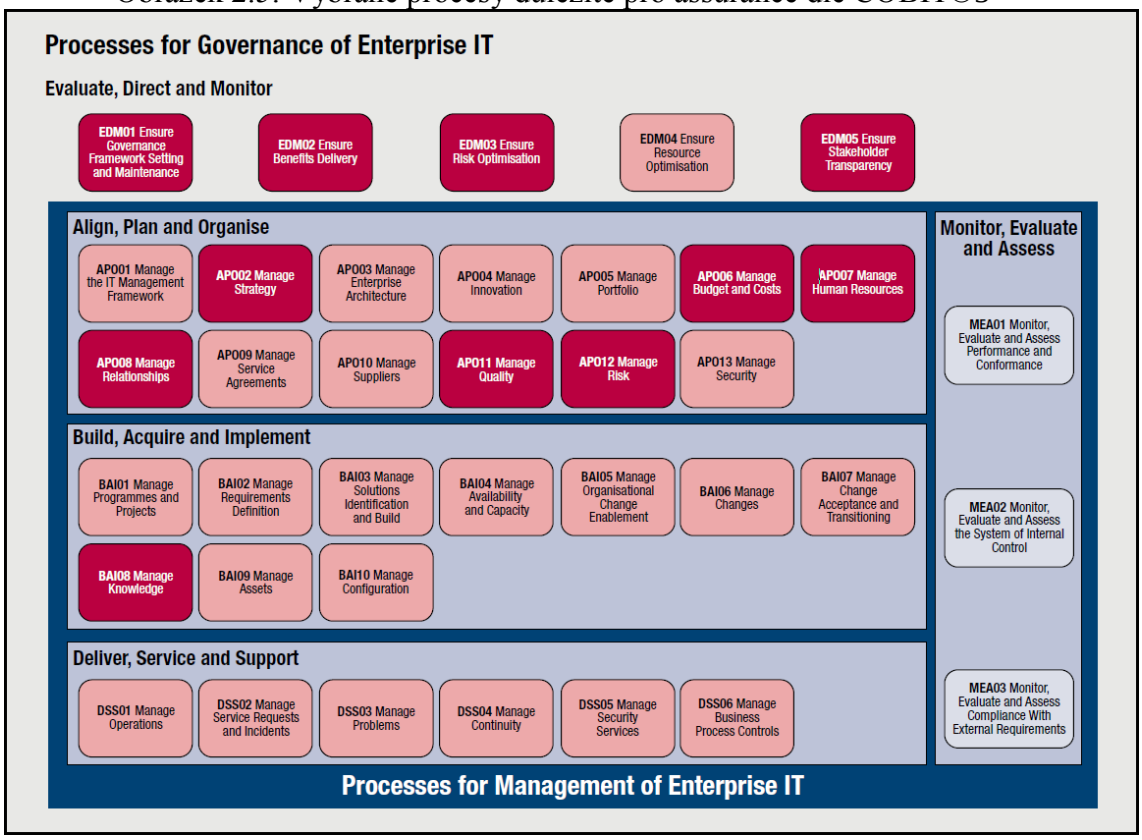
Obrázek 2.4: Typy Assurance



Zdroj: COBIT®5 for Assurance [5]

Pro assurance se nevyužívají všechny procesy, které byly zobrazeny na obrázku 2.3. Na následujícím obrázku 2.5 je možné vidět rudě vyznačené procesy, které se z celků Governance a Management a jejich oblastí v metodice COBIT® Assurance využívají.

Obrázek 2.5: Vybrané procesy důležité pro assurance dle COBIT®5



Zdroj: COBIT®5 for Assurance [5]

Důležité jsou tedy následující procesy:

- EDM - Ensure Governance Framework Setting and Maintanance, tedy Zajištění nastavení a údržby rámce Governance.
- EDM - Ensure Benefits Delivery, tedy Ujištění o benefitech dodávky.
- EDM - Ensure Risk Optimisation, tedy Ujištění o kompletnosti analýzy rizik.
- EDM - Ensure Stakeholder Transparency, tedy Zajištění správné komunikace klíčovým osobám.
- APO - Manage Strategy, tedy Řízení strategie.
- APO - Manage Budget and Costs, tedy Řízení rozpočtu a nákladů.
- APO - Manage Human Resources, tedy Řízení lidských zdrojů.

- APO - Manage Relationship, tedy Řízení vztahů.
- APO - Manage Quality, tedy Řízení kvality.
- APO - Manage Risk, tedy Řízení rizik.
- BAI - Manage Knowledge, tedy Řízení znalostí.

Metodika Assurance dále obsahuje rámce, jak vhodně nastavit audit/ujištění a jak v něm postupovat. Z důvodu, že danou metodiku ve své praktické části nebudu používat, nebudu toto téma rozebírat do hlubšího detailu a případné čtenáře, kteří by o toto téma měli zájem, bych rád odkázal na organizaci ISACA® a její literaturu.

Základní nevýhodou standardu COBIT® je, že se zaměřuje především na strategické řízení cílů IT, provedení jejich auditu a rychlému odhalení chyb vzniklých při jeho řízení, avšak neříká moc o tom, jak implementovat a designovat role, aktivity a procesy. To všechno je potřebné k zajištění splnění principů, které pak COBIT® popisuje z pohledu auditora.

[3][5][8][11]

2.5 Obecný plán auditu

Cílem této kapitoly je zmapovat obecné fáze, činnosti a výstupy, které jsou s auditem spojené. Všechny fáze a činnosti nemusí být nutnou součástí auditu. Podle druhu auditu a jeho cíle je možné jednotlivé fáze modifikovat, případně i některé vynechat. Pro účel diplomové práce jsem z jednotlivých fází vybíral jenom teorii, která mi přišla důležitá s ohledem na praktickou část. Při popisu postupu auditu jsem se opíral o literaturu Svatá,[3], která nemá základ v žádné metodice a je spíše výsledkem zkušeností z daného oboru.

0. fáze – Uzavření smlouvy auditu

Cílem této fáze je nastavení základních parametrů auditu. Ve většině případů u externích i interních auditů se musí předmět auditu (vymezení informačních systémů, databází atd.) definovat ve spolupráci auditora a zadavatele. Touto spolupráci je možné předejít případným nedorozuměním v očekáváních mezi zadavatelem a auditorem.

Auditor může v určování rozsahu auditu postupovat několika způsoby, které je možné i kombinovat.

U vertikálního přístupu se auditor nejdříve seznámí se strategickými cíli podniku. Z těch cílů si vybere ten nejrizikovější případně nejdůležitější a k němu přiřadí vhodné IT cíle, které následně provazuje s IT procesy a jejich kontrolními cíli. Tento postup je podporován i metodikou COBIT®.

U horizontálního přístupu auditor upřednostňuje pohled na jednotlivé prvky IS (aplikací, datových objektů, zařízení, lidi), které se následně mohou sdružovat například podle byznys procesů, funkčních oblastí, dat, nebo dle prvků infrastruktury

Další přístup využívá analýzu rizik na základě, v jejímž rámci jsou zmapovány jednotlivá aktiva IS, jejich slabiny a hrozby. Tento přístup je často preferován právě v případech, kdy funguje IT audit jako podpora pro finanční audit.

Životní cyklus IS a jeho prvků od jeho pořízení přes implementaci až po vyřazení upřednostňuje dynamický přístup. Auditor se u tohoto typu přístupu zaměřuje na prvky IS, které fungují už delší dobu bez radikálních změn anebo na prvky nové případně uvažované.

Důležitou součástí 0. fáze je také sestavení harmonogramu auditu. Ten vymezuje časový úsek, ve kterém budou realizovány průchozí testy, testování a vydání závěrečné zprávy. Harmonogram by také měl definovat potřebné vstupy pro audit, základní fáze, jejich kroky a výstupy.

1. fáze – Předběžné plánování

Před předběžným plánovaním je důležité, aby nejdříve auditor porozuměl následujícímu:

- podnikovým procesům,
- architektuře IS/IT,
- systému vnitřních kontrol.

Pro splnění tohoto cíle musí auditor získat spoustu informací zejména nastudováním interní dokumentace společnosti, pomocí dotazování a pozorování.

Potřebná míra porozumění procesů společnosti se liší v závislosti na hlavním cíli auditu. V případě, kdy je cíl obecnější jako například audit účetního systému, je potřebná komplexnější studie procesů, systémů a kontrol společnosti. Naopak za specifičtější cíl auditu se může považovat například audit legálnosti programového vybavení.

2. fáze – Vytvoření plánu auditu

Pro ověření informací a výstupů získaných v předchozí fázi auditor využívá svoje zkušenosti, existující standardy a ověřenou praxi (good practice).

Hlavním výstupem z této fáze je plán auditu, který by měl zahrnovat následující:

- cíl auditu (předmět auditu) – v případě, že byl v úvodních fázích cíl auditu úzce specifikován ve srozumitelném detailu pro auditora i zadavatele je možné tento bod vyloučit,
- určení rizik a zdůvodnění dalšího postupu auditu,
- plán testování,
- určení potřebných zdrojů a jejich rozvrh.

3. fáze – Realizace auditu

Realizace spočívá v testování kontrol, které byly identifikovány v předchozích fázích. Testuje se srovnání "teoretického" popisu kontrol (politik) ve společnosti s jejich praktickou realizací. Veškeré testování je pečlivě dokumentováno v předem specifikovaných formulářích.

V případě zjištění nesouladu je potřeba odhalit dopad nesrovnalostí na IT prostředí. K tomu slouží tzv. substantivní testování, jehož předmětem jsou nikoliv kontroly, ale předměty těchto kontrol. Pokud toto testování vzhledem k rozsahu není možné použít, využívají se různé metody výběrů vzorků. O celé realizaci a výsledcích testování je nutné vést důkazní materiál, který musí být součástí dokumentace.

4. fáze – Závěr a vydání auditorské zprávy

Před konečnou verzí auditorské zprávy by měla být nejdříve vydaná předběžná auditorská zpráva, která by se měla projednat s odpovědnými pracovníky, jichž se audit týkal. Hlavním smyslem této předběžné zprávy je ujištění, že všechny nálezy a závěry jsou relevantní a že nebyla pominuta hlavní rizika. Dále mají relevantní osoby možnost provést u některých nálezů nápravu a tím redukovat jejich významnost. Následně po tomto projednání je možné vytvořit závěrečnou zprávu auditu, která je hlavním výstupem.

5. fáze – Sledování plnění závěrů auditorské zprávy

U interního auditu je sledování plnění auditorských doporučení zcela přirozenou součástí auditu. Interní auditor vede seznam veškerých nálezů ze svých misí a dále v průběhu roku zjišťuje způsob jejich nápravy.

Z pohledu externího auditu je tato fáze více problematická. Obecně je externí audit často jednorázový projekt a tím pádem auditor nemá možnost ověřit, zda se společnost řídí dle jeho doporučení. Avšak u externího finančního auditu, který je obvykle prováděn jednou ročně, mají auditoři alespoň částečnou možnost kontroly, zda společnost učinila nápravy dle doporučení.

[11]

3. GOOD PRACTICE

V následující kapitole bych rád popsal standardy a ověřenou praxi, které budu ve své praktické části využívat.

3.1 ITIL®

ITIL® neboli Information Technology Infrastructure Library je mezinárodní řídící rámec popisující ověřenou praxi (good practice) pro řízení IT služeb. Rámec ITIL® se vyvinul ze snahy britské vlády během roku 1980 zdokumentovat, jak úspěšné organizace přistupují k řízení služeb. Na počátku roku 1990 vyrobili velkou sbírku knih dokumentujících "best practices" pro IT Service Management neboli řízení IT služeb. Tato knihovna byla nakonec přejmenována na IT Infrastructure Library. Office of Government Commerce ve Velké Británii i nadále funguje jako vlastník ochranné známky ITIL®.

ITIL® byl naposled aktualizován s vydáním verze 3 v roce 2007 a skládá se z následujících celků:

- Service Strategy,
- Service Design,
- Service Transition,
- Service Operation,
- Continual Service Improvement.

Ve své praci budu dále čerpat informace z vybraných kapitol jako Change management z celku Service Transition a dále IT Operations management spadající do Service Operation také s Event, Incident, Problem a Access managementem.

[4]

3.1.1 Change management

Cílem Change managementu neboli procesu řízení změn je zajistit, aby byly použity standardizované metody a postupy pro kontrolované, efektivní a rychlé vyřizování všech

změn, s cílem minimalizovat dopad změn na kvalitu služeb a následně zlepšit dennodenní fungování organizace.

Důležité kroky:

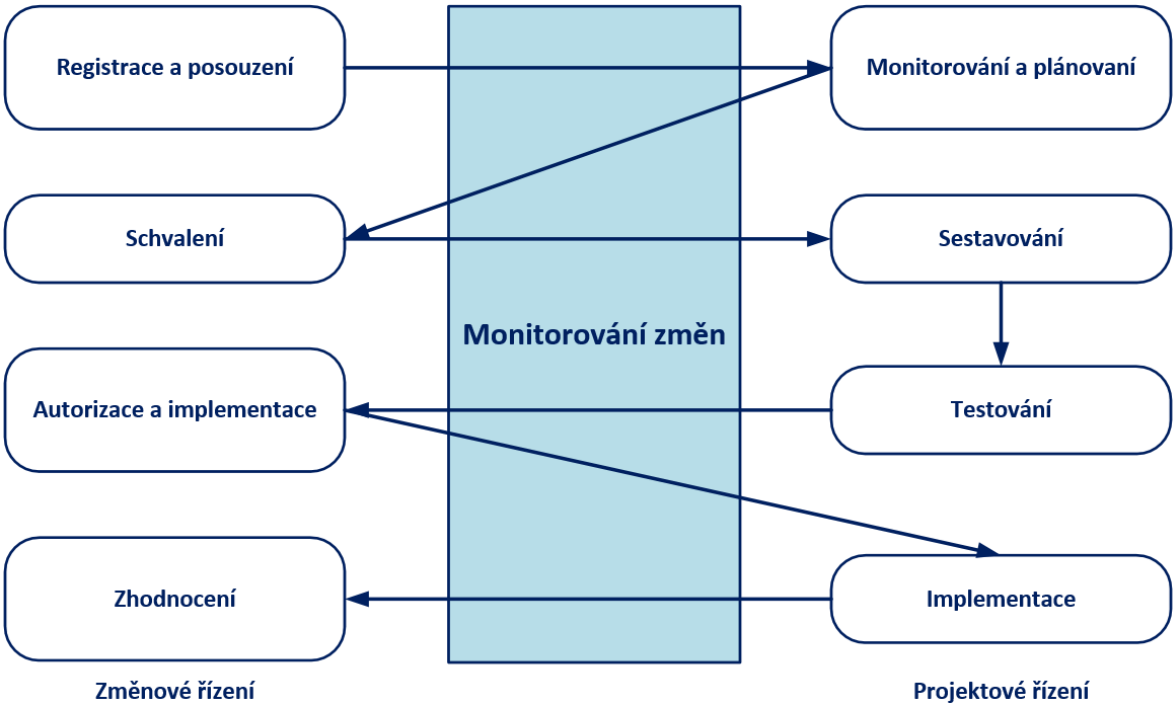
1. Zaznamenání žádosti o změnu.
2. Počáteční prozkoumání žádostí o změnu (filtrace žádostí dle relevance).
3. Posouzení žádosti o změnu – může vyžadovat zapojení změnového výboru (zvážení náročnosti požadavku, atd.).
4. Schválení změny odpovědným manažerem.
5. Vydaní pracovních příkazů na sestavení změny.
6. Koordinace prováděné práce na změnovém řízení (s několika milníky).
7. Změna je prozkoumána (otestována).
8. Změna je nasazena a změnové řízení je uzavřeno.

Při posuzování změnových požadavků je důležité znát odpovědi na následující otázky:

- Kdo vyžádal změnu?
- Jaký je důvod pro změnu?
- Jaký je přínos požadován ze změny?
- Jaká jsou rizika související se změnou?
- Jaké zdroje jsou zapotřebí pro dodání změny?
- Kdo je odpovědná osoba pro vývoj, testování a implementaci změny?
- Jaké je propojení mezi touto a dalšími změnami?
- Jaký je dopad změny na cílový systém?

Na obrázku 3.1 je zobrazen vztah mezi změnovým řízením a projektovým řízením.

Obrázek 3.1: Vztah mezi projektovým a změnovým řízením dle ITIL® v3



Zdroj: Vlastní tvorba

[4]

3.1.2 IT Operations management

Cílem řízení IT operací je provádění každodenních provozních činností potřebných pro správu IT infrastruktury. Činnosti se provádí v souladu s výkonnostními normami definovanými v průběhu definování servisního designu. V mnoha smyslech, IT operace provádí mnohé z logistických činností nutných pro efektivní a účinnou dodávku a podporu služeb (např. Správa událostí neboli Event Management).

V některých organizacích jsou IT operace spravovány a provozovány jediným, centralizovaným útvarem. V jiných některé aktivity a zaměstnanci z části centralizovány a z části poskytovány prostřednictvím distribuovaných a specializovaných oddělení.

Role a odpovědnosti:

- Údržba k dosažení stability dennodenních procesů a činností organizace.
- Pravidelná kontrola a vylepšení pro dosažení lepší služby za nižší cenu, při zachování stability.

- Rychlá aplikace operačních schopností za účelem diagnostikování a vyřešení případného selhání IT operací.

IT Operace se obvykle rozdělují do dvou skupin:

Obrázek 3.2: Rozdělení IT Operací dle ITIL® v3

Zdroj: Vlastní tvorba

[4]

3.1.3 Incident management

Cílem řízení incidentů je v co nejkratším čase obnovit normální provoz IT služeb a minimalizovat nepříznivý dopad na obchodní operace.

Incident lze charakterizovat jako:

- Neplánované přerušení IT služeb.
- Snížení kvality IT služeb.
- Selhání konfigurační položky (žádost o změnu, záznam o incidentu, Service Level Agreement), která doposud neovlivnila službu, ale v případě neřešení by ji mohla narušit. To může být vyvoláno interním IT pracovníkem.

Pro incident management neboli řízení incidentů jsou důležité následující aktivity.

Vlastnictví, monitorování, sledování a komunikace

- Service Desk je obvykle odpovědný za veškeré incidenty.
- Monitorování pokroku, eskalace incidentů.
- Sdělení uživateli a IT managementu.

Identifikace incidentů a protokolování

° Aktualizace potvrzení o incidentech a uživatelských údajích.

Kategorizace, prioritizace (nejkritičtější aktivita) a počáteční podpora

° Kategorizace jaký přesný typ "volání" je zaznamenán např. Incident (např. Desktop, sítě, e-mail).

° Posouzení naléhavosti a dopadu pro přiřazení správné priority.

° Párování proti existujícím problémům / známým chybám.

° Párování celé řady incidentů a vytvoření nových Problém záznamů (v případě potřeby).

° Poskytnutí počáteční podpory založené na zatím získaných znalostech o problému.

Vyšetřování a diagnostika

° Posouzení údajů o incidentech a poskytnutí řešení (pokud je k dispozici).

° Eskalace pro podporu oblastí (funkční) nebo IT managementu (hierarchicky).

Řešení a obnova

° Vyřešení incidentu nebo podání změnového požadavku.

Uzavření incidentu

° Podrobné informace o aktualizaci uskutečněných činností a klasifikace incidentu.

° Potvrzení uzavření s uživatelem.

Rozdíl mezi incident a problem managementem je ten, že problem management se zaobírá jádrem vzniku problému, aby už žádné další problémy z dané příčiny nevznikly. Incident management se zaobírá pouze řešením vzniklých problému, v co nejkratším čase bez ohledu na jádro problému. Obecný postup řešení je však z velké časti shodný.

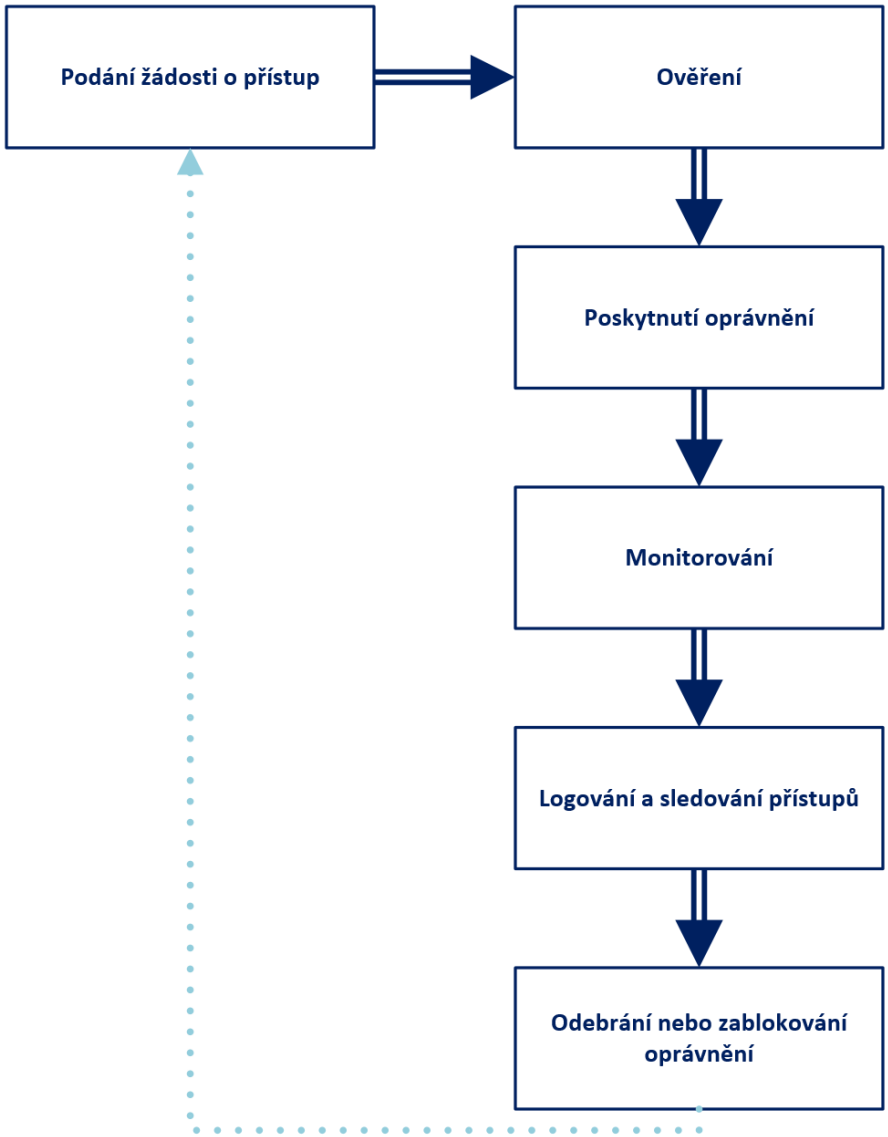
[4]

3.1.4 Access management

Hlavním cílem procesu řízení přístupů je poskytovat podporu při udělování přístupů oprávněným uživatelům k využívání služeb, které potřebují k náplni své pracovní činnosti a zároveň zabránit přístupu neoprávněným osobám.

Na následujícím obrázku 3.3 je možné vidět životní cyklus řízení přístupů v několika aktivitách.

Obrázek 3.3: Životní cyklus řízení přístupů dle ITIL®



ZDROJ: Vlastní tvorba

Životní cyklus řízení přístupů je využívaný pro řízení přístupu ke službám, informacím a zařízení. V mnoha implementacích, tato činnost souvisí s životním cyklem uživatele,

který naváže s organizací pracovní poměr (zřízení přístupů), změní pozici (změní se mu role) a nakonec opustí organizaci. Tento proces by měl být integrován se stávajícími byznys procesy v oblasti lidských zdrojů, takže správnost úrovně přístupu lze průběžně kontrolovat proti definovaným pracovním pozicím.

[4]

3.2 Heslová politika

Nejzákladnějším avšak ne jediným kritériem pro nastavení heslové politiky dle good practice neboli ověřené praxe je aby heslo obsahovalo alespoň 8 znaků.

Dalším ze základních, ale neméně důležitých kritérií je, že heslo musí splňovat pravidlo komplexnosti. V praxi to znamená, že by heslo mělo obsahovat alespoň malé a velké písmeno, číslici případně speciální znak jako například !, @, #, $, %, ^, &, *. Některé zdroje good practice již vyžadují kombinaci všech čtyř typů znaků.

Další kritéria dle good practice zveřejněné společností Microsoft jsou, aby maximální životnost hesla nebyla nastavena na více, než 60 dní a aby bylo zapnuto zapamatování historie hesel. Tím pádem aby byla nastavena hodnota 1 a více.

Posledním důležitým kritériem z mého pohledu je, že hesla musí být uložena ve složce v zašifrované anebo zahashované podobě a nesmí být uloženy jenom jako prostý text.

Do bezpečnostní good practice bych ještě zařadil automatické uzamčení počítače, které by mělo být nastaveno na míň než jednu hodinu.

[16] [17] [18] [19]

3.3 Systémy

Tak jako je důležité dodržování určitých pravidel good practice u procesů tak je stejně důležité je dodržovat standardy nastavení pro aplikační, databázové i operační systémy. Jednotlivá pravidla bezpečnosti jsou ve většině případů dost obecná a dají se aplikovat na téměř jakýkoliv z těchto systémů.

Kromě heslové politiky zmíněné v kapitole 3.2 je důležité u operačních systémů dodržovat následující kritéria, která by měla minimalizovat rizika zneužití:

- Uživatelům by měly být udělovány oprávnění pouze na to, k čemu systém pravidelně využívají.
- Výchozí účet s plnými administrátorskými oprávněními by měl být zablokován, případně by měl být dostupný pouze úzké skupině vyhrazených uživatelů.
- Logování přihlašování, provádění změn v nastavení, provádění změn v systému a provádění změn a mazání dat by mělo být zapnuté.
- Přihlášení a práce přes vzdálený přístup k systému (např. FTP - File Transfer Protocol) musí být zabezpečena a šifrována.

4. INFORMAČNÍ SYSTÉM

Účelem informačního systému je adekvátní podpora podnikových procesů informačními a komunikačními technologiemi. Nový podnikový IS může často při zvyšování celkové efektivity podniku změnit i podobu podnikání.

[1]

4.1 Vrstvy podnikového IS

Jednou z důležitých součástí při architektuře IS je pohled datové vrstvy. Ten je využíván například těmi, kteří programují v databázových prostředích vlastní aplikace a následně realizují aplikační řešení prostřednictvím vlastního programu včetně uživatelského rozhraní a dokumentace. Tento přístup chápání je možné označit za technologický. Znázornit ho můžeme pomocí jednotlivě navazujících vrstev, kde základ tvoří hardware a úplně nahoře je aplikační software.

[2]

Obrázek 4.1: Technologický model podnikového informačního systému

Zdroj: Podnikové informační systémy [2]

4.2 Hlavní data používaná IS

Z hlediska používaných dat v informačním systému podniku, konkrétněji ERP, existuje pět základních skupin.

1. Číselníky: Tato data jsou používána pro identifikaci položek, pracovišť, skladových míst, nákladových středisek, kont, referentů, dodavatelů apod. Dle základního principu jmenné konvence musí být identifikátor unikátní číslo.
2. Kmenová data: Obsahují údaje o výrobcích (o jejich komponentech a struktuře), způsobu realizace výrobku (receptury, technologické postupy atd.), výrobní základně (strojích a dalších pracovištích), dodavatelích materiálu (adresy a další údaje) a zákaznících (adresy a další údaje).
3. Zakázková data: Tato data uchovávají vazby na jednotlivé zakázky i s vazbou na dané zákazníky a požadované termíny, množství, strukturu atd.

Pro správnou funkci IS jsou také důležitá:

4. Archivní data: Obsahují informace o již zrealizovaných a uzavřených zakázkách.
5. Parametry: Zde jsou uloženy hodnoty pro optimální nastavení a fungování ERP a jeho modulů.

[2]

4.3 SAP R/3

SAP neboli anglicky „System – Applications – Products in data processing“ je firma se sídlem v Německu. V současnosti je SAP celosvětovým lídrem na trhu s ERP systémy a zaměstnává přes 30000 lidí ve více než 50 zemích. Zaměřuje se hlavně na velké firmy a korporace a jejich produkty používá více než 12 milionů uživatelů.

Systém SAP je na trhu je od roku 1993. Využívá třívrstvý model, kde databázová vrstva ukládá všechna data v systému. V aplikační vrstvě je uložena tzv. business logika a prezentační vrstva je ta, přes kterou komunikuje uživatel s klientem.

ABAP/4 neboli (Advanced Business Application Programming) je čtvrtá generace vlastního proprietárního jazyku pomocí kterého je programována funkčnost systému SAP R/3. Dále obsahuje i vývojové prostředí, které umožňuje vývojářům upravovat už existující programový kód anebo také vytvářet s využitím SAP frameworku vlastní funkčnost od reportů až po transakční systém. Pomocí SQL dotazů umožňuje ABAP komunikaci s databázemi, ve kterých může vybírat, mazat nebo měnit data. Dále je možné v ABAP vytvářet GUI (grafical user interface) neboli grafická uživatelská rozhraní.

R/3 se skládá ze 12 modulů, avšak některé firmy zavádí jenom některé z nich, protože ve většině případů se cena licence odvíjí od jejich počtu.

FI (Financial Accounting) Finanční účetnictví

CO (Controlling) Controlling

AM (Asset Management) Evidence majetku

PS (Project system) Plánování projektů

WF (Workflow) Řízení oběhu

IS (Industry Solutions) Specifická řešení různých odvětví

HR (Human Resources) Řízení lidských zdrojů

PM (Plant Maintenance) Údržba

MM (Materials Management) Skladové hospodářství a logistika

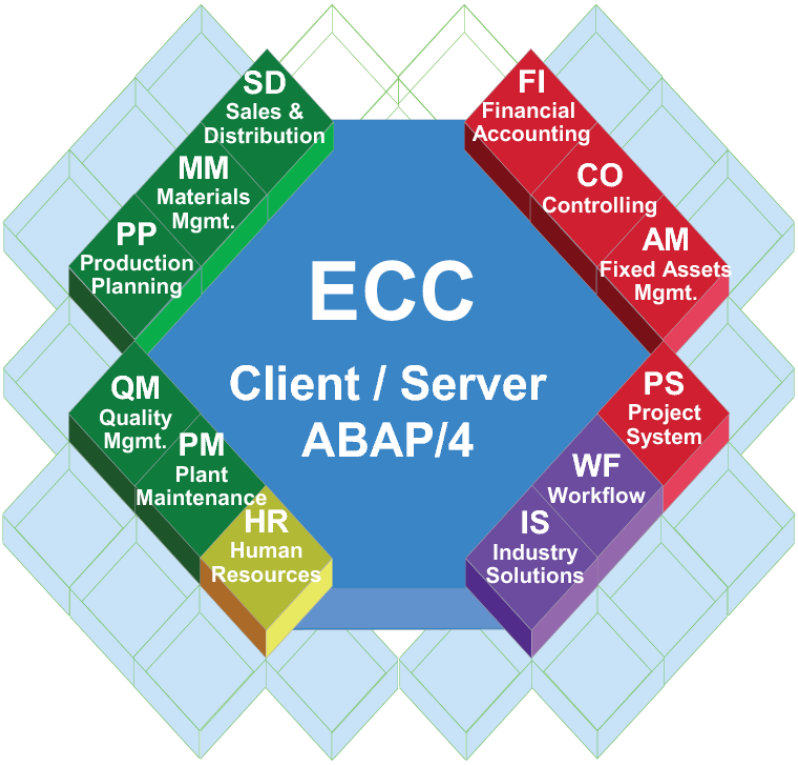
QM (Quality Management) Řízení kvality

PP (Production Planning) Plánování výroby

SD (Sales and Distribution) Prodej a distribuce

[6][12]

Obrázek 4.1: Moduly informačního systému SAP



Zdroj: ITACA.cz [12]

4.3.1 Transakce

Standardní způsob pro spuštění nějakého programu v SAP R/3 je jeho vyhledání v nabídce. Současně však systém nabízí možnost přímého spuštění požadované transakce. Transakce je program v modulu, který se chova dle svého kódu a zadaných parametrů. Každá transakce má unikátní kód, za kterým jsou ukryty procesy pro spouštění automatických procedur, vytváření nových záznamů, změnu a prohlížení dat. V takovém případě je potřeba do příkazového okna zadat příkaz mající standardní syntaxi /Nnnnn, kde nnnn znamená kód transakce. Chceme-li danou transakci spustit v novém režimu (v novém okně), pak použijte syntaxi /Onnnn. Standardní systém SAP R/3 Enteprise obsahuje celkem 72 205 různých transakcí.

Kód každé transakce je složen z abecedních a číselných znaků. Logika kódování transakcí není v SAP nijak nastavena. V některých případech je možné nastavení kódu vyvodit dle účelu transakce anebo dle náležitého modulu. Transakce, které končí na “01“, slouží většinou pro vytváření nových dat. Transakce končící na “02“ obvykle slouží pro změnu a končící na “03“ pro zobrazení dat. Koncové označení “04“ má obvykle specifické funkce nebo slouží k vymazání dat. Transakce, které začínají stejně jako zkratka modulu, patří většinou do tohoto modulu a tvoří jeho základ např. MM01, MM02, MM03 jsou transakce pro zadávání, změnu a zobrazení základních dat o materiálu. Jsou součástí modulu MM, ale data do nich může vkládat několik oddělení (logistika, prodej, účetnictví, controlling, nákup a atd.). Kromě obecných transakcí mohou být v systému další transakce, které byly vyvinuty na míru, aby zabezpečovali procedury specifické pro danou firmu.

Mezi nejpoužívanější transakce v SAPu patří již zmíněné MM01, 02 a 03, dále transakce pro logistický příjem materiálu MIGO. V logistice se dále používají transakce MB51 pro sledování pohybů materiálů a MB5L pro zobrazování stavu dostupných zásob. Se zaměřením na účetnictví/logistiku patří, mezi nejpoužívanější transakce MIRO, která slouží pro logistickou likvidaci faktur. Pro otevřené položky dodavatelů se používá FBL1N. Pro provádění automatických platebních běhů F110 a pro otevřené položky odběratelů FB5N. V oblasti controllingu patří mezi nejvýznamnější transakce CK40N a CK11N pro provádění kalkulací. Základní správa uživatele je obvykle na úrovni transakce SU01 a detailní seznámení s generátorem profilů a pokročilé nástroje jsou v transakci PFCG.

Dle typu transakce jsou v systému řešena také přístupová oprávnění jednotlivých uživatelů. Každý uživatel by měl mít nadefinovanou strukturu transakcí, které by měli odpovídat jeho pracovnímu zařazení. Při nastavování práv uživatelů se vychází z pravidel stanovených vnitřními předpisy. SAP umožňuje nastavit práva uživatelů k různým objektům v databázi.

[6] [7]

5. METODIKA

Metodika provedení ověření IT systémů se může lišit dle externího auditora (společnosti), která audit provádí. Cíl je však vždy stejný. Metoda, která bude v diplomové práci použita, je založená na analýze rizik a ujištění se, že jsou pokryta správným nastavením procesů a systémů.

V praktické části byly po prostudování kapitol auditu, good practice a informačního systému identifikovány a otestovány procesy a systémy. Identifikace systémů je provedena ve spolupráci s finančním auditem na první schůzce. Cílem auditu je ubezpečit se, že dané systému jsou v pořádku a tím pádem jsou důležitá data pro ověření finanční závěrky za rok 2015 validní a kompletní.

Na začátku auditu bude sestaven plán, podle kterého se bude dále pokračovat v ověření. Dalším důležitým krokem bude zaslání požadavku na export dat potřebných k ověření. Po jejich dodání budou nejprve ověřeny klíčové procesy společnosti. Procesy se budou skládat ze tří větších celků a to z procesu řízení přístupů, procesu změnového řízení a z IT operací. Procesy i systémy budou ověřovány proti standardům nastaveným v good practice.

Následně budu pokračovat ověřením zabezpečení a hardwaru, na kterém jsou všechny klíčové systémy. Poté bude následovat ověření operačního systému a databázového systému, na kterém je postaven aplikační systém. Pokud bude nastavení daných systémů v souladu s good practice budu na závěr pokračovat testováním klíčového systému.

Testování bude uzpůsobeno záměru diplomové práci. Z důvodu nutného anonymizování dokumentace nebude ve formě, jakou by měla splňovat pro skutečný audit. Testování na vzorcích bude také omezeno jenom na průchozí testy na jednom vzorku.

6. PRAKTICKÁ ČÁST

6.1 Plán auditu

Jako jednu z prvních věcí jsem si v praktické části připravil předběžný plán IT auditu. Plán se zakládá na kooperaci s finančním auditem a je strukturován do několika kroků.

1. Úvodní schůzka externího auditu s CIO a CFO společnosti.
2. Schůzka s finančními auditory ohledně analýzy rizik ve společnosti podstatné pro finanční audit.
3. Zaslání požadavku na export potřebných dat z rizikových systémů a aplikací a interních politik týkajících se IS/IT.
4. Analýza interních procesů.
5. Schůzky se zaměstnanci odpovědnými za aplikace, infrastrukturu a firemní procesy.
6. Kontrola fyzické bezpečnosti serverové místnosti a případné dotazování.
7. Testování operačních a databázových systémů a případné dotazování.
8. Testování aplikačních systémů a případné dotazování.
9. Shrnutí výsledků a projednání nálezů s finančním auditem.
10. Schůzka s managementem společnosti ohledem auditních nálezů a doporučení.

6.2 Identifikace systémů

Na úvodní schůzce s CIO společnosti jsem se dozvěděl strukturu aplikačního portfolia společnosti spolu s využitím jednotlivých aplikací. Na základě informací získaných z první schůzky bylo možné provést spolu s finančním auditem analýzu rizik, které by mohli narušit kompletnost a korektnost dat důležitých pro finanční závěrku. Identifikován jako rizikový byl jeden aplikační systém. Jednalo se o systém SAP, který byl ve společnosti používaný jako klíčový účetní systém, a je postaven na operačním systému Rad Hat Enterprise Linux a na databázi Oracle.

Ve spolupráci s klientem jsme podrobili systém hlubší analýze rizik. Soustředili jsme se na tři větší celky – změnové řízení, řízení přístupů uživatelů a IT operace (zálohování a naplánované systémové úlohy). Rizika za jednotlivé oblasti jsou vždy psány před testováním.

6.3 Vyžádání exportů ze systémů

6.3.1 Infrastruktura

Pod produkčním informačním systémem byla identifikována databáze Oracle a operační systém RedHat.

Pro provedení testování byli administrátoři požádáni o spuštění následujících příkazů za účelem získání exportů systémových konfiguračních souborů. Při následné osobní schůzce se zodpovědným IT administrátorem jsem osobně ověřil kompletnost zaslaných dat.

OS Red Hat Enterprise Linux

- /bin/cat /etc/passwd > etc_passwd.txt,
- /bin/cat /etc/group > etc_group.txt,
- /bin/cat /etc/security/access.conf > hostname_sec_access.txt,
- /bin/cat /var/log/secure > hostname_secure_log.txt,
- /bin/cat /etc/group | grep root > hostname_root_grp.txt,
- /bin/cat /etc/vsftpd/vsftpd.conf > hostname_vsftpd_conf.txt,
- /bin/cat /etc/vsftpd.user_list > hostname_vsftpuser.txt,
- /bin/cat /etc/ftpaccess > hostname_wuftpuser.txt,
- /bin/cat /etc/login.defs > etc_logindefs.txt,
- /bin/cat /etc/pam.d/system-auth > etc_pamd_systemauth.txt,
- /bin/cat /etc/login.defs > etc_logindefs.txt,
- /bin/ls –l /etc/security/opasswd > etc_security_opasswd.txt,
- /bin/cat /etc/passwd > hostname_etc_passwd.txt,

- /bin/ls –l /etc/passwd > hostname_perm_etcpasswd.txt,
- /bin/ls –l /etc/shadow > hostname_perm_shadowpasswd.txt.

Oracle DB

- SELECT * FROM DBA_USERS_WITH_DEFPWD,
- SELECT * FROM DBA_ROLE_PRIVS,
- SELECT * FROM DBA_USERS,
- SELECT * FROM v$parameter2,
- SELECT GRANTEE, OWNER, TABLE_NAME, PRIVILEGE FROM DBA_TAB_PRIVS WHERE TABLE_NAME = ‘AUD$’,
- SELECT USER_NAME, FAILURE FROM SYS.DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION = 'CREATE SESSION',
- SELECT * FROM SYS.DBA_ROLE_PRIVS WHERE ADMIN_OPTION = 'YES'.

6.3.2 Aplikační systém SAP

Pro ověření nastavení a procesů v core systému bylo potřebné získat od administrátorů kompletní exporty reportů a tabulek.

Z transakce SA38 byly vyžádány exporty následujících reportů. Viz tabulka 6.1.

Tabulka 6.1: Seznam vyžádaných exportů reportů ze systému SAP

Transakce	**Reporty**
SA38	RSPARAM
	RSUSR003

Zdroj: Vlastní tvorba

Následně byly vyžádány ještě exporty tabulek přes transakci SE16.Viz tabulka 6.2.

Tabulka 6.2: Seznam vyžádaných exportu tabulek ze systému SAP

Transakce	**Tabulky**	
SE16	USOBT_C	ADRP
	USOBX_C	AGR_PROF
	USR02	AGR_USERS
	USR03	AGR_AGRS
	USR04	AGR_1251
	USR10	AGR_1016b
	USR11	AGR_DEFINE
	USR13	TOBJ_CD
	USR21	TOBJ_OFF
	USR40	TSTCA
	UST04	T000
	UST10c	T001
	UST10s	E070
	UST12	V_USERNAME

Zdroj: Vlastní tvorba

6.4 Ověření IT politik a procesů společnosti

Na začátku ověřování jsem se seznámil s politikami, které ve společnosti popisují a definují rámce procesů související s IT/IS. U ověřování jsem kladl důraz také na to, zda jsou politiky pravidelně aktualizovány. Všechny relevantní směrnice byly schváleny a podepsány CIO a případně CSO společnosti.

Poté byla domluvena schůzka se zaměstnanci, které za dané procesy odpovídají.

Jak již bylo zmíněno výše, před schůzkou jsem ověřil následující politiky:

- provoz a bezpečnost IS,
- řízení uživatelských přístupů do IS,
- tvorba a správa uživatelských hesel,
- IT změnové řízení,

- IT problem management.

Poté, co jsem se seznámil s interními politikami, jsem si sjednal schůzky se zaměstnanci odpovědnými za dané procesy a to ředitel IT úseku a aplikační manažer, kteří jsou také členy změnového výboru ve společnosti.

6.4.1 Ověření procesu řízení přístupů

Rizika

1. Do IT prostředí mají přístup i neoprávnění z důvodu nedostatečného nastavení ověřování a zabezpečení.
2. Uživatelům IT prostředí za byznys a IT může být / byl přidělen přístup bez adekvátního schválení.
3. Uživatelům IT prostředí za byznys a IT může být / byl přidělen neoprávněný přístup nebo oprávnění, případně při změně pracovní pozice u uživatele došlo k porušení principu minimálních potřebných přístupů.
4. Přímé změny dat na úrovni databáze byly vykonány bez řádného schválení.

Ověření

Přístup do aplikace SAP je řízený pomocí přihlašovací funkce Single-Sign-On. Tato funkce využívá nastavení heslové politiky na úrovni domény.

Heslovou politiku jsem ověřil proti standardům good practice. Na obrázcích 6.1, 6.2 a 6.3 je možné vidět nastavení jednotlivých parametrů na úrovni domény (Active Directory).

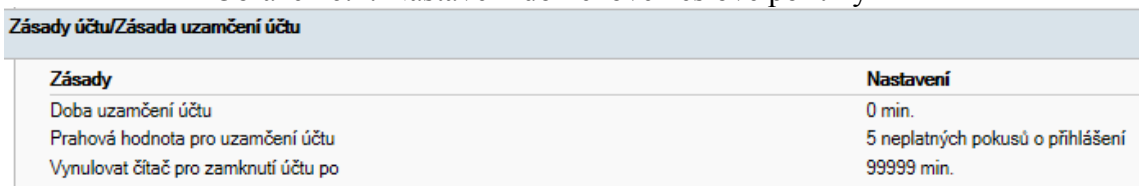
Obrázek 6.1: Nastavení doménové heslové politiky

Zásady účtu/Zásada hesel

Zásady	Nastavení
Heslo musí splňovat požadavky na složitost	Povoleno
Maximální stáří hesla	60 dní
Minimální délka hesla	9 znaků
Minimální stáří hesla	0 dní
Ukládat hesla pomocí reverzibilního šifrování	Zakázáno
Vynutit použití historie hesel	5 hesel zapamatováno

Zdroj: Vlastní tvorba

Obrázek 6.2: Nastavení doménové heslové politiky 2



Zdroj: Vlastní tvorba

Obrázek 6.3: Nastavení doménové heslové politiky 3

Zdroj: Vlastní tvorba

Porovnání nastavení domény proti good practice spolu se zhodnocením je zaznamenané v tabulce 6.3.

Tabulka 6.3: Nastavení heslové politiky na úrovni domény

Parametr	**Good practice**	**Nastavení**	**Zhodnocení**
Minimální délka hesla	8	9	**Efektivní**
Kompozice hesla	Ano	Ano	**Efektivní**
Maximální stáří hesla	60 dní	60 dní	**Efektivní**
Minimální stáří hesla	1 a více	0	**Neefektivní***
Prahová hodnota pro uzamčení účtu	5	5	**Neefektivní****
Historie hesel	5	5	**Efektivní**
Uzamčení v případě neaktivity	60 min	15min	**Efektivní**

Zdroj: Vlastní tvorba

*V případě pokud je hodnota "minimální stáří hesla" nastavena na 0, může dojít k opětovnému použití hesla jeho opakovaným přenastavením na požadovanou hodnotu. Tím pádem je přístup do systému špatně zabezpečený. Pokud je hodnota parametru rovná nebo větší než jedna znamená to, že uživatel musí počkat alespoň jeden den, než si může změnit heslo.

** Jak je možné vidět na obrázku 6.2, nastavení počtu neúspěšných pokusů přihlášení před uzamčením účtu je nastaveno na 5, což by dle good practice odpovídalo standardům. Když jsem však vzal v úvahu parametr “doba uzamčení účtu“ s nastavenou hodnotou 0 (obrázek 6.2), vyhodnotil jsem, že tento parametr neguje jakékoliv nastavení počtu pokusů před uzamčením. Proto je vyhodnocení neefektivní.

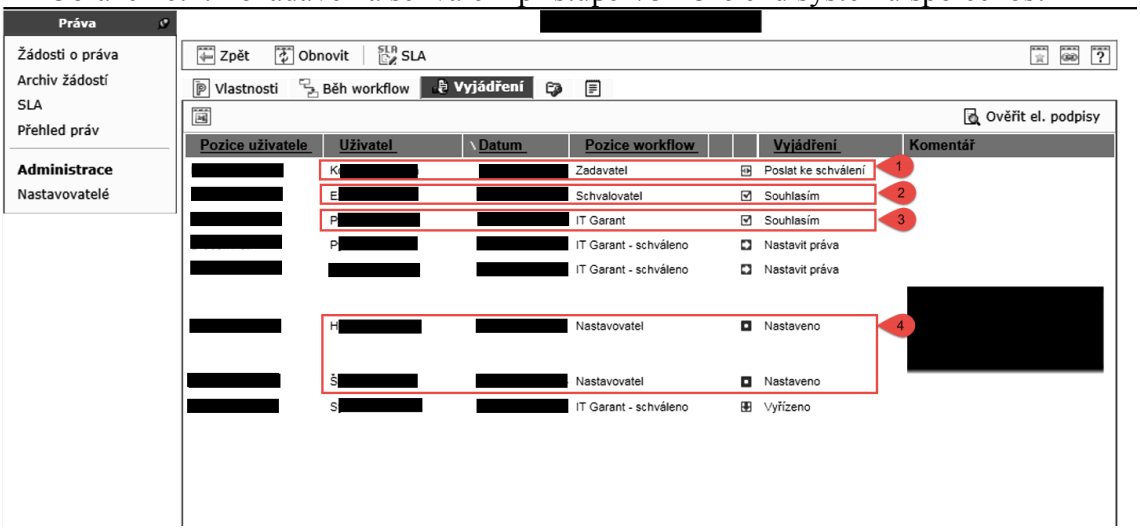
Pro správu uživatelských přístupů se ve společnosti používá frontendový nástroj, který slouží pro zaznamenání celého postupu přiřazování a přes který se ve společnosti spravují uživatelské přístupy a přiřazení rolí.

Pří příchodu nového zaměstnance anebo při změně zaměstnancovy pozice zodpovídá za přidělení oprávnění do systému jeho nadřízeny. Ten je povinen vytvořit v nástroji požadavek na přiřazení dané pracovní pozice. Každá pracovní pozice nese určitá specifická oprávnění, která jsou na základě matice oprávnění přiřazována v systému. Každá žádost musí být schválená gestorem (procesním byznys vlastníkem) daného oprávnění a aplikačním manažerem. V případě, že požadována oprávnění dané pozice spadají pod více gestorů, žádost musí být schválená všemi odpovědnými osobami.

V případě zřizování účtu nového zaměstnance je před přiřazením oprávnění nejdříve IT administrátory manuálně vytvořen uživatelský účet.

Na náhodně vybraném vzorku, který je možné vidět na obrázku 6.4, jsem ověřil, že proces pro řízení přístupů funguje v souladu s interními politikami.

Obrázek 6.4: Požadavek a schválení přístupu ve front-end systémů společnosti



Zdroj: Vlastní tvorba

1 - Přístup byl vyžádán uživatelem K.

2 - Oprávnění bylo schváleno byznys vlastníkem E.

3 - Oprávnění bylo také schváleno aplikačním manažerem P.

4 - Oprávnění byla nastavena administrátory H a Š.

Přiřazena oprávnění z matice oprávnění byla také otestována proti aktuálním oprávněním v systému.

Všechny přístupy do systému jsou logovány a změna v logu ze strany zaměstnanců není možná. Změny v nastavení logování může vykonávat jenom dodavatel systému na základě změnového požadavku, který musí projít klasickým změnovým procesem (viz Kapitola 3.1.1). Tento proces je také ošetřen pomocí SLA (Service Level Agreement) mezi společností a dodavatelem.

Na schůzce jsem také ověřil, že do frontendového nástroje používaných k řízení přístupů mají přístup jenom IT administrátoři a byznys vlastníci jednotlivých firemních procesů tedy osoby, které jsou odpovědné za fungování jednotlivých procesů ve společnosti.

Periodické kontroly přístupů a přístupových oprávnění uživatelů

Periodické kontroly přístupů a přístupových oprávnění jsou důležité pro kontrolu přístupů do IT prostředí. Pomocí těchto kontrol je zajištěno, že do prostředí nemají přístup nesprávní uživatelé nebo uživatelé s ukončeným pracovním poměrem. Kontroly také zajišťují, že uživatelé mají přidělené a aktualizované role v souladu s jejich pozicí.

U odchodu zaměstnance vzniká riziko, že jeho účet nebude zablokován a tak by mohl být použit k nekalé činnosti.

Při změně pracovní pozice se stává, že jsou zaměstnancům jenom přiřazena nová oprávnění, avšak nebývají jim odebrána předchozí oprávnění. Tím pádem má zaměstnanec pořád přístup i do agendy, která už není v náplni jeho práce.

Jednotlivým vedoucím oddělení jsou z personálního oddělení jednou za čtvrt roku posílány seznamy zaměstnanců, kteří se v liniové struktuře nacházejí pod nimi. Tento

seznam je následně porovnán s aktuálním exportem uživatelů a jejich oprávnění z Identity Management systému.

U každého zaměstnance musí být ověřeno, že jeho pracovní pozice odpovídá jeho aktuálním rolím přiřazeným v ITIMu a také, že se v systému nenachází žádný aktivní uživatel, který by už nebyl zaměstnancem společnosti.

Pokud by vedoucí neučinil do dvou týdnů od jejího začátku, uživatelům spadajícím pod jeho agendu by byl účet zablokován.

Na schůzce byla ověřena dokumentace z posledních tří periodických kontrol. Na základě efektivní a pravidelné kontroly aktuálnosti uživatelských účtů a oprávnění, je pokryto riziko vznikající při odchodu nebo změně pracovní pozice zaměstnance.

Shrnutí

Proces řízení přístupů, nastavení heslové politiky a periodických kontrol byly v souladu s interními politikami společnosti a v souladu s good practice.

6.4.2 Změnové řízení

Riziko

1. Nové aplikační programy nebo změny stávajících programů, reportů, konfigurací a rozhraní IT, nefungují, jak je popsáno, nebo požadováno, protože nejsou dostatečně testovány jinými osobami než vývojáři.
2. Nové aplikační programy nebo změny aplikačních programů v produkčním prostředí (včetně reportů a rozhraní), nejsou v souladu s byznys procesy nebo IT prostředím.
3. Programy v produkčním prostředí nejsou zabezpečeny a je umožněno vývojářům přesunout neoprávněné nebo neověřené změny do produkčního prostředí.
4. Konfigurační měny programů nebo aplikací provedené pracovníky IT jsou nepřiměřené nebo neoprávněné.

Ověření změnového řízení

Změny mohou být vyžádány vedoucími oddělení případně pracovníky z úseku IT. Všechny změny podléhají víceúrovňovému schválení. V prvé úrovni je změna schvalována byznys garantem, který zastává roli byznys vlastníka procesů v daném

systému. Následně je změnový požadavek ověřen aplikačním manažerem, ředitelem úseku IT anebo change managerem. Všichni tito tři zaměstnanci jsou součásti změnového výboru společnosti.

Po schválení je změnový požadavek zaslán posledním schvalovatelem dodavateli na nacenění. Po doručení finální nabídky od dodavatele je dále změna schvalována podle výše nacenění změny neboli navrženého rozpočtu na změnu.

V případě nahlašovaní incidentů v systému, můžou vedoucí oddělení poslat požadavek přímo na dodavatele pomocí helpdeskového nástroje dodavatele.

Systémové prostředí se ve společnosti rozdělují na vývojové, testovací a produkční.

Vývojové prostředí slouží pro dodavatele k vývoji a technickému testování systémových změn. Po vývoji a technickém otestování může být změna v systému nasazena na testovací prostředí.

Do testovacího prostředí mají kromě dodavatele přístup jenom jednotliví vlastníci byznys procesů ve společnosti a pracovníci úseku IT. Tito zaměstnanci testují jim přiřazené systémové změny za byznys a za IT. Ve většině případů jsou právě oni žadatelé anebo schvalovatelé na první úrovni. Testování musí být zadokumentováno a v případě akceptace změnový požadavek podepsán.

Po schválení od testerů za byznys a IT je změna posunuta na změnový výbor, který určí datum, kdy bude změna nasazena do systému tak, aby co nejméně narušila chod systému a tím pádem i byznysu společnosti. Po následovném schválení nasazení na produkci členem změnového výboru může být dodavatelem změna nasazena do produkčního systému.

Ve společnosti se dle politiky změnového řízení rozdělují do následujících skupin:

- emergency (akutní),
- malé,
- velké,
- projektové změny.

Emergency a malé změny jsou nasazovaný do produkce v kratších intervalech vždy každé pondělí v noci.

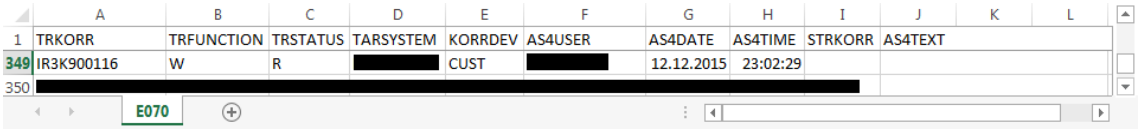
Velké změny jsou nasazovány v průměru jednou měsíčně a o plánu nasazování rozhoduje změnový výbor společnosti.

Projektové změny jsou samostatná kategorie změn, které se kvůli své důležitosti neřadí mezi normální změny. Většinou je celý změnový proces rozdělen do více milníků.

Na základě exportu tabulky E070 tedy všech transportů změn na produkčním systému jsem za rok 2015 náhodně vybral jeden vzorek, na kterém jsem následujícím postupem, který je popsán dále ověřil, že systémové změny podléhají změnovému řízení, jak je psáno v politikách společnosti.

Jak je možné vidět na obrázku 6.5, z exportu jsem vybral změnu IR3K900116.

Obrázek 6.5: Export transportu/změn z tabulky E070 v programu excel.



	A	B	C	D	E	F	G	H	I	J	K	L
1	TRKORR	TRFUNCTION	TRSTATUS	TARSYSTEM	KORRDEV	AS4USER	AS4DATE	AS4TIME	STRKORR	AS4TEXT		
349	IR3K900116	W	R	[redacted]	CUST	[redacted]	12.12.2015	23:02:29				
350	[redacted]											

E070

Zdroj: Vlastní tvorba

Na obrázku 6.6 je možné vidět protokol k vybrané změně IR3K900116 na kterém proběhlo ověření procesu.

1 - Změnový požadavek byl založen 27. 11. 2015 zaměstnancem na pozici IT specialista.

2 - Požadavek byl schválen ředitelem úseků financí a ředitelem IT úseku.

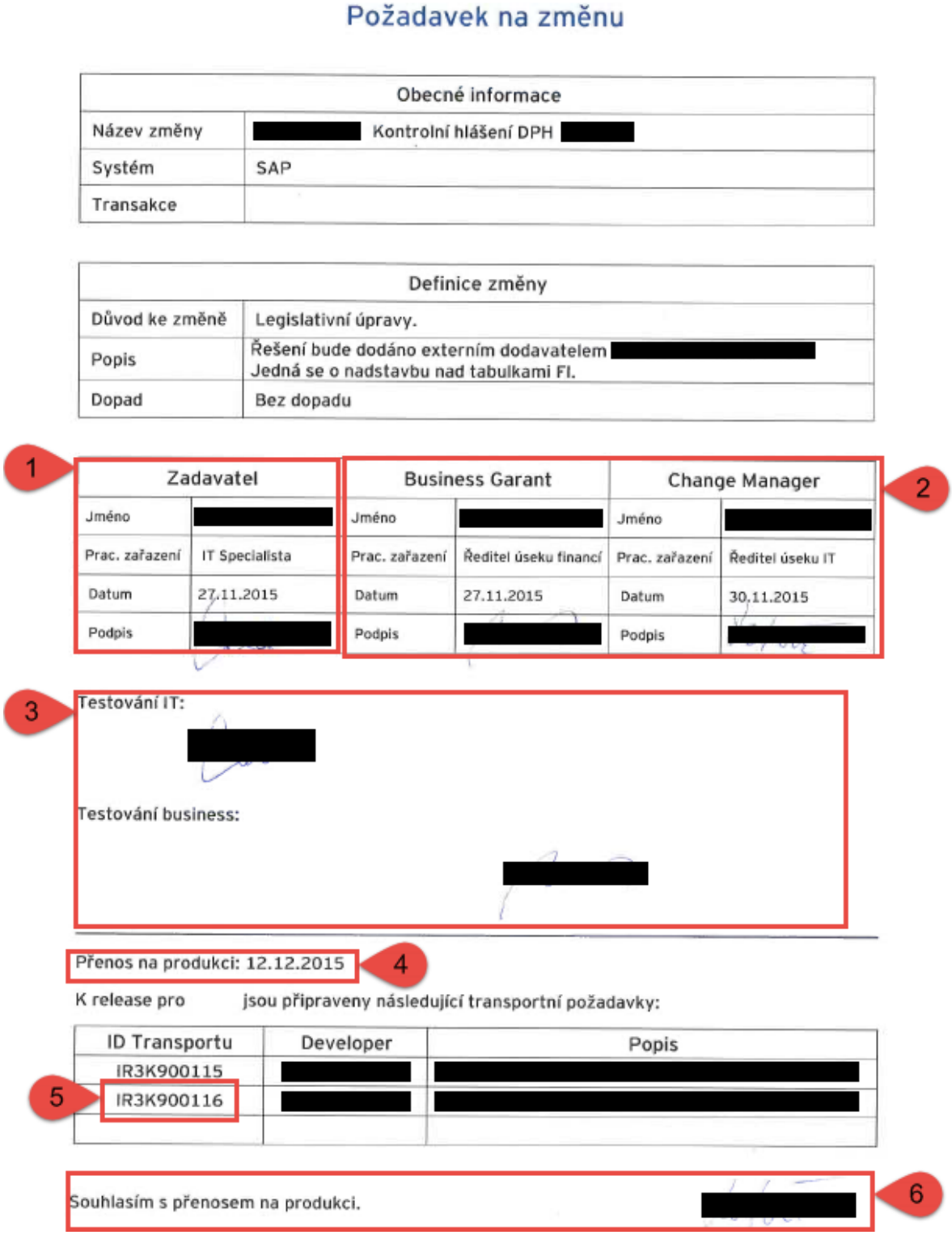
3 - Změna byla otestována jak za IT tak za byznys. Za IT to byl IT specialista, který změnu vyžádal. Za byznys byla změna otestována ředitelem úseku financí, který se nacházel v pozici byznys vlastníka procesu.

4 - Datum nasazení do produkce byl určen na 12. 12. 2015.

5 - ID transportu sedí s ID vybraným v systému.

6 - Nasazení do produkce bylo schváleno ředitelem IT úseku.

Obrázek 6.6: Změnový protokol pro transport IR3K900116



Požadavek na změnu

Obecné informace	
Název změny	[redacted] Kontrolní hlášení DPH [redacted]
Systém	SAP
Transakce	

Definice změny	
Důvod ke změně	Legislativní úpravy.
Popis	Řešení bude dodáno externím dodavatelem [redacted] Jedná se o nadstavbu nad tabulkami FI.
Dopad	Bez dopadu

1

Zadavatel	
Jméno	[redacted]
Prac. zařazení	IT Specialista
Datum	27.11.2015
Podpis	[redacted]

Business Garant	
Jméno	[redacted]
Prac. zařazení	Ředitel úseku financí
Datum	27.11.2015
Podpis	[redacted]

Change Manager	
Jméno	[redacted]
Prac. zařazení	Ředitel úseku IT
Datum	30.11.2015
Podpis	[redacted]

2

3 Testování IT: [redacted]

Testování business: [redacted]

Přenos na produkci: 12.12.2015 4

K release pro jsou připraveny následující transportní požadavky:

ID Transportu	Developer	Popis
IR3K900115	[redacted]	[redacted]
5 IR3K900116	[redacted]	[redacted]

Souhlasím s přenosem na produkci. [redacted] 6

Zdroj: Vlastní tvorba

V ověřeném procesu fungovala správně segregace rolí i kontrola čtyř očí. Při této kontrole jsou dva schvalovatelé a tím pádem nemůže dojít k situaci, kdy by zaměstnanec změnu sám vyžádal i schválil.

Shrnutí

Proces změnového řízení byl v souladu s interními politikami společnosti a good practice.

6.4.3 IT operace

Riziko

1. Problémy s hardwarem nebo softwarem mohou vést ke ztrátě dat.

2. Problémy s naplánovanými úlohami, které nedoběhly ke zdárnému výsledku, nejsou řešeny nebo jsou řešeny nevhodně.

Ověření

Zálohování systému ve společnosti probíhá na produkční i vývojové databázi, file serverech, AD a dalších částech, které jsou mimo rámec testování.

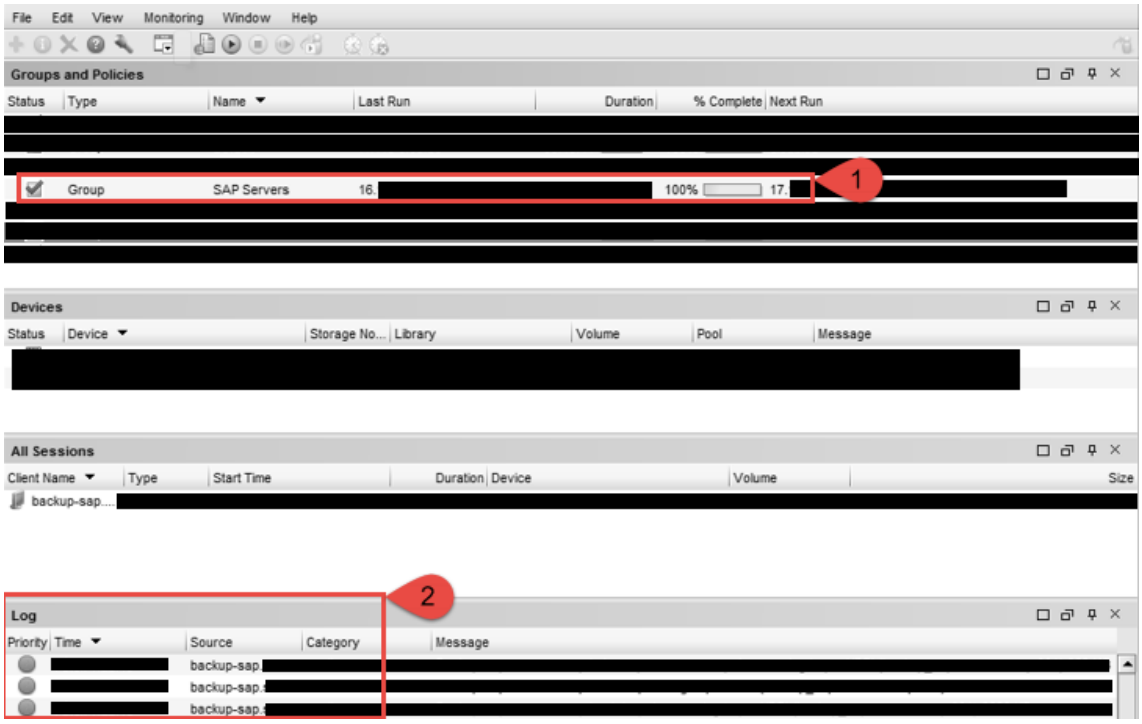
Automatický proces zálohování databáze je nastaven na každý den od 0:00 do 5:00. zálohy se ukládají na separátní zálohovací server, který se nachází v jiné budově než produkční systém. Ze zálohovacího serveru jsou následně zálohy přesouvány na pásky a poté transportovány do trezoru v bance kde jsou uschovány po dva roky.

Jednou měsíčně je otestována funkcionalita nahrání systému ze zálohy.

Nad celým procesem zálohováním běží monitorovací nástroj, který hlídá úspěšnost automatických procesů zálohování. V případě neúspěšné zálohy posílá email na relevantní IT administrátory.

Na obrázku 6.7 je možné vidět ověření, že zálohování probíhá denně a že je daný proces logován.

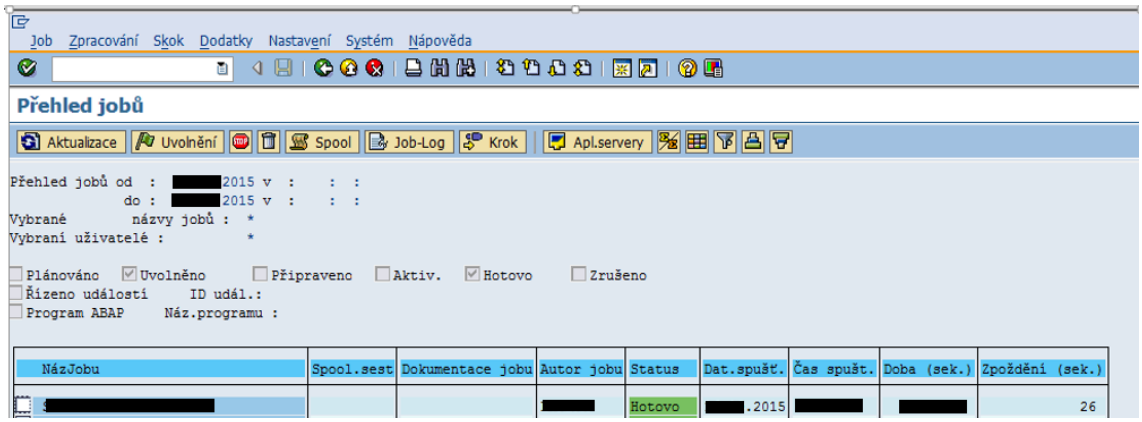
Obrázek 6.7: Ověření zálohování



Zdroj: Vlastní tvorba

Automatické systémové úlohy (dále joby) v systému SAP jsou nastavovány v transakci SE37 (obrázek 6.8). Monitoring nad těmito joby je prováděn administrátory systému. Ve výpisu je možné vidět název jobu, autora jobu, datum a čas spuštění, dobu trvání a zpoždění a status zdali job pořád běží, byl dokončen, případně jestli selhal.

Obrázek 6.8: Printscreen transakce SE37



Zdroj: Vlastní tvorba

Joby, které selhaly, je možné taky ověřit v transakci ST22. Jednou týdně je také administrátorům zasílán EWA neboli (EarlyWatchAlert) report.

Shrnutí

Proces zálohování a monitorování byl v souladu s interními politikami společnosti a good practice.

6.5 Ověření fyzické bezpečnosti

Servery jsou uloženy v centrále společnosti. Pro ověření fyzické bezpečnosti jsme se zaměřili na několik faktorů:

- přístup neoprávněných osob,
- protipožární ochrana,
- výpadek elektrického proudu.

Přístup do serverové místnosti byl zabezpečený čtečkou čipových karet a čtyřmístným PIN kódem. Seznam zaměstnanců s povoleným přístupem do místnosti jsem zkontroloval spolu s odpovědnou osobou a také jsem ověřil, že pracovní pozice osob s přístupem do serverovny, tomu odpovídají. Všichni zaměstnanci s přístupem pracovali na pozici IS specialista nebo IT architekt. V místnosti se také nacházela kniha návštěv pro zapisování prezence ostatních osob (např. auditor), které vstoupily do místnosti s osobou oprávněnou pro vstup. Zapisování, vchod do místnosti i místnost jako taková byla monitorována kamerovým systémem nepřetržitě 24/7. V případě, že by byly dveře otevřeny déle, než 20 vteřin je automaticky spuštěn tichý alarm, kterým je informována ostraha budovy.

Po místnosti byly rozmístěny teplotní senzory a 8 samostatných klimatizací, které měli za úkol regulovat teplotu. Na stropech a v dvojité podlaze byly umístěny požární a kouřové detektory. Pro případné hašení byl v místnosti automatický hasící systém s inertním plynem a jako doplněk se v místnosti i před ní nacházel práškový hasicí přístroj. Zdi místnosti byly vymalovány protipožární barvou a dveře byly také protipožární. V případě jakéhokoliv poplachu (požárního/bezpečnostního) jsou odpovědné osoby okamžitě informovány.

V případě výpadku elektrického proudu byly v serverovně umístěny tři samostatné záložní zdroje UPS (Uninterruptible Power Supply (Source)), z toho dva pro servery a jeden pro zabezpečení místnosti. Záložní zdroje neustále monitorují napájení serverů a v případě potřeby začnou automaticky napájet servery. V takovýchto případech je vždy

informován přes SMS odpovědný IT specialista. Pro větší výpadek elektřiny je v areálu budovy umístěn dieselový agregát, který je jednou ročně testován a kontrolován externí firmou způsobem plné zátěže. Interně je dieselový agregát testovaný jednou za dva týdny.

6.6 Ověřené operačního a databázového systémů

Před ověřením aplikace SAP jsem nejdříve ověřil infrastrukturu, na které byl systém postavený. Jak již bylo zmíněno výše v praktické části, jednalo se o operační systém Red Hat Enterprise Linux a databázi Oracle.

6.6.1 Ověření operačního systému Red Hat Enterprise Linux

Riziko

1. Účty se silnějšími oprávněními než ty, které jsou potřebné k výkonu pracovní funkce, zvyšují riziko, že na základě chybně uděleného neoprávněného přístupu na vysoké úrovni bude mít uživatel přístup do systémových zdrojů nebo k citlivým informacím.
2. Umožnění přímého přihlášení k účtu Root přes vzdálenou relaci zvyšuje riziko, že účet Root bude hlavním cílem v útoku na systém. Pokud je Root účet kompromitovaný, okamžitě poskytuje útočníkovi plnou kontrolu nad systémem. Při umožněném přístupu je také mnohem obtížnější identifikovat a sledovat události v systému.
3. File Transfer Protocol (FTP) předává uživatelovo data pře síť ve formátu prostého textu. Použití FTP účtem root nebo systémovými uživateli zvyšuje riziko, že jejich hesla jsou zachycené neoprávněným jedincem.
4. Použití nekomplexního hesla zvyšuje riziko útočníka získávat neautorizovaný přístup k informačním aktivům společnosti. Nedostatečná složitost hesla je jedním z nejběžnějších mechanismů jak může být ohrožen účet s použitím běžně dostupných nástrojů prolomení hesla.
5. Chybné nastavení anebo vypnutí exspirace hesla v pravidelných cyklech zvyšuje riziko úspěšnosti útoku Brute force, jehož výsledkem by bylo získání neoprávněného přístupu k informačním aktivům společnosti. Kromě toho, existuje

zvýšené nebezpečí, že v průběhu použití hesla bude toto postupně známo více uživatelům.

6. Umožnění znovupoužití stejného hesla oslabuje kontrolu exspirace hesla. Neschopnost udržet nastavení historie hesla zvyšuje riziko, že útočník získá neautorizovaný přístup k informačním aktivům společnosti.
7. Neschopnost ukládat hesla v šifrované podobě zvyšuje riziko jejich zneužití nebo zpřístupnění nepovolenému jedinci a může vést k neoprávněnému přístupu.

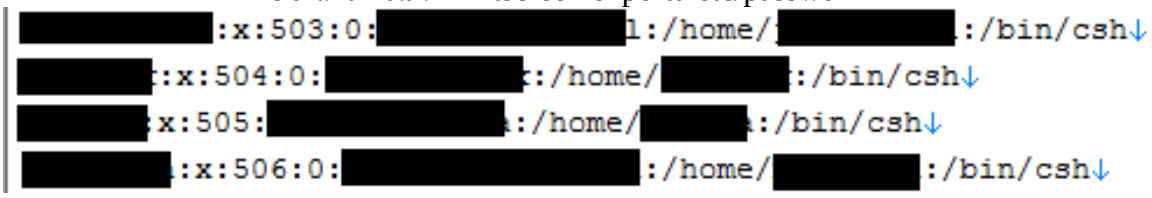
Testování

V souboru etc/passwd bylo otestováno, že žádný uživatelský účet nemá UserID < 100. Z obecných nepsaných standardů se tak zvyknou z důvodu přehlednosti označovat účty v závislosti na konfigurační soubor. V exportu bylo identifikováno 43 účtů, ze kterých byly jenom čtyři uživatelské. Zbylé účty byly technické. Všechny uživatelské účty měli UserID větší než 100.

Při testování účtů byl zohledněn také sloupec "Shell". V případě, kdy má účet hodnotu "nologin" tak se na daný účet není možné přihlásit. Na obrázku 6.9 je část exportu souboru etc/passwd s uživatelskými účtu v následujícím tvaru:

'Name:Password:UserID:PrincipleGroup:Gecos: HomeDirectory:Shell'

Obrázek 6.9: Printscreen exportu etc/passwd



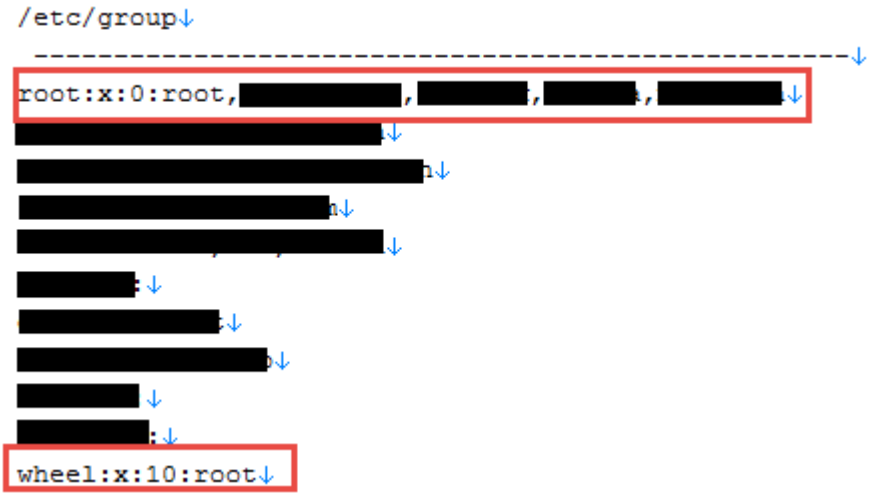
Zdroj: Vlastní tvorba

V souboru etc/group bylo otestováno, že jenom oprávnění uživatelé jsou přiřazeny v administrátorských skupinách. Na obrázku 6.10 je možné vidět, že ve skupině root byly další čtyři uživatelské účty. Ve všech případech se jednalo o IT administrátory a jejich přístup byl oprávněn. Další důležité skupiny již obsahovaly jenom technické účty. Také bylo ověřeno, že účet root je ve skupině wheel a tedy je možné se naň přehlásit z jiného účtu.

Export souboru etc/group byl ve tvaru:

Name:Password:UserID:User1,User2,...,User'

Obrázek 6.10: Printscreen exportu etc/group



Zdroj: Vlastní tvorba

V souboru etc/security/access.conf bylo ověřeno, že je možné se přihlásit na účet root jenom z lokální stanice. Nastavení "wheel login" vypadalo následovně.

 # Disallow non-local logins to privileged accounts (group wheel).

-:wheel:ALL EXCEPT LOCAL .win.tue.nl

Otestování nastavení v souboru etc/ssh/sshd_config je možné vidět v následující tabulce 6.4. Nastavení pro přímé přihlášení na root bylo zakomentováno a tím pádem byla tato část kódu nefunkční. Dále byla v souboru otestována také verze SSH. Zjistil jsem, že se jednalo o Protokol 2 a tím pádem se jednalo o aktuální verzi protokolu. Maximální doba na přihlášení než se spojení uzavře, byla nastavena na dvě minuty. Na závěr jsem ověřil maximální počet neúspěšných pokusů. Zhodnocení je znázorněno v tabulce 6.4.

Tabulka 6.4: Otestování vybraných parametrů z konfiguračního souboru etc/ssh/sshd_config

Hodnota v souboru	**Zhodnocení**
#PermitRootLogin yes	**Efektivní**
Protokol 2	**Efektivní**
LoginGraceTime 2m	**Efektivní**
MaxAuthTries 6	**Efektivní**

Zdroj: Vlastní tvorba

Dále bylo ověřeno, že pro přihlášení na root se musí uživatele nejdříve přihlásit na svůj účet a až následně pomocí příkazu “su“ se můžou přehlášení na účet root.

Na základě výpisu běžících služeb na OS jsem ověřil, že služba FTP(file transfer protocol) je vypnutá.

Heslová politika na OS byla ověřována pomocí více souborů jako /etc/login.defs , etc/pam.d/system-auth , ls -l /etc/opasswd , ls -l /etc/shadow , ls -l /etc/passwd.

Minimální délka hesla byla nastavená na 5 znaků. Platnost hesla byla nastavena na nekonečno.

PASS_MIN_LEN 5

PASS_MAX_DAYS 99999

PASS_MIN_DAYS 0

Síla hesla byla částečně pokryta modulem “cracklib“, který zajišťuje bezpečný výběr hesla po jeho resetu. Délka hesla byla nastavena na osm znaků.

password requisite pam_cracklib.so try_first_pass retry=3 minlen=8 dcredit=0 lcredit=0 ucredit=0 type=

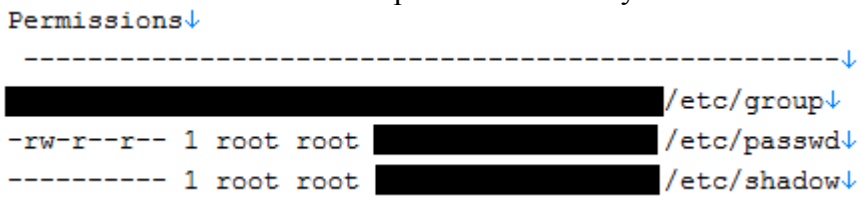
Pamatování předchozích hesel bylo na OS vypnuto.

Jak již bylo možné vidět v exportu etc/passwd, ve sloupci “Password“ měli všichni uživatelé “x“. Z toho vyplývá, že hesla jsou ve složce Shadow ve tvaru hashe.

Dále bylo ověřeno, že použitý hash uložený v souboru shadow začínal na “6“ a tím pádem hash funkce SHA-512, což se považuje za bezpečné. V případě, že by se jednalo o hash funkci MD5, bylo by to bráno jako neefektivní.

Na obrázku 6.11 je možné vidět nastavení přístupu ke složkám shadow a passwd.

Obrázek 6.11: Printscreen nastavení oprávnění na složky etc/shadow a etc/passwd



Zdroj: Vlastní tvorba

Složka byla vlastněna účtem root a oprávnění zapisovat má ve složce pouze vlastník. Skupiny a ostatní můžou složku jenom číst. Na složku shadow neměl nikdo přístup ani na čtení.

Základní bezpečností balík "SELinux" (security enchanted linux) je povolen a běží v systému.

Dále byl zkontrolován soubor "access.conf", ve kterém bylo ověřeno, že tam nebyl nadefinován uživatel nebo skupina jako administrátor, bez toho aniž by se to zobrazilo kdekoliv jinde.

Shrnutí

Všechny administrátorské účty jsou vyžadovány a aktivní.

Přístup k systémovému účtu root je možný jedině po přihlášení na individuální uživatelský účet a následné přehlášením na root.

FTP v systému není povoleno.

Systém vyžaduje komplexní osmi znakové heslo.

Uživatelé nemají systémově vynuceno měnění hesel v určitém časovém cyklu.

Systém neudržuje historii hesel a tím pádem může být heslo recyklováno dokola.

Heslo jsou uložena v zašifrované podobě ve složce shadow.

Nastavení je až na několik nedostatků, které budou zmíněny v doporučeních v souladu s good practice.

6.6.2 Ověření databázového systému Oracle

Riziko

1. Neoprávněním uživatelům jsou udělena klíčové administrátorská oprávnění. Neoprávněné pokusy o přístup nejsou zjistitelné a tím pádem nejsou řešeny vedením.
2. Konfigurace bezpečnosti a hesla nejsou optimalizovány tak, aby se zabránilo neoprávněnému přístupu. Neoprávněným uživatelům jsou uděleny přístupy k

informačním aktivům společnosti, včetně přístupu k citlivým nastavením a kmenovým datům.

Ověření

Z tabulky "DBA_USERS_WITH_DEFPWD"bylo zjištěno, že tři účty mají původní přednastavené heslo.

Obrázek 6.12: Printscreen exportu tabulky DBA_USERS_WITH_DEFPWD

[Query] : SELECT * FROM DBA_USERS_WITH_DEFPWD

USERNAME
[redacted]P
[redacted]DCM
[redacted]YS

Zdroj: Vlastní tvorba

Následně bylo v tabulce DBA_USERS ověřeno, zda-li jsou tyto účty aktivní. Na obrázku 6.13 je možné vidět, že všechny tři účty exspirovaly a byly zablokovány.

Export tabulky DBA_USERS byl ve tvaru:

USERNAME | USER_ID | PASSWORD | **ACCOUNT_STATUS**

Obrázek 6.13: Printscreen export tabulky DBA_USERS

[redacted]SYS	[redacted]		EXPIRED & LOCKED
[redacted]DCM	[redacted]		EXPIRED & LOCKED
[redacted]P	[redacted]		EXPIRED & LOCKED

Zdroj: Vlastní tvorba

Dále bylo identifikováno pět administrátorských účtů. Jeden účet byl využívaný administrátorem databáze a jeho přístup byl oprávněný. Další účty nebyly využívány uživateli. Jednalo se dva technické účty SAPu a dva technické účty databáze.

Na databázi byl kromě výchozího profilu identifikován ještě další profil pro technické SAP účty. Při testování heslové politiky byl tento profil vynechán. Důvodem je, že například pravidelné resetovaní hesla by u technických účtů mohl být problém (např. nefungovaly by automatické přenosy dat, které se pod těmito účty provádějí).

Výchozí profil měl nastavenou minimální délku hesla na osm znaků. Také bylo vynuceno, aby heslo bylo složené ze speciálních znaků, čísel atd. Životnost hesla byla

nastavená na 180 dní. Maximum neúspěšných pokusů o přihlášení před zablokováním účtu, byl nastaven na deset pokusů. Znovupoužití neboli recyklování hesla nebylo v systémových nastaveních zakázáno.

Systémové funkce auditování (logování aktivit uživatelů) jako “audit_sys_operations“ a “audit_trail“ byly vypnuty.

Shrnutí

Administrátorská oprávnění byla přidělena pouze vhodným účtům.

Na základě vypnutého auditování není možné zjistit pokusy o neoprávněné přihlášení.

Pro přihlášení je vyžadováno komplexní heslo o délce osmi znaků.

Limit pro neúspěšný počet přihlášení je nastaven.

Životnost hesla je nastavená na 180 dní.

Znovu použití hesla je povoleno.

Nastavení je až na několik nedostatků, které budou zmíněny v doporučeních v souladu s good practice.

6.7 Ověření SAP

Riziko

1. Konfigurace bezpečnosti a hesla nejsou optimalizovány tak, aby se zabránilo neoprávněnému přístupu do systému.

2. Neoprávněním uživatelům jsou uděleny přístupy k informačním aktivům společnosti, včetně přístupu k citlivým nastavením a kmenovým datům.

3. Účty se silnějšími oprávněními než ty, které jsou potřebné k výkonu pracovní funkce, zvyšují riziko, že na základě chybně uděleného neoprávněného přístupu na vysoké úrovni bude mít uživatel přístup do systémových zdrojů nebo k citlivým informacím.

Ověření

Na úvod testování jsem ověřil nastavení vynucení hesla v systému, kde byly skoro všechny parametry nastaveny na 0. Jak už ale bylo zmíněno v kapitole Řízení přístupů, přihlašování do aplikace funguje na principu Single-Sign-On. Tím pádem je zabezpečení přihlašování pokryto nastavením heslové politiky v doméně.

Nastavení systému bylo testováno na exportech tabulek T000 a T001 vyexportovaných přes transakci SE16. Ověřeno bylo nastavení následujících parametrů zobrazených v tabulce 6.5.

Tabulka 6.5: Testování nastavení z tabulek T000 a T001

Parametr	Good Practice (popis)	Hodnota v SAP	Zhodnocení
CCCATEGORY	"P" (productive)	P	**Efektivní**
CCNOCLIIND	"3" (změny nejsou povoleny)	3	**Efektivní**
CCCOPYLOCK	"X" (produkční klient nemůže být přepsán kopií klienta)	X	**Efektivní**
CCCORACTIV	"2" (žádné změny povoleny)	2	**Efektivní**
XPROD	"X" nebo "L" (nastaven produkční status relevantní pro auditování)	X	**Efektivní**

Zdroj: Vlastní tvorba

U exportu reportu “rsparam“ ověřena následující nastavení zobrazena v tabulce 6.6.

Tabulka 6.6: Testování nastavení z reportu RSPARAM

Parametr	Good Practice (popis)	Hodnota v SAP	Zhodnocení
rec/client	"ALL" anebo produkční klient "číslo" (logování změn je povoleno)	ALL	**Efektivní**
auth/no_check_on_tcode	"NO" – původní hodnota (TCODE je kontrolován při běhu transakce)	Blank	**Efektivní**
login/no_automatic_user_sap*	"1" – původní hodnota (smazaný uživatelé SAP* nebudou obnoveni s výchozím heslem)	1	**Efektivní**

Zdroj: Vlastní tvorba

V reportu RSUSR003 vygenerovaném pomocí transakce SA38 byly ověřeny výchozí systémové účty za účelem, zdali na účtech není nastavené původní heslo. Jednalo se o účty jako například sys, system, ddic, sap* atd. U všech účtů byla v kolonce Password Status nastavena hodnota "Exists; Password not trivial". Takovéto nastavení je považováno v souladu s good practice.

Dále bylo v transakci SE16 a tabulce USR02 otestována hodnota UFLAG. Tato hodnota určuje zamčení/odemčení daného účtu. Základní možné hodnoty je vidět v následující tabulce 6.7.

Tabulka 6.7: Základní hodnoty UFLAG v systému SAP

UFLAG	Popis
0	odemknutý účet
32	uzamčený účet administrátorem centrálně
64	uzamčený účet administrátorem
128	účet uzamčen systémem

Zdroj: Vlastní tvorba

Při testování účtu SAP* jsem zjistil, že byla nastavena hodnota UFLAG = 0. Toto nastavení se neslučovalo s dobrou praxí a zvyšovalo se tím riziko, že mohl být tento účet zneužit. Abych zjistil, zda mohl být účet v auditní periodě zneužit, zkontroloval jsem z dostupných informací (kolonky lastlogon) údaj o posledním přihlášení účtu do systému. Ověřil jsem, že se na daný účet nikdo nepřihlásil už několik let.

Následně jsem otestoval účty s profilem SAP_ALL. Na základě tohoto profilu jsou oprávnění jednotlivých účtů na úrovni plného oprávnění. V tabulce USR02 bylo nalezeno dvanáct účtů se jmenovaným profilem. Šest účtu bylo identifikováno jako technické/systémové účty, avšak ne všechny účty byly blokovány. Zbylých šest byly uživatelské účty. Na základě schůzky s aplikačním manažerem a dotazování na jednotlivé účty bylo zjištěno, že dva z účtů patří externímu dodavateli a zbylé čtyři účty byly zaměstnanců společnosti z oddělení IT.

Je důležité, aby do určitých kritických transakcí v systému SAP měly přístup jenom oprávněné osoby. Jako kritické, byly identifikovány následující transakce:

SE16 / SE16N – správa tabulek, přímý přístup k informacím v tabulkách

SM30 / SM31 – přímý přístup k informacím v tabulkách

SCC4 – administrace klienta

SA38 – spouštění programů

SE38 – přístup ke zdrojovým kódům programů s možností změny

SU01 – správa uživatelů

SU03 – správa autorizací

PFCG – konfigurátor profilů

SE09 / SE10 / SE01 – organizér transportů

Přístup do výše zmíněných transakcí byl zjištěn u více uživatelských účtů. V následující tabulce je vyhodnocena přiměřenost přístupů jednotlivých uživatelských účtů, vzhledem k jejich pracovní pozici. Jména uživatelských účtů byla z důvodu anonymizace v tabulce 6.8 pozměněna.

Tabulka 6.8: Otestování přístupů uživatelů k citlivým transakcím

		Uživatelské účty							
		U1	U2	U3	U4	U5	U6	U7	U8
Transakce	SE16	X	X	X	X	X	X	X	X
	SE16N	X	X	X	X	X			
	SM30	X	X	X	X	X	X		
	SM31	X	X	X	X	X			
	SCC4	X	X	X	X	X			
	SA38	X	X	X	X	X	X		
	SE38	X	X	X	X	X			
	SU01	X	X	X	X	X			
	SU03	X	X	X	X	X			
	PFCG	X	X	X	X	X			
	SE09	X	X	X	X	X			
	SE10	X	X	X	X	X			
	SE01	X	X	X	X	X			
Zařazení		Default	IT	IT	IT	IT	Finanční ředitel *	Reporting**	Referent ***
Zhodnocení		**Efektivní**	**Efektivní**	**Efektivní**	**Efektivní**	**Efektivní**	**Efektivní**	**Efektivní**	**Neefektivní**

Zdroj: Vlastní tvorba

* Na základě vysvětlení byznys potřeby aplikačním manažerem byl přístup akceptovatelný.

** Na základě vysvětlení byznys potřeby aplikačním manažerem byl přístup akceptovatelný.

*** Referent měl dané oprávnění na transakci jenom na dočasné bázi, avšak po uplynutí doby, kdy danou transakci využíval mu nebylo oprávnění odebráno. Spolu s administrátorem aplikace jsem ověřil, že v době když už mělo být oprávnění odebráno, uživatel danou transakci nepoužil.

Shrnutí

Ne všechny technické účty byly zablokovány.

Na produkčním prostředí byly objeveny dva odemčené účty externího dodavatele.

U jednoho uživatele bylo identifikováno nevhodné oprávnění na transakci, kterou však za daný čas nepoužil.

Nastavení je až na několik nedostatků, které budou zmíněny v doporučeních v souladu s good practice.

.

6.8 Zhodnocení ověření a doporučení

Při ověření byly objeveny pouze nedostatky s nízkou prioritou, jejichž kombinace nijak významně neohrožují systém. Na základě toho bych mohl finančnímu auditu oznámit, že nastavení rizikových systémů společnosti je v souladu s good practice i jejich interními politikami. Dále bych jim předal doporučení na změny, které by byly po ukončení finančního auditu diskutovány s vedením společnosti.

Doporučení pro IT procesy

Doporučují u heslové politiky změnit nastavení parametru "doba uzamčení účtu" na doméně alespoň na 30min. Dále doporučuji nastavit na doméně minimální stáří hesla na 1 a více.

Doporučení Red Hat

Doporučuji nastavení vynucení změny hesla v časovém intervalu 60 dnů, avšak minimální hodnotu na 1 a také zapnout udržovaní historie hesel.

Doporučení Oracle DB

Doporučuji změnu nastavení vynucení změny hesla na časový interval 60 dnů, zapnout auditování "audit_sys_operations" a "audit_trail" a zakázat znovupoužití hesla alespoň s historií pěti hesel.

Doporučení SAP

Doporučuji změnit hodnotu UFLAG u technických účtů a výchozího účtu SAP na 64 tj. uzamknout účty. Přístup externích dodavatelů do produkčního systému by měl být hlídán a povolen vždy jenom na vyžádání s udáním důvodu. Také doporučuji uživateli U8 odebrat přistup do transakce SE16.

Závěr

Cílem diplomové práce bylo ověřit nastavení IT infrastruktury a procesů společnosti důležitých pro finanční audit. V praktické části byl nejdříve popsán plán auditu a vyžádání dokumentace potřebné pro ověření. Jako rizikový systém byl identifikován aplikační systém SAP a operační a databázový systém, na kterých daná aplikace běžela.

Jako první byly po prostudování interních politik společnosti ověřeny procesy společnosti, ke kterým bylo také několik schůzek. Nejdříve byl ověřen proces řízení přístupů a s tím související správa uživatelů. Poté následoval proces změnového řízení a IT operací. Všechny ověřované procesy byly až na pár malých nedostatků v souladu s interními politikami a good practice.

Po ověření procesů následovalo ověření infrastruktury, kde jsem postupoval metodou bottom-up neboli ze zdola nahoru. Nejdříve byla ověřena serverová místnost, ve které se nacházeli servery, na kterých byly všechny rizikové systému. Ověřena byla rizika neoprávněného přístupu, požární ochrany a výpadku elektrického proudu. Daná serverovna bez problémů splňovala všechno potřebné a v mnoha ohledech byla lépe zabezpečená, než je potřebné minimum. Následné byly dle stanovených rizik otestovány operační a databázový systém, ve kterých bylo dohromady objeveno pět nedostatků s nízkou prioritou, a tím pádem byly nastavení v systému prohlášeny jako efektivní.

Na závěr testování jsem ověřil nastavení a uživatele aplikace. Zde byl objeven jeden výrazný nález. Jeden z uživatelů měl přístup k rizikové transakci i po uplynutí jeho potřeby přístupu. Riziko jsem následně pokryl ověřením logu aktivity uživatele, kde jsem se ujistil, že za daný časový úsek tuto transakci nepoužil. Dalším nedostatkem byly otevřené účty externího dodavatele na produkčním systému. Správně by dané účty měly být uzamčeny a odemčeny jenom v případě pádného důvodu a schválení přístupu aplikačním manažerem. Riziko bylo pokryto SLA mezi společností a dodavatelem. K danému systému následovalo ještě doporučení o zablokování technických a výchozích účtů systému.

Největší přínos práce vidím v možnosti čtenáři přiblížit, jak IT část finančního auditu probíhá a jaké všechny činnosti obsahuje.

Na základě výše zmíněného se domnívám, že v úvodu stanovený cíl práce byl splněn.

Summary and keywords

Diploma thesis is about IT assurance as a part of financial audit support. The thesis is based on the fact that the reader will have basic knowledge about Information Technologies. It is separated in two bigger parts. First, theoretical part starts with general information about audit/assurance and IT audit/assurance. Through other part of theory I have described methodologies of IT audit, good practice and information system. In the second practical part I reviewed the policies and IT infrastructure of the company. As the first step I have made plan of the audit and after that I started with the test of IT processes. For the infrastructure I have used bottom-up method. It started with testing of server room and continued with testing and reviewing of operating, database and application system. In the general speaking conclusion of the audit was that the settings of processes and the systems are effective. However there were several small discrepancies in settings which were at the end of thesis recommended changes in the line with good practice.

IT audit, IT assurance, good practice, ITIL®, SAP

Seznam použité literatury

[1] GÁLA Libor, Podniková informatika, 2. přepracované a aktualizované vydání. Praha: Grada Publishing, 2009 ISBN 978-80-247-2615-1

[2] BASL, Josef; BLATÍČEK, Roman. Podnikové informační systémy: Podnik v informační společnosti. 2., výrazně přepracované a rozšířené vydání. Praha: Grada Publishing, 2008. 277 s. ISBN 978-80-247-2279-5

[3] SVATÁ Vlasta. Audit informačního systému. Praha: Professional publishing. 2011. 228s. ISBN 978-80-7431-034-8

[4] MALONE, T; WEDEMEYER, M. ITIL® V3 Foundation Complete Certification Kit: 2009 edition. Emereo Publishing. 2009. 186s. ISBN 978-1921573606

[5] ISACA® org. COBIT®5 for Assurance. USA: ISACA®. 2013. 318s. ISBN: 978-1604203394

[6] MAASSEN, André; GADATSCH Andreas; FRICK Detlev; SCHOENEN Markus. SAP R/3 Kompletní průvodce. Brno: Computer Press, a.s., 2007; ISBN 978-8025117507.

[7] HURST, Q.; NOWAK, D. Configuring SAP R/3 FI/CO. 1st ed., SYBEX. 2000. 846s. ISBN 0-7821-2597-2.

[8] ISACA® org. COBIT® 5 Framework. USA: ISACA®. 2012. 94s. ISBN 978-1604202373

[9] Zákon pro lidi.cz [online]. [cit. 2016-08-19] Dostupné z: http://www.zakonyprolidi.cz/cs/2014-334

[10] Certifikace CISA. [online]. [cit. 2016-08-19] Dostupné z: http://www.isaca.cz/cs/certifikace-cisa

[11] Vztah ITIL® a COBIT® [online]. [cit. 2016-08-19] Dostupné z: https://www.bestpractice.cz/cs/Best-practice/-ITSM-ITIL-/-Vztah-ITIL-a-dalsich-pristupu/Vztah-ITIL-a-CobiT.alej

[12] SAP R/3 informační systém. [online]. [cit. 2016-08-19] Dostupné z: http://www.itica.cz/sap-r3-informacni-system/

[13] Komora auditorů ČR , ISA 315 [online]. [cit. 2016-08-19] Dostupné z: http://www.kacr.cz/file/1716/ ISA%20315 _final.pdf

[14] Komora auditorů ČR , ISA 315 [online]. [cit. 2016-08-19] Dostupné z: http://www.kacr.cz/data/Metodika/Auditing/Handbook%202010/17_ISA%20330.pdf

[15] JURAJDOVÁ, Hana. Audit ve veřejném sektoru. [online]. [cit. 2016-08-19] Dostupné z: http://is.muni.cz/th/26482/esf_d/Disertacni_prace_k_velke_obhajobe_c.4.doc

[16] Windows password security policy and tools [online]. [cit. 2016-08-21] Dostupné z: http://www.computerweekly.com/tip/Windows-password-security-policy-and-tools

[17] Password special characters [online]. [cit. 2016-08-21] Dostupné z: https://www.owasp.org/index.php/Password_special_characters

[18] Password Policy [online]. [cit. 2016-08-21] Dostupné z: https://technet.microsoft.com/en-us/library/hh994572(v=ws.11).aspx

[19] Enforce password history [online]. [cit. 2016-08-21] Dostupné z: https://technet.microsoft.com/en-us/library/hh994571(v=ws.11).aspx

Seznam obrázků

Seznam tabulek