Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Audit informačních systémů

Daniel Pitín

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Daniel Pitín

Informatika

Název práce

Audit informačních systémů

Název anglicky

Information systems audit

Cíle práce

Hlavním cílem této práce bude zhodnocení nastavení informačních systémů, které mají vliv na finanční data či bezpečnost společnosti. Dílčím cílem této práce bude vytvoření doporučení, které povede ke zlepšení funkčnosti informačních systémů a eliminaci nalezených rizik.

Metodika

Metodika této práce bude založena na zpracování literární rešerše odborných a vědeckých knih a ověřených internetových zdrojů.

V praktické části bude zpracováno auditní testování vybraných systémů a na základě výsledků a po zvážení mitigačních faktorů budou vytvořenoy návrhy pro zlepšení funkčnosti informačních systémů..

Doporučený rozsah práce

40 stran

Klíčová slova

IT, IT audit, bezpečnost IT systémů, hodnocení IT systémů, případová studie

---

Doporučené zdroje informací

BASL, J. – BLAŽÍČEK, R. – ČESKÁ SPOLEČNOST PRO SYSTÉMOVOU INTEGRACI. *Podnikové informační systémy : podnik v informační společnosti.* Praha: Grada, 2008. ISBN 978-80-247-2279-5.

GÁLA, L. – POUR, J. – ŠEDIVÁ, Z. *Podniková informatika : počítačové aplikace v podnikové a mezipodnikové praxi.* Praha: Grada Publishing, 2015. ISBN 978-80-247-5457-4.

KAFKA, T. *Průvodce pro interní audit a risk management.* Praha: C.H. Beck, 2009. ISBN 978-80-7400-121-5.

SVATÁ, V. *Audit informačního systému.* Praha: Professional Publishing, 2011. ISBN 978-80-7431-034-8.

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

doc. Ing. Edita Šilerová, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 14. 7. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 27. 10. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 15. 03. 2023

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Audit informačních systémů" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15. 3. 2023 _____

Poděkování

Rád bych touto cestou poděkoval doc. Ing. Editě Šilerové, Ph.D. za vedení bakalářské práce, poskytnutí cenných rad a za ochotu a vstřícnost během tvorby této práce.

Dále bych rád poděkoval všem kolegům z práce za předání zkušeností v oblasti auditu IS a za jejich rady a motivaci při vytváření praktické části této práce.

Audit informačních systémů

Abstrakt

Bakalářská práce se v první kapitole teoretické části zaměřuje na obecnou teorii auditu, konkrétně na jeho definici, historii, druhy a na největší externí auditorské firmy. Druhá kapitola definuje audit informačních systémů, uvádí nejdůležitější standardy a regulace a popisuje metodiky a certifikace důležité pro audit IS.

Zbývající kapitoly mají podobu případové studie, na které je provedeno auditní testování vybraných systémů a aplikací a na základě jehož výsledků je vytvořeno doporučení pro zlepšení.

Teoretická část je prováděna na základě rešerše odborných a vědeckých knih a ověřených internetových zdrojů, jak v českém, tak v anglickém jazyce. Praktická část je provedena na případové studii, která je vytvořena na základě vlastních zkušeností z profese auditora IS. Součástí případové studie je popis a ukázka celého procesu auditu IS, včetně vyvození závěru a vytvoření doporučení.

Klíčová slova:

audit, audit informačních systémů, teorie auditu, teorie auditu informačních systémů, externí audit, ITAF, ISO, COBIT 2019, ITIL, certifikace pro IT audit, případová studie, auditní testování, doporučení pro zlepšení

Information systems audit

Abstract

In the first chapter of the theoretical part, the bachelor thesis focuses on the general theory of audit, specifically on its definition, history, types and the largest external audit firms. The second chapter defines information systems auditing, lists the most important standards and regulations and describes methodologies and certifications relevant to IS auditing.

The remaining chapters take the form of a case study where audit testing of selected systems and applications is performed and recommendations for improvement are made based on the results.

The theoretical part is conducted on the basis of a review of professional and scientific books and verified Internet sources, both in Czech and English. The practical part is carried out on a case study, which is created on the basis of own experience in the IS auditor profession. The case study includes a description and demonstration of the entire IS audit process, including drawing conclusions and making recommendations.

Keywords:

audit, information systems audit, audit theory, information systems audit theory, external audit, ITAF, ISO, COBIT 2019, ITIL, IT audit certification, case study, audit testing, recommendations for improvement

Obsah

1 Úvod

Tato bakalářská práce se věnuje problematice auditu informačních systémů, který je v současnosti nezbytnou součástí finančního auditu. Žijeme totiž v době, která díky rychle se rozvíjejícím technologiím vyžaduje po společnostech, které chtějí být úspěšné a konkurenceschopné, aby investovali do informačních systémů, které zefektivní přenos a využití jejich dat a usnadní komunikaci se zaměstnanci.

S inovacemi a se zaváděním informačních systémů však přichází i mnoho rizik jako je například nedostatečné zabezpečení dat apod.. K této kontrole slouží audit informačních systémů, který pomáhá potenciální rizika odhalovat a dává tak společnostem možnost přijmout opatření a rizika eliminovat.

Snahou této práce je poukázat na důležitost auditu informačních systémů a přiblížit čtenáři práci a každodenní agendu auditora. Hlavní cílem je zhodnocení nastavení informačních systémů, které mají vliv na finanční data či bezpečnost společnosti. Dílčím cílem je poté vytvoření doporučení, které povede ke zlepšení funkčnosti systémů a eliminaci nalezených rizik.

Metodika této práce je založena na rešerši odborných a vědeckých knih a ověřených internetových zdrojů, jak v českém, tak v anglickém jazyce.

Práce bude rozdělena na dvě hlavní části, a to na část teoretickou a část praktickou. Teoretická část bude obsahovat dvě kapitoly (Teorie auditu a Audit informačních systémů). V první kapitole bude audit definován, bude krátce přiblížena jeho historie, bude popsáno jeho rozdělení a budou představeny největší externí auditorské firmy. Ve druhé kapitole bude poté přiblížen audit informačních systémů – jeho definice, nejdůležitější standardy a regulace ovlivňující profesi auditu IS, jako je ITAF a ISO, metodiky auditu IS, konkrétně COBIT 2019 a ITIL, a certifikace pro IT audit.

Praktická část se bude zaměřovat na auditní testování vybraných systémů a aplikací, které bude provedeno na případové studii, a na jehož základě bude vytvořeno doporučení pro zlepšení.

2 Teorie auditu

2.1 Definice auditu

Pojem audit vznikl z latinského slova audire, které v doslovném překladu znamená naslouchat nebo poslouchat. Pokud bychom tento pojem hledali v anglickém slovníku, narazíme na definici auditu jako revizi či kontrolu. Samotná definice tohoto oboru je však obtížně definovatelná, jelikož existuje v mnoha interpretacích rozdílně. [1]

Jako příklad uvádím definici auditu Komory auditorů České republiky: „*Audit je ověřovací zakázkou, která znamená zakázku, v níž odborník vyjadřuje závěr s cílem zvýšit míru důvěry předpokládaných uživatelů jiných než odpovědná strana ohledně výsledku hodnocení či oceňování předmětu zakázky vůči daným kritériím*.“.[1]

Jiří Dvořáček ve své knize Interní audit a kontrola, definuje audit jako: „Systematický *proces objektivního získávání a vyhodnocování důkazů, týkajících se informací o ekonomických činnostech a událostech, s cílem zjistit míru souladu mezi těmito informacemi a stanovenými kritérii a sdělit výsledky zainteresovaným zájemcům.*“.[2]

Z výše uvedených definic je možné odvodit, že cílem a účelem provádění auditu je poskytnutí odborného a objektivního názoru na stav, spolehlivost, úplnost a pravdivost dat uváděných vedením firmy. [2]

2.2 Historie auditu

Prvotní náznaky auditu můžeme spatřit již při vzniku prvních civilizací, jeho historie a vznik je úzce spojen se vznikem samotného účetnictví a jeho výkazů. Pojem audit v dřívějších dobách se diametrálně liší od pojmu, který používáme dnes.

Primitivní formy auditu se začaly vyskytovat na území Indie, Babylonu, Mezopotámie a Egypta v období 1500 př. n. l., kde jeho hlavním cílem byla evidence a kontrola majetku. Nejstarší zmínky se nacházejí v tzv. Vedách a Arthasatře. Úloha tehdejších auditorů se od

---

[1] *Komora auditorů České republiky. (2012). Poslání a smysl auditu. Komora auditorů České republiky. Dostupné z: https://www.kacr.cz/poslani-a-smysl-auditu [cit. 04.08.2022]*

[2] *Dvořáček, Jiří. Interní audit a kontrola. 2. přeprac. a dopl. vyd. Praha: C.H. Beck, 2003. C.H. Beck pro praxi. ISBN 80-7179-805-3 [cit. 04.08.2022]*

těch dnešních lišila v tom, že nekontrolovali již vypracované výkazy, ale vedli samotnou evidenci o majetku vládců, kterou měli za úkol průběžně aktualizovat tzv. nasloucháním' informací, které jim byly ústně předávány, jelikož lidé v těchto dobách neuměli číst ani psát.

Když se přesuneme do Řecka a Říma do období 800 př. n. l., tak se k samotnému auditu přidal i audit veřejných účtů, který měl zabránit chybám a podvodům ze stran veřejných úředníků.

Dalším milníkem ve vývoji auditování se stalo období středověku, především v oblasti Velké Británie. Auditoři byli považováni za vysoce postavené a uznávané úředníky, kteří se zodpovídali hlavě státu. Do jejich kompetence spadalo prověřování účtů, které byly předkládány úředníky z jednotlivých hrabství. Zde se poprvé začal používat systém tzv. oddělení odpovědnosti, který spočíval v rozdělení úkolů a pravomocí mezi jednotlivé úředníky, což vedlo k větší přesnosti, správnosti a pravdivosti záznamů a chránilo před možnými podvody.

V průběhu průmyslové revoluce, konkrétně v roce 1844, vznikla ve Velké Británii první legislativní úprava auditu v zákonu o společnostech (Companies Act 1844) a zároveň v tomto období začaly vznikat organizace evidované státem. Tato legislativní úprava určila, že jeden či více akcionářů přezkoumává bilance organizací, které vytvářel ředitel dané společnosti. Díky tomuto právními ukotvení nabyli akcionáři práva ke kontrole účetních výkazů a ke kladení otázek směřujících k vedení a k zaměstnancům společnosti. Účetní výkazy a následná kontrola akcionářů byly vkládány do tzv. Registru akciových společností.

Podobný způsob převzaly na přelomu 19. a 20. století i další státy. Audit sloužil ke kontrole fungování společností a k předcházení potenciálních podvodů. Nejdříve se kontrolovaly veškeré operace, ale kvůli velkému množství dat se začaly používat výběrové vzorky.

Do této doby jsme hovořili pouze o finančním auditu, ale vznik auditu informačních systémů se datuje do 70. let minulého století. K jeho rozvoji došlo díky vzrůstajícímu využívání počítačových systémů, které sloužili k zachycování jednotlivých účetních operací. Smyslem auditu informačních systémů byla kontrola správného fungování jednotlivých aplikací, které zachycovaly účetní operace. V roce 1969 vznikla Asociace EDP (Electronic Data Processing) auditorů za účelem vytváření návodů, postupů a standardů. V této době také vznikl první obecný auditní software GAS (Generalized Audit Software) a v roce 1968 byla vydána publikace s názvem Auditing & EDP, kterou vytvořil American Institute of Certified Public Accountants (AICPA) ve spolupráci s auditorskými firmami. Jelikož byl ale audit

informačních systémů stále na samém počátku, neexistovalo mnoho dostupných informací a vzdělání v tomto oboru, tak byl tento typ auditu brán spíše jako forma umění než vědní disciplína.

V průběhu 80. a 90. let se však audit informačních systémů přetransformoval do vědní disciplíny a z Asociace EDP auditů se v roce 1994 stala organizace ISACA (Information Systems Audit and Control Association), která v dnešní době patří mezi nejvýznamnější mezinárodní organizaci. Byla vydána softwarová struktura COBIT, rámec finančních kontrol COSO a v roce 1998 byl založen IT Governance Institute.

Mezi lety 2000 – 2010 vyšlo na povrch několik finančních afér firem jako byl např. Enron, WorldCom nebo Parmalat, jejichž auditorské zprávy nenaznačovaly žádné pochybení ve vedení daných firem. V roce 2002 došlo k bankrotu společnosti Enron o jejíž audit se starala auditorská a poradenská firma Arthur Andersen, která byla považována za součást Velké pětky spolu s PricewaterhouseCoopers, Deloitte Touche, Ernst & Young a KMPG, které dnes známe jako Velká čtyřka. Firma Arthur Andersen byla donucena po skandálu ukončit svoji činnosti a již nikdy se nevrátila mezi renomované auditorské firmy. V reakci na skandály byl vydán v roce 2002 americký zákon SOX (Sarbanes-Oxley Act), který zpřísnil kontrolní systémy. O tři roky později, v roce 2005, byl vydán soubor praktik COBIT 4.

Od roku 2010 došlo k růstu využívání informačních technologií a začaly se vytvářet nové nástroje a formy auditu. V roce 2012 byl vydán COBIT 5.

Audit informačních systémů v České republice se dostal do povědomí v roce 1996. V roce 1997 byla zřízena pobočka ISACA Czech Republic Chapter (ISACA CRC), která se stará o samotný audit, chod, bezpečnost a kontrolu informačních systémů. V rámci certifikací je možné v České republice složit mezinárodní certifikační zkoušky CISA (Certified Information Systems Auditor), která zaručuje odbornost v dané oblasti.

Finanční audit byl nedílnou součástí života již od počátku prvních civilizací. Prošel si dlouhým vývojem. Od pouhého zapisování majetku se utvořil do podoby, v jaké ho známe dnes. Naopak význam auditu informačních systémů se začal prosazovat až v posledních několika letech. Díky rychlému rozvoji informačních technologií stále narůstá jeho důležitost. Společnost jako taková využívá informační technologie na každodenní bázi a stejně je tomu tak u firem. Audit informačních systémů se nebere již jako pouhé umění, ale jako důležitá součást kontroly fungování společností. [1][2]

2.3 Druhy auditu

2.3.1 Interní a externí audit

Základními druhy auditu jsou audit interní (dobrovolný) a audit externí (zákonný). Tyto dva druhy jsou často zaměňovány, nicméně jsou mezi nimi značné rozdíly. Externí audit se zaměřuje na správnost a pravdivost účetních výkazů a výročních zpráv, kdežto audit interní prověřuje vše, co je důležité pro správné fungování společnosti. [15]

2.3.1.1 Interní audit

Cílem interního auditu je hodnocení a následné zlepšování procesů v oblasti řízení rizik, kontroly a celkového vedení společnosti. Interní auditoři se zabývají zkoumáním veškerých systémů a operací, které jsou důležité pro správný chod společnosti. Jedná se tedy spíše o poradenskou funkci než o funkci kontrolní.

Auditoři mají za úkol prověřit, jestli jsou správně řízena rizika, zda fungují správně procesy a zda jsou dodržovány předepsané postupy. Tyto audity také vymezují oblasti, které je možné modernizovat nebo kde by bylo možné zvýšit efektivnost.

Interní audity se provádějí ve všech oblastech, kromě finanční kontroly a kontroly informačních systémů, se interní auditoři zabývají také např. dodavatelským řetězcem, organizační kulturou nebo také etikou a pověstí společnosti. Obecně řečeno, interní audit zasahuje do všech oblastí, které mají dopad na správní fungování společnosti.

Auditorské zprávy jsou předkládány vedení společnosti a poskytují nestranné a objektivní informace o chodu společnosti a doporučení na zlepšení a zvýšení efektivity. Tyto zprávy nejsou veřejně přístupné.

Interní audit se vyskytuje jak v sektoru veřejném, tak v sektoru soukromém a neziskovém. Audit mohou provádět interní zaměstnanci společnosti nebo prostřednictvím externího poskytovatele auditorských služeb. [15]

2.3.1.2 Externí audit

Úkolem externího auditu je objektivní a nestranná kontrola účetních výkazů a výročních zpráv. Externí audit zkoumá, zda účetní závěrka obsahuje pravdivé a nijak nezkreslené informace a zda jsou tyto informace v souladu s účetními standardy.

Externí audit je důležitý nejen pro vedení společnosti, ale také pro investory, kteří díky auditorské zprávě mohou posoudit zdraví a transparentnost společnosti a snížit tak riziko své investice.

Externí auditoři jsou jmenováni akcionáři společnosti a musí být zcela samostatní a nestranní, aby byla zajištěna objektivnost celé kontroly

Auditorská zpráva se řídí auditorskými standardy a obsahuje informace o tom, zda jsou finanční pravdivé a zda jsou v souladu s účetními standardy. Tyto zprávy jsou veřejně přístupné a jsou součástí ročních finančních výkazů. [16]

2.3.2 Další druhy auditu

Audit se nerozděluje pouze na audit interní a externí, ale může se zaměřovat na různé oblasti. Kromě auditu finančního a auditu informačních systému existuje také např. audit informační, ekologický, bezpečnostní, technický, manažerský, strategický, forenzní nebo energetický. V této kapitole bude popsán audit finanční, informační, ekologický a forenzní. Audit informačních systémů bude popsán samostatně ve čtvrté kapitole této práce.

2.3.2.1 Finanční audit

Nejvíce známým typem auditu je audit finanční. Jedná se o objektivní zhodnocení finančních výkazů společnosti. Tento audit prověřuje, zda jsou finanční výkazy pravdivé a zda odpovídají příslušným zákonům a standardům, jako jsou např. standardy ISA.

Finanční audit přezkoumává především majetek, závazky a výsledek hospodaření společnosti. Stejně jako u většiny auditů je výstupem auditorská zpráva, která obsahuje hodnocení a doporučení. Ke zhotovení auditorské zprávy využívá auditor stanovené postupy řídící se daným standardem.

Výsledek finančního auditu je důležitý zejména pro investory a akcionáře, kteří díky auditorským zprávám mohou posuzovat rizika své investice. [17]

2.3.2.2 Informační audit

Podstatou informačního auditu je prověřování informačních toků a zdrojů ve společnosti a zkoumání, jak společnost působí navenek.

Neexistuje přesná definice, ale jedná se především o interní vyšetřování, jež je podkladem pro sestavení nové strategie a hierarchie ve společnosti, především v případě změny vedení. [18]

2.3.2.3 Ekologický audit

Ekologický audit je audit, který se zabývá zkoumáním chování společnosti, jaký dopad má toto chování na životní prostředí a zda je v souladu s příslušnou legislativou. O ekologický audit žádají společnosti, které ve své firemní strategii mají zahrnutou environmentální etiku a dodržují např. ISO 14001 pro environmentální management, SA 8000 pro sociální otázky a OHSAS 18001 pro řízení ohrožení zdraví a bezpečnosti.

Výsledkem auditu je doporučení, v jaké oblasti by mohlo dojít ke zlepšení a případné upozornění na nesoulad s legislativou. [19]

2.3.2.4 Forenzní audit

Forenzní audit, také vyšetřovací audit, je vždy prováděn nezávislým auditorem. Jedná se o prozkoumání konkrétního případu a prošetřuje podezření na podvodné či protiprávní jednání.

Tento druh auditu může cílit na odkrývání účetních a majetkových podvodů, na odhalení korupce nebo na kontrolu transparentnosti veřejných zakázek.

Auditorská zpráva neobsahuje doporučení, ale slouží jako důkaz, který je určen soudu či vyšetřovacímu orgánu. [20]

2.4 Největší externí auditorské firmy

Mezi největší auditorské firmy dnes patří společnosti KPMG, PricewaterhouseCoopers (PWC), Ernst & Young a Deloitte. Tyto auditorské společnosti se sdružují pod jedním názvem, a to Velká čtyřka (Big Four). Velká čtyřka se zformovala z velké pětky, do které, kromě výše uvedených, patřila i auditorská a poradenská firma Arthur Andersen. Po bankrotu firmy Enron, ke kterému došlo v roce 2002, bylo proti Arthur Andersen vedeno několik soudních sporů, a přestože byla tato auditorská firma očištěna, již nikdy neobnovila své původní postavení. [1]

2.4.1 Arthur Andersen

Společnost Arthur Andersen byla založena v roce 1913 Arthurem E. Andersenem a v průběhu 90. letech se stala jednou z největších účetních a auditorských firem. Operovala v 84 zemích, kde zaměstnávala více než 85 000 zaměstnanců. Auditorská firma Arthur Andersen se starala o několik významných klientů, mezi něž patřily např. firmy Enron Corp. nebo WorldCom Inc.

Auditorská firma Arthur Andersen byla v červnu 2001 Komisí pro cenné papíry a burzu (SEC) upozorněna, že při jakémkoliv budoucím pochybení bude potrestána ministerstvem spravedlnosti. Toto upozornění společnost obdržela na základě odhalení účetního podvodu ve výši 1,43 miliardy USD ve společnosti Waste Management Inc. [3]

V roce 2001 však došlo k dalšímu skandálu, a to ve společnosti Enron. Enron, založená v roce 1985, byla významnou mezinárodní společností, která se zabývala výrobou elektřiny, zemního plynu a podnikala v oblasti komunikace a v papírenském průmyslu. V roce 2001 bylo odhaleno několik finančních a účetních podvodů, mezi něž patřil např. pokles akcií z 90 USD za akcii (polovina roku 2000) na méně než 1 USD na akcii (konec roku 2001). Tento pokles způsobil akcionářům ztrátu ve výši téměř 11 miliard USD. Po odhalení podvodů upadla společnost Enron 2. prosince 2001 do konkurzu. [4]

Auditorské zprávy společnosti Arthur Andersen neobsahovaly žádná upozornění na pochybné vedení účetnictví společnosti Enron, které by varovalo akcionáře před případnou ztrátou. Po oznámení provozní ztráty Enronu za třetí čtvrtletí požádala komise SEC o auditní informace. Vedení firmy Arthur Andersen však záměrně skartovalo velikou část dokumentace, která obsahovala informace týkající se společnosti Enron. Následně 14. března 2002 obvinilo ministerstvo spravedlnosti společnost Arthur Andersen z maření spravedlnosti. 15. června 2002 byla společnost shledána vinnou a byla jí odebrána licence k vedení veřejného účetnictví. V roce 2005 Nejvyšší soud Spojených států zrušil jednomyslně verdikt na základě chybných pokynů poroty, avšak společnost Arthur Andersen se již nevrátila ke své původní činnosti. [3]

2.4.2 KPMG

Společnost KMPG, která dnes patří mezi nejvýznamnější auditorské firmy, byla založena roku 1987 sloučením Peat Marwick International a Klynveld Main Goerdeler.

Písmena ve slově KMPG jsou odvozena od příjmení čtyř zakladatelů – William Barclay Peat, James Marwick, Piet Klynveld a Reinhard Goerdeler.

William Barclay Peat pracoval pro společnost Robert Fletcher & Co., ve které roku 1891 převzal vedení a následně společnost přejmenoval na William Barclay Poat & Co.

James Marwick a Roger Mitchell založili roku 1897 americkou firmu Marwick, Mitchell & Company, která měla sídlo v New Yorku.

V roce 1917 vybudoval Piet Klynveld malou účetní firmu se sídlem v Amsterdamu, která se později spojila do Klynveld Kraayenhof & Company a stala se největší účetní firmou v Nizozemsku.

Teprve až v roce 1953 zahájil svou kariéru čtvrtý a poslední zakladatel společnosti KMPG, který začal pracovat ve společnosti Deutsche Treuhand-Gesellschaft (DTG).

K první fúzi došlo v roce 1911, kdy se na plavbě po Atlantiku z Evropy do Ameriky setkal Peat a Mitchell a ze dvou společností vznikla společnost pod názvem Peat, Marwick, Mitchell & Co. V roce 1978 se společnost přejmenovala na Peat Marwick International (PMI). O rok později se Klynveld Kraayenhof & Company spojilo s DTG a McLintock Main Lafrentz a vznikla společnost Klynveld Main Goerdeler (KMG). Následně roku 1986 nastala největší fúze tehdejší doby, kdy se spojilo PMI a KMG a roku 1987 byla společnost přejmenována na Klynveld Peat Marwick Goerdeler (KPMG). [5]

V současné době operuje společnost KPMG ve 144 zemích světa a zaměstnává více než 236 000 lidí. V České republice pracuje pro KMPG více než 1000 zaměstnanců. [6]

2.4.3 PricewaterhouseCoopers (PWC)

Společnost PWC vznikla v roce 1998 fúzí společností Price Waterhouse a Coopers & Lybrand. V roce 1849 poté, co Anglie vydala zákony, které vyžadovaly prověřování finančních záznamů společností, si Samuel Lowell Price založil vlastní účetní firmu. Dále se jako obchodní partneři přidali roku 1865 William Hopkins Holyland a Edwin Waterhouse a společnost se přejmenovala na Price, Holyland, & Waterhouse. Holyland však v roce 1874 společnost opustil a nadále fungovala pod jménem Price Waterhouse až do roku 1998, kdy došlo ke spojení s Coopers & Lybrand a vzniklo jméno, pod kterou známe tuto firmu dnes. PWC operuje ve 156 zemích a zaměstnává 295 000 lidí. [7]

Do Československa přišli společnosti Price Waterhouse a Coopers & Lybrand po pádu železné opony. Zaměstnává více než 1000 odborníků a má své kanceláře v Praze, Brně a Ostravě. [8]

2.4.4 Ernst & Young

Počátky vzniku společnosti Ernst & Young sahají do roku 1903, kdy se Alwyn C. a Theodore Ernst rozhodli otevřít svoji vlastní účetní firmu. O tři roky později však Theodore Ernst firmu opustil a v roce 1908 založil oddělení speciálních služeb v Clevelandu, kde nabízel poradenské služby. O rok později otevřel pobočky v New Yorku, Chicagu a několika dalších městech.

Během 20. let se firma rozrůstala a v roce 1923 Ernst uzavřel spolupráci se sirem Arthurem Whinneym a sirem Chasem Palmourem, kteří byli partnery britské účetní firmy Whinney, Murray & Co. V průběhu let vznikla mezinárodní pobočka Ernst & Ernst, která nesla název Whinney, Murray, Ernst & Ernst.

V roce 1979 došlo k vytvoření Ernst & Whinney Intl. Se sídlem v Clevelandu a kancelářemi v New Yorku. V roce 1989 došlo k dohodě s Arthurem Youngem a vznikla společnost známá jako Ernst & Young. [9]

Společnost Ernst & Young nabízí své služby ve 150 zemích a v České republice působí od roku 1991. Pro Ernst & Young Česká republika pracuje 1 100 zaměstnanců v kancelářích v Praze, Brně a Ostravě. [10]

2.4.5 Deloitte

Historie společnosti Deloitte začíná v roce 1845, kdy si William Welch Deloitte otevřel v Londýně svou vlastní kancelář. Deloitte byla první společnost, která byla pověřena provést nezávislý audit veřejné společnosti, konkrétně Great Western Railway. V roce 1880 došlo k otevření kanceláře v New Yorku, v roce 1890 otevření nové pobočky na Wall Street a dále následovalo Chicago a Buenos Aires.

Charles Waldo Haskins a Elijah Watt Sells založili v New Yorku roku 1896 společnost s názvem Haskins & Sells. O čtyři roky později vzniká v New Yorku také společnost Touche, Niven & Co.

V průběhu dalších desítek let docházelo ke slučování několika společností. Významným milníkem je rok 1972, kdy došlo ke sloučení firmy Deloitte s Haskins & Sells a vytvořila se společnost Deloitte Haskins & Sells. V roce 1989 poté došlo k fúzi Deloitte Haskins & Sells s Touche Ross a vznikla společnost Deloitte & Touche. Deloitte Haskins & Sells ve Velké Británii, v Nizozemsku a Touche Ross v Austrálii však toto sloučení odmítlo a později se spojilo s Coopers & Lybrand a vytvořilo Coopers & Lybrand Deloitte. [11]

Působení v České republice zahájila společnost Deloitte v roce 1990. Deloitte zaměstnává více než 1000 zaměstnanců, operuje v 5 kancelářích a má 33 partnerů. Kanceláře lze najít v Praze, Plzni, Brně, Ostravě a Hradci Králové. [12]

3 Audit informačních systémů

3.1 Definice auditu informačních systémů

Audit informačních systémů je v dnešní době definován a interpretován několika způsoby. Definice auditu IS vychází ze základní definice, která říká, že audit je věcná, nestranná a objektivní kontrola, která porovnává určitý stav s danou legislativou, zákony, normou, standardem nebo modelem.

V oficiálním slovníku pojmů vydaným institucí ISACA je audit definován takto: „Audit *je formální prověření a ověření za účelem kontroly, zda je dodržována norma nebo soubor pokynů a zda jsou záznamy přesné nebo jsou splněny cíle účinnosti a efektivity.*“.[3]

Audit IS může být obnáší stejné aspekty, jaké jiné druhy auditů, ale místo kontroly, např. účetních výkazů, se zabývá kontrolou a funkčností informačních systémů.

Ing. Vlasta Svatá CSc. definuje audit IS následovně: „*Audit informačního systému je specifický proces, který se zabývá posuzováním a poradenstvím objektů v prostředí, kde se používají informační technologie. Jeho cílem je kvalitativně a/nebo kvantitativně přispět ke správné organizaci informačního systému tak, aby byly splněny požadavky uživatelů, zákonů, smluv či jiných regulací (externích či interních). Objekty mohou být organizace a*

[3] *ISACA. Interactive Glossary & Term Translations. ISACA. Dostupné z: https://www.isaca.org/resources/glossary [cit. 10.08.2022]*

řízení IS, základní aplikační software, technické vybavení, telekomunikační systémy, procesy tvorby a údržby systémů, ochrana a bezpečnost systému, data (databáze) apod.‘‘.[4]

Ing. Zdeněk Vaněk uvádí definici auditu IS jako: „*Informační audit představuje jednorázovou prověrku, jejímž výsledkem je zjištění, jak ve skutečnosti funguje informatika v prověřovaných oblastech. Výsledný protokol informačního auditu je v současné době fakticky standardizován tak, aby vedoucím pracovníkům srozumitelnou formou poskytl verifikovanou informaci, jaké služby (za jakou cenou a s jakým rizikem) informatika poskytuje pro plnění hlavních činností organizace. Výsledek informačního auditu zpravidla navrhuje krátkodobá neinvestiční nápravná opatření a současně slouží jako základ pro formulaci dlouhodobých priorit a věcných cílů informační strategie.*‘‘.[5]

Jako třetí uvádím definici z Encyclopedia Britannica: „*Efektivita kontrol informačního systému je hodnocena prostřednictvím auditu informačních systémů. Cílem auditu je zjistit, zda informační systémy chrání podniková aktiva, udržují integritu uložených a sdělovaných dat, účinně podporují podnikové cíle a zda fungují efektivně. Je součástí obecnějšího finančního auditu, který ověřuje účetní záznamy a finanční výkazy organizace. Informační systémy jsou navrženy tak, aby bylo možné dohledat každou finanční transakci. Jinými slovy, musí existovat auditní záznam, který dokáže určit, kde každá transakce vznikla a jak byla zpracována. Kromě finančních auditů se provozní audity používají k hodnocení efektivity a efektivity provozu informačních systémů a technologické audity ověřují, že informační technologie jsou vhodně zvoleny, nastaveny a implementovány.*‘‘. [6]

Obecně lze audit IS charakterizovat jako rozšiřující prvek klasického auditu, který se ale s rozvojem informačních technologií stává nedílnou součástí kontroly fungování společnosti. Jeho cílem je kontrola, zda informační systémy podávají pravdivé a nezkreslené informace a zda jsou správně implementovány do chodu společnosti.

---

[4] *Svatá, Vlasta. Audit informačního systému. V Praze: Oeconomica, nakladatelství VŠE, 2016. ISBN 978-80-245-2168-8. [cit. 10.08.2022]*

[5] *Vaněk, Zdeněk. (nedatováno). Cíle a postup informačního auditu. Dostupné z: https://www.dcit.cz/papers/ISO_Cile_Auditu.pdf [cit. 10.08.2022]*

[6] *Encyclopedia Britannica. (2001). Information systems audit. Encyclopedia Britannica. Dostupné z: https://www.britannica.com/topic/information-system/Information-systems-audit [cit.10.08.2022]*

3.2 Nejdůležitější standardy a regulace ovlivňující profesi auditu IS

3.2.1 ITAF

První verze dokumentu ITAF (IT Audit Framework) byla vydána organizací ISACA v roce 2007 v návaznosti na požadavek sjednotit a zpřehlednit existující standardy týkající se profese auditu IT systémů. Od prvního vydání byl ITAF třikrát aktualizovaný a jeho nejaktuálnější verzí je nyní ITAF 4th edition, která byla vydána v roce 2020. Jedná se o jednu z nejobsáhlejších regulací v tomto oboru, jejíž aktualizování patří mezi nejvýznamnější činnosti společnosti ISACA.

Regulace v dokumentu ITAF se rozdělují na 3 hlavní úrovně, které se odvíjejí od stupně podrobnosti. Tyto úrovně jsou standardy, návody a nástroje a techniky. Mimo regulace obsahuje dokument ITAF také etický kodex auditora IS, kterým se musí řídit každý držitel certifikace od společnosti ISACA v tomto oboru.

3.2.1.1 Standardy

Standardy jsou nejméně podrobné regulace, které se dělí na 3 kategorie:

- obecné standardy (série 1000) – Tato sekce obsahuje detailní popis postupů v profesi IT assurance. Tyto principy jsou vyžadovány pro všechny auditní zakázky. Týkají se především profesní etiky, nezávislosti, objektivity, náležité péče na zakázce a také požadavků na dovednosti, znalosti a kompetence.
- výkonnostní standardy (série 1200) – Tato sekce se zabývá postupem a průběhem auditu, jako je například plánování, supervize a řízení zakázky, stanovení rozsahu, posouzení rizik, definice auditní evidence a uplatnění profesionálního úsudku.
- standardy pro reporting (série 1400) – Tato sekce se zaměřuje na popis typů auditních zpráv a jejich povinného obsahu, náležité komunikace s klienty a prezentace výsledků auditu.

3.2.1.2 Návody

Návody jsou podrobněji popsané postupy na uplatňování povinných standardů při realizaci auditu IS. Tato úroveň se také dělí na tři kategorie podle toho, ke kterému typu standardů se vztahuje:

- obecné návody (série 2000),
- výkonnostní návody (série 2200),
- návody pro reporting (série 2400).

3.2.1.3 Nástroje a techniky

Nástroje a techniky jsou nejpodrobněji popsané pokyny pro řešení nejčastějších problému při auditních zakázkách, které vycházení z reálných příkladů z minulosti. Skládá se například z tzv. white papers, programy pro auditu a assurance, referenčních knih a dokumentů COBIT 5. [1] [21]

3.2.2 Standardy ISO

Mezinárodní organizace ISO (International Organization for Standardization) vznikla oficiálně v únoru roku 1947 spojením organizací ISA (International Federation of the National Standardizing Associations) a UNSCC (United Nations Standards Coordinating Committee). Sídlo organizace ISO se nachází od roku 1949 ve švýcarské Ženevě. Tato organizace se zabývá hlavně vytvářením, sjednocením a aktualizací mezinárodních norem a standardů. Pro profesi auditora IS existují dvě stěžejní oblasti standardů od společnosti ISO a těmi jsou: standardy bezpečnosti informací a standardy kvality IT/IS. [1] [22]

3.2.2.1 Standardy bezpečnosti informací

První sada norem ISO/IEC 27000 týkající se bezpečnosti informací a jejich řízením byla vydána organizací ISO roku 2005 ve snaze o sjednocení a zpřehlednění několika standardů/norem, které vedly k neefektivnímu nasazení postupů v organizacích, jež se jimi řídily. Tato sada norem je průběžně doplňována a aktualizována. Byl zde také zaveden systém ISMS (Information Security Management Systems), který eliminuje rizika ztráty či poškození informačních aktiv pomocí implementace bezpečnostních opatření a jejich pravidelné kontrole efektivity. Ze sady norem ISO/IEC 27000 jsou nejdůležitější tyto standardy/normy:

- ISO/IEC 27001 – Tato norma obsahuje popis, jak vytvořit, implementovat, provozovat, monitorovat, kontrolovat a neustále zlepšovat ISMS. Vznikla z druhé části standardu BS 7799, který byl vydán roku 1999 ministerstvem obchodu a průmyslu Spojeného království. Poslední verze normy byla vydána v roce 2022 a

největší změny proběhly v dodatku A kvůli sjednocení s novou verzí ISO/IEC 27002, která byla vydána dříve stejného roku. Detaily o změnách spojených s normou ISO/IEC 27002 budou popsány v následující kapitole.

- ISO/IEC 27002 – Aktuální verze této normy z února 2022 obsahuje popis 93 bezpečnostních kontrol, které jsou členěny do čtyř kategorií:
    - organizační kontroly (obsahuje 37 kontrol),
    - kontroly lidských zdrojů (obsahuje 8 kontrol),
    - kontroly fyzické bezpečnosti (obsahuje 14 kontrol),
    - technologické kontroly (obsahuje 34 kontrol).

  Oproti předešlé verzi normy z roku 2013 se nová verze liší hlavně větší přehledností (nově jsou kontroly dělené do čtyř kategorií oproti původním čtrnácti), menším počtem kontrol (mnoho kontrol se spojilo) a v drobných změnách povinných klauzulí jako např. nová norma na identifikaci IT procesů a jejich interakcí, požadavek na dokumentování všech provedených změn atd. Oproti minulé verzi také obsahuje jedenáct nových kontrol. [1] [23] [24]

- ISO/IEC 27006 – Tato norma je určena převážně pro akreditované třetí strany, které udělují certifikace ISMS nebo provádějí audit společnosti, která se řídí sadou norem ISO/EIC 27000. [1] [25]

3.2.2.2 Standardy kvality IT/IS

Pro zhodnocení kvality IS jsou nejdůležitější následující sady ISO norem:

- ISO 9000 (Obecné normy pro řízení a zajištění kvality) – Sada norem ISO 9000 definuje standardy tzv. Quality management Systems (QMS), které pomáhají společnostem zajistit kvalitu jejich výrobků či služeb, kterou vyžadují zákazníci. Tato sada norem však není přímo věnována kvalitě IS, ale jedná se spíše o obecné ustanovení, které vyžaduje dokumentaci jednotlivých procesů v certifikované firmě a ujišťuje o pravidelné kontrole těchto procesů, nikoliv však o jejich bezchybnosti. [1] [26]
- ISO/IEC 15504 (Hodnocení zralosti procesu) – Normy ze sady ISO/IEC 15504 se zaměřují primárně na hodnocení zralosti procesů od roku 2004, kdy byla od této sady oddělena norma ISO 12207, která se zaměřuje na životní cyklus SW. Od této doby lze sadu norem ISO/IEC 15504 používat univerzálně pro posouzení všech procesů

v rámci auditované organizace, a nikoliv pouze pro procesy vývoje softwaru. Procesy jsou v této sadě norem rozděleny do pěti kategorií: zákazník-dodavatel, inženýrství, podpora, řízení a organizace. Tato sada norem také definuje tzv. úrovně zralosti, které jsou rozděleny na 6 úrovní (0 – neúplné procesy až 5 – optimalizované procesy). [1] [27]

- ISO/IEC 12207 (Procesy v životním cyklu softwaru) – Jak již bylo naznačeno v předchozí části, norma ISO/IEC 12207 se zaměřuje především na procesy v životním cyklu softwaru, jejich kontrolu a vylepšování. Tyto procesy jsou dále členěné do tří kategorií na:
    - primární procesy – mezi primární procesy se řadí následující procesy životního cyklu SW: nákup, dodání, vývoj, provozování, správa a likvidace,
    - podpůrné procesy – mezi podpůrné procesy se řadí následující procesy životního cyklu SW: dokumentace, řízení konfigurace, řízení kvality, verifikace, validace, revize a audit,
    - organizační procesy – mezi organizační procesy se řadí: řízení, zajištění infrastruktury, optimalizace, školení.

  Kromě výše zmíněných procesů tato norma také definuje organizační role odpovědné za jednotlivé procesy jako jsou např.: nakupující, dodavatel, vývojář, provozovatel a správce. [1] [28]

- ISO/IEC 19770 (Správa softwarových aktiv) – Tato norma se zabývá převážně procesy a technologiemi pro správu softwarových aktiv v organizacích. Největší přínos této normy pro organizace spočívá v doporučených směrnicích, které pomáhají snížit náklady, redukovat rizika porušování autorských práv a zvýšit efektivnost rozhodování při nákupu softwarových aktiv. [1] [29]
- ISO 25000 (Požadavky a hodnocení kvality systémů a softwaru) – Sada norem ISO 25000 je většinou označována svou zkratkou SQuaRE, která vznikla z anglického názvu Software Quality Requirements and Evaluation. Tyto normy se zaměřují na vytvoření směrnic pro hodnocení kvality SW produktů a důvod jejich vzniku je podobný jako u ostatních sad ISO norem – nepřehlednost a nejednotnost standardů, které se dříve problematikou zabývaly. Tato sada se svou strukturou rozděluje na pět divizí:
    - divize řízení kvality,

- divize kvality modelu,
- divize měření kvality,
- divize požadavků kvality,
- divize hodnocení kvality.

Mimo jiné jsou zde také definovány tři druhy kvality, které jsou mezi sebou vztahově provázané:

- vnitřní kvalita SW – kvalita vestavěných vlastností softwaru,
- vnější kvalita SW – kvalita výpočetního systému aplikace,
- kvalita užití SW – kvalita softwaru z hlediska uživatelů a nastavených podnikových procesů. [1] [30]

3.3 Metodiky auditu informačních systémů

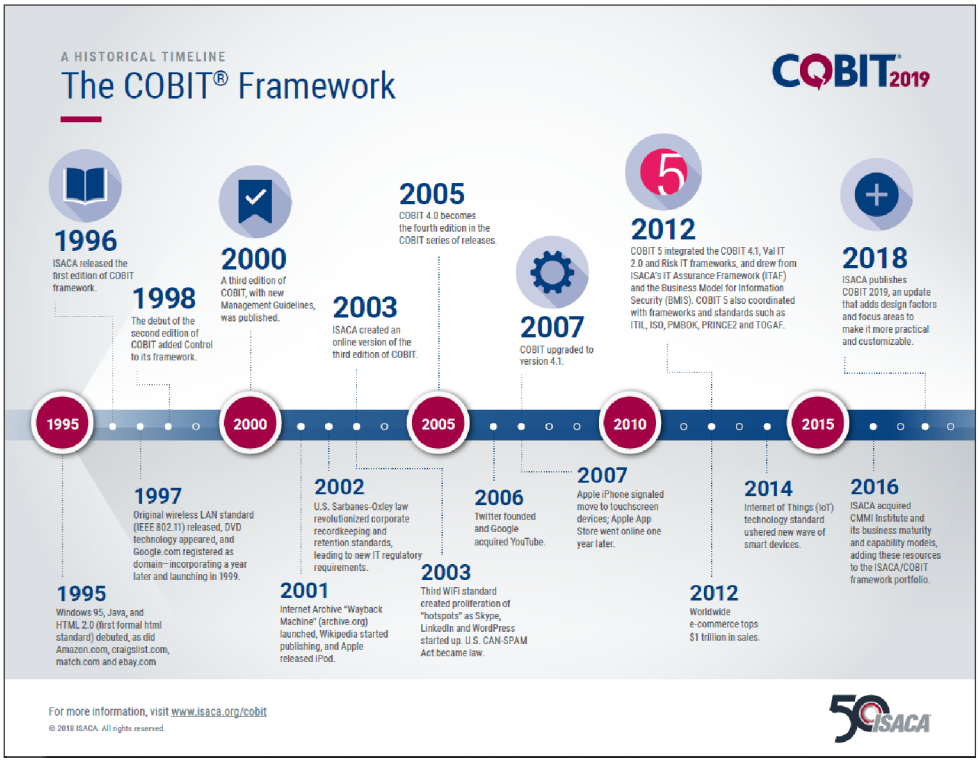
V této kapitole budou popsány důležité metodiky pro audit IS, které slouží k posouzení účinnosti a efektivity IT procesů a zároveň slouží jako návod pro dodržení souladu se standardy, kterými se auditovaná společnost řídí. Mimo jiné jsou metodiky velmi důležité pro správnou identifikaci rizik a nedostatků v IT procesech včetně následného návrhu na zlepšení procesů či zmírnění rizika, které přestavují. Mezi nejdůležitější metodiky z tohoto oboru se řadí zejména rámce COBIT (Control Objectives for Information and Related Technology) a ITIL (Information Technology Infrastructure Library), jejichž aktuální verze budou popsány v této kapitole.

3.3.1 COBIT 2019

COBIT (Control Objectives for Information and Related Technology) je mezinárodně uznávaný rámec pro správu IT, který poskytuje metodiku a dobrou praxi (good practice) pro řízení IT v organizacích. Jedná se o rozsáhlý framework, který popisuje metody a postupy pro řízení IT, správu IT procesů, řízení rizik a Governance. Pro profesi auditora IS je COBIT důležitým dokumentem, protože definuje rámec pro provádění IT auditu, definuje IT procesy důležité pro poskytování služeb v IT a určuje kritické kontroly těchto procesů, které by měly být implementovány pro zajištění účinnosti a efektivity. [31]

První dokument COBIT vznikl v roce 1996 pod křídly společnosti ISACA, která tento rámec vytvořila ve snaze o zefektivnění a sjednocení řízení IT v organizacích podle aktuálních

standardů. Od svého vzniku byl dokument několikrát aktualizovaný až do své nynější podoby COBIT 2019. [32] Detailní vývoj této metodiky je více popsaný na obrázku č. 1.



Obrázek 1- Historie frameworku COBIT do roku 2018

Zdroj: ISACA [33]

3.3.1.1 Hlavní rozdíly mezi COBIT 2019 a COBIT 5

Z důvodu velkého objemu informací obsažených ve frameworku COBIT jsem se rozhodl zdůraznit pouze rozdíly, které s sebou přinesla poslední verze dokumentu, protože tyto rozdíly nejsou z pouhého vývoje metodiky na obrázku č. 1 viditelné.

č. rozdílu	COBIT 5	COBIT 2019
1	Řídí se pěti principy Governance	Řídí se šesti principy Governance
2	Rámec pro 37 procesů	Rámec pro 40 procesů
3	Principy rámce Governance nejsou přítomny	Obsahuje principy rámce Governance
4	Hodnocení zralosti procesů je založeno na standardu ISO/IEC 33000, který používá stupnici 0-5	Hodnocení zralosti procesů je založeno na CMMI (Stupňovitý model zralosti)
5	Obsahuje aktivátory (enablers)	Aktivátory (enablers) byly aktualizované a přejmenované na komponenty
6	Neobsahuje designové faktory procesů	Byly přidány designové faktory procesů

Tabulka 1- Hlavní rozdíly COBIT 5 x COBIT 2019

Zdroj: vlastní zpracování podle ISACA [34]

Rozdíl 1

Nejnovější verze dokumentu COBIT 2019 se nově řídí šesti principy IT Governance místo pěti, které byly využívány v COBIT 5. Tyto principy slouží pro zajištění posouzení a odsouhlasení potřeb zainteresovaných stran ve vztahu k cílům podniku. Pro lepší představu o změně jsem jednotlivé definice z obou dokumentů shrnul do tabulky níže. [34]

č. principu	COBIT 5	COBIT 2019
1	Uspokojení potřeb zainteresovaných skupin	Poskytnutí hodnoty pro zainteresované skupiny
2	End-to-end pokrytí podniku	Podpora holistického přístupu
3	Aplikace jednoho integrovaného rámce	Zavedení dynamického Governance systému
4	Podpora holistického přístupu	Oddělení úrovně Governance od úrovně řízení (Management)
5	Oddělení úrovně Governance od úrovně řízení (Management)	Přizpůsobení potřebám organizace
6		End-to-end pokrytí podniku

Tabulka 2- Rozdíly v principech IT Governance
Zdroj: Vlastní tvorba

Rozdíl 2

Definované procesy se v COBIT 2019 oproti verzi COBIT 5 rozšířily o tři nové definice pro procesy ze skupin APO (Align, Plan and Organize), BAI (In Build, Aquire and Implement) a MEA (In Monitor, Evaluate and Assess).

Managed Data (APO14)

Hlavním cílem tohoto nového procesu je vytvořit systematickou a organizovanou metodu pro správu dat a zajištění jejich kvality v celé organizaci. Tento proces pokrývá všechny fáze životního cyklu dat jako například jejich tvorbu a získávání, jejich uchovávání a používání až po jejich likvidaci.

Managed Projects (BAI11)

Tento nový proces se zaměřuje na plánování, přidělování zdrojů a monitorování projektů v průběhu jejich životního cyklu, aby bylo zajištěno jejich úspěšné dokončení v rámci stanoveného rozpočtu a časového harmonogramu a zároveň byla zajištěna jejich kvalita dle definovaných standardů.

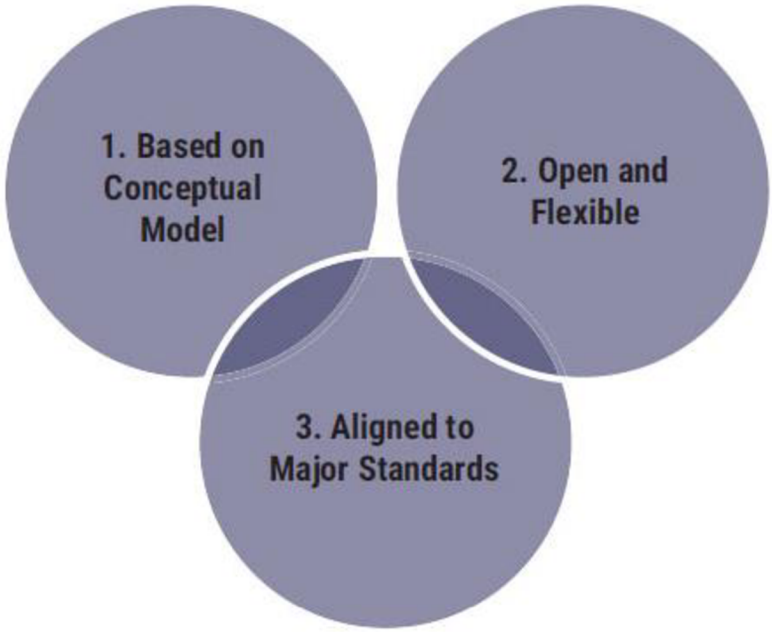
Managed Assurance (MEA04)

Cílem procesu Managed Assurance je zajistit, aby funkce IT assurance byla řízena s co největší účinností a efektivitou. Tohoto cíle se snaží dosáhnout pomocí definic pro

plánovaní, provádění a reportování auditních kontrol, které hodnotí účinnost IT systémů a jejich procesů.

Rozdíl 3

Do COBIT 2019 byly nově zavedeny principy z rámce Governance, které jsou znázorněné na obrázku č. 2.



Obrázek 2- Principy Governance
Zdroj: ISACA [34]

První princip zahrnuje koncepční model, který identifikuje klíčové komponenty, včetně jednotlivých vztahů mezi nimi, s cílem umožnit jejich automatizaci.

Druhý princip, který klade důraz na otevřenost a flexibilitu se vztahuje hlavně na to, že model může zahrnovat nový obsah a může se přizpůsobovat novým problémům při zachování konzistence a spolehlivosti výsledků.

Třetí princip poukazuje na to, že by model měl být vždy v souladu s hlavními normami, standardy a regulacemi.

Rozdíl 4

Dokument COBIT 2019 využívá k měření úrovně zralosti procesů model CMMI (Stupňovitý model zralosti) oproti své starší verzi, která pro tuto činnost používala model ze standardu ISO/IEC 33000. CMMI model byl v nové verzi zvolen nejspíše kvůli tomu, že pokrývá hodnocení širší oblasti činností organizace, mezi které patří například softwarové a

systémové inženýrství, řízení projektů, zatímco ISO/IEC 33000 se zaměřuje hlavně na softwarové inženýrství. [34] Detailní rozdíly mezi jednotlivými stupni zralosti procesů ve verzích COBIT 5 a COBIT 2019 jsou dále popsány na obrázku č. 3.

Obrázek 3- Rozdíly v hodnocení vyspělosti procesů
Zdroj: ISACA [34]

Rozdíl 5

Rámec COBIT 5 představil aktivátory (enablers) jako novou součást modelu správy a řízení, které se týkají především faktorů ovlivňujících implementaci a následné provádění procesů z tohoto modelu. Mezi aktivátory se řadí principy, politiky a rámce, procesy, organizační struktury, kultura, etika, chování, informace, služby, infrastruktura, aplikace, lidé, dovednosti a kompetence.

COBIT 2019 oproti své starší verzi využívá pro stejné faktory název komponenty (components). [34]

Rozdíl 6

COBIT byl ve své nejnovější verzi rozšířen o tzn. designové faktory (design factors), které slouží k implementaci rámce COBIT pro společnosti všech velikostí a druhů. Jelikož má každá společnost své jedinečné charakteristiky a požadavky, musí se i rámec COBIT přizpůsobovat těmto potřebám. Designové faktory zohledňují potřeby zainteresovaných stran, poslání, vize a cíle společnosti, ale také podnikové procesy, organizační struktury,

využívané technologie a styl řízení společnosti. Díky těmto faktorům je možné rámec COBIT aplikovat a vytěžit z něj přínos pro chod organizace. [34] [35] Jednotlivé designové faktory, které byly představeny v COBIT 2019 jsou znázorněny na obrázku č. 4.

Obrázek 4 - Designové faktory COBIT 2019
Zdroj: ISACA [34]

3.3.2 ITIL

IT Infrastructure Library (ITIL) je framework týkající se řízení IT služeb a je klíčovou metodikou IT Service Managementu (ITSM). Byl vytvořen Centrální počítačovou a telekomunikační agenturou (CCTA) ve Velké Británii v 80. letech 20. století a od roku 2013 je vlastněn společností Axelos. Slouží k řízení rizika, zavádění nákladově efektivních postupů a ke stabilizaci IT prostředí. Jedná se o tzv. sadu best practice, což je soubor ověřených metod, které jsou obecně uznávané jako nejlepší.

ITIL byl v průběhu let několikrát revidován a zužován. Ve svých začátcích se skládal ze 30 knih a v roce 2000, kdy byl vydán ITIL V2, byl zúžen na sedm. V roce 2007, v rámci projektu ITIL Refresh, vyšel v pěti knihách ITIL V3, který byl následně v roce 2011 aktualizován a pojmenován jako verze ITIL 2011. Nejaktuálnější verzí je ITIL 4 z roku 2019. [36]

ITIL 4 klade důraz na větší spolupráci, usnadnění komunikace v organizaci a integraci agilních a DevOps strategií do ITSM. Je více flexibilní a podporuje holistický přístup k IT prostředí.

Důležitou součástí ITIL 4 je sedm zásad, které byly převzaty z ITIL Practitioner. Tyto zásady jsou univerzální, lze je aplikovat na kteroukoli společnost a poskytují dlouhodobou pomoc. Mezi tyto zásady patří:

- zaměřte se na hodnotu (focus on value),
- začněte tam, kde jste (start where you are),
- postupujte iterativně se zpětnou vazbou (progress iteratively with feedback),
- spolupracujte a podporujte viditelnost (collaborate and promote visibility),
- myslete a pracujte holisticky (think and work holistically),
- udržujte jednoduchost a praktičnost (keep it simple and practical),
- optimalizujte a automatizujte (optimize and automate).

Významným prvkem ITIL 4 Service Value System (SVS) jsou také techniky řízení. Řídící postup se dá popsat jako soubor organizačních prostředků, které jsou využívané k dosažení cíle. Mezi nejdůležitější praktiky řízení patří:

- obecné praktiky řízení (general management practices),
- praktiky řízení služeb (service management practices),
- technické praktiky řízení (technical management practices).

Obecné praktiky řízení jsou univerzální postupy, které lze využít napříč celou organizací. Slouží k zajištění úspěchu společnosti a poskytovaných služeb. Obecné praktiky řízení zahrnují čtrnáct oblastí, mezi něž patří řízení talentované pracovní síly, vztahů, bezpečnosti informací, architektury, znalostí, organizačních změn, portfolia, strategie, projektů, dodavatelů, rizik, finanční řízení služeb, neustálé zlepšování a měření a podávání zpráv.

Praktiky řízení služeb jsou spojeny s vývojem, zaváděním, poskytováním a podporou služeb v organizaci. Spadá pod ně sedmnáct okruhů, kterými jsou správa prostředků IT, problémů, katalogu služeb, požadavků na služby, incidentů, úrovně služeb, dostupnosti, vydání, konfigurace služby, umožnění změn, analýza podnikání, ověřování a testování služeb, Service Desk, monitorování a správa událostí, návrh služby, řízení kontinuity služeb a kapacity a výkonu.

Mezi technické praktiky řízení patří vývoj a správa softwaru, řízení nasazení a správa infrastruktury a platforem. [37]

3.4 Certifikace pro IT audit

Profesní certifikace v oboru IT auditu jsou poskytovány třemi typy institucí a to konkrétně:

- mezinárodní instituce,
- národní instituce,

- podnikové instituce.

Hlavní mezinárodní institucí zabezpečující profesní kvalifikace v oblasti auditu informačních systémů je již zmíněná instituce ISACA ® (Information Systems Audit and Control Association). Tato instituce se orientuje převážně na oblast auditu, řízení, kontroly a bezpečnosti informačních systémů. Společnost ISACA vznikla v roce 1969 v USA původně jako sdružení EDP (Electronic Data Processing) auditorů. V současné době pod tuto organizaci spadá přes 165 000 certifikovaných odborníků ze 188 zemí. Momentálně poskytuje následující certifikační/vzdělávací programy:

- CISA (Certified Information Systems Auditor) – Je světově uznávanou certifikací v oblasti auditu, kontroly, monitoringu a posouzení podnikových informačních systémů. Momentálně tuto certifikaci vlastní přes 151 000 expertů. Certifikace CISA ujišťuje o expertíze držitelů v následujících oblastech:
  - proces auditu informačních systémů (21 %),
  - IT management a Governance (17 %),
  - pořízení, vývoj a implementace informačních systémů (12 %),
  - provoz informačních systémů a odolnost podnikání (23 %),
  - ochrana informačního majetku (27 %).
- CRISC (Certified in Risk and Information Systems Control) – Tato certifikace je určena k ověření zkušeností s budováním správně nadefinovaného agilního procesu řízení rizik a jeho následné správy. Certifikace CRICS se skládá z následujících oblastí:
  - Governance (26 %),
  - hodnocení rizik v IT (20 %),
  - reakce na rizika a jejich reporting (32 %),
  - informační technologie a bezpečnost (22 %).
- CISM (Certified Information Security Manager) – Tato certifikace je určena převážně pro manažery bezpečnosti informačních systémů, kteří složením zkoušky dokazují zkušenosti v oblastech jako je řízení bezpečnosti informací, vývoj a správa aplikací, management incidentů a řízení rizik. Certifikace CISM se skládá z následujících oblastí:
  - řízení informační bezpečnosti (17 %),
  - řízení rizik informační bezpečnosti (20 %),

- vývoj a správa programu informační bezpečnosti (33 %),
- řízení bezpečnostních incidentů (30 %).

- CGEIT (Certified in Governance of Enterprise IT) – Tato certifikace je určena především pro poradce a profesionály v odvětví IT Governance, které se zaměřuje zejména na velké mezinárodní organizace a zajišťuje zlepšení komunikace mezi IT odděleními, vyšším managementem a majiteli těchto společností. Certifikace CGEIT se skládá z následujících oblastí:
  - řízení IT v podniku (40 %),
  - plánování a optimalizace IT zdrojů (15 %),
  - realizace benefitů (26 %),
  - optimalizace rizik (19 %).
- CSX-P (Cybersecurity Practitioner Certification) – Tato výkonnostní certifikace testuje schopnosti profesionálů v pěti oblastech kybernetické bezpečnosti, které jsou odvozené od NIST (National Institue of Standards and Technology) frameworku. Je určena převážně pro odborníky v oboru, kteří získáním této certifikace ujišťují svého zaměstnavatele o praktických dovednostech v oboru kybernetické bezpečnosti. CSX-P se skládá z následujících oblastí:
  - obchodní a bezpečnostní prostředí (25 %),
  - připravenost provozního zabezpečení (25 %),
  - detekce a hodnocení hrozeb (25 %),
  - reakce na bezpečnostní incidenty (12,5 %),
  - obnova (zotavení) po bezpečnostním incidentu (12,5 %).
- CDPSE (Certified Data Privacy Solutions Engineer) – Tato certifikace se zaměřuje primárně na ověření technických dovedností a znalostí potřebných k implementaci a posouzení komplexních řešení pro ochranu osobních údajů. Je vhodná především pro profesionály, kteří se zabývají vytvářením a implementací řešení pro ochranu osobních údajů a datové analytiky, kteří těží a analyzují data za účelem získání dat o zákaznících. CDPSE se skládá z následujících oblastí:
  - řízení soukromí (33,3 %),
  - architektura ochrany osobních údajů (33,3 %),
  - životní cyklus dat (33,3 %).
- ITCA (Information Technology Certified Associate) – Tato certifikace je vhodná především pro studenty a čerstvé absolventy či pro kandidáty o práci v IT, kteří

nemají velké zkušenosti nebo hledají univerzální rekvalifikační IT kurz. ITCA se skládá z pěti samostatných certifikací v oblasti IT, po jejichž úspěšném složení dostane uchazeč certifikát ITCA. Jednotlivé oblasti zkoušek jsou následující:

- základy výpočetní techniky,
- základy sítí a infrastruktury,
- základy kybernetické bezpečnosti,
- základy vývoje softwaru,
- základy datových věd.

- CET (Certified in Emerging Technology Cerfitication) – Tato certifikace je vhodná pro každého, kdo si chce potvrdit svou odbornou znalost nových technologií v odvětvích IT auditu, hodnocení rizik, zabezpečení IT systémů, kybernetické bezpečnosti, správě a řízení v oboru IT, ochrany soukromí a rozvoje podnikání. Tato certifikace se skládá ze čtyř samostatných certifikací v oblasti IT, po jejichž úspěšném složení dostane uchazeč certifikát CET. Jednotlivé oblasti zkoušek jsou následující:
  - základy cloud computingu,
  - základy blockchainu,
  - základní principy IoT,
  - základy umělé inteligence (AI).

Mimo jiné společnost ISACA úzce spolupracuje s institucí IT Governance Institute, publikuje a doplňuje framework COBIT (aktuální verze 5), dokument ITAF (IT Assurance Framework) a pořádá konference a workshopy. [1] [13]

Další významnou organizací pro audit informačních systémů je Institut interních auditorů (The Institute of Internal Auditors Inc.), který byl založen v New Yorku v roce 1941 a dnes sídlí v Altamonte Springs ve státě Florida. V současné době pod tuto organizaci a její národní pobočky spadá více než 180 000 odborníků ve 190 zemích. V České republice služby této organizace zastřešuje od roku 1995 tzv. Český institut interních auditorů (CIIA), který čítá přes 1000 členů. Tato organizace podobně jako ISACA vydává profesní standardy a publikace v oblasti interního auditu, nabízí certifikaci interních auditorů (CIA – Certified Internal Auditor) a pořádá různé konference, semináře a workshopy. [1] [2] [14]

4 Případová studie (vlastní práce)

4.1 Vytvoření plánu auditu

Na začátku každého auditu je potřeba vytvořit plán, podle kterého se bude průběh auditu řídit. Následující plán pro provedení auditu IS ve fiktivní společnosti byl vytvořen na základě reálných zkušeností získaných při realizaci bakalářské praxe v nejmenované externí auditorské firmě.

Audit IS se bude skládat z následujících kroků:

1. Úvodní schůzka s ředitelem IT oddělení pro identifikaci klíčových systémů s dopadem na finanční závěrku a jejich procesů, získání přehledu o struktuře IT oddělení a kontaktů na osoby odpovědné za jednotlivé systémy a jim přidružené procesy, získání přehledu o interních směrnicích společnosti, domluva ohledně předávání auditních podkladů, kontrola fyzického zabezpečení firmy apod.
2. Identifikace a analýza rizik IT systémů relevantních pro finanční audit. Tento krok bude probíhat ve spolupráci s finančním auditním týmem, který stanoví, na jaké procesy a systémy potřebuje získat od auditního IT týmů reliance neboli potvrzení spolehlivosti.
3. Vytvoření úvodních auditních požadavků na základě analýzy rizik a jejich následná distribuce řediteli IT oddělení.
4. Realizace úvodních schůzek s odpovědnými IT manažery pro získání podrobnějšího detailu o jednotlivých procesech a IT systémech, zabezpečení a monitoring aktivit uživatelů, plánovaných a proběhlých změnách oproti poslední auditované periodě, infrastruktuře apod.
5. Dokumentace tzv. IT understandingu neboli porozumění IT prostředí klientské společnosti. V tomto procesu se dokumentují jednotlivé procesy a jejich průběh, plánované změny, smlouvy s dodavateli IT služeb, využití datových center, informace o IT systémech, kontaktní osoby za jednotlivé oblasti, informace o kybernetické bezpečnosti, fyzickém zabezpečení IT prostředí společnosti atd.
6. Kontrola dodaných auditních podkladů na základě poskytnutých požadavků a evidence jejich kompletnosti (pokud nebudou podklady exportovány za přítomnosti auditora).

7. Provedení auditního testování identifikovaných kritických systémů a aplikací pro finanční závěrku a případné vyžádání chybějících / nepoužitelných podkladů.
8. Případné vyptávání doplňujících podkladů a dotazování se managementu společnosti na nejasnosti / nesoulady procesů s definovanými interními směrnicemi a good practice v případě jejich výskytu.
9. Shrnutí auditních nálezů za IT prostředí, komunikace s finančním týmem ohledně dopadu nálezů na finanční závěrku.
10. Příprava MLP (Management Letter Points) neboli shrnutí nálezů a doporučení za auditovanou periodu a následný reporting nálezů managementu společnosti, který zahrnuje získání vyjádření managementu k jednotlivým nálezům.

4.2 Identifikace klíčových systémů / aplikací pro finanční závěrku

Na úvodní auditní schůzce s ředitelem IT oddělení byl získán základní přehled využívaných aplikací, procesů a seznam periodických interních kontrol prováděných interním auditním oddělením společnosti. Na základě těchto informací byly při následné analýze s finančním auditním týmem identifikovány kritické aplikace Warehouse 7.5 a ProUcto, protože v nich společnost vede všechny důležité informace, které zajímají finanční audit. Na základě provedené analýzy rizik jsem byl finančním týmem osloven o provedení ITGC (IT General Controls) kontrol těchto kritických aplikací pro následující oblasti:

- Access to Programs and Data
- Computer Operations

Jednotlivá rizika těchto oblastí a jejich pokrytí bude popsáno v následujících podkapitolách této práce.

4.3 Tvorba auditních požadavků

Na základě stanovených kontrolních oblastní pro IT audit jsem mohl následně vytvořit úvodní auditní požadavky podkladů, které budou potřebné pro úspěšné dokončení jednotlivých auditních kontrol.

Následující seznam požadavků byl zaslán řediteli IT oddělení auditované společnosti, který následně pověřil odpovědné zaměstnance jejich zpracováním.

ID	Oblast	Aplikace	Popis	Preferované datum dodání	Stav podkladů
HR1	Human resources	-	Seznam všech nových zaměstnanců včetně zaměstnanců s částečným úvazkem a externistů, kteří nastoupili do společnosti během roku 2022. Pokud je to možné, prosím o vytvoření exportu tak, aby obsahoval ID zaměstnance, začátek platnosti kontraktu a pracovní pozici.	15.10.2022	Vyžádáno
HR2	Human resources	-	Seznam všech aktuálních zaměstnanců včetně zaměstnanců s částečným úvazkem. Pokud je to možné, prosím o vytvoření exportu tak, aby obsahoval ID zaměstnance a pracovní pozici.	15.10.2022	Vyžádáno
HR3	Human resources	-	Seznam všech uživatelů, kteří odešli ze společnosti v roce 2022. Pokud je to možné, prosím o vytvoření exportu tak, aby obsahoval ID zaměstnance a datum ukončení kontraktu.	15.10.2022	Vyžádáno
APD1	Access management	-	Interní směrnice k procesu řízení uživatelských přístupů viz jednotlivé body níže: 1) Směrnice k vytváření a modifikaci uživatelských účtů / přístupů 2) Směrnice k terminaci uživatelských účtů / přístupů 3) Směrnice ohledně heslové politiky pro in-scope aplikace 4) Směrnice periodických kontrol přístupů do in-scope aplikací	15.10.2022	Vyžádáno
APD2	Access management	Warehouse 7.5, ProUcto	Systémově generovaný export všech uživatelů (aktivních i neaktivních) aplikací. Pokud to je možné, prosím o vytvoření exportu tak, aby obsahoval následující parametry: ID uživatele, celé jméno, přiřazené role, založení účtu a ukončení účtu.	15.10.2022	Vyžádáno
APD3	Access management	Warehouse 7.5, ProUcto	Systémově generovaný export privilegovaných uživatelů v in-scope aplikacích včetně data poslední aktivity.	15.10.2022	Vyžádáno
APD4	Access management	Warehouse 7.5, ProUcto	Systémově generovaný export databázových uživatelů pomocí příkazů uvedených na listu "DB export".	15.10.2022	Vyžádáno
APD5	Access management	Warehouse 7.5, ProUcto	Systémově generovaný export privilegovaných databázových uživatelů pomocí příkazů uvedených na listu "DB export".	15.10.2022	Vyžádáno
APD6	Access management	Active Directory	Screenshot nastavení vynucené komplexity hesla a jeho obnovovacích parametrů.	15.10.2022	Vyžádáno
APD7	Access management	Warehouse 7.5, ProUcto	Report o provedení periodické kontroly uživatelů včetně evidence o vyřešení / řešení identifikovaných nedostatků.	15.10.2022	Vyžádáno
CO1	Computer Operations	-	Interní směrnice k procesu zálohování dat	15.10.2022	Vyžádáno
CO2	Computer Operations	Warehouse 7.5, ProUcto	Plán datových záloh (nastavení frekvence a typu zálohy)	15.10.2022	Vyžádáno
CO3	Computer Operations	Warehouse 7.5, ProUcto	Historie záloh pro ověření, že jsou zálohy prováděné podle definovaného plánu.	15.10.2022	Vyžádáno
CO4	Computer Operations	Warehouse 7.5, ProUcto	Ukázka notifikace v případě výskytu chyby při zálohování.	15.10.2022	Vyžádáno

Tabulka 3- Auditní požadavky
Zdroj: Vlastní tvorba

Databázové příkazy pro vygenerovaní privilegovaných uživatelů budou popsány samostatně v kapitole Access to program and data.

4.4 IT understanding (porozumění IT prostředí klienta)

Na základě proběhlých schůzek s odpovědnými IT manažery za oblasti řízení uživatelských přístupů, změnového řízení a řízení zálohování dat jsem ze získaných informací zadokumentoval tzv. IT understanding neboli porozumění IT prostředí klienta, které je detailně popsáno níže.

4.4.1 Proces autentizace uživatelů

Na schůzkách s IT manažery odpovědných za správu aplikací Warehouse 7.5 a ProUcto byly získány základní informace o autentizaci uživatelů. Jako první mě zajímalo, jakým

způsobem se uživatelé mohou přihlásit do in-scope aplikací. Konkrétně, zda se uživatelé přihlašují do aplikací pomocí metody SSO (Single-Sign-On) nebo například přes oddělené uživatelské jméno a heslo. Na schůzkách jsem se dozvěděl, že obě in-scope aplikace využívají pro autentizaci uživatelů single-sign-on metodu přes doménu Active Directory, do které se přihlašují zároveň s prvním přihlášením do služebního počítače. Zároveň jsem získal informaci, že se uživatelé nemohou přihlásit napřímo do databázové vrstvy aplikací. Tento přístup je umožněn pouze databázovým administrátorům, kteří se buďto přihlašují na svůj oddělený privilegovaný účet nebo k systémovým / servisním účtům, jejichž správu mají mezi sebou rozdělenou, aby nedocházelo ke sdílení hesla ke kritickým účtům.

4.4.2 Proces vytvoření nového uživatele

Na schůzkách byla získána informace, že jsou nové přístupy do aplikací zakládány na základě žádosti od přímého nadřízeného nového zaměstnance, který specifikuje přesné role, které má nový uživatel do aplikací dostat, případně může jít o žádost o přidělení přístupů podle referenčního uživatele (tzn. jiného zaměstnance, který má aktuálně stejná přístupová práva, jako by měl dostat nový zaměstnanec). Tato žádost musí být založena pro každého nového uživatele od začátku roku 2021 a tento proces je tudíž využíván už téměř druhým rokem. Přímý nadřízený by měl tuto žádost podat před prvním pracovním dnem nového zaměstnance, avšak ne dříve, než jeden týden dopředu. Operátor ServiceDesku poté ověří identitu žadatele na organizační strukturu společnosti a následně přiřadí vyžádané role k novému uživatelskému účtu, který následně vytvoří podle žádosti. V případě, že si není operátor ServiceDesku jistý, jakou roli má nový uživatel dostat, se dále doptává žadatele na podrobnosti, aby nedošlo k nechtěnému přiřazení role s vyššími oprávněními, než bude nový uživatel potřebovat pro výkon své práce. Dále mi bylo sděleno, že proces pro přiřazení rolí nad rámec nutných rolí pro výkon práce stávajících zaměstnanců je totožný s procesem vytvoření nového uživatele.

4.4.3 Proces terminace uživatele

Za proces terminace odchozích uživatelů je odpovědní zaměstnanci HR oddělení, kteří mají povinnost vytvořit a zaslat žádost o odstranění přístupových práv odchozích zaměstnanců na ServiceDesk. Standardně je součástí žádosti i výstupní list, do kterého jsou odchozí zaměstnanci povinni vyplnit všechny aplikace, ve kterých mají přístupová práva a následně si tento výstupní list nechat podepsat svým přímím nadřízeným. Operátor ServiceDesku

následně odebere všechny přístupy do aplikací dle žádosti a následně potvrdí tuto skutečnost a uzavře ticket se žádostí. K odebrání přístupových práv by mělo dojít nejpozději do tří dnů od odchodu zaměstnance ze společnosti. Odebrání přístupových práv v identifikovaných aplikacích probíhá pomocí blokace doménového účtu v AD, bez kterého se uživatelé nemohou přihlásit do aplikací Warehouse 7.5 a ProUcto.

4.4.4 Periodická kontrola přístupových oprávnění

Periodická kontrola přístupových práv probíhá pravidelně jednou za rok a má ji na starosti oddělení IT bezpečnosti, které si nechá vytvořit aktuální exporty uživatelů Active Domain a aplikací Warehouse 7.5 a ProUcto, pomocí kterých následně probíhá ověření správnosti přístupů na aktuální seznam zaměstnanců z HR systému. Mimo to probíhá zároveň analýza přístupových práv v aplikacích a pokud je nalezen zaměstnanec s vyššími oprávněními než definuje jeho pracovní pozice, je kontrolorem vznesena žádost o odůvodnění jejich přidělení. V případě, že majitel aplikace identifikuje tyto práva jako nepotřebná pro výkon práce zaměstnance, jsou následně odebrány.

4.4.5 Proces zálohování dat

Proces zálohování in-scope aplikací Warehouse 7.5 a ProUcto probíhá pomocí nastavených batchových procesů (jobů), které jsou automaticky spouštěné dle nastaveného zálohovacího plánu. Data v obou aplikacích jsou zálohována na úrovni oddělených databází Oracle ve verzi 11g. Zálohovací batchové procesy jsou rozděleny dle jejich frekvence využívání a to na denní inkrementální neboli částečnou zálohu dat a týdenní plnou zálohu dat. Denní inkrementální záloha probíhá každý den kromě neděle v 23:00. Plné týdenní zálohy dat jsou prováděny každou neděli v měsíci v 22:00. Plné zálohy jsou následně nahrány na zálohovací pásku, která se uchovává v zabezpečeném trezoru s retencí 4 týdnů. K tomuto trezoru mají přístup pouze odpovědní zaměstnanci z IT oddělení. Jednou ročně také probíhá tzv. backup recovery test neboli vyzkoušení obnovy dat za pomocí provedené zálohy. Tento proces pokrývá riziko ztráty dat v případě výpadku či jiné nedostupnosti dat v produkčním prostředí.

4.5 Provedení auditních ITGC kontrol

4.5.1 Oblast Access to Programs and Data (APD)

Jednou z identifikovaných rizikových oblastí pro finanční audit byla stanovena oblast APD neboli přístup k datům a aplikacím. Do této oblasti ITGC se řadí například kontroly heslové politiky pro přístup do aplikací a jim přidruženým databázím, kontrola procesu přidělování přístupových práv pro nové zaměstnance, kontrola procesu terminace uživatelů v aplikacích a kontrola správnosti a vyřešení nesrovnalostí při provedené periodické interní kontrole přístupových oprávnění. Hlavním cílem těchto kontrol je ujistit kolegy z finančního auditu o tom, že k finančním datům společnosti mají přístup pouze autorizovaní uživatelé / zaměstnanci, kteří pro přístup k datům používají hesla s adekvátním stupněm zabezpečení.

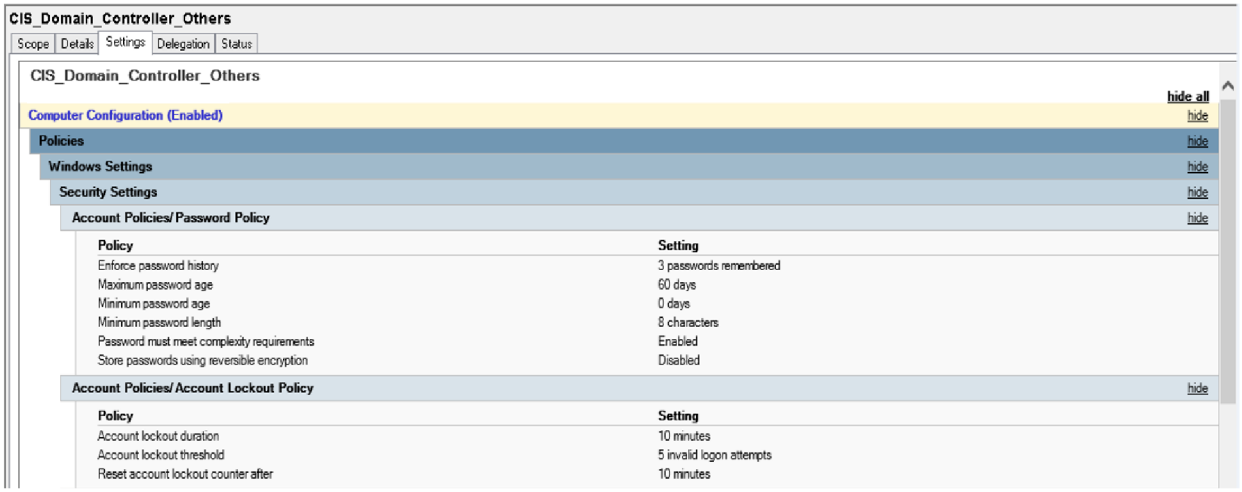
Hlavní rizika této oblasti jsou následující:

- Uživatelé aplikací obcházejí systémem vynucenou autorizaci či zavedený princip SoD (Segregation of Duties).
- Privilegovaní uživatelé obcházejí systémem vynucenou autorizaci či zavedený princip SoD (Segregation of Duties).
- Jsou prováděny neschválené / nesprávné přímé změny transakčních záznamů či kmenových dat.
- Slabá kontrola hesel nebo konfigurace zabezpečení umožnují uživatelům obcházet doporučené nastavení komplexity hesla.

4.5.1.1 Kontrola heslové politiky v Active Directory

Na schůzkách bylo zjištěno, že obě in-scope aplikace (Warehouse 7.5 a ProUcto) využívají pro přihlášení k aplikačním datům autentizaci přes doménu Active Directory pomocí Single-Sign-On principu. Z tohoto důvodu byla v úvodních auditních požadavcích vznesena žádost o dodání evidence vynucené komplexity hesel pro doménové účty.

Na základě tohoto dotazu byl od managementu společnosti obdržen následující screenshot:



Obrázek 5- Heslová komplexita v Active Directory

Zdroj: Vlastní tvorba

Nastavení heslové komplexity viditelné na dodaném screenshotu bylo následně možné porovnat s interní směrnicí týkající se heslové politiky a se zásadami good practice viz výstřižek z interní heslové politiky přiložený níže (Tabulka č.6):

2. Uživatelské heslo

Uživatelské heslo musí splňovat kritéria uvedené v tabulce níže:

Parametr	Požadovaná hodnota
Minimální délka hesla	10 znaků
Minimální komplexita hesla	3 ze 4 typů znaků (malá písmena, velká písmena, číslice, speciální znaky)
Maximální platnost hesla	90 dní
Maximální počet neúspěšných pokusů o přihlášení	5
Doba uzamčení účtu po dosažení limitu neúspěšných pokusů o příhlášení	10 minut
Historie držených předchozích hesel	3

Obrázek 6 - Interní heslová politika společnosti

Zdroj: Vlastní tvorba

Následně proběhlo porovnání nastavení heslové politiky v Active Directory na požadované parametry komplexity hesla v interní směrnici viz tabulka č. 4.

Parametr	Požadavky v interní směrnici	Nastavení v AD
Minimální délka hesla	10 znaků	8 znaků
Minimální komplexita hesla	3 ze 4 typů znaků	3 ze 4 typů znaků
Maximální platnost hesla	90 dní	90 dní
Minimální platnost hesla	Není uvedeno	0
Maximální počet neúspěšných přihlášení	5	5
Doba uzamčení účtu po dosažení limitu neúspěšných pokusů o přihlášení	10 minut	10 minut
Historie držených hesel	3	3

Tabulka 4 - Porovnání parametrů hesla

Zdroj: Vlastní tvorba

Při porovnání nastavení heslové komplexity v Active Directory bylo nalezeno několik nesrovnalostí s interní směrnicí či s good practice.

První nalezenou nesrovnalostí je nastavení minimální délky hesla, která by dle směrnice měla být nastavena na hodnotu 10 znaků, ale dle nastavení v AD je zřetelné, že je tento parametr nastaven pouze na 8 znaků.

Vynucená komplexita hesla je v souladu s interní směrnicí, jelikož parametr Password must meet complexity requirements je ve stavu Enabled, což znamená, že heslo musí obsahovat minimálně 3 ze 4 typů znaků. Tato informace byla ověřena z oficiální webové stránky společnosti Microsoft. [38]

Parametr pro určení maximálního stáří hesla je nastaven v souladu s interní politikou.

Parametr pro určení minimálního stáří hesla není v interní směrnici definován, každopádně tento parametr by měl být nastaven alespoň na hodnotu 1. Tento parametr je důležitý, protože jeho nastavení na hodnotu 0 dovoluje uživatelům při vynucené změně hesla po 90 dnech využít toto nastavení k nastavení stejného hesla, jako bylo poslední používané. Zde by k tomu stačilo pouze třikrát změnit heslo a následně by systém dovolil uživateli použít původní heslo.

Zbylé heslové parametry jako maximální počet neúspěšných přihlášení, doba uzamčení účtu po dosažení limitu neúspěšných pokusů o přihlášení jsou nastaveny v souladu s interní politikou.

Doporučení managementu na základě nalezených nesrovnalostí bude vytvořeno v kapitole Zhodnocení auditovaných procesů / systémů a vytvoření doporučení.

4.5.1.2 Kontrola privilegovaných účtů na úrovni databází Oracle

Ověření pouze privilegovaných účtů na úrovni databází Oracle je důležité z toho důvodu, že běžní uživatelé nemají k databázové vrstvě aplikací přístup, a tudíž jsou všechny operace na úrovni databáze prováděny pouze privilegovanými zaměstnanci, kteří se mohou přihlásit na databázovou vrstvu aplikací. V úvodních auditních požadavcích byl management společnosti požádán o spuštění příkazů pro vyhodnocení následujících kontrol:

1. Kontrola databázových účtů s defaultním heslem

Pro tento test jsem management společnosti požádal o spuštění příkazu a následný export výsledku, který zobrazí tabulku všech uživatelů s defaultním neboli původním a nezměněným heslem.

Použitý příkaz: SELECT * FROM DBA_USERS_WITH_DEFPWD;

Na základě dodaného exportu nebyly identifikovány žádné účty s defaultním heslem ani v jedné z aplikačních databází.

2. Kontrola databázových účtů s privilegovanými oprávněními

Pro tento test jsem management společnosti poprosil o spuštění příkazů a následný export tabulek DBA_USERS (seznam všech uživatelů databází), DBA_ROLE_PRIVS (seznam všech přidělených rolí v databázích) a tabulky DBA_SYS_PRIVS (systémová práva, která jsou přiřazena jednotlivým účtům a jejich rolím). Tabulka DBA_SYS_PRIVS ovšem nebyla vyžádána kompletní. Rozsah byl určen pouze na rozšířená privilegovaná práva jako například vytváření uživatelů a profilů, změny v tabulkách apod. viz přiložený dotaz pro export níže.

Použité příkazy:

Tabulka DBA_USERS: SELECT * FROM DBA_USERS,

Tabulka DBA_ROLE_PRIVS: SELECT * FROM DBA_ROLE_PRIVS,

Tabulka DBA_SYS_PRIVS: příkaz pro export je uveden na obrázku č. 7 z důvodu jeho velikosti.

```
SELECT * FROM DBA_SYS_PRIVS
 WHERE
 PRIVILEGE='CREATE USER' OR
 PRIVILEGE='BECOME USER' OR
 PRIVILEGE='ALTER USER' OR
 PRIVILEGE='DROP USER' OR
 PRIVILEGE='CREATE ROLE' OR
 PRIVILEGE='ALTER ANY ROLE' OR
 PRIVILEGE='DROP ANY ROLE' OR
 PRIVILEGE='GRANT ANY ROLE' OR
 PRIVILEGE='CREATE PROFILE' OR
 PRIVILEGE='ALTER PROFILE' OR
 PRIVILEGE='DROP PROFILE' OR
 PRIVILEGE='CREATE ANY TABLE' OR
 PRIVILEGE='ALTER ANY TABLE' OR
 PRIVILEGE='DROP ANY TABLE' OR
 PRIVILEGE='INSERT ANY TABLE' OR
 PRIVILEGE='UPDATE ANY TABLE' OR
 PRIVILEGE='DELETE ANY TABLE' OR
 PRIVILEGE='CREATE ANY PROCEDURE' OR
 PRIVILEGE='ALTER ANY PROCEDURE' OR
 PRIVILEGE='DROP ANY PROCEDURE' OR
 PRIVILEGE='CREATE ANY TRIGGER' OR
 PRIVILEGE='ALTER ANY TRIGGER' OR
 PRIVILEGE='DROP ANY TRIGGER' OR
 PRIVILEGE='CREATE TABLESPACE' OR
 PRIVILEGE='ALTER TABLESPACE' OR
 PRIVILEGE='DROP TABLESPACES' OR
 PRIVILEGE='ALTER DATABASE' OR
 PRIVILEGE='ALTER SYSTEM';
```

Obrázek 7 - Příkaz pro export tabulky DBA_SYS_PRIVS
Zdroj: Vlastní tvorba

Na základě zaslaného exportu těchto tabulek jsem identifikoval pět privilegovaných / administrátorských účtů. Tři z těchto účtů jsou považovány jako standardní systémové účty (2 z účtů jsou navíc zamknuté viz obrázek č.8.) a dva účty jsou využívány databázovými administrátory, což bylo ověřeno dle jmenné konvence účtů na organizační strukturu IT oddělení. Tyto účty byly identifikovány v obou in-scope databázích se stejnými oprávněními a stejným přiřazeným profilem.

USERNAME	ACCOUNT_STATUS	PROFILE
S[redacted]	OPEN	DEFAULT
S[redacted]	LOCKED	DEFAULT
S[redacted]	LOCKED	DEFAULT
K[redacted]	OPEN	DBA_PROFILE
H[redacted]	OPEN	DBA_PROFILE

Tabulka 5- Seznam privilegovaných účtů v databázích (citlivá data byla anonymizována)
Zdroj: Vlastní tvorba

3. Kontrola databázových účtů s externím či globálním heslem

V tomto testu jsem zkontroloval, zda se pro přístup k některým databázovým účtům nepoužívá externí či globální heslo. Pokud databázový účet využívá externí nebo globální heslo, tak to v principu znamená, že se na tento účet nevztahuje heslová politika, která je nastavená na úrovni přiřazeného databázového profilu. Do takového účtu se nejčastěji přihlašuje například pomocí protokolů Kerberos nebo SSL. Pokud by byly identifikovány takovéto účty, bylo by nutné kontaktovat vlastníka účtu a následně od něj zjistit, jakým způsobem se dá k danému účtu přihlásit.

K provedení tohoto testu nebyla vyžádána žádná další tabulka, jelikož se provádí na základě hodnot obsažených v tabulce DBA_USERS v parametru PASSWORD.

Na základě provedení tohoto testu nebyly identifikovány žádné účty s externím ani s globálním heslem v žádné z testovaných databází.

4. Kontrola nastavení logování aktivity

V tomto testu jsem ověřil, jakým způsobem jsou aktivity v in-scope aplikacích logovány. Jelikož obě in-scope aplikace běží na databázi Oracle ve verzi 11g, tak bylo ověření provedeno na základě obdrženého výstupu následujícího příkazu:

SELECT * FROM V$PARAMETER2 WHERE NAME LIKE '%audit%';

Z tohoto exportu mě nejvíce zajímalo nastavení parametrů audit_sys_operations a audit_trail.

Parametr audit_sys_operations zobrazuje nastavení logování systémového účtu SYS, jelikož má tento účet vždy přidělen profil SYSDBA, který mu umožňuje provádění všech činností nad databází, mezi které se řadí také logování aktivit účtů s přiřazenými profily SYSDBA a

SYSOPER. Je důležité, aby tento parametr byl v zapnutém stavu, aby bylo možné dohledat, z jakého místa došlo k přihlášení na dané účty a jaké operace byly v rámci těchto účtů prováděny.

Parametr audit_trail může mít nastaveno několik různých stavů mezi které se řadí například hodnota „NONE“, která znamená, že je logy nejsou uchovávány, hodnoty OS, DB a XML znamenají, že je logování zapnuto a logy jsou přesměrovány do souboru v operačním systému, databáze nebo do XML souboru podle zvolené varianty. Možnosti logování na úrovni databáze a XML je možné ještě rozšířit (stav DB_EXTENDED / XML_EXTENTED) o logování sloupců SQL_TEXT a SQL_BIND, které slouží pro ukládání dynamický parametrů. Zároveň s tímto nastavením ovšem dochází k nárůstu velikosti logů, na což je dobré pamatovat, pokud je úložiště logů limitováno.

NAME	TYPE	VALUE
audit_sys_operations	1	TRUE
audit_trail	2	DB

Tabulka 6- Nastavení parametrů logování v databázích Oracle
Zdroj: Vlastní tvorba

Na základě dodaného výstupu databázového dotazu uvedeného výše v této kapitole jsem zjistil, že parametr audit_sys_operations je zapnutý a parametr audit_trail je nastavení na hodnotu DB, což znamená, že logování aktivit probíhá do tabulky SYS.AUD$ na úrovni databází. Toto nastavení bylo opět identické v obou in-scope databázích.

5. Kontrola heslových parametrů na úrovni databázových profilů

V tomto testu jsem ověřil nastavení heslové politiky využívaných profilů pro privilegované uživatele / účty na interní heslovou politiku společnosti, která je přiložena na obrázku č. 7. Konkrétně jsem zkontroloval, zda a jak mají databázové profily DEFAULT a DBA_PROFILE nastavený parametr PASSWORD_VERIFY_FUNCTION, který naznačuje, zda je pro tyto profily vynucená komplexita hesla. Mimo kontrolu heslové politiky jsem se zaměřil také na další parametry jako je maximální platnost hesla, historie hesel, maximální počet neúspěšných pokusů o přihlášení a podobně.

Výše zmíněné nastavení bylo ověřeno za pomocí výstupu následujícího dotazu:

SELECT NAME,TEXT FROM DBA_SOURCE WHERE NAME in (SELECT LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME ='PASSWORD_VERIFY_FUNCTION') ORDER BY NAME,LINE;

Na základě dodaného výstupu daného dotazu jsem vytvořil shrnující tabulku č. 5, která zobrazuje nastavení parametrů pro výše zmíněné profily DEFAULT a DBA_PROFILE.

		PROFILE	
Feature	Parameter name	DEFAULT	DBA_PROFILE
Verify function	PASSWORD_VERIFY_FUNCTION	ORA_STRONG_VERIFY_FUNCTION	ORA_STRONG_VERIFY_FUNCTION
Minimum password length	N/A - enforced by specific code in PW Verify function		
Password composition			
Frequency of forced password changes	PASSWORD_LIFE_TIME	UNLIMITED	90
number of unsuccessful login attempts allowed before lockout	FAILED_LOGIN_ATTEMPTS	5	5
Number of passwords that must be used prior to using a password again	PASSWORD_REUSE_MAX	3	3
Days before a password can be reused	PASSWORD_REUSE_TIME	UNLIMITED	UNLIMITED
Idle session time out	IDLE_TIME	UNLIMITED	UNLIMITED

Tabulka 7- Shrnutí nastavení privilegovaných profilů
Zdroj: Vlastní tvorba

Z tabulky je viditelné, že profil DEFAULT má nastavenou maximální platnost hesla na UNLIMITED, což znamená, že přidružené účty nemají nikdy vynucenou změnu hesla. Na základě přechozího zjištění, že je profil DEFAULT využíván pouze třemi systémovými účty, není nastavení tohoto parametru považováno za chybné, jelikož by vynucená změna hesla mohla narušit například automatické batchové procesy, které jsou přes tyto účty pravidelně spouštěny. Ostatní parametry profilu DEFAULT jsou v souladu s interní směrnicí.

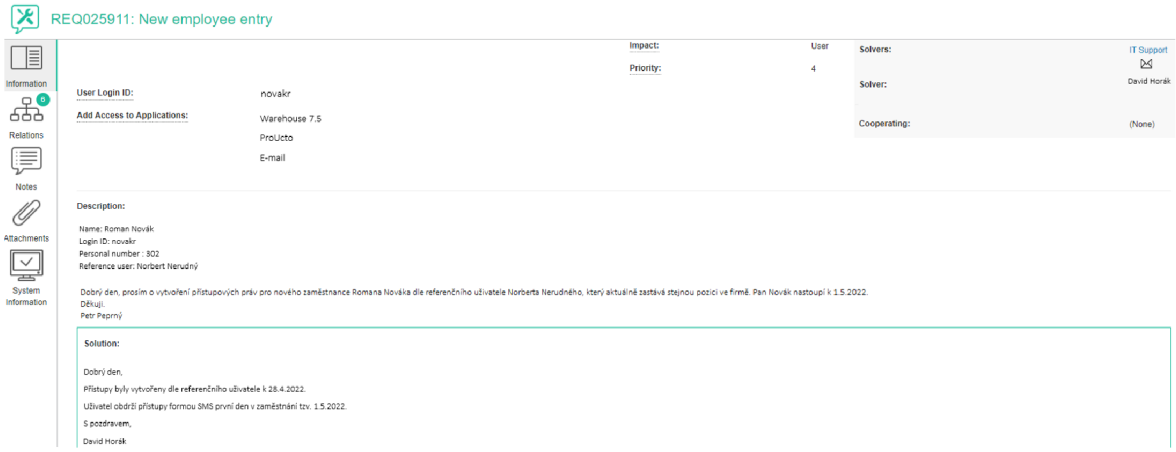
Nastavené parametry pro uživatelský profil DBA_PROFIL má všechny viditelné parametry v Tabulce č. 5 nastavené v souladu s interní směrnicí.

Jako poslední bylo ověřeno nastavení heslové komplexity, které je uchováno ve funkci ORA_STRONG_VERIFY_FUNCTION. Při kontrole bylo zjištěno, že pro oba ověřované profily tato funkce vyžaduje minimální délku hesla 8 znaků a komplexitu hesla ve formě tří ze čtyř typů znaků (malá písmena, velká písmena a číslice). Mimo jiné část ověřovací funkce obsahuje část, kde blokuje příliš jednoduchá slova v heslu a kontroluje, jestli se heslo změnilo alespoň ve čtyřech znacích.

Doporučení managementu na základě nalezených nesrovnalostí bude vytvořeno v kapitole Zhodnocení auditovaných procesů / systémů a vytvoření doporučení.

4.5.1.3 Kontrola nově přidělených přístupů do aplikací

Pro ověření tohoto procesu byl vybrán vzorek o velikosti jednoho nového přístupu do aplikací Warehouse 7.5 a ProUcto z důvodu, že celková populace nových uživatelů byla o velikosti dvou uživatelů. Jako vzorek byl vybrán nový přístup pro pana Romana Nováka s ID 302, který nastoupil do společnosti 1.5.2022 na pozici Finanční Analytik. Na základě mojí žádosti o dodání evidence ke zřízení tohoto přístupu jsem obdržel screenshot ticketu ze ServiceDesku s formální žádostí viz Obrázek č.10.



Obrázek 8 - Žádost o přidělení přístupů
Zdroj: Vlastní tvorba

Z dodaného screenshotu jsem mohl ověřit, že tento přístup pro nového zaměstnance byl žádán manažerem finančního oddělení společnosti Petrem Peprným, jehož pracovní pozice byla získána na základě dodaných seznamů zaměstnanců z HR oddělení. Jako druhé jsem ověřoval, zda byla žádost vytvořena s adekvátním předstihem, avšak ne dříve než jeden týden před nástupem nového zaměstnance. V ticketu lze najít, že byly uživatelské přístupy vytvořeny ke dni 28.4.2022 a zaměstnanec nastupoval 1.5.2022. Posledním důležitým údajem v ticketu je, že přístupová práva vytvořil pan David Horák, který má dle obdržených informací pozici Operátor ServiceDesku a spadá pod oddělení IT Support. Tento proces byl ověřen bez nálezu porušení definované workflow, a tudíž ho hodnotím jako efektivní.

4.5.1.4 Kontrola ukončených přístupů

Tato kontrola spočívá v ověření, zda některý z odchozích uživatelů nemá stále aktivní účet in-scope aplikacích. V tomto konkrétním případě byla kontrola provedena za pomocí dodaného seznamu zaměstnanců, kteří odešli z auditované společnosti v roce 2022, kompletního seznamu uživatelů v AD. Po získání byla provedena analýza dat v programu MS Excel, ve které jsem pomocí funkce SVYHLEDAT (anglicky VLOOKUP) porovnal ID odchozích uživatelů na ID uživatelů v AD. U několika uživatelů byla nalezena shoda ID a na základě tohoto zjištění jsem pomocí stejné funkce získal data blokace účtů v AD viz tabulka č. 6.

ID uživatele (HR leavers)	Platnost smlouvy do	Kontrola AD	Datum ukončení v AD
375	6.1.2022	#NENÍ_K_DISPOZICI	#NENÍ_K_DISPOZICI
673	20.9.2022	673	21.9.2022
551	30.7.2022	#NENÍ_K_DISPOZICI	#NENÍ_K_DISPOZICI
807	11.3.2022	807	12.3.2022
411	19.6.2022	#NENÍ_K_DISPOZICI	#NENÍ_K_DISPOZICI
794	26.5.2022	#NENÍ_K_DISPOZICI	#NENÍ_K_DISPOZICI
447	30.5.2022	#NENÍ_K_DISPOZICI	#NENÍ_K_DISPOZICI
577	7.9.2022	#NENÍ_K_DISPOZICI	#NENÍ_K_DISPOZICI
496	31.5.2022	#NENÍ_K_DISPOZICI	#NENÍ_K_DISPOZICI
652	1.9.2022	#NENÍ_K_DISPOZICI	#NENÍ_K_DISPOZICI
798	26.2.2022	#NENÍ_K_DISPOZICI	#NENÍ_K_DISPOZICI
638	4.8.2022	#NENÍ_K_DISPOZICI	#NENÍ_K_DISPOZICI
500	15.1.2022	#NENÍ_K_DISPOZICI	#NENÍ_K_DISPOZICI
630	11.1.2022	#NENÍ_K_DISPOZICI	#NENÍ_K_DISPOZICI

Tabulka 8 - Auditní testování odchozích uživatelů
Zdroj: Vlastní tvorba

Na základě testování jsem zjistil, že žádní odchozí zaměstnanci neměli v době testování aktivní účet v AD, a tudíž hodnotím tento proces jako efektivní.

4.5.1.5 Periodická kontrola přístupových oprávnění

Evidence k periodické kontrole oprávnění byla po domluvě ověřena na osobní schůzce s klientem, jelikož dokumentace nebyla dostatečně přehledná bez vysvětlení jednotlivých kroků interním zaměstnancem, který kontrolu prováděl. Na schůzce bylo ověřeno, že v roce 2022 byla provedena jedna kontrola periodických oprávnění koncem ledna. Při kontrole byli identifikováni dva odchozí uživatelé v aplikaci Warehouse 7.5, u kterých si kontrolor nebyl jistý, zda již mají zablokovaný přístup v Active Directory či nikoliv z důvodu časového

odstupu při vytváření podkladů pro tuto kontrolu (konkrétně se jednalo o to, že seznam uživatelů Active Directory byl vytvořen o týden dříve než export uživatelů aplikace Warehouse 7.5). Kontrolorem byla následně vznesena žádost o ověření ukončení těchto uživatelů v AD pomocí e-mailové komunikace. Administrátor AD následně dodal evidenci o tom, kdy proběhlo poslední přihlášení těchto uživatelů a také dodal evidenci o jejich včasné blokaci. Kromě tohoto problému nebyly nalezeny žádné jiné nesrovnalosti, a tudíž jsem vyhodnotil interní periodickou kontrolu přístupů jako efektivní.

4.5.2 Oblast Computer Operations

Druhou testovanou oblastí identifikovaných IT systémů je oblast Computer Operations, (CO). Z této oblasti by potřeboval finanční auditní tým získat reliance pouze na proces zálohování dat.

Hlavní rizika této oblasti jsou následující:

- Záznamy transakcí jsou ztraceny (např. kvůli selhání systému).
- Data nelze obnovit nebo jsou během procesu obnovy poškozena.

4.5.2.1 Kontrola procesu zálohování dat

Jak bylo zmíněno výše v kapitole IT understanding, data in-scope aplikací jsou zálohována pomocí automatických batchových procesů, které se spouštění nad databázemi Oracle. Z tohoto důvodu jsem si vyžádal formální zálohovací plán těchto databází a evidenci o provedení batchových jobů dle plánu ve formě logu.

Plán zálohování								
Název úlohy	Denní plán							Start úlohy
	Po	Út	St	Čt	Pá	So	Ne	
ORACLE_DB_backup_daily								23:00
ORACLE_DB_backup_weekly								22:00

Tabulka 9 - Zálohovací plán Oracle databází
Zdroj: Vlastní tvorba

Na základě obdrženého formálního plánu jsem následně mohl ověřit pomocí logu, zda všechny úlohy proběhly podle plánu. Evidence ve formě logu byla obdržena za posledních 15 dní.

Na úvodní schůzce byla rovněž ověřeno, zda jsou odpovědné osoby za oblast zálohování dat notifikovány v případě, že automatická úloha skončí chybou. Podle informací získaných od

odpovědné osoby jsem zjistil, že jsou notifikace prováděny pomocí e-mailové zprávy, která v případě chyby obsahuje název daného jobu a důvod, proč skončil chybou. Za rok 2022 takováto situace ovšem nenastala a z tohoto důvodu není možné přiložit relevantní evidenci.

Kromě notifikací v případě chyby automatické úlohy mi byl na schůzce ukázán log z proběhlého testu obnovy dat ze zálohy z července 2022.

Job name	Start time	Total duration	Job status
ORACLE_DB_backup_daily	1.10.2022 23:00	888	succeeded
ORACLE_DB_backup_weekly	2.10.2022 22:00	24784	succeeded
ORACLE_DB_backup_daily	3.10.2022 23:00	840	succeeded
ORACLE_DB_backup_daily	4.10.2022 23:00	715	succeeded
ORACLE_DB_backup_daily	5.10.2022 23:00	779	succeeded
ORACLE_DB_backup_daily	6.10.2022 23:00	922	succeeded
ORACLE_DB_backup_daily	7.10.2022 23:00	793	succeeded
ORACLE_DB_backup_daily	8.10.2022 23:00	707	succeeded
ORACLE_DB_backup_weekly	9.10.2022 22:00	24295	succeeded
ORACLE_DB_backup_daily	10.10.2022 23:00	774	succeeded
ORACLE_DB_backup_daily	11.10.2022 23:00	602	succeeded
ORACLE_DB_backup_daily	12.10.2022 23:00	674	succeeded
ORACLE_DB_backup_daily	13.10.2022 23:00	692	succeeded
ORACLE_DB_backup_daily	14.10.2022 23:00	677	succeeded
ORACLE_DB_backup_daily	15.10.2022 23:00	691	succeeded

Tabulka 10- Log zálohovacích úloh
Zdroj: Vlastní tvorba

Na základě ověření logu automatických zálohovacích úloh jsem neidentifikoval žádné porušení nastaveného procesu zálohování dat.

4.6 Zhodnocení auditovaných procesů / systémů a vytvoření doporučení

Posledním krokem provedeného auditu je zdokumentování auditních nálezů a následné předání dokumentu managementu společnosti, aby se k těmto záležitostem mohli vyjádřit.

Zhodnocení procesů aplikací Warehouse 7.5 a ProUcto je následující:

Kontrola heslové politiky v Active Directory

Nález

Heslová politika pro doménu Active Directory není nastavena v souladu s interní směrnicí v následujících parametrech: minimální délka hesla, minimální stáří hesla.

Parametr minimální délky hesla je aktuálně nastaven na 8 znaků, ačkoliv interní směrnice vyžaduje mít tento parametr nastavený minimálně na 10 znaků.

Parametr minimální stáří hesla je aktuálně nastaven na hodnotu 0, což uživatelům domény umožňuje při vynucené změně hesla po 90 dnech vytvořit 3 nová hesla a následně nastavit původní heslo pro přístup, a tudíž je možno obejít tento proces.

Doporučení

Doporučuji nastavit heslové parametry dle interní směrnice, aby nedocházelo k uživatelskému obcházení stanovených požadavků na heslo.

Kontrola privilegovaných účtů na úrovni databází Oracle

Nález

Heslová politika uložená ve funkci ORA_STRONG_VERIFY_FUNCTION není v souladu s interní směrnicí v následujícím parametru: minimální délka hesla.

Parametr minimální délky hesla pro privilegované databázové účty není nastaven v souladu s interní politikou, jelikož aktuálně vyžaduje délku o velikosti 8 znaků místo 10 znaků.

Doporučení

Doporučuji nastavit heslový parametr minimální délky hesla ve funkci ORA_STRONG_VERIFY_FUNCTION, která je využívána privilegovanými účty na úrovni databáze na požadovanou hodnotu 10 znaků.

Kontrola nově přidělených přístupů do aplikací

Při kontrole tohoto procesu nebyly nalezeny žádné nesrovnalosti a z tohoto důvodu ho hodnotím jako efektivní.

Kontrola ukončených přístupů

Při kontrole tohoto procesu nebyly nalezeny žádné nesrovnalosti a z tohoto důvodu ho hodnotím jako efektivní.

Periodická kontrola přístupových oprávnění

Při kontrole tohoto procesu nebyly nalezeny žádné nesrovnalosti a z tohoto důvodu ho hodnotím jako efektivní.

Proces zálohování dat

Při kontrole tohoto procesu nebyly nalezeny žádné nesrovnalosti a z tohoto důvodu ho hodnotím jako efektivní.

5 Závěr

Hlavním cílem této bakalářské práce bylo zhodnotit nastavení informačních systémů, které mají vliv na finanční data či bezpečnost společnosti. Na základě stanovení tohoto cíle byla vypracována teoretická část práce, která je složena ze dvou hlavních kapitol (Teorie auditu a Audit informačních systémů). V první z těchto kapitol jsem se věnoval především vzniku profese auditora a jejímu následnému vývoji až do dnešní podoby, druhům auditu a největším současným externím firmám, které tuto službu nabízí společnostem. V druhé ze zmíněných kapitol jsem se dopodrobna věnoval auditu infomačních systémů a to konkrétně jeho definicím, nejdůležitějším standardům a regulacím, jako jsou například sady norem ISO, které se týkají kvality a bezpečnosti nebo také dokumentu ITAF. Dále jsem zde představil nejdůležitější metodiky, které se využívají v praxi – COBIT 2019 a ITIL a jako poslední část teoretické části této práce byly představeny profesní certifikace pro auditory IS, které jsou dostupné od uznávané nadnárodní společnosti ISACA.

V praktické části jsem se snažil co nejvíce přiblížit veřejnosti plánování a průběh zakázky auditu IS na mnou vytvořené případové studii. V této části práce jsem krok po kroku poslal, jak vypadá plánování a stanovení rozsahu auditu IS, dokumentace porozumění klientského IT prostředí, auditní testování IS a následné vyvození výsledků a dokumentace nálezů. Proces průběhu auditu IS byl vytvořen pro dvě oblasti ITGC kontrol – Access to Program and Data a Computer Operations.

V první oblasti jsem se věnoval hlavně nastavení uživatelských hesel v doméně Active Directory, kontrolám souvisejících s přístupovými oprávněními uživatelů, ale také celkovému nastavení privilegovaných účtů na databázové vrstvě in-scope aplikací.

Druhá oblast byla konkrétně zaměřená na auditní testování procesu zálohování dat, kde byl ověřen zálohovací plán, logy automatických batchových procesů zálohování a provedení testu obnovy dat.

Na závěr jsem z analyzovaných dat vyvodil efektivnost nastavení in-scope aplikací na základě good practice či ustanovených interních směrnic společnosti a následně vytvořil doporučení pro zlepšení nalezených nedostatků.

6 Seznam použitých zdrojů

[1] Svatá, Vlasta. Audit informačního systému. V Praze: Oeconomica, nakladatelství VŠE, 2016. ISBN 978-80-245-2168-8.

[2] Dvořáček, Jiří. Interní audit a kontrola. 2. přeprac. a dopl. vyd. Praha: C.H. Beck, 2003. C.H. Beck pro praxi. ISBN 80-7179-805-3.

[3] Collins, D. (2023). Arthur Andersen | American company. Encyclopedia Britannica. Dostupné z: https://www.britannica.com/topic/Arthur-Andersen

[4] Christopher, A. (2016). The Case Analysis of the Scandal of Enron. Academia.edu. Dostupné z: https://www.academia.edu/30500625/The_Case_Analysis_of_the_Scandal_of_Enron?auto=citations&from=cover_page

[5] KPMG. (nedatováno). Our History. KPMG Global. Dostupné z: https://home.kpmg/xx/en/home/about/who-we-are/our-history.html

[6] KPMG. (nedatováno). O společnosti. KPMG Česká republika. Dostupné z: https://home.kpmg/cz/cs/home/o-nas/o-spolecnosti.html

[7] PwC. (nedatováno). Corporate History. PwC US. Dostupné z: https://www.pwc.com/us/en/about-us/pwc-corporate-history.html

[8] PwC. (nedatováno). O nás. PwC Česká republika. Dostupné z: https://www.pwc.com/cz/cs/o-nas.html

[9] Ernst & Young. (2018). Encyclopedia of Cleveland History. Case Western Reserve University. Dostupné z: https://case.edu/ech/articles/e/ernst-young

[10] EY. (nedatováno). EY v České republice. EY Česká republika. Dostupné z: https://www.ey.com/cs_cz/people/ey-czech-republic

[11] Zippia. (2022). Deloitte history: Founding, Timeline, and Milestones. Zippia. Dostupné z: https://www.zippia.com/deloitte-careers-21198/history/

[12] Deloitte. (nedatováno). Deloitte v České republice. Deloitte Česká republika. Dostupné z: https://www2.deloitte.com/cz/cs/pages/about-deloitte/articles/about-us.html

[13] ISACA. (nedatováno). Information Technology (IT) Certification Programs. ISACA. Dostupné z: https://www.isaca.org/credentialing/certifications

[14] Český institut interních auditorů. (nedatováno). Co je interní audit? ČIIA - Český institut interních auditorů. Dostupné z: https://www.interniaudit.cz/ciia/?idKategorie=3

[15] Institute of Internal Auditors. (nedatováno). What is Internal Audit. Institute of Internal Auditors Australia. Dostupné z: https://www.iia.org.au/about-iia-australia/WhatIsInternalAudit.aspx

[16] Menzies. (2020) Differences between an Internal Audit vs. External Audit. Menzies Chartered Accountants. Accounting & Audit Services. Dostupné z: https://www.menzies.co.uk/helping-you/audit-compliance/what-is-an-audit/internal-audit-vs-external-audit/

[17] Management Mania. (nedatováno). Finanční audit. ManagementMania.com. Dostupné z: https://managementmania.com/cs/financni-audit

[18] Ikaros. (2005). Informační audit - cesta k rozvoji znalostní organizace. Ikaros elektronický časopis o informační společnosti. Dostupné z: http://ikaros.cz/informacni-audit-–-cesta-k-rozvoji-znalostni-organizace

[19] Ecodis. (nedatováno). Environmentální audity. Ecodis - Projektové studie v oblasti ochrany životního prostředí. Dostupné z: http://www.ecodis.cz/ru/produkty-a-sluzby/environmentalni-audity

[20] Management Mania. (nedatováno). Forenzní audit (Forensic Audit). ManagementMania.com. Dostupné z: https://managementmania.com/cs/forenzni-audit

[21] IT Audit Framework (ITAF™): A Professional Practices Framework for IT Audit, 4th Edition, Printed in the United States of America, 2020. ISBN 978-1-60420-834-4

[22] ISO. (nedatováno). About us. ISO. Dostupné z: https://www.iso.org/about-us.html

[23] Honan, B. ISO27001 in a Windows Environment: The best practice handbook for a Microsoft® Windows® environment. IT Governance Ltd., 3rd Edition, ITGP, 2014. ISBN 978-1849286039.

[24] ISMS. (2022). ISO 27002:2022 Changes, Updates & Comparison. ISMS.online. Dostupné z: https://www.isms.online/iso-27002/iso-27002-revisions-updates-comparison/#:~:text=In%20ISO%2027002%3A2022%2C%20the,controls%E2%80%9D%20in%20the%202022%20revision

[25] ISO. (2015). ISO/IEC 27006:2015. ISO. Dostupné z: https://www.iso.org/standard/62313.html

[26] ISO. (2021). ISO 9001 and related standards – Quality management. ISO. Dostupné z: https://www.iso.org/iso-9001-quality-management.html

[27] PDQM. (nedatováno). ISO/IEC 15504. PDQM. Dostupné z: https://www.pdqm.cz/terms/standards/iso-15504

[28] PDQM. (nedatováno). ISO/IEC 12207. PDQM. Dostupné z: https://www.pdqm.cz/terms/standards/iso-12207

[29] Tayllorcox. (nedatováno). ISO 19770 certification confirms that you really have ITAM under control. Tayllorcox. Dostupné z: https://www.tayllorcox.com/vn/audit/iso-19770

[30] Portal ISO. (nedatováno). ISO 25000 STANDARDS. Portal ISO 25000. Dostupné z: https://iso25000.com/index.php/en/iso-25000-standards

[31] ISACA. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Printed in the United States of America, 2012. ISBN: 978-1-60420-237-3

[32] ISACA. (nedatováno). How COBIT has Changed IT. COBIT History. ISACA. Dostupné z: https://www.isaca.org/why-isaca/about-us/isaca-50/cobit-over-the-years

[33] ISACA. (nedatováno). The COBIT Framework Timeline. Infographic. ISACA. Dostupné z: https://www.isaca.org/resources/infographics/the-cobit-framework-timeline

[34] ISACA. (nedatováno). COBIT 2019 and COBIT 5 Comparison. ISACA. Dostupné z: https://www.isaca.org/resources/news-and-trends/industry-news/2020/cobit-2019-and-cobit-5-comparison

[35] ISACA. (nedatováno). COBIT Design Factors: A Dynamic Approach to Tailoring Governance in the Era of Digital Disruption. ISACA. Dostupné z: https://www.isaca.org/resources/news-and-trends/industry-news/2019/cobit-design-factors

[36] White, S. K., Greiner, L. (2022) What is ITIL? Your guide to the IT Infrastructure Library. CIO. Dostupné z: https://www.cio.com/article/272361/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html

[37] Terra, J. (2023). ITIL® V3 vs. ITIL® V4: The Major Differences. Simplilearn. Dostupné z: https://www.simplilearn.com/itil-4-vs-itil-v3-whats-new-article

[38] Microsoft. (2023). Password must meet complexity requirements (Windows 10). Microsoft. Dostupné z: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements

Citace

1 Komora auditorů České republiky. (2012). Poslání a smysl auditu. Komora auditorů České republiky. Dostupné z: https://www.kacr.cz/poslani-a-smysl-auditu [cit. 04.08.2022].

2 Dvořáček, Jiří. Interní audit a kontrola. 2. přeprac. a dopl. vyd. Praha: C.H. Beck, 2003. C.H. Beck pro praxi. ISBN 80-7179-805-3 [cit. 04.08.2022]

3 ISACA. Interactive Glossary & Term Translations. ISACA. Dostupné z: https://www.isaca.org/resources/glossary [cit. 10.08.2022]

4 Svatá, Vlasta. Audit informačního systému. V Praze: Oeconomica, nakladatelství VŠE, 2016. ISBN 978-80-245-2168-8. [cit. 10.08.2022]

5 Vaněk, Zdeněk. (nedatováno). Cíle a postup informačního auditu. Dostupné z: https://www.dcit.cz/papers/ISO_Cile_Auditu.pdf [cit. 10.08.2022]

6 Encyclopedia Britannica. (2001). Information systems audit. Encyclopedia Britannica. Dostupné z: https://www.britannica.com/topic/information-system/Information-systems-audit [cit.10.08.2022]

7 Seznam obrázků, tabulek, grafů a zkratek

7.1 Seznam obrázků

7.2 Seznam tabulek