Ekonomická fakulta
Faculty of Economics

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

Jihočeská univerzita v Českých Budějovicích

Ekonomická fakulta

Katedra aplikované informatiky a matematiky

Diplomová práce

Audit ERP systému SAP

Vypracovala: Markéta Lišková
Vedoucí práce: doc. Ing. CSc. Ladislav Beránek

České Budějovice 2020

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH

Ekonomická fakulta

Akademický rok: 2018/2019

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Markéta LIŠKOVÁ**
Osobní číslo:	**E18350**
Studijní program:	**N6209 Systémové inženýrství a informatika**
Studijní obor:	**Ekonomická informatika**
Téma práce:	**Audit ERP systému SAP**
Zadávající katedra:	**Katedra aplikované matematiky a informatiky**

Zásady pro vypracování

Cílem práce je popsat princip auditu ERP SAP a prakticky provést takový audit na systému provozovaném pro výukové účely na Ekonomické fakultě JU v Českých Budějovicích. Dále zmapovat způsob administrace uživatelů, zmapovat oddělení pravomocí v procesech, příslušné změnové řízení a případně určitý procesní audit, související se shora uvedenými činnostmi. Ukázat nástroje SAP pro takový bezpečnostní audit, jako je např. SAP Repository Information System apod. Součástí práce bude popis jednotlivých kroků testování a postupů a popis podkladů. Následně bude provedeno shrnutí a vyhodnocení míry rizika spojeného se zjištěnými nedostatky. Na základě toho bude proveden návrh případných změn ve způsobu administrace uživatelů apod.

Metodický postup:

1. Analýza postupů v relevantních knižních a elektronických zdrojů, seznámení se s výukovou verzí ERP SAP na Ekonomické fakultě.
2. Příprava vhodných nástrojů a postupů, analýza prostředí ERP SAP na Ekonomické fakultě.
3. Provedení testování, vyhodnocení testů, zhodnocení rizik.
4. Návrh opatření, závěr.

Rozsah pracovní zprávy:	**50 – 60 stran**
Rozsah grafických prací:	**dle potřeby**
Forma zpracování diplomové práce:	**tištěná**

Seznam doporučené literatury:

1. BISKIE, Steve. (2010). *Surviving an SAP audit.* Boston, MA: Galileo Press.
2. FIŠER, Marek. (2017). *Zabezpečení ERP SAP jako součást finančního auditu v prostředí velkých firem.* Diplomová práce. Praha: VŠE.
3. MAASSEN, André. (2007). *SAP R/3: kompletní průvodce.* Brno: Computer Press.
4. SCHRECKENBACH, Sebastian. (2015). *SAP administration: practical guide.* Bonn: Rheinwerk Publishing.

Vedoucí diplomové práce: **doc. Ing. Ladislav Beránek, CSc.**
Katedra aplikované matematiky a informatiky

Datum zadání diplomové práce: **15. ledna 2019**
Termín odevzdání diplomové práce: **12. dubna 2020**

V Českých Budějovicích dne 18. března 2019

L.S.

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

doc. Dr. Ing. Dagmar Škodová Parmová
děkanka

doc. RNDr. Jana Klicnarová, Ph.D.
vedoucí katedry

Prohlášení

Prohlašuji, že svou diplomovou práci “Audit ERP systému SAP” jsem vypracoval/a samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

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

…….....

V Českých Budějovicích dne 8. 8. 2020 Markéta Lišková

Ráda bych poděkovala vedoucímu diplomové práce doc. Ing. CSc. Ladislavu Beránkovi za vedení této práce a za cenné rady, podněty a připomínky, které mi poskytl v průběhu jejího zpracování.

Obsah

1 Úvod

Informační technologie jsou nedílnou součástí každodenního života a s vývojem doby se staly i základním pilířem efektivního a úspěšného podnikání, proto i jejich odpovídající a komplexní kontroly jsou potřeba. Audit je rozsáhlá vědní disciplína, která má mnoho podob, způsobů, nástrojů i metod, kterých využívá. S ohledem na informační systémy je důležité zejména prověřovat, jakým způsobem jsou data uchovávána, zpracována, poskytována a zpřístupněna. Účelem je zamezit nekalým praktikám a jiným rizikům, která mohou poškodit nebo ohrozit dotčené subjekty.

Cílem práce je popsat princip auditu ERP SAP a prakticky provést takový audit na systému provozovanému pro výukové účely na Ekonomické fakultě. Zmapovat způsob administrace uživatelů, zmapovat oddělení pravomocí v procesech, příslušné změnové řízení, a případně určitý procesní audit související se shora uvedenými činnostmi. Ukázat nástroje SAP pro takový bezpečnostní audit, jako je např. SAP Repository Information System. Dále navrhnout případné změny ve způsobu administrace uživatelů apod.

V teoretické části jsou objasněny základních terminologické pojmy. Vymezení pojmu audit a audit informačních systému spolu s náležitostmi souvisejícími. Následně je definován pojem ERP a představena organizace SAP spolu s auditovaným produktem.

Vlastní práce je provedena prostřednictvím testování kontrolních cílů stanovených s ohledem na cíl práce, uvedenou literaturu a za využití metodiky COBIT. Výsledky jednotlivých testů jsou zaznamenány a vyhodnoceny. Následně na základě provedeného výzkumu, byla navržena vhodná opatření k zajištění přijatelně zabezpečeného a administrovaného systému.

2 Literární přehled

2.1 Vymezení pojmu audit

Audit je systematické a objektivní přezkoumání jednoho nebo více aspektů organizace, porovnává, co organizace dělá, s definovaným souborem kritérií nebo požadavků za účelem sdělit výsledky zainteresovaným zájemcům. (Gantz, 2013)

Audit musí vždy splňovat čtyři základní vlastnosti, kterými jsou:

- komplexnost - musí postihnout všechny relevantní aspekty a vazby,
- objektivnost - musí se opírat o existující standardy, případně zkušenosti, pokud standardy neexistují,
- nezávislost - auditor nemá s objektem auditu ani se zadavatelem auditu žádné spojení, které by představovalo konflikt zájmů,
- formalizovanost - proces auditu se musí řídit metodikou a existujícími standardy.

(Svatá, 2018)

Audit může být zaměřen na různé oblasti lidské činnosti. Odlišnosti jednotlivých auditů mohou být v cíli, předmětu, uživatelích, v metodách a postupech i v požadavcích na odbornost osob, které audit provádějí. Významné rozdíly jsou i v rozsahu a obsahu legislativní úpravy. (Müllerová & Králíček, 2014)

2.1.1 Druhy auditu

Účel a rozsah auditu a postupy používané k jejich provádění se výrazně liší u externího a interního auditu. Interní audit je nezávislá, objektivní ověřovací a poradenská činnost, jejímž cílem je přidat hodnotu a zlepšit fungování organizace. Pomáhá organizaci dosáhnout jejích cílů zavedením systematického a disciplinovaného přístupu k hodnocení a zlepšování efektivity procesů řízení rizik, kontroly a řízení. Interní audity provádějí zaměstnanci organizace nebo pracovníci najatí k práci jménem organizace. (Gantz, 2013)

Oproti tomu externí audity provádějí externí auditoři nebo profesionální auditorské firmy a tím pádem jsou standardy, požadavky nebo jiná kritéria auditu použitá při externích

auditech definovány mimo auditovanou organizaci. Mezi nejvýznamnější důvody, proč se organizace podrobují externím auditům, kromě dodržování právních a regulačních předpisů jsou dále certifikace, zabezpečování kvality nebo ověřování hlášených a osvědčených informací, které organizace poskytuje k různým účelům. (Gantz, 2013)

Mimo členění na interní a externí audit lze rozlišit další druhy auditu, mezi ty nejznámější patří audit účetní závěrky, který je zaměřen na individuální nebo konsolidované účetní závěrky a jeho posláním je především zvýšit věrohodnost účetních uzávěrek zveřejňovaných podnikovým managementem. (Müllerová & Králíček, 2014)

Dále jím je interní audit, který se zabývá zkoumáním ekonomických procesů a jevů uvnitř účetních jednotek. Forenzní audit, jež je zaměřen proti hospodářské kriminalitě, ale obecně i proti nedodržování vnitrofiremních předpisů a směrnic. Audit jakosti prověřující kvalitu výkonů jako jsou výrobky nebo systém řízení poskytovaných podnikem. Ekologický audit, který představuje soustavné dokumentované a objektivní vyhodnocování řídicího systému podniku a kontrolu procesů, které mohou mít dopad na životní prostředí a počítačový audit, který je dále více v práci rozebrán a kdy se jedná nejen o prověřování a kontrolu používaných integrovaných informačních systémů v podniku, ale i způsob ochrany dat těchto systémů. (Müllerová & Králíček, 2014)

2.1.2 Výhody auditu

Audit přináší mnoho výhod, proto i subjekty, které nemají jeho povinnost, ho mohou vyžadovat. Výčet výhod, které audit přináší je následovný:

- Zvyšuje kvalitu a důvěryhodnost informací, poskytuje důvěru investorům a zlepšuje pověst subjektu na trhu,
- nezávislé kontroly a ověřování mohou být užitečné pro řízení auditovaného subjektu,
- může snížit riziko předpojatosti, podvodů a chyb,
- může odhalit zkreslení, podvody a chyby,
- zvyšuje důvěryhodnost účetní závěrky, např. pro daňové úřady nebo věřitele,
- auditor může upozornit na nedostatky v systému vnitřní kontroly.

(ACCA Paper F8 Audit and Assurance, 2016)

2.1.3 Regulace auditu

Národní a mezinárodní regulátoři zavedli tři iniciativy, aby zajistili důvěru auditorské profesi. Těmito iniciativy jsou sjednocení auditorských postupů tak, aby uživatelé auditorských služeb měli důvěru v povahu auditů prováděných po celém světě. Zaměření na kvalitu auditu, aby byla splněna očekávání uživatelů a dodržování přísného etického kodexu chování a snaha o zlepšení vnímání auditorů jako nezávislých, nezaujatých poskytovatelů služeb. K dosažení iniciativ se musí odborníci řídit regulačními nařízeními, konkrétně národním právem obchodních společností, auditorskými standardy a etickým kodexem. Následně různé země mohou mít různé požadavky, ale obecně platí stejné zásady po celém světě. (ACCA Paper F8 Audit and Assurance, 2016)

Vnitrostátní právo pak zpravidla zahrnuje, které společnosti jsou povinny mít audit, kdo může a nemůže provést audit, jmenování auditora, jeho rezignace a odvolání a zejména práva a povinnosti auditora. (ACCA Paper F8 Audit and Assurance, 2016)

Audit v mnoha zemích dodržuje široké standardy a zásady souhrnně známé jako GAAS, koncepčně analogické s obecně uznávanými účetními zásadami GAAP používanými ve finančním účetnictví a auditu. Mezinárodní organizace usilují o dosažení určité úrovně mezinárodního konsensu, ale normy a specifikum toho, co představuje obecně přijímaný formát v jednotlivých jurisdikcích liší, tím pádem neexistuje jediný zdroj auditorských standardů. Proto spíše vedoucí národní normalizační organizace v mnoha zemích pracují na vývoji standardů, které ztělesňují GAAS a zveřejňují tyto standardy ve svých vlastních zemích. (Gantz, 2013)

Některé mezinárodní normalizační organizace pak vyvíjejí standardy pro všeobecnou dostupnost a poskytují orgánům a jednotlivým organizacím ve více zemích možnost tyto standardy použít nebo upravit. (Gantz, 2013)

2.1.4 Osoba auditora

Činnost auditora je činností vysoce odbornou a náročnou na teoretické znalosti i praktické zkušenosti. Specifickou vlastností auditorské činnosti je dále to, že výsledky práce auditora slouží primárně širší veřejnosti. Z těchto důvodů je nutné činnost auditorů regulovat. Právní úprava specifikuje podmínky pro výkon auditorské činnosti především

ve formě požadavků obecné způsobilosti, kvalifikačních požadavků a pravidel pro vlastní odbornou činnost. (Müllerová & Králíček, 2014)

Konkrétní požadavky na auditorskou profesi jsou poté logické myšlení spolu se schopností vést skupinu zaměstnanců, dále musí být schopný získávat informace, provádět jejich hodnocení a prodávat výsledky. Auditor musí být znalý specifického odvětví ve kterém audituje a strategických znalostí. Především by měl znát kritické klíčové faktory úspěchu v odvětví, společné podnikatelské praktiky a univerzální měření použitá v odvětví. Mezi strategické znalosti se řadí důvěrná znalost strategických plánovacích konceptů a schopnost identifikovat nekonzistentní strategické iniciativy, klíčové faktory úspěchu a měření. (Dvořáček, 2005)

Obecně by pak auditor měl dosáhnout specifických znalostí zajišťujících vysokou odbornost a účastnit se zkouškového a vzdělávacího systému k prověřování a udržování znalostí. Spolu s oprávněním auditorské služby poskytovat se od auditora očekává podřízenost veřejnému zájmu, znalost odborných norem, dodržování etického kodexu a společenské uznání. (Müllerová & Králíček, 2014)

Předpokladem je také, že auditoři s delším funkčním obdobím jsou schopni poskytovat auditorské služby ve vyšší kvalitě, jelikož potřebují čas na rozvoj znalostí specifických pro klienta, aby mohli provádět efektivní audit. (Yangyang et al., 2016)

Naplnění požadavků na profesi auditora zajišťují především profesní organizace účetních a auditorů, kterými jsou:

- Americký institut certifikovaných účetních,
- Organizace certifikovaných účetních,
- Mezinárodní federace účetních a auditorů,
- Federace evropských účetních,
- Komora auditorů České republiky.

(Müllerová & Králíček, 2014)

2.1.5 Postup auditu

Z praktického hlediska je audit považován za proces vyhledávání, zpracování, posuzování a úpravy informací. Z teoretického hlediska pak kompletní proces auditu obvykle zahrnuje přijetí obchodního pověření, plánování auditu, identifikaci, vyhodnocení a reakci na riziko nesprávnosti a přípravu auditorských zpráv. Celkovým cílem auditu je získat přiměřenou jistotu, že nedošlo k žádné významné nesprávnosti způsobené podvodem nebo chybou, a vydávat zprávy o auditu v souladu s auditorskými standardy včetně zajištění komunikace s auditovaným subjektem. (Tusheng et al., 2020)

Proces auditu lze na základě povahy prováděných činností a jejich zamýšlených výsledků odkázat na Demingův cyklus a jeho čtyřfázový proces pro trvalé zlepšování. Přesto, že se názvy používané k označení těchto kroků v různých metodikách mohou lišit, obecně jsou tedy zaměřené na plánování auditu, provádění, hlášení nálezů a nápravná zajištění spolu s nápravnými opatřeními. (Gantz, 2013)

Plánování auditu zahrnuje všechny činnosti nezbytné k zajištění toho, aby konkrétní audit mohl být proveden zcela a efektivně, aby byly splněny cíle organizace v oblasti auditu. Při plánování je třeba určit předmět auditu, cíl auditu, rozsah auditu, předpokládané požadavky na zdroje a doporučující protokoly, které budou auditoři využívat. (Information Systems Auditing: Tools and Techniques: Creating Audit Programs, 2016)

Určit předmět auditu znamená identifikovat oblast, která má být auditovaná například obchodní funkce, systém, fyzické umístění. Cílem neboli účelem auditu může být například zjištění, zda ke změnám zdrojového kódu programu dochází v dobře definovaném a kontrolovaném prostředí. V rámci stanovení rozsahu auditu je třeba identifikovat konkrétní systémy, funkce nebo jednotky organizace, které mají být zahrnuty do zkoumání. (Information Systems Auditing: Tools and Techniques: Creating Audit Programs, 2016)

Jakmile je následně definován předmět, cíl a rozsah, může auditorský tým identifikovat zdroje, které budou k provedení auditorské práce nezbytné a zároveň by měl mít auditorský tým dostatek informací k identifikaci a výběru přístupu nebo strategie. Mezi zdroje, které by měli být definovány patří:

- Potřebné technické dovednosti a zdroje.
- Rozpočet a úsilí potřebné k dokončení auditu.
- Místa nebo zařízení, která mají být auditována.
- Úlohy a povinnosti auditorského týmu.
- Časový rámec pro různé fáze auditu.
- Zdroje informací pro hodnocení nebo přezkum, jako jsou funkční vývojové diagramy, zásady, normy, postupy a pracovní dokumenty z předchozího auditu, testovací skripty.
- Kritéria pro vyhodnocení testů.
- Kontakty pro administrativní a logistická opatření.
- Komunikační plán, který popisuje, komu, kdy, jak často a jak sdělovat, případně pro jaké účely.

(Information Systems Auditing: Tools and Techniques: Creating Audit Programs, 2016)

Při samotném výkonu auditu, auditorský tým realizuje plán vytvořený pro audit a provádí podrobné zkoumání procesů, prostředků a kontrol, porovnávající shromážděné důkazy o organizaci a jejich schopnostech a postupech se stanovenými požadavky v kritériích auditu, příslušných protokolech nebo použitelných standardech. Činnosti spojené s prováděním auditu zahrnují, že auditoři prověřují veškerou dokumentaci a kontextové informace, které jsou k dispozici o předmětu auditu, shromažďování důkazů prostřednictvím pozorování, rozhovory a testy a analýza těchto důkazů za účelem zjištění slabých stránek, kontroly nedostatky nebo jiné problémy. (Gantz, 2013)

V posledních fázích se ohlašují zjištěné nedostatky nebo neshody s kritériemi, jelikož tyto oblasti představují zdroje rizika, na které musí auditovaná organizace reagovat a zpracovává auditorská zpráva. V závislosti na cílech auditu a zamýšleném publiku pro auditorskou zprávu může obsah zprávy zahrnovat uspokojivá zjištění a oblasti shody, jakož i slabosti nebo nedostatky. (Gantz, 2013)

2.2 Vymezení pojmu audit informačního systému

V ČR se audit informačních systémů začal prosazovat v roce 1996 a lze jej definovat jako proces vyhodnocování účinnosti, hospodárnosti a bezpečnostních postupů informačního

systému k zajištění ochrany integrity dat a toho, že systém splňuje příslušné zásady, postupy, normy, pravidla, zákony a předpisy. (Majdalawieh, 2009)

Audit informačních technologií zkoumá procesy, prostředky IT a kontroly na více úrovních v rámci organizace, aby určil, do jaké míry se organizace řídí příslušnými standardy nebo požadavky. Prakticky všechny organizace využívají IT k podpoře svých operací a dosahování svých úkolů a obchodních cílů. To dává organizacím oprávněný zájem na zajištění toho, aby jejich využívání IT bylo efektivní, aby systémy a procesy IT fungovaly podle plánu a aby byla aktiva IT a další zdroje účinně přidělovány a náležitě chráněny. Audit IT pomáhá organizacím pochopit, posoudit a zlepšit jejich používání k zabezpečení IT, měření a správného výkonu a dosažení cílů a zamýšlených výsledků. (Gantz, 2013)

2.2.1 Formy auditu IS

Formy auditu lze rozlišovat na základě několika hledisek:

- Hledisko komplexnosti - ověření, audit, prověrka, dohodnutá procedura, kontrola.
- Hledisko realizátora - sebehodnocení, interní audit, externí audit.
- Hledisko objektu hodnocení - audit obecných kontrol, audit aplikací, audit vývoje systémů, technický nebo specializovaný audit, audit interních kontrol, audit souladu, audit výkonu.
- Hledisko úrovně řízení - organizace jsou vždy součástí vyšších organizačních entit, záleží na tom z jaké úrovně řízení se audit provádí.
- Hledisko časové - jednorázový audit, opakující se audit, průběžný audit.
- Hledisko metodologie - audit věcné správnosti, audit založený na kontrolách, audit založený na riziku, procesně orientovaný audit.

Audit IS má zejména formu auditu interních kontrol. Můžeme být testován jak návrh kontrol, tak skutečná realizace kontrol s cílem hodnotit jejich existenci, hospodárnost a účelnost. Součástí každého druhu auditu IS může být rovněž audit souladu, pokud je jeho cílem stanovit míru souladu dodržování stanovených politik, nařízení, standardů, vyhlášek, zákonů apod. (Svatá, 2018)

2.2.2 Prvky auditu IS

Jak už bylo zmíněno, audit informačního systému se netýká pouze samotného počítače. Dnešní informační systémy jsou komplexní a mají mnoho komponent, které jejich spojením tvoří obchodní řešení. Záruku správného řešení informačního systému lze získat pouze tehdy, jsou-li všechny komponenty hodnoceny a zabezpečeny. (Svatá, 2018)

Hlavní prvky auditu IS jsou fyzická a environmentální kontrola, kdy sem patří fyzická bezpečnost, napájení, klimatizace, regulace vlhkosti a další faktory prostředí. Kontrola správy systému, která zahrnuje kontrolu zabezpečení operačních systémů, systémů správy databází, všech postupů správy systému a dodržování předpisů. Revize aplikačního softwaru, kdy aplikační software může být výplatní listina, fakturace, webový systém zpracování zákaznických objednávek nebo systém plánování podnikových zdrojů. Přezkum takového aplikačního softwaru zahrnuje řízení přístupu a autorizace, ověření, zpracování chyb a výjimek, toky obchodních procesů v aplikačním softwaru a doplňkové manuální kontroly a postupy. Kontrola zabezpečení sítě, pro kterou typické oblasti pokrytí jsou kontrola interních a externích připojení k systému, obvodové zabezpečení, kontrola brány firewall, řízení přístupu k routeru, skenování portů a detekce narušení. Kontrola kontinuity provozu, kdy sem patří existence a údržba redundantního hardwaru odolného proti chybám, zálohovacích procedur a úložiště a zdokumentovaného a testovaného plánu obnovy po havárii. Přezkum integrity dat, kdy cílem je kontrola skutečných údajů, za účelem ověření přiměřenosti kontrol a dopadu slabých stránek, jak bylo zjištěno při kterémkoli z výše uvedených přezkumů. Takové testování věcné správnosti může být provedeno s pomocí auditorského softwaru. (Sayana, 2002)

2.2.3 Regulace auditu IS

Ne všechny standardy a certifikace personálu vztahující se k auditu IT pocházejí z oborů specifických pro audit, ale jak už bylo zmíněno v předchozích kapitolách, externí i interní audit prakticky ve všech organizacích je do jisté míry ovlivněn standardy, zásadami a pokyny vypracovanými organizacemi zaměřenými na audit nebo obecně vývoj standardů. (Gantz, 2013)

V souvislosti s auditováním IS je důležité regulovat samotnou profesi auditora IS. Regulovány jsou postavení, postupy, nástroje a další náležitosti, které jsou společné všem auditům bez ohledu na objekt auditu. Nejznámější organizací zajišťující výše uvedené regulace je ITAF, která reprezentuje organizaci ISACA a představuje nejkomplexnější regulaci profese auditora IS. (Svatá, 2018)

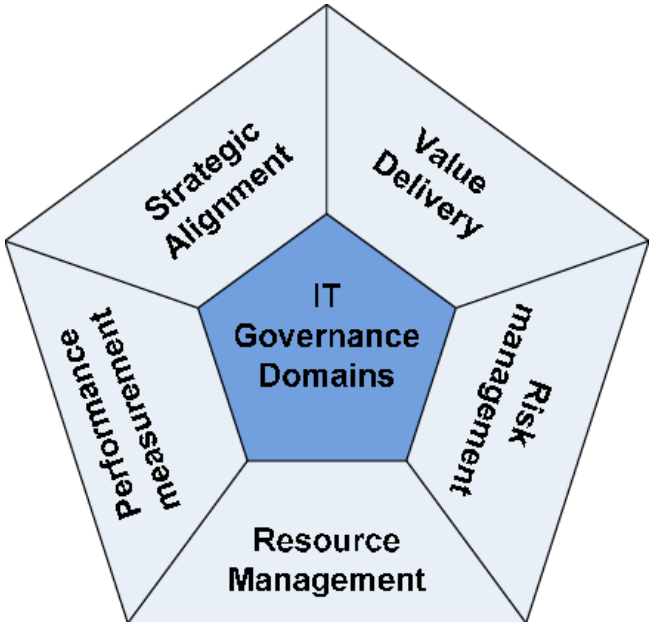
Nutné je také regulovat vlastní audit, ve formě objektivních měřítek, o která se může auditor při realizaci různých druhů auditu opřít. Nejznámější organizací zajišťující tyto regulace je ISO, která společně s organizací IEC vytvořila technický výbor ISO/IEC JTC 1. Následně tento výbor vytváří standardy v oblasti IT. Jelikož důležitou součást auditu informačního systému v organizacích tvoří bezpečnost informací, jejich řízení a hodnocení je třeba regulovat i samotnou informační bezpečnost. Především, že informace jsou správné, úplné a přístupné, nebo sděleny pouze těm, kteří k tomu mají oprávnění. (Svatá, 2018)

2.2.4 IT Governance

Governance IT je odpovědností vedoucích pracovníků a představenstva a skládá se z vedení organizace, organizačních struktur a procesů, které zajišťují, aby podnikové IT udržovalo a rozšiřovalo strategie a cíle organizace. (COBIT 4.1, 2007)

Governance IT dále integruje a institucionalizuje osvědčené postupy, aby zajistila, že podnikové IT podporuje obchodní cíle. Governance IT umožňuje organizaci plně využít její informace k maximalizaci užitku a využít příležitost pro získání konkurenční výhody. Tyto výstupy vyžadují rámec pro kontrolu IT, který je podporován Výborem sponzorských organizací interní kontroly Komise pro koridor Treadway (COSO). Jedná se o široce uznávaný integrovaný, kontrolní rámec pro řízení podniků a řízení rizik. (COBIT 4.1, 2007)

Obrázek 1: oblasti zaměření IT governance



Zdroj: (Wahab & Arief, 2015)

IT governance vyžaduje značný čas a pozornost managementu, jelikož úspěšná IT governance sjednocuje rozhodnutí managementu a využití IT s požadovaným chováním a obchodními cíli. Mezi důležité otázky patří, jaká rozhodnutí musí být provedena a kdo by je měl provést, k tomu je vhodné sestavit matici, která by obsahovala vymezení obchodních rolí, definici požadavků na integraci a standardizaci, stanovení sdílených a dostupných služeb, určení účelu zakoupených nebo interně vyvinutých IT aplikací, výběr iniciativ, které se mají financovat, a kolik za ně utratit. (Weill & Ross, June 1, 2004)

2.2.5 Metodiky

Zatímco některé organizace mohou upřednostňovat zaměření na jediný kontrolní rámec a odpovídající soubor auditorských standardů a postupů, jiné považují za účinnější rozlišit různé potřeby auditu a oblasti důrazu a zvolit specializované auditorské přístupy pro každou předmětnou oblast. (Gantz, 2013)

V rámci auditování se lze opřít o relevantní dokumenty obsahující metodické informace. V souvislosti s informačními systémy se jedná o metodiky COBIT, COSO, ITIL, ISO 17799 a ISO 38500. Metodika COBIT je pevně spojena s organizací ISACA a jedním ze základních nástrojů podporujících IT Governance v organizacích. (Svatá, 2018)

COSO byla založena pro podávání zpráv na podporu Národní komisi pro podvodné finanční jednání. Přístup COSO spočívá v tom, že vnitřní kontrolní proces je prováděn představenstvem nebo vedením účetní jednotky, za účelem poskytnutí přiměřené jistoty pro splnění cílů v rámci některých konkrétních oblastí (účinnost a efektivnost operací, spolehlivost finančního výkaznictví, soulad s platnými zákony a předpisy). Interní rámec COSO zahrnuje oblasti zájmů, které se týkají činnosti manažera, jako osob odpovědných za podnikání, jsou jimi kontrolní prostředí, odhad rizika, informace, komunikace a monitorování. (Gheorghe, 2010)

Obrázek 2: rámec metodiky COSO

Zdroj: (Surjadi et al., 2015)

ITIL (Knihovna infrastruktury informačních technologií) představuje soubor osvědčených postupů pro správu IT služeb, a to jak v oblasti zavedení, tak i zlepšení. Ve své podstatě ITIL vyjadřuje důležitost pro soulad IT služeb s potřebami podniku a podporuje jeho základní procesy poskytováním poradenství v souvislosti s používáním nástrojů IT v podnikání. ITIL jako procesně a obchodně orientovaný se skládá z pěti hlavních procesů, kterými jsou strategie služeb, návrh služeb, přechod služeb, provoz služeb a neustálé zlepšování služeb. (Drljača & Latinović, 2016)

Obrázek 3: Model životního cyklu ITIL

Zdroj: (Evelina et al., 2010)

ISO 17799 (ISO 27002) představuje kodex osvědčených postupů pro management informačních technologií. Slouží jako průvodce pro provádění souboru politik a postupů s cílem konsolidovat informační bezpečnost spravovanou organizací. Provádění této normy představuje konkurenční výhodu pro každou organizaci, která prokáže, že informační bezpečnost je dobře kontrolovaný proces. ISO / IEC 27002 vyžaduje, aby management systematicky zkoumal v organizaci bezpečnostní rizika informací, s přihlédnutím k hrozbám, zranitelnosti a dopadům, navrhoval a implementoval koherentní a komplexní sadu kontrol informační bezpečnosti, zajistil soulad kontroly zabezpečení informací s potřebami organizace v oblasti zabezpečení informací. (Gheorghe, 2010)

ISO 38500 představuje soubor pravidel pro vyšší úroveň řízení organizace, které reprezentují právní, regulační a etické zásady týkající se využívání IT v organizaci. Standard je založen na šesti klíčových principech, odpovědnost, strategie, akvizice, výkon, soulad a lidské chování. Standard dále stanovil přesné úkoly pro ředitele v souvislosti se správou IT. Tyto úkoly jsou z oblastí vyhodnocování, řízení a monitorování. (Gheorghe, 2010)

2.2.6 COBIT

COBIT je zkratka odvozena z Control Objectives for Information and related Technology. Rámec poskytuje osvědčené postupy a praktiky. Tyto postupy pomohou organizaci dosáhnout strategických cílů pomocí efektivního využití dostupných zdrojů a minimalizace IT rizik. (COBIT 4.1, 2007)

Konkrétně kontrolní rámec COBIT přispívá k těmto potřebám tím, že:

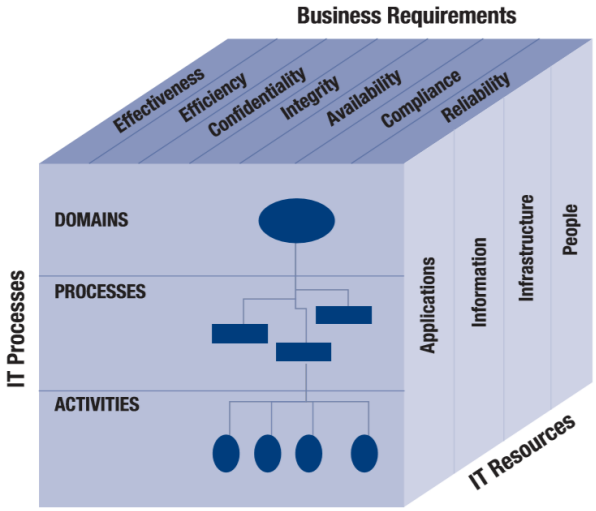
- Vytvoří spojení na obchodní požadavky.
- Uspořádá IT aktivity do obecně přijímaného procesního modelu.
- Identifikuje hlavní zdroje IT, které mají být využívány.
- Definuje kontrolní cíle řízení, které je třeba zvážit.

(COBIT 4.1, 2007)

COBIT vzájemně propojuje řízení podniku a řízení informatiky. Je toho docíleno propojením podnikových a IT cílů, definováním metrik a modelů zralosti pro měření dosahování cílů a definováním odpovědností vlastníků podnikových a IT procesů. (COBIT 4.1, 2007)

V roce 1996 byla vydána první verze organizací ISACA. Tato první verze obsahovala samotný rámec, následně druhá verze byla doplněna o auditní postupy, sadu implementačních nástrojů a rozpracované procesy kontroly. Další vydání, konkrétně třetí bylo rozšířeno o manažerské postupy. Současná verze je COBIT 5 a rozšiřuje COBIT 4.1. (“COBIT 5 (Control Objectives for Information and related Technology)”, c2016)

Obrázek 4:rámec COBIT ilustrovaný COBIT kostkou



Zdroj: (COBIT 4.1, 2007)

Procesní model COBITu rozděluje IT do 4 domén a 34 procesů v souladu s oblastmi odpovědnosti plánovat, budovat, provozovat a monitorovat a poskytovat komplexní pohled na IT. Jednotlivé domény se nazývají:

- Plánovat a organizovat (PO) - poskytuje směr k dodání řešení (AI) a poskytování služeb (DS).
- Získat a implementovat (AI) - poskytuje řešení a předává je, aby se proměnily ve služby.
- Dodání a podpora (DS) - přijímá řešení a činí je použitelnými pro koncové uživatele.
- Monitorovat a vyhodnocovat (ME) - monitoruje všechny procesy, aby zajistil, že se bude postupovat podle daného směru

COBIT pak definuje procesy IT v jednotlivých doménách:

Plánování a organizace (Plan and Organize PO)

- PO1 Define a strategic IT plan - Definice strategického plánu IT
- PO2 Define the information architecture - Definice informační architektury
- PO3 Determine technological direction - Determinace technologického směru

- PO4 Define the IT processes, organisation and relationships - Definice IT procesů, určení organizace a vzájemných vztahů mezi procesy
- PO5 Manage the IT investment - Správa investic do IT
- PO6 Communicate management aims and direction - Sdílení manažerských cílů a směrů
- PO7 Manage IT human resources - Řízení lidských zdrojů v IT
- PO8 Manage quality - Řízení jakosti
- PO9 Assess and manage IT risks - Určení a řízení rizik IT
- PO10 Manage projects - Řízení projektů

Akvizice a implementace (Acquire and Implement AI)

- AI1 Identify automated solution - Identifikace automatizovaných řešení
- AI2 Acquire and maintain application software - Pořízení a údržba aplikačního software
- AI3 Acquire and maintain technology infrastructure - Pořízení a údržba technologické infrastruktury
- AI4 Enable operation and use - Postoupení a provoz programového vybavení
- AI5 Procure IT resources - Zajištění zdrojů IT
- AI6 Manage changes - Řízení změn
- AI7 Install and accredit solutions and changes - Zavedení a prověření úprav a změn

Dodávka a podpora (Deliver and Support DS)

- DS1 Define and manage service levels - Definice a řízení úrovně služeb
- DS2 Manage third-party service - Řízení služeb třetích stran
- DS3 Manage performance and capacity - Řízení výkonnosti a kapacity
- DS4 Ensure continuous service - Zajištění kontinuálních služeb
- DS5 Ensure systems security - Zajištění bezpečnosti systému
- DS6 Identify and allocate costs - Identifikace a alokace nákladů
- DS7 Educate and train users - Vzdělání a školení uživatelů
- DS8 Manage service desk and incidents - Řízení service desku a incidentu
- DS9 Manage the configuration - Řízení konfigurace

- DS10 Manage problems - Řízení problémů
- DS11 Manage data - Řízení dat
- DS12 Manage the physical environment - Řízení okolí
- DS13 Manage operations - Řízení provozu

Monitoring a evaluace (Monitor and Evaluate ME)

- ME1 Monitor and evaluate IT performance - Průběžné sledování a hodnocení výkonnosti IT
- ME2 Monitor and evaluate internal control - Průběžné sledování a hodnocení interních kontrol
- ME3 Ensure compliance with external requirements - Získávání nezávislého posudku
- ME4 Provide IT governance - Realizace IT Governance

(COBIT 4.1, 2007)

2.3 Vymezení pojmu ERP

Systém plánování podnikových zdrojů (Enterprise resource planning) je plně integrovaný systém řízení podniku zahrnující funkční oblasti podniku, jako je logistika, výroba, finance, účetnictví a lidské zdroje. Organizuje a integruje provozní procesy a informační toky za účelem optimálního využití zdrojů, kterými jsou lidé, materiál, peníze a stroje. ERP systémy představují jednu databázi, aplikaci a uživatelské rozhraní pro celý podnik a zejména pro hlavní funkční oblasti podniku, kterými jsou výroba, distribuce, financování a prodej. (“An Overview of Enterprise Resource Planning (ERP)”)

Každý systém musí mít několik klíčových funkcí, aby mohl reprezentovat ERP řešení. Těmito klíčovými funkcemi jsou:

- Flexibilita, aby systém reagoval na měnící se potřeby podniku.
- Modularita a otevřenost, kdy systém musí mít otevřenou systémovou architekturu, aby jakýkoliv modul mohl být kdykoliv je to třeba propojen nebo odpojen, aniž by to ovlivnilo ostatní moduly.

- Měl by podporovat více hardwarových platforem kvůli organizacím, které mají heterogenní systémy.

- Komplexnost, jelikož ERP by měl být schopen podporovat různé organizační funkce a musí být vhodný pro širokou škálu obchodních organizací.
- Připojení mimo společnost, aby systém nebyl omezen hranicemi organizace, ale podporoval i připojení k jiným obchodním subjektům organizace. (“An Overview of Enterprise Resource Planning (ERP)”)

ERP tvoří základ organizace a jsou zejména odpovědné za operace s údaji, informacemi a interními znalostmi organizace. Jádro ERP musí spravovat interní data, které jsou organizovány v datových skladech a odkud jsou extrahovány a analyzovány pomocí systémů na podporu rozhodování a nástrojů typu OLAP nebo OLTP. Tím také poskytují solidní platformu pro získání historických za účely jejich analýzy. Integrace lze dosáhnout na kterékoli obchodní úrovni pomocí jakéhokoliv typu technologie. (Cristescu & Stancu, 2019)

Implementací ERP systému pak mohou v organizaci vzniknout nová rizika. Proto následně jejich hodnocení a kontrola vyžaduje určitý rámec, který pokrývá oblast řízení podnikových procesů, zabezpečení aplikace, technologické infrastruktury a projektového managementu. (Deloitte Touche Tohmatsu Research Team & ISACA, 2006)

2.3.1 Vlastnosti

Mezi charakteristické vlastnosti ERP systému patří:

- Podpora více platforem, více zařízení, více výrobních režimů, více měnových jednotek a jedná se o lingvální systém.
- Pokrývá všechny funkční oblasti, jako je výroba, prodej a distribuce, závazky, pohledávky, zásoby, účty, lidské zdroje, nákupy a jiné činnosti a zvyšují kvalitu zákaznického servisu, čímž zvyšují image společnosti.
- Překlenuje informační mezeru napříč organizacemi. Poskytuje kompletní integraci systémů nejen napříč odděleními, ale také napříč společnostmi pod jednou správou.

- Umožňuje automatické zavádění nejnovějších technologií, jako je elektronický převod prostředků (EFT), elektronická výměna dat (EDI), internet, intranet, videokonference, elektronický obchod atd.
- Eliminuje většinu obchodních problémů, jako je nedostatek materiálu, zvýšení produktivity, zákaznický servis, správa hotovosti, problémy se zásobami, problémy s kvalitou, rychlé dodání a jiné.
- Poskytuje inteligentní obchodní nástroje, jako je systém podpory rozhodování, výkonný informační systém, dolování dat a snadné pracovní systémy, které umožňují lepší rozhodování.

(“An Overview of Enterprise Resource Planning (ERP)”)

2.4 SAP

2.4.1 SAP SE

Název společnosti SAP je odvozen ze Systems, Applications a Products in Data Processing přeloženo z německého Anwendungen und Produkte in der Datenverarbeitung. SE znamená Societas Europaea. Jedná se o mezinárodní softwarovou společnost sídlící ve Walldorfu v Německu. Společnost byla založena v roce 1972, 5 podnikateli a zároveň bývalými zaměstnanci společnosti IBM, konkrétně jimi byli Dietmar Hopp, Hasso Plattner, Hans Werner Hector, Klaus Tschira a Claus Wellenreuther. V této době pojmenovali společnost Systemanalyse und Programmentwicklung (SAPD). Následně se název společnosti ještě několikrát změnil až na současné SAP SE. V roce 1973 uvedla svůj první produkt na trh, kdy se jednalo o systém finančního účetnictví. Na základě toho mohl následně vzniknout systém nazvaný R/1 skládající se z několika modulů. (“About SAP SE”), (“SAP History”)

2.4.2 Produkty SAP

Společnost má mnoho produktu v této práci jsou uvedeny pouze ty nejvýznamnější.

Prvním produktem společnosti byl v roce 1973 systém pro finanční účetnictví (RF). Na základě tohoto systému byl vyvinut software s názvem R/1, který se skládal z několika modulů. V roce 1979 SAP rozšířil možnosti systému do dalších oblastí pod názvem R/2.

V roce 1992 SAP uvedl R/3, u kterého bylo zveřejněno hned několik verzí. Jakmile se SAP zaměřil místo mainframe na klient - server architekturu, nástupcem systému R/3 se stal v roce 2004 SAP ERP Central Component. Poslední verze SAP ERP vyšla v roce 2006 a jedná se o verzi 6.0 od této doby byla dále pouze rozšiřována balíčky, kdy poslední je z roku 2016. V roce 2014 začala společnost spolupracovat s IBM za účelem prodeje cloudově založených služeb. Další významnou spoluprací je se společností Microsoft za účelem poskytnutí zákazníkům nástroje pro vizualizaci dat a ke zlepšení mobilních aplikací. V roce 2015 společnost uvedla systém 4HANA, který nabízí zákazníkům možnost cloudového, místního a hybridního nasazení. Mezi výhody patří menší datová stopa, vyšší propustnost, rychlejší analýzy a rychlejší přístup k datům. Jedná se o novou generaci SAP Business Suite. Dalším produktem je SAP HANA, který byl vytvořen pro spuštění na osobních počítačích. (“All Products”)

2.5 SAP ERP

2.5.1 Moduly a operace

SAP ERP tvoří operace (prodej a distribuce, správa materiálů, plánování výroby, provádění logistiky a řízení kvality), finance (finanční účetnictví, manažerské účetnictví, řízení finančních dodavatelských řetězců), řízení lidského kapitálu (školení, mzdy, e-nábor) a firemní Služby (správa cest, životní prostředí, zdraví a bezpečnost a správa nemovitostí). (Slooten & Yap, 1999)

Integrovaný software podnikových procesů SAP R/3 zahrnuje moduly finance, účetnictví a kontrolu, prodej a distribuci, správu výroby a materiálů, řízení kvality a údržbu zařízení, lidské zdroje a řízení projektů. Informační systémy navíc automaticky sumarizují provozní data do významných informací, které slouží jako podpora při rozhodování a pro kontrolu kritických faktorů úspěchu na všech úrovních podnikání. Hlavní důvody implementování SAP řešení jsou:

- Přepracování společných funkcí za účelem zlepšení kvality informací a snížení nákladů.
- Zlepšení stávající provozní struktury.
- Výměna zastaralých systémů a procesů.

- Zlepšení integrity a dostupnosti dat.

(Slooten & Yap, 1999)

Modul SAP FI je integrován do logistického řetězce, který začíná získáváním a končí zaplacením a distribucí. Účtová osnova slouží jako základ pro všechny automatické integrované účtování. obchodní transakce se zadávají a ukládají do databáze ve formě dokumentů. FI systém podporuje generování výkazu zisku a ztráty a rozvahy v reálném čase. FI zahrnuje následující dílčí moduly:

- Hlavní knihu
- Pohledávky
- Splatné účty
- Účtování aktiv
- Účetní knihu pro zvláštní účely
- Právní konsolidace

(Deloitte Touche Tohmatsu Research Team & ISACA, 2006)

Modul SAP CO se zaměřuje na funkce manažerského účetnictví, jako je účtování nákladů a analýza ziskovosti. CO zahrnuje následující dílčí moduly:

- Účetnictví ziskového centra
- Účetnictví nákladového střediska
- Kontrolu nákladů na produkt
- Analýzu ziskovosti
- Kalkulaci na základě aktivity
- Interní objednávky

(Deloitte Touche Tohmatsu Research Team & ISACA, 2006)

Modul SAP SD provádí prodejní, distribuční, přepravní, cenové a fakturační funkce. Automatizuje administrativní práci od okamžiku vytvoření nabídky zákazníka až po distribuci a fakturaci zboží. Zlepšuje schopnost dodávat produkty včas. Mezi klíčové dílčí moduly patří:

- Podpora prodeje

- Odbyt
- Lodní doprava
- Fakturace
- Přeprava

(Deloitte Touche Tohmatsu Research Team & ISACA, 2006)

Modul SAP MM řídí různé funkce související se zásobami a nákupy, včetně nákupu a přijímání zboží, řízení a oceňování zásob a řízení skladu. Dílčí moduly v MM zahrnují:

- Řízení zásob
- Řízení skladu
- Nákup
- Ověření faktury

(Deloitte Touche Tohmatsu Research Team & ISACA, 2006)

Modul SAP PP řídí různé funkce související s plánováním a zpracováním výroby. Sleduje nákup, skladování a převod materiálů a meziproduktů. Důležitou součástí jsou pracovní centra, účty za materiál a postupy. Submodody v PP zahrnují:

- Plánování materiálových požadavků
- Kanban
- Plánování produkce
- Výrobní zakázky
- Prodej a plánování operací

(Deloitte Touche Tohmatsu Research Team & ISACA, 2006)

Modul SAP PM řídí všechny funkce související s údržbovými činnostmi, zejména kontrolu, preventivní údržbu a opravy. Dílčí moduly v PM zahrnují:

- Preventivní údržbu
- Zpracování údržby
- Projekty údržby
- Řízení pracovního odbavení

(Deloitte Touche Tohmatsu Research Team & ISACA, 2006)

Modul SAP PS se používá k plánování, správě, sledování a účtování projektů. PS má neustálý přístup k datům ve všech ostatních odděleních zapojených do projektu, což umožňuje organizační řízení projektu. PS nemá žádnou vlastní organizační strukturu, ale je začleněn do stávající struktury organizačních jednotek v účetnictví a logistice. (Deloitte Touche Tohmatsu Research Team & ISACA, 2006)

2.5.2 Prostředí a základy

Tato kapitola obsahuje seznam základních pojmů a znalostí, který jsou významné pro pochopení prostředí auditovaného systému a jeho rizikových oblastí.

Transakce

Každá funkce v systému SAP je spojena s kódem transakce. Kód transakce se skládá z písmen, čísel nebo z obou. Pomocí kódu transakce lze rychleji přejít na jakoukoli úlohu v aplikaci SAP. (Working with Transaction Codes)

V tabulce 1 jsou uvedeny transakce užitečné pro zpracování praktické části této práce:

Tabulka 1: Užitečné transakční kódy

Transakční kód	Popis
SPRO	Konfigurace a provedení všech modulů
SA38	Provedení všech programů a reportů
SE11	Správa slovníku ABAP
SE12	Zobrazí slovník ABAP
SE15	ABAP Repository information system
SE16	Prohlížeč dat
SE37	Zpřístupní sestavené funkce
SE38	Editování všech programů a reportů
SE80	Navigátor objektů
SQ01	Správa dotazů
AL01	Monitor výstrah
RZ20	Monitorování CCMS
SM01	Uzamknutí transakce

Transakční kód	Popis
SM13	Aktualizační požadavky
SM30	Údržba tabulek
SM31	Údržba tabulek
SM35	Spuštění dávkových vstupů
SM36	Definování dávkových úloh
SM37	Sledování dávkových úloh
SM49	Spuštění příkazů externího OS
SM64	Správa událostí na pozadí
SM69	Údržba příkazů externího OS
PFCG	Genarátor profilů pro udržování autorizačních rolí
SCC4	Správa klienta
SCC5	Vymazání klienta
SU01	Údržna uživatele
SU02	Údržba autorizačních profilů
SU03	Autorizační objekty a třídy
FD02	Změna zákazníka (účetnictví)
VD02	Změna zákazníka (prodej)
XD02	Změna zákazníka (centrálně)
FK01	Vytvořit dodavatele (účetnictví)
FK02	Změna dodavatele (účetnictví)
FK05	Zablokovat dodavatele (účetnictví)
MK01	Vytvořit dodavatele (nákup)
MK02	Změna dodovatele (nákup)
MK05	Zablokovat dodavatele (nákup)
XK01	Vytvořit dodavatele (centrálně)
XK02	Změnit dodavatele (centrálně)
XK05	Zablokovat dodavatele (centrálně)
MM01	Vytvořit materiál
MM02	Změnit materiál
DB12	Zálohovací protokoly databáze

Zdroj: (Schreckenbach, 2011)

Autorizační objekty

Objekty autorizace sdružují jedno nebo více polí, jejichž kombinace udává akci v systému SAP. To obvykle zahrnuje několik možných aktivit (například vytváření, změna nebo zobrazení) v souvislosti s objektem v systému (například tabulka nebo role autorizace). V této souvislosti aktivita a objekt představují pole v rámci autorizačního objektu. Uživatelé mohou provádět akce v systému SAP, pouze pokud mají příslušné oprávnění. Pokud nemají povolení pro konkrétní akce, nemusí je provést. Uživatelé získají oprávnění k provedení akce přiřazením požadované autorizace. To se provádí prostřednictvím autorizačních rolí nebo pomocí autorizačních profilů. (Schreckenbach, 2011)

Kompozitní profily

Výkonné profily SAP_ALL, pokud má některý z uživatelských účtů přiřazen tento profil, tak je mu automaticky umožněno spouštět libovolné transakce a přistupovat do vývojového prostředí a SAP_NEW, tento profil je využíván v situaci, kdy se chystá upgrade systému, jelikož eliminuje možnost ohrožení funkcionality systému a jeho klíčových procesů. (Fišer, 2017)

Klienti

Oblast obsahující nezávislá aplikační data v systému. V jednom systému může paralelně existovat několik klientů, přičemž každý klient představuje samostatnou jednotku, pokud jde o kmenová a aplikační data. Klienti v systému sdílejí různé systémové prostředky napříč ostatními klienty, například instance SAP, databázi a slovník ABAP. (Schreckenbach, 2011)

IMG

Online manuál využívaný k usnadnění konfigurace SAP R/3. Může být zpřístupněn prostřednictvím transakčního kódu SPRO, který zahrnuje globální nastavení, organizační model (OM), činnosti pro implementování každého modulu SAP/R3, vlastnosti určené pro dokumentaci a monitorování implementace. (Deloitte Touche Tohmatsu Research Team & ISACA, 2006)

Tabulky

Tabulky lze definovat nezávisle na databázi ve slovníku ABAP. Pole v tabulce jsou definována s jejich datovými typy a délkami. (Tables)

ABAP/4

Advanced Business Application Programming/4. Programovací jazyk 4. generace a hlavní programovací jazyk SAP R/3. ABAP/4 Workbench (TSC S001) představuje vývojové prostředí pro SAP R/3 systém. Poskytuje nástroje pro pro programování, navigaci, debugování a kontrolní vývoj. (Deloitte Touche Tohmatsu Research Team & ISACA, 2006)

ABAP slovník

Slovník ABAP se používá k vytváření a správě definic dat (metadata). Slovník ABAP umožňuje centrální popis všech dat použitých v systému bez redundancí. Nové nebo upravené informace jsou automaticky poskytovány pro všechny systémové komponenty. Tím je zajištěna integrita dat, konzistence dat a bezpečnost dat. Podporuje uživatelem definované typy (datové prvky, struktury a typy tabulek). (ABAP Dictionary)

SAP Query

SAP Query se používá k vytváření sestav, které nejsou obsaženy ve výchozím nastavení, slouží především uživatelům s malou nebo žádnou znalostí programovacího jazyka ABAP. Query nabízí uživatelům širokou škálu způsobů definování reportovacích programů a vytváření různých typů reportů. (SAP Query)

CCMS

Monitor výstrah CCMS (Monitorovací systém pro správu výpočetního centra) umožňuje živé monitorování systémů SAP v reálném čase. Kromě toho ho lze také použít k řízení a konfiguraci. Monitory, které poskytuje CCMS jsou pro spuštění a zastavení systémů a instancí SAP, zpracování a řízení úloh na pozadí, plánování záloh databází, konfiguraci systému SAP a sledování systému a automatické hlášení výstrah. (Schreckenbach, 2011)

Dávkové zpracování

V systému SAP se dávkové úlohy nazývají úlohy na pozadí. Jsou prováděny bez ohledu na to, zda je uživatel přihlášen k systému nebo ne. (Schreckenbach, 2011)

Protokolování

Systém SAP zaznamenává všechny systémové chyby, varování, zámky uživatelů v důsledku neúspěšných pokusů o přihlášení a zpracovává zprávy do systémového

protokolu. Každý aplikační server SAP System má místní protokol, který přijímá všechny zprávy odeslané tímto serverem. (The System Log)

2.5.3 Nástroje pro SAP audit

Ve výchozím nastavení má systém SAP několik nástrojů pro poskytování podpory při provádění úkolů správy systému souvisejících s bezpečností. K těmto nástrojům patří Informační systém auditu (AIS) a Protokol auditu zabezpečení. (Schreckenbach, 2011)

Informační systém auditu (AIS) byl vyvinut pro systémové a obchodní audity a zahrnuje zprávy, které automaticky analyzují určité aspekty zabezpečení systému. Díky těmto zprávám již není nutné ručně zpracovávat jednotlivé body auditu, analyzovat tabulky nebo psát programy auditu. Auditoři proto rádi používají systém AIS při auditování. (Schreckenbach, 2011)

Protokol auditu zabezpečení hraje důležitou roli pro správce systému SAP, když monitorují akce související s bezpečností v systému. Protokol zabezpečení auditu lze použít k protokolování a následné analýze různých typů uživatelských činností, například:

- Pokusy o přihlášení do systému.
- Změna a zamykání kmenových dat uživatele.
- Změna a generování oprávnění.
- Spuštění a zastavení aplikačního serveru.
- Změny v konfiguraci protokolu auditu zabezpečení.

(Schreckenbach, 2011)

3 Metodický postup

3.1 Teoretická východiska

První část diplomové práce je věnována specifikaci pojmu audit a audit informačního systému, včetně vymezení náležitostí s nimi souvisejících. Je zde vysvětlen postup auditu, druhy auditu a jeho regulace.

V další části této práce jsou definovány některé metodiky využívané pro audit IS a obecná specifikace ERP systémů včetně hlavních charakteristik a vlastností. Je zde vysvětlena metodika COBIT, její zaměření a části.

Poslední kapitola teoretické části diplomové práce je zaměřena na samotnou organizaci SAP, její vznik, vývoj, podstatu a představení jednotlivých produktů.

3.2 Cíl diplomové práce

Cílem práce je popsat princip auditu ERP SAP a prakticky provést takový audit na systému provozovanému pro výukové účely na Ekonomické fakultě. Zmapovat způsob administrace uživatelů, zmapovat oddělení pravomocí v procesech, příslušné změnové řízení, a případně určitý procesní audit související se shora uvedenými činnostmi. Ukázat nástroje SAP pro takový bezpečnostní audit, jako je např. SAP Repository Information System. Dále navrhnout případné změny ve způsobu administrace uživatelů apod.

3.3 Předmět a plán auditu

Audit informačního systému je prováděn s odkazem na metodiku COBIT, která byla již představena v teoretické části této práce. Bylo zmíněno, že metodika COBIT slouží jako podpora při auditování informačního systému v prostředí organizace, kdy kromě samotného informačního systému bere ohled i na procesy, které uvnitř organizace probíhají.

Auditovaným systémem v této práci je konkrétně ERP systém SAP, využívaný v akademickém prostředí pro výukové účely. Cíl diplomové práce je orientován do oblasti

administrace a její bezpečnosti, proto právě tato oblast bude s odkazem na metodiku auditována.

S ohledem na kapitolu 2.1.5, bude postup auditu následovný. Jak už bylo zmíněno, předmětem auditu je ERP systém SAP určený pro výukové účely, cíl auditu je definován v kapitole 3.2, kdy cíl auditu je zároveň cílem diplomové práce. Audit se bude výhradně týkat pouze SAP systému, nebudou auditovány další jiné komponenty. Nejprve bude představeno prostředí auditovaného systému, následně vybrána relevantní procesní oblast metodiky COBIT v závislosti na cíli auditu a sestaven seznam kontrolních cílů odpovídajících procesní oblasti. Dále bude otestován seznam kontrolních cílů, zpracovány kroky testování a jejich výsledky a na závěr shrnuta a vyhodnocena míra rizika zjištěných nedostatků, případně navrženy změny na základě výsledků testování.

3.4 Prostředí auditovaného systému

Dříve už bylo zmíněno, že ERP systém SAP se nachází v akademickém prostředí na fakultě univerzitní instituce. Systém je využíván pro výukové účely, kde se studenti seznamují s funkcionalitou ERP a simulují obchodní procesy. Odpovědnost za systém spadá pod vybranou katedru. V tomto prostředí má nízkou úroveň propracovanosti a složitosti, proto i klíčové oblasti pro audit jsou právě bezpečnost a administrace, naopak nejsou důležité funkcionality souvisejí s obchodními procesy. V rámci výsledků jsou posuzovány všechny dostupné vzorky od doby zavedení systému. Jedná se zároveň o audit mimořádný a nepředpokládá se tedy jeho opakování.

Základní údaje o auditovaném systému jsou uvedeny v tabulce 2.

Tabulka 2: Základní údaje o auditovaném systému

Základní údaje SAP ERP	
Verze	SAP R/3 6.0
Operační systém	Microsoft Windows Server 2012 R2 Standard
Databáze	Microsoft SQL Server
ID produkčního klienta	120
Zodpovědnost fakultní katedry	• Správa uživatelských účtů • Logická bezpečnost • Konfigurace a monitorování dávkových úloh

Zdroj: Vlastní zpracování

3.5 Vybraný proces metodiky COBIT

V závislosti na prostředí, do kterého je systém zasazen, byl vybrán proces, podle něhož budou stanoveny kontrolní cíle a které budou následně detailně prověřeny a otestovány.

Proces metodiky COBIT, který nejlépe definuje požadovaný audit systému, je proces DS5. Z hlediska administrace, mohou mít uživatelé v rámci výuky přístup k funkcionalitám simulující obchodní procesy a dalším relevantním oblastem pro seznámení se s ERP. Přesto zůstávají oblasti, ke kterým by měli mít přístup pouze s dostatkem informací a s povědomím o následcích, které jejich používáním mohou způsobit. Tedy studenti by především neměli mít přístup k funkcím, které mohou poškodit nebo značně pozměnit systém.

DS5 – Zajištění bezpečnosti systému

Cílem procesu je zajistit bezpečnost systému porozuměním bezpečnostních požadavků, zranitelností a hrozeb, správou identit a oprávnění uživatelů standardizovaným způsobem a pravidelným testováním bezpečnosti. Proces zahrnuje definování bezpečnostních politik, plánu a postupů a sledování, detekování, hlášení a řešení bezpečnostních chyb a incidentů.

Každý proces, který je stanoven v metodice COBIT, je následně rozdělen ještě do několika podrobnějších kontrolních cílů, které jsou definovány v dokumentu IT

Assurance Guide. Zde jsou pro jednotlivé cíle stanoveny hodnotové a rizikové faktory. Pro znázornění cílů, stanovených v dokumentu IT Assurance Guide jsou uvedeny všechny kontrolní cíle procesu DS5 a z toho následně 2 vybrány a detailněji popsány.

Kontrolní cíle:

- DS5.1 Řízení informační bezpečnosti
- DS5.2 Plánování informační bezpečnosti
- DS5.3 Správa autentizace a autorizace
- DS5.4 Správa uživatelských účtů
- DS5.5 Testování, dohled a monitorování bezpečnosti
- DS5.6 Definování bezpečnostních incidentů
- DS5.7 Ochrana bezpečnostních technologií
- DS5.8 Správa kryptografických klíčů
- DS5.9 Prevence, detekce a korekce škodlivých programů
- DS5.10 Bezpečnost sítí
- DS5.11 Výměna citlivých dat

Jelikož konkrétní cíle diplomové práce souvisí zejména s administrací byli vybrány kontrolní cíle DS5.3 a DS5.4.

Kontrolní cíl DS5.3 - Správa autentizace a autorizace

Cílem je zajistit, aby všichni uživatelé (interní, externí a dočasní) a jejich aktivity prováděné v IT systémech (obchodní aplikace, IT prostředí, provoz systému, vývoj a údržba) byly jednoznačně identifikovatelný. Povolit přístup a identifikování uživatelů pomocí mechanismů ověřování. Potvrdit, že přístupová práva uživatelů k systémům a datům jsou v souladu s definovanými a zdokumentovanými obchodními potřebami, a že požadavky pro práci jsou uvedeny u totožnosti uživatele. (IT Assurance Guide: USING COBIT, © 2007)

Ověření návrhu kontrolního cíle DS5.3:

- Zjistit, zda bezpečnostní postupy vyžadují, aby uživatelé a systémové procesy byly jednoznačně identifikovatelní a systémy jsou nakonfigurovány tak, aby vynucovaly ověření před povolením přístupu.
- Pokud jsou pro udělení přístupu předem určené a schválené role, určit, zda tyto role mají jasně vymezené odpovědnosti. Zajistit, aby založení a úprava rolí byla schvalována vlastníkem procesu.
- Zjistit, zda mechanismus zajištění přístupu a ověřování je využíván pro řízení logického přístupu všech uživatelů, systémových procesů, prostředků IT a interních a externích uživatelů.

Proces DS5.4 - Správa uživatelských účtů

Odkázat požadavky, zřizování, pozastavení, úpravy a uzavírání uživatelských účtů a související uživatelská oprávnění na sadu postupů pro správu uživatelských účtů. Zahrnout schvalovací postup, v němž bude uveden vlastník dat nebo systému udělující přístupová oprávnění. Tyto postupy by se měly vztahovat na všechny uživatele, včetně správců (privilegovaných uživatelů) a interních a externích uživatelů, pro běžné a nouzové případy. Práva a povinnosti týkající se přístupu k podnikovým systémům a informacím by měla být smluvně upravena pro všechny typy uživatelů. Provádět pravidelné kontroly všech účtů a souvisejících oprávnění. (IT Assurance Guide: USING COBIT, © 2007)

Ověření návrhu kontrolního cíle DS5.4

- Zjistit, zda existují postupy pro pravidelné vyhodnocování a certifikaci přístupu a oprávnění k systémům a aplikacím.
- Zjistit, zda existují postupy řízení přístupu ke kontrole a správě práv a oprávnění systémů a aplikací podle bezpečnostních zásad organizace a regulačních požadavků.
- Zjistit, zda byly systémy, aplikace a data klasifikovány podle úrovně důležitosti a rizika a zda byli identifikováni a přiřazeni k nim vlastníci procesů.
- Zjistit, zda se zásady, standardy a postupy zajišťování uživatelů vztahují na všechny uživatele a procesy systému, včetně dodavatelů, poskytovatelů služeb a obchodních partnerů.

3.6 Seznam kontrolních cílů

Seznam kontrolních cílů je uspořádán v tabulce 3, kdy jednotlivé cíle jsou navíc odděleny podle oblasti, ve které jsou v systému využívány. Cíle, které byly vybrány mohou značně ovlivnit systém, ať už žádoucím nebo nežádoucím způsobem. Především se jedná o testování autorizovaného přístupu v systému, kdy uživatel bez dostatku kvalifikace může ohrozit jeho správné fungování. Pro každý kontrolní cíl byl využit Repository information system, prostřednictvím kterého byly určeny vhodné autorizační objekty s odpovídajícími hodnotami pro testy. Repository information system může být navíc při vyvolání transakce SU53 využit ke zjištění, zda daný uživatel má odpovídající autorizaci.

Tabulka 3: Seznam kontrolních cílů

Oblast	Kontrolní cíl
instalace systému	IMG
	Úprava kritických tabulek
Vývoj systému	Přizpůsobení a provedení programu ABAP/4
	ABAP/4 Vývoj v produkci
	Datový slovník ABAP
	Dotazy
Operace systému	Konfigurace CCMS
	Dávkové zpracování
	Parametry aplikačního serveru
	Uzamčení transakčních kódů
	Nepovolená hesla
	Zálohování databáze
	Aktualizační požadavky
Bezpečnost systému	Správa zabezpečení
	Zabezpečení SAP* a DDIC uživatele
	Správa výkonných profilů
	Správa výkonných skupin uživatelů
	Protokolování tabulek
Obchodní procesy	Přístup ke kmenovým datům dodavatele, zákazníka a materiálu

Zdroj: Vlastní zpracování

3.7 Testování kontrolních cílů

3.7.1 Průvodce implementací (IMG)

Tabulka 4: Kontrolní cíl IMG

Předmět testování	• přístup k transakčnímu kódu SPRO • přístup k autorizačnímu objektu S_IMG_ACTV • přístup k autorizačnímu objektu S_TRANSPRT s hodnotou 03
Vyžadovaná evidence	• Výstup transakce SCC4 • Výstup reportu RSUSR002

Zdroj: Vlastní zpracování

Riziko: Pokud jsou konfigurační činnosti povoleny v produkčním systému, mohou být provedeny nežádoucí a neautorizované změny, proto přístup k transakčnímu kódu SPRO a autorizačnímu objektu S_IMG_ACTV (oprávnění k provádění funkcí v IMG) by měl být omezen v produkčním prostředí.

Testování: Pro otestování je třeba zobrazit report RSUSR002 s transakčním kódem SPRO a autorizačním objektem S_IMG_ACTV a poté report s autorizačním objektem S_TRANSPRT (transport organizer) s hodnotou 03. Následně vyvolání transakčního kódu SCC4 zobrazí nastavení produkčního klienta. Zde by přístup měl být omezen a nastavené změny nepovoleny pro ostatní klienty.

Závěr: Na základě provedeného testu, lze v tabulce 5 vidět, že v systému se nachází 10 klientů. Klient, který je určen pro výukové účely na Ekonomické fakultě je klient 120. Následně v příloze 1 této práce lze vidět, že pro klienta 120 jsou změny povoleny, a to i jiným klientům. Zároveň všech 106 uživatelů, kteří se v systému nachází má přístup k autorizačnímu objektu S_TRANSPRT a S_IMG_ACTV, tuto skutečnost lze vidět v tabulce 6.

Tabulka 5: Klienti v systému

Klient	Označení
000	SAP AG
001	Delivery
066	early Watch
100	jmenný
110	jmenný
120	jmenný
800	jmenný
810	jmenný
811	jmenný
812	jmenný

Zdroj: Vlastní zpracování

Tabulka 6: Ověření přístupu k IMG

Transakční kód	Autorizační objekt	Hodnoty	Počet uživatelů
SPRO	S_IMG_ACTV		106
	S_TRANSPRT	03	106

Zdroj: Vlastní zpracování

3.7.2 Úprava kritických tabulek

Tabulka 7: Kontrolní cíl úprava kritických tabulek

Předmět testování	• přístup k transakčnímu kódu SM30 a SM31 • přístup k autorizačnímu objektu S_TABU_DIS s hodnotou 02
Vyžadovaná evidence	• Výstup reportu RSUSR002

Zdroj: Vlastní zpracování

Riziko: Neautorizované změny mohou mít nežádoucí vliv na produkčního klienta. Přístup k ovládání systému a přizpůsobení tabulek by měl být omezen uživatelům, kteří jsou obeznámeni s možnými následky změn těchto tabulek. Kritické tabulky by měly být

přiřazeny k vhodné autorizační skupině a možnost úpravy být omezena v produkčním prostředí.

Testování: Riziko vyplývající z přizpůsobených tabulek může být zmírněno omezením přístupu k úpravě kritických tabulek. Přístup k úpravě kritických tabulek lze otestovat prostřednictvím objektu S_TABU_DIS (údržba tabulky) s hodnotou 02 (změna) a transakčního kódu SM30 nebo SM31. Test byl proveden nejprve vyvoláním transakčního kódu SA38, zobrazením reportu RSUSR002 a následném zadání již zmíněných hodnot.

Závěr: Na základě provedeného testu bylo zjištěno, že všech 106 uživatelů má přístup k úpravě kritických tabulek. Tuto skutečnost lze také vidět v tabulce 8.

Tabulka 8: Ověření přístupu k úpravě kritických tabulek

Transakční kód	Autorizační objekt	Hodnoty	Počet uživatelů
SM31	S_TABU_DIS	02	106

Zdroj: Vlastní zpracování

3.7.3 Přizpůsobení a provedení programu ABAP/4

Tabulka 9: Kontrolní cíl provedení ABAP

Předmět testování	• přístup k transakčnímu kódu SA38, SE38 a SE37 • přístup k autorizačnímu objektu S_PROGRAM s hodnotou SUBMIT • přístup k autorizačnímu objektu S_TCODE
Vyžadovaná evidence	• Výstup reportu RSABAPCS • Výstup reportu RSUSR002

Zdroj: Vlastní zpracování

Riziko: Uživatel, který má oprávnění autorizačního objektu S_PROGRAM a přístup k transakčnímu kódu SA38 nebo SE38, může vyvolat program ABAP/4, bez jakékoliv další kontroly. Následně má uživatel přístup k veškerým datům zpřístupněných programem. Proto by přizpůsobené programy měli být přiřazeny autorizačním skupinám.

Testování: Pro otestování je třeba zjistit, kteří uživatelé mají přístup k vykonání programů. Testujeme zobrazením programu RSUSR002 a zadáním autorizačního objektu

S_PROGRAM (ABAP: kontroly průběhu programu) s hodnotou SUBMIT (provedení programu ABAP) a objektu S_TCODE (kontrola kódu transakce při spuštění transakce) s hodnotami SA38, který je pro provedení všech programů, SE37 zpřístupní sestavené funkce a SE38 pro editování programů.

Závěr: Na základě provedeného testu bylo zjištěno, že všech 106 uživatelů má přístup k přizpůsobení a provedení programu ABAP/4. Provedený test je zaznamenán v tabulce 10.

Tabulka 10: Ověření přístupu k provedení ABAP

Transakční kód	Autorizační objekt	Hodnoty	Počet uživatelů
SA38, SE37, SE38	S_PROGRAM	SUBMIT	106

Zdroj: Vlastní zpracování

3.7.4 ABAP/4 Vývoj v produkci

Tabulka 11: Kontrolní cíl ABAP vývoj

Předmět testování	• přístup k transakčnímu kódu SE38 a SE37 • přístup k autorizačnímu objektu S_DEVELOP s hodnotami 01, 02 a 06 • přístup k autorizačnímu objektu S_TCODE
Vyžadovaná evidence	• Výstup reportu RSUSR002

Zdroj: Vlastní zpracování

Riziko: Tvorba a úprava ABAP/4 programu by měla být prováděna ve vývojovém systému a následně migrována do produkce. Pokud by tomu, tak nebylo, mohla by tvorba a úprava poškodit obchodní operace nebo způsobit neautorizované změny produkčních dat programů. Přístup ke zdrojovému kódu produkčního prostředí by měl být kontrolován a pouze odpovídající uživatelé mít přístup autorizačního objektu S_DEVELOP (ABAP Workbench) s hodnotou v produkčním systému.

Testování: Pro otestování kontrolního cíle je třeba zjistit, kteří uživatelé mají přístup k vývoji programů v produkčním systému. Test lze provést zobrazením reportu RSUSR002 a zadáním autorizačního objektu S_DEVELOP s hodnotami 01, 02, 06 (založení, změna a výmaz) a objektu S_TCODE s hodnotami SE38, SE37. Jelikož programy, které nejsou

přiřazeny k žádné autorizační skupině, mohou být změněny jakýmkoliv uživatelem s autorizací pro objekt S_DEVELOP.

Závěr: Na základě provedené testu bylo zjištěno, že všech 106 uživatelů má přístup k vývoji programů v produkčním systému. Provedený test je zaznamenán v tabulce 12.

Tabulka 12: Ověření přístupu k vývoji ABAP

Transakční kód	Autorizační objekt	Hodnoty	Počet uživatelů
SE37, SE38	S_DEVELOP	01, 02, 06	106

Zdroj: Vlastní zpracování

3.7.5 Datový slovník ABAP

Tabulka 13: Kontrolní cíl datový slovník ABAP

Předmět testování	• přístup k transakčnímu kódu SE11, SE12, SE15, SE16, SE38 a SE80 • přístup k autorizačnímu objektu S_DEVELOP s hodnotami 01, 02, 06 a 07 • přístup k autorizačnímu objektu S_TCODE
Vyžadovaná evidence	• Výstup reportu RSUSR002

Zdroj: Vlastní zpracování

Riziko: Změny v ABAP/4 datovém slovníku mohou mít nežádoucí vliv na systém, proto by i přístup k němu, měl být omezen pouze autorizovaným osobám. Změny v datovém slovníku by měly být prováděny ve vývojovém prostředí a následně přesunuty do produkce.

Testování: Pro otestování kontrolního cíle je třeba zobrazit report RSUSR002 a zjistit, kteří uživatelé mají přístup autorizačního objektu S_DEVELOP s hodnotami 01, 02, 06, 07 (založení, změna, výmaz a aktivace) a objektu S_TCODE s hodnotami SE11, SE12, SE15, SE16, SE38, SE80.

Závěr: Na základě provedené testu bylo zjištěno, že všech 106 uživatelů má přístup pro udržování datového slovníku. Provedený test je zaznamenán v tabulce 14.

Tabulka 14: Ověření přístupu k datovému slovníku ABAP

Transakční kód	Autorizační objekt	Hodnoty	Počet uživatelů
SE11, SE12, SE15, SE16, SE38, SE80	S_DEVELOP	01, 02, 06, 07	106

Zdroj: Vlastní zpracování

3.7.6 Dotazy

Tabulka 15: Kontrolní cíl dotazy

Předmět testování	• přístup k transakčnímu kódu SQ01 • přístup k autorizačnímu objektu S_QUERY s hodnotou 02 • přístup k autorizačnímu objektu S_TCODE
Vyžadovaná evidence	• Výstup reportu RSUSR002

Zdroj: Vlastní zpracování

Riziko: Prostřednictvím dotazů lze zobrazit informace a reporty v systému, které jsou významné pro rozhodování managementu. Proto pokud není přístup k tvorbě a úpravě dotazů omezen autorizovaným osobám, mohou mít tyto činnosti nežádoucí důsledky.

Testování: Pro otestování se opět využije report RSUSR002 a zadá autorizační objekt S_QUERY (oprávnění SAP query) s hodnotou 02 (změna) a objekt S_TCODE s hodnotou SQ01. Následně se zobrazí seznam uživatelů, kteří mohou vytvořit a upravit dotazy.

Závěr: Na základě provedeného testu bylo zjištěno, že všech 106 uživatelů může vytvořit a upravit dotazy. Provedený test je zaznamenán v tabulce 16.

Tabulka 16: Ověření přístupu k úpravě dotazů

Transakční kód	Autorizační objekt	Hodnoty	Počet uživatelů
SQ01	S_QUERY	02	106

Zdroj: Vlastní zpracování

3.7.7 Konfigurace CCMS

Tabulka 17: Kontrolní cíl CCMS

Předmět testování	• přístup k transakčnímu kódu AL01 a RZ20 • přístup k autorizačnímu objektu S_RZL_ADM s hodnotami 01 a 03 • přístup k autorizačnímu objektu S_TCODE
Vyžadovaná evidence	• Výstup reportu RSUSR002

Zdroj: Vlastní zpracování

Riziko: CCMS nemusí být užitečné, pokud operační mód, instance nebo rozvrhy nejsou nastaveny správně. Následně změny parametrů profilů mohou nežádoucím způsobem ovlivnit funkce systému. Proto pokud systémové aktivity nejsou proaktivně monitorovány, může to mít dopad na operace a integritu dat, jelikož nemusí být zjištěny příčiny problému se zpracováním.

Testování: Pro otestování je třeba zobrazit report RSUSR002 a zjistit, kteří uživatelé mají přístup k varovným zprávám. V rámci testu se využije autorizační objekt S_RZL_ADM (správa systému) s hodnotami 01 pro administraci, 03 pro zobrazení a objekt S_TCODE s hodnotami AL01, RZ20.

Závěr: Na základě provedeného testu bylo zjištěno, že všech 106 uživatelů má přístup ke správě varovných zpráv. Provedený test je zaznamenán v tabulce 18.

Tabulka 18: Ověření přístupu k CCMS

Transakční kód	Autorizační objekt	Hodnoty	Počet uživatelů
AL01, RZ20	S_RZL_ADM	01, 03	106

Zdroj: Vlastní zpracování

3.7.8 Dávkové zpracování

Tabulka 19: Kontrolní cíl dávkové zpracování

Předmět testování	• přístup k transakčnímu kódu SM35, SM64, SM36, SM37 • přístup k autorizačnímu objektu S_BDC_MONI s hodnotami DELE, FREE a LOCK • přístup k autorizačnímu objektu S_BTCH_ADM s hodnotou Y • přístup k autorizačnímu objektu S_BTCH_JOB s hodnotami DELE, RELE a PLAN • přístup k autorizačnímu objektu S_TCODE
Vyžadovaná evidence	• Výstup reportu RSUSR002

Zdroj: Vlastní zpracování

Riziko: Administrátoři mohou zpřístupnit všechny úlohy na pozadí a provést jakoukoliv operaci na kterékoliv úloze. Také jelikož dávkový vstup je automatický proces pro přenos dat do systému bez dialogu uživatele, měla by možnost zpracovávat a zadávat dávkové úlohy být omezena autorizovaným uživatelům.

Testování: Pro otestování je třeba zobrazit report RSUSR002 a zjistit, kteří uživatele mají přístup k administraci a uveřejnění úloh na pozadí. V rámci testu se využijí autorizační objekty pro dávkový vstup, S_TCODE s hodnotou SM35 a S_BDC_MONI (oprávnění pro dávkový vstup) s hodnotami DELE (výmaz složek), FREE (uvolnění map) a LOCK (blokování a odblokování složek). Dávkovou administraci, S_TCODE s hodnotou SM64 a S_BTCH_ADM (správce zpracování na pozadí) s hodnotou Y (Autorizace administrátora na pozadí). Dávkové zpracování, S_TCODE s hodnotou SM36 a S_BTCH_JOB (operace v dávkových úlohách) s hodnotami DELE (výmaz úloh na pozadí), RELE (zveřejnění úloh) a druhá varianta pro S_TCODE s hodnotou SM37 a S_BTCH_JOB s hodnotami DELE, RELE, PLAN (kopírování nebo opakování úloh).

Závěr: Na základě provedeného testu bylo zjištěno, že všech 106 uživatelů má přístup k výše zmíněným činnostem v souvislosti s dávkovým zpracováním. Provedené testy lze vidět v tabulce 20.

Tabulka 20: Ověření přístupu k dávkovému zpracování

Transakční kód	Autorizační objekt	Hodnoty	Počet uživatelů
SM35	S_BDC_MONI	DELE, FREE, LOCK	106
SM64	S_BTCH_ADM	Y	106
SM36	S_BTCH_JOB	DELE, RELE	106
SM37	S_BTCH_JOB	DELE, RELE, PLAN	106

Zdroj: Vlastní zpracování

3.7.9 Parametry aplikačního serveru

Tabulka 21: Kontrolní cíl parametry systému

Předmět testování	• nastavení parametru Login/password_expiration_time • nastavení parametru Login/min_password_lng • nastavení parametru Login/fails_to_session_end • nastavení parametru Login/fails_to_user_lock • nastavení parametru Login/failed_user_auto_unlock • nastavení parametru Auth/rfc_authority_check • nastavení parametru Rdisp/gui_auto_logout
Vyžadovaná evidence	• Výstup reportu RSPARAM

Zdroj: Vlastní zpracování

Riziko: Systém má své defaultní nastavení systémových parametrů, které ale nezaručují dostatečnou úroveň zabezpečení. Pokud toto defaultní nastavení není změněno samotnou organizací, může tím ohrozit bezpečnost systému a umožnit získat přístup neautorizovaným osobám. Proto během implementace by měla organizace nastavit parametry přijatelným způsobem.

Testování: Pro otestování lze zadat transakční kód SA38 a zobrazit report RSPARAM (seznam parametrů profilu), kde je možné zkontrolovat a zhodnotit nastavení klíčových parametrů. Mezi tyto parametry patří Login/password_expiration_time, tedy doba, po které musí heslo být změněno, defaultní hodnota je nastavena na 0 dní, která vlastně udává, že heslo nemusí být nikdy změněno. Login/min_password_lng, minimální délka hesla, kdy defaultní hodnota je nastavena na 6 znaků. Login/disable_multi_gui_login, zda

je povoleno vícenásobné přihlášení, defaultně nastaveno na hodnotu 0, což značí, že není. Login/fails_to_session_end, kolikrát uživatel může zadat špatně heslo, než bude zablokován, defaultně jsou nastaveny 3 pokusy. Login/fails_to_user_lock, kolikrát za den, uživatel může zadat nesprávné heslo, než systém uzamkne možnost dalšího přihlášení, defaultně je nastaveno 5 pokusů. Login/failed_user_auto_unlock, zdali se přihlášení musí obnovit manuálně nebo se provede automaticky o půlnoci, defaultně je nastavena hodnota 0 pro manuální resetování. Auth/rfc_authority_check, zdali je objekt S_RFC kontrolován při vzdáleném spouštění funkcí. Defaultně je nastavena hodnota 1, která vyjadřuje aktivní kontrolu. Posledním klíčovým parametrem je Rdisp/gui_auto_logout, určuje počet sekund, pro které uživatel může být nečinný, než bude ze systému automaticky odhlášen, defaultně je parametr nastaven na hodnotě 0, která znamená, že parametr je deaktivován. Následně je vhodné ještě zjistit, kteří uživatelé si ponechali defaultní heslo a kteří uživatelé se nikdy do systému nepřihlásili.

Závěr: Na základě provedeného testu bylo zjištěno, že uživatelé nejsou omezeny dobou, za kterou musí změnit své heslo. Minimální délka hesla uživatele musí být 6 znaků, tedy stejně, tak jako bylo nastaveno defaultně systémem. Počet pokusů na správné zadání hesla, než bude uživatel zablokován se také nezměnil a jako u defaultního nastavení se jedná tedy o 3 pokusy. Defaultní nastavení zůstalo i pro počet špatně zadaného hesla za den, než bude uživateli zakázána možnost přihlášení, tedy 5 pokusů. Možnost odemknutí přihlášení uživatele se musí, jak tomu bylo nastaveno i defaultně, provést manuálně, jelikož je nastavena hodnota 0. Na základě testu bylo dále zjištěno, že aktivní kontrola objektu S_RFC (kontrola oprávnění při přístupu RFC) probíhá v systému, tedy hodnota parametru je nastavena na 1 a tak tomu bylo i v rámci defaultního nastavení systému. Posledním testovaným parametrem je po jak dlouho může být uživatel nečinný, než bude automaticky odhlášen ze systému, defaultně hodnota byla nastavena na 0 sekund a stejně, tak jako u ostatních parametrů i tato hodnota se nezměnila. Přehled jednotlivých parametrů lze vidět v tabulce 22. Uživatele, který se do systému nikdy nepřihlásili lze vidět v příloze 14 této práce.

Tabulka 22: Nastavení parametrů uživatelem

Parametr	Nastavení systému	Uživatel
Login/password_expiration_time	0	0
Login/min_password_lng	6	6
Login/fails_to_session_end	3	3
Login/fails_to_user_lock	5	5
Login/failed_user_auto_unlock	0	0
Auth/rfc_authority_check	1	1
Rdisp/gui_auto_logout	0	0

Zdroj: Vlastní zpracování

3.7.10 Uzamčení transakčních kódů

Tabulka 23: Kontrolní cíl uzamčení transakčních kódů

Předmět testování	• přístup k transakčnímu kódu SM01 • přístup k transakci SCC5, SM49 a SM69
Vyžadovaná evidence	• Výstup reportu RSUSR002 • Výstup transakce SM01

Zdroj: Vlastní zpracování

Riziko: Některé citlivé transakce by měly být využívány pouze ve vývojovém prostředí anebo obezřetně v produkci. Obzvlášť transakce související s vývojem by měly být trvale uzamčeny v produkčním systému. Ostatní citlivé transakce je třeba kontrolovat a případně uzamknout v produkčním prostředí.

Testování: Pro otestování se použije report RSUSR002 s transakčním kódem SM01 ke zjištění, kteří uživatelé mají přístup k odemčení a uzamčení transakcí v systému. Následně je třeba vyvolat samotný transakční kód SM01 pro zobrazení seznamu transakčních kódů. Vedle jednotlivých transakčních kódu se nachází zaškrtávací pole, která označuje, zdali byla transakce uzamčena. Mezi citlivé transakce patří SCC5 pro vymazání klienta, SM49 a SM69 pro provedení logických příkazů.

Závěr: Na základě provedených testů bylo zjištěno, že všech 106 uživatelů má přístup k odemčení a uzamčení vybraných transakcí v systému. V druhé části testu bylo zjištěno,

že vybrané citlivé transakce uzamčeny nejsou. Provedené testy jsou zaznamenány v tabulkách 24 a 25.

Tabulka 24: Ověření přístupu k transakčním kódům

Transakční kód	Počet uživatelů
SM01	106

Zdroj: Vlastní zpracování

Tabulka 25: Zamknuté transakce

Transakční kód	Blokováno
SCC5	ne
SM49	ne
SM69	ne

Zdroj: Vlastní zpracování

3.7.11 Nepovolená hesla

Tabulka 26: Kontrolní cíl nepovolená hesla

Předmět testování	• seznam nepovolených hesel
Vyžadovaná evidence	• Výstup tabulky USR40

Zdroj: Vlastní zpracování

Riziko: Systém nabízí možnost záznamů zakázaných a nepovolených hesel ke snížení rizika zpřístupnění systému neautorizovanými osobami. Tím pádem, se uživatelé nemohou přihlásit jednoduchými nebo snadno uhodnutelnými hesly. Proto je doporučeno, aby organizace během implementace sama nastavila hesla, která uživatel nesmí používat. Systém má navíc několik vlastních kontrolních mechanismů, mezi které patří, uživatelé si musí změnit heslo, když se přihlásí do systému poprvé, heslo nemůže být SAP* nebo PASS, heslo nemůže obsahovat jakýkoliv tříznakový řetězec obsažený v ID uživatele, první znak nemůže být ! nebo ?, první 3 znaky nemohou být mezera, heslo nemůže začínat se 3 stejnými znaky, nebo že uživatel si nemůže změnit heslo víckrát jak jednou denně.

Testování: Pro otestování je třeba zvolat transakci SE16 a zobrazit tabulku USR40, kde jsou zakázaná hesla zaznamenány.

Závěr: Na základě provedeného testu lze v příloze 19 vidět, že v systému nejsou zaznamenány žádná nepovolená hesla.

3.7.12 Zálohování databáze

Tabulka 27: Kontrolní cíl zálohování

Předmět testování	• Četnost zálohování • Úspěšné dokončení zálohování
Vyžadovaná evidence	• Výstup transakčního kódu DB12 • Výstup reportu RSUSR002

Zdroj: Vlastní zpracování

Riziko: Pokud neprobíhá obnova dat, může to značně ovlivnit správné reflektování obchodních procesů, zejména v oblasti finančních a citlivých dat.

Testování: Pro otestování je třeba zobrazit transakční kód DB12 a zjistit, jak často je databáze zálohována a zda zálohy proběhly v pořádku.

Závěr: Na základě provedeného testu bylo zjištěno, že obnova probíhá pravidelně každý týden a vždy je v pořádku dokončena. Jelikož v systému není mnoho dat, záloha probíhá velmi krátkou dobu, konkrétně 2 vteřiny. Poslední provedena záloha a zálohy za posledních 30 dní jsou zaznamenány v přílohách 20 a 21.

3.7.13 Aktualizační požadavky

Tabulka 28: Kontrolní cíl aktualizační požadavky

Předmět testování	• Aktuální verze systému • Úspěšné dokončení aktualizačních požadavků
Vyžadovaná evidence	• Výstup transakčního kódu SM13

Zdroj: Vlastní zpracování

Riziko: Pokud není systém pravidelně aktualizován, mohou být zneužity bezpečnostní mezery a hrozí riziko vzniku neautorizovaného přístupu do systému.

Testování: Pro otestování je třeba zobrazit transakční kód SM13, prostřednictvím kterého lze zjistit, zda je systém aktualizován.

Závěr: Na základě provedeného testu bylo zjištěno, že aktualizace je aktivní. Tuto skutečnost, lze ověřit v příloze 22. Následně v příloze 23 je zobrazen počet aktualizačních požadavků a jejich úspěšné dokončení.

3.7.14 Správa zabezpečení

Tabulka 29: Kontrolní cíl správy zabezpečení

Předmět testování	• přístup k autorizačnímu objektu S_USER_AGR s hodnotami 01, 02, 21, 22 • přístup k transakčnímu kódu PFCG, SU03, SU02, SU01 • přístup k autorizačnímu objektu S_USER_AUT s hodnotami 01, 02, 07 a 22 • přístup k transakčnímu objektu S_USER_PRO s hodnotami 01, 02, 07, 22 • přístup k transakčnímu objektu S_USER_GRP s hodnotami 01, 02, 05, 06 a 22
Vyžadovaná evidence	• Výstup reportu RSUSR002

Zdroj: Vlastní zpracování

Riziko: Oddělit povinnosti v prostředí správy zabezpečení je vhodné pro zamezení jakémukoliv jednotlivci mít veškerý přístup k systému. Mezi 3 významné funkce pro které je vhodné přístup uživatelů oddělit jsou vytvoření a udržování autorizačních profilů, aktivace autorizačních profilů, vytvoření a udržování privilegií uživatelských přístupů. Oddělením těchto objektů se zmírní riziko, že jeden administrativní správce by mohl, jak udržovat uživatelské skupiny, tak vytvořit profily i udržovat autorizace.

Testování: Ke zjištění, zda administrátorské úlohy jsou odděleny podle jednotlivých funkcí, je třeba zobrazit seznam uživatelů vybraných autorizací. To lze zobrazením reportu RSUSR002 a následně pro generátor profilů, konkrétně činnost vytvářet a měnit skupiny aktivit se použije autorizační objekt S_USER_AGR (oprávnění: kontrola rolí) s hodnotami 01, 02 (založení, změna) a transakční kód PFCG. Pro přesun skupiny aktivit se použije autorizační objekt S_USER_AGR s hodnotou 21 (transport) a transakčním kódem PFCG. Pro přenos profilů do kmenových záznamů uživatele se použije objekt

S_USER_AGR s hodnotou 22 (zadání, zahrnutí, přiřazení) a transakčním kódem PFCG. Pro údržbu hlavního uživatele, konkrétně autorizace se použije objekt S_USER_AUT (údržba kmenového souboru uživatele: oprávnění) s hodnotami 01, 02, 07 a 22 (založení, změna, aktivace, přiřazení) s transakčním kódem SU03. Pro aktivaci autorizačních profilů a autorizací se použije objekt S_USER_PRO (údržba kmenového souboru uživatele: profil oprávnění) s hodnotami 01, 02, 07, 22 s transakčním kódem SU02. Pro vytvoření a úpravu kmenových záznamů uživatele a jeho seznam profilů a parametrů se použije objekt S_USER_GRP (údržba kmenového souboru uživatele: skupiny uživatelů) s hodnotami 01, 02, 05, 06 a 22 (založení, změna, blokování, výmaz a přiřazení) s transakčním kódem SU01.

Závěr: Na základě provedeného testování bylo zjištěno, že všech 106 uživatelů může měnit, vytvořit a přesouvat skupiny aktivit. Stejně tak i všech 106 uživatelů smí přiřadit profily do kmenových záznamů uživatele, spravovat záznam hlavního uživatele, aktivovat autorizační profily a autorizace a vytvořit a změnit kmenové záznamy uživatele včetně jeho seznamu profilů a parametrů. Všechny provedené testy lze vidět v tabulce 30.

Tabulka 30: Ověření přístupu ke správě zabezpečení

Transakční kód	Autorizační objekt	Hodnoty	Počet uživatelů
PFCG	S_USER_AGR	01, 02, 21, 22	106
SU03	S_USER_AUT	01, 02, 07, 22	106
SU02	S_USER_PRO	01, 02, 07, 22	106
SU01	S_USER_GRP	01, 02, 05, 06, 22	106

Zdroj: Vlastní zpracování

3.7.15 Zabezpečení SAP* a DDIC uživatele

Tabulka 31: Kontrolní cíl uživatel SAP a DDIC*

Předmět testování	• uživatel SAP* • uživatel DDIC
Vyžadovaná evidence	• Výstup reportu RSUSR002 • výstup reportu RSUSR003

Zdroj: Vlastní zpracování

Riziko: SAP* je defaultní uživatel systému. Při instalaci systému je kmenový záznam SAP* uživatele automaticky vytvořen v klientovi 000 a 001. Pokud jsou kmenové záznamy vymazány, proběhne resetování a nastaví se defaultní heslo na PASS. V případě, že je tento uživatel nesprávně nebo nedostatečně zabezpečen, mohou být provedeny neautorizované transakce, které obejdou zřízené kontroly v systému. Proto je vhodné, alespoň uživatele uzamknout a změnit jeho defaultní heslo.

Testování: Pro testování, zda je uživatel uzamknut je třeba zadat transakční kód SA38 a zobrazit report RSUSR002, ve kterém lze tuto informaci zjistit. Následně ke zjištění, zda bylo defaultní heslo změněno se využije report RSUSR003 (kontrola hesel standardních uživatelů ve všech klientech). Tento report obecně zobrazuje všechny klienty, které byli instalování v systému a podléhají kontrole. U každého uživatele může zobrazit, pokud se jedná o jednoduché či defaultní heslo. Dalšími významným uživatelem je DDIC, který udržuje ABAP/4 datový slovník a má stejně jako SAP* velmi důležitá privilegia.

Závěr: Na základě provedeného testu bylo zjištěno, že v klientovi 120 uživatel SAP* neexistuje, tuto skutečnost lze i vidět v příloze 24, kde byl proveden test pro zjištění, zda je SAP* uzamčen, ale jak je vidět uživatel SAP* vůbec neexistuje. Při zobrazení druhého zmíněného reportu můžeme vidět všechny uživatele jednotlivých klientů v systému. Pro klienta 120 existuje pouze uživatel DDIC a jak můžeme vidět v tabulce 32 defaultní heslo uživatele bylo změněno a není triviální. V této tabulce, ale také můžeme vidět, že uživatele založil uživatel SAP* a že nepatří do skupiny super uživatelů “super”.

Tabulka 32: Nastavení uživatele SAP a DDIC*

Klient	Uživatel	Status hesla	Skupina uživatelů	Uživatele založil
120	DDIC	Existuje; heslo není triviální		SAP*
	SAP*	Neexistuje; Přihlášení není možné		

Zdroj: Vlastní zpracování

3.7.16 Správa výkonných profilů

Tabulka 33: Kontrolní cíl výkonné profily

Předmět testování	• profil SAP_ALL • profil SAP_NEW
Vyžadovaná evidence	• Výstup reportu RSUSR002

Zdroj: Vlastní zpracování

Riziko: Jedná se o profily, které poskytují stejný přístup k systému jako superuživatel. Profil SAP_ALL zajišťuje přístup k celému systému. SAP_NEW může poskytnou dodatečný a neautorizovaný přístup během aktualizace. Tyto profily by měly být používány spíše v krizových situací, a proto i přístup k nim by měl být omezen.

Testování: Pro otestování se použije report RSUSR002, který zobrazí uživatele přiřazené k těmto profilům.

Závěr: Na Základě provedeného testu bylo zjištěno, že všech 106 uživatelů je přiřazeno k výše uvedeným profilům. Tuto skutečnost lze vidět i v tabulce 34.

Tabulka 34: Ověření přiřazení k výkonným profilům

Profil	Počet uživatelů
SAP_ALL	106
SAP_NEW	106

Zdroj: Vlastní zpracování

3.7.17 Správa výkonných skupin uživatelů

Tabulka 35: Kontrolní cíl výkonné skupiny uživatelů

Předmět testování	• přístup k autorizačnímu objektu S_USER_AGR s hodnotami 01, 02, 21 a 22 • přístup k autorizačnímu objektu S_USER_GRP s hodnotami 01, 02, 05 a 06 • přístup k transakčnímu kódu PFCG, SU01
Vyžadovaná evidence	• Výstup reportu RSUSR002

Zdroj: Vlastní zpracování

Riziko: Administrátoři systému by neměli být schopni sami změnit své autorizace, jelikož by měli bez limitní přístup a možnost provést neautorizované transakce v systému. Skupina autorizací, která obsahuje výkonné uživatele, by měla být omezena alespoň novým superuživatelem.

Testování: Pro otestování se použije report RSUSR002, který zobrazí uživatele, kteří mají přístup autorizačního objektu S_USER_GRP s hodnotami 01, 02 a 06 a objektu S_TCODE s hodnotou SU01.

Závěr: Na základě provedeného testu můžeme vidět, že všech 106 uživatelů má přístup ke správě výkonných skupin uživatelů. Provedený test si lze vidět v tabulce 36.

Tabulka 36: Ověření přístupu k výkonným skupinám

Transakční kód	Autorizační objekt	Hodnoty	Počet uživatelů
SU01	S_USER_GRP	01, 02, 06	106

Zdroj: Vlastní zpracování

3.7.18 Protokolování tabulek

Tabulka 37: Kontrolní cíl protokolování tabulek

Předmět testování	• tabulka T000 • tabulka T001
Vyžadovaná evidence	• Výstup tabulky TPROT • Výstup transakce SE11

Zdroj: Vlastní zpracování

Riziko: V systému se mohou nacházet tabulky u kterých by neměly probíhat změny v produkčním klientovi, jelikož jejich změny mohou ovlivnit samotnou strukturu systému. Tyto tabulky by měly být vyvinuty tak, aby bylo sníženo riziko nemožnosti identifikace jejich neautorizovaných změn. Proto by všechny jejich změny měly být protokolovány a následně tyto protokoly zkontrolovány, zda nedošlo k neautorizovaným změnám.

Testování: Pro otestování je třeba použít tabulku TPROT, která zobrazí tabulky, jež vyžadují protokolování. Následně se názvy jednotlivých tabulek vyplní po zvolání transakce SE11, poté se zobrazí seznam, kde v záložce technické nastavení zjistíme, zda

je zaškrtnuto pole změny dat protokolu. Mezi tabulky, které by měly být protokolovány patří klienti T000 a kódy organizace T001.

Závěr: V příloze 29 lze vidět vzorek tabulek, které musí být protokolovány. Následně na základě provedeného testu můžeme v tabulce 38 vidět, že vybrané tabulky jsou protokolovány.

Tabulka 38: Ověření protokolování tabulek

Tabulka	Protokolování změn dat
T000	ano
T001	ano

Zdroj: Vlastní zpracování

3.7.19 Přístup ke kmenovým datům dodavatele, zákazníka a materiálu

Tabulka 39: Kontrolní cíl udržování kmenových dat

Předmět testování	• přístup k transakčním kódům FD02, VD02, XD02, FK01, FK02, FK05, FK06, MK01, MK02, MK05, MK06, XK01, XK02, XK05 a XK06, MM01 a MM02 • Přístup k vybraným autorizačním objektům: F_KNA1_AEN, F_KNA1_APP, F_KNA1_BED, F_KNA1_BUK, F_KNA1_GEN, F_KNA1_GRP, V_KNA1_VKO, V_KNA1_BRG, C_TCLA_BKA, C_TCLS_BER, M_MATE_BUK, M_MATE_LGN, M_MATE_MAN, M_MATE_MAR, M_MATE_MAT, M_MATE_MEX, M_MATE_MZP, M_MATE_NEU, M_MATE_STA, M_MATE_VKO, M_MATE_WGR, M_MATE_WRK • s hodnotami 01 a 02
Vyžadovaná evidence	• Výstup reportu RSUSR002

Zdroj: Vlastní zpracování

Riziko: Kmenová data ovlivňují efektivní tok dokumentů a transakcí v systému. Nedostatečné udržování, nesprávná tvorba nebo nekompletní záznam mohou ovlivnit většinu oblastí v organizaci. Pokud by například uživatel vyplnil nesprávné jméno a

adresu zákazníka, mohl by způsobit, že zboží bude odesláno na špatnou adresu. Proto by přístup k vytvoření a úpravě kmenových dat zákazníků, dodavatelů měl být omezen autorizovaným uživatelům, stejně tak jako k úpravě záznamu materiálu nebo pravidel pro vyřizování objednávek, které by mohly způsobit nesprávné zhodnocení zboží.

Testování: Pro testování je třeba zobrazit report RSUSR002 a vyplnit transakční kódy pro zjištění uživatelského přístupu pro vytvoření a úpravu zákazníků, materiálů a ceny. F_KNA1_AEN (odběratel: oprávnění ke změně pro určitá pole), F_KNA1_APP (odběratel: oprávnění pro aplikaci), F_KNA1_BED (odběratel: oprávnění pro účet), F_KNA1_BUK (odběratel: oprávnění pro účetní okruhy), F_KNA1_GEN (odběratel: centrální data), F_KNA1_GRP (odběratel: oprávnění ke skupině účtů) s hodnotami 01 a 02 a transakcemi FD02, VD02, XD02. V_KNA1_BRG (zákazník: oprávnění k účtu: oblast odbytu), V_KNA1_VKO (zákazník: oprávnění pro prodejní organizace) s hodnotami 01 a 02 a transakcemi VD02, XD02. C_TCLA_BKA (oprávnění k druhům třídy), C_TCLS_BER (oprávnění pro views ve všeobecném systému tříd) s hodnotami 01 a 02 a transakcemi VD02. Transakce FK01, FK02, FK05, FK06, MK01, MK02, MK05, MK06, XK01, XK02, XK05 a XK06. C_AENR_BGR (CC kmenový soubor změn - skupina oprávnění), C_AENR_ERW (CC změnová služba - rozšířená kontrola oprávnění), C_AENR_RV1 (CC změnová služba - stav revize materiálu), C_DRAD_OBJ (založení/změna/zobrazení/výmaz objektových propojení), C_KLAH_BKL (oprávnění, klasifikace), C_TCLA_BKA, C_TCLS_MNT (oprávnění údržby pro atributy view) s hodnotami 01 a 02 a transakcemi MM01 a MM02. M_MATE_BUK (kmen. Soub. Mater.: účet. Okruh) , M_MATE_LGN (kmen. Soub. Mater.: č. Skladu), M_MATE_MAN (kmenový soubor materiálu: centrální data), M_MATE_MAR (kmenový soubor materiálu: druh materiálu), M_MATE_MAT (kmenový soubor materiálu: materiál), M_MATE_MEX (kmenový soubor materiálu: data vývozního povolení pro jednotlivé státy, M_MATE_MZP (kmenový soubor materiálu: data celních preferencí), M_MATE_NEU (kmenový soubor materiálu: nové založení), M_MATE_STA (kmenový soubor materiálu: status údržby), M_MATE_VKO (kmenový soubor materiálu: cesta odbytu), M_MATE_WGR (kmenový soubor materiálu: skupina materiálu), M_MATE_WRK (kmenový soubor materiálu: závod) s hodnotami 01 a 02 a transakcemi MM01 a MM02.

Závěr: Na základě provedeného testu bylo zjištěno, že všech 106 uživatelů má přístup k vybraným funkcím obchodních procesů. Tuto skutečnost lze vidět i v tabulce 40.

Tabulka 40: Ověření přístupu ke kmenovým datům

Transakční kód	Autorizační objekt	Hodnoty	Počet uživatelů
FD02, VD02, XD02	F_KNA1_AEN	01, 02	106
FD02, VD02, XD02	F_KNA1_APP	01, 02	106
FD02, VD02, XD02	F_KNA1_BED	01, 02	106
FD02, VD02, XD02	F_KNA1_BUK	01, 02	106
FD02, VD02, XD02	F_KNA1_GEN	01, 02	106
FD02, VD02, XD02	F_KNA1_GRP	01, 02	106
VD02, XD02	V_KNA1_BRG	01, 02	106
VD02, XD02	V_KNA1_VKO	01, 02	106
VD02	C_TCLA_BKA	01, 02	106
VD02	C_TCLS_BER	01, 02	106
MM01, MM02	C_AENR_BGR	01, 02	106
MM01, MM02	C_AENR_ERW	01, 02	106
MM01, MM02	C_AENR_RV1	01, 02	106
MM01, MM02	C_DRAD_OBJ	01, 02	106
MM01, MM02	C_KLAH_BKL	01, 02	106
MM01, MM02	C_TCLA_BKA	01, 02	106
MM01, MM02	C_TCLS_MNT	01, 02	106
MM01, MM02	M_MATE_BUK	01, 02	106
MM01, MM02	M_MATE_LGN	01, 02	106
MM01, MM02	M_MATE_MAN	01, 02	106
MM01, MM02	M_MATE_MAR	01, 02	106
MM01, MM02	M_MATE_MAT	01, 02	106
MM01, MM02	M_MATE_MEX	01, 02	106
MM01, MM02	M_MATE_MZP	01, 02	106
MM01, MM02	M_MATE_NEU	01, 02	106
MM01, MM02	M_MATE_STA	01, 02	106
MM01, MM02	M_MATE_VKO	01, 02	106
MM01, MM02	M_MATE_WGR	01, 02	106
MM01, MM02	M_MATE_WRK	01, 02	106
MK01, MK02, MK05, MK06, XK01, XK02, XK05, XK06, FK01, FK02, FK05, FK06			106

Zdroj: Vlastní zpracování

4 Vyhodnocení výsledků testování

Metodika COBIT, kromě specifikace procesních oblastí, poskytuje nástroj, který pomáhá zhodnotit současnou efektivitu auditovaného systému z hlediska vybraného procesu a zároveň má pomoci nalézt odpovídající opatření pro zlepšení.

Tento nástroj se nazývá model zralosti a definuje celkem 6 úrovní, kterých lze dosáhnout. Nultá úroveň značí nejnižší soulad s procesní oblastí a pátá úroveň naopak absolutní soulad s procesní oblastí.

Na základě provedeného testování a zhodnocení dosažených výsledků se ERP systém SAP pro procesní oblast DS5 nachází na nulté úrovni. Tedy organizace nesplňuje ani nejnižší úroveň definovanou metodikou COBIT pro IT bezpečnost. Auditovaný systém zejména postrádá přesné definování odpovědností, systém pro podávání zpráv a správu administrace.

Systém sám o sobě je dokumentací, a tak lze i z testů vyhodnotit určité náležitosti v souvislosti s administrací a bezpečností systému. Na základě testování bylo prokázáno, že uživatelé jsou v systému vytvořeny a dále nijak zvlášť administrování. V prvních dvou letech byly vytvořeny jmenné účty s uvedením celého jména uživatele, ale v dalších letech byly už pouze vytvořeny účty odlišující se číslovkou, ale jinak se stejným uživatelským jménem, bez jakékoliv další vazby na konkrétní osobu. Zároveň uživatelé, kteří již nejsou studenty fakulty, zůstávají nadále v systému namísto toho, aby byli odstraněni.

Současný systém administrace je pochopitelný, z toho důvodu, že každý semestr v systému pracují jiní studenti, a tedy využívání univerzálních účtů je efektivní z hlediska času, ale už ne z hlediska bezpečnosti. Samotný problém spočívá v tom, že systém může být zpřístupněn nepovolaným osobám. Přesněji může vzniknout situace, že jeden účet je sdílen více uživateli a tuto skutečnost nelze jednoduše prokázat, tedy nelze ani jednoznačně určit, kdo daným účtem disponuje. Snadno se poté mohou poskytnout uživatelské údaje úplně cizí osobě a ta se dostat do systému bez možnosti jejího odhalení. Systém může samozřejmě zobrazit záznam změn, které uživatel provedl, ale jelikož se u něj nenachází žádné konkrétní údaje, lze to považovat za zcela zbytečné. Přístup by neměli mít také již zmíněný studenti, kteří na fakultě nestudují, a tedy nemají žádný vztah

k této organizaci. Významným nálezem je také to, že každý uživatel v systému může měnit údaje jiného uživatele, včetně hesla. Implementace kontrol nadále prokázala, že se v systému nachází uživatelské účty, ke kterým se nikdo nepřihlásil nebo jsou blokovány.

Kontrolní cíle, které v této práci byly stanoveny, odkazují na oblasti, jejichž změny mohou značně ovlivnit strukturu a funkcionalitu systému. Každý test, který byl založen na ověření přístupu, prokázal, že všech 106 uživatelů má přístup, tím pádem při administraci není kladen důraz na přiřazení k autorizačnímu objektu, skupině nebo roli. V tomto případě lze vzít v úvahu, že se jedná o systém určený pro výuku a kde tedy studenti mohou mít přístup k mnoha funkcionalitám. Přesto byly identifikovány oblasti, u kterých to není vhodné, alespoň dokud nejsou získány odpovídající znalosti. Mezi takové oblasti patří například možnost vytvořit přepsat nebo smazat klienta a uživatele. Následně pokud uživatelé mohou sami vytvořit nového uživatele, mohou tím zároveň zpřístupnit systém nepovolané osobě. Dalšími oblastmi, ke kterým mají uživatelé neomezený přístup jsou dávková zpracování, IMG, CCMS, dotazy, datový slovník a prostředí ABAP/4.

Bylo zjištěno, že všichni uživatelé mají přiřazeny výkonné profily SAP_ALL a SAP_NEW, které jim navíc byly přiřazeny ihned po vytvoření, což bylo zjištěno na základě změnových záznamů zpřístupněných reportem RSUSR101 a RSUSR102, které jsou zobrazeny v příloze 32 a 33 této práce.

Všechny defaultní parametry, zůstaly nastaveny systémem. Tato skutečnost neznamená nutně problém, spíše se tím prokázalo, že systém nemá nijak zvlášť nastavena bezpečnostní opatření. Tuto skutečnost potvrzuje i fakt, že nejsou stanoveny a zaznamenány žádná nepovolená hesla. Pokud uživatelé zvolí některá z běžně využívaných a snadno uhodnutelných hesel, může se opět snadno do systému dostat nepovolená osoba.

Test na ověření přístupu ke kmenovým datům se dá považovat za nejméně významný, jelikož účelem výuky v systému je simulace obchodních procesů a je tedy pochopitelné, že studenti budou mít přístup k široké škále funkcí. Přesto by tady opět mohl být zaveden systém na poskytování přístupu na základě získaných znalostí a opět tím bylo potvrzeno, že administrace není nijak zvlášť spravována.

Za příhodné lze považovat, že alespoň změny tabulek jsou zaznamenávány a je tedy možné sledovat provedené změny. Také databáze je pravidelně zálohována, aktualizace systému je aktivní a jsou tedy zpracovávány aktualizační požadavky a že hesla defaultních uživatelů byla změněna.

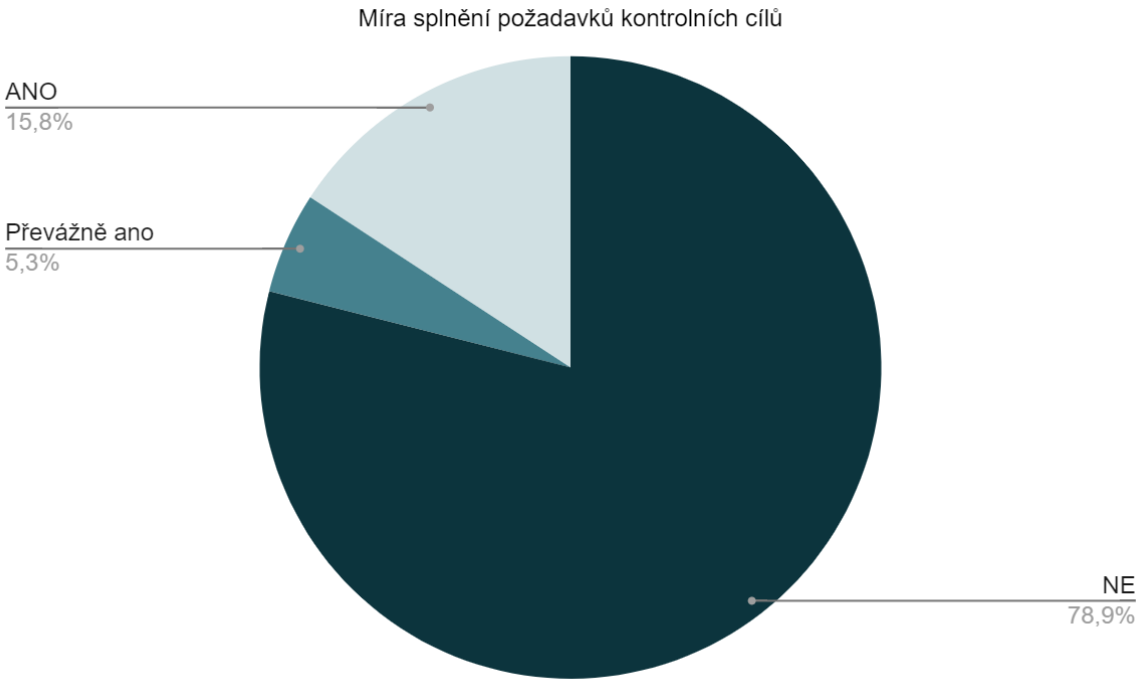
V tabulce 41 jsou shrnuty výsledky jednotlivých testů a určena míra splnění požadavků. Jsou zde uvedeny kontrolní cíle spolu s označením, zda splňují požadované zabezpečení a administraci systému. Pro určení míry splnění byly zvoleny metriky NE, Částečně, Převážně ano a ANO. Následně graf 1 zobrazuje splnění požadavků jednotlivých kritérií vizuálně.

Tabulka 41: Míra splnění požadavků kontrolních cílů

Kontrolní cíl	NE	Částečně	Převážně ano	ANO
IMG	X			
Úprava kritických tabulek	X			
Přizpůsobení a provedení programu ABAP/4	X			
ABAP/4 Vývoj v produkci	X			
Datový slovník ABAP	X			
Dotazy	X			
Konfigurace CCMS	X			
Dávkové zpracování	X			
Parametry aplikačního serveru	X			
Uzamčení transakčních kódů	X			
Nepovolená hesla	X			
Zálohování databáze				X
Aktualizační požadavky				X
Správa zabezpečení	X			
Zabezpečení SAP* a DDIC uživatele			X	
Správa výkonných profilů	X			
Správa výkonných skupin uživatelů	X			
Protokolování tabulek				X
Přístup ke kmenovým datům dodavatele, zákazníka a materiálu	X			

Zdroj: Vlastní zpracování

Graf 1: Míra splnění požadavků kontrolních cílů



Zdroj: Vlastní zpracování

5 Návrh na zlepšení

Po zhodnocení výsledků testování jsou navrhovány a doporučeny následující opatření k zajištění lepší bezpečnosti a administrace systému. V rámci základní administrace uživatelů je doporučeno vymazat uživatele, kteří již nepotřebují mít přístup k systému. Každému uživateli, by měla být odebrána možnost měnit údaje jiných uživatelů, a především samotného klienta. Systém univerzálních účtů by mohl být zachován za podmínky, že uživatelé si po přihlášení vyplní případně přepíšou jmenné údaje. Ostatní rizikové oblasti by měly být prověřeny a vyhodnoceno, zda by i přístup k nim neměl být omezen.

Bylo by vhodné udělovat jednotlivá oprávnění v průběhu výuky, kdy studenti získávají postupně odpovídající znalosti. Stejně tak by tomu mohlo být i s výkonnými profily SAP_ALL a SAP_NEW, tam by ovšem bylo lepší, tyto profily vůbec nepřiřazovat uživatelům z řad studentů a ponechat je pouze uživatelům zodpovědným za správu systému. Doporučeno je například z řad studentů vybrat někoho, kdo je odpovědný a mohl by průběžně přiřazovat autorizace jiným uživatelům.

Měl by být vytvořen seznam nepovolených hesel, který by omezil možnost stanovení hesla jako je SAP, USER a jiná běžně používaná jako je HESLO.

Vyhodnocenou míru rizika zmírňuje skutečnost, že systém je nasazen v počítači zabezpečeném uživatelským účtem a v uzamčené učebně.

Organizace by měla usilovat o dosažení alespoň úrovně 3 v modelu zralosti, tedy úrovně “definované” kdy IT bezpečnostní procedury jsou stanoveny v souladu s bezpečnostní politikou. Bezpečnost je zajištěna, ale nijak zásadně neprosazována.

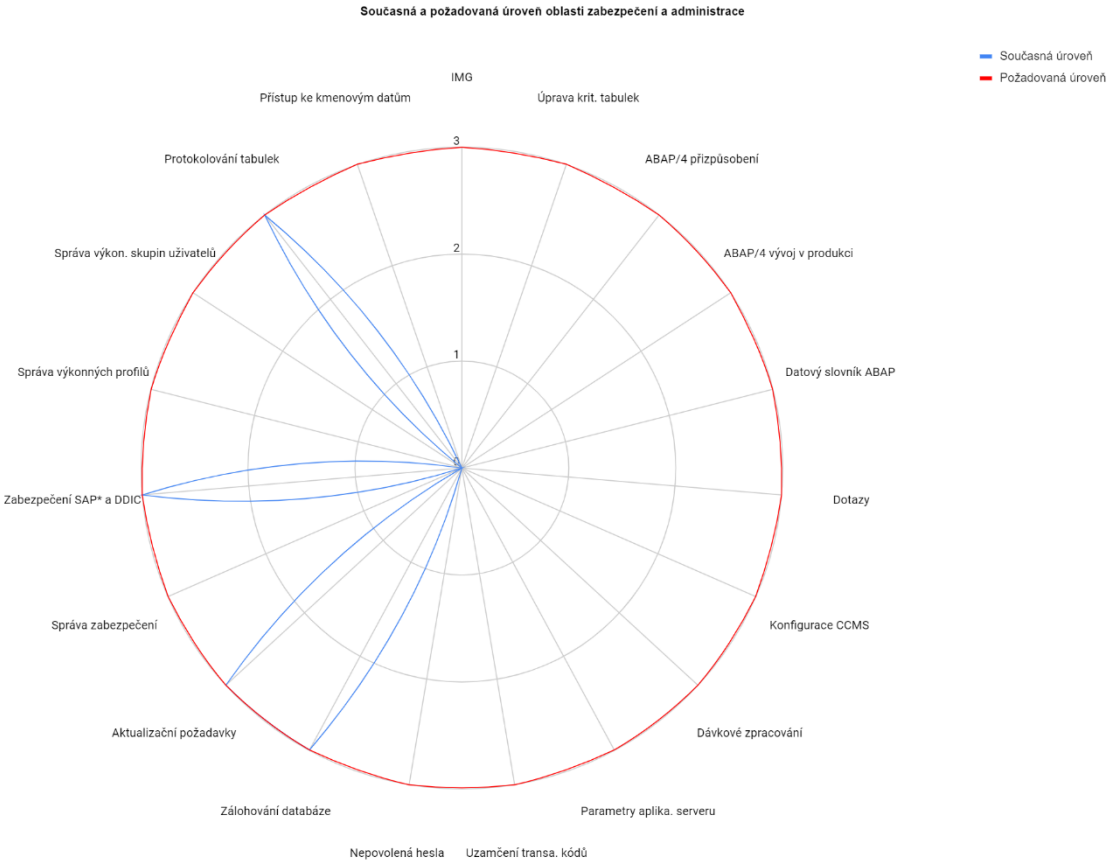
V tabulce 42 jsou shrnuty jednotlivé kontrolní cíle a navržena opatření, která by měla být prověřena pro splnění požadované úrovně. Následně v grafu 2 je vizuálně znázorněno, na jaké úrovni se v současné době jednotlivé kontrolní cíle nacházejí a zda se jedná již o požadovanou úroveň.

Tabulka 42: Navržená opatření kontrolních cílů

Kontrolní cíl	Návrh opatření
IMG	Uvážit, zda neomezit přístup k vybrané oblasti a odpovídajícím autorizacím.
Úprava kritických tabulek	Uvážit, zda neomezit přístup k vybrané oblasti a odpovídajícím autorizacím.
Přizpůsobení a provedení programu ABAP/4	Uvážit, zda neomezit přístup k vybrané oblasti a odpovídajícím autorizacím.
ABAP/4 Vývoj v produkci	Uvážit, zda neomezit přístup k vybrané oblasti a odpovídajícím autorizacím.
Datový slovník ABAP	Uvážit, zda neomezit přístup k vybrané oblasti a odpovídajícím autorizacím.
Dotazy	Uvážit, zda neomezit přístup k vybrané oblasti a odpovídajícím autorizacím.
Konfigurace CCMS	Uvážit, zda neomezit přístup k vybrané oblasti a odpovídajícím autorizacím.
Dávkové zpracování	Uvážit, zda neomezit přístup k vybrané oblasti a odpovídajícím autorizacím.
Parametry aplikačního serveru	Uvážit, nastavení klíčových parametrů, odlišné od defaultního nastavení systémem.
Uzamčení transakčních kódů	Uvážit, zda neomezit přístup k vybrané oblasti a odpovídajícím autorizacím.
Nepovolená hesla	Uvážit, zda nevytvořit seznam nepovolených hesel.
Zálohování databáze	Oblast poskytuje odpovídající výstupy.
Aktualizační požadavky	Oblast poskytuje odpovídající výstupy.
Správa zabezpečení	Uvážit, zda neomezit přístup k vybrané oblasti a odpovídajícím autorizacím.
Zabezpečení SAP* a DDIC uživatele	Oblast je odpovídajícím způsobem zabezpečena a administrována.
Správa výkonných profilů	Uvážit, zda neomezit přístup k vybrané oblasti a odpovídajícím autorizacím.
Správa výkonných skupin uživatelů	Uvážit, zda neomezit přístup k vybrané oblasti a odpovídajícím autorizacím.
Protokolování tabulek	Oblast je odpovídajícím způsobem zabezpečena a administrována.
Přístup ke kmenovým datům dodavatele, zákazníka a materiálu	Uvážit, zda neomezit přístup k vybrané oblasti a odpovídajícím autorizacím.

Zdroj: Vlastní zpracování

Graf 2: Současná a požadovaná úroveň oblasti zabezpečení a administrace



Zdroj: Vlastní zpracování

6 Závěr

Na základě získaných teoretických znalostí byl proveden audit ERP systému SAP zasazeného do akademického prostředí. Hlavní funkce systému, tedy zajištění a podpora obchodních procesů jsou v tomto prostředí využívány pouze pro výukové účely. Z tohoto důvodu bylo důležité zaměřit se zejména na bezpečnost a zmapovat způsob administrace. Jednalo se o audit mimořádný, který byl proveden ke dni odevzdání diplomové práce a nepředpokládá se tedy jeho opakování. Zároveň byly testovány všechny dostupné vzorky od doby zavedení systému.

V rámci teoretické části byly s ohledem na literaturu vymezeny klíčové oblasti, které mohou značným způsobem ovlivnit strukturu a funkcionalitu systému. Stejně tak byly i v rámci teorie zjištěny transakční kódy jednotlivých funkcionalit systému. Prostřednictvím nástroje Repository information system byly následně vybrány odpovídající autorizované objekty a jejich hodnoty. Při provádění samotného auditu nebylo třeba žádných dodatečných rozhovorů s odpovědnými osobami, jelikož je systém sám o sobě dokumentací. Zároveň byl audit proveden s odkazem na vybraný proces metodiky COBIT, konkrétně proces DS5 a jeho kontrolní cíle.

S ohledem na provedené testování, bylo zjištěno, že systém není odpovídajícím způsobem administrován, a tedy ani zabezpečen. Podle modelu zralosti definovaného také metodikou COBIT bylo stanoveno, že systém se v rámci procesu DS5 nachází konkrétně na nulté úrovni, tedy není považován za efektivní z hlediska zabezpečení a organizace nebere v potaz důležitost administrace. V podstatě každý uživatel, který je v systému vytvořen má neomezený přístup ke všem zmíněným klíčovým oblastem. Za nejrizikovější aspekty považuji to, že uživatelé, míněno studenti, mohou sami přidávat a měnit údaje ostatních uživatelů nebo klienta. Naopak v systému nebyla potřeba kontrola správnosti dat funkcí souvisejících s obchodními procesy, jelikož reálně zde neprobíhají.

Výsledky auditu byly následně vyhodnoceny a doplněny vhodnými opatřeními a doporučeními ke zlepšení bezpečnosti a administrace systému. Zejména byla doporučeno omezit přístup k výše zmíněným nejrizikovějším aspektům.

Již bylo také zmíněno, že pro usměrnění rozsahu auditu byla využita metodika COBIT, která je charakteristická tím, že dává do souladu podnikové procesy s informačními technologiemi. Metodika poskytuje metriky, na co se zaměřit, cíle a jak jich dosáhnout. Zároveň uvádí dále kontrolní cíle, které jsou podrobněji specifikovány v IT Assurance Guide, tam jsou uvedeny i rizikové faktory. Využití metodiky COBIT pro auditování informačního systému v ekonomickém prostředí lze hodnotit jako příhodné, a to i přesto, že byla použita pro auditování systému s nízkou úrovní propracovanosti a složitosti a nebylo tedy třeba využít její široký rozsah. Především její využití bylo efektivní z hlediska přesného vymezení, a tedy i auditování vybrané oblasti.

I Summary and keywords

The main aim of the master thesis is performing an audit of the ERP system SAP operated in an academic environment and determine, how the system is administrated by the academic organization.

The theoretical part contains specification of general audit and audit of information systems along with terms related. Furthermore, in the theoretical part, the master thesis contains general description of ERP systems and more detailed description of SAP organization and its products.

The practical part is focused on the selection of appropriate COBIT process and determining control objectives. Based on that, are performed tests with appropriate transaction codes and authorizations objects, gained by the literature and Repository information system. The outcomes of performed test should determine, how the organization is doing with security and administration of information system.

It turned out that the system is not so well secured and administered, mainly because each user has access to all risk areas. Based on that, some recommendation for ensure secure and well administered system were written.

Keywords: Audit, Information system, SAP, ERP, COBIT

II Seznam použitých zdrojů

ACCA Paper F8 Audit and Assurance. (2016). Berkshire: Kaplan Publishing UK

Deloitte Touche Tohmatsu Research Team, & ISACA. (2006). Security, Audit and Control Features SAP R/3: A Technical and Risk Management Reference Guide, 2nd Edition (2nd). Isaca.

Dvořáček, J. (2005). Audit podniku a jeho operací. C H Beck.

Müllerová, L., & Králíček, V. (2014). *Auditing* (1st ed.). Praha: Oeconomica.

Schreckenbach, S. (2011). SAP Administration – Practical Guide: Step-by-step instructions for running SAP Basis. SAP PRESS.

Svatá, V. (2018). *Audit informačního systému* (3rd ed.). Praha: Oeconomica.

Weill, P., & Ross, J. (June 1, 2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business Review Press.

Elektronické zdroje

ABAP Dictionary. Sap Help Portal. Retrieved July 30, 2020, from https://help.sap.com/doc/saphelp_nw73ehp1/7.31.19/en-US/cf/21ea0b446011d189700000e8322d00/frameset.htm

About SAP SE [Online]. Retrieved December 29, 2019, from https://www.sap.com/corporate/en/company.html

All Products [Online]. Retrieved December 29, 2019, from https://www.sap.com/products.html?infl=2c18272f-82ce-4991-b96f-0a262aa0c891

An Overview of Enterprise Resource Planning (ERP) [Online]. In sonu kumar. C.A. FINAL ISCA. Retrieved from http://www.retawprojects.com/uploads/An-Overview-Enterprise-Resource-Planning__ERP.pdf

COBIT 4.1 [Online]. (2007). IT Governance Institute. Retrieved from file:///C:/Users/Markéta/Desktop/JCU/diplomka/cobit.4.1.pdf

COBIT 5 (Control Objectives for Information and related Technology) [Online]. (c2016). Retrieved December 30, 2019, from https://managementmania.com/cs/cobit-control-objectives-for-information-and-related-technology

Cristescu, M. P., & Stancu, A. R. (2019). TRENDS IN AUDITING ERP SYSTEMS. Knowledge Horizons.Economics, 11(4), 46-53. Retrieved from https://search.proquest.com/docview/2343691801?accountid=9646

Drljača, D., & Latinović, B. (2016). FRAMEWORKS FOR AUDIT OF AN INFORMATION SYSTEM IN PRACTICE. *Jita*. https://doi.org/10.7251/JIT1602078D

Fišer, M. (2017). *Zabezpečení ERP SAP jako součást finančního auditu v prostředí velkých firem* [Diplomová práce]. Vysoká škola ekonomická v Praze.

Gantz, S. D. (2013). The basics of it audit : Purposes, processes, and practical information. Retrieved from https://search.proquest.com

GHEORGHE, M. Audit Methodology for IT Governance [Online]. *Informatica Economică*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.652.1508&rep=rep1&type=pdf

IT Assurance Guide: USING COBIT. (© 2007). The IT Governance Institute. https://csbweb01.uncw.edu/people/ivancevichd/classes/MSA%20516/Extra%20Readings%20on%20Topics/COBiT/IT%20Assurance%20Guide%20Using%20COBit.pdf

Information Systems Auditing: Tools and Techniques: Creating Audit Programs [Online]. (2016). Information Systems Audit and Control Association, Inc. (ISACA. Retrieved from https://www.isaca.org/COBIT/Documents/IS-auditing-creating-audit-programs_whp_eng_0316.pdf

Majdalawieh, M., & Zaghloul, I. (2009). Paradigm shift in information systems auditing. Managerial Auditing Journal, 24(4), 352-367. doi:http://dx.doi.org/10.1108/02686900910948198

SAP History [Online]. Retrieved December 29, 2019, from https://www.sap.com/corporate/en/company/history.html

SAP Query. Sap Help Portal. Retrieved July 30, 2020, from https://help.sap.com/viewer/40d2cb3a4f9249d58e9bbc95f4dbaff8/7.51.1/en-US

Sayana, S. A. (2002). The IS Audit Process [Online]. *Information Systems Control Journal, 1*. Retrieved from http://carl.sandiego.edu/ctu/IS_audit_process.pdf

Slooten, K. van, & Yap, L. (1999). *Implementing ERP Information Systems using SAP* [Online]. Retrieved from https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1438&context=amcis1999

Surjadi, J., Prabowo, H., Jap, T., & Agoes, S. (2015). Is there a correlation between ERP implementation, adherence to COSO and GCG implementation? *Journal Of Theoretical And Applied Information Technology*, (73), 283-289. https://www.researchgate.net/figure/The-COSO-Framework_fig2_281924044

Tables. Sap Help Portal. Retrieved July 30, 2020, from https://help.sap.com/doc/saphelp_nw73ehp1/7.31.19/en-US/cf/21ea43446011d189700000e8322d00/content.htm?no_cache=true

Tusheng, X., Chunxiao, G., & Chun, Y. (2020). How audit effort affects audit quality: An audit process and audit output perspective. China Journal Of Accounting Research, 109-127. https://doi.org/10.1016/j.cjar.2020.02.002

The System Log. Sap Help Portal. Retrieved July 30, 2020, from https://help.sap.com/viewer/12b9c3746c53101486a59afda7426260/7.0.37/en-US/c769bcbaf36611d3a6510000e835363f.html

van Slooten, Kees and Yap, Lidwien, "Implementing ERP Information Systems using SAP" (1999). AMCIS 1999 Proceedings. 81. http://aisel.aisnet.org/amcis1999/81

Yangyang, C., Gul, F. A., Truong, C., & Veeraraghavan, M. (2016). Auditor client specific knowledge and internal control weakness: Some evidence on the role of auditor tenure and geographic distance. Journal Of Contemporary Accounting & Economics, 121-140. https://doi.org/10.1016/j.jcae.2016.03.001

Wahab, I., & Arief, A. (2015). An integrative framework of COBIT and TOGAF for designing IT governance in local government, 36-40. https://doi.org/10.1109/ICITACEE.2015.7437766

Working with Transaction Codes. Sap Help Portal. Retrieved July 30, 2020, from https://help.sap.com/saphelp_nwmobile711/helpdata/en/f9/e1a442dc030e31e10000000a1550b0/content.htm?no_cache=tru

III Seznam tabulek

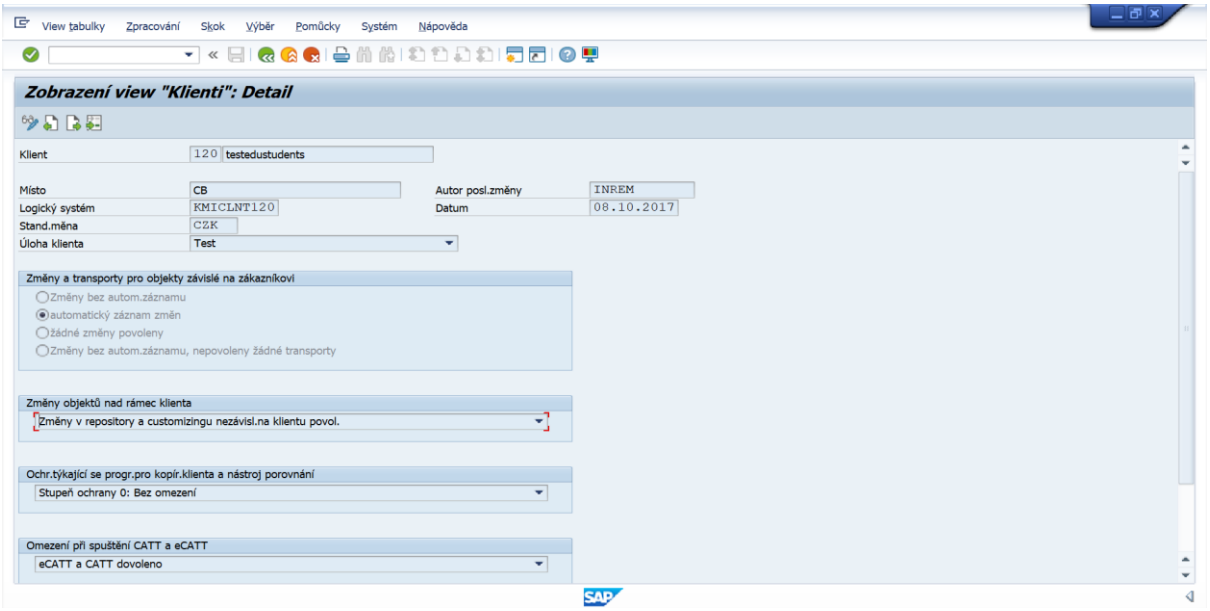
IV Seznam grafů

V Seznam obrázků

VI Seznam příloh

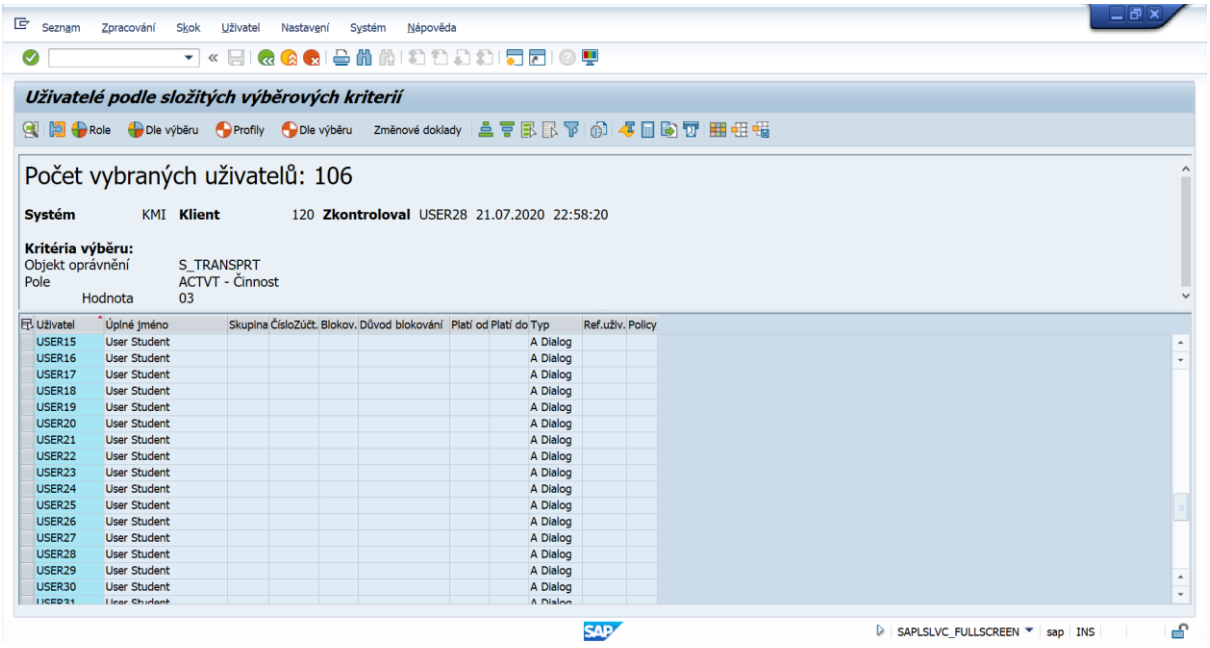
VII Přílohy

Příloha 1: Zobrazení detailu klienta



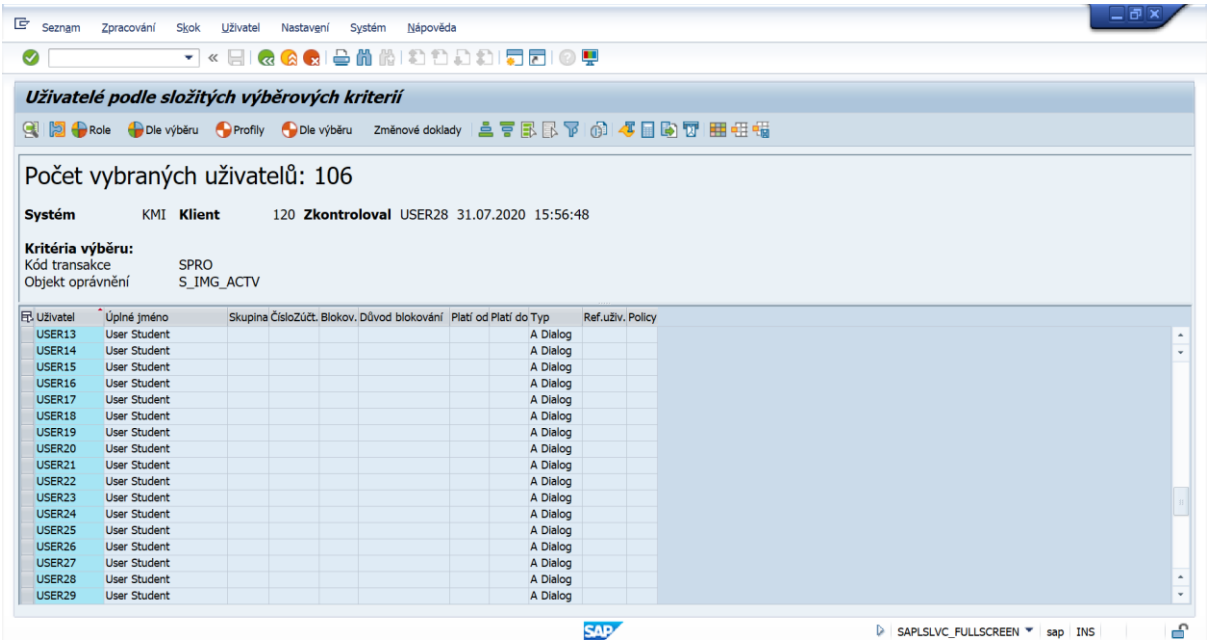
Zdroj: Vlastní zpracování

Příloha 2: Přístup k autorizačnímu objektu S_TRANSPRT pro IMG



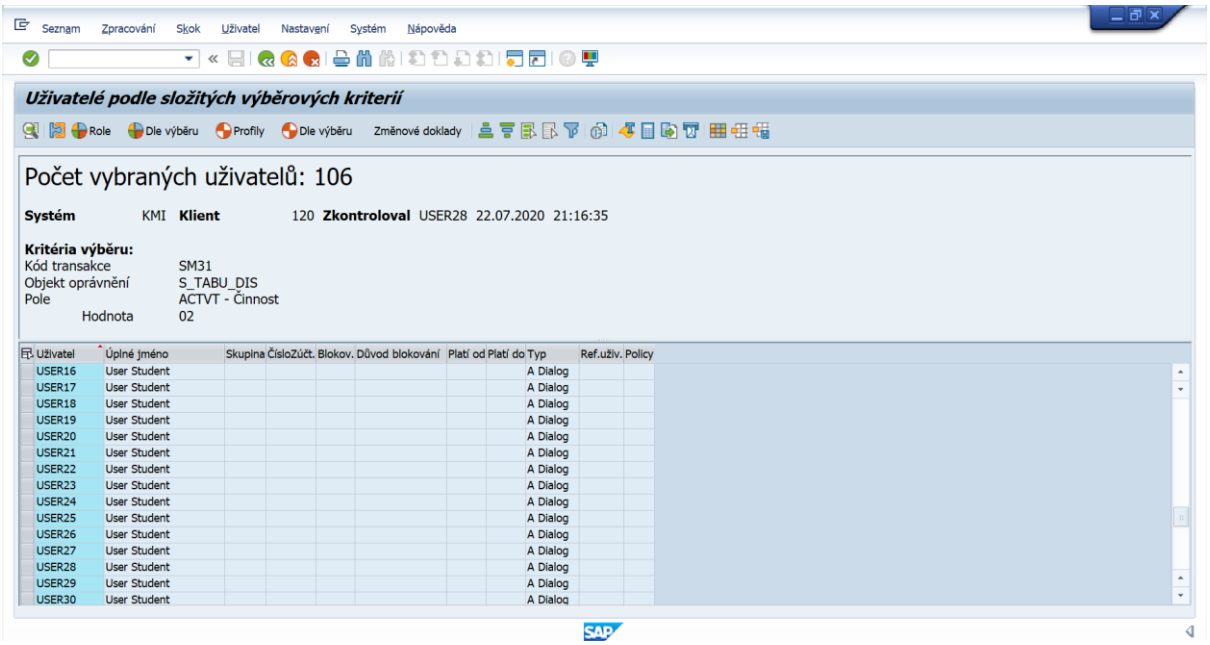
Zdroj: Vlastní zpracování

Příloha 3: Přístup k autorizačnímu objektu S_IMG_ACTV pro IMG



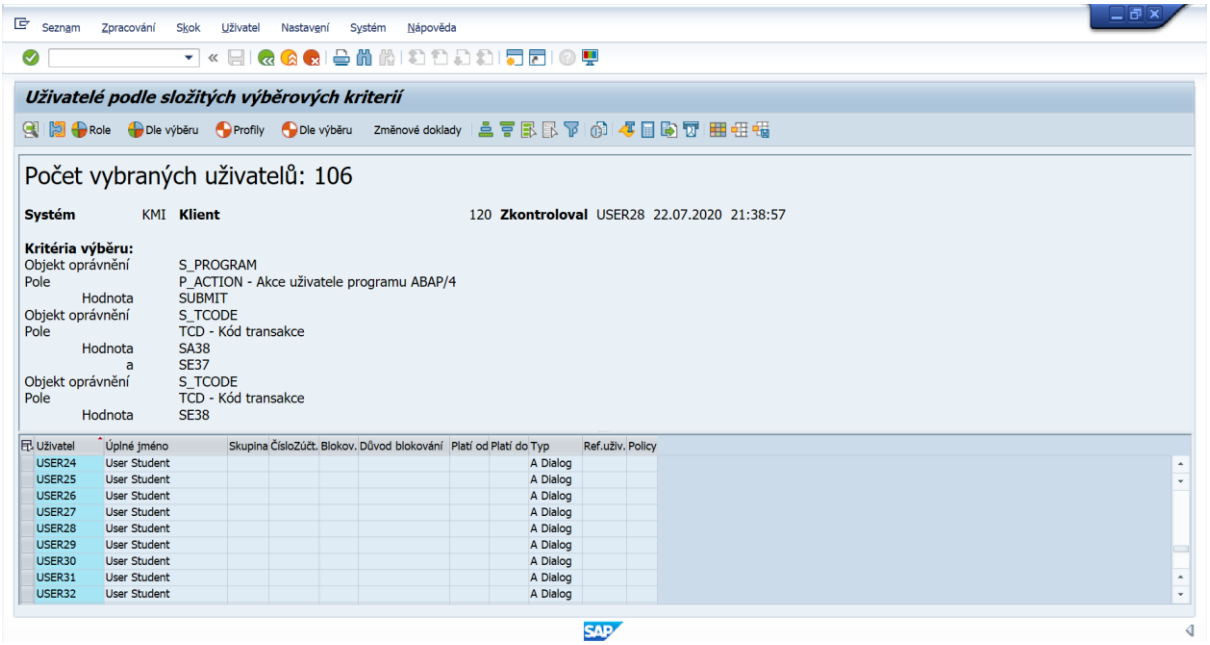
Zdroj: Vlastní zpracování

Příloha 4: Přístup k transakčnímu kódu SM31 pro úpravu tabulek



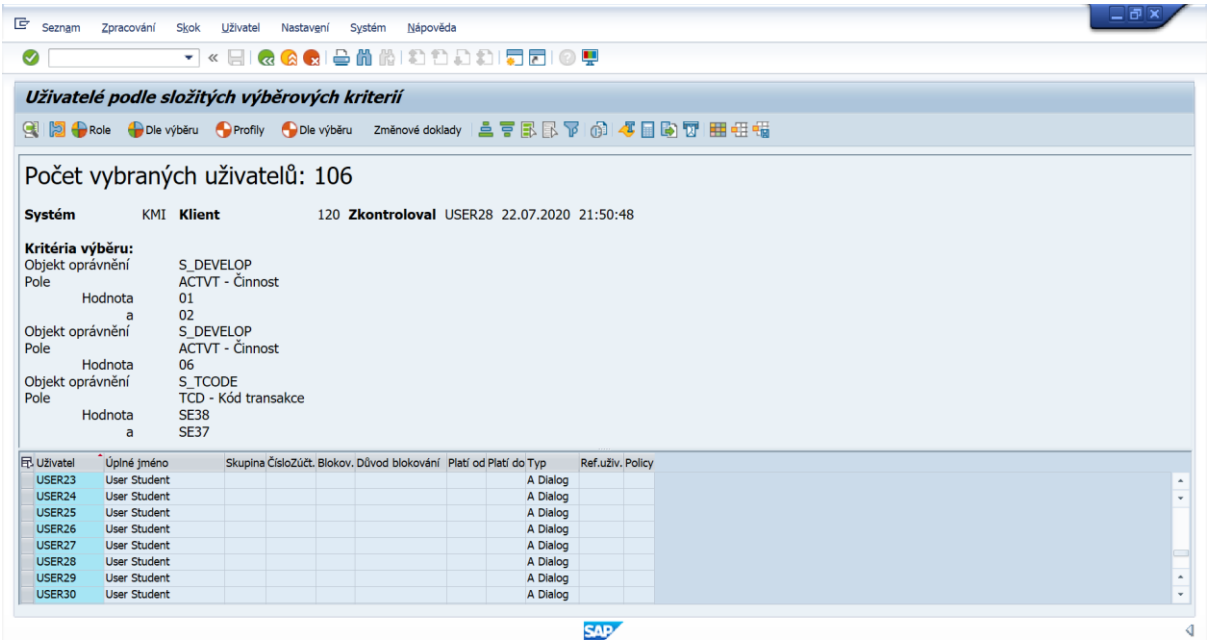
Zdroj: Vlastní zpracování

Příloha 5: Přístup k přizpůsobení programů ABAP



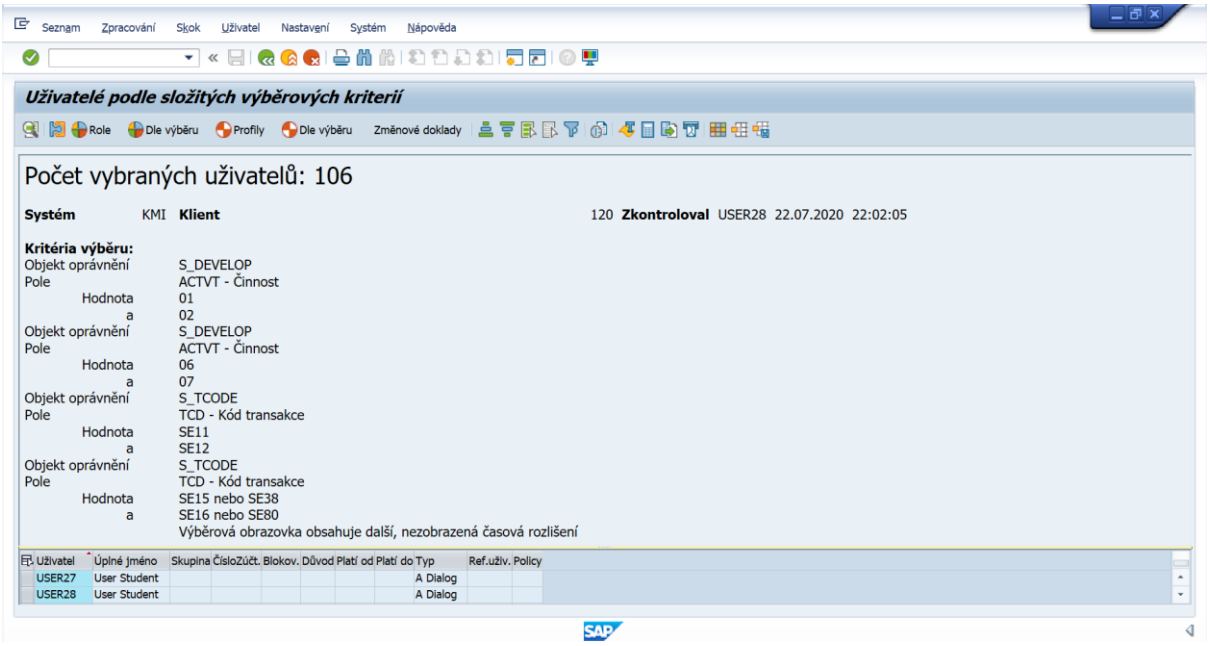
Zdroj: Vlastní zpracování

Příloha 6: Přístup k vývoji ABAP



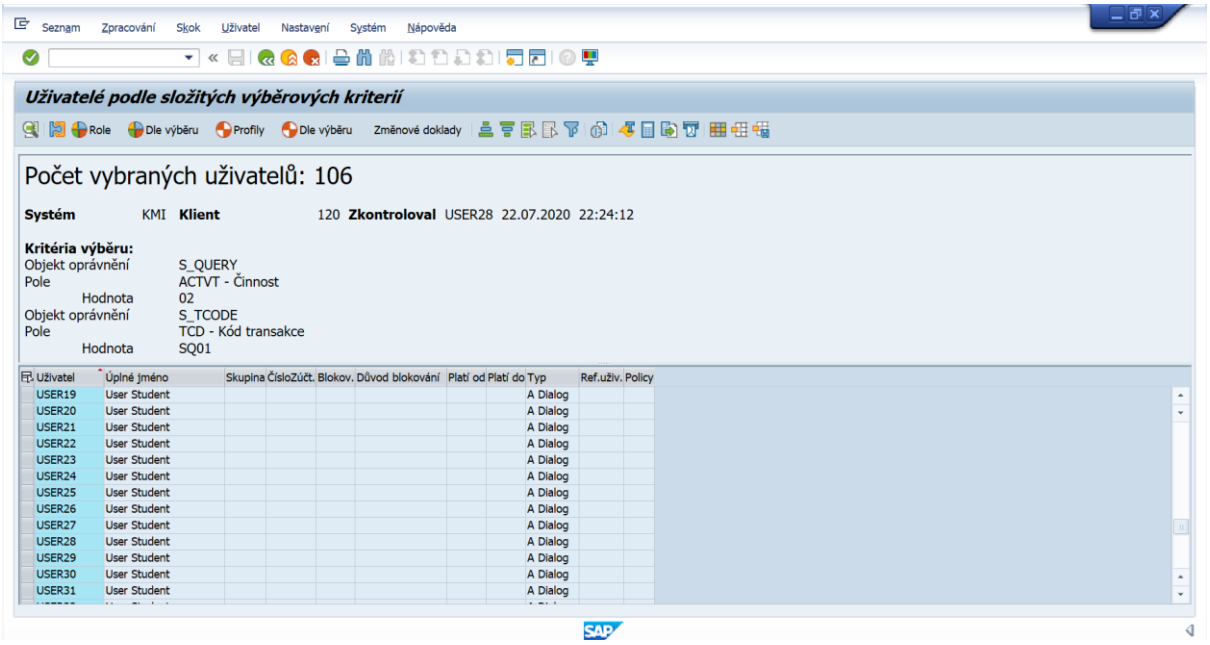
Zdroj: Vlastní zpracování

Příloha 7: Přístup k datovému slovníku ABAP



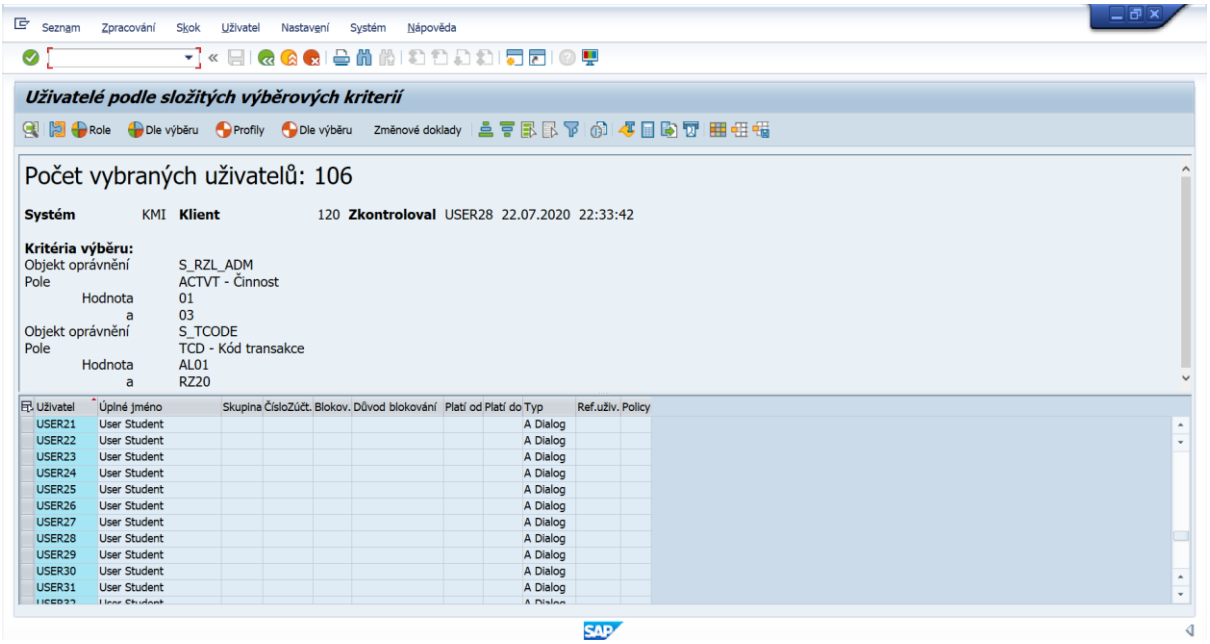
Zdroj: Vlastní zpracování

Příloha 8: Přístup k dotazům



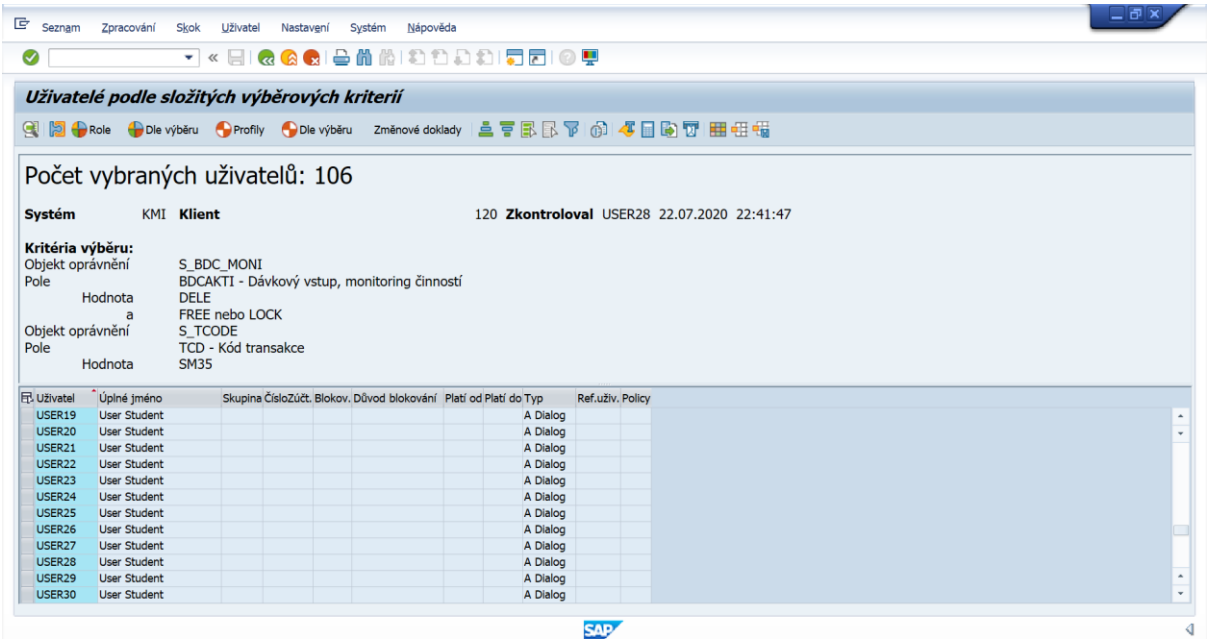
Zdroj: Vlastní zpracování

Příloha 9: Přístup ke konfiguraci CCMS



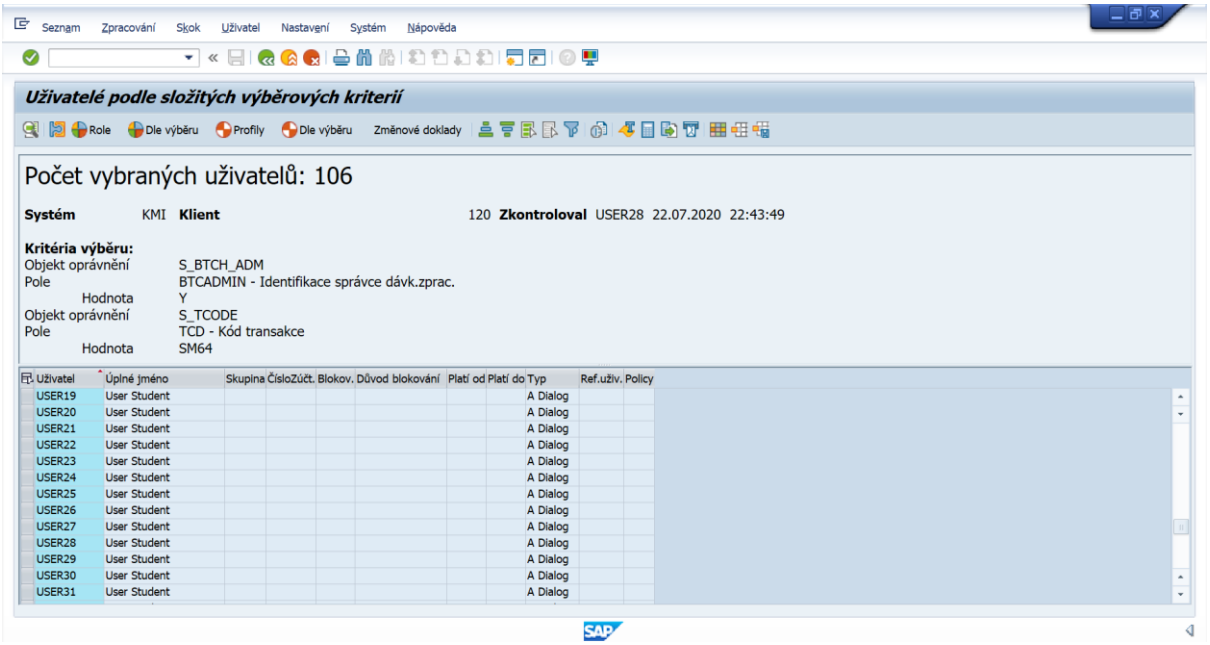
Zdroj: Vlastní zpracování

Příloha 10: Přístup k transakčnímu kódu SM35 pro dávkové zpracování



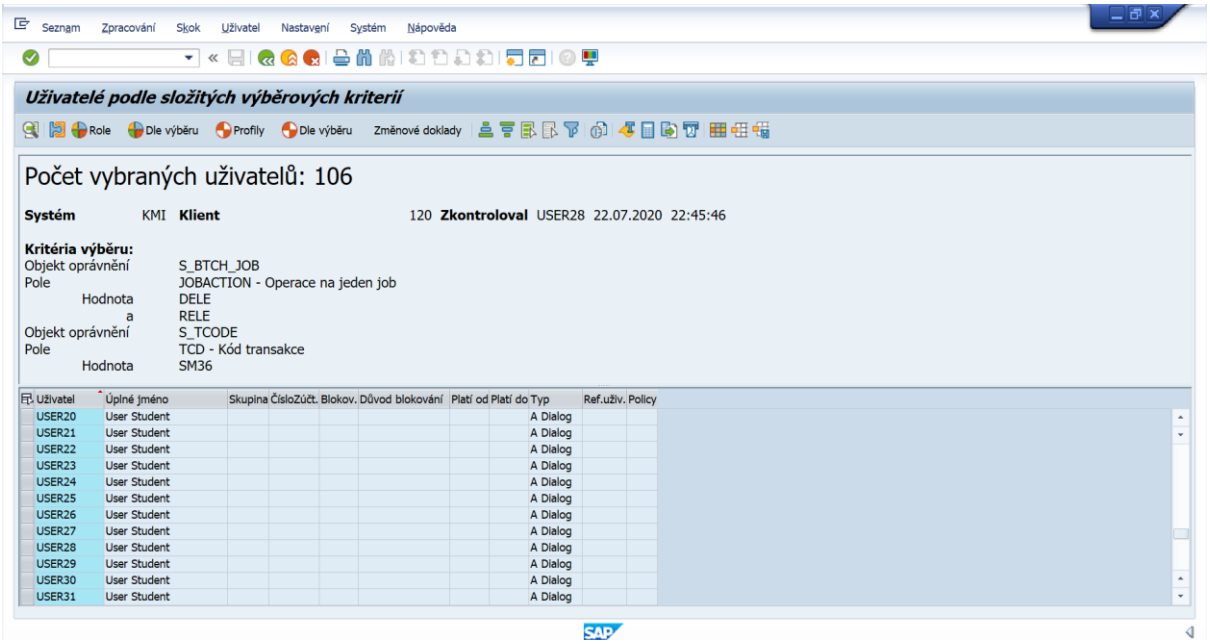
Zdroj: Vlastní zpracování

Příloha 11: Přístup k transakčnímu kódu SM64 pro dávkové zpracování



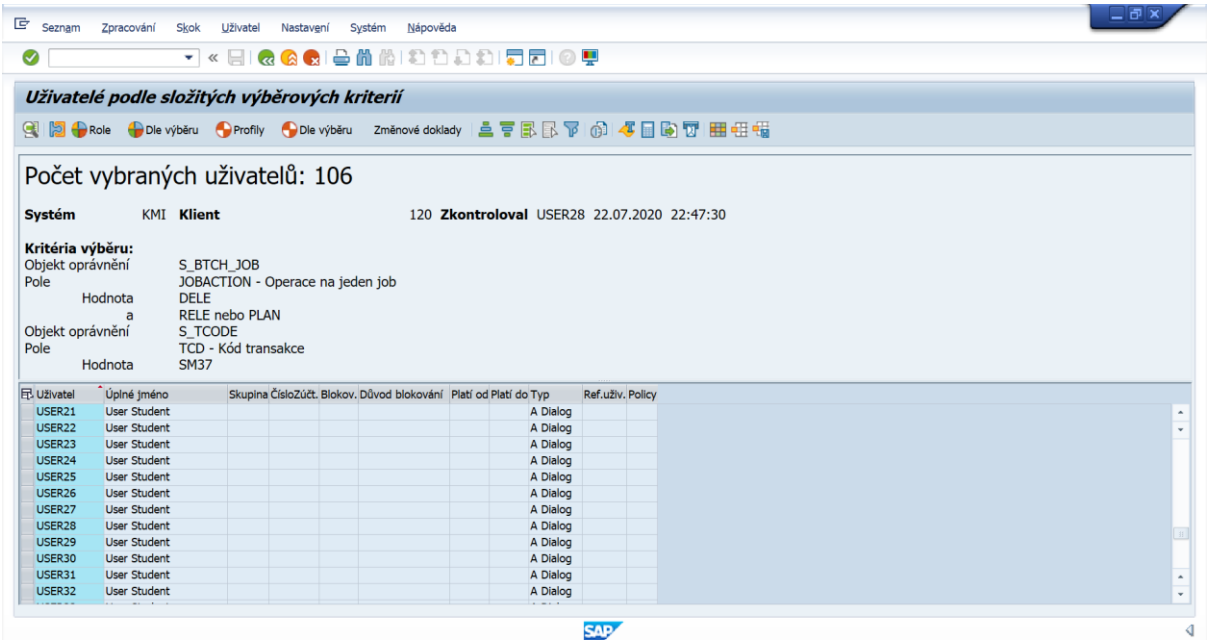
Zdroj: Vlastní zpracování

Příloha 12: Přístup k transakčnímu kódu SM36 pro dávkové zpracování



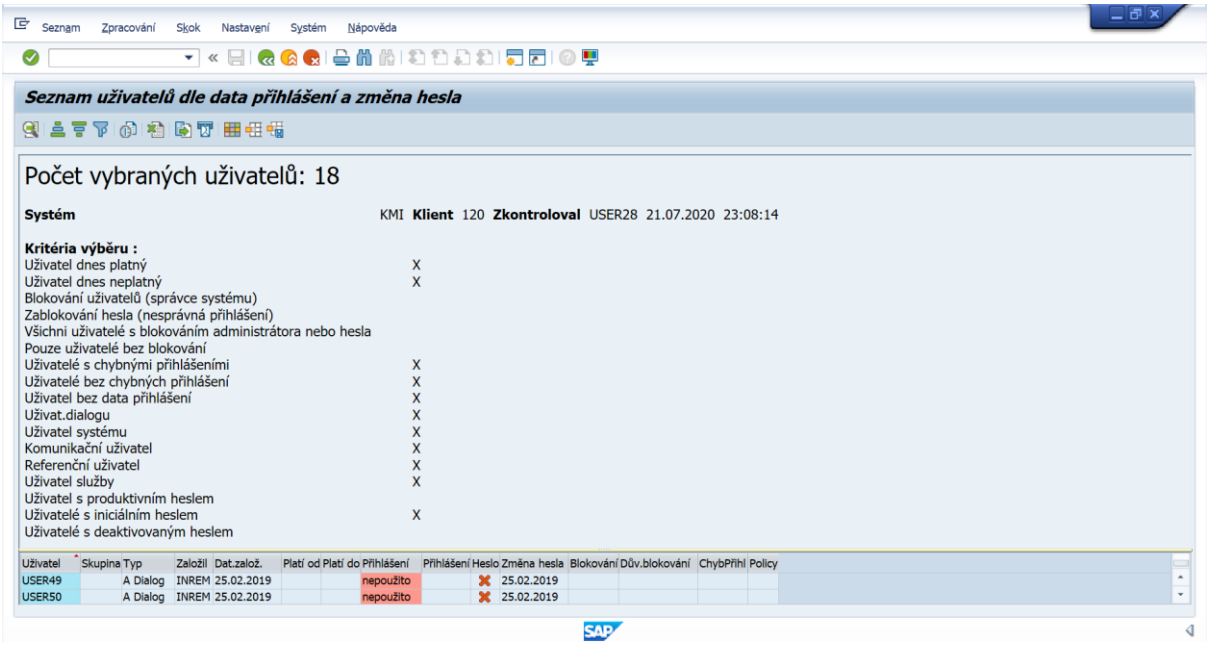
Zdroj: Vlastní zpracování

Příloha 13: Přístup k transakčnímu kódu SM37 pro dávkové zpracování



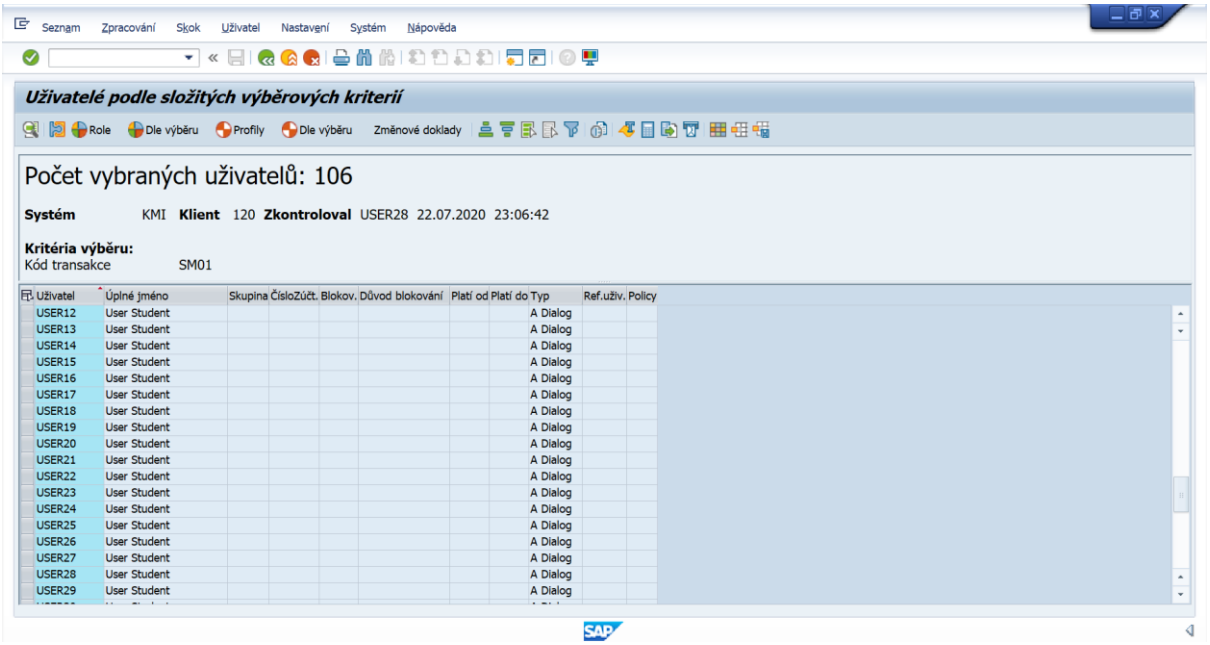
Zdroj: Vlastní zpracování

Příloha 14: Nepřihlášení uživatelé



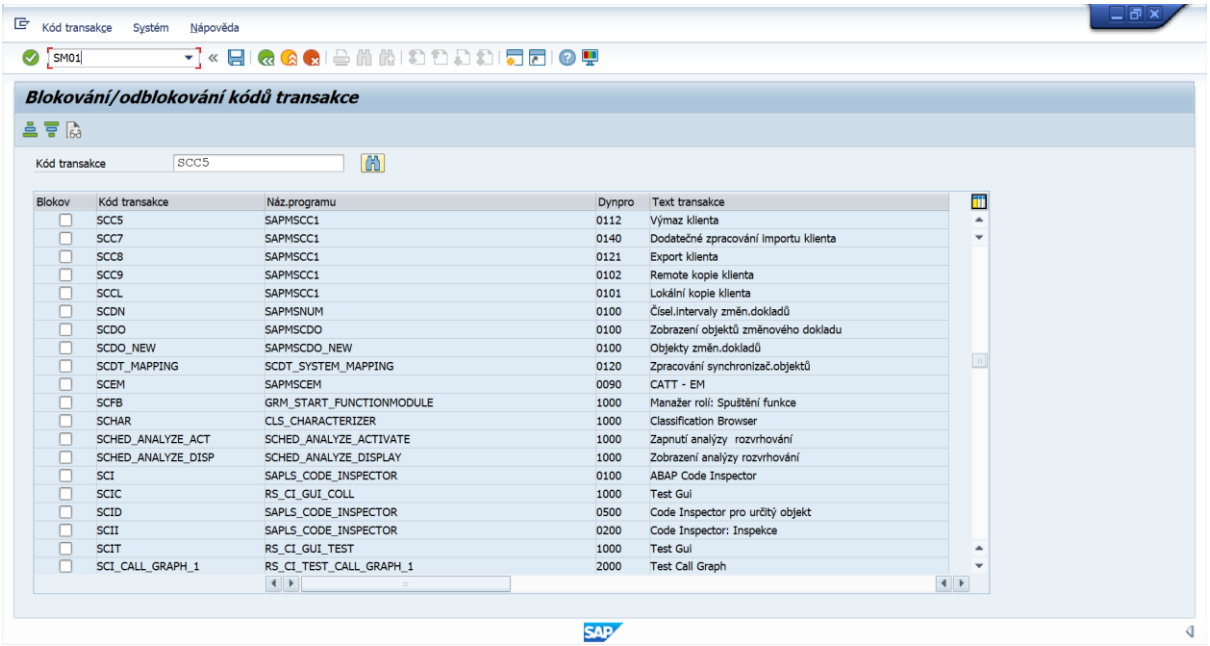
Zdroj: Vlastní zpracování

Příloha 15: Přístup k transakčnímu kódu SM01 pro uzamčení kódů



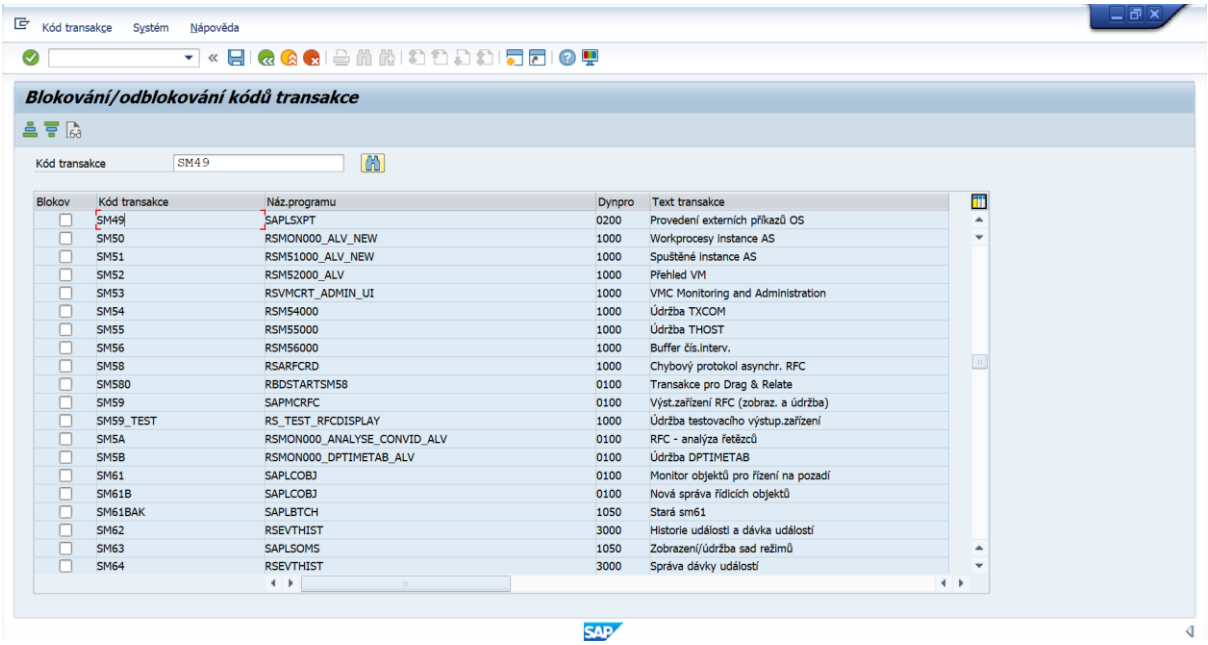
Zdroj: Vlastní zpracování

Příloha 16: Uzamčení kódu SCC5



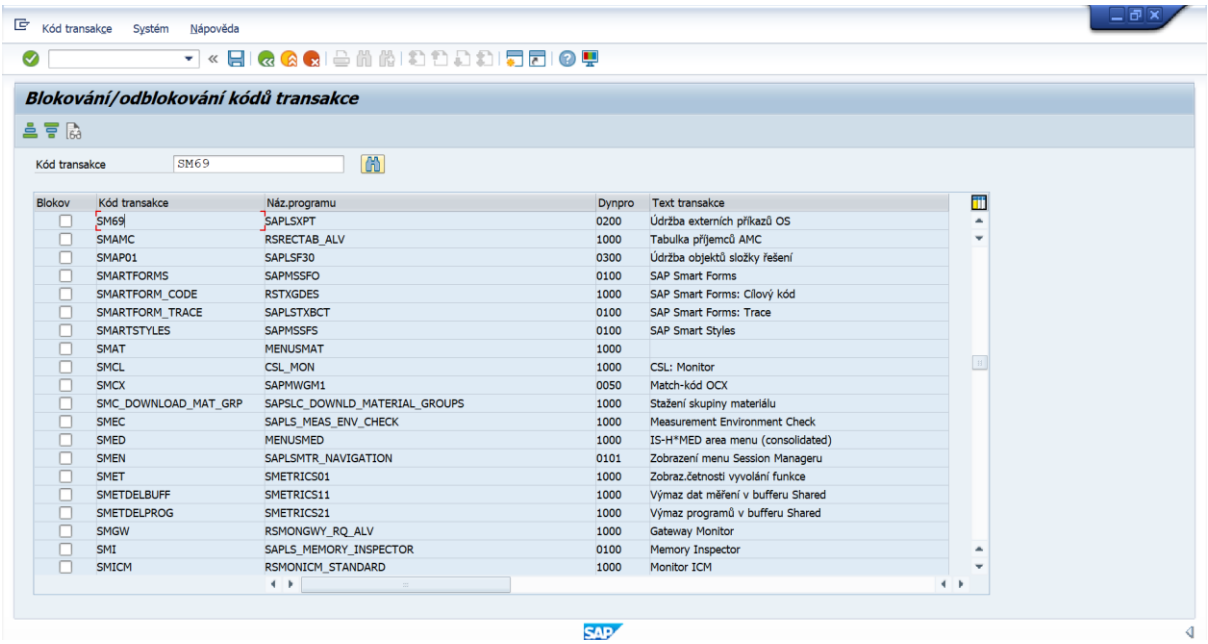
Zdroj: Vlastní zpracování

Příloha 17: Uzamčení kódu SM49



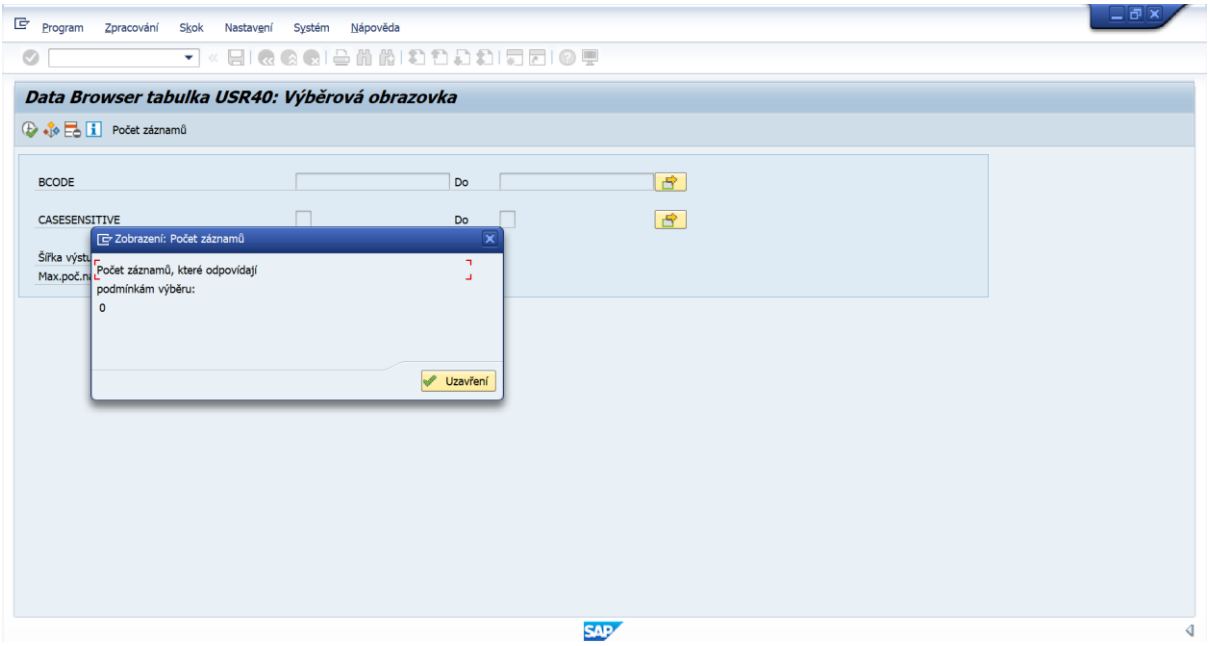
Zdroj: Vlastní zpracování

Příloha 18: Uzamčení kódu SM69



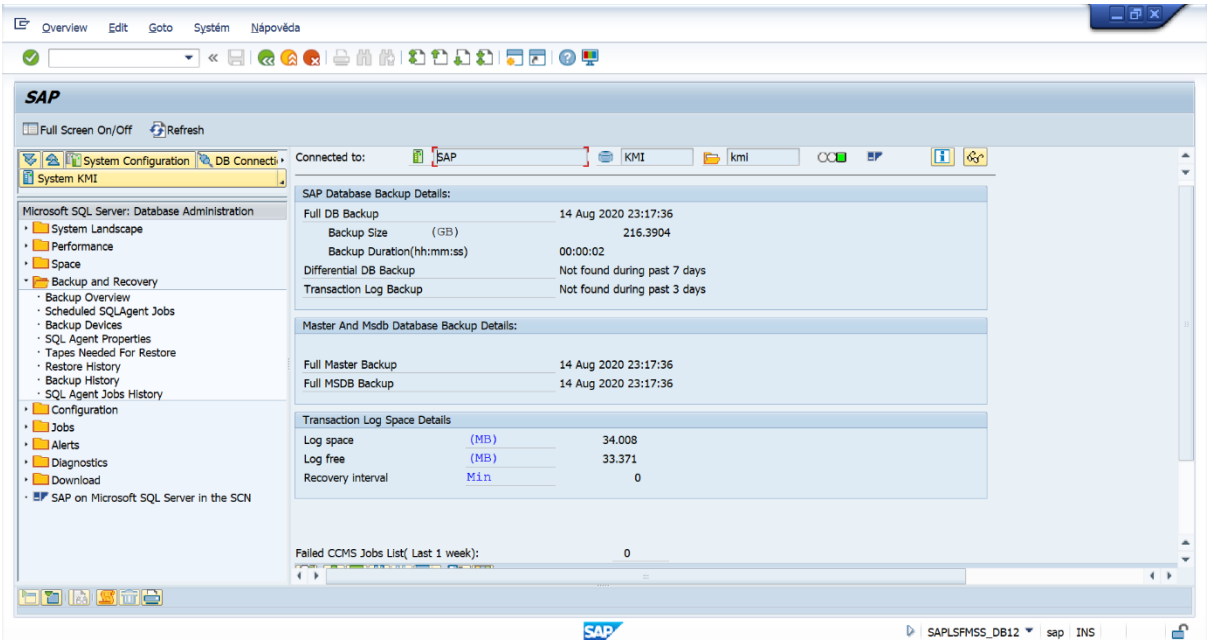
Zdroj: Vlastní zpracování

Příloha 19: Nepovolená hesla



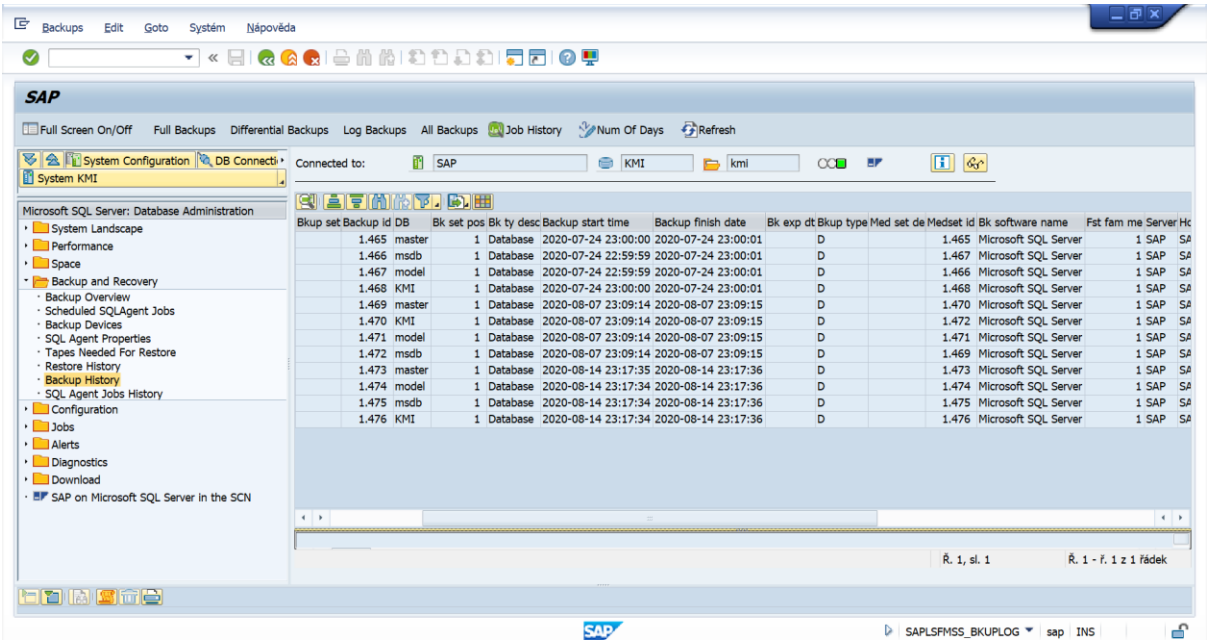
Zdroj: Vlastní zpracování

Příloha 20: Poslední zaznamenána záloha



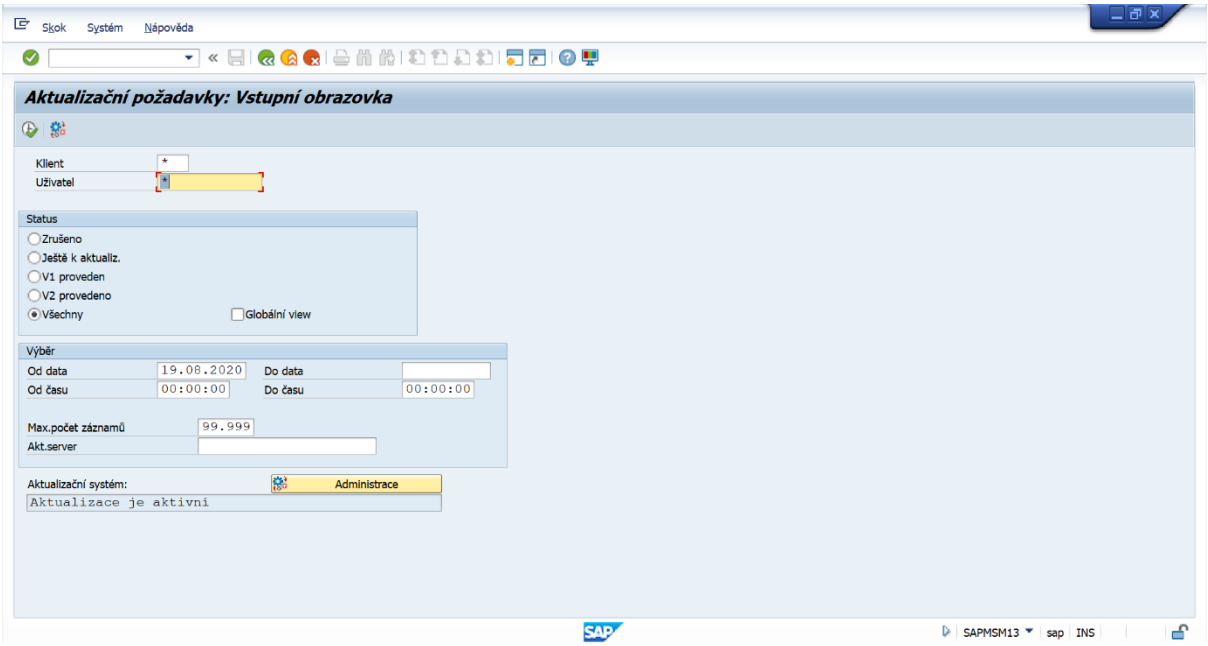
Zdroj: Vlastní zpracování

Příloha 21: Četnost zálohování za posledních 30 dní



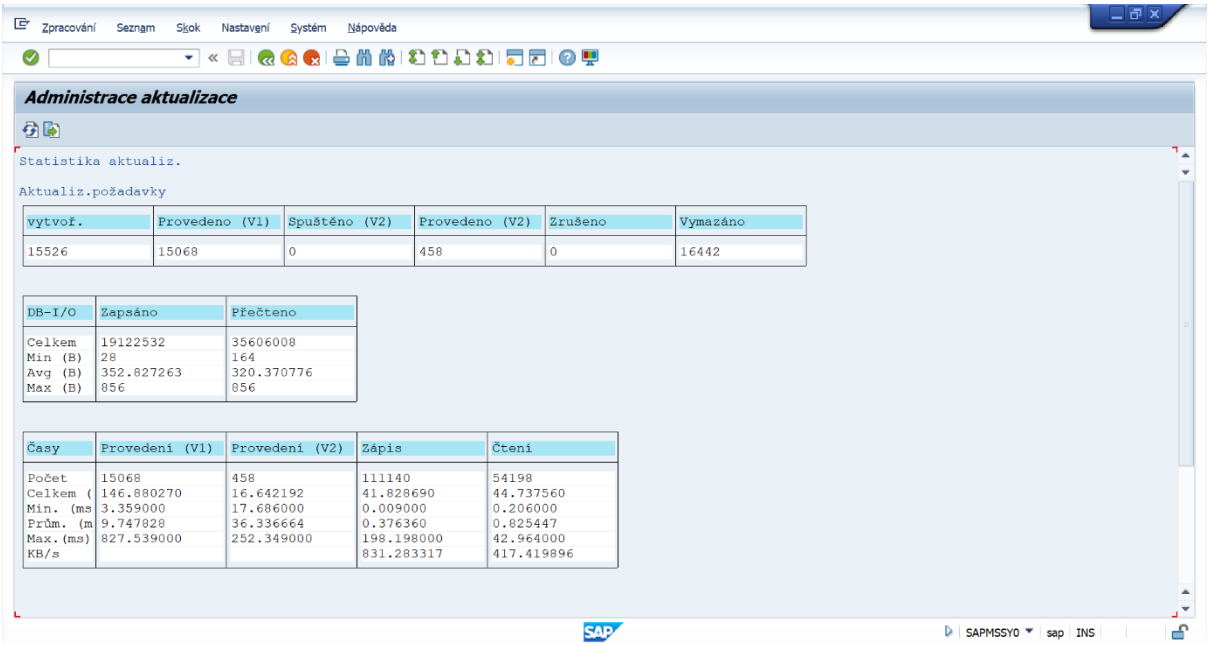
Zdroj: Vlastní zpracování

Příloha 22: Zjištění aktualizace systému



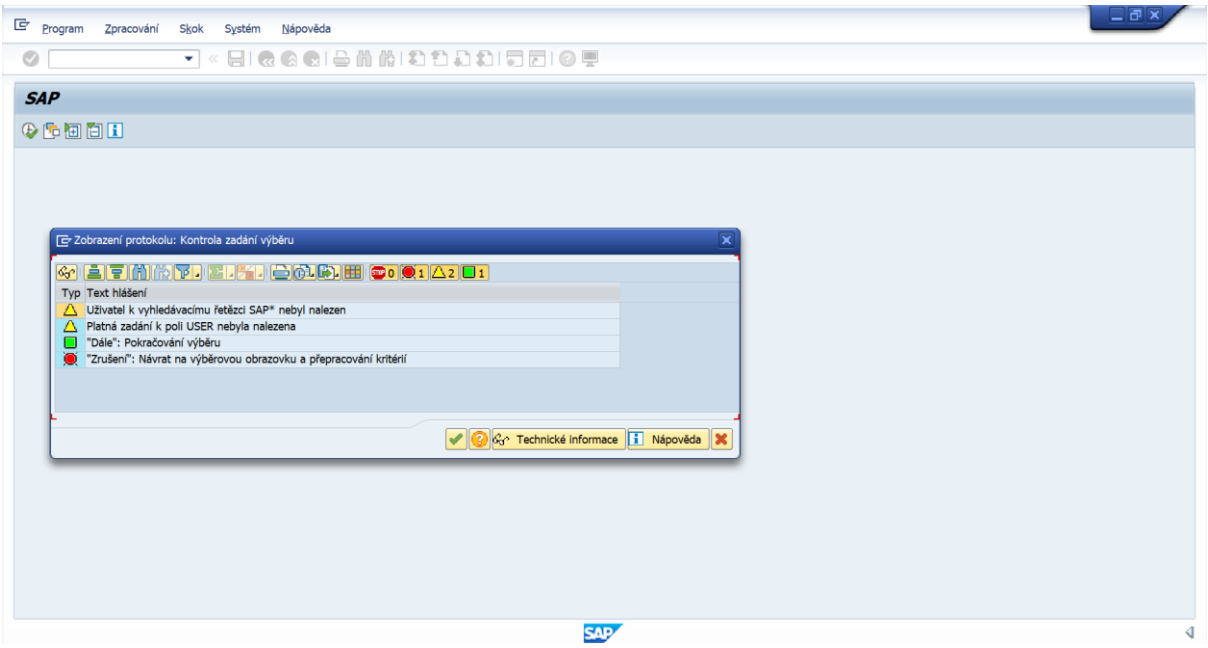
Zdroj: Vlastní zpracování

Příloha 23: Počet aktualizačních požadavků



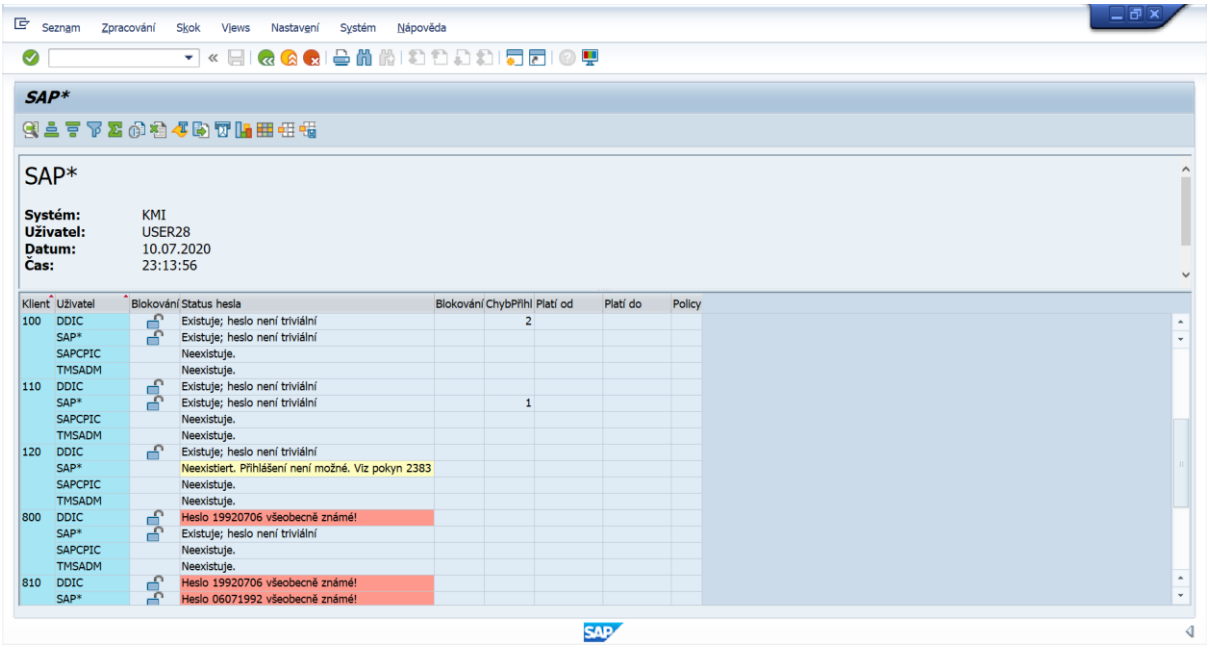
Zdroj: Vlastní zpracování

*Příloha 24: Nastavení klienta SAP**



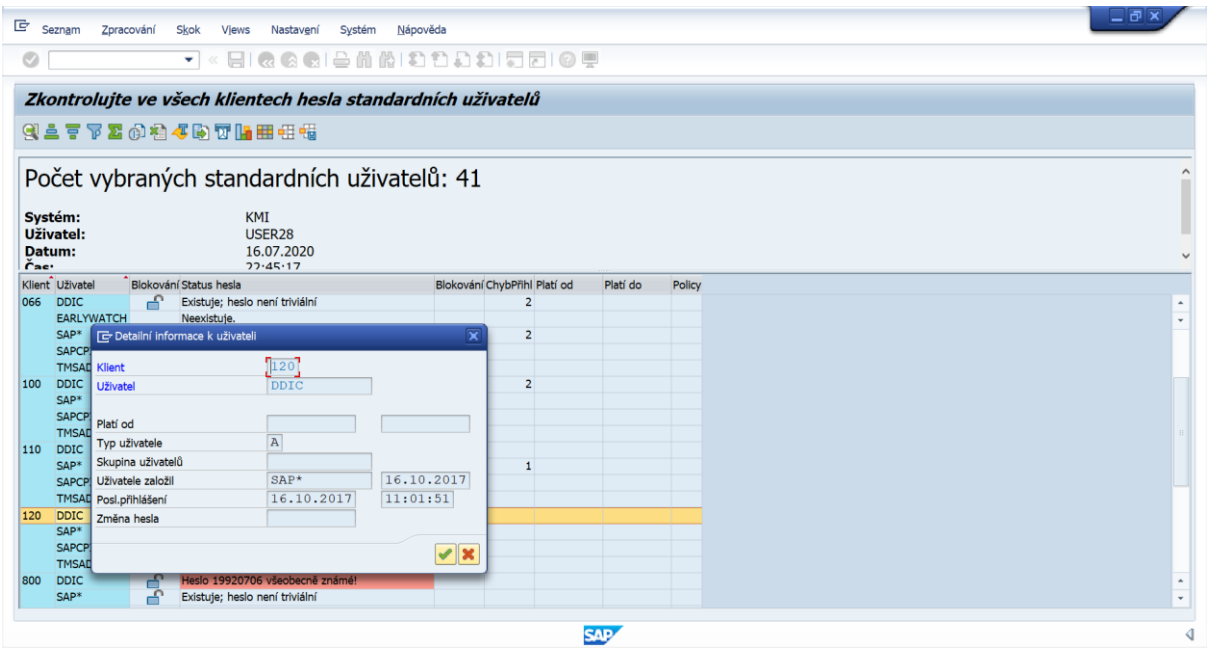
Zdroj: Vlastní zpracování

Příloha 25: Uživatelé definovaní systémem



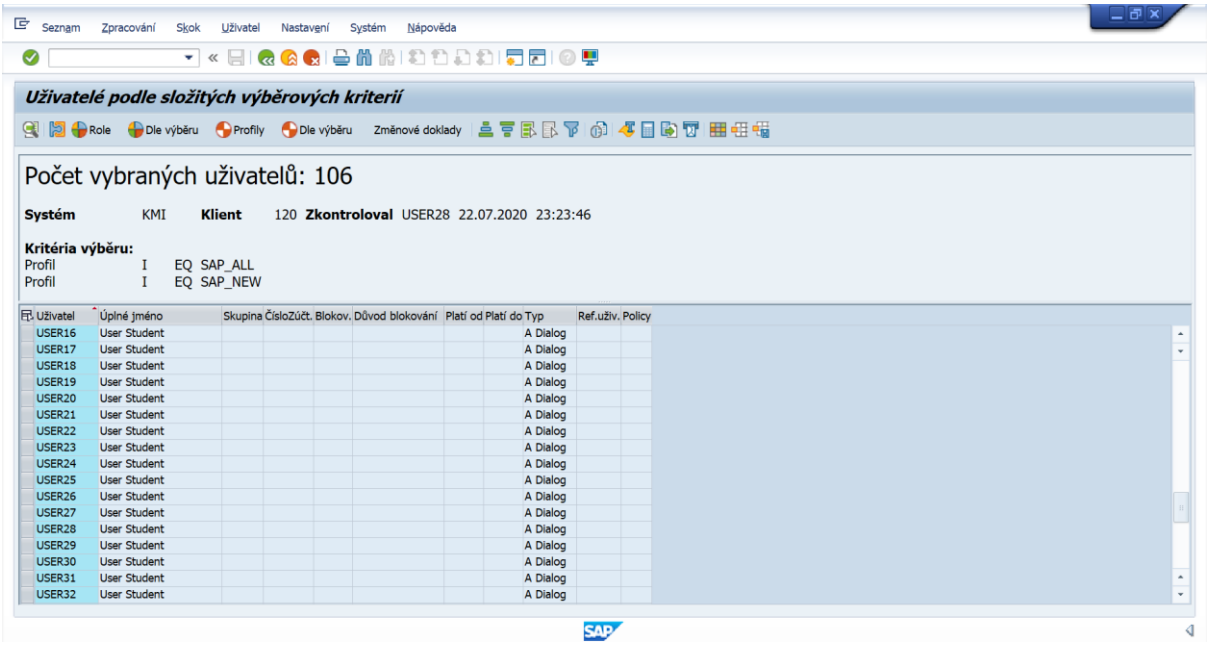
Zdroj: Vlastní zpracování

Příloha 26: Detail uživatele DDIC



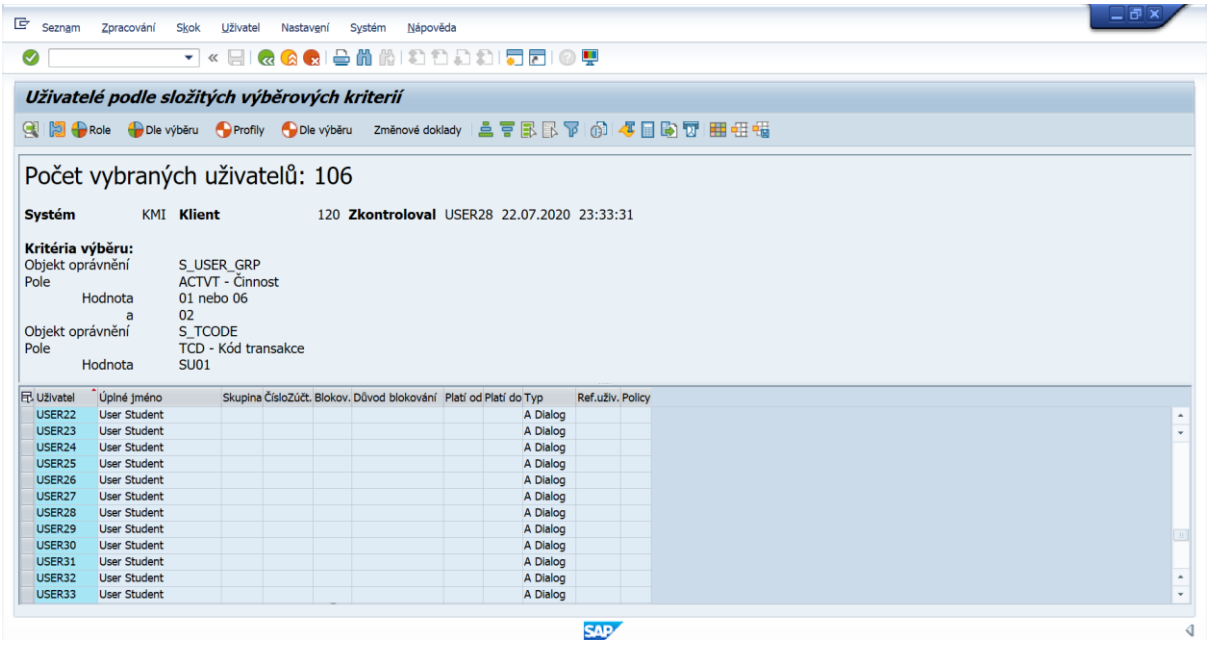
Zdroj: Vlastní zpracování

Příloha 27: Přiřazení k výkonným profilům



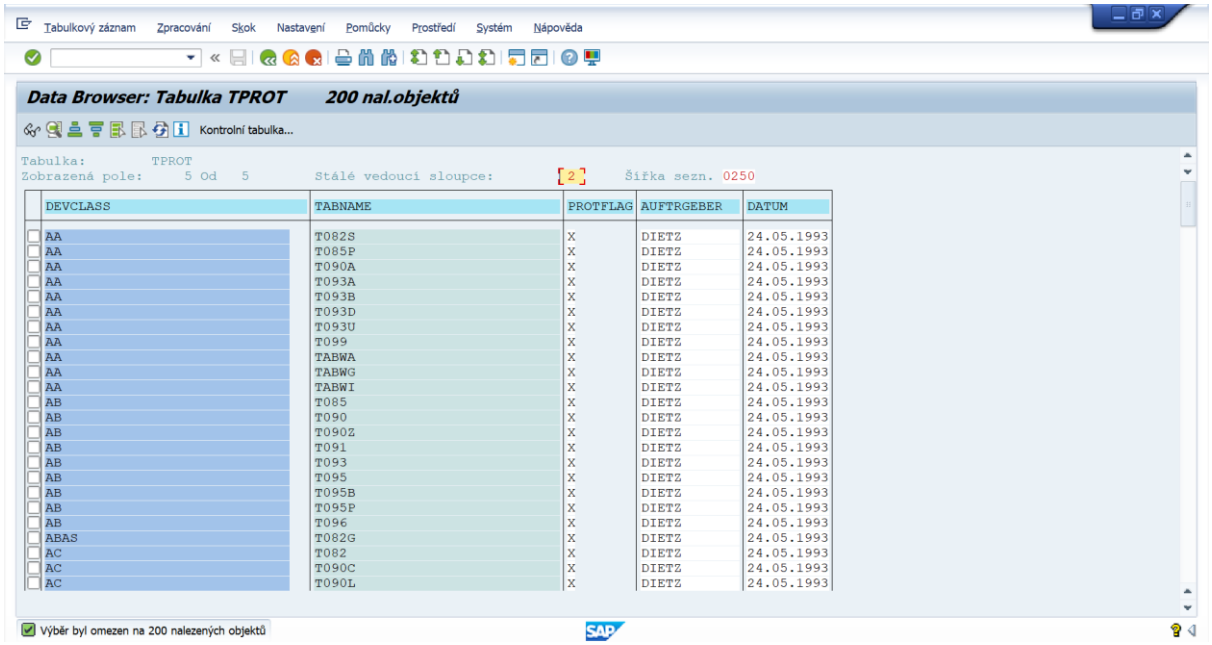
Zdroj: Vlastní zpracování

Příloha 28: Přístup k transakčnímu kódu SU01 pro výkonné skupiny



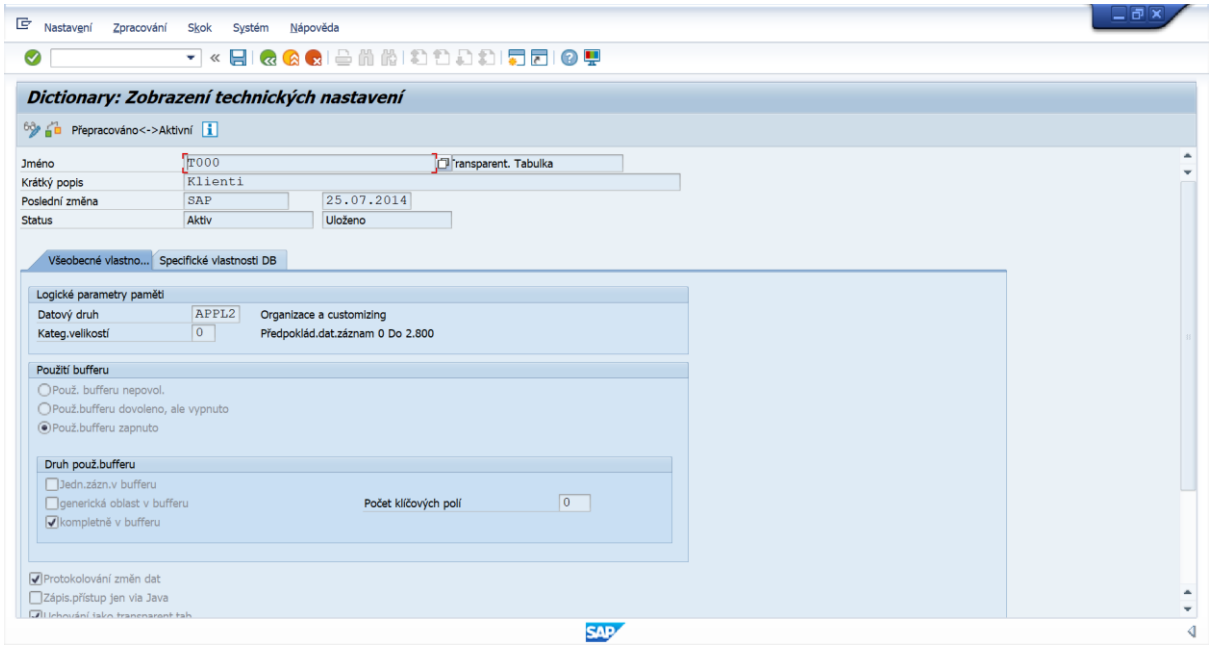
Zdroj: Vlastní zpracování

Příloha 29: Seznam tabulek pro protokolování



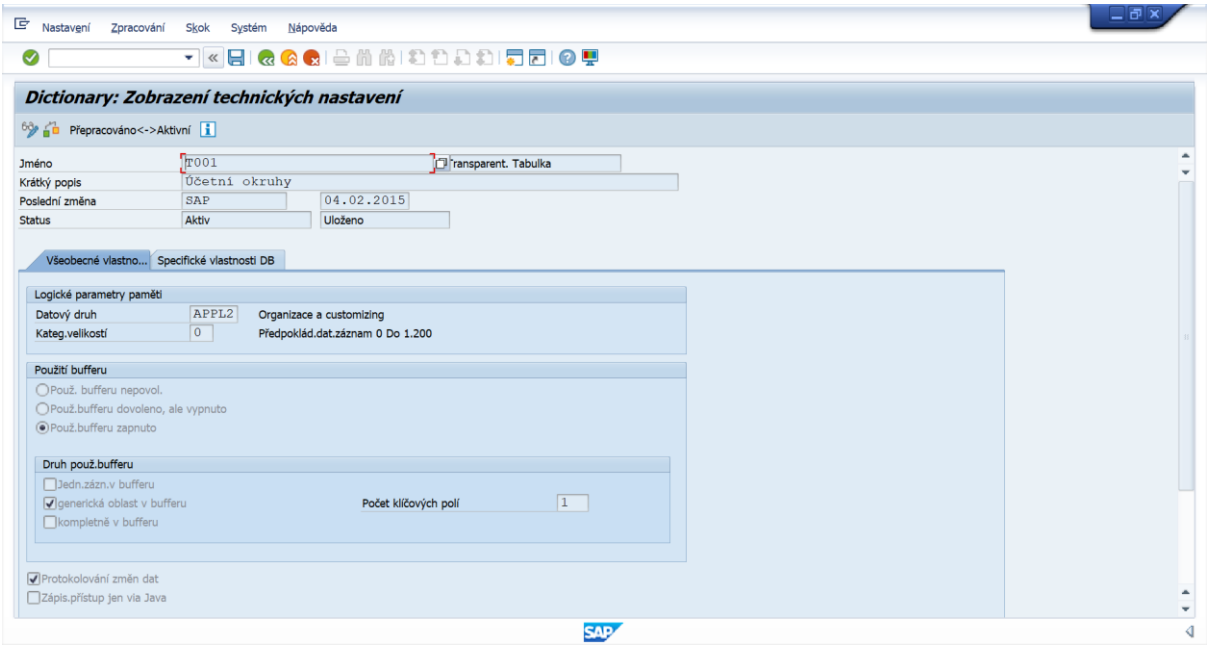
Zdroj: Vlastní zpracování

Příloha 30: Protokolování tabulky T000



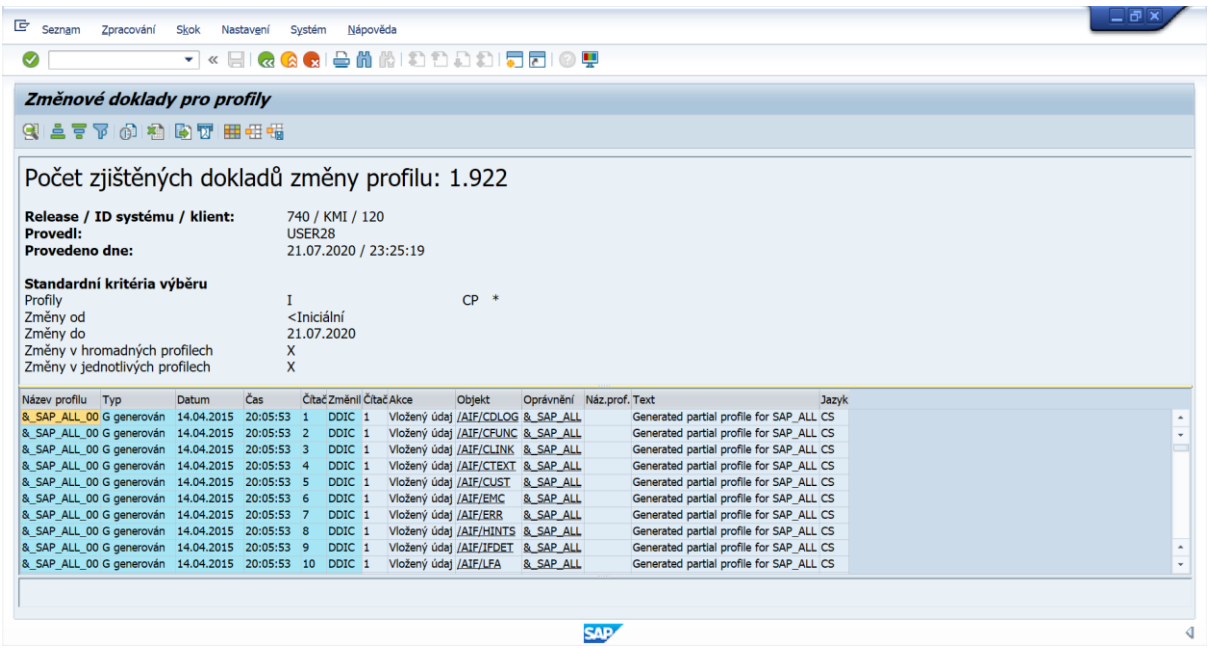
Zdroj: Vlastní zpracování

Příloha 31: Protokolování tabulky T001



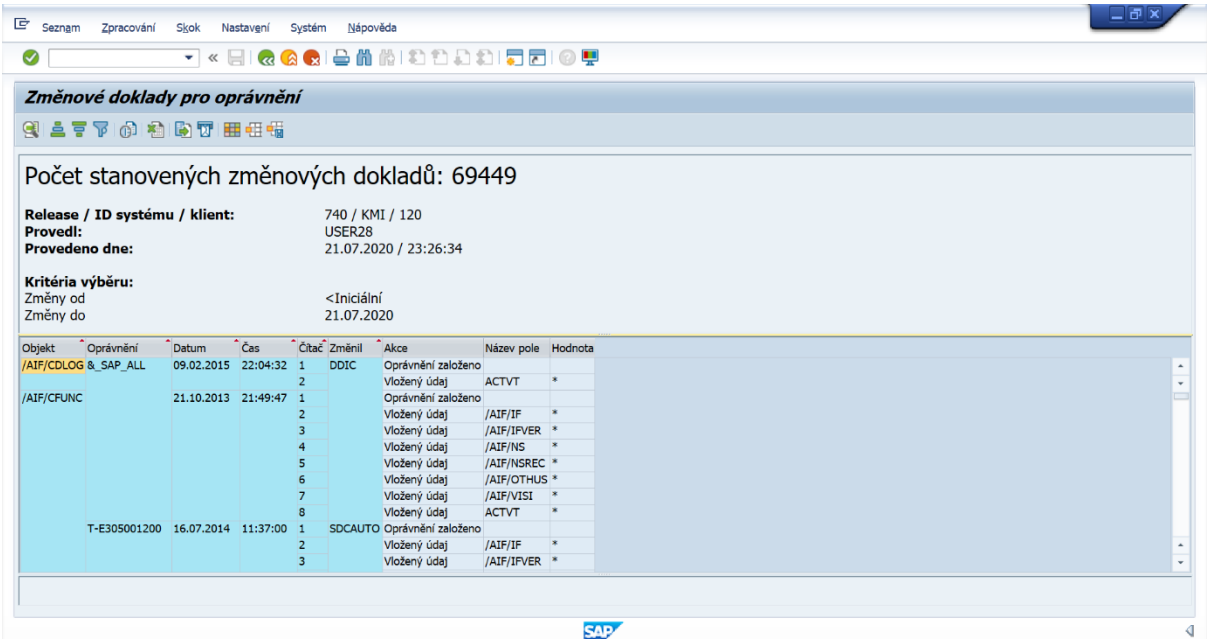
Zdroj: Vlastní zpracování

Příloha 32: Doklady změny profilů



Zdroj: Vlastní zpracování

Příloha 33: Změnové doklady



Objekt	Oprávnění	Datum	Čas	Čítač	Změnil	Akce	Název pole	Hodnota
/AIF/CDLOG	&_SAP_ALL	09.02.2015	22:04:32	1	DDIC	Oprávnění založeno		
				2		Vložený údaj	ACTVT	*
/AIF/CFUNC		21.10.2013	21:49:47	1		Oprávnění založeno		
				2		Vložený údaj	/AIF/IF	*
				3		Vložený údaj	/AIF/IFVER	*
				4		Vložený údaj	/AIF/NS	*
				5		Vložený údaj	/AIF/NSREC	*
				6		Vložený údaj	/AIF/OTHUS	*
				7		Vložený údaj	/AIF/VISI	*
				8		Vložený údaj	ACTVT	*
	T-E305001200	16.07.2014	11:37:00	1	SDCAUTO	Oprávnění založeno		
				2		Vložený údaj	/AIF/IF	*
				3		Vložený údaj	/AIF/IFVER	*

Zdroj: Vlastní zpracování